UDC 004.93

DETECTING OBJECTS MOVING IN SPACE FROM A MOBILE VISION SYSTEM

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.

Matiushin I. S. – Student of the Information Security Department, Southwest State University, Kursk, Russian Federation.

ABSTRACT

Context. In the study, the task of identifying objects moving in space from a mobile system of technical vision is considered. The analysis of the modern methods of dynamic object identification from both stationary and moving platforms is conducted. The need to create a new method for the identification of dynamic objects with a mobile optical-electronic system, which is adaptive to changing observation conditions, is identified. This is a relevant scientific and technical problem. The object of the study is the model of moving object detection from a mobile vision system.

Objective. The objective of this article is the analysis of the modern methods of moving object identification and the creation of a new method. The method must allow observation from a mobile vision system and must be able to adapt to changing observation conditions.

Method. A method for identifying objects moving in space from a mobile vision system is proposed, which allows to automatically detect moving objects, determine their three-dimensional coordinates with a given accuracy, and adapt to changing observation conditions. This method is based on the developed mathematical model of stereoscopic determination of motion parameters of objects in space, which allows us to increase the detection accuracy.

Results. The proposed method is implemented in software. An experiment confirming the adequacy of this mathematical model was conducted. As the result of the experiment, data on the movement of the object and the mobile coordinate system were obtained.

Conclusions. The experiments have confirmed the performance of the proposed method and allow us to recommend it when building mobile automatic tracking and identification systems for objects. The method allows automatic isolation of the moving objects, determining their three-dimensional coordinates, and adapting to changing observation conditions. Prospects for further research may be in the creation of hardware tools for the selection of moving objects, allowing to improve the accuracy of the selection.

KEYWORDS: moving object detection, vision systems, object detection method, mobile systems.

NOMENCLATURE

E_i is contour energy;

α, β are constants that provide relative energy correction;

$E_{int}(v_i)$ is an energy function depending on the shape of the contour;

$E_{ext}(v_i)$ is the energy function depending on the properties of the image and the type of gradient in the neighborhood of the point vi;

α_d, α_u, α_v are threshold constants;

u_p, v_p are velocity components of point p in coordinates (x_p, y_p);

E is a given non-negative threshold;

A is the set non-negative angular threshold;

H is the maximum level of brightness in the image;

$f(p)$, $f(q)$ are the brightness of the pixels p and q, respectively;

$P(X, Y, Z)$ is a point of the object in three-dimensional space;

F is the focal length of the lens;

B is the distance between the optical axes;

Dispar is disparity;

Z is an unknown parameter;

$(\Delta X, \Delta Y, \Delta Z)$ is the direction of movement of the observation system relative to the environment;

(k_x, k_y) is the direction of the gradient vector;

X_n is the normal flow vector;

$0x_0y_0z_0$ is the coordinate system associated with the movable base of the optical device;

ψ, υ, γ, σ, φ are angles;

ω_{x0}, ω_{y0}, ω_{z0} are angular velocities;

$O'x_py_pz_p$ is the coordinate system associated with the vision system.

INTRODUCTION

Due to the intensifying implementation of vision systems in the industry, the developments connected with the visual perception of moving objects are relevant [1]. An important task in this field is the detection of objects moving in space. Another reason why the task of the detection of the moving objects is interesting and significant is the possibility of the wide use of the method in systems of robotic vision technologies [2].

If a vision system is stationary, and the object is moving relative to it and enters its field of vision, the task of object selection is narrowed down to the analysis of a sequence of images and the detection of changes [3]. A more complicated situation is the case of a dynamic vision system, when not only there is a movement of the target object, but also a movement of the observation system relative to the surrounding environment. Therefore, even the static parts of the scene are subject to dynamic changes depending on the movement of the observation system. Dynamic vision systems are of the

DOI 10.15588/1607-3274-2019-4-10

greatest interest since it is possible to use them in mobile observation systems [4].

The object of the research is the model of moving object detection from a mobile vision system.

The subject of the research is the methods of separation of objects moving in space.

The aim of the work is to analyze the modern methods of identifying objects moving in space and to create a method that allows observing from a mobile vision system that is adaptive to changing observation conditions.

1 PROBLEM STATEMENT

A stereo image includes two separate types of the imaged object. It is required to determine the coordinates (X, Y, Z) of the point P, given by the projections p (x_1, y_1) and p (x_2, y_2) of its image on the matrix photodetectors of image sensors.

Let us consider in more detail the coordinate system of a stereoscopic vision system and construct its geometrical model. It is possible to establish the relationship between the point P (X, Y, Z) and the coordinates (x, y) of its projection on the matrix photodetector.

2 REVIEW OF THE LITERATURE

In the case of the analysis of the two-dimensional movement of the object, any of its points can be defined as $P(x, y)$, where x and y are the two-dimensional coordinates of the object. Such objects can be detected by analyzing the changing sequence of images, adjusted for the change of the observation system's position relative to the target object's plane of movement since the changes to the scene depth are negligible in comparison to the distance between the vision system and the target object [5].

Usually, image analysis involves obtaining the outer contour of the depicted objects and recording the coordinates of points of this contour. Most often it is necessary to get the outer contour in the form of a closed curve or a set of segments of arcs [6].

Consider the various methods of contour analysis.

Active contours are widely used in the tasks of selecting contours, borders, and image segmentation. To detect the contours in the image, the minimum energy curves, or snakes, are used. The algorithm is as follows: first, the contour is initialized as a simple line, and then it is deformed to create the area of the object. Points in the contour tend to the boundary of the object while minimizing the energy of the contour. For each point v_i, the energy

$$E_i = \alpha E_{int}(v_i) + \beta E_{ext}(v_i),$$

where α, β are constants providing relative energy correction; $E_{int}(v_i)$ is an energy function depending on the shape of the contour; $E_{ext}(v_i)$ is the energy function depending on the properties of the image and the type of gradient in the neighborhood of the point v_i [7].

The values E_i, $E_{int}(v_i)$, $E_{ext}(v_i)$ are square matrices. The value at the center of each matrix corresponds to the energy of the contour at level v_i [8].

Each vertex v_i potentially can go to any point v_i' corresponding to the minimum energy E_i.

This method has the following disadvantages:

– If the object does not have clear boundaries or the area is heterogeneous and contains smooth gradients, the algorithm will not solve the segmentation problem correctly, making further automated analysis impossible;

– The normal of the tangent vector at a point can vary greatly in the direction, which can lead to the merging of points. Because of this, the contour can turn out to be rough and very different from the borders of the selected object.

Unlike the usual active contour model, the active contour model without prior selection of boundaries does not require prior selection of the boundaries of the image object, and it is not necessary to smoothen the original image. The curve moves, starting from an arbitrary point of the image. When crossing the border, it begins to deform and take the form of an object in the image, as if filling its internal part [9].

J. Canny studied the mathematical problem of obtaining a filter that is optimal in terms of the selection, localization, and minimization of several responses of one edge. This means that the detector (known as the Canny edge detector) should react to the borders, but at the same time ignore the false ones, accurately determine the boundary line and react to each border only once, which allows avoiding the perception of wide bands of brightness as a combination of borders [10].

The algorithm includes:

– Anti-aliasing - blurring the image to remove noise;

– Search for gradients – borders are marked where the gradient of the image gets the maximum value;

– Suppression of non-maximums – only local maxima are marked as borders;

– Double threshold filtering – potential boundaries are determined by thresholds;

– Trace ambiguity – the final boundaries are set by suppressing all edges that are not associated with certain (strong) boundaries.

To reduce the sensitivity of the algorithm to noise, the first derivative of the Gaussians is applied [11]. After applying the filter, the image becomes slightly blurred.

The tracing contours method consists of sequentially drawing the border between the object and the background. A tracking point moves along the image until it reaches the dark area (the object). Then it turns left and moves along the curve until it reaches the borders of the object, and after that, it turns right and repeats the process until it reaches the vicinity of the starting point [12].

With respect to speed and distance, the nearest neighbor clustering is used. Let us denote two lines as

$$\{p_1, ..., p_m\} \in S_1$$

and

DOI 10.15588/1607-3274-2019-4-10

$$\{q_1, ..., q_n\} \in S_2,$$

provided that they satisfy the following conditions:

$$\{|x_{pi} - x_{qj}| + |y_{pi} - y_{qj}|\} \le \alpha_d;$$
$$\{|u_{pi} - u_{qj}|\} \le \alpha_u;$$
$$\{|v_{pi} - v_{qj}|\} \le \alpha_v,$$

where α_d, α_u, α_v are threshold constants; u_p, v_p are the velocity components of the point p with the coordinates (x_p, y_p); $i \in \{1, ..., m\}$, $j \in \{1, ..., n\}$.

Closest neighbor clustering is the most efficient method for scenes with interference. Interference is processed during the tracking phase [13].

Border detection methods highlight in the image only the pixels lying on the contour. In practice, this set of pixels rarely displays the contour accurately due to noise, contour breaks due to inhomogeneous illumination, etc. Therefore, contour detection algorithms are usually supplemented with binding procedures to form sets of contour points [14]. One way to associate contour points is to analyze the characteristics of pixels in a small vicinity of each image point, which has been marked as a contour. All points that are similar in accordance with some criteria are connected and form a contour consisting of pixels corresponding to these criteria. It uses two main parameters to establish the similarity of the contour pixels: the response of the gradient operator, which determines the value of the contour pixel, and the direction of the gradient vector. A contour pixel (x_0, y_0) located inside a given vicinity of a point (x, y) is considered to be similar to a pixel (x, y) modulo the gradient if

$$\nabla f(x, y) - \nabla f(x_0, y_0) \le E,$$

where E is a given non-negative threshold, and in the direction of the gradient, if

$$\alpha(x, y) - \alpha(x_0, y_0) \le A,$$

where

$$\alpha(x, y) = \text{arctg}(\partial x \setminus \partial y);$$

A is a given non-negative angular threshold.

A pixel in a given vicinity is combined with a central pixel (x, y) if the similarity criteria are met both in value and in direction. This process is repeated at each point of the image while simultaneously memorizing the found associated pixels when the center of the vicinity moves.

A simple way to account for the data is to assign its own brightness value to each set of bound pixels of the contour [15].

Finally, the approach to detecting and linking contours based on the representation in the form of a graph and finding the least-cost paths on this graph, which correspond to significant contours, allows us to construct a method that works well in the presence of noise. Such a procedure is rather complicated and requires a lot of processing time [16].

The outline element is the border between two pixels p and q, which are neighbors. Contour elements are identified by the coordinates of the points p and q. A contour is a sequence of interconnected elements.

Each contour element defined by pixels p and q corresponds to a certain value

$$c(p, q) = H - [f(p) - f(q)],$$

where H is the maximum level of brightness in the image; $f(p)$, $f(q)$ are the brightness of the pixels p and q, respectively.

The task of finding the minimum cost path on a graph is nontrivial in computational complexity, making it necessary to sacrifice optimality in favor of the computational speed.

The complexity of implementation and high resource intensity are the main disadvantages of such an analysis. Its main advantage is low sensitivity to noise [17].

3 MATERIALS AND METHODS

When selecting objects moving in three-dimensional space, a point of the objects is defined as $P(X, Y, Z)$, i.e. it is necessary to define an additional variable characterizing the depth of the points of the scene [18]. To solve this problem, we use a monocular vision system, the coordinate system of which is shown in Fig. 1. Supposing that the optical axis of the camera coincides with the Z-axis, the coordinates of point P have the following form:

$$X = (x/F)(F - Z),$$
$$Y = (y/F)(F - Z), \quad (1)$$

where F is the focal length of the lens, and x, y are the coordinates of the projection of the image element onto the plane (Fig. 1).

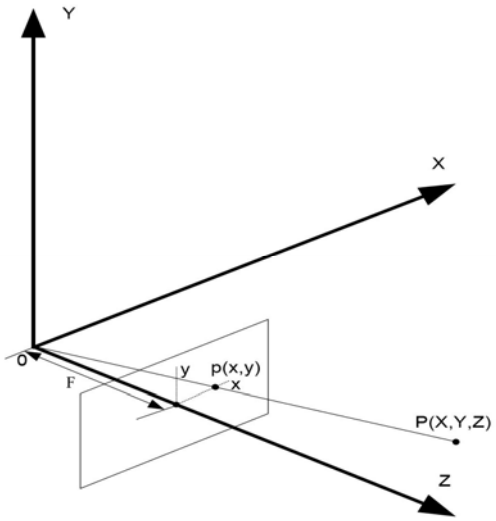


Figure 1 – Coordinate system of the monocular vision system

DOI 10.15588/1607-3274-2019-4-10

It can be observed from Equation (1) that to determine the coordinates of the point *P* of the object it is necessary to determine the unknown parameter *Z*, meaning that in order to solve this problem we need to use a stereoscopic vision system (Fig. 2).

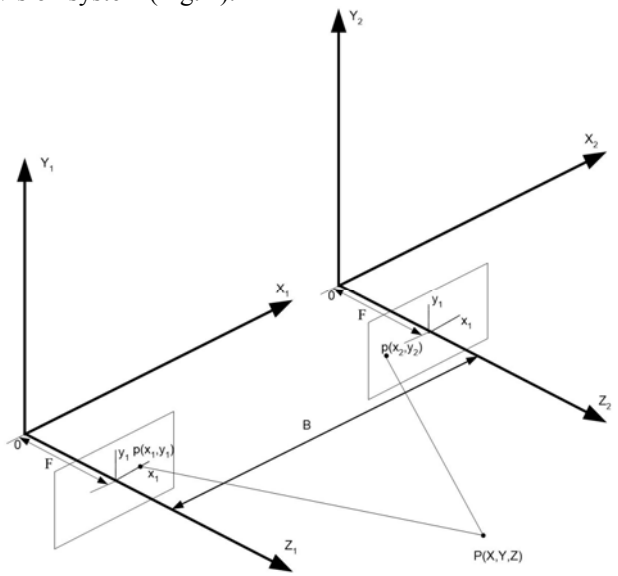


Figure 2 – Coordinate system of the stereoscopic vision system

Knowing the focal length *f* and the distance between the optic axis *B*, we can find *Z*:

$$Z = F - F \bullet B/Dispar, \quad (2)$$

where *Dispar* stands for the disparity [19].

The equations above are correct only for static vision systems. Let us consider a dynamic vision system, which allows us to detect objects moving in a three-dimensional space. Supposing that the observation system is moving relative to the surrounding environment with the movement direction (ΔX, ΔY, ΔZ), the equation connecting the three-dimensional coordinates of the point P(X,Y,Z) of the dynamic object with the coordinates of the projection p(x,y) will take the following form:

$$\Delta x = (-\Delta X \bullet F + x \bullet \Delta Z)/Z + x \bullet y/F - (x^2/F + F) + y, \quad (3)$$

$$\Delta y = (-\Delta Y \bullet F + y \bullet \Delta Z)/Z + x \bullet y/F - (y^2/F + F) + x. \quad (4)$$

In order to detect a dynamic object, we designate the direction of the gradient vector as (k_x, k_y), then the normal flux vector will take the following form:

$$X_n = \Delta X \bullet k_x + \Delta Y \bullet k_y. \quad (5)$$

Combining (5) with (3), (4), we obtain:

$$X_n = -k_x F \Delta X/Z - k_y F \Delta Y/Z + (xk_x + yk_y)\Delta Z/Z + (xyk_x/F + +(y^2/F + F)k_y) - ((x^2/F + F)k_x + xyk_y/F) + (yk_x + xk_y),$$

and from this we get:

$$Z = -k_x F/((x^2/F + F)k_x + xyk_y/F).$$

Consider the process of detecting a moving object from a moving base. Let the coordinate system $0xyz$ be associated with the object space. We will associate the coordinate system $0x_0y_0z_0$ with the moving base of the optical instrument. Moreover, the order of rotation of the moving coordinate system is as follows: angle ψ in the plane $0xy$, angle υ in the plane $0y_0z$, angle γ in the plane $0x_0y_0$. If the angular velocities of turns are designated accordingly ψ', υ', γ', then the projections of the angular velocities of the base on the axis of the moving coordinate system can be written in the form:

$$\omega_{x0} = \upsilon' \cos\gamma - \psi' \cos\upsilon \sin\gamma;$$
$$\omega_{y0} = \gamma' + \psi' \sin\upsilon;$$
$$\omega_{z0} = \upsilon' \sin\gamma - \psi' \cos\upsilon \cos\gamma. \quad (6)$$

Angular velocities ω_{x0}, ω_{y0}, ω_{z0} can be measured using gyroscopes oriented along the axes of the mobile coordinate system and fixed on the base [20].

The orientation of the vision system is defined by two angles: σ and φ (Fig. 3).

At these angles, the coordinate system $O'x_py_pz_p$ associated with the vision system is deployed relative to the base. We choose this coordinate system so that the axis $O'x_p$ coincides with the main optical axis of the device, and the axes $O'y_p$ and $O'z_p$ are oriented along and across the frame. The vector of the linear velocity of the center of gravity of the base can be represented as its projection on the base axis v_{x0}, v_{y0}, v_{z0} [21].

Consider the equation of motion of the system at the initial moment of time, when the axes of the base coincide with the axes of the fixed coordinate system, i.e. $\psi = \upsilon = \gamma = 0$. Let us place two additional coordinate systems that are parallelly transferred from point O to the field of images $O_ix_iy_iz_i$ and to the field of objects $O_px_py_pz_p$ (Fig. 3).

Then, considering the distance between the origins of the coordinate systems, we can write down the equations of the coordinates in two systems:

$$x_p = H + z_p \mathrm{ctg}\,\varphi;$$
$$y_p = -(1/f)x_p y_i;$$
$$z_p = -(1/f)x_p z_i; \quad (7)$$

where

$$H = O'Op;$$
$$f = O'Oi.$$

Differentiating the last two equations with respect to time and performing transformations with respect to variables y_i', z_i', we obtain:

$$y_i' = -(f/x_p)y_p' + ay_p x_p'/(x_p^2);$$
$$z_i' = -(f/x_p)z_p' + az_p x_p'/(x_p^2); \quad (8)$$

Rearranging equations (8), we get:

$$x_p = H/(1 + (1/f)z_i \mathrm{ctg}\,\varphi);$$

$$y_p = -Hy_i/(f(1 + (1/f)z_i \mathrm{ctg}\,\varphi));$$

$$z_p = -Hz_i/(f(1 + (1/f)z_i \mathrm{ctg}\,\varphi)); \quad (9)$$

DOI 10.15588/1607-3274-2019-4-10

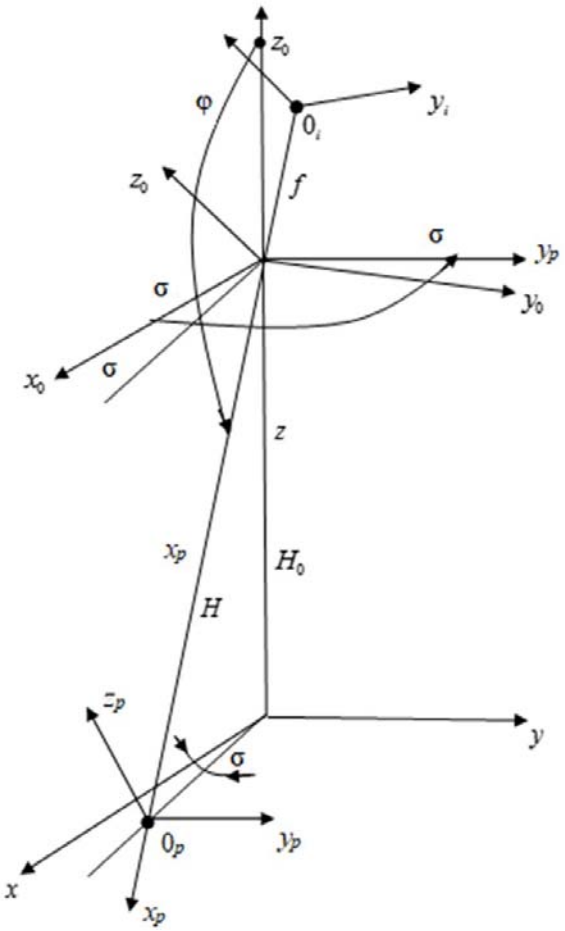


Figure 3 – Orientation of the vision system

Substituting relations (9) into equations (8), we obtain:

$$y_i' = -(1 + (1/f)z_i \operatorname{ctg} \varphi)(fy_p'/H + (1/H)y_i x_p');$$

$$z_p = -Hz_i/(f(1 + (1/f)z_i \operatorname{ctg} \varphi)); \quad (9)$$

$$z_i' = -(1 + (1/f)z_i \operatorname{ctg} \varphi)(fz_p'/H + (1/H)z_i x_p'). \quad (10)$$

4 EXPERIMENTS

To confirm the adequacy of this mathematical model, the mathematical method proposed by us was implemented in software. A program was developed in which the equations of motion of the moving reference system (that is, the trolley on which the cameras were mounted, which tracked the movement of the object) and the object of observation were set.

With the help of software, an experiment was performed. In the course of the experiment, the motion of the object and the moving reference system was modeled. The data on the change of coordinates of the object and the moving report system in space were obtained. The frequency of measuring the coordinates was 30 times per second, the total time of the experiment was 3 minutes.

5 RESULTS

The data obtained during the experiment are shown in Tables 1–4.

Table 1 – The coordinates of the mobile reference system relative to the static coordinate system

x	0,00	1,12	2,37	3,63	5,01	5,23	5,46	…
y	0,00	0,00	0,00	0,00	0,01	1,25	2,49	…
z	0,00	0,00	0,05	0,06	0,09	0,08	0,08	…

Table 2 – The coordinates of the moving object relative to the mobile reference system

x	12,53	15,81	19,27	23,02	27,01	33,41	38,55	…
y	4,67	6,54	8,31	10,11	11,58	12,93	13,31	…
z	15,01	15,03	15,02	15,02	14,59	15,05	15,09	…

Table 3 – The coordinates of the moving object relative to the static coordinate system (theoretical)

x	12,53	15,93	21,64	26,65	32,02	38,28	43,91	…
y	4,67	6,54	8,31	10,11	12,01	14,14	16,22	…
z	15,01	15,03	15,06	15,09	15,12	15,16	15,21	…

Table 4. The coordinates of the moving object relative to the static coordinate system (experimental)

x	12,53	15,93	21,64	26,65	32,02	38,28	43,91	…
y	4,67	6,54	8,31	10,11	12,01	14,14	16,22	…
z	15,01	15,03	15,06	15,09	15,12	15,16	15,21	…

6 DISCUSSION

As a result of the experiment, data were obtained on the motion of the object and the moving coordinate system. In particular, we have found:

– Coordinates *x*, *y*, *z* of the moving reference system relative to the static coordinate system;

– Coordinates *x*, *y*, *z* of the moving object relative to the moving reference system;

– Coordinates *x*, *y*, *z* of the moving object in the static coordinate system.

As you can see, the coordinates of a moving object, calculated using the proposed mathematical model, completely coincide with the coordinates obtained experimentally.

Based on these results, it can be concluded that the proposed mathematical model adequately describes the change in the coordinates of the moving object and the moving reference system.

Most vision systems in use today have a number of issues that limit the possibilities for their practical use. In particular, some methods, such as the active contours model and border detection methods have limited accuracy, especially in conditions where interference is present. Other systems are impossible to implement on a mobile platform, which limits their ability to detect moving objects. The new method allows us to solve these problems and to get accurate coordinates of a target object.

The method proposed by us can be used in practice for constructing mobile automatic tracking systems and the identification of objects.

CONCLUSIONS

The offered method allows us to determine the coordinates of dynamic objects from mobile bases of vision systems.

The **scientific novelty** of the results obtained is that a method has been proposed for isolating objects moving in space from a mobile vision system, which allows to

DOI 10.15588/1607-3274-2019-4-10

automatically isolate moving objects, determine their three-dimensional coordinates with a given accuracy, and adapt to changing observation conditions.

The **practical significance** of the results obtained is that experiments have been conducted to confirm the adequacy of the proposed mathematical model. The results of the experiment allow us to recommend the proposed method for constructing mobile automatic tracking systems and the identification of objects.

Prospects for further research are in exploring the possibility of implementing this method on a software and hardware system that allows you to improve the accuracy of the selection of objects.

ACKNOWLEDGEMENTS

Titov Vitaliy Semyonovich, D.Sc. (eng), Professor, Honoured Worker of Science, Member of the International Higher Education Academy of Sciences, for assistance in providing an opportunity for conducting research at the "Information Detection Telecommunication Intellectual Systems" research laboratory of the Information Technologies and Design Center of the Russian Academy of Sciences.

REFERENCES

1. Spevakov A. G., Rubanov A. F., Zhukovskiy D. V. Real-time dynamic parameters, *Information and telecommunication technologies in intelligent systems: Second international conference, Barcelona, 10–12 May 2004, proceedings*. Barcelona: International Academy of Informatization, 2004, pp. 177–180.
2. Verma R. A Review of object detection and tracking methods, *International Journal of Advance Engineering and Research Development*, 2017, No. 4, pp. 569–578.
3. Titov D. V., Shirabakina T. A. Integrated optoelectronic devices for recognition of complex objects, *Medical and environmental information technologies, Kursk, 25–26 October 2014, proceedings.* Kursk, Southwestern State University, 2014, pp. 134–136.
4. Li J., Wan J. Robust object tracking based on sparse eigenbasis, *IET Computer Vision*, 2014, No. 8, pp. 601–610.
5. Yemelyanov S. G., Titov D. V. Embedded optical electronic image recognition devices in the multidimensional feature space. Textbook. Kursk, South-West State University, 2013, 130 p.
6. Sharma K., Thakur N. A review and an approach for object detection in images, *International Journal of Computational Vision and Robotics,* 2017, No. 7, pp. 196–197.
7. Wu J., Peng B., Huang Z. et al. Research on computer vision-based object detection and Classification, *CCTA,* 2012, No. 1, pp. 10–12.
8. Tiwari M., Singhai R. A video sequences, *International Journal of Computational Intelligence Research,* 2017, No. 5, pp. 745–765.
9. Trufanov M. I., Boletsky E. B., Frolov M. M. et al. Vision system based on mobile transport robots, *Information technologies and mathematical modeling of systems: Odintsovo, 1–3 March 2017: proceedings.* Odintsovo, Federal State Budgetary Institution of Science "Center for Information Technologies in the Design of the Russian Academy of Sciences", 2017, pp. 164–168.
10. Polunin A. V., Trufanov M. I., Titov V. S. Binocular system of technical vision with a video sensor with variable focal length for a mobile robot, *News of the Volgograd State Technical University*, 2014, No. 1, pp. 83–87.
11. Kumar P., Chakraborty R., Sarkar A. Robust object tracking under cluttered environment, *International Journal of Emergency Technology and Advanced Engineering,* 2014, No. 1, pp. 18–19.
12. Boletsky E. B., Vakun V. V., Trufanov M. I. Binocular optoelectronic device with variable focal length, *Bulletin of Higher Educational Institutions. Instrument Engineering*, 2015, No. 7, pp. 147–150.
13. Gridin V. N., Trufanov M. I., Pomelnikov A. V. et al. Optical-electronic device with variable focal length for calculating the parameters of objects of a three-dimensional working scene (Varifocal binocular vision system for 3D scene reconstruction), *Information technologies in science, education and management: Moscow, 19–21 October 2016, proceedings*. Moscow, Limited Liability Company "Institute of New Information Technologies", 2016, pp. 78–87.
14. Frolov M. M., Trufanov M.I. Structural and functional organization of a three-dimensional technical vision system based on geographically distributed optical-electronic sensors, *Modern problems of physical and mathematical sciences, Oryol, 14–15 October 2017, proceedings*. Oryol, Oryol State University, 2017, pp. 367–368.
15. Wenbo Y., Cao Z., Tan M. et al.] Multiple-object tracking in large-Scale scene, *IEICE Transactions on Information and Systems*, 2016, No. 99, pp. 1903–1909.
16. Sakovich I. O., Belov Y. S. Overview of the main methods of contour analysis for the selection of the contours of moving objects, *Engineering Journal: Science and Innovations,* 2014, № 12, pp. 35–38.
17. Bertinetto L., Valmadre J., Henriques J. et al. Fully-convolutional Siamese networks for object tracking, *IEEE,* 2016, No. 9, pp. 85–89.
18. Shirabakina T. A., Spevakov A. G. Stereoscopic optoelectronic system for determining parameters of dynamic objects in real time, *Sensors and Systems,* 2004, No. 1, pp. 65–67.
19. Cyganek B. Object detection and tracking, *IEEE*, 2013, No. 4, pp. 42–46.
20. Keuper M., Tang S., Andres B. et al. Motion segmentation and multiple object tracking by correlation co-clustering // *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2018, No. 1, pp. 1–10.
21. Spevakov A. G., Rubanov A. F. Stereoscopic optical-electronic tracking system, *News of Higher Educational Institutions. Instrument making,* 2005, No. 4, pp. 62–67.

Received 11.06.2019.
Accepted 02.10.2019.

УДК 004.056.5

ВИДІЛЕННЯ ОБ'ЄКТІВ, ЩО РУХАЮТЬСЯ В ПРОСТОРІ, З РУХЛИВОЇ СИСТЕМИ ТЕХНІЧНОГО ЗОРУ

Спеваков А. Г. – канд. техн. наук, доцент кафедри інформаційної безпеки Південно-західного державного університету, Курськ, Російська Федерація.

DOI 10.15588/1607-3274-2019-4-10

Спевакова С. В. – аспірант кафедри обчислювальної техніки Південно-західного державного університету, Курськ, Російська Федерація.

Матюшин Ю. С. – студент кафедри інформаційної безпеки Південно-західного державного університету, Курськ, Російська Федерація.

АНОТАЦІЯ

Актуальність. Розглянуто завдання виділення об'єктів, що рухаються в просторі, з рухливої системи технічного зору. Проведений аналіз сучасних методів виділення динамічних об'єктів із стаціонарних і рухливих платформ. Виявлена необхідність створення нового методу виділення динамічних об'єктів з рухливої оптико-електронної системи, що має адаптивність до умов спостереження, що змінюються, що є актуальним науково-технічним завданням. Об'єктом дослідження була модель виділення об'єктів, що рухалися в просторі, з рухливої системи технічного зору.

Мета. Метою роботи є аналіз сучасних методів виділення об'єктів, що рухаються в просторі, і створення нового методу, що дозволяє вести спостереження з рухливої системи технічного зору і що є адаптивною до умов спостереження, що змінюються.

Метод. Запропоновано метод виділення об'єктів, що рухаються в просторі, з рухливої системи технічного зору, що дозволяє автоматично виділяти об'єкти, що рухаються, визначати їх тривимірні координати із заданою точністю, адаптуватися до умов спостереження, що змінюються. Цей метод грунтований на розробленій математичній моделі стереоскопічного визначення параметрів руху об'єктів в просторі, що дозволяє підвищити точність виділенн.

Результати. Запропонований метод реалізовано програмно. Проведений експеримент, що підтверджує адекватність цієї математичної моделі. В результаті проведення експерименту отримані дані про рух об'єкту і мобільної системи координат.

Висновки. Проведені експерименти підтвердили працездатність запропонованого методу і дозволяють рекомендувати його при по-строении мобільних автоматичних систем стеження і ідентифікації об'єктів. Перспективи подальших досліджень можуть полягати в створенні апаратних засобів виділення об'єктів, що рухаються, дозволяють підвищити точність выделения.

КЛЮЧОВІ СЛОВА: виявлення рухливих об'єктів, технічний зір, системи технічного зору, метод виділення об'єктів, мобільні системи

УДК 004.056.5

ВЫДЕЛЕНИЕ ОБЪЕКТОВ, ДВИЖУЩИХСЯ В ПРОСТРАНСТВЕ, С ПОДВИЖНОЙ СИСТЕМЫ ТЕХНИЧЕСКОГО ЗРЕНИЯ

Спеваков А. Г. – канд. техн. наук, доцент кафедры информационной безопасности Юго-Западного государственного университета, Курск, Российская Федерация.

Спевакова С. В. – аспирант кафедры вычислительной техники Юго-Западного государственного университета, Курск, Российская Федерация.

Матюшин Ю. С. – студент кафедры информационной безопасности Юго-Западного государственного университета, Курск, Российская Федерация.

АННОТАЦИЯ

Актуальность. Рассмотрена задача выделения объектов, движущихся в пространстве, с подвижной системы технического зрения. Проведён анализ современных методов выделения динамических объектов с стационарных и подвижных платформ. Выявлена необходимость создания нового метода выделения динамических объектов с подвижной оптико-электронной системы, обладающего адаптивностью к изменяющимся условиям наблюдения, что является актуальной научно-технической задачей. Объектом исследования являлась модель выделения движущихся в пространстве объектов с подвижной системы технического зрения.

Цель. Целью работы является анализ современных методов выделения движущихся в пространстве объектов и создание нового метода, позволяющего вести наблюдение с подвижной системы технического зрения и являющегося адаптивной к изменяющимся условиям наблюдения**.**

Метод. Предложен метод выделения объектов, движущихся в пространстве, с подвижной системы технического зрения, позволяющий автоматически выделять движущиеся объекты, определять их трёхмерные координаты с заданной точностью, адаптироваться к изменяющимся условиям наблюдения. Данный метод основан на разработанной математической модели стереоскопического определения параметров движения объектов в пространстве, позволяющей повысить точность выделения.

Результаты. Предложенный метод реализован программно. Проведен эксперимент, подтверждающий адекватность данной математической модели. В результате проведения эксперимента получены данные о движении объекта и мобильной системы координат.

Выводы. Проведённые эксперименты подтвердили работоспособность предложенного метода и позволяют рекомендовать его при построении мобильных автоматических систем слежения и идентификации объектов. Перспективы дальнейших исследований могут заключаться в создании аппаратных средств выделения движущихся объектов, позволяющих повысить точность выделения.

КЛЮЧЕВЫЕ СЛОВА: обнаружение подвижных объектов, техническое зрение, системы технического зрения, метод выделения объектов, мобильные системы.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Spevakov A. G. Real-time dynamic parameters / A. G. Spevakov, A. F. Rubanov, D. V. Zhukovskiy // Information and telecommunication technologies in intelligent systems: Second international conference, Barcelona, 10–12 May 2004: proceedings. – Barcelona: International Academy of Informatization, 2004. – P. 177–180.

DOI 10.15588/1607-3274-2019-4-10

2. Verma R. A Review of object detection and tracking methods / R. Verma // International Journal of Advance Engineering and Research Development – 2017 – № 4 – P. 569–578.
3. Titov D. V. Integrated optoelectronic devices for recognition of complex objects / D. V. Titov, T. A. Shirabakina // Medical and environmental information technologies: Kursk, 25–26 October 2014: proceedings. – Kursk : Southwestern State University, 2014. – P. 134–136.
4. Li J. Robust object tracking based on sparse eigenbasis / J. Li, J. Wan // IET Computer Vision – 2014 – № 8 – P. 601–610.
5. Yemelyanov S. G. Embedded optical electronic image recognition devices in the multidimensional feature space. Textbook / S. G. Yemelyanov, D. V. Titov. – Kursk : South-West State University, 2013. – 130 p.
6. Sharma K. A review and an approach for object detection in images / K. Sharma, N. Thakur // International Journal of Computational Vision and Robotics – 2017 – № 7 – P. 196–197.
7. Research on computer vision-based object detection and Classification / [J. Wu, B. Peng, Z. Huang et al.] // CCTA – 2012– № 1 – P. 10–12.
8. Tiwari M. A video sequences / M. Tiwari, R. Singhai // International Journal of Computational Intelligence Research – 2017 – № 5 – P. 745–765.
9. Vision system based on mobile transport robots / [M. I. Trufanov, E. B. Boletsky, M. M. Frolov et al.] // Information technologies and mathematical modeling of systems: Odintsovo, 1–3 March 2017: proceedings. – Odintsovo: Federal State Budgetary Institution of Science "Center for Information Technologies in the Design of the Russian Academy of Sciences", 2017. – P. 164–168.
10. Polunin A. V. Binocular system of technical vision with a video sensor with variable focal length for a mobile robot / A. V. Polunin, M. I. Trufanov, V. S. Titov // News of the Volgograd State Technical University. – 2014. – № 1. – P. 83–87.
11. Kumar P. Robust object tracking under cluttered environment / P. Kumar, R. Chakraborty, A. Sarkar // International Journal of Emergency Technology and Advanced Engineering. – 2014. – № 1. – P. 18–19.
12. Boletsky E. B. Binocular optoelectronic device with variable focal length / E. B. Boletsky, V. V. Vakun, M. I. Trufanov // Bulletin of Higher Educational Institutions. Instrument Engineering. – 2015. – № 7. – P. 147–150.
13. Optical-electronic device with variable focal length for calculating the parameters of objects of a three-dimensional working scene (Varifocal binocular vision system for 3D scene reconstruction) / [V. N. Gridin, M. I. Trufanov, A. V. Pomelnikov et al.] // Information technologies in science, education and management : Moscow, 19–21 October 2016 : proceedings. – Moscow : Limited Liability Company "Institute of New Information Technologies", 2016. – P. 78–87.
14. Frolov M. M. Structural and functional organization of a three-dimensional technical vision system based on geographically distributed optical-electronic sensors / M. M. Frolov, M. I. Trufanov // Modern problems of physical and mathematical sciences : Oryol, 14–15 October 2017: proceedings. – Oryol : Oryol State University, 2017. – P. 367–368.
15. Multiple-object tracking in large-Scale scene / [Y. Wenbo, Z. Cao, M. Tan et al.] IEICE Transactions on Information and Systems – 2016 – № 99 – P. 1903–1909.
16. Sakovich I.O. Overview of the main methods of contour analysis for the selection of the contours of moving objects / I. O. Sakovich, Y. S. Belov // Engineering Journal: Science and Innovations – 2014 – №12 – P. 35–38.
17. Fully-convolutional Siamese networks for object tracking / [L. Bertinetto, J. Valmadre, J. Henriques et al.] // IEEE – 2016 – № 9 – P. 85–89.
18. Shirabakina T.A. Stereoscopic optoelectronic system for determining parameters of dynamic objects in real time / T. A. Shirabakina, A. G. Spevakov // Sensors and Systems. – 2004. – № 1. – P. 65–67.
19. Cyganek B. Object detection and tracking / B. Cyganek // IEEE. – 2013. – № 4. – P. 42–46.
20. Motion segmentation and multiple object tracking by correlation co-clustering / [M. Keuper, S. Tang, B. Andres et al.] // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2018. – № 1. – P. 1–10.
21. Spevakov A. G. Stereoscopic optical-electronic tracking system / A. G. Spevakov, A. F. Rubanov // News of Higher Educational Institutions. Instrument making. – 2005. – № 4 – P. 62–67.

DOI 10.15588/1607-3274-2019-4-10

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

PROGRESSIVE INFORMATION TECHNOLOGIES

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 528.29

МЕТОДИКА ВИБОРУ ОПТИМАЛЬНОГО МАРШРУТУ РУХУ КОЛОНИ ТЕХНІКИ ПО НЕСТАЦІОНАРНІЙ МЕРЕЖІ ДОРІГ

Боровик О. В. – д-р техн. наук, професор, заступник ректора з навчальної роботи, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький, Україна.

Рачок Р. В. – д-р техн. наук, доцент, начальник кафедри загальнонаукових та інженерних дисциплін, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький, Україна.

Боровик Л. В. – д-р пед. наук, доцент, професор кафедри загальнонаукових та інженерних дисциплін, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький, Україна.

Купельський В. В. – ад'юнкт, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький, Україна.

АНОТАЦІЯ

Актуальність. Ефективне вирішення значного числа прикладних задач, що стосуються перевезень, у ряді випадків залежить від вдалого вибору маршруту руху. Побудова оптимальних маршрутів на розміченому графі, що описує мережу доріг і який має сталі ваги ребер, є класичним і детально вивченим завданням. Проте в багатьох застосуваннях виникає потреба врахування можливої динаміки зміни в часі ваг ребер, що відповідає випадкам зміни дорожніх умов. Останнє вимагає розвитку відповідного науково-методичного апарату.

Мета. Метою роботи є розробка методики вибору оптимального маршруту руху колони техніки по нестаціонарній мережі доріг у розумінні змінності ваг ребер графа, що відповідає цій мережі.

Метод. У роботі запропонована математична модель вибору оптимального маршруту руху колони техніки по мережі доріг. Для опису мережі доріг використаний граф. Критерієм оптимальності при виборі маршруту руху є мінімізація часу, який витрачається на пересування. Особливістю моделі є урахування можливості динамічної зміни ваг ребер графу при реалізації пересування колони техніки по обраному маршруту. На основі використання даної моделі запропонована методика, яка забезпечує вибір оптимальних маршрутів руху для дискретно-стохастичного, дискретно-детермінованого та неперервно-невизначеного випадків зміни ваг ребер графу.

Результати. У статті запропоновано алгоритми, що забезпечують розв'язування задачі вибору оптимального маршруту в умовах нефіксованої в часі ваги ребер, які описують мережу доріг, а також показано особливості застосування алгоритмів. З використанням розробленого програмного забезпечення досліджений варіант мережі доріг з нестаціонарною вагою ребер. На прикладі показано недосконаліть рішень щодо вибору оптимального маршруту при нестаціонарній вазі ребер графу, отриманих з використанням класичних методів.

Висновки. Неврахування можливої зміни дорожньої обстановки, що проявляється зміною в часі ваг ребер графа, який описує мережу доріг, може призвести до неоптимальності отримуваних рішень з використанням класичних методів пошуку найкоротшого маршруту в графі. Для отримання оптимальних маршрутів з урахуванням зміни в часі дорожньої обстановки при русі колони, можливо використати запропоновану у даному дослідженні методику. Отримані результати розширюють можливості щодо вирішення задач в галузі дискретної оптимізації з урахуванням динаміки зміни обстановки при реалізації оптимальних розв'язків.

КЛЮЧОВІ СЛОВА: оптимізація маршруту, граф, метод Дейкстри.

НОМЕНКЛАТУРА

$f_{(i;j)}(t)$ – первісна функції $v_{(i;j)}(t)$ на проміжку $\left\lfloor t_{0(i;j)}; t_{0(i;j)} + t_{(i;j)} \right\rfloor$;

$f_{(i;j)}^{-1}$ – функція, що обернена до функції $f_{(i;j)}(t)$ на проміжку $\left\lfloor t_{0(i;j)}; t_{0(i;j)} + t_{(i;j)} \right\rfloor$.

DOI 10.15588/1607-3274-2019-4-11

n – кількість вершин графа, що описує мережу доріг;

$\{i, j\}$ – ребро графа, що з'єднує вершини i та j;

l – кількість видів транспортних засобів;

$\Delta L_{(i;j)}$ – відома довжина шляху між точками 0 і s ребра $\{i; j\}$;

$T^{(i)}$ – тривалість реалізації i-го альтернативного шляху між вершинами графа a і z;

$t_{s(i;j)}$ – момент часу, в який колона техніки перебуває в точці s;

$t_{0(i;j)}$ – момент часу, в який колона техніки перебуває в точці, яка відповідає вершині графа i;

$\Delta L_{\omega(i;j)}$ – довжина шляху між точками $\omega-1$ і ω ребра $\{i, j\}$;

$v_k\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]$ – швидкість k-го виду техніки на часовому проміжку $\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]$ ребра $\{i, j\}$;

$W^{(i)} = \left(w_{ij}^{(i)}\right)_{n\times n}$. – матриця ваг графа;

$w_{ij}^{(i)}$ – вага ребра $\{v_i, v_j\}$ у момент перебування у вершині v_i;

$V = \left(v_{ij}\right)_{n\times n}$ – матриця швидкостей руху вздовж ребер графа;

v_{ij} – швидкість руху вздовж ребра $\{v_i, v_j\}$ у фіксований момент t, тобто $v_{ij} = f_{ij}(t)$ (функції $f_{ij}(t)$ можуть бути різними в залежності від того, вздовж якого ребра здійснюється рух);

$v_{k(i;j)}(t)$ – швидкість k-го виду техніки у момент часу t, який належить часовому проміжку $\left[t_{0(i;j)}; t_{0(i;j)} + t_{(i;j)}\right]$;

$v^{(0)}$ – вершина графу, з якої розпочинається рух.

ВСТУП

На сьогоднішній день питання оптимізації перевезень є надзвичайно важливими в різних галузях діяльності людства, зокрема, при вирішенні різноманітних завдань логістичної сфери. Успішне здійснення багатьох перевезень суттєво залежить від своєчасності прибуття колони техніки у визначене місце призначення. Для ефективного перевезення різноманітних вантажів по суші використовується широке коло сучасних транспортних засобів з різними можливостями. Перед плануванням перевезень можливе проведення оптимізації складу колони техніки з урахуванням широкого кола факторів [13]. Однак, на наступному етапі необхідно вирішити задачу визначення оптимального маршруту руху колони техніки.

Наявна достатньо розгалужена мережа автомобільних доріг обумовлює значну кількість можливих маршрутів руху, які поєднують місце вибуття з пунктом призначення. Така багатоваріантність, звичайно, спостерігається навіть при незначних відстанях, які потрібно подолати.

На вибір оптимального маршруту суттєво може вплинути динаміка розвитку дорожньої обстановки. Внаслідок впливу прогнозованих і стохастичних факторів швидкість пересування колони по окремих ділянках маршруту може суттєво змінюватись. Недостатнє врахування зміни у часі дорожньої обстановки може призвести до неправильного вибору маршруту руху, який не забезпечить своєчасність прибуття колони у пункт призначення. Внаслідок такої затримки може відбутись зрив виконання визначених завдань. Тому задача вибору оптимального маршруту руху колони техніки з урахуванням динаміки зміни дорожньої обстановки є актуальною.

Об'єктом дослідження є вибір маршруту руху колони техніки.

Предметом дослідження є науково-методичний апарат оптимізації вибору маршрутів.

Метою роботи є розробка методики вибору оптимального маршруту руху колони техніки по нестаціонарній мережі доріг.

1 ПОСТАНОВКА ЗАДАЧІ

Колона техніки повинна вибути з пункту відправлення (точки А) та прибути в пункт призначення (точку В) за найкоротший час. Математична модель мережі доріг являє собою розмічений граф, що наведений на рис. 1, вага ребер якого відображає час руху колони вздовж них.

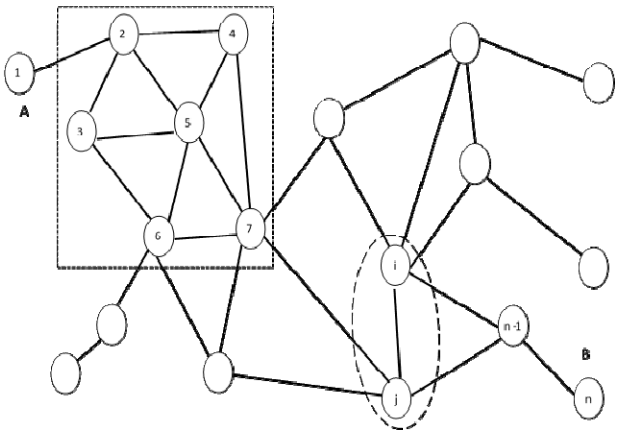


Рисунок 1 –Мережа автомобільних доріг між вихідним пунктом А та пунктом призначення В представлена графом

Необхідно знайти маршрут руху, при якому реалізується переміщення колони техніки з пункту А в пункт В за мінімальний проміжок часу.

Припустимо, що швидкість руху окремих одиниць техніки одного виду є сталою, а швидкість руху різних видів техніки у загальному випадку різна.

Вершини графа є вузлами розгалуження доріг. Вага ребра графа являє собою час руху колони між його вершинами. Швидкість колони визначається швидкіс-

DOI 10.15588/1607-3274-2019-4-11

тю виду транспортного засобу, яка має мінімальне значення для фіксованого проміжку часу. Останній є однією з складових загального часу руху колони вздовж ребра $\{i, j\}$.

Критерієм оптимальності маршруту є мінімізація часу руху по ньому. При цьому потрібно врахувати, що при русі колони час подолання окремих ділянок маршруту може бути змінним. Це обумовлено можливістю впливу на рух транспортних засобів різноманітних факторів, зокрема, погодно-кліматичних (сніг, туман, дощ, ожеледь, тощо), техногенних (завали, ремонт дорожнього полотна, його пошкодження внаслідок підтоплень ділянок дороги тощо), період доби (день, ніч) тощо.

У математичній моделі руху колони потрібно врахувати, що зміна ваг ребер може відбуватись:

1) дискретно, при досягненні колоною вершин графа з оновленням матриці ваг саме в ці моменти. У такому випадку рішення щодо наступного прокладання маршруту формується у вузлах графа з урахуванням дорожньої обстановки, яка динамічно змінюється і дані щодо якої надходять періодично. Цей випадок у подальшому називатимемо дискретно-стохастичним.

2) аналогічно попередньому випадку з наперед відомою зміною ваг ребер графа. При цьому, оптимальний маршрут руху може бути обраний на початку з урахуванням інформації про подальшу відому зміну стану доріг. Цей випадок у подальшому називатимемо дискретно-детермінованим;

3) неперервно при русі колони по мережі доріг. Цей випадок у подальшому називатимемо неперервно-невизначеним.

2 ЛІТЕРАТУРНИЙ ОГЛЯД

Вирішення задач вибору маршрутів руху колон транспортних засобів для ефективного переміщення вантажів, а також суміжним задачам приділялась увага у ряді робіт, зокрема в роботах [1–14].

Підхід щодо вибору маршруту, який ґрунтується на edgelabels, наведений у праці [1]. Його застосування дозволяє прискорити пошук найкоротшого шляху в 500 разів у порівнянні зі стандартним алгоритмом Дейкстри над великим графом. У роботі [2] наведено алгоритм для вибору оптимальних маршрутів у мультимодальному режимі мережі громадського транспорту. За результатами цього дослідження підхід щодо маршрутизації транзитних вузлів був адаптований для планування переміщення громадським транспортом. У науковій праці [3] для пошуку найкоротшого шляху застосовано метод ієрархії контракції. У дослідженні [4] на основі застосування алгоритму SHARC наведено можливості з відшукання найкоротших шляхів для довільних засобів переміщення у транспортній мережі континентального масштабу. У науковій праці [5] досліджено проблему планування мультимодальних маршрутів. У роботі [6] наведено модель для оцінки трафіку затримки транспортних засобів з урахуванням довільних навантажень у процесі руху. У дослідженні [7] наведене планування маршрутів для військових наземних транспортних засобів на полі бою. У роботі проведено моделювання невизначеностей, що мають місце на дорожній мережі, за допомогою набору дискретних сценаріїв. Запропоновано метод відшукання найкоротшого шляху для кожного окремого транспортного засобу. Результати розрахунків свідчать про те, що запропонований метод може забезпечити якісне рішення лише для мереж з невеликою кількістю вузлів. У науковій праці [8] розроблено алгоритм розв'язування задачі пошуку найкоротших за часом шляхів у міських маршрутних мережах транспорту загального користування з урахуванням тривалості пересадок методом віток і меж.

У джерелах [9–11] описуються можливості застосування геоінформаційних програмних продуктів ArcGIS для відшукання раціональних маршрутів руху. Маршрутний аналіз ArcGIS дозволяє здійснювати пошук найшвидшого за часом, найкоротшого за відстанню або навіть найбільш живописного маршруту з вихідної до кінцевої точки. До параметрів аналізу маршруту можуть входити час початку руху, час доби, точна дата, день тижня тощо. При виборі маршруту руху враховуються бар'єри – об'єкти, які обмежують, ускладнюють чи змінюють маршрут руху. За результатами обчислення з урахуванням вихідних параметрів та обмежень програмним продуктом формується певний маршрут руху.

У дослідженні [12] сформовано та досліджено варіант моделі планування вантажоперевезень, представлено прикладну програму для знаходження у транспортній мережі оптимального маршруту перевезення вантажів від одного постачальника до кількох споживачів.

У праці [13] задача вибору найкоротшого маршруту розв'язувалась за критерієм максимізації рівня готовності транспортних засобів та мінімізації марочного складу й кількості транспортних засобів у колоні. Обмеження моделі стосувалися забезпечення нормативно встановлених часу на перевезення та коефіцієнта готовності техніки, перевезення колоною особового складу заданої кількості та вантажу, заданої маси і об'єму, витрат різних видів пального, що не перевищують встановлених значень, не зниження запасу ходу по моторесурсу кожним транспортним засобом зі складу колони.

В авторській роботі [14] було здійснено формалізацію постановки задачі розмічення графа з неоднорідними ребрами та обґрунтовано метод її вирішення у двох різних випадках: у випадку, коли можливим є розбиття довільного ребра досліджуваного графа точками, що відповідають моментам часу, коли швидкість колони дискретно змінює своє значення, а також у випадку, коли розбиття ребра точками, що відповідають моментам часу, коли швидкість колони дискретно змінює своє значення, є проблемним, але при цьому швидкість колони у кожен фіксований момент часу є відомою.

DOI 10.15588/1607-3274-2019-4-11

З наведеного випливає, що у проаналізованих працях залишилися поза увагою наступні аспекти, які потребують урахування при виборі оптимального маршруту руху колони техніки:

– перевезення військових підрозділів вимагає дотримання вимог режимності, тому застосування загальнодоступного програмного забезпечення з великою ймовірністю може створювати передумови для прогнозування вибору маршруту руху ймовірним противником або порушником;

– перевезення потребує прогнозування зміни дорожньої обстановки з урахуванням комплексної статистичної інформації щодо проблемних ситуацій (аналіз ДТП на маршруті руху за минулий рік, інформації щодо проведення ремонтних робіт, врахування прогнозу погоди та ін.) на усьому маршруті руху з метою своєчасного виходу у визначений район;

– перевезення передбачають переміщення значної кількості людей і специфічних вантажів як на невеликі, так і на значні відстані;

– у зв'язку зі специфікою окремих завдань під час перевезення сумісно застосовується не тільки різномарочна, але і достатньо різнотипна техніка;

– виконання перевезень передбачає широке застосування будь-яких доріг, в тому числі ґрунтових, а іноді і бездоріжжя.

Отже, підходи та методи, які проаналізовані у наведених вище роботах, не можуть бути застосовні для розв'язування досліджуваної задачі безпосередньо. Разом з тим, запропонований у праці [14] метод є базовим і таким, що дозволяє впритул наблизитися до вирішення задачі вибору оптимального маршруту руху колони техніки. Особливість досліджуваної задачі полягає в нефіксованості ваг ребер, які описують окремі ділянки мережі доріг, у процесі руху колони.

Враховуючи це, метою даної роботи є розробка методики вибору оптимального маршруту руху колони техніки по нестаціонарній мережі доріг.

3 МАТЕРІАЛИ І МЕТОДИ

Зважаючи на те, що задача, яка адекватна реальному процесу, може мати місце у трьох постановках, необхідним є формування математичної моделі для кожної з них.

Розглянемо дискретно-стохастичний випадок. Нехай задано розмічений граф. Нехай v_i – деяка вершина графа. Необхідно знайти найкоротший шлях від заданої початкової вершини a до заданої вершини z, якщо величини $w_{ij}^{(i)}$ наперед невідомі і стають відомими лише в момент перебування у вершині v_i.

Інший можливий випадок – дискретно-детермінований, коли необхідно знайти найкоротший шлях від заданої початкової вершини a до заданої вершини z, якщо величини $w_{ij}^{(i)}$ наперед відомі.

Найбільш складним є неперервно-невизначений варіант завдання, у якому необхідно знайти найкоротший шлях від заданої початкової вершини a до заданої вершини z, якщо величина шляху визначається часом руху вздовж нього.

Розглянемо можливі підходи до алгоритмізації методу розв'язування досліджуваної задачі.

З урахуванням фізичного змісту задачі можна стверджувати, що матриця ваг $W^{(i)} = \left(w_{ij}^{(i)}\right)_{n\times n}$ може бути різною в залежності від часу, коли колона перебуває у вершині v_i. Тому природно, що матрицю ваг слід диференціювати в залежності від часу перебування колони у певній вершині.

Цей процес реалізуємо так. Початковий момент часу вважатимемо нульовим етапом.

Момент часу, коли колона перемістилася вздовж одного ребра і знаходиться у деякій вершині графа, вважатимемо першим етапом.

Момент часу, коли колона перемістилася вздовж двох ребер і знаходиться у деякій вершині графа, вважатимемо другим етапом і т.д.

З урахуванням цього, матрицю ваг у подальшому позначатимемо $W^{(i.k)} = \left(w_{ij}^{(i.k)}\right)_{n\times n}$. Тут k визначає етап реалізації руху колони.

Для формування матриць ваг може бути застосований підхід, який описаний у роботі [14] і вибір складових якого залежить від початкових умов задачі, що проаналізовані у цій праці, та фізичного змісту досліджуваної задачі.

У випадку дискретно-стохастичної постановки задачі для її вирішення можна використати метод Дейкстри [10] пошуку найкоротшої відстані між заданими вершинами графа a і z.

Якою саме буде матриця ваг, залежатиме від того, з якої вершини розпочинається рух. Тобто, для досліджуваної задачі $a = v^{(0)}$.

Таким чином, застосування алгоритму Дейкстри дозволяє встановити оптимальний маршрут руху для етапу 0.

Однак цей маршрут не буде оптимальним в цілому для задачі, оскільки матриця ваг у момент перебування колони у наступній вершині після вершини $v^{(0)}$ зміниться.

З урахуванням цього, для етапу 1 відомою буде кінцева вершина графа, яка залишається незмінною, а також початкова вершина, яка визначатиметься з оптимального маршруту, отриманого для етапу 0, як його друга вершина ($v^{(1)}$).

З урахуванням того, що в момент перебування колони у першій вершині етапу 1, тобто в вершині $v^{(1)}$, матриця ваг зміниться (якою саме буде матриця ваг, залежатиме від того, з якої вершини розпочинається рух), задачу визначення оптимального маршруту можна далі розглядати як задачу пошуку найкоротшої відстані між вершинами $v^{(1)}$ і z.

Для її розв'язування знову можна скористатися алгоритмом Дейкстри, як і на попередньому етапі. За-

DOI 10.15588/1607-3274-2019-4-11

стосування цього алгоритму дозволяє встановити оптимальний маршрут руху для етапу 1.

Таким чином, для етапу 2 відомою буде не лише кінцева вершина графа, яка залишається незмінною (вершина z), а й початкова вершина, яка визначатиметься з оптимального маршруту, отриманого для етапу 1, як його друга вершина ($v^{(2)}$).

З урахуванням того, що в момент перебування колони у першій вершині етапу 2, тобто в вершині $v^{(2)}$, матриця ваг зміниться (якою саме буде матриця ваг, залежатиме від того, з якої вершини розпочинається рух), задачу визначення оптимального маршруту можна далі розглядати як задачу пошуку найкоротшої відстані між вершинами $v^{(2)}$ і z.

З наведеного можна зробити висновок, що метод розв'язування задачі для розглянутого випадку полягає в ітераційному застосуванні алгоритму Дейкстри із змінною першою вершиною та різними матрицями ваг на окремих етапах його застосування.

Якщо прийняти, що $z = v^{(g)}$, то ознакою зупинки запропонованого алгоритму є суміжність вершин $v^{(g-1)}$ і $v^{(g)}$ в оптимальному маршруті $(g-1)$-го етапу.

Наглядне представлення наведеного алгоритму можна оцінити з табл. 1.

Таблиця 1 - Етапи реалізації ітераційного застосування алгоритму Дейкстри із змінною першою вершиною та різними матрицями ваг на окремих етапах його застосування

Етап	Вершини оптимального маршруту руху в залежності від етапу						
	a						z
0	$v^{(0)}$	$v^{(1)}$					
1		$v^{(1)}$	$v^{(2)}$				
2			$v^{(2)}$	$v^{(3)}$			
…					…		
$g-1$						$v^{(g-1)}$	$v^{(g)}$

Таким чином, оптимальний маршрут руху колони у випадку 1 являтиме собою наступну послідовність вершин: $a = v^{(0)}$, $v^{(1)}$, $v^{(2)}$,…, $v^{(g-1)}$, $v^{(g)} = z$.

А отже, оптимальна тривалість руху колони у досліджуваному випадку становить $T = \sum_{i=0}^{g-1} w_{v^{(i)}v^{(i+1)}}^{\left(v^{(i)},i\right)}$, де $w_{v^{(i)}v^{(i+1)}}^{\left(v^{(i)},i\right)}$ – вага ребра між вершинами $v^{(i)}$ і $v^{(i+1)}$ матриці ваг $W^{\left(v^{(i)},i\right)}$.

Для дискретно-детермінованого варіанту можливо використати інший підхід. Наведена математична модель досліджуваної задачі у цьому випадку дозволяє зробити висновок, що для її розв'язування можна скористатися методом, алгоритм якого полягає у побудові на початковому етапі усіх можливих шляхів між заданими вершинами графа a і z, встановленні сукупностей матриць ваг для кожного знайденого шляху, що відповідають кожній вершині на відповідному етапі, подальшому визначенні тривалості реалізації кожного шляху та вибору найкоротшого з шляхів на основі порівняння знайдених тривалостей. Слід звернути увагу на те, що при побудові альтернативних варіантів можливих шляхів між вершинами графа можливо уникнути розгляду тих з них, які містять повтори вершин, у яких колона вже побувала.

Тривалості реалізації альтернативних шляхів між вершинами графа a і z будуть рівні

$$T^{(1)} = w_{1.2}^{(1.0)} + w_{2.4}^{(2.1)} + w_{4.z}^{(4.2)},$$

$$T^{(2)} = w_{1.3}^{(1.0)} + w_{3.4}^{(3.1)} + w_{4.6}^{(4.2)} + w_{6.z}^{(6.3)},$$

$$T^{(3)} = w_{1.2}^{(1.0)} + w_{2.3}^{(2.1)} + w_{3.5}^{(3.2)} + w_{5.7}^{(5.3)} + w_{7.6}^{(7.4)} + w_{6.z}^{(6.5)}.$$

З урахуванням цього, мінімальний час руху колони між заданими вершинами графа a і z рівний

$$T = \min\left\{T^{(1)};\ T^{(2)};\ T^{(3)};\ ...\right\}.$$

Тоді, якщо $T = T^{(i)}$, то i-й маршрут є оптимальним.

Третій випадок постановки завдання – неперервно-невизначений. Наведена математична модель досліджуваної задачі при цьому дозволяє зробити висновок, що для її розв'язування можна скористатися методами, запропонованими для випадків 1 або 2 з урахуванням підходу до розмічення графа, що наведений нижче. Розглянемо ребро графа (рис. 2).

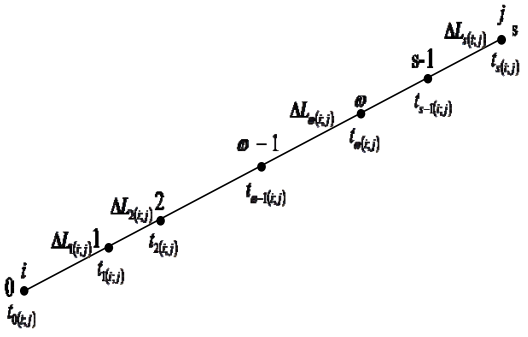


Рисунок 2 – Ребро графа, що представляє мережу автомобільних доріг

Розіб'ємо ребро $\{i; j\}$ точками 0, 1, 2, …, $\omega-1$, ω, …, s-1, s, що відповідають моментам часу, коли швидкість колони дискретно змінює своє значення. При цьому точка 0 співпадає з кінцем i, а точка s з кінцем j ребра $\{i; j\}$.

Ділянці $\Delta L_{\omega(i;j)}$ відповідають такі швидкості усіх видів техніки колони: $v_1\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]$, $v_2\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]$, …, $v_k\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]$, …, $v_l\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]$.

Тоді, з урахуванням того, що швидкість колони визначається швидкістю того виду транспортного засобу, який має мінімальне значення для фіксованого

DOI 10.15588/1607-3274-2019-4-11

проміжку часу, швидкість колони на ділянці $\Delta L_{\omega(i;j)}$ визначатиметься за формулою

$$\bar{v}_{\omega\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]} = \min\left\{ v_1\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right], v_2\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right], \ldots, v_k\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right], \ldots, v_l\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right] \right\}. \quad (1)$$

Слід зауважити, що в загальному випадку для ділянки $\Delta L_{\omega(i;j)}$ величина $\bar{v}_{\omega\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]}$ є сталою для всіх видів техніки, що рухаються в складі колони.

Наведене дозволяє зробити висновок, що час руху колони на ділянці $\Delta L_{\omega(i;j)}$ буде рівним

$$\bar{t}_{\omega(i;j)} = \frac{\Delta L_{\omega(i;j)}}{\bar{v}_{\omega\left[t_{\omega-1(i;j)};t_{\omega(i;j)}\right]}} . \quad (2)$$

При цьому, формулою (2) можна користуватися при довільному $\omega = \overline{1,s}$.

А отже, вага ребра $\{i;j\}$ може бути знайдена за формулою

$$t_{(i;j)} = \sum_{\omega=1}^{s} \bar{t}_{\omega(i;j)} . \quad (3)$$

Описаний підхід дозволяє підійти до розв'язування задачі розмічення графа і у випадку, коли розбиття ребра $\{i;j\}$ точками 0, 1, 2, …, $\omega-1$, ω, …, s–1, s, що відповідають моментам часу, коли швидкість колони дискретно змінює своє значення, є проблемним, але при цьому швидкість колони у кожен фіксований момент часу є відомою.

Розв'язування задачі при цьому виглядає так. З урахуванням того, що швидкість колони визначається швидкістю того виду транспортного засобу, який має мінімальне значення для фіксованого моменту часу $t \in \left[t_{0(i;j)}; t_{0(i;j)} + t_{(i;j)}\right]$, швидкість колони у момент t буде рівна

$$v_{(i;j)}(t) = \min\left\{ v_{1(i;j)}(t), v_{k(i;j)}(t), v_{l(i;j)}(t) \right\}. \quad (4)$$

А отже, справедливою буде формула

$$\int_{t_{0(i;j)}}^{t_{0(i;j)}+t_{(i;j)}} v_{(i;j)}(t)dt = \Delta L_{(i;j)} . \quad (5)$$

Застосування формули Ньютона-Лейбніца до лівої частини формули (5) дозволяє отримати, що

$$f_{(i;j)}(t)\Big|_{t_{0(i;j)}}^{t_{0(i;j)}+t_{(i;j)}} = \Delta L_{(i;j)} . \quad (6)$$

Здійснивши серію перетворень, з (6) можна отримати

$$f_{(i;j)}\left(t_{0(i;j)} + t_{(i;j)}\right) - f_{(i;j)}\left(t_{0(i;j)}\right) = \Delta L_{(i;j)},$$
$$f_{(i;j)}\left(t_{0(i;j)} + t_{(i;j)}\right) = f_{(i;j)}\left(t_{0(i;j)}\right) + \Delta L_{(i;j)},$$
$$t_{0(i;j)} + t_{(i;j)} = f_{(i;j)}^{-1}\left(f_{(i;j)}\left(t_{0(i;j)}\right) + \Delta L_{(i;j)}\right).$$

А отже, шукана вага ребра $\{i;j\}$ буде рівна

$$t_{(i;j)} = f_{(i;j)}^{-1}\left(f_{(i;j)}\left(t_{0(i;j)}\right) + \Delta L_{(i;j)}\right) - t_{0(i;j)} . \quad (7)$$

Використовуючи аналогічні підходи, можна знайти вагу кожного ребра графа, що описує транспортну мережу, як у випадку можливості розбиття ребер графа на окремі фрагменти, так і в протилежному випадку.

Застосування одного з методів, що запропоновані для дискретно-стохастичного і дискретно-детермінованого випадків, залежить від того, відомими чи невідомими є моменти перебування колони у вершинах графа.

У разі, якщо завчасно відомі можливі моменти перебування колони у кожній вершині графа, то застосовуючи описаний вище підхід, можна завчасно встановити матриці ваг графа, сформувавши їх до початку руху колони. А отже, в цьому випадку для відшукання оптимального шляху руху колони можна скористатися методом, що запропонований у даній роботі для дискретно-детермінованого випадку.

Якщо ж можливі моменти перебування колони у кожній вершині графа завчасно невідомі, то застосування наведеного вище способу розмічення графа можливе на етапі перебування колони у певній вершині. А отже, в цьому випадку для відшукання оптимального шляху руху колони можна скористатися методом, що запропонований у даній роботі для дискретно-стохастичного випадку.

Таким чином, метод розв'язування досліджуваної задачі у третьому випадку полягає в комплексуванні алгоритмів розмічення графа та безпосередньо визначення оптимального шляху в залежності від часу формування матриці ваг графа.

4 ЕКСПЕРИМЕНТИ

Розглянемо приклад використання запропонованої методики для оптимізації побудови маршруту руху колони техніки по мережі доріг, яка зображена на рис. 3.

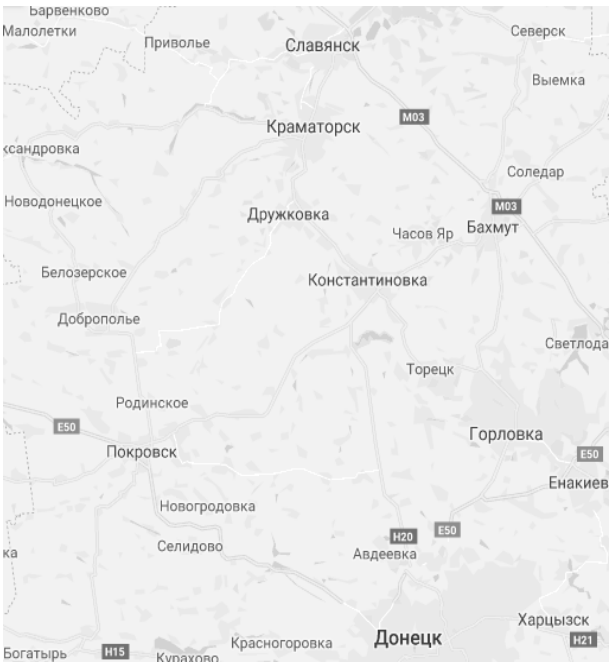


Рисунок 3 – Досліджувана ділянка місцевості

DOI 10.15588/1607-3274-2019-4-11

Мережі доріг цієї ділянки відповідає граф, що відображений на рис. 4, ваги ребер якого обчислені з використанням описаного вище підходу.

Рисунок 4 – Граф мережі доріг

З метою алгоритмічно-програмної реалізації описаних вище методик було розроблене програмне забезпечення, що відображене на рис. 5.

З метою проведення досліджень у програмі реалізовані наступні методики пошуку маршрутів: на основі класичного алгоритму Дейкстри без урахування динаміки зміни дорожньої обстановки (*розрахунок 1*); покрокове застосування алгоритму Дейкстри з коригуванням матриці ваг на кожному кроці побудови маршруту (*розрахунок 2*); повний перебір усіх можливих маршрутів, що поєднують пункт вибуття з пунктом призначення без повернень (*розрахунок 3*) і з поверненнями та обмеженою глибиною пошуку (*розрахунок 4*).

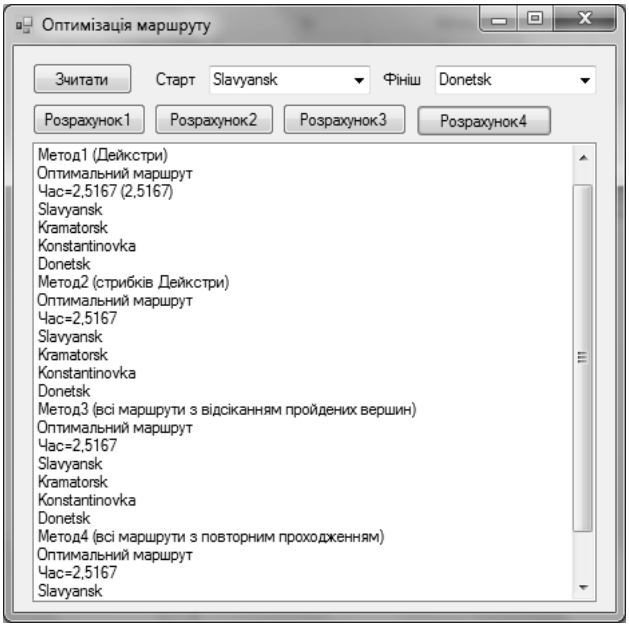


Рисунок 5 – Головне вікно програми визначення оптимального маршруту руху колони

5 РЕЗУЛЬТАТИ

Для випадку, коли розглядається стала дорожня обстановка, всі реалізовані у програмному забезпеченні методики очікувано забезпечують отримання однакового оптимального маршруту руху (Слов'янськ, Краматорськ, Константинівка, Донецьк) з однаковим значенням показника ефективності – часу на подолання маршруту 2,5167 (рисунок 5).

Однак, припустимо, що через деякий час (на третьому кроці) відбудеться тривале погіршення дорожньої обстановки на ділянці Константинівка-Донецьк (значне пошкодження дорожнього покриття). Внаслідок цього вага відповідного ребра зміниться з 1,616 до 10,6.

У цьому випадку, застосування алгоритму Дейкстри, що не враховує зміну матриці ваг ребер, приведе до отримання маршруту, який є оптимальним лише для початкового стану ваг ребер графу. При урахуванні зміни стану дорожнього покриття показник ефективності для такого маршруту суттєво погіршиться (рис. 6).

При послідовному використанні алгоритму Дейкстри зі зміною матриці ваг ребер на кожному етапі ситуація суттєво покращується.

З використанням даної методики отримується інший маршрут, який за показником ефективності є кращим практично в три рази.

Найкраще і, очевидно, оптимальне рішення забезпечує третя і четверта методика, які приводять до отримання однакових результатів. При цьому показник ефективності у порівнянні з класичним алгоритмом Дейкстри зростає в понад 3,5 рази.

Розглянемо ще один випадок динамічної зміни дорожньої обстановки з короткотривалою перешкодою (рис. 7).

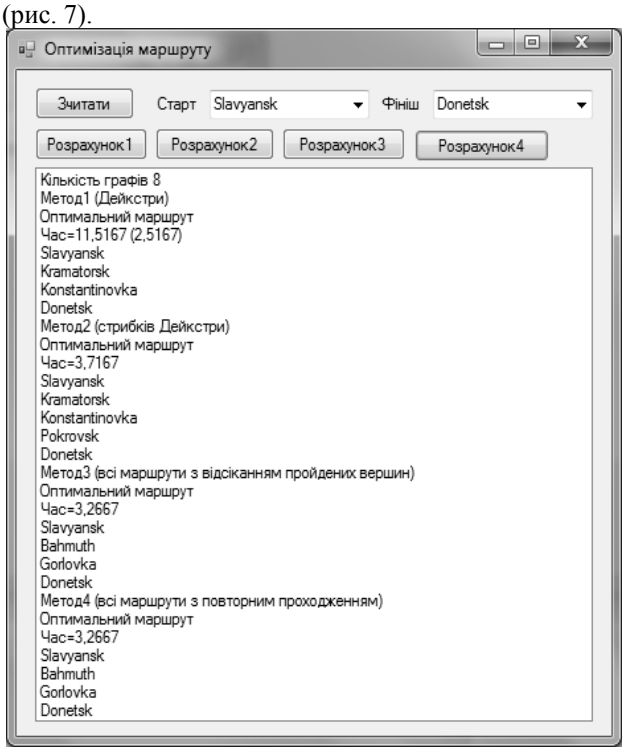


Рисунок 6 – Результати пошуку оптимального маршруту при тривалій зміні дорожньої обстановки

DOI 10.15588/1607-3274-2019-4-11

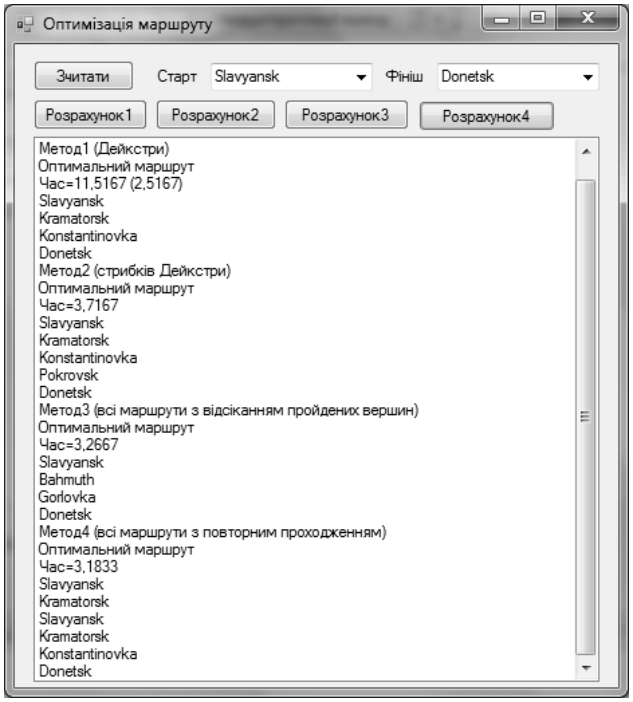


Рисунок 7 – Результати пошуку оптимального маршруту при короткотривалій зміні дорожньої обстановки

Внаслідок появи короткотривалої перешкоди дорожньому руху лише на 3 етапі вага ребра, яке пов'язує Константинівку з Донецьком, зміниться з 1,616 до 10,6, але вже на наступному кроці відновить своє попереднє значення і залишатиметься в подальшому 1,616.

У цьому випадку результати використання перших трьох методик збігаються з попереднім випадком тривалої зміни дорожньої обстановки. Однак, ці маршрути виявляються неоптимальними, оскільки з урахуванням можливості повернення у попередні вузли наявний маршрут, який додатково забезпечує покращення показника ефективності на понад 2,5%.

6 ОБГОВОРЕННЯ

Запропонована у даному дослідженні методика дозволяє враховувати динаміку зміни дорожньої обстановки при плануванні оптимальних маршрутів колон техніки.

Проте, хоча при визначенні ваг ребер графа, що описує мережу доріг, і розглянутий неперервний в часі випадок, при пошуку оптимального маршруту досліджується лише варіант дискретної його побудови зі стрибкоподібними змінами матриці ваг у вузлах графу.

Потребує окремих досліджень також і питання прогнозування зміни дорожньої обстановки з урахуванням як детермінованих, так і стохастичних факторів (планових і позапланових ремонтних робіт, планових обмежень руху, ймовірнісної оцінки аварійності окремих ділянок доріг тощо).

Для прогнозування зміни дорожньої обстановки доцільно розглянути можливість використання методів штучного інтелекту, зокрема, нейронних мереж.

ВИСНОВКИ

Таким чином, у роботі поставлена задача вибору оптимального маршруту руху колони техніки з урахуванням динаміки зміни дорожньої обстановки та інших факторів; сформовано математичні моделі досліджуваної задачі для дискретно-стохастичного, дискретно-детермінованого та неперервно-невизначеного випадків. У відповідності з цими моделями запропоновано методику вибору оптимального маршруту руху колони техніки. У дослідженні розглянуто приклад використання цієї методики для фрагменту мережі доріг та показано суттєвий вплив динамічної зміни обстановки на ефективність маршруту. Урахування зміни в часі ваг ребер графу, що відображає мережу доріг, дозволяє уникати неоптимальних розв'язків задачі.

Наукова новизна отриманих результатів полягає у формалізації задачі пошуку оптимального маршруту руху колони техніки з урахуванням динаміки зміни дорожньої обстановки, побудові відповідних математичних моделей та методики її розв'язання. Результати обчислювальних експериментів підтвердили важливість урахування зміни ваг ребер графа в ході реалізації визначеного маршруту. Запропонований науково-методичний апарат розширює науковий інструментарій теорії дискретної оптимізації.

Практичне значення отриманих результатів полягає в підвищенні ефективності застосування підрозділів швидкого реагування за рахунок оптимізації маршрутів їх переміщення. Програмно-алгоритмічна реалізація запропонованої методики дозволяє розширити функціональні можливості відповідних програмно-технічних комплексів.

Перспективи подальших досліджень полягають у дослідженні неперервного випадку зміни ваг ребер графу мережі доріг та пошуку методики вирішення оптимізаційного завдання у цьому випадку. Також, перспективним є прогнозування зміни дорожньої обстановки з урахуванням факторів як детермінованої, так і стохастичної природи.

ПОДЯКИ

Роботу виконано в рамках спільних наукових досліджень кафедри транспортних засобів і спеціальної техніки й кафедри загальнонаукових та інженерних дисциплін Національної академії Державної прикордонної служби України.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Fast point-to-point shortest path computations with arc-flags / [M. Hilger, E. Kohler, R. H. Mohring, H. Schilling] // The Shortest Path Problem. – Rhode Island: American Society, 2009. – (DIMACS). – (Discrete Mathematics and Theoretical Computer Science; Vol. 74). – P. 41–72.
2. Antsfeld L. Finding Multi-criteria Optimal Paths in Multi-modal Public Transportation Networks using the Transit Algorithm /

DOI 10.15588/1607-3274-2019-4-11

L. Antsfeld, T. Walsh // Artificial Intelligence and Logistics AILog 2012 Workshop Proceedings. – 2012. – №1. – P. 7–11.
3. Contraction Hierarchies: Faster and Simpler Hierarchical Routing in Road Networks / [R. Geisberger, P. Sanders, D. Schultes et al.] // Experimental Algorithms. – Berlin : Springer-Verlag Berlin Heidelberg, 2008. – (Springer-Verlag Berlin Heidelberg). – (Theoretical informatics and general questions; vol. 5038). – P. 319–333.
4. Delling D. Time-dependent SHARC-routing / Daniel Delling // Algorithmica. – Cham: Springer International Publishing AG, 2011. – (Springer-Verlag). – (Special Issue: European Symposium on Algorithms; Vol. 60). – P. 60–94.
5. Route Planning in Transportation Networks / [H. Bast, D. Delling, A. Goldberg et al.] // Algorithm Engineering. – Cham: Springer International Publishing AG, 2016. – (Springer Nature). – (Theoretical informatics and general questions; Vol. 9220). – P. 19–80.
6. Resilience and efficiency in transportation networks / [A. A. Ganin, M. Kitsak, D. Marchese et al.]. // Science Advances. – 2017. – №3. – P. 1–8.
7. Route Planning for Military Ground Vehicles in Road Networks under Uncertain Battlefield Environment / [T. Zhao, J. Huang, J. Shi et al.]. // Journal of Advanced Transportation Received. – 2018. – №1. – pp. 1–10.
8. Кузькін О. Ф. Пошук шляхів у маршрутних мережах міст методом відгалужень і меж / О. Ф. Кузькін // Комунальне господарство міст. – 2012. – № 103. – С. 378–388.
9. Лейс Т. Г. ArcGIS. ArcMap. Руководство пользователя / Т. Г. Лейс. – М. : МГУ, 2005. – 558 с.
10. Crosier S. ArcGIS 9: Getting started with ArcGIS / Scott Crosier. – Redlands, Calif.: ESRI, 2004. – 256 с. – (ESRI).
11. ArcGIS 9 ArcMap Руководство пользователя [Електронний ресурс] // ESRI. – 2004. – Режим доступу до ресурсу: https://www.rulit.me/books/arcgis-9-arcmap-rukovodstvo-polzovatelya.
12. Матвейчук Т. А. Моделювання та програмна реалізація процесу планування вантажоперевезень у військовій логістиці / Т. А. Матвейчук // Військово-технічний збірник АСВУ. – 2016. – № 14. – С. 18–25.
13. Математична модель задачі формування складу транспортної колони прикордонної комендатури швидкого реагування та її програмно-алгоритмічна реалізація / О. В. Боровик, Л. В. Рачок, Л. В. Боровик, В. В. Купельський. // Збірник наукових праць ВІКНУ. – 2017. – № 55. – С. 17–30.
14. Боровик О. В. Розмічення графа мережі доріг при розв'язуванні задачі вибору оптимального маршруту руху колони техніки прикордонної комендатури швидкого реагування / О. В. Боровик, В. В. Купельський. // Збірник наукових праць НАДПСУ. – 2018. – № 76. – С. 244–255.

Стаття надійшла до редакції 03.06.2019.
Після доробки 09.10.2019.

УДК 528.29

МЕТОДИКА ВЫБОРА ОПТИМАЛЬНОГО МАРШРУТА ДВИЖЕНИЯ КОЛОННЫ ТЕХНИКИ ПО НЕСТАЦИОНАРНОЙ СЕТИ ДОРОГ

Боровик О. В. – д-р техн. наук, профессор, заместитель ректора по учебной работе, Национальная академия Государственной пограничной службы Украины имени Богдана Хмельницкого, Хмельницкий, Украина.

Рачок Р. В. – д-р техн. наук, доцент, начальник кафедры общенаучных и инженерных дисциплин, Национальная академия Государственной пограничной службы Украины имени Богдана Хмельницкого, Хмельницкий, Украина.

Боровик Л. В. – д-р пед. наук, доцент, профессор кафедры общенаучных и инженерных дисциплин, Национальная академия Государственной пограничной службы Украины имени Богдана Хмельницкого, Хмельницкий, Украина.

Купельский В. В. – адъюнкт, Национальная академия Государственной пограничной службы Украины имени Богдана Хмельницкого, Хмельницкий, Украина.

АННОТАЦИЯ

Актуальность. Эффективное решение значительного числа прикладных задач, касающихся перемещений, в ряде случаев зависит от удачного выбора маршрута движения. Построение оптимальных маршрутов на размеченном графе, который описывает сеть дорог и имеет постоянные веса ребер, является классической и подробно изученной задачей. Однако во многих приложениях возникает необходимость учета возможной динамики изменения во времени весов ребер, что соответствует случаям изменения дорожных условий. Последнее требует развития соответствующего научно-методического аппарата.

Цель. Целью работы является разработка методики выбора оптимального маршрута движения колонны техники по нестационарной сети дорог в понимании переменности веса ребер графа, соответствующего этой сети.

Метод. В работе предложена математическая модель выбора оптимального маршрута движения колонны техники по сети дорог. Для описания сети дорог использован граф. Критерием оптимальности при выборе маршрута движения является минимизация времени, затрачиваемого на передвижение. Особенностью модели является учет возможности динамического изменения весов ребер графа при реализации передвижения колонны техники по выбранному маршруту. На основе использования данной модели предложена методика, которая обеспечивает выбор оптимальных маршрутов движения для дискретно-стохастического, дискретно-детерминированного и непрерывно-неопределенного случаев изменения весов ребер графа.

Результаты. В статье предложены алгоритмы, обеспечивающие решение задачи выбора оптимального маршрута в условиях нефиксированного во времени веса ребер, которые описывают сеть дорог, а также проанализированы особенности применения алгоритмов. С использованием разработанного программного обеспечения исследован вариант сети дорог с нестационарным весом ребер. На примере показано несовершенство решений относительно оптимального маршрута при нестационарном весе ребер графа, полученных с использованием классических методов.

Выводы. Отсутствие учета возможного изменения дорожной обстановки, которое проявляется изменением во времени весов ребер графа, описывающего сеть дорог, может привести к неоптимальности получаемых решений с использованием классических методов поиска кратчайшего маршрута в графе. Для получения оптимальных маршрутов с учетом изменения во времени дорожной обстановки при движении колонны, возможно использовать предложенную в данном исследовании методику. Полученные результаты расширяют возможности по решению задач в области дискретной оптимизации с учетом динамики изменения обстановки при реализации оптимальных решений.

КЛЮЧЕВЫЕ СЛОВА: оптимизация маршрута, граф, метод Дейкстры.

DOI 10.15588/1607-3274-2019-4-11

UDC 528.29

THE METHOD OF SELECTION OF THE OPTIMAL ROUTE OF MOVEMENT OF COLUMNS OF VEHICLES UNDER NON-STATIONARY ROAD NETWORK

Borovyk O. V. – Dr. Sc., Deputy Rector of the Academy of Educational Work, the National Academy of State Border Guard Service of Ukraine Named After Bohdan Khmelnitsky, Khmelnitsky, Ukraine.

Rachok R. V. – Dr. Sc., Associate Professor, Chief of the Department of General Scientific and Engineering Disciplines, the National Academy of State Border Guard Service of Ukraine Named After Bohdan Khmelnitsky, Khmelnitsky, Ukraine.

Borovyk L. V. – Dr. Sc., Associate Professor, Professor of the Department of General Scientific and Engineering Disciplines, the National Academy of State Border Guard Service of Ukraine Named After Bohdan Khmelnitsky, Khmelnitsky, Ukraine.

Kupelsky V. V. – Adjunct, the National Academy of State Border Guard Service of Ukraine Named After Bohdan Khmelnitsky, Khmelnitsky, Ukraine.

ABSTRACT

Context. Effective solution of a large number of applications requires optimal transportation. Construction of optimal routes on a static in time graph describing a network of roads is a classic and detailed study of tasks. However, in many applications, there is a need to take into account the possible dynamics of the change in time of road conditions, which requires the development of the appropriate scientific and methodical apparatus.

Objective. The purpose of the work is to develop a methodology for choosing the optimal route of movement of the equipment column on a non-stationary road network.

Method. In the paper a mathematical model of the choice of the optimal route of the movement of the vehicles column along the network is proposed. A graph is used to describe the network of roads. The criterion of optimality when choosing a route is to minimize the time spent on travel. The peculiarity of the model is to take into account the possibility of dynamically changing the weight of the edges of the graph when moving the column of technology on the chosen route. Based on the use of this model, a technique is proposed which ensures the selection of optimal route for discrete-stochastic, discrete-deterministic and continuously-indefinite cases of changes in the weight of the edges of the graph.

Results. In the article the algorithms are chosen and the features of their application are shown, which provide solution of the problem of choosing the optimal route in the conditions of the ribs that are not fixed in time, which describe the network of roads. The description of the algorithmic and programmatic implementation of the proposed methodology is given. With the use of developed software, the research model of the road network with a non-stationary weight of the ribs. The example shows the imperfection of the solutions for optimal route under the non-stationary weight of the edges of the graph obtained using classical methods.

Conclusions. Failure to take into account the possible change in the road situation, which manifests itself in the change in the time scale of the edges of the graph, which describes the network of roads, may lead to the non-optimality of the solutions obtained using the classic methods of finding the shortest route in the graph. To get the best routes, taking into account the change in the time of the road situation during the movement of the column, it is possible to use the method proposed in this study. The obtained results extend the possibilities for solving the problems in the field of discrete optimization taking into account the dynamics of the changing situation in the implementation of optimal solutions.

KEYWORDS: Route Optimization, Graph, Dijkstra's Method.

REFERENCES

1. Hilger M., Kohler E., Mohring R. and Schilling H., Fast point-to-point shortest path computations with arc-flags, *DIMACS,* 2009, Vol. 74, pp. 41–72.
2. Antsfeld L. and Walsh T. Finding Multi-criteria Optimal Paths in Multi-modal Public Transportation Networks using the Transit Algorithm, *Artificial Intelligence and Logistics AILog 2012 Workshop Proceedings*, 2012, No. 1, pp. 7–11.
3. Geisberger R., Sanders P., Schultes D. and Delling D., Contraction Hierarchies: Faster and Simpler Hierarchical Routing in Road Networks. Springer-Verlag Berlin Heidelberg, 2008, Vol. 5038, pp. 319–333.
4. Delling D. Time-dependent SHARC-routing, Springer International Publishing AG, 2008, Vol. 60, pp. 60–94.
5. Bast H., Delling D., Goldberg A., Müller-Hannemann M., Pajor T., Sanders P., Wagner D. and Werneck R. F. Route Planning in Transportation Networks, Springer International Publishing AG, 2016, Vol. 9220, pp. 19–80.
6. Ganin A. A., Kitsak M., Marchese D., Keisler J. M., Seager T. and Linkov I. Resilience and efficiency in transportation networks, *Science Advances*, 2017, No. 3, pp. 1–8.
7. Zhao T., Huang J., Shi J. and Chen C. Route Planning for Military Ground Vehicles in Road Networks under Uncertain Battlefield Environment, *Journal of Advanced Transportation Received*, 2018, No. 1, pp. 1–10.
8. Kuz'kin O. F. Poshuk shlyakhiv u marshrutnykh merezhakh mist metodom vidhaluzhen' i mezh, *Communal economy of cities*, 2012, No. 103, pp. 378–388.
9. Leys T. G., ArcGIS. ArcMap. Rukovodstvo pol'zovatelya. Moscow, MSU, 2005, 558 p.
10. Crosier S. ArcGIS 9: Getting started with ArcGIS, Redlands, Calif., 2005, 256 p.
11. ArcGIS 9 ArcMap Rukovodstvo pol'zovatelya, Access mode to the resource: https://www.rulit.me/books/arcgis-9-arcmap-rukovodstvo-polzovatelya.
12. Matveychuk T. A. Modelyuvannya ta prohramna realizatsiya protsesu planuvannya vantazhoperevezen' u viys'koviy lohistytsi, *Military-technical collection*, 2016, No. 14, pp. 18–25.
13. Borovik, O.V., Rachok, R.V., Borovik, L.V. and Kupelskiy V. V. The mathematical model of the problem of formation of the convoy of frontier commandant rapid response and its software-algorithmic implementation, *Military-technical collection*, 2017, No. 55, pp. 17–30.
14. Borovik O. V. and Kupelskiy V. V., Rozmichennya hrafa merezhi dorih pry rozv'yazuvanni zadachi vyboru optymal'noho marshrutu rukhu kolony tekhniky prykordonnoyi komendatury shvydkoho reahuvannya, *Military-technical collection*, 2018, No. 76, pp. 244–255.

DOI 10.15588/1607-3274-2019-4-11

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

UDC 004.9

ОСОБЛИВОСТІ АРХІТЕКТУРИ ІНТЕРНЕТ СИСТЕМИ УПРАВЛІННЯ КОМЕРЦІЙНИМ КОНТЕНТОМ НА ОСНОВІ МЕТОДІВ MACHINE LEARNING, WEB MINING ТА SEO-ТЕХНОЛОГІЙ

Висоцька В. А. – канд. техн. наук, доцент, доцент кафедри «Інформаційні системи та мережі», Національний університет «Львівська політехніка», Львів, Україна.

Демчук А. Б. – канд. техн. наук, асистент кафедри «Інформаційні системи та мережі», Національний університет «Львівська політехніка», Львів, Україна.

Литвин В. В. – д-р техн. наук, професор, завідувач кафедри «Інформаційні системи та мережі», Національний університет «Львівська політехніка», Львів, Україна.

АНОТАЦІЯ

Актуальність. Сьогодні більшість корпорацій постійно переосмислює бізнес з точки зору можливостей Інтернет, а саме його доступність, широке охоплення і постійно мінливі потреби користувача. Web-ресурс е-комерції, який забезпечує зручний для користувача досвід, зокрема, можливість швидко знаходити необхідні згідно його портеб та смаку товари, більше підтримує конкурентні переваги.

Метою дослідження є розроблення загальної архітектури інтелектуальної системи поширення комерційного контенту в Інтернет-просторі на основі навчання нейронної мережі згідно історії постійної аудиторії для подачі унікального контенту з використанням підходу персоналізації та використання тегів.

Метод. Розроблено модель інформаційної системи персоналізації комерційного контенту згідно потреб користувача. Також розроблено метод поширення комерційного контенту на основі підходу персоналізації та використання тегів. При цьому використано навчання нейронної мережі для створення тег рекомендацій та доступні на ринку засоби персоналізації. Розроблений алгоритм персоналізації дозволяє пов'язати кожного користувача з списком продуктів, які найімовірніше його зацікавлять, а також може прогнозувати те, що клієнти можуть хотіти бачити, навіть якщо вони ще не знають про це. Розроблений метод можна використати для забезпечення більш релевантного набору контенту. Також розроблений метод дає можливість класифікувати відповідний контент або показати його раніше в процесі гортання сторінок для уникнення споживачами вибору неправильного контенту або витрати часу на прокручування при пошуці товару.

Результати. Розроблена система призначена для поширення продуктів інформаційних технологій (публікацій, книг, курсів, відео, файлів тощо) за допомогою Інтернет.

Висновки. Інтернет. Впровадження цієї системи дасть змогу отримувати доступ до певного роду контенту широкому загалу користувачів, адже сайт буде розміщено у всесвітній павутині, з другого боку інша частина мети створення цієї системи є комерційна складова, а саме отримання прибутків власником чи адміністратором інтелектуальної системи, через механізми е-комерції.

КЛЮЧОВІ СЛОВА: комерційни контент, персоналізація, Web mining, Machine Learning, SEO-технологія, метрики пошуку, електронна комерція, NLP, контент-моніторинг, контент-аналіз, статистичний лінгвістичний аналіз, квантитативна лінгвістика.

АБРЕВІАТУРА

БЗ – база знань;
ІА – інтелектуальний агент;
ІС – інформаційна система;
ІТ – інформаційна технологія;
ПО – предметна область.

НОМЕНКЛАТУРА

S_{ec} – модель системи персоналізації контенту згідно потреб та вподобань користувача;

IdnUsr – колекція правил ідентифікації користувача;

CntRvw – колекція правил перегляду контенту;

PchPcs – колекція правил оформлення замовлення;

PdtPmt – колекція правил оплати замовлення;

α – оператор збору даних при перегляді контенту користувачем;

β – оператор пошукових тегів;

γ – оператор аналізу отриманих даних після збору даних при перегляді контенту;

AdgSchTgs – колекція правил додавання пошукових тегів;

RvwRzt – колекція правил формування результатів перегляду контенту користувачем;

PdtSch – колекція правил пошуку продукту згідно персоналізації потреб користувача;

PdtLstOr – колекція правил перегляду списку продуктів;

AngPdt – колекція правил додавання в список персоналізованого продукту;

RmdPdt – колекція правил перегляду персоналізованих продуктів;

AngLst – колекція правил додавання продукту в список побажань;

AngCrt – колекція правил додавання в кошик;

PdtDsr – колекція правил опису продуктів;

DOI 10.15588/1607-3274-2019-4-12

δ – оператор додавання в список персоналізованого продукту;

χ – оператор роботи нейромережі аналізу рекомендованих тегів;

NrlNwRmd – нейромережа рекомендованих тегів;

SchRzt – колекція правил формування результатів пошуку на основі існуючих тегів та категорій;

ϕ – оператор формування результатів пошуку;

PsnCnt – множина персоналізованого контенту;

φ – оператор;

ChgCnt – колекція зміненного контенту на сайті;

μ – оператор аналізу збережених тегів та категорій в Sitecore;

SvdTgs –множина збережених тегів та категорій;

ν – оператор формування множини персоналізованого контенту;

UstHst – колекція параметрів історії перегляду користувача;

Recall – повнота пошуку;

Precision – точність пошуку;

Accuracy – акуратність пошуку;

AvgPrec – середня точність пошуку;

Error – помилка пошуку;

F-measure – F-міра пошуку;

Precision(*n*) – точність на рівні *n* документів пошуку;

R-precision – R-точність пошуку;

a – кількість документів, знайдених системою і релевантних з точки зору експертів;

b – кількість документів, знайдених системою, але нерелевантних з точки зору експертів;

c – кількість релевантних документів, не знайдених системою;

d – кількість нерелевантних документів, не знайдених системою;

P – список всіх можливих морфо-синтаксичних описів для даного слова;

n – довжина кодування морфо-синтаксичних описів (110 біт);

o – вихід нейронної мережі для поточного слова;

e – двійкове кодування для морфо-синтаксичних описів в *P*.

ВСТУП

Сьогодні ефективність функцій пошуку та навігація по Web-сайту е-комерції зростає експоційно [1]. Це є важливою складовою успішної стратегії е-комерції [2]. Учасники Інтетнет-ринку збільшують інвестиції в персоналізацію контенту на Web-ресурсі для отримання низки переваг в е-бізнесі [3]. Ключові слова від користувачів Web-ресурсу е-комерції при пошуці в реальному часі формують профіль поведінки постійних/потенційних клієнтів і надають неоціненні статистичні дані для подальших досліджень [4]. Вдало використана така інформація збільшує кількість продаж, покращує механізми утримання клієнтів та збільшує обсяги потенціїних і постійних користувачів Web-ресурсу е-комерції [5–8].

Метою ІС е-комерції є формування унікального контенту на основі підходу персоналізації та використання тегів [9–10]. Об'єктом дослідження є використання нейронних мереж для створення тегів рекомендацій на основі методів персоналізації даних. Предметом дослідження є метод формування рекомендацій кінцевому користувачу Web-ресурсу е-комерції на основі персоналізації даних.

Метою дослідження є розроблення загальної архітектури ІС поширення комерційного контенту в Інтернет на основі навчання нейронної мережі на основі методів персоналізації даних.

1 ПОСТАНОВКА ПРОБЛЕМИ

Сучасні успішні проекти у вигляді ІС е-комерції зазвичай використовують персоналізацію на Web-сайті на відмінну від стандартної навігації [11]. Загальну модель ІС е-комерції подамо як кортеж:

$$S_{ec} =< IdnUsr, CntRvw, PchPcs, PdtPmt, \alpha, \beta, \gamma > .$$

Коли люди здійснюють покупки з намірами (знають, чого хочуть), і мають можливість швидко та легко це знайти, то вони, швидше за все, здійснять цю покупку [12–14]. Якщо користувачу презентувати відразу шуканий товар по категоріях та розташувати його в блоках контенту на головній сторінці, шанси на привернення уваги різко збільшуються. Тому процес персоналізованого перегляду контенту, рекомендованого конкретному користувачу згідно його побажань, залежить від декількох факторів:

$$CntRvw = \alpha(IdnUsr, AdgSchTgs, RvwRzt) .$$

Персоналізований підхід до користувача Web-ресурсу е-комерції призводить до більш високого коефіцієнта продаж. Клієнти, які не можуть знайти необхідну інформацію, зазвичай залишають Web-ресурс незадоволеними і шукають найкращі альтернативи [15]. Необхідно звертатися до Machine Learning для покращення формування рекомендацій кінцевому користувачу Web-ресурсу на основі результатів пошуку при кожному відвідуванні через періодичне поповнення бази пошукових тегів:

$$AdgSchTgs = \beta(PdtCrt, AgrRmdTgs) .$$

Застосування технології Machine Learning дозволяє генерувати рейтинг пошуку, відсортований за релевантністю чи оціночною актуальністю:

$$RvwRzt = \gamma(PdtSch, PdtLstOrw, AngPdt, RmdPdt, AngLst, AngCrt).$$

Ця оцінка враховує специфічні пошукові терміни (теги), а також особливості конкретного профілю користувача (наприклад, віковий діапазон, попередні замовлення, попередні пошукові терміни) [16]:

$$AngPdt = \delta(PdtDsr, \chi(NrlNwkRmd)) .$$

DOI 10.15588/1607-3274-2019-4-12

Алгоритми персоналізації дозволяють пов'язати кожного користувача зі списком найімовірніше необхідних товарів, поповнюючи альтернативими товарими, які не були обєктом пошуку [17]:

$$SchRzt = \phi(PdtSch, PsnCnt, \varphi(ChgCnt), \mu(SvdTgs)).$$

Розпізнавання контексту запиту коритсувачів за допомогою глибоких нейронних мереж забезпечує автоматичне додавання тегів в описи товару Web-ресурсу. Ці методи використовують для класифікації міміки і розпізнавати емоції користувача [18]:

$$PsnCnt = \nu(UstHst, SvdTgs, ChgCnt).$$

Кожний користувач має власні вимоги до формування запиту. Але типові пошукові системи повертають один і той самий результат для одного запиту, поданого різними користувачами. Для вирішення проблеми інформаційного перевантаження та надання користувачам необхідного контенту використовують персоналізацію. Вона підвищує точність пошуку, спрощує процес пошуку, зберігає час та надає необхідний контент користувачам. Персоналізація створює відчуття індивідуальності та унікальності. Шляхом сегментації та націлювання на різних покупців, персоналізація відповідає різним потребам кожного користувача Web-ресурсу.

2 АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

Ефективність реалізації штучного інтелекту для персоналізації передбачення побажань користувача в результатах пошуку товару значно залежить від роботи вбудованої в Web-ресурс інформаційно-пошукової системи. Для її стандартного оцінення використовують компоненти [19–26] як:

– Колекція документів.

– Набір тестових інформаційних потреб, поданих у вигляді запитів користувачів.

– Набір оцінок релевантності, поданих через бінарні твердження релевантний-нерелевантний відносно кожної пари запит-контент.

Релева́нтність є мірою відповідності отримуваного результату бажаному, тобто результатам пошуку відповідно до запиту [1–7, 12–18]. Колекція контенту і набір запитів повинні мати достатній обсяг: чим більша тестова вибірка, тим точніша оцінка якості роботи алгоритму [5–8, 27–32]. Інтерпретації тих або інших оцінок часто відмінні [33–35]. Більшість метрик в сучасній оцінці текстового пошуку ґрунтуються на матриці класифікації [1–5, 36–39]:

Recall характеризує здатність системи знаходити необхідний користувачу контент, але не враховує кількість виданого нерелевантного контенту [1–5, 40]. Наприклад, якщо $Recall = 50\%$, то половина релевантного контенту системою не знайдена.

$$Recall = \frac{a}{a+c}.$$

Precision характеризує здатність системи видавати в списку результатів тільки релевантний контент [1–5, 41]. Наприклад, якщо $Precision = 50\%$, то серед знайденого контенту половина релевантного.

$$Precision = \frac{a}{a+b}.$$

Для *Accuracy* передбачається, що система приймає рішення про приналежність до цієї категорії для кожного контенту колекції [1–5, 42].

$$Accuracy = \frac{a+d}{a+b+c+d}.$$

Error обчислюється як [43]:

$$Error = \frac{b+c}{a+b+c+d}.$$

F-measure використовують як єдину метрику, що об'єднує метрики *Recall* і *Precision* [1–5, 44]:

$$F = \frac{2}{\frac{1}{Precision} + \frac{1}{Recall}} = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall}.$$

Відмітимо основні властивості метрики F [45]:

– $0 \le F \le 1$;

– якщо $Recall = 0$ або $Precision = 0$, то $F = 0$;

– $Recall = Precision$, то $F = Recall = Precision$;

– $\min(Recall, Precision) \le F \le \frac{Recall + Precision}{2}$.

Загальна формула для *F-measure* обчислюється як:

$$F_\beta = (1+\beta^2) \cdot \frac{Precision \cdot Recall}{(\beta^2 \cdot Precision) + Recall}.$$

Для *AvgPrec* розглядають дві послідовності дій:

– вичислити метрики по кожному запиту окремо і потім їх усереднити (macroaverage);

– знайти загальну кількість документів, що відносяться до категорій табл. 1 і вже на їх основі вичислити шукану метрику (microaverage).

Таблиця 1 – Основні категорії документів

Кількість контенту	Релевантного	Не релевантного
виданого по запиту	*a* (правильно виданого контенту)	*c* (виданого нерелевантного даній рубриці контенту)
не виданого по запиту	*b* (неправильно виданого контенту)	*d* (не виданого і нерелевантного контенту)

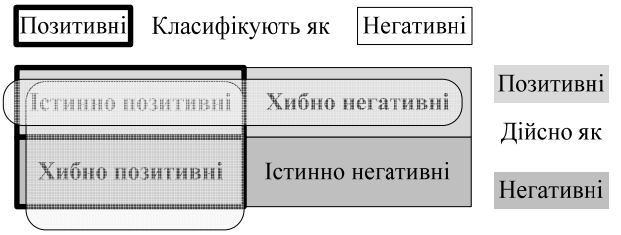


Рисунок 1 – Категорії документів

Величина macroaverage характерна для оцінки завдань пошуку, в яких важливий результат в середньому за запитом, незалежно від потужності відповіді на цей запит. Величина microaverage знайшла більше застосування в оцінці класифікації і фільтрації, де необхідно враховувати обсяги запитів.

DOI 10.15588/1607-3274-2019-4-12

Метрики на послідовностях документів, відсортованого по релевантності, враховують не лише факт наявності документу в списку знайдених документів, але і його положення в цьому списку.

Precision(*n*) визначається як кількість релевантних документів серед перших *n* виданих документів, ділене на *n* [1–5]. Якщо система видала більше за *n* документів, то *Precision*(*n*) дорівнює точності системи на перших *n* документах результатів запиту. Якщо система видала менш *n* документів, то *Precision*(*n*) буде не вища за точність системи. *Precision*(*n*) характеризує здатність системи видавати релевантні документи на початку списку результатів. Наприклад, якщо система видає не більше 10 документів на першій сторінці, то *Precision*(*n*) відбиває якість результатів системи, що отримуються на першій сторінці. Ця метрика має ряд недоліків. Зокрема, для різних запитів метрики *Precision*(*n*) можуть бути незрівняні. Наприклад, для ідеальної системи, яка видає тільки релевантні документи, *Precision*(100)=0.2 для запиту, по якому існує 20 релевантних документів, і *Precision*(100)=0,3 для запиту, по якому існує 30 релевантних документів. Але *Precision*(*n*) є незамінною метрикою сучасних систем пошуку оскільки, зокрема, дозволяє оцінити корисність першої сторінки відповіді системи для користувача.

R-precision дорівнює точності на рівні *n* документів для *n* рівної кількості релевантних документів для цього запиту [1–5]. Ця метрика покликана замінити *Precision*(*n*) в тих випадках, коли необхідно врахувати велику різницю у кількості релевантних документів різних запитів. *AvgPrec* для цього запиту визначається таким чином [1–5]: нехай для цього запиту є *k* релевантних документів. Точність на рівні *i*-го релевантного документу $prec\_rel(i) = Precision(pos(i))$, якщо *i*-й релевантний документ знаходиться в результатах запиту на позиції *pos*(*i*). Якщо *i*-й релевантний документ не знайдений, то $prec\_rel(i)=0$. *AvgPrec* для цього запиту дорівнює середньому значенню величини *prec_rel*(*i*) по усім *k* релевантним документам [1–5, 46]:

$$AvgPrec = \frac{1}{k}\sum_{i=1}^{k} prec\_rel(i).$$

Основні властивості метрики *AvgPrec*:

– $AvgPrec \le Recall$;

– якщо релевантні документи знаходяться тільки на початку списку, то $AvgPrec \approx Recall$;

– якщо релевантні документи рівномірно розподілені в списку, то $AvgPrec \approx Precision \cdot Recall$;

– кількість документів, які ранговані нижче останнього релевантного, не впливає на значення.

AvgPrec дозволяє оцінювати якість роботи системи, враховуючи пріоритет високо ранжируваних документів перед документами, що знаходяться у кінці списку. На відміну від метрик *Precision*(*n*) і *R-precision*, *AvgPrec* враховує усі знайдені документи.

3 МАТЕРІАЛИ ТА МЕТОДИ

Покращити персоналізацію можна в два етапи.

1. Сгенерувати найбільш релевантну персоналізовану колекцію контенту.

2. Класифікувати відповідний персоналізований контент за потребами користувача та демонстувати його в зручний спосіб в процесі гортання сторінок для уникнення вибору нерелевантного контенту або втрати часу на пошук релевантного контенту.

Користувач Web-ресурсу користується послугами е-комерції для здійснення покупок для зручності, економії часу та зусиль. Покращення умов співпраці з кожним кінцевим користувачем значно спростить процес ведення е-бізнесу та зменшить зусилля користувачу на пошук необхідного товару (рис. 2).

Блок реєстрації клієнтів дозволяє отримати знижки або запрошення на закриті продажі. Блок перегляду товару включає додавання пошукових тегів. Також клієнт може шукати товари, переглядати список продуктів, переглядати рекомендації, додавати продукти до кошику або списку бажань.

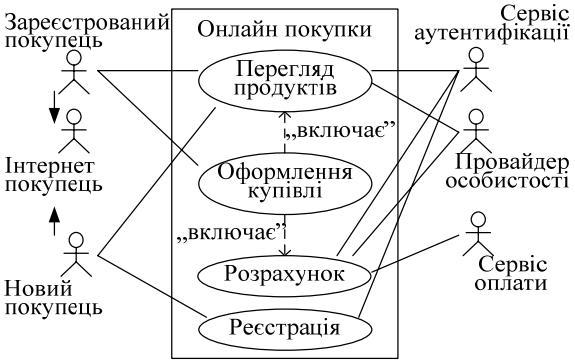


Рисунок 2 – Use case діаграма для Web-ресурсу

Блок додавання пошукових тегів розширюється за допомогою автогенерування рекомендованих тегів, та включає створення товару (рис. 3). Блок автентифікації клієнтів включає блок перегляду рекомендованих продуктів та доданих до списку бажань, оскільки обидва вимагають перевірки автентичності клієнта. У той же час товар може бути доданий до кошика для покупок без перевірки автентичності користувача. Система прийняття рішень для Web-сайту е-комерції при додаванні контент-модератором кожного нового товару забезпечує надання розширеного опису продуктів. Також надає відповідні рекомендовані категорії та теги з використанням синонімічних варіантів. Синонімічний ряд визначається через нейронну мережу та алгоритми Machine Learning, наприклад, на основі .Net CMS Sitecore (рис. 4), яка володіє засобами персоналізації, доступними для розширення і додавання власних правил, базуючись на доступному core-функціоналі (рис. 5). Кожний клієнт має унікальний ідентифікатор, пов’язаний з точно одним обліковим записом (рис. 6). Web-користувач

DOI 10.15588/1607-3274-2019-4-12

може перебувати в кількох станах: нові, активні, тимчасово заблоковані або заборонені, і бути пов'язаними з кошиком для покупок. Клієнт може не мати замовлень чи історії попередніх пошуків, чи переглядів сторінок. Замовлення клієнтів сортуються та є унікальними. Продукти мають теги, які їх позначають, а також категорії, до яких відносяться. Кожен продукт може відноситись до одної категорії, та мати багато тегів.

Персоналізація є методом відображення цільового, релевантного контенту для користувачів з урахуванням їх характеристик і поведінки, наприклад, місцезнаходження, статі, контенту і/або попередніх візитів. Через персоналізацію необхідний контент досягає відповідних користувачів, наприклад, можна:

– показати інший контент для різних користувачів на основі даних геолокації;

– сховати реєстраційну форму користувачів, які раніше заповнили форму;

– змінити текст на Web-сайті банера через посилання на Web-сайт користувача.

Для умовної візуалізації контенту використовують умовні відтінки, щоб контролювати, як відвідувачі переглядають та взаємодіють з Web-ресурсом.

Персоналізація на відмінну від умовної візуалізації відноситься до широкого процесу доставки цілеспрямованого необхідного контенту для відповідних користувачів. Персоналізація включає:

– адаптивну/динамічну зміну контенту Web-ресурсу на основі поведінки користувача;

– на основі створення та впровадження правил умовного відтворення контенту Web-ресурсу.

Рисунок 3 – Use case діаграма для блоку перегляд продуктів

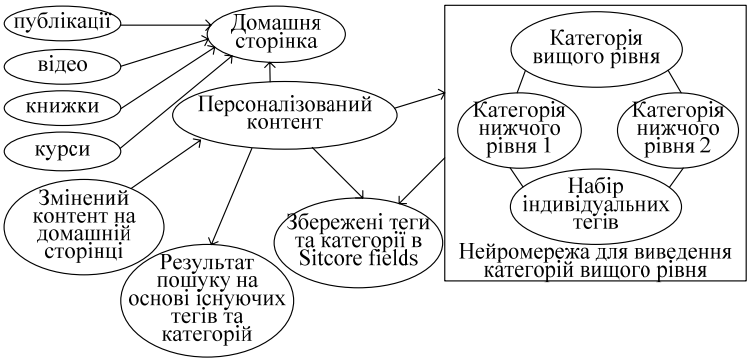


Рисунок 4 – Use case діаграма для процесу персоналізації контенту

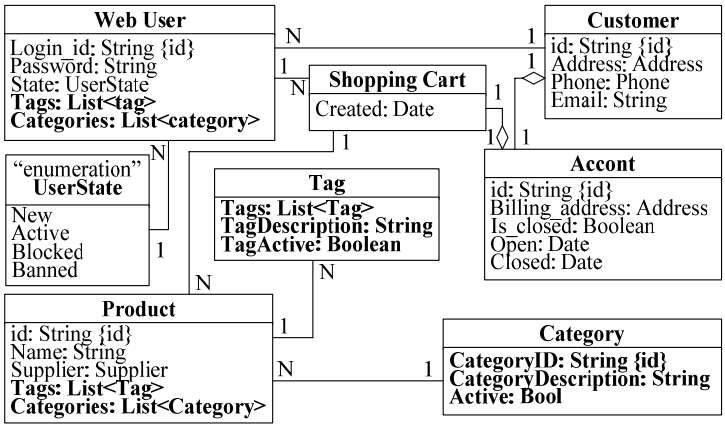


Рисунок 6 – ER-діаграма для для Web-ресурсу

DOI 10.15588/1607-3274-2019-4-12

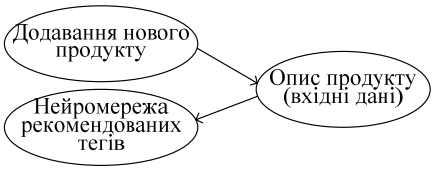


Рисунок 5 – Use case для процесу додавання продукту

В Sitecore встановлюють умови для умовної візуалізації в редакторі правил набору на основі логіки для визначення істинності умови. Визначають також дії як умовний рендерінг, який набуває чинності, якщо умова дійсна. Умова, пов'язана з дією, є правилом. Доступ до редактора коду правил отримують з редактора подій, редактора контенту та панелі керування маркетингом, але зазвичай створюють умовні виправлення в редакторі досвіду. Профілі контенту є категоріями для відстеження поведінки користувача під час навігації по Web-ресурсу е-комерції. Він допомагає краще зрозуміти поведінку, дії та інтереси користувачів. Вміст профілів складаються з ключів профілю; значення профілю; профільної картки. Також створюють в Sitecore власні властивості для відображення типових користувачів, яким також призначають картки профілю. Користувачів використовують для здійснення персоналізації правил. Створюють профілі контенту, ключі профілю, профілі та особи в центрі маркетингу. Значення профілю для елементів призначають у редакторі досвіду. Ключі профілю описують різні аспекти профілів. Призначають цифрові значення профілю для ключів профілю, а потім використовують значення профілю для відстеження взаємодії користувачів з Web-ресурсом е-комерції. Sitecore має деякі попередньо визначені профілі, які вже мають призначені профілі. Також можна створити власні ключі профілю. Коли користувачі здійснюють навігацію через Web-ресурс, їм призначаються значення профілю контенту, які визначаються для кожного відвіданого елемента. Ці значення накопичуються при повторних відвідувань ресурсу користувачем. Це допомагає створити контактний профіль постійних користувачів. Інформація про дії користувачів (переглянуті сторінки, виконані цілі, і шлях навігації по Web-ресурсу, тощо) визначає ділянки Web-ресурсу для вдосконалення. Також це використовують для сегментування користувачів та створення правил персоналізації для продажу. Наприклад, якщо користувач часто здійснює навігацію у певних категоріях або досяг високого профілю, то він є потенційною клієнтом цього напряму. Тоді вносять у систему CRM як потенційного покупця або надсилають йому е-повідомлення.

Картки профілю містять збережені ключі профілю та значення профілю. Профільні картки використовують для призначення стандартних значень профілів для елементів Web-ресурсу. Під час налаштування профілів для контенту створюють осіб. Це вигадані персонажі як певні типи користувачів у межах цільової демографічної групи. Особи описують життя, вік, звички, передумови, інтереси та професію вигаданого персонажа, який може використовувати Web-ресурс е-комерції певним чином. Створюють профільні карти, які описують спосіб, яким особа споживає контент Web-ресурсу. Вихідними даним профілів користувачів Web-ресурсу в Sitecore є вхідними даним для нейронної мережі в Machine Learning для персоналізації при формуванні рекомендацій кінцевому клієнту е-комерції.

Введення тексту в нейронній мережі особливо складне. Є певні проблеми, з якими необхідно боротися. Окремі слова мають різну довжину. Нейронні мережі вимагають фіксованого вхідного та вихідного розмірів. Використання рекурентної нейронної мережі, наприклад, нейронної мережі Елмана, вирішує частину проблем при розпізнаванні літер. Вона використовує контекстний шар для запам'ятовування замовлення. Опрацювання тексту використовує один довгий потік повідомлень. Кожен вхід є кількістю одного конкретного слова. Весь вхідний вектор міститиме одне значення для кожного унікального слова, наприклад, «з брюками і без», «двоє спортивних брюк», «темний спортивний костюм» та «брюки та чорні брюки». Є такі унікальні слова. Це словник.

– Input 0: та – Input 1: темний
– Input 2: костюм – Input 3: спортивний
– Input 4: без – Input 5: брюки
– Input 6: чорний – Input 7: з
– Input 8: два

Рядки кодують наступним чином, заповнюючи пропущені слова з нулем:

– «з брюками і без» [0 4 5 7] → [1, 0, 0, 0, 1, 1, 0, 1, 0];
– «двоє спортивних брюк» [1 5 8] → [0,1,0,0,0,1,0,0,1];
– «темний спортивний костюм» [1 2 3] → [0,1,1,1,0,0,0,0,0];
– «брюки та чорні брюки» [0 5 6] → [1,0,0,0,0,2,1,0,0].

Тепер є постійна векторна довжина. Дев'ять – загальна кількість слів у словнику. Кожен номер компонента у векторі – індекс у словнику доступних слів. На кожному векторному компоненті зберігається підрахунок кількості слів для цього словника. Кожен рядок зазвичай містить лише невелику підмножину словника. Як результат, більшість векторних значень є нульовим. Один з найважчих аспектів програмування Machine Learning перекладає проблему на масив фіксованої кількості чисел з плаваючою точкою.

4 ЕКСПЕРИМЕНТИ

Після збору персоналізованих даних користувачів будуємо нейронну мережу на прикладі хеш-таблиці. Її використовують для відображення ключів до значень, наприклад, «чуєш» → «сприймається вухом»; «бігти» → «йти швидше, ніж прогулянка»; «написати» → «для формування інструментом зображення на поверхні».

DOI 10.15588/1607-3274-2019-4-12

Це відображення між словами та визначенням кожного слова. Використовують ключ рядка для іншого значення рядка. Ключ повертає значення. Нейронна мережа є двонаправленою асоціативною пам'ятю, тобто фактично дозволяє також передавати значення і отримувати ключі. Наприклад, шаблон, який надсилається на вхідний шар нейронної мережі, подібний на процес введення ключа до хеш-таблиці. Але нейронні мережі не повертають порожній результат, а знаходять найближче значення.

Якщо задати ідеальний результат, то це контрольоване навчання і навпаки. Наглядова підготовка вчить нейронну мережу виробляти ідеальний вихід. Непідконтрольний тренінг зазвичай вчить нейронну мережу групувати вхідні дані в декілька груп, визначених вихідним числом нейронів. Наглядова та безконтрольна підготовка є ітераційним процесом. Для керованого тренування кожна ітерація тренування обчислює наскільки близький фактичний результат до ідеального виходу. Ця близькість виражається як відсоток помилки. Кожна ітерація змінює внутрішні матриці ваги нейронної мережі, щоб отримати рівень помилки на досить низькому рівні. Непідконтрольний тренінг також є ітераційним процесом. Проте обчислення помилки не таке просте. Немає очікуваного виходу, тому не можна виміряти, наскільки непідконтрольна нейронна мережа від ідеального виходу, бо немає ідеального виходу. Часто повторюють кілька ітерацій, а потім використовують мережу. Якщо потрібні додаткові тренування, то це навчання. Інший дуже важливий аспект вищезазначених тренувальних даних полягає у можливості використання в будь-якому порядку.

Тегер при Machine Learning автоматично призначає чотири фіктивних теги (два на початку і два наприкінці) для цільового висловлювання. Тоді нейронна мережа навчається автоматично призначати морфо-синтаксичні описи, що враховує контекст, тобто два раніше призначені теги та можливі теги для поточних та наступних двох слів. Навчальний приклад складається з функцій, витягнутих для одного слова всередині висловлювання як введення. Це морфо-синтаксичні описи в межах цього виразу як виведення. Функції витягуються з 5 слів, орієнтованих на поточне слово. Одне слово характеризується вектором, який кодує його морфо-синтаксичний опис. Для кодування можливих морфо-синтаксичних описів використовуємо $P(a|w)$, де кожен можливий атрибут має одну відповідну позицію усередині закодованого вектора. Вектори використовують для кодування можливих морфо-синтаксичних описів для поточного слова та наступних двох слів.

$$P(a \mid w) = \frac{C(w,a)}{C(w)}.$$

Під час навчання обчислюємо список суфіксів з відповідними морфо-синтаксичними описами, які використовують під час виконання, щоб створити можливий морфо-синтаксичний вектор для невідомих слів. Коли такі слова зустрічаються в даних тесту, наближаємо їх можливий морфо-синтаксичний вектор, використовуючи метод Брантса. Коли тегер застосовують до нового висловлювання, система ітеративно обчислює вихідний морфо-синтаксичний опис для кожного окремого слова. Після того, як мітку присвоєно одному слову, пов'язаний із цим словом вектор змінюється таким чином, що буде мати значення 1 для кожного атрибута, присутнього у його знову призначеному морфо-синтаксичному описі. Як наслідок кодування кожного окремого атрибута окремо для морфо-синтаксичних описів, тегер призначає нові теги, які ніколи не були пов'язані з поточним словом у навчальному процесі. Хоча це є недоліком для роботи з невідомими словами. Тоді використовуємо додатковий список слів із їх дозволеними морфо-синтаксичними описами. Для слова список розраховується як об'єднання з усіх морфо-синтаксичних описів, що з'являються з суфіксами, які застосовують до цього слова. Коли тегер призначає морфо-синтаксичний опис до певного слова, обирає один з морфо-синтаксичних описів можливих словоформ у списку зі словом, використовуючи функцію відстані:

$$\min_{e \in P} \sum_{k=0}^{n} | o_k - e_k |.$$

5 РЕЗУЛЬТАТИ

Розглянемо аналіз імен людей та місць у тексті для автоматичного додавання тегів про новини з людьми та назвами місць, що містяться в статтях. Особливість для ідентифікації назв і місць у тексті – це дані у файлі test data / propername.ser – спеціальний файл даних Java, що містить хеш-таблиці для людей і назв місць. Ці дані читаються в конструкторі класу Names. Значення хеш-таблиць використовується так:

```
while (keysE.hasMoreElements()) {
 Object key = keysE.nextElement();
 System.out.println(key+":"+placeNameHash.get(key));}
```

Які виведуть наступне:

```
Mauritius : country
Port-Vila : country_capital
Hutchinson : us_city
Mississippi : us_state
Lithuania : country
```

Наступний приклад використовує методи isPlaceName, isHumanName, та getProperNames:

```
System.out.println("Los Angeles: " +
names.isPlaceName("Los Angeles"));
   System.out.println("President Bush: " +
names.isHumanName("President Bush"));
   System.out.println("President George Bush: " +
names.isHumanName("President George Bush"));
   System.out.println("President George W. Bush: " +
names.isHumanName("President George W. Bush"));
   ScoredList[] ret = names.getProperNames("George Bush
played golf. President \George W. Bush went to London
England, \and Mexico to see Mary \Smith in Moscow.
President Bush will \return home Monday.");
   System.out.println("Human names: " +
ret[0].getValuesAsString());
   System.out.println("Place names: " +
ret[1].getValuesAsString());
```

Вихідні значення цього прикладу є таким:

DOI 10.15588/1607-3274-2019-4-12

```
   Los Angeles: true
   President Bush: true
   President George Bush: true
   President George W. Bush: true
   * place name: London,
          placeNameHash.get(name): country_capital
   * place name: Mexico,
          placeNameHash.get(name): country_capital
   * place name: Moscow,
          placeNameHash.get(name): country_capital
   Human names: George Bush:1,
                President George W . Bush:1,
                Mary Smith:1,
                President Bush:1
   Place names: London:1, Mexico:1, Moscow:1
```

Методи HumanName і isPlaceName шукають рядок в хеш-таблиці з назвою людини або місця:

```
public boolean isPlaceName(String name){
   return placeNameHash.get(name) != null;}
```

Версії API, які опрацьовують імена, що містять кілька слів, є трохи складнішими. Необхідно побудувати рядок із слів між початковими та кінцевими індексами та перевірити, чи це нове значення рядка є дійсним ключем у хеш-таблицях імен людей або назв місць:

```
public boolean isPlaceName(List<String> words, int
startIndex, int numWords){
   if ((startIndex + numWords) > words.size()) {
      return false;  }
   if (numWords == 1) {
      return isPlaceName(words.get(startIndex)); }
   String s = "";
   for (int i = startIndex;
      i < (startIndex + numWords); i++){
      if (i < (startIndex + numWords - 1)){
          s = s + words.get(startIndex) + " ";  }
      else{ s = s + words.get(startIndex); } }
   return isPlaceName(s);}
```

Токенінг тексту є процесом розщеплення рядка до окремих токенів. В результаті цього відбувається зменшення кількості слів до скороченого кореня слова, що дозволяє легко порівнювати рівність подібних слів. Тегування є визначенням того, яка частина кожного слово знаходиться у вхідному тексті. Позначення міток ускладнюється багатьма словами, що мають різні частини мовлення залежно від контексту (наприклад, «bank the airplane», «the river bank», тощо). Перш ніж опрацьовувати будь-який текст, необхідно розбити на окремі токени (слова, цифри та пунктуаційні символи). Клас Tokenizer має два статичні способи, обидва беруть вхідний рядок для токенування та повертають список токенів. Другий спосіб має додатковий аргумент для визначення максимальної кількості токенів:

```
static public List<String> wordsToList(String s)
static public List<String> wordsToList(String s, int
maxR)
String text = "The ball, rolling quickly, went down the
hill.";
List<String> tokens = Tokenizer.wordsToList(text);
System.out.println(text);
for (String token : tokens)
System.out.print("\""+token+"\" ");
System.out.println();
```

Цей фрагмент коду виводить наступне:

```
The ball, rolling quickly, went down the hill.
"The" "ball" "," "rolling" "quickly" "," "went" "down"
"the" "hill" "."
```

Краще витягнути токени слова для спрощення порівняння подібних слів. В класі є два зручні інтерфейси API для створення рядка з декількох слів та для одого токена слова:

```
public List<String> stemString(String str)
public String stemOneWord(String word)
```

Приклади опису тегів:

Tag	Description	Examples
NN	singular noun	dog
NNS	plural noun	dogs
NNP	singular proper noun	California
NNPS	plural proper noun	Watsons
CC	conjunction	and, but, or
CD	cardinal number	one, two
DT	determiner	the, some
IN	preposition	of, in, by
JJ	adjective	large, small, green
JJR	comparative adjective	bigger
JJS	superlative adjective	biggest
PP	proper pronoun	I, he, you
RB	adverb	slowly
RBR	comparative adverb	slowest
RP	particle	up, off
VB	verb	eat
VBN	past participle verb	eaten
VBG	gerund verb	eating
VBZ	present verb	eats
WP	wh* pronoun	who, what
WDT	wh* determiner	which, that

FastTag використовує методи Machine Learning для визначення правила переходу для тегів тексту, використовуючи ручне позначення тексту як приклад навчання. Клас Tagger читає файлову лексику як потік ресурсів або як локальний файл. Кожен рядок у файлі lexicon.txt проходить через метод utility parseLine, який опрацьовує вхідний рядок, використовуючи перший токен у рядку як хеш-ключ, і розміщає решту токенів у масиві, що є хеш-значенням. Отже, будемо опрацьовувати рядок «fair JJ NN RB» як хеш-ключ «fair», а хеш-значення – масив рядків: [«JJ», «NN», «RB»]. Коли Tagger опрацьовує список токенів слова, кожний токен звертається до хеш-таблиці та зберігає перший можливий тип тегів для цього слова. У прикладі слово «fair» буде призначено (можливо, тимчасово) тегом «JJ». Тепер є список токенів слова та пов'язаний список можливих типів тегів. Детально розглянемо rule 1: *i* – це змінна циклу в діапазоні [0, кількість токенів слова – 1], а слово – поточне слово в індексі *i*:

```
// rule 1: DT, {VBD | VBP} --> DT, NN
if (i > 0 && ret.get(i - 1).equals("DT")) {
    if (word.equals("VBD") || word.equals("VBP") ||
word.equals("VB")) {ret.set(i, "NN");  }}
```

Англійською це правило позначає визначник (DT) в токені слова (індекс *i*–1 супроводжується минулим часом дієсловом (VBD)), або дієслово теперішнього часу (VBP), після чого змінюється тип тегу індексу *i* на «NN». Інші правила у короткому синтаксисі:

– rule 2: перетворити іменник на номер (CD), якщо «.» з'являється у слові;

– rule 3: перетворити іменник на дієприкметник в минулому часі, якщо words.get(i) закінчується на «ed»;

DOI 10.15588/1607-3274-2019-4-12

– rule 4: перетворити будь-який тип на прислівник, якщо він закінчується на «ly»;

– rule 5: перетворити іменник (NN/NNS) на прикметник, якщо він закінчується «al»;

– rule 6: перетворити іменник в дієслово, якщо попереднє слово є «would»;

– rule 7: якщо слово класифіковано як загальний підсумок, та закінчується нв=а«s», встановлюється тип на множинний загальний іменник (NNS);

– rule 8: перетворення іменника в діюче дієслово.

Клас WordNetTest знаходить різні значення слова для даного слова і виводить ці дані до стандартного виводу. Конструктор класу з'єднується з даними WordNet файлу для повторного використання:

```
public WordNetTest(){
  database = WordNetDatabase.getFileInstance();}
```

Тут метод JAWS повертає список синонімів:

```
public List<Synset> getSynsets(String word){
   return Arrays.asList(database.getSynsets(word));}
public static void main(String[] args) {
System.setProperty(PropertyNames.DATABASE_DIRECTORY,
   "/Users/markw/temp/wordnet3/dict");
WordNetTest tester = new WordNetTest();
String word = "bank";
List<Synset> synset_list = tester.getSynsets(word);
System.out.println("\n\n** Process word: " + word);
for (Synset synset : synset_list) {
   System.out.println("\nsynset type: " +
   SYNSET_TYPES[synset.getType().getCode()]);
   System.out.println(" definition: " +
      synset.getDefinition());
   // word forms are synonyms:
   for (String wordForm : synset.getWordForms()) {
      if (!wordForm.equals(word)) {
        System.out.println(" synonym: "+wordForm);
```

Антоніми – протилежності синонімів. Антоніми є специфічними для індивідуальних слів. Тому використовуємо такий код для відображення антонімів всередині циклу над формою слова для кожного сенсу слова для «bank»:

```
// antonyms mean the opposite:
for (WordSense antonym :synset.getAntonyms(wordForm)) {
   for (String opposite :
   antonym.getSynset().getWordForms()) {
      System.out.println(" antonym (of " +
         wordForm + "): " + opposite);   }}}}
System.out.println("\n");}}
private WordNetDatabase database;
private final static String[] SYNSET_TYPES =
{ "", "noun", "verb" };}
```

Слово «bank» має 18 різних значень, 10 іменників і 8 дієслів, наприклад:

```
synset type:      noun
   definition: sloping land (especially the slope
      beside a body of water)
synset type:      noun
   definition: a financial institution that accepts
   deposits and channels the money into
      lending activities
   synonym: depository financial institution
   synonym: banking concern
   synonym: banking company
synset type:      noun
      definition: a long ridge or pile
synset type: noun
      definition: an arrangement of similar objects
      in a row or in tiers
synset type:      noun
      definition: a supply or stock held in reserve
      for future use (especially in
      emergencies)
synset type:      noun
      definition: the funds held by a gambling house
      or the dealer in some gambling games
```

6 ОБГОВОРЕННЯ

Аналізатор шляхів показує цифрову доріжку (або послідовність) користувачів, відображаючи її на простий у використанні візуальний спосіб. Ці візуальні шляхи відображають життєві уявлення з метою виявлення можливостей е-комерції. Якщо, наприклад, багато відвідувачів дивляться на певні сторінки, що переходять за кліками, без перетворення, це може означати, що щось не працює належним чином. Після декількох тестових проходжень по Web-сайту можна побачити відображення переходів по сторінках на наступній діаграмі на рис. 7.

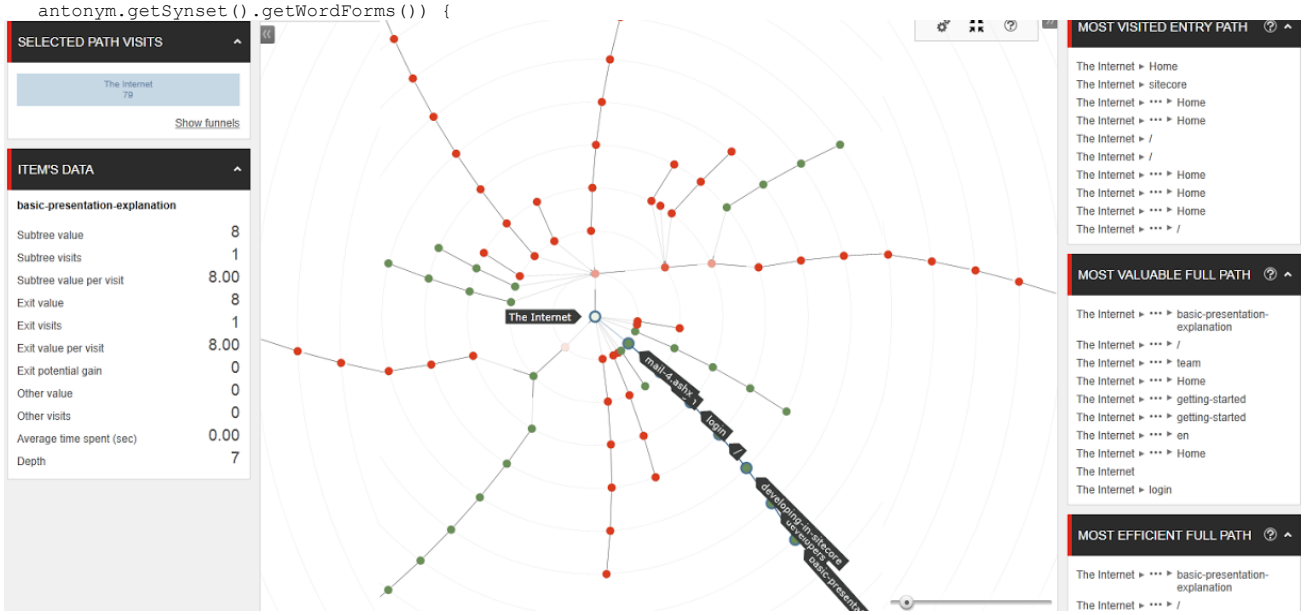


Рисунок 7 – Виведення статистики збору інформації по профілю користувача та його навігації по сайту

DOI 10.15588/1607-3274-2019-4-12

Можливості створення профілів теоретично необмежені. Після використання Chrome браузера в якості одного унікального клієнта, та здійснення купівельної активності на сайті розглянемо отримані результати профілю користувача. Підсумуємо отримані деталі профілю користувача:

– surfing behaviour: new visitors vs. returning visitors, websites visited, etc.;

– purchasing behaviour: popular brands, price ranges, related products, etc.;

– geographical data;

– demographics: age and gender;

– sociological data: family situation, profession, interests, etc.

Запустимо консольну програму для навчання нейромережі для отримання вихідних даних у вигляді таблиці наближеності до списку заданих в системі тегів для контенту (рис. 8).

```
C:\Windows\System32\cmd.exe
* ======================== Tags recommendations report =
* model = [W52/WSJTP.TRAIN.W5]
* testset = [/home/me/WSJTP/WSJTP.TEST]
* ========================================================
* ================ TAGGING SUMMARY =====================
#WORDS = 129654
#KNOWN = 126005 / 129654 --> (97.1856 %)
#UNKNOWN = 3649 / 129654 --> (2.8144 %)
#AMBIGUOUS = 45779 / 129654 --> (35.3086 %)
* ================ ACCURACY PER LEVEL OF AMBIGUITY =====
POS HITS TRIALS ACCURACY MFT-ACCURACY
* --------------------------------------------------------
# 15 / 15 = 100 % 100 %
$ 943 / 943 = 100 % 100 %
ÆÆ 1044 / 1045 = 99.9043 % 99.0431 %
( 186 / 186 = 100 % 100 %
) 187 / 187 = 100 % 100 %
, 6876 / 6876 = 100 % 100 %
. 5381 / 5381 = 100 % 100 %
: 752 / 752 = 100 % 100 %
CC 3237 / 3250 = 99.6 % 99.5692 %
CD 4789 / 4823 = 99.295 % 90.6075 %
DT 11117 / 11183 = 99.4098 % 98.453 %
EX 126 / 126 = 100 % 100 %
FW 7 / 30 = 23.3333 % 20 %
IN 13322 / 13492 = 98.74 % 98.3398 %
JJ 7617 / 8215 = 92.7206 % 85.2708 %
JJR 388 / 423 = 91.7258 % 95.9811 %
JJS 262 / 267 = 98.1273 % 95.5056 %
LS 10 / 15 = 66.6667 % 0 %
MD 1264 / 1267 = 99.7632 % 99.8421 %
NN 17257 / 17834 = 96.7646 % 91.9143 %
NNP 12717 / 13177 = 96.5091 % 85.0118 %
NNPS 98 / 170 = 57.6471 % 49.4118 %
* ================ OVERALL ACCURACY ====================
* --------------------------------------------------------
125966 / 129654 = 97.1555 % 91.3015 %
* ========================================================
C:\Storage\Library\projects\Naz_mag\new>
```

Рисунок 8 – Проміжні результати навчання нейромережі

Оцінимо вихідні дані:

```
# single output{
  'governance': 0.00004324968926091062,
  'risk': 0.007702528578033991,
  'compliance': 0.0002575132225946431,
  'risk management',
  'data management': 0.2071775132225946431,
  'big data': 0.008160047807935744,
  'administration': 0.00015069427192724994 }
```

ВИСНОВКИ

В роботі вирішено задачу розроблення загальної архітектури ІС поширення комерційного контенту в Інтернет-просторі на основі навчання нейронної мережі згідно історії постійної аудиторії для подачі унікального контенту з використанням підходу персоналізації та використання тегів. В роботі також сформульовані загальні вимоги до типової архітектури ІС поширення комерційного контенту на основі підходу персоналізації та використання тегів.

Наукова новизна полягає у розроблені моделі та методу поширення комерційного контенту на основі підходу персоналізації та використання тегів. При цьому використано навчання нейронної мережі для створення тег рекомендацій та доступні на ринку засоби персоналізації. А алгоритм персоналізації дозволяє пов'язати кожного користувача з списком продуктів які найімовірніше його зацікавлять, а також можуть прогнозувати те, що клієнти можуть хотіти бачити, навіть якщо вони ще не знають про це.

Як правило, кожен користувач має різні вимоги до інформації для запиту. Але типові пошукові системи повертають один і той самий результат для одного запиту, поданого різними користувачами. Для вирішення проблеми інформаційного перевантаження та надання користувачам відповідної інформації використовується Web-персоналізація. Персоналізація в Інтернет підвищує точність пошукової системи, спрощує процес пошуку, зберігає час та надає відповідну інформацію користувачам. Персоналізація створює почуття індивідуальності та унікальності. Клієнти почувають себе особливими та важливими, наче компанія звертає на них особливу увагу. Більш того, шляхом сегментації та націлювання на різних покупців, персоналізація відповідає різним потребам кожного клієнта, тим самим оптимізуючи клієнтський досвід, а також той же середній досвід для всіх.

Робота має практичну цінність у розробленні правил перетворення ключових слів інформаційного пошуку конкретного користувача на персоналізований список тегів для навчання нейронної мережі формування рекомендацій кінцевому користувачу згідно його вподобань.

Перспективи подальших досліджень полягають у аналізі статистики функціонування впроваджених аналогічних систем для вдосконалення методів персоналізації у формуванні рекомендацій кінцевому користувачу. Необхідно адаптувати розроблені алгоритми створення списків персоналізованих тегів для україномовног пошуку та відповідно формування рекомендацій кінцевому користувачу. Впровадження цієї системи дасть змогу отримувати доступ до необхдного контенту широкому загалу користувачів, адже сайт буде розміщено у всесвітній павутині, з другого боку інша частина мети створення цієї системи є комерційна складова, а саме отримання прибутків власником чи адміністратором ІС, через механізми е-комерції. Проект у закінченому вигляді має практичне своє застосування, а саме може бути використаний, як один з Інтернет-магазинів у всесвітній мережі, за умови заповнення його реальними продуктами та послугами. Якщо надати оцінку ступеня готовності до впровадження то

DOI 10.15588/1607-3274-2019-4-12

потрібно спочатку провести відповідні дослідження попиту та пропозиції представлених послуг на ринку, перш ніж запускати весь цикл робіт, пов'язаних з електронною комерцією. Успіх залежить не тільки від грамотності та якості побудови сайту, але й від зацікавленості в запропонованих послугах, реклами та відомості ресурсу.

ПОДЯКИ

Роботу виконано в рамках держбюджетної теми «Методи та засоби функціонування систем підтримки прийняття рішень на основі онтологій» (ID:839 2017-05-15 09:20:01 (2459–315)). Дослідження провадилось в межах спільних наукових досліджень кафедри інформаційних систем та мереж НУ «Львівська політехніка» на тему «Дослідження, розроблення і впровадження інтелектуальних розподілених інформаційних технологій та систем на основі ресурсів баз даних, сховищ даних, просторів даних та знань з метою прискорення процесів формування сучасного інформаційного суспільства». Наукові дослідження провадилися також в рамках ініціативної тематики досліджень кафедри ІСМ НУ «Львівська політехніка» на тему «Розроблення інтелектуальних розподілених систем на основі онтологічного підходу з метою інтеграції інформаційних ресурсів».

СПИСОК ЛІТЕРАТУРИ

1. Mobasher B. Data mining for web personalization / B. Mobasher // The adaptive web. – 2007. – Vol. 4321. – P. 90–135.
2. Dinucă C. Web Content Mining. In: University of Petroşani / C. Dinucă, D. Ciobanu // Economics. – 2012. – Vol. 12. – P. 85–92.
3. Xu G. Web content mining / G. Xu, Y. Zhang, L. Li // Web Mining and Social Networking. – 2011. – Vol. 6. – P. 71–87.
4. Khribi M. K. Automatic recommendations for e-learning personalization based on web usage mining techniques and information retrieval / M. K. Khribi, M. Jemni, O. Nasraoui // Advanced Learning Technologies : International Conference, 1–5 July 2008 : proceedings. – Santander, Cantabria, Spain : IEEE, 2008. – P. 241–245.
5. Automatic web content personalization through reinforcement learning / [S. Ferretti, S. Mirri, C. Prandi, P. Salomoni] // Journal of Systems and Software. – 2016. – Vol. 121. – P. 157–169.
6. User attitudes towards news content personalization / [T. Lavie, M. Sela, I. Oppenheim et al] // International journal of human-computer studies. – 2010. – Vol. 68(8). – P. 483–495.
7. Fredrikson M. Repriv: Re-imagining content personalization and in-browser privacy / M. Fredrikson, B. Livshits // Symposium on Security and Privacy: Conference, 22–25 May 2011 : proceedings. – Berkeley, CA, USA : IEEE, 20011. – P. 131–146.
8. Application of neural networks and Kano's method to content recommendation in web personalization / [C. C. Chang., P. L. Chen, F. R. Chiu, Y. K. Chen] // Expert Systems with Applications. – 2009. – Vol. 36(3). – P. 5310–5316.
9. Pat. US7,571,226B1 US Content personalization over an interface with adaptive voice character / H. Partovi, R. Brathwaite, A. Davis, M. McCue, B. Porter, J. Giannandrea, Z. Li (US) ; TellMe Networks, Inc., Mountain View, CA (US). – No.: 09/523,853 ; Marz 14, 2009; August 4, 2009, Patent and Trademark Office. – 20 p.
10. Pat. US2009/0171968A1 US Widget-assisted content personalization based on user behaviors tracked across multiple web sites / F. J. Kane, C. Hicks (US) ; Amazon Technologies Inc (US). – No.: 11/966,817 ; December 28, 2007; Jule 2, 2009, Google Patents. – 24 p.
11. Mirri S. Experiential adaptation to provide user-centered web content personalization / S. Mirri, C. Prandi, P. Salomoni // Advances in Human oriented and Personalized Mechanisms, Technologies, and Services : The Sixth International Conference, October 27 – November 1, 2013: proceedings. – Venice, Italy : IARIA, 2003. – P. 31–36.
12. Fernandez-Luque L. Review of extracting information from the Social Web for health personalization / L. Fernandez-Luque, R. Karlsen, J. Bonander // Journal of medical Internet research. – 2011. – Vol. 13(1). – P. 15.
13. Pat. US8,019,777B2 US Digital content personalization method and system / E. Hauser (US) ; CRICKET MEDIA Inc (US). –No.: 12/795,419 ; June 7, 2010; September 13, 2011, Patent and Trademark Office. – 15 p.
14. Ho S. Y. Timing of adaptive web personalization and its effects on online consumer behavior / S. Y. Ho, D. Bodoff, K. Y. Tam // Information Systems Research. – 2011. – Vol. 22(3). – P. 660–679.
15. Uchyigit G. Personalization techniques and recommender systems / G. Uchyigit, M. Y. Ma. – Singapore: World Scientific,– 2008. – 322 p.
16. Pat. US2006/0020883A1 Web page personalization / N. Kothari, M. Harder, R. Howard, A. Sanabria, S. Schackow (US) ; Microsoft Technology Licensing LLC (US). – No.: 10/857,724 ; May 28, 2004; Januar 26, 2006, Patent and Trademark Office. – 18 p.
17. Zhang H. Construction of ontology-based user model for web personalization / H. Zhang, Y Song., H. T. Song // Lecture Notes in Computer Science. – 2007. – Vol. 4511. – P. 67–76.
18. Pat. US 8,254,892 B2 US Methods and apparatus for anonymous user identification and content personalization in wireless communication / H. Chien (US) ; AT&T Mobility II LLC (US). – No.: 12/468,708 ; September 10, 2009; August 28, 2012, Patent and Trademark Office. – 9 p.
19. Pat. US7,970,664B2 US Content personalization based on actions performed during browsing sessions / G. D. Linden, B. R. Smith, N. K. Zada (US) ; Amazon Technologies Inc (US). – No.: 11/009,732 ; December 10, 2004; June 28, 2011, Patent and Trademark Office. –36 p.
20. Web personalization using web mining: concept and research issue / [P. Mehtaa, B. Parekh, K. Modi, P. Solanki] // International Journal of Information and Education Technology. – 2012. – Vol. 2(5). – P. 510–512.
21. Zhezhnych P. Linguistic Comparison Quality Evaluation of Web-Site Content with Tourism Documentation Objects / P. Zhezhnych, O. Markiv // Advances in Intelligent Systems and Computing. – 2018. – Vol. 689. – P. 656–667.
22. Basyuk T. The main reasons of attendance falling of internet resource / T. Basyuk // Computer Sciences and Information Technologies : Xth International Scientific and Technical Conference, 14–17 September 2015 : proceedings. – Lviv : IEEE, 2015. – P. 91–93.
23. Uniform Method of Operative Content Management in Web Systems / [A. Gozhyj, L. Chyrun, A. Kowalska-Styczen,

DOI 10.15588/1607-3274-2019-4-12

O. Lozynska] // CEUR Workshop Proceedings. – 2018. – Vol. 2136. – P. 62–77.
24. Kravets P. The control agent with fuzzy logic / P. Kravets // Perspective Technologies and Methods in MEMS Design : VIth International Conference, 20–23 April 2010 2015 : proceedings. – Lviv : IEEE, 2015. – P. 40–41.
25. Davydov M. Linguistic Models of Assistive Computer Technologies for Cognition and Communication / M. Davydov, O. Lozynska // Computer Science and Information Technologies : XIth International Scientific and Technical Conference, 6–10 September 2016 : proceedings. – Lviv : IEEE, 2016. – P. 171–175.
26. Design and implementation of visitors queue density analysis and registration method for retail videosurveillance purposes / [Peleshko D., Ivanov Y., Sharov B., Izonin I., Borzov Y.] // Data Stream Mining & Processing : First International Conference, 23–27 August 2016 : proceedings. – Lviv : IEEE, 2016. – P. 159–162.
27. Adaptive moving object segmentation algorithms in cluttered environments / [Y. Ivanov, D. Peleshko, O. Makoveychuk et al] // The Experience of Designing and Application of CAD Systems in Microelectronics : Comference, 24–27 February 2015 : proceedings. – Lviv : IEEE, 2015. – P. 97–99.
28. Vitynskyi P. Hybridization of the SGTM Neural-like Structure through Inputs Polynomial Extension / [P. Vitynskyi, R. Tkachenko, I. Izonin, H. Kutucu] // Data Stream Mining & Processing : Second International Conference, 21–25 August 2018 : proceedings. – Lviv : IEEE, 2018. – P. 386–391.
29. Development of the Non-Iterative Supervised Learning Predictor Based on the Ito Decomposition and SGTM Neural-Like Structure for Managing Medical Insurance Costs / [R. Tkachenko, I. Izonin, P. Vitynskyi et al] // Data. – 2018. – Vol. 3(4). – P. 1–14.
30. Mykich K. Algebraic model for knowledge representation in situational awareness systems / K. Mykich, Y. Burov // Computer Sciences and Information Technologies : nternational Scientific and Technical Conference, 6–10 September 2016 : proceedings. – Lviv : IEEE, 2016. – P. 165–167.
31. Mykich K. Uncertainty in situational awareness systems / K. Mykich, Y. Burov // Modern Problems of Radio Engineering, Telecommunications and Computer Science : 13th International Conference, 623–26 Februar 2016 : proceedings. – Lviv : IEEE, 2016. – P. 729–732.
32. Mykich K. Algebraic Framework for Knowledge Processing in Systems with Situational Awareness / K. Mykich, Y. Burov // Advances in Intelligent Systems and Computing. – 2017. – Vol. 512. – P. 217–227.
33. Mykich K. Research of uncertainties in situational awareness systems and methods of their processing / K. Mykich, Y. Burov // EasternEuropean Journal of Enterprise Technologies. – 2016. – Vol. 1(79). –P. 19–26.
34. The Risk Management Modelling in Multi Project Environment / [V. Lytvyn, V. Vysotska, O. Veres et al] // Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings. – Lviv : IEEE, 2017. – P. 32–35.
35. Vysotska V. Linguistic Analysis of Textual Commercial Content for Information Resources Processing / V. Vysotska // Modern Problems of Radio Engineering, Telecommunications and Computer Science : 13th International Scientific and Technical Conference, 23–26 February 2016 : proceedings. – Lviv : IEEE, 2016. – P. 709–713.
36. Information resources processing using linguistic analysis of textual content / [J. Su, V. Vysotska, A. Sachenko et al] // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : 9th International Conference, 21–23 September 2017 : proceedings. – Bucharest, Romania: IEEE, 2017. – P. 573–578.
37. Content Linguistic Analysis Methods for Textual Documents Classification / [V. Lytvyn, V. Vysotska, O. Veres et al] // Computer Science and Information Technologies : 11th International Scientific and Technical Conference, 6–10 September 2016 : proceedings. – Lviv : IEEE, 2016. – P. 190–192.
38. Bisikalo O.V. Identifying keywords on the basis of content monitoring method in ukrainian texts / O. V. Bisikalo, V. A. Vysotska // Radio Electronics, Computer Science, Control. – 2016. – Vol. 1(36). – P. 74–83.
39. Bisikalo O. V. Sentence syntactic analysis application to keywords identification Ukrainian texts / O. V. Bisikalo, V. A. Vysotska // Radio Electronics, Computer Science, Control. – Vol. 3(38). – 2016. – P. 54–65.
40. Lytvyn V. Application of algorithmic algebra system for grammatical analysis of symbolic computation expressions of propositional logic / V. Lytvyn, I. Bobyk, V. Vysotska // Radio Electronics, Computer Science, Control. – 2016. – Vol. 4(39). – P. 54–67.
41. Alieksieieva K. Technology of commercial web-resource management based on fuzzy logic / K. Alieksieieva, A. Berko, V. Vysotska // Radio Electronics, Computer Science, Control. – Vol. 3(34). – 2015. – P. 71–79.
42. Peculiarities of Content Forming and Analysis in Internet Newspaper Covering Music News / [M. Korobchinsky, V. Vysotska, L. Chyrun, L. Chyrun] // Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings. – Lviv : IEEE, 2017. – P. 52–57.
43. Intellectual System Design for Content Formation / [O. Naum, L. Chyrun, O. Kanishcheva, V. Vysotska] // Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings. – Lviv : IEEE, 2017. – P. 131–138.
44. Application of Sentence Parsing for Determining Keywords In Ukrainian Texts / [Vasyl Lytvyn, Victoria Vysotska, Dmytro Dosyn, Roman Holoschuk, Zoriana Rybchak] // Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings. – Lviv : IEEE, 2017. – P. 326–331.
45. Vysotska V. Process analysis in electronic content commerce system / V. Vysotska, R. Hasko, V. Kuchkovskiy // Computer Science and Information Technologies : Xth International Scientific and Technical Conference, 14–17 September 2015 : proceedings. – Lviv : IEEE, 2015. – P. 120–123.
46. Lytvyn, V. Designing architecture of electronic content commerce system / V. Lytvyn, V. Vysotska // Computer Science and Information Technologies : Xth International Scientific and Technical Conference, 14–17 September 2015 : proceedings. – Lviv : IEEE, 2015. – P. 115–119.

Received 17.06.2019.
Accepted 18.09.2019.

DOI 10.15588/1607-3274-2019-4-12

УДК 004.9

ОСОБЕННОСТИ АРХИТЕКТУРЫ ИНТЕРНЕТ СИСТЕМЫ УПРАВЛЕНИЯ КОММЕРЧЕСКИМ КОНТЕНТОМ НА ОСНОВЕ МЕТОДОВ MACHINE LEARNING, WEB MINING И SEO-ТЕХНОЛОГИЙ

Высоцкая В. А. – канд. техн. наук, доцент, доцент кафедры «Информационные системы и сети», Национальный университет «Львовская политехника», Украина.

Демчук А. Б. – канд. техн. наук, ассистент кафедры «Информационные системы и сети», Национальный университет «Львовская политехника», Украина.

Лытвын В. В. – д-р техн. наук, профессор, заведующий кафедрой «Информационные системы и сети», Национальный университет «Львовская политехника», Украина.

АННОТАЦИЯ

Актуальность. Сегодня большинство корпораций постоянно переосмысливает бизнес с точки зрения возможностей Интернет, а именно его доступность, широкий охват и постоянно меняющиеся потребности пользователя. Web-ресурс электронной коммерции, который обеспечивает удобный пользовательский опыт, в частности, возможность быстро находить необходимые согласно его портеб и вкуса товары, больше поддерживает конкурентные преимущества.

Целью исследования является разработка общей архитектуры интеллектуальной системы распространения коммерческого контента в Интернет-пространстве на основе обучения нейронной сети согласно истории псотийнои айдитории для подачи уникального контента с использованием подхода персонализации и использование тегов.

Метод. Разработана модель информационной системы персонализации коммерческого контента согласно потребностям пользователя. Также разработан метод распространения коммерческого контента на основе подхода персонализации и использования тегов. При этом использовано обучения нейронной сети для создания тегов рекомендаций и доступных на рынке средств персонализации. Разработанный алгоритм персонализации позволяет связать каждого пользователя со списком продуктов, которые вероятнее всего его заинтересуют, а также может прогнозировать то, что клиенты могут хотеть видеть, даже если они еще не знают об этом. Разработанный метод можно использовать для обеспечения более релевантного набора контента. Также разработан метод дает возможность классифицировать соответствующий контент или показать его раньше в процессе перелистывания страниц во избежания потребителями выбора неправильного контента или затраты времени на прокрутки при поиске товара.

Результаты. Разработанная система предназначена для распространения продуктов информационных технологий (публикаций, книг, курсов, видео, файлов и т.д.) с помощью интернета.

Выводы. Внедрение этой системы позволит получать доступ к определенного рода контента широкой общественности пользователей, ведь сайт будет размещен во всемирной паутине, с другой стороны другая часть цели создания этой системы является коммерческая составляющая, а именно получение прибыли владельцем или администратором интеллектуальной системы, через механизмы е- коммерции.

КЛЮЧЕВЫЕ СЛОВА: коммерческий контент, персонализация, Web mining, Machine Learning, SEO-технология, метрики поиска, электронная коммерция, NLP, контент-мониторинг, контент-анализ, статистический лингвистический анализ, квантитативных лингвистика.

UDC 004.9

FEATURES OF THE ARCHITECTURE FOR INTERNET COMMERCIAL CONTENT MANAGEMENT SYSTEM BASED ON METHODS OF MACHINE LEARNING, WEB MINING AND SEO TECHNOLOGIES

Vysotska V. – PhD, Associate Professor of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine.

Demchuk A. – PhD, Assistant of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine.

Lytvyn V. – Dr. Sc., Professor, Head of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine.

ABSTRACT

Context. Today, most corporations are constantly rethinking business from the point of view of the Internet, namely its availability, broad reach and ever-changing needs of the user. The e-commerce web-site, which provides user-friendly experience, including the ability to quickly find the products that are necessary for its portables and taste, is more in favor of competitive advantage.

Objective of the study is to develop a general architecture of the intellectual system for the distribution of commercial content in the Internet space, based on the study of the neural network in accordance with the history of the psychedelic region to provide unique content using the approach of personalization and the use of tags.

Method. The model of information system of commercial content personalization for the user needs is developed. Also the method of distributing commercial content based on the approach of personalization and the tags use is developed. In this case, the neural network training is used to create a recommendation tag and marketable personalization tools. The customization algorithm allows you to associate each user with a list of products that they are most likely to be interested in, and can predict what customers might want to see even if they do not yet know about it. The developed method can be used to provide a more relevant set of content. Also, the developed method gives the opportunity to classify the relevant content or show it earlier in the process of rolling the pages to avoid consumers choosing the wrong content or spending time scrolling when looking for a product.

Results. The developed system is intended for distribution of information technology products (publications, books, courses, videos, files, etc.) through the Internet.

DOI 10.15588/1607-3274-2019-4-12

Conclusions. Implementation of this system will allow access to certain types of content to the general public, since the site will be placed on the World Wide Web; on the other hand, another part of the purpose of creating this system is a commercial component, namely, the receipt of profits by the owner or administrator of the intellectual system, through the mechanisms of e- commerce.

KEYWORDS: commercial content, personalization, Web mining, Machine Learning, SEO technology, metrics search, e-commerce, NLP, content monitoring, content analysis, statistical linguistic analysis, quantitative linguistics.

REFERENCES

1. Mobasher B. Data mining for web personalization, *The adaptive web*, 2007, Vol. 4321, pp. 90–135.
2. Dinucă C., Ciobanu D. Web Content Mining. In: University of Petroşani, *Economics,* 2012, Vol. 12, pp. 85–92.
3. Xu G., Zhang Y., Li L. Web content mining, *Web Mining and Social Networking*, 2011, Vol. 6, pp. 71–87.
4. Khribi M. K., Jemni M., Nasraoui O. Automatic recommendations for e-learning personalization based on web usage mining techniques and information retrieval, *Advanced Learning Technologies : International Conference, 1–5 July 2008 : proceedings. Santander, Cantabria, Spain*, *IEEE,* 2008, pp. 241–245.
5. Ferretti S., Mirri S., Prandi C., Salomoni P. Automatic web content personalization through reinforcement learning, *Journal of Systems and Software,* 2016, Vol. 121, pp. 157–169.
6. Lavie T., Sela M., Oppenheim I., Inbar O., Meyer J. User attitudes towards news content personalization, *International journal of human-computer studies*, 2010, Vol. 68(8), pp. 483–495.
7. Fredrikson M., Livshits B. Repriv: Re-imagining content personalization and in-browser privacy, *Symposium on Security and Privacy: Conference, 22–25 May 2011 : proceedings.* Berkeley, CA, USA, IEEE, 20011, pp. 131–146.
8. Chang C., Chen P., Chiu F., Chen Y. Application of neural networks and Kano's method to content recommendation in web personalization, *Expert Systems with Applications,* 2009, Vol. 36(3), pp. 5310–5316.
9. Partovi H., Brathwaite R., Davis A., McCue M., Porter B., Giannandrea J., Li Z. (US) Pat. US7,571,226B1 US Content personalization over an interface with adaptive voice character, U.S. ; TellMe Networks, Inc., Mountain View, CA (US), No.: 09/523,853 ; Marz 14, 2009; August 4, 2009, Patent and Trademark Office, 20 p.
10. Kane F. J., Hicks C. (US) Pat. US2009/0171968A1 US Widget-assisted content personalization based on user behaviors tracked across multiple web sites, Amazon Technologies Inc (US), No.: 11/966,817 ; December 28, 2007; Jule 2, 2009, Google Patents, 24 p.
11. Mirri S., Prandi C., Salomon P. Experiential adaptation to provide user-centered web content personalization, *Advances in Human oriented and Personalized Mechanisms, Technologies, and Services : The Sixth International Conference, October 27 – November 1, 2013: proceedings.* Venice, Italy, IARIA, 2003, pp. 31–36.
12. Fernandez-Luque L., Karlsen R., Bonander J. Review of extracting information from the Social Web for health personalization, *Journal of medical Internet research*, 2011, Vol. 13(1), P. 15.
13. Hauser E. (US) Pat. US8,019,777B2 US Digital content personalization method and system /; CRICKET MEDIA Inc (US). No.: 12/795,419 ; June 7, 2010; September 13, 2011, Patent and Trademark Office, 15 p.
14. Ho S. Y., Bodoff D., Tam K. Y. Timing of adaptive web personalization and its effects on online consumer behavior *Information Systems Research*, 2011, Vol. 22(3), pp. 660–679.
15. Uchyigit G., Ma M. Y. Personalization techniques and recommender systems. Singapore, World Scientific, 2008, 322 p.
16. Kothari N., Harder M., Howard R., Sanabria A., Schackow S. Pat. US2006/0020883A1 Web page personalization / (US) ; Microsoft Technology Licensing LLC (US). No.: 10/857,724 ; May 28, 2004; Januar 26, 2006, Patent and Trademark Office. – 18 p.
17. Zhang H., Song Y., Song H. T. Construction of ontology-based user model for web personalization, *Lecture Notes in Computer Science*, 2007, Vol. 4511, pp. 67–76.
18. Chien H. (US) Pat. US 8,254,892 B2 US Methods and apparatus for anonymous user identification and content personalization in wireless communication; AT&T Mobility II LLC (US). No.: 12/468,708 ; September 10, 2009; August 28, 2012, Patent and Trademark Office, 9 p.
19. Linden G. D., Smith B. R., Zada N. K. (US) Pat. US7,970,664B2 US Content personalization based on actions performed during browsing sessions; Amazon Technologies Inc (US). No.: 11/009,732 ; December 10, 2004; June 28, 2011, Patent and Trademark Office. –36 p.
20. Mehtaa P., Parekh B., Modi K., Solanki P. Web personalization using web mining: concept and research issue, *International Journal of Information and Education Technology*, 2012, Vol. 2(5), pp. 510–512.
21. Zhezhnych P., Markiv O. Linguistic Comparison Quality Evaluation of Web-Site Content with Tourism Documentation Objects, *Advances in Intelligent Systems and Computing*, 2018, Vol. 689, pp. 656–667.
22. Basyuk T. The main reasons of attendance falling of internet resource, C*omputer Sciences and Information Technologies : Xth International Scientific and Technical Conference, 14–17 September 2015 : proceedings*. Lviv, IEEE, 2015, pp. 91–93.
23. Gozhyj A., Chyrun L., Kowalska-Styczen A., Lozynska O. Uniform Method of Operative Content Management in Web Systems, *CEUR Workshop Proceedings*, 2018, Vol. 2136, pp. 62–77.
24. Kravets P. The control agent with fuzzy logic, *Perspective Technologies and Methods in MEMS Design : VIth International Conference, 20–23 April 2010 2015 : proceedings*. Lviv, IEEE, 2015, pp. 40–41.
25. Davydov M., Lozynska O. Linguistic Models of Assistive Computer Technologies for Cognition and Communication, *Computer Science and Information Technologies : XIth International Scientific and Technical Conference, 6–10 September 2016 : proceedings*. Lviv, IEEE, 2016, pp. 171–175.
26. Peleshko D., Ivanov Y., Sharov B., Izonin I., Borzov Y. Design and implementation of visitors queue density analysis and registration method for retail videosurveillance purposes, *Data Stream Mining & Processing : First International Conference, 23–27 August 2016 : proceedings*. Lviv, IEEE, 2016, pp. 159–162.
27. Ivanov Y., Peleshko D., Makoveychuk O., Izonin I., Malets I., Lotoshunska N., Batyuk D. Adaptive moving object segmentation algorithms in cluttered environments, *The Experience of Designing and Application of CAD Systems in*

DOI 10.15588/1607-3274-2019-4-12

Microelectronics : Comference, 24 February 2015 : proceedings. Lviv, IEEE, 2015, pp. 97–99.
28. Vitynskyi P., Tkachenko R., Izonin I., Kutucu H. Hybridization of the SGTM Neural-like Structure through Inputs Polynomial Extension, *Data Stream Mining & Processing : Second International Conference, 21–25 August 2018 : proceedings*. Lviv, IEEE, 2018, pp. 386–391.
29. Tkachenko R., Izonin I., Vitynskyi P., Lotoshynska N., and Pavlyuk O. Development of the Non-Iterative Supervised Learning Predictor Based on the Ito Decomposition and SGTM Neural-Like Structure for Managing Medical Insurance Costs, *Data*, 2018, Vol. 3(4), pp. 1–14.
30. Mykich K., Burov Y. Algebraic model for knowledge representation in situational awareness systems, *Computer Sciences and Information Technologies : 11th International Scientific and Technical Conference, 6–10 September 2016 : proceedings*. Lviv, IEEE, 2016, pp. 165–167.
31. Mykich K., Burov Y. Uncertainty in situational awareness systems, *Modern Problems of Radio Engineering, Telecommunications and Computer Science : 13th International Conference, 623–26 Februar 2016 : proceedings*. Lviv, IEEE, 2016, pp. 729–732.
32. Mykich K. Algebraic Framework for Knowledge Processing in Systems with Situational Awareness, *Advances in Intelligent Systems and Computing*, 2017, Vol. 512, pp. 217–227.
33. Mykich K., Burov Y. Research of uncertainties in situational awareness systems and methods of their processing, *Eastern European Journal of Enterprise Technologies,* 2016, Vol. 1(79), pp. 19–26.
34. Lytvyn V., Vysotska V., Veres O., Rishnyak I., Rishnyak H. The Risk Management Modelling in Multi Project Environment, *Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings.* Lviv, IEEE, 2017, pp. 32–35.
35. Vysotska V. Linguistic Analysis of Textual Commercial Content for Information Resources Processing, *Modern Problems of Radio Engineering, Telecommunications and Computer Science : International Scientific and Technical Conference, 23–26 February 2016 : proceedings*. Lviv, IEEE, 2016, pp. 709–713.
36. Su J., Vysotska V., Sachenko A., Lytvyn V., Burov Y. Information resources processing using linguistic analysis of textual content, *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : 9th International Conference, 21–23 September 2017 : proceedings*. Bucharest, IEEE, 2017, pp. 573–578.
37. Lytvyn V., Vysotska V., Veres O., Rishnyak I., Rishnyak H. Content Linguistic Analysis Methods for Textual Documents Classification, *Computer Science and Information Technologies : 11th International Scientific and Technical Conference, 6–10 September 2016 : proceedings*. Lviv, IEEE, 2016, pp. 190–192.
38. Bisikalo O. V., Vysotska V. A. Identifying keywords on the basis of content monitoring method in ukrainian texts, *Radio Electronics, Computer Science, Control*, 2016, Vol. 1(36), pp. 74–83.
39. Bisikalo O. V., Vysotska V. A. Sentence syntactic analysis application to keywords identification Ukrainian texts, *Radio Electronics, Computer Science, Control*, 2016, Vol. 3(38), pp. 54–65.
40. Lytvyn V., Bobyk I., Vysotska V. Application of algorithmic algebra system for grammatical analysis of symbolic computation expressions of propositional logic, *Radio Electronics, Computer Science, Control*, 2016, Vol. 4(39), pp. 54–67.
41. Alieksieieva K., Berko A., Vysotska V. Technology of commercial web-resource management based on fuzzy logic, *Radio Electronics, Computer Science, Control,* 2015, Vol. 3(34), pp. 71–79.
42. Korobchinsky M., Vysotska V., Chyrun L., Chyrun L. Peculiarities of Content Forming and Analysis in Internet Newspaper Covering Music News, *Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings*. Lviv, IEEE, 2017, pp. 52–57.
43. Naum O., Chyrun L., Kanishcheva O., Vysotska V. Intellectual System Design for Content Formation, *Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings*. Lviv, IEEE, 2017, pp. 131–138.
44. Lytvyn Vasyl, Vysotska Victoria, Dosyn Dmytro, Holoschuk Roman, Rybchak Zoriana Application of Sentence Parsing for Determining Keywords In Ukrainian Texts, *Computer Science and Information Technologies : 12th International Scientific and Technical Conference, 5–8 September 2017 : proceedings*. Lviv, IEEE, 2017, pp. 326–331.
45. Vysotska V., Hasko R., Kuchkovskiy V. Process analysis in electronic content commerce system, *Computer Science and Information Technologies : Xth International Scientific and Technical Conference, 14–17 September 2015 : proceedings*. Lviv, IEEE, 2015, pp. 120–123.
46. Lytvyn V., Vysotska V. V. Designing architecture of electronic content commerce system, *Computer Science and Information Technologies : Xth International Scientific and Technical Conference, 14–17 September 2015 : proceedings*. Lviv, IEEE, 2015, pp. 115–119.

DOI 10.15588/1607-3274-2019-4-12

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

УДК 006.015.5

ПРОГРАМНІ ЗАСОБИ МОНІТОРИНГУ ЦІННОСТІ ЯК ІНСТРУМЕНТ АДАПТАЦІЇ ДО ЗМІН У ВИМОГАХ СТЕЙКХОЛДЕРІВ ПРОЕКТІВ

Гусєва Ю. Ю. – канд. техн. наук, доцент, доцент кафедри управління проектами в міському господарстві і будівництві, Харківський національний університет міського господарства імені О. М. Бекетова, Харків, Україна.

Чумаченко І. В. – д-р техн. наук, професор, завідувач кафедри управління проектами в міському господарстві і будівництві, Харківський національний університет міського господарства імені О. М. Бекетова, Харків, Україна.

АНОТАЦІЯ

Актуальність. В умовах динамічного середовища, коли вимоги зацікавлених сторін можуть змінюватись, традиційні методи моніторингу і контролю виконання програмного проекту мають певні обмеження. Отже, є необхідність в створенні підходів та відповідних програмних засобів для моніторингу виконання вимог стейкхолдерів проекту, зокрема, з урахуванням їх особистісної оцінки цінності вимог та ресурсів.

Мета роботи. Розробка методу моніторингу цінності вимог стейкхолдерів програмного проекту та відповідних інструментів його впровадження.

Метод. Використано методи аналізу та синтезу, операції над матрицями, систему вагових коефіцієнтів Фішберна, методи теорії управління проектами. Запропоновано ціннісний підхід до моніторингу вимог зацікавлених сторін проекту. Запропоновано підходи до визначення цінності вимог стейкхолдерів на основі наявної інформації з типових проектних документів. Запропоновано метод моніторингу цінності вимог стейкхолдерів проектів, зокрема, програмних, та відповідні інструменти його впровадження.

Результати. На основі ціннісного підходу до моніторингу вимог розроблено програмні інструменти відстеження досягнення планової цінності проекту. Відповідність запропонованого методу процесам традиційного проектного менеджменту дає змогу використовувати стандартне програмне забезпечення для формування вихідних даних та відображення результатів розрахунків.

Висновки. На основі методу освоєних вимог проекту розроблено метод моніторингу цінності вимог, який, на відміну від існуючих, дозволить враховувати особистісні оцінки цінності вимог та ресурсів під час моніторингу виконання проекту, здійснювати відповідні прогнози та розробляти стратегії роботи з певними зацікавленими сторонами або їх групами. Інструменти використання запропонованого методу в середовищі MS Project забезпечують інформаційну підтримку для прийняття ґрунтовних рішень щодо адаптації проекту до змін у вимогах стейкхолдерів, зокрема, розраховується відхилення у досягненні цінності за розкладом та індекс досягнення цінності за розкладом. Перспективою подальших досліджень є вирішення задачі оптимізації розподілу ресурсів у проекті за умов максимізації досягнутої цінності проекту.

КЛЮЧОВІ СЛОВА: управління вимогами, програмний проект, цінність, моніторинг, стейкхолдер.

АБРЕВІАТУРИ

АС – фактичний обсяг ресурсів (в грошовій формі), що витрачено на виконання робіт проекту на момент звіту за освоєним обсягом;

ACWP – Actual Cost of Work Performed (фактична вартість виконаних робіт);

BCWP – Budgeted Cost for Work Performed (бюджетні витрати на виконану роботу);

BCWS – Budgeted Cost for Work Performed (бюджетна вартість запланованої роботи);

CPIR – індекс виконання вимог стейкхолдерів за вартістю;

CR – відхилення у виконанні вимог за вартістю;

ER – фактичний обсяг вимог (в грошовій формі), що дійсно виконано на момент звіту за освоєним обсягом;

ES – Earned Schedule (метод освоєного розкладу);

EValM – метод моніторингу досягнення вимог проекту;

EVM – Earned Value Method (метод освоєного обсягу);

PMBOK – Project Management Body Of Knowledge;

PMI – Project Management Institute;

PR – запланований обсяг вимог (в грошовій формі), що за планом повинен бути виконаним на момент звіту за освоєним обсягом;

SPIR – індекс виконання вимог стейкхолдерів за розкладом;

SR – відхилення у виконанні вимог за розкладом;

WBS – Work Breakdown Structure (ієрархічна структура робіт проекту).

НОМЕНКЛАТУРА

EVal – фактична цінність проекту, яку досягнуто на момент звіту;

F – функція, що описує взаємозв'язок між двома елементами моделі;

m – кількість робіт рівня i–1;

$M_{i,i-1}$ – матриця взаємозв'язків робіт рівнів i та i–1 ієрархічної структури робіт проекту;

n – кількість робіт рівня i;

PVal – запланована цінність проекту, яка повинна бути досягнутою на момент звіту;

req – множина вимог;

Req_{pk} – k-та вимога p-го стейкхолдера;

R_p – ряд пріоритетів цінностей вимог p-го стейкхолдера;

DOI 10.15588/1607-3274-2019-4-13

RVal – матриця розподілу цінностей зацікавлених сторін за роботами проекту;

SPIVal – індекс досягненні цінності за розкладом;

St – множина стейкхолдерів;

St_u – u-й стейкхолдер проекту;

SVal – відхилення у досягненні цінності за розкладом;

u – кількість стейкхолдерів;

Val – матриця розподілу вимог між стейкходерами проекту;

Val_{pk} – оцінка цінності k-ої вимоги p-го стейкхолдера;

w_{ij} – j-та робота i-го рівня ієрархічної структури робіт проекту;

z – кількість вимог;

Φ – функція, що описує взаємозв'язок між двома елементами моделі у нечіткій формі.

ВСТУП

Моніторинг і контроль програмного проекту, зазвичай, здійснюється у три етапи: встановлення стандартів ефективності, порівняння фактичних показників з цими стандартами та вжиття необхідних коригувальних дій [1].

Об'єктом дослідження є процеси моніторингу і контролю у програмному проекті, а **предметом** – методи моніторингу вимог у програмному проекті.

На цей час дослідниками розроблено різноманіття відповідних рішень але, слід зазначити, що існуючи методи переважно спрямовані на контроль часу і вартості в проекті, як основних обмежень – сторін його «трикутника». При цьому третьою стороною трикутника є зміст проекту, який, в свою чергу, визначається вимогами його стейкхолдерів. В умовах динамічного середовища вимоги зацікавлених сторін можуть змінюватись, і якщо для проектів, що виконуються за гнучкими фреймворками, ці зміни відстежуються за рахунок ітеративності, для традиційних програмних проектів загальновідомих методів моніторингу і прогнозу виконання вимог не існує. На основі аналізу методів управління зацікавленими сторонами авторами було запропоновано метод освоєних вимог [2], та відповідні програмні інструменти [3, 4]. Розширення цього методу дозволяє відстежувати також ризики проекту [5]. Таким чином, якщо метод освоєного обсягу [6, 7] дозволяє відстежувати прогрес проекту з точки зору виконання його робот вчасно і в межах бюджету, то метод освоєних вимог пов'язує певні вимоги з роботами проекту і дає змогу проводити моніторинг виконання саме вимог, що, в свою чергу, дозволяє проектній команді адаптуватися до ймовірних змін у вимогах зацікавлених сторін.

Обмеженням цього методу є необхідність визначення обсягу вимог у грошовій формі та відсутність можливості враховувати особистісну оцінку вимог та ресурсів певним стейкхолдером. Ці обмеження знімає підхід, який буде відстежувати не грошовий обсяг виконаних вимог, а цінність, яку отримують зацікавлені сторони при виконанні програмного проекту – перехід до моніторингу цінності вимог. Теоретичною базою для такого підходу (у визначенні цінності) може бути, наприклад, стандарт P2M (з точки зору якого проект – це захід, орієнтований на створення цінності, що базується на певній місії, здійснюється в домовлений період часу і в обмеженнях у вигляді ресурсів і зовнішніх обставин).

Отже, більш загальний підхід до моніторингу виконання вимог зацікавлених сторін програмного проекту може передбачати відстеження виконання не переліку вимог, а досягнення певної цінності для кожного стейкхолдера і проекту в цілому.

Стосовно програмних засобів підтримки процесів моніторингу і контролю, то основним інструментом на сьогодні є MS Project та його аналоги (з підтримкою методу освоєного обсягу). Для проектів, що плануються та виконуються за гнучкими методологіями, це такі сервіси, як Jira або Trello.

Метою даної роботи є розробка методу моніторингу цінності вимог стейкхолдерів проектів, зокрема, програмних, та відповідних інструментів його впровадження.

1 ПОСТАНОВКА ЗАДАЧІ

Вхідними даними для проведення аналізу є: матриця взаємозв'язків робіт WBS програмного проекту $M_{i,i-1}$; матриця відстеження вимог R_i; реєстр стейкхолдерів (зацікавлених сторін) програмного проекту St.

Задача моніторингу досягнення цінності полягає в тому, щоб на підставі визначеної запланованої та фактичної цінності програмного проекту отримати значення відхилення та індексу досягнення цінності за розкладом.

Отже, результуючими змінними є SVal та SPIVal. Обмеженням методу є наявність відносин типу $\mathrm{Re}q_{ps} \succ \mathrm{Re}q_{pk}$ між пріоритетами (цінностями) вимог певного стейкхолдера.

Результатом використання методу моніторингу цінності вимог є інформаційна підтримка прийняття рішень щодо адаптації програмного проекту до змін у вимогах стейкхолдерів.

2 ОГЛЯД ЛІТЕРАТУРИ

Існуючи методи моніторингу і контролю проектів можна класифікувати за чотирма основними категоріями: оцінка виконання проекту, прогнозування остаточної тривалості та вартості проекту, визначення контрольних точок, а також генерація сигналів раннього попередження для запуску коригувальних дій [1].

В таблиці 1 представлено критичний огляд та узагальнення відповідних досліджень. Показано, що переважна більшість відомих методів концентруються на контролі вартості та тривалості проекту, при чому вони еволюціонували від простої фіксації відхилень від плану (традиційні S-криві) до відстеження прогресу виконання проекту з використанням ймовірнісного підходу та моделювання.

DOI 10.15588/1607-3274-2019-4-13

Таблиця 1 – Результати критичного аналізу методів контролю у проектах

Група	Метод	Джерело	Характеристика
Моніторинг і контроль прогресу	S-крива	[6]	Концепцію S-кривої було впроваджено як систему раннього попередження для контролю виконання проекту. Порівнюється фактичний прогрес і планові показники вартості. У разі, якщо зміни фактичної вартості перевищують визначені межі, необхідно вжити певні заходи.
	EVM	[6, 7]	S-криві мають багато обмежень через їх агрегативність, тому розробляється метод освоєного обсягу (основний інструмент вимірювання продуктивності проекту у традиційному проектному менеджменті на цей час). EVM базується на трьох ключових показниках: бюджетна вартість запланованої роботи BCWS (або планова вартість PV), фактична вартість виконаних робіт ACWP, (або фактичні витрати AC), а також бюджетні витрати на виконану роботу BCWP (або освоєний обсяг EV). Співвідношення цих показників дає проектному менеджеру інформацію щодо стану виконання проекту.
	Розширення EVM, нові показники	[8–15]	Якщо традиційний EVM передбачає визначеність щодо тривалості та вартості проекту, розширені методи EVM включають аналіз ризиків проекту [8, 9], у тому числі пропонується використання методу Монте Карло для моделювання BCWS, ACWP та BCWP [10]. Метод Earned Schedule (ES) [11], навпаки, звужує межи використання традиційного EVM, залишаючи для аналізу лише показники часу для підвищення точності оцінювання ефективності графіка проекту та прогнозування його тривалості. З метою підвищення ефективності EVM в розрізі контролю за витратами в реальному часі, автори [12] пропонують оцінювати прогрес і вартість шляхом динамічної оцінки на основі часових інтервалів. Автори [13] запровадили новий підхід до встановлення меж для метрики SPI, щоб оцінити споживання буфера під час виконання проекту. Інші модифіковані підходи EVM, як і ES, зосереджені на прогнозуванні тривалості проекту [14]. Наприклад, автори [15] у спробі підвищити точність прогнозування тривалості проекту, об'єднали EVM з кривими навчання для моделювання нелінійних змін у роботі команди проекту.
Прогноз	Детермінований та ймовірнісний EVM	[16, 17]	Крім відстеження прогресу проекту, EVM використовується для прогнозування часу та витрат на завершення. Методи прогнозування часу на основі EVM можуть бути згруповані у два основні класи: детерміновані та ймовірнісні підходи [16]. Детерміністичні методи генерують точкову оцінку кінцевої тривалості проекту та часто застосовуються для аналізу грошових потоків [17]. Ймовірнісні методи забезпечують довірчі інтервали або розподіли можливих тривалостей.
	Стохастичні S-криві	[17, 18]	Окрім EVM, найбільш поширеними методами прогнозування є статистичні методи. До них відносяться curve fitting і регресійний аналіз. Стохастичні S-криві дають верхню і нижню межі для діапазону прийнятних результатів на основі невизначеності про прогнози. Ці стохастичні методи можуть бути розширені, щоб запропонувати коригувальні дії [17]. S-криві також є основою для прогнозування грошових потоків [18].
	Регресійний аналіз	[14]	Регресійний аналіз часто застосовується для оцінки форми S-кривої та прогнозування грошового потоку. Екстраполюючи S-криву до завершення проекту, отримують оцінки часу та вартості по завершенні. Статистичні методи також були інтегровані в EVM з метою поліпшення його прогнозування [14].
	Нейронні мережі	[16]	Техніки штучного інтелекту, такі як нейронні мережі та системи на основі знань, зазвичай використовуються до початку проекту як засоби прогнозування часу [17].
Контрольні точки	Фіксовані та динамічні	[19]	Контроль за проектом зосереджується на критичних порушеннях, що виникають під час виконання проекту на потенційних «контрольних точках». Час цих контрольних точок може бути або фіксований до початку проекту, або динамічно змінюватися під час виконання проекту відповідно до стану виконання розкладу [19].
Коригувальні дії	Статистичні контрольні діаграми	[20]	Під час виконання проекту індекси EVM, такі як CPI та SPI, надають інформацію про ефективність роботи. Однак, ці індекси відносяться до витрат і графіку виконання тільки на дату звіту і не відстежують динаміку. Статистичні контрольні діаграми намагаються подолати це обмеження за допомогою графічного відображення варіацій [20].
	Імітаційні моделі	[8, 10]	На додаток до статистичних контрольних карт, імітаційні моделі також часто використовуються для надання попереджувальних сигналів керівнику проекту для вжиття відповідних коригувальних дій.

Але найбільш використовуваним на сьогодні є метод освоєного обсягу, який, до того ж, рекомендується до використання PMI PMBOK та має свій власний стандарт [6, 7].

Для компенсації відсутності інструментів моніторингу і контролю вимог зацікавлених сторін проекту в роботах [2–5] авторами запропоновано підхід, який дозволяє відстежувати і контролювати виконання вимог стейкхолдерів проекту.

Так, визначено показники методу освоєного обсягу вимог зацікавлених сторін проекту: PR, ER, AC, SR, CR, індекси SPIR та CPIR. Дані показники та індекси є підставою для подальшого прогнозу виконання проекту і визначають необхідність та напрям корегувальних дій. Надалі пропонується розвинення цього методу з переходом до моніторингу цінності програмного проекту, що надасть змогу, зокрема, враховувати нематеріальні вимоги та балансувати інтереси стейкхолдерів з урахуванням їх особистісних оцінок цінності вимог та ресурсів в проекті. Наступним етапом є розробка програмних засобів реалізації запропонованого методу.

DOI 10.15588/1607-3274-2019-4-13

3 МАТЕРІАЛИ І МЕТОДИ

Як вказано у [21], зв'язки між роботами різних рівнів WBS можуть бути представлені у вигляді матриці (1), елементи якої вказують на наявність або відсутність зв'язку між роботами *i*-го та (*i*–1)-го рівнів: $F = 1$, якщо зв'язок є, і $F = 0$ за відсутністю зв'язку (1).

У свою чергу, кожна з елементарних робіт програмного проекту може бути асоційована з певними вимогами стейкхолдерів, виконання яких підтримує дана робота (2):

$$M_{i,i-1}=\begin{array}{c|ccc} & w_{i-1,1} & \dots & w_{i-1,m} \\ w_{i,1} & F(w_{i,1},w_{i-1,1}) & \dots & F(w_{i,1},w_{i-1,m}) \\ w_{i,2} & F(w_{i,2},w_{i-1,1}) & \dots & F(w_{i,2},w_{i-1,m}) \\ \dots & \dots & \dots & \dots \\ w_{i,n} & F(w_{i,n},w_{i-1,1}) & \dots & F(w_{i,n},w_{i-1,m}) \end{array} \quad (1)$$

$$Req_i=\begin{array}{c|ccc} & w_{i,1} & \dots & w_{i,n} \\ req_1 & \Phi(req_1,w_{i,1}) & \dots & \Phi(req_1,w_{i,n}) \\ req_2 & \Phi(req_2,w_{i,1}) & \dots & \Phi(req_2,w_{i,n}) \\ \dots & \dots & \dots & \dots \\ req_z & \Phi(req_z,w_{i,1}) & \dots & \Phi(req_z,w_{i,n}) \end{array} \quad (2)$$

Показано, що взаємозв'язок вимог стейкхолдерів програмного проекту та робіт *i*-го рівня може бути заданий у нечіткій формі.

Якщо $\Phi(req_k, w_{i,j}) : req_k \times w_{i,j} \to [0;1]$ – це функція приналежності нечіткого бінарного відношення (2), то для всіх $req_k \in req$ та $w_{i,j} \in w_i$ функція $\Phi(req_k, w_{i,j})$ – це ступінь, у якому виконання *j*-ї роботи *i*-го рівня зумовлює виконання вимоги *k*.

Якщо традиційні методи відстежують вартість виконання робіт проекту, то запропонований в даній роботі підхід надає можливість відстежувати цінність вимоги для певного стейкхолдера:

$$Val=\begin{array}{c|ccc} & req_1 & \dots & req_z \\ st_1 & \mathrm{Val}(st_1,req_1) & \dots & \mathrm{Val}(st_1,req_z) \\ st_2 & \mathrm{Val}(st_2,req_1) & \dots & \mathrm{Val}(st_2,req_z) \\ \dots & \dots & \dots & \dots \\ st_u & \mathrm{Val}(st_u,req_1) & \dots & \mathrm{Val}(st_u,req_z) \end{array}. \quad (3)$$

Так, матриця (3) задає взаємозв'язок між вимогами та їх цінністю для кожного зі стейкхолдерів. Тоді формула $R\mathrm{Val} = Req_i \cdot \mathrm{Val}$ задає розподіл цінностей зацікавлених сторін за роботами програмного проекту.

Відстеження досягнення планової цінності проекту пропонується здійснювати через наступну низку показників:

– запланована цінність програмного проекту, яка повинна бути досягнутою на момент звіту;

– фактична цінність програмного проекту, яку дійсно досягнуто на момент звіту;

– відхилення у досягненні цінності за розкладом $S\mathrm{Val} = E\mathrm{Val} - P\mathrm{Val}$;

– індекс досягнення цінності за розкладом $SPI\mathrm{Val} = \dfrac{E\mathrm{Val}}{P\mathrm{Val}}$.

Для отримання вхідних даних (PVal, EVal) необхідно запропонувати інструменти для кількісної оцінки цінності виконання вимог. На основі [22–24] пропонується використовувати наступні способи:

Безпосереднє оцінювання. Метод полягає у віднесенні цінності певної вимоги до деякого значення за оціночною шкалою. Для подальшої обробки отримані оцінки мають бути пронормовані, тобто їх сума має бути приведена до одиниці шляхом ділення кожної оцінки на їх загальну суму.

Цінність вимоги може, зокрема, визначатися її пріоритетом. Наприклад, за стандартом PMBOK, параметри, пов'язані з кожною вимогою, фіксуються в матриці відстеження вимог, де вказується й оцінка пріоритетності кожної вимоги.

Ряд пріоритетів. Якщо відомі лінійні співвідношення компонентів ряду цінностей вимог (пріоритетів вимог), для оцінки значень цінностей Val_{pk}, $p = \overline{1,u}$, $k = \overline{1,z}$ можуть бути використані формули Фішберна. На основі вербальної (чи статистичної) інформації здійснюється якісне відображення пріоритетів цінностей вимог. Якщо для кожних двох вимог Req_{ps} та Req_{pk} є підстави вважати, що $\mathrm{Re}\, q_{ps} \succ \mathrm{Re}\, q_{pk}$, $s,k = \overline{1,z}$, то можна побудувати ряд пріоритетів всіх цінностей вимог *p*-го стейкхолдера R_p = [Req_{p1}; Req_{p2}; ...[Req_{pk}; Req_{pk+1}]; ...; Req_{pz}], де Req_{p1} – вимога з найвищим пріоритетом; Req_{pz} – з найнижчим; внутрішніми квадратними дужками у формулі відзначені рівнозначні цінності $Req_{pk} \sim Req_{pk+1}$. Отже, згідно з побудованим рядом пріоритетів $\mathrm{Val}_{p1} \ge \mathrm{Val}_{p2} \ge \ldots \ge \mathrm{Val}_{pz}$.

Для даної ситуації Фішберн висунув гіпотезу, що для практичних досліджень достатньо вибрати оцінки апріорних значень цінності у вигляді спадної арифметичної прогресії, і показав, що їх можна обчислювати за формулою:

$$\mathrm{Val}_{pk} = \frac{2(z-k+1)}{z(z+1)}. \quad (4)$$

Бінарне співвідношення. У випадку, коли на вербальному рівні здійснена побудова ряду пріоритетів і суб'єкт управління володіє додатковою інформацією, можна здійснити кількісне уточнення ряду пріоритетів.

Це уточнення можна подати у вигляді ряду бінарних відношень пріоритетів RV = {v_{p1}; v_{p2};...; v_{pz}}, де v_{pk} – це числові оцінки результатів попарних порівнянь між собою всіх цінностей виконання вимог проекту.

Наприклад, якщо v_{pk}=*t*, то це вказує на те, що цінність вимоги Req_{pk} в *t* раз більша за цінності вимоги Req_{pk+1}. Якщо, p_{kj}=1, це вказує на однакову цінність вимог Req_{pk} та Req_{pk+1}.

Якщо покласти v_{pz} = 1, то для обчислення відповідних оцінок цінностей можна скористатись формулою:

DOI 10.15588/1607-3274-2019-4-13

$$Val_{pk} = \frac{\prod_{s=k}^{z} v_{ps}}{\sum_{k=1}^{z}\prod_{s=k}^{z} v_s}. \quad (5)$$

Якщо на базі наявної інформації можна стверджувати, що мають місце частково посилені лінійні співвідношення впорядкованості то, згідно з гіпотезою Фішберна для практичних досліджень оцінки Val_{pk}, можна вибрати у вигляді спадної геометричної прогресії. Фішберн показав, що:

$$Val_{pk} = \frac{2^{z-k}}{2^z - 1}. \quad (6)$$

Якщо відомі інтервальні співвідношення впорядкованості щодо цінностей вимог $\alpha_k \le Val_k \le \beta_k$ і $\alpha_k, \beta_k \ge 0$, то оцінки Фішберна задаються формулою

$$Val_k = \alpha_k + \frac{1 - \sum_{k=1}^{z} \alpha_k}{\sum_{s=1}^{z} (\beta_s - \alpha_s)} \cdot (\beta_k - \alpha_k) \cdot \quad (7)$$

При цьому накладаються умови:

$$\sum_{s=1}^{z} (\beta_s - \alpha_s) > 0; \quad \sum_{s=1}^{z} \alpha_s \le 1; \quad \sum_{s=1}^{z} \beta_s \ge 1.$$

Так, можна задати числові оцінки цінності вимог проекту.

Надалі необхідно визначити, яким чином буде оцінюватись досягнення цінності під час виконання програмного проекту (процесу). Для цього пропонується використовувати фактичні дані або адаптовані правила EVM:

– правило 50/50. Цінність вважається досягнутою на 50 %, коли відповідні роботи розпочалися; останні 50 % вважаються досягнутими лише після завершення робіт;

– правило 20/80. Цінність вважається досягнутою на 20 %, коли відповідні роботи розпочалися; останні 80 % вважаються досягнутими лише після завершення робіт;

– правило 0/100. Цінність вважається досягнутою лише після завершення робіт.

Отже, можна отримати план досягнення цінності вимог стейкхолдерів проекту і відстежувати його виконання у часі. Так, на рисунку 1 показано, що у момент часу *T* спостерігається випередження графіку досягнення цінності вимог у проекті.

Процесну модель запропонованого методу моніторингу досягнення цінності вимог у програмному проекті показано на рисунку 2.

4 ЕКСПЕРИМЕНТИ

Для демонстрації практичної реалізації розробленого методу було проведено відповідні розрахунки.

На моделі певного програмного проекту, розробленій в середовищі MS Project, було визначено планові показники досягнення цінності для кожної роботи проекту:

– планову цінність вимог стейкхолдерів, що забезпечує кожна робота (в даному проекті використано метод безпосереднього оцінювання з врахуванням вартості виконання робіт);

– планову цінність вимог стейкхолдерів, що забезпечує кожна робота на момент звіту (цінність вимог стейкхолдерів, яка повинна бути виконаною на момент звіту за планом).

Відповідну інформацію внесено до полей *Val* та *PVal* моделі (рис. 3).

Визначено, що оцінювання досягнення цінності здійснюється за фактичними даними щодо виконання проекту. Розраховано показники *SVal* та *SPIVal*, додано графічний індикатор, який показує, в яких межах знаходиться *SPIVal.*

5 РЕЗУЛЬТАТИ

Таким чином, за допомогою запропонованого методу та розроблених інструментів MS Project розраховано показники фактичного досягнення цінності вимог певного програмного проекту.

Для кожної роботи програмного проекту розраховано відхилення у досягненні цінності за розкладом *S*Val та індекс досягнення цінності за розкладом *SPI*val.

Інтерпретація отриманих результатів здійснюється за допомогою таблиці 2.

Розраховано також відповідні показники за сумарними роботами (етапами проекту) і проекту в цілому. Так, наприклад, на момент проведення аналізу індекс досягнення цінності за розкладом для проекту склав 0,46, що свідчить про відставання у виконанні плану досягнення цінності вимог.

Індикатори на рисунку 3 вказують на «проблемні» роботи, за якими треба вжити корегувальні дії.

6 ОБГОВОРЕННЯ

Як видно з таблиці 1, існуючи методи контролю в проектах здебільшого сконцентровані на моніторингу вартості та тривалості. Програмне забезпечення для планування і контролю проектів, відповідно, вирішує аналогічні задачі. Типовим представником згаданих методів є метод освоєного обсягу, який дозволяє відстежувати прогрес проекту з точки зору виконання його робот вчасно і в межах бюджету, але не дає можливості у явному вигляді відстежувати виконання вимог стейкхолдерів.

Таблиця 2 – Інтерпретація результатів для методу моніторингу цінності вимог

Показники виконання проекту	*S*Val >0; SPIVal>1	***S*Val =0; *SPI*val=1**	***S*Val <0; *SPI*val<1**
Стан виконання програмного проекту	випередження плану досягнення цінності вимог (зелений індикатор)	виконання плану досягнення цінності вимог (жовтий індикатор)	відставання у виконанні плану досягнення цінності вимог (червоний індикатор)

DOI 10.15588/1607-3274-2019-4-13

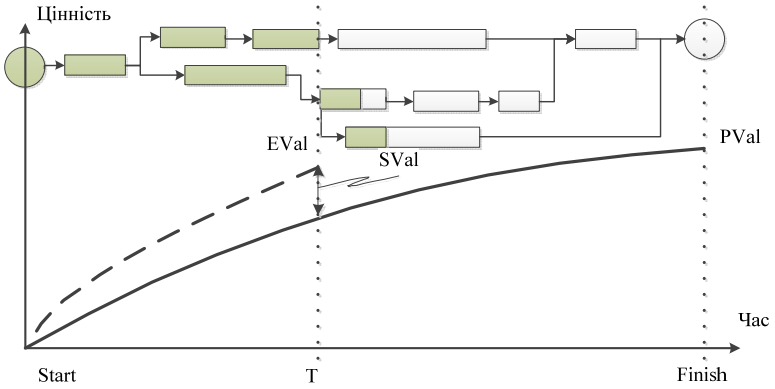


Рисунок 1 – Моніторинг цінності проекту

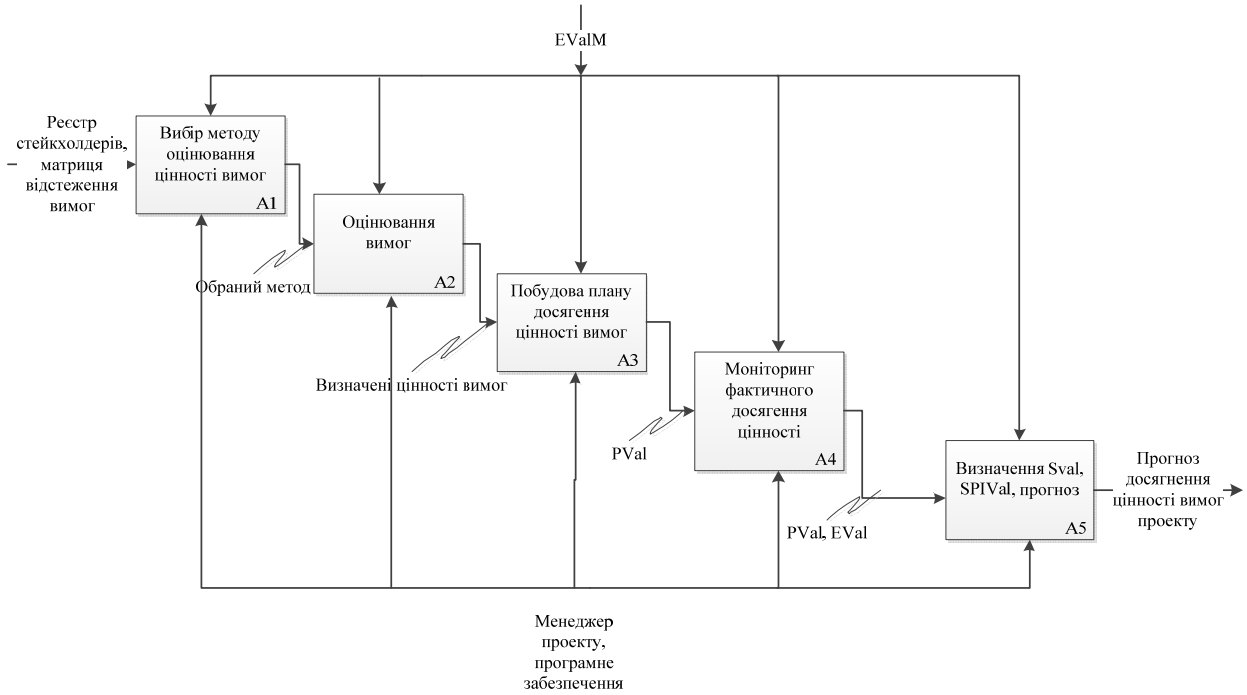
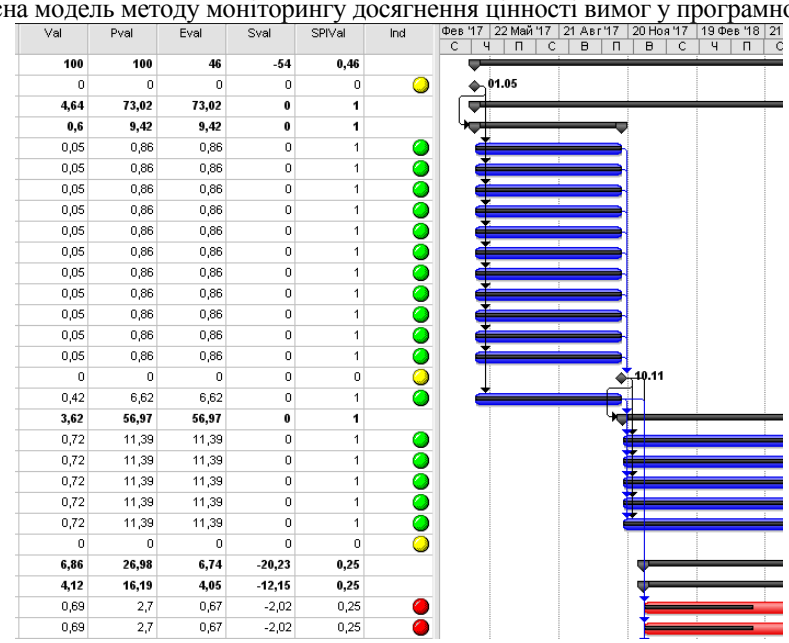


Рисунок 2 – Процесна модель методу моніторингу досягнення цінності вимог у програмному проекті (EValM)



Val	Pval	Eval	Sval	SPIVal	Ind
100	**100**	**46**	**-54**	**0,46**	
0	0	0	0	0	
4,64	**73,02**	**73,02**	**0**	**1**	
0,6	**9,42**	**9,42**	**0**	**1**	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0,05	0,86	0,86	0	1	
0	0	0	0	0	
0,42	6,62	6,62	0	1	
3,62	**56,97**	**56,97**	**0**	**1**	
0,72	11,39	11,39	0	1	
0,72	11,39	11,39	0	1	
0,72	11,39	11,39	0	1	
0,72	11,39	11,39	0	1	
0,72	11,39	11,39	0	1	
0	0	0	0	0	
6,86	**26,98**	**6,74**	**-20,23**	**0,25**	
4,12	**16,19**	**4,05**	**-12,15**	**0,25**	
0,69	2,7	0,67	-2,02	0,25	
0,69	2,7	0,67	-2,02	0,25	

Рисунок 3 – Результати програмного використання методу моніторингу цінності вимог

DOI 10.15588/1607-3274-2019-4-13

Дана робота є логічним продовженням попередніх робіт авторів, де було запропоновано проводити моніторинг виконання вимог зацікавлених сторін проекту, що є дієвим інструментом реагування на зміни динамічного середовища проекту. Запропонований у даному дослідженні ціннісний підхід знімає обмеження методу моніторингу вимог щодо необхідності визначення обсягу вимог у грошовій формі та надає можливість враховувати особистісну оцінку вимог та ресурсів певним стейкхолдером.

В таблиці 3 наведено порівняльну характеристику можливостей MS Project з розробленим додатковим функціоналом та базової версії MS Project з іншими поширеними програмними засобами управління проектами.

Таблиця 3 – Порівняльний аналіз програмного забезпечення з управління проектами

Інструменти моніторингу та контролю	Microsoft Project з додатковим функціоналом	Microsoft Project	Primavera	Spider Project
Аналіз план / факт	+	+	+	+
Професійна проектна статистика на базі промислового OLAP-сервера	+	+	–	–
Автоматичний запит про стан роботи виконавців	+	+	+	–
Інформування про систему роботи топ-менджерів	+	+	+	–
Відстеження об'ємів	+	+	–	+
Освоенний об'єм	+	+	+	+
Освоєні вимоги (грошова форма)	+	–	–	–
Моніторинг досягнення цінності	+	–	–	–

ВИСНОВКИ

Вирішено важливу наукову задачу математичної та інформаційної підтримки прийняття рішень щодо адаптації програмного проекту до змін у вимогах стейкхолдерів.

Науковою новизною отриманих результатів є розроблений метод моніторингу цінності вимог програмного проекту, який, на відміну від існуючих, дозволить враховувати особистісні оцінки цінності вимог та ресурсів проекту та забезпечить інформаційну підтримку для прийняття ґрунтовних рішень щодо адаптації до змін у вимогах стейкхолдерів.

DOI 10.15588/1607-3274-2019-4-13

Практичне значення результатів дослідження полягає в тому, що використання розроблених інструментів MS Project надає можливість визначити стан виконання програмного проекту (або його певних робіт) щодо досягнення цінностей його зацікавлених сторін. Так, наприклад, інформація щодо робіт з відставанням у графіку досягнення цінностей надає можливість ґрунтовного ресурсного планування в умовах обмеженості ресурсів.

Тому перспективою подальших досліджень є, зокрема, формулювання та вирішення оптимізаційної задачі розподілу ресурсів у програмному проекті за умов максимізації досягнутої цінності проекту.

ПОДЯКИ

Робота виконана на кафедрі управління проектами в міському господарстві і будівництві Харківського національного університету міського господарства імені О.М. Бекетова в межах наукових досліджень, що проводяться кафедрою.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Pellerin R. A review of methods, techniques and tools for project planning and control / R. Pellerin, N. Perrier // International Journal of Production Research. – 2018. – № 57(2) – P. 1–19. DOI: 10.1080/00207543.2018.1524168
2. Гусєва Ю. Ю. Динамічній аналіз методів та інструментальних засобів управління зацікавленими сторонами проектів / Ю. Ю. Гусєва, О. С. Мартиненко, І. В. Чумаченко // Управління розвитком складних систем: зб. наук. праць. – 2018. – № 35. – С. 27–36.
3. Martynenko O. The method of earned requirements for project monitoring / O. Martynenko, Yu. Husieva, I. Chumachenko // Innovative technologies and scientific solutions for industries. – 2017. – № 1. – P. 57–63. DOI: 10.30837/2522-9818.2017.1.058
4. Гусєва Ю. Ю. Інструментальні засоби реалізації моніторингу вимог у проекті в MS Project / Ю. Ю. Гусєва, О. С. Мартиненко, І. В. Чумаченко // Управління розвитком складних систем: зб. наук. праць. – 2017. – № 31. – С. 26–31.
5. Гусєва Ю. Ю. Матрична модель 4R & WS для класифікації стейкхолдерів проекту / Ю. Ю. Гусєва, О. С. Мартиненко, І. В. Чумаченко // Вісник Національного технічного університету «ХПІ»: зб. наук. праць. – 2017. – № 2 (1224). – С. 17–22.
6. A Guide to the Project Management Body of Knowledge (PMBOK®Guide) – 6th Edition. Newtown Square, Pa.: Project Management Institute, Inc., 2017. – 756 p.
7. Practice Standard for Earned Value Management – Second Edition. Newtown Square, Pa.: Project Management Institute, Inc., 2011. – 135 p.
8. A New Approach for Project Control Under Uncertainty. Going Back to the Basics / F. Acebes, J. Pajares, J. M. Galán at al. // International Journal of Project Management. 2014. – № 32 (3). – P. 423–434. DOI: 10.1016/j.ijproman.2013.08.003
9. Batson R. G. Project Risk Identification Methods for Construction Planning and Execution / R. G Batson // Proceedings of the 2009 Construction Research Congress, ASCE. – 2009. – P. 746–755. DOI: 10.1061/41020(339)76
10. Czemplik A. Application of Earned Value Method to Progress Control of Construction Projects / A. Czemplik // Procedia Engineering 91. – 2014. – P. 424–428. DOI: 10.1016/j.proeng.2014.12.087
11. The official site for Earned Schedule information [Electronic resource]. Acces mode: http://www.earnedschedule.com/

12. Liu L. The Control Model of Engineering Cost in Construction Phase of High-speed Railway / L. Liu, Y. Su // Proceeding of the 5th International Conference on Computer Sciences and Convergence Information Technology, IEEE. – 2010. – P. 766–771. DOI: 10.1109/ICCIT.2010.5711158
13. Martens A. A Buffer Control Method for Top-down Project Control / A. Martens, M. Vanhoucke // European Journal of Operational Research. – 2017. – № 262 (1). – P. 274–286. DOI: 10.1016/j.ejor.2017.03.034
14. Prediction of Project Outcome – The Application of Statistical Methods to Earned Value Management And Earned Schedule Performance Indexes / W. Lipke, O. Zwikael, K. Henderson at al. // International Journal of Project Management 27 (4). – 2009. – P. 400–407. DOI: 10.1016/j.ijproman.2008.02.009
15. Plaza M. A Model-based DSS for Integrating the Impact of Learning in Project Control / M. Plaza, O. Turetken // Decision Support Systems. – 2009. – № 47 (4). – P. 488–499. DOI: 10.1016/j.dss.2009.04.010
16. Batselier J. Evaluation of Deterministic State-of-the-Art Forecasting Approaches for Project Duration Based on Earned Value Management / J. Batselier, M. Vanhoucke // International Journal of Project Management. – № 33 (7). – 2015. – P. 1588–1596. DOI: 10.1016/j.ijproman.2015.04.003
17. Willems L. L. Classification of Articles and Journals on Project Control and Earned Value Management / L. L. Willems, M. Vanhoucke // International Journal of Project Management. – 2015. – № 33 (7). – P. 1610–1634. DOI: 10.1016/j.ijproman.2015.06.003
18. San Cristobal, J. R. 2017. "The S-curve Envelope as a Tool for Monitoring and Control of Projects." Procedia Computer Science 121: 756–761.
19. Determining the Timing of Project Control Points Using a Facility Location Model and Simulation / N. Sabeghi, H. R. Tareghian, E. Demeulemeester et al. // Computers and Operations Research. – 2015. – № 61. – P. 69–80. DOI: 10.1016/j.cor.2015.03.006
20. Leu S.-S. Project Performance Evaluation Based on Statistical Process Control Techniques / S.-S. Leu, Y.-C. Lin // Journal of Construction Engineering and Management. – 2008. – № 134 (10). – P. 813–819. DOI: 10.1061/(ASCE)0733-9364(2008)134:10(813)
21. Метрики процесів управління та контролю вимог у проектах / Ю. Ю. Гусєва, О. С. Мартиненко, І. М. Кадикова et al // Радіоелектроніка, інформатика, управління. – 2017. – №4. – С. 179–186. DOI: 10.15588/1607-3274-2017-4-20
22. Вітлінський В. В. Економічний ризик і методи його вимірювання / В. В. Вітлінський, С. І. Наконечний, О. Д. Шарапов. – К. : ІЗМН, 1996. – 400 с.
23. Теория прогнозирования и принятия решений / Под. ред. С. А. Саркисяна. – М. : Высшая школа, 1977. – 353 с.
24. Вітлінський В. В. Аналіз, моделювання та управління економічним ризиком / В. В. Вітлінський, П. І. Верченко – К. : КНЕУ, 2000. – 292 с.

Стаття надійшла до редакції 25.06.2019.
Після доробки 12.10.2019.

УДК 006.015.5

ПРОГРАММНЫЕ СРЕДСТВА МОНИТОРИНГА ЦЕННОСТИ КАК ИНСТРУМЕНТ АДАПТАЦИИ К ИЗМЕНЕНИЯМ В ТРЕБОВАНИЯХ СТЕЙКХОЛДЕРОВ ПРОЕКТОВ

Гусева Ю. Ю. – канд. техн. наук, доцент, доцент кафедры управления проектами в городском хозяйстве и строительстве, Харьковский национальный университет городского хозяйства имени А. Н. Бекетова, Харьков, Украина.

Чумаченко И. В. – д-р техн. наук, профессор, заведующий кафедрой управления проектами в городском хозяйстве и строительстве, Харьковский национальный университет городского хозяйства имени А. Н. Бекетова, Харьков, Украина.

АННОТАЦИЯ

Актуальность. В условиях динамичной среды, когда требования заинтересованных сторон могут меняться, традиционные методы мониторинга и контроля выполнения программного проекта имеют определенные ограничения. Следовательно, есть необходимость в создании подходов и соответствующих программных средств для мониторинга выполнения требований стейкхолдеров проекта, в частности, с учетом их личностной оценки ценности требований и ресурсов.

Цель работы. Разработка метода мониторинга ценности требований стейкхолдеров программного проекта и соответствующих инструментов его внедрения.

Метод. Использованы методы анализа и синтеза, операции над матрицами, система весовых коэффициентов Фишберна, методы теории управления проектами. Предложено ценностный подход к мониторингу требований заинтересованных сторон проекта. Предложены подходы к определению ценности требований стейкхолдеров на основе имеющейся информации из типовых проектных документов. Предложен метод мониторинга ценности требований стейкхолдеров проектов, в частности, программных, и соответствующие инструменты его внедрения.

Результаты. На основе ценностного подхода к мониторингу требований разработаны программные инструменты отслеживания достижения плановой ценности проекта. Соответствие предложенного метода процессам традиционного проектного менеджмента позволяет использовать стандартное программное обеспечение для формирования исходных данных и отображения результатов расчетов.

Выводы. На основе метода освоенных требований проекта разработан метод мониторинга ценности требований, который, в отличие от существующих, позволит учитывать личностные оценки ценности требований и ресурсов в ходе мониторинга выполнения проекта, осуществлять соответствующие прогнозы и разрабатывать стратегии работы с определенными заинтересованными сторонами или их группами. Инструменты использования предложенного метода в среде MS Project обеспечивают информационную поддержку для принятия обоснованных решений по адаптации проекта к изменениям в требованиях стейкхолдеров, в частности, рассчитывается отклонение в достижении ценности по расписанию и индекс достижения ценности по расписанию. Перспективой дальнейших исследований является решение задачи оптимизации распределения ресурсов в проекте в условиях максимизации достигнутой ценности проекта.

КЛЮЧЕВЫЕ СЛОВА: управление требованиями, проект, ценность, мониторинг, стейкхолдеры.

UDC 006.015.5

SOFTWARE FOR VALUE MONITORING AS AN ADAPTATION TOOL FOR CHANGES IN PROJECT STEAKHOLDERS' REQUIREMENTS

Husieva Yu. Yu. – PhD, Associate Professor, Associate Professor of the Department of Project management in urban economy and construction, O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine.

Chumachenko I. V. – Dr. Sc. Professor, Head of the Department of Project management in urban economy and construction, O. M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine.

DOI 10.15588/1607-3274-2019-4-13

ABSTRACT

Context. In a dynamic environment where stakeholder requirements may change, traditional project monitoring and control methods have some limitations. Therefore, there is a need to develop approaches and appropriate software to monitor the requirements of the software project stakeholders, in particular, taking into account their personal assessment of the value of requirements and resources.

Objective. The goal of the work is the development of a method for monitoring the value of the software project stakeholders' requirements and the corresponding tools for its implementation.

Method. Methods of analysis and synthesis, operations on matrices, a system of weighting coefficients of Fishburne, methods of the project management theory are used. A value-based approach to monitoring the requirements of the project stakeholders is proposed. The approaches to determining the value of the requirements of stakeholders are proposed based on available information from standard project documents. The method of project stakeholders' value monitoring, in particular, for software projects, and the appropriate tools for its implementation are proposed.

Results. Based on the value-added approach to monitoring requirements, tools have been developed to track the achievement of the project's planned value. Compliance of the proposed method with the processes of traditional project management allows using standard software for generating initial data and displaying the results of calculations.

Conclusions. Based on the method of the earned requirements of the project, a method of requirements' value monitoring has been developed that, unlike existing ones, will allow to take into account personal assessments of the value of requirements and resources during project monitoring; to carry out relevant forecasts and develop strategies for working with certain interested parties or groups. The tools of using the proposed method in the MS Project environment provide information support for making fundamental decisions on adapting the project to changes in the requirements of stakeholders, in particular, the schedule variance and schedule performance index is calculated. The prospect of further research is to solve the problem of optimizing the distribution of resources in the project in the conditions of maximizing the achieved value of the project.

KEYWORDS: requirements management, project, value, monitoring, stakeholders.

REFERENCES

1. Pellerin R., Perrier N. A review of methods, techniques and tools for project planning and control, *International Journal of Production Research*, 2018, No. 57(2), pp. 1–19. DOI: 10.1080/00207543.2018.1524168
2. Husieva Yu. Yu., Martynenko O. S., Chumachenko I. V. Dynamichnii analiz metodiv ta instrumentalnykh zasobiv upravlinnia zatsikavlenymy storonamy proektiv, *Upravlinnia rozvytkom skladnykh system: zb. nauk. prats,* 2018, No. 35, pp. 27–36.
3. Martynenko O., Husieva Yu., Chumachenko I. The method of earned requirements for project monitoring, *Innovative technologies and scientific solutions for industries*, 2017, No. 1, pp. 57–63. DOI: 10.30837/2522-9818.2017.1.058
4. Husieva Yu. Yu., Martynenko O. S., Chumachenko I. V. Instrumentalni zasoby realizatsii monitorynhu vymoh u proekti v MS Project, *Upravlinnia rozvytkom skladnykh system: zb. nauk. prats,* 2017, No. 31, pp. 26–31.
5. Husieva Yu. Yu., Martynenko O. S., Chumachenko I. V. Matrychna model 4R & WS dlia klasyfikatsii steikkholderiv proektu, *Visnyk Natsionalnoho tekhnichnoho universytetu «KhPI»: zb. nauk. prats*, 2017, № 2 (1224), pp. 17–22.
6. A Guide to the Project Management Body of Knowledge (PMBOK®Guide) – 6th Edition. Newtown Square, Pa.: Project Management Institute, Inc., 2017, 756 p.
7. Practice Standard for Earned Value Management – Second Edition. Newtown Square, Pa.: Project Management Institute, Inc., 2011, 135 p.
8. Acebes F., Pajares J., Galán J. M. et al. A New Approach for Project Control Under Uncertainty. Going Back to the Basics, *International Journal of Project Management.* 2014, No. 32 (3). pp. 423–434. DOI: 10.1016/j.ijproman.2013.08.003
9. Batson R. G. Project Risk Identification Methods for Construction Planning and Execution, *Proceedings of the 2009 Construction Research Congress, ASCE,* 2009, pp. 746–755. DOI: 10.1061/41020(339)76
10. Czemplik A. Application of Earned Value Method to Progress Control of Construction Projects, Procedia Engineering 91, 2014, pp. 424–428. DOI: 10.1016/j.proeng.2014.12.087
11. The official site for Earned Schedule information [Electronic resource]. Acces mode: http://www.earnedschedule.com/
12. Liu L., Su Y. The Control Model of Engineering Cost in Construction Phase of High-speed Railway, *Proceeding of the 5th International Conference on Computer Sciences and Convergence Information Technology, IEEE,* 2010, pp. 766–771. DOI: 10.1109/ICCIT.2010.5711158
13. Martens A., Vanhoucke M. A Buffer Control Method for Top-down Project Control, *European Journal of Operational Research*, 2017, No. 262 (1), pp. 274–286. DOI: 10.1016/j.ejor.2017.03.034
14. Lipke W., Zwikael O., Henderson K. et al. Prediction of Project Outcome – The Application of Statistical Methods to Earned Value Management And Earned Schedule Performance Indexes, *International Journal of Project Management,* 2009, No. 27 (4), pp. 400–407. DOI: 10.1016/j.ijproman.2008.02.009
15. Plaza M., Turetken O. A Model-based DSS for Integrating the Impact of Learning in Project Control, *Decision Support Systems*, 2009, No. 47 (4), pp. 488–499. DOI: 10.1016/j.dss.2009.04.010
16. Batselier J., Vanhoucke M. Evaluation of Deterministic State-of-the-Art Forecasting Approaches for Project Duration Based on Earned Value Management, *International Journal of Project Management,* 2015, No. 33 (7), pp. 1588–1596. DOI: 10.1016/j.ijproman.2015.04.003
17. Willems L. L., Vanhoucke M. Classification of Articles and Journals on Project Control and Earned Value Management, *International Journal of Project Management,* 2015, No. 33 (7), pp. 1610–1634. DOI: 10.1016/j.ijproman.2015.06.003
18. San Cristobal, J. R. 2017. "The S-curve Envelope as a Tool for Monitoring and Control of Projects." Procedia Computer Science 121: 756–761.
19. Sabeghi N., Tareghian H. R., Demeulemeester E. et al. Determining the Timing of Project Control Points Using a Facility Location Model and Simulation, *Computers and Operations Research,* 2015, No. 61, pp. 69–80. DOI: 10.1016/j.cor.2015.03.006
20. Leu S.-S., Lin Y.-C. Project Performance Evaluation Based on Statistical Process Control Techniques, *Journal of Construction Engineering and Management,* 2008, No. 134 (10), pp. 813–819. DOI: 10.1061/(ASCE)0733-9364(2008)134:10(813)
21. Husieva Yu. Iu., Martynenko O. S., Kadykova I. M. et al Metryky protsesiv upravlinnia ta kontroliu vymoh u proektakh, *Radio Electronics, Computer Science, Control,* 2017, No. 4, pp. 179–186. DOI: 10.15588/1607-3274-2017-4-20
22. Vitlinskyi V. V., Nakonechnyi S. I., Sharapov O. D. *Ekonomichnyi ryzyk i metody yoho vymiriuvannia*, Kiev, IZMN, 1996, 400 p.
23. Teoryia prohnozyrovanyia y pryniatyia reshenyi. Pod. red. S. A. Sarkysiana. Moscow, Vyshaia shkola, 1977, 353 p.
24. Vitlinskyi V. V., Verchenko P. I. Analiz, modeliuvannia ta upravlinnia ekonomichnym ryzykom. Kiev, KNEU, 2000, 292 p.

DOI 10.15588/1607-3274-2019-4-13

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

УДК 621.391:681.5

МЕТОД ВИЗНАЧЕННЯ ЙМОВІРНІСНО-ЧАСОВИХ ХАРАКТЕРИСТИК РІВНЯ СЕРВЕРІВ СЕРВІСІВ ТА ДОДАТКІВ IMS

Князєва Н. О. – д-р техн. наук, професор, професор кафедри Комп'ютерної інженерії, Одеська національна академія харчових технологій, Одеса, Україна.

Шестопалов С. В. – канд. техн. наук, доцент кафедри Комп'ютерної інженерії, Одеська національна академія харчових технологій, Одеса, Україна.

Сіренко О. І. – старший викладач кафедри Комп'ютерної інженерії, Одеська національна академія харчових технологій, Одеса, Україна.

АНОТАЦІЯ

Актуальність. Стаття присвячена розробці методу визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS. Показано, що завдяки постійно зростаючій різноманітності сервісів, котрі спроможна надати IMS, та збільшенню попиту на них серед користувачів, а також тому, що з розвитком телекомунікацій все більша увага приділяється якості надання сервісів – QoS, задача оцінки якості надання сервісів обумовлює актуальність розробки методу визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS.

Мета. Розробити метод визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS з урахуванням різних видів сервісів, котрі спроможна надати IMS.

Метод. Розглянуто архітектуру IMS. Основна увага приділена рівню серверів сервісів та додатків. Для розробки методу визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS запропоновано скористатися підходами теорії телетрафіку та тензорним аналізом мереж. Запропонований метод являє послідовність етапів, виконання яких дозволяє: визначити структурні блоки рівня серверів сервісів та додатків IMS, які відповідають за надання сервісів різних видів; представити блок управління сеансами зв'язку та рівня серверів сервісів та додатків у вигляді окремої накладної мережі – вихідної мережі масового обслуговування; для використання контурного методу ввести уявну гілку, котра створює замкнутий контур; ввести контурні інтенсивності та визначити їх напрямки; визначити матрицю переходу від вихідної мережі до примітивної мережі; представити інваріантне рівняння для вихідної мережі; визначити контурні інтенсивності та на їх основі розрахувати інтенсивності надходження заявок на сервіси та завантаження серверів в вихідній мережі. В результаті – отримати вирази для розрахунку ймовірнісно-часових характеристик рівня серверів сервісів та додатків.

Результати. Запропоновано метод визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS на основі підходів теорії телетрафіку та тензорного аналізу мереж, який надає можливість ураховувати різні видів сервісів, котрі спроможна надати IMS.

Висновки. Метод визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS надасть можливість проектувальникам IMS на ранніх етапах проекту розрахувати ймовірнісно-часові характеристики, що дозволить визначити потрібні мережні ресурси для забезпечення необхідного значення якості надання сервісів різних видів. В подальшому, при розвитку запропонованого методу, при дослідженні рівня серверів сервісів та додатків IMS з метою визначення ймовірнісно-часових характеристик доцільно урахування самоподібного характеру потоку заявок на сервіси та обмеження буферної пам'яті серверів.

КЛЮЧОВІ СЛОВА: IMS, ймовірнісно-часові характеристики, рівень серверів сервісів та додатків, підходи теорії телетрафіку, тензорний аналіз, види сервісів.

АБРИВІАТУРИ

BGCF – Breakout Gateway Control Function;
CSCF – Call Session Control Function;
GPSS – General Purpose Simulation System;
HSS – Home Subscriber Server;
I-CSCF – Interrogating-CSCF;
IDN – Integrated Digital Network;
IMS – IP Multimedia Subsystem;
IM-SSF – IP Multimedia − Service Switching Function;
IN – Intelligent Network;
IPTD – IP packet transfer delay;
ISDN – Integrated Service Digital Network;
MGCF – Media Gateway Control Function;
MRF– Media Resource Function;
NGN – Next Generation Network;
OSA-GW – Open Service Access – Gate Way;
OSA-SCS – Open Service Access − Service Capability Server;
P-CSCF – Proxy-CSCF;
PSTN – Public Switched Telephone Network;
QoS – quality of service;
SCIM – Service Capability Interaction Manager;
SCP – Service Control Point;
S-CSCF – Serving-CSCF;
SIP AS – SIP Application Server;
TAS – Telephony Application Server;
ЙЧХ – ймовірнісно-часові характеристики;
МеМО – мережа масового обслуговування;
РССД – рівень серверів сервісів та додатків;
СМО – система масового обслуговування;
ТМЗК – телефонна мережа загального користування;
ТМО – теорія масового обслуговування.

НОМЕНКЛАТУРА

a – перше значення індексу контурів;

DOI 10.15588/1607-3274-2019-4-14

$\overline{C}$ – матриця переходу від вихідної мережі до примітивної мережі;

i – номер СМО примітивної мережі;

$\overline{L}$ – середня довжина черги при серверах кожного структурного блоку рівня серверів сервісів та додатків, що формується заявками відповідних видів;

$\overline{L}_i$ – середня довжина черги заявок відповідних видів у кожному i-му структурному блоці рівня серверів сервісів та додатків (i-й СМО в вихідній мережі);

r – розмір буфера при серверах кожного структурного блоку;

$\overline{t'_{\text{обсл}}}$ – середній час обслуговування заявок в примітивній мережі;

$\overline{t_{\text{обсл}}}$ – середній час обслуговування заявок відповідних видів у кожному структурному блоці рівня серверів сервісів та додатків (в блоці вихідної мережі);

$\overline{T}$ – середній час перебування заявок в системі;

$\overline{T}_i$ – середній час перебування заявок відповідних видів у кожному i-му структурному блоці рівня серверів сервісів та додатків (в i-й СМО в вихідній мережі);

$\overline{T}_{\text{оч}}$ – середній час очікування в черзі при серверах кожного структурного блоку рівня серверів сервісів та додатків, що формується заявками відповідних видів;

$\overline{T}_{\text{оч}i}$ – середній час очікування в черзі заявок відповідних видів у кожному i-му структурному блоці рівня серверів сервісів та додатків (i-й СМО в вихідній мережі);

z – останнє значення індексу контурів;

λ – інтенсивність потоку заявок на надання сервісів;

λ_j – контурні інтенсивності, $j = \overline{a, z}$;

λ'_i – інтенсивності i-ї СМО примітивної мережі;

$\overline{\lambda}$ – інтенсивність надходження заявок на сервіси в вихідній мережі;

$\overline{\lambda}'$ – інтенсивність надходження заявок на сервіси в примітивній мережі;

$\overline{\lambda}'_i$ – інтенсивності гілок в примітивній мережі;

ρ'_i – завантаження i-ї СМО примітивної мережі;

$\overline{\rho}'$ – завантаження вузла в примітивній мережі;

$\overline{\rho}$ – середнє завантаження кожного структурного блоку рівня серверів сервісів та додатків (вузла в примітивній мережі).

ВСТУП

Незважаючи на постійно зростаючу складність телекомунікаційних пристроїв і систем, протоколів, додатків та сервісів, роботи в напрямку створення універсальної мережної інфраструктури тривають. В історичному розвитку мереж та сервісів зв'язку можна виділити етапи: PSTN, IDN, ISDN, IN [1].

Подальшим розвитком стала поява мереж зв'язку наступного покоління NGN. Основу мережі NGN складає мультипротокольна мережа – транспортна мережа зв'язку, яка входить до складу мультисервісної мережі, що забезпечує перенос різних типів інформації з використанням різних протоколів передачі [1, 2]. NGN являє собою єдину транспортну платформу, на базі якої об'єднуються різні види сервісів. Нарешті, – створення концепції IMS – мультимедійної IP-орієнтованої підсистеми зв'язку, або підсистеми мультимедійних IP-сервісів, мета якої – забезпечити реальну мультисервісну і мультимедійну мережу з наданням всього спектра сервісів за допомогою єдиної платформи [3].

Концепція IMS визначає засновану на загальнопоширених протоколах сімейства TCP/IP архітектуру надання сервісів, яка забезпечує управління сеансами зв'язку і доставку в рамках цих сеансів будь-яких типів інформації – мови, даних, відео, мультимедіа. Принцип, на якому базується концепція IMS, полягає в тому, що доставка будь-якого сервісу ніяким чином не співвідноситься з комунікаційною інфраструктурою (за винятком обмежень по пропускній здатності). Втіленням цього принципу є багаторівневий підхід, який використовується при побудові IMS.

В даний час архітектура IMS розглядається багатьма операторами і сервіс-провайдерами, а також постачальниками обладнання як можливе рішення для побудови мереж наступного покоління і як основа конвергенції мобільних і стаціонарних мереж на платформі IP.

З кожним етапом розвитку телекомунікацій все більша увага приділяється якості надання сервісів – QoS. Пропонувалися методи, аналітичні та імітаційні моделі для розрахунку ЙЧХ та визначення на їх основі QoS. Враховуючи те, що постійно зростають як різноманітність сервісів, котрі спроможна надати IMS, так і попит на них серед користувачів, дослідження, що присвячене розробці методу розрахунку ЙЧХ рівня серверів сервісів та додатків IMS для визначення QoS, є безумовно актуальним.

Об'єктом дослідження являються процеси визначення показників якості надаваних сервісів рівня серверів сервісів та додатків.

Процеси визначення показників якості на рівні серверів сервісів та додатків орієнтовані на застосування математичного апарату теорії масового обслуговування та тензорного аналізу. Оцінка якості надаваних сервісів здійснюється для конвергентного трафіку. Впровадження концепції IMS потребує подальшого розвитку підходів щодо визначення показників якості на рівні серверів сервісів та додатків з урахуванням поділу трафіку у відповідності з видами сервісів.

Предметом дослідження є метод визначення ЙЧХ рівня серверів сервісів та додатків IMS.

DOI 10.15588/1607-3274-2019-4-14

Існуючі методи визначення ЙЧХ [4–10] орієнтовані на використання для мереж з конвергентним трафіком, але ці методи не орієнтовані на врахування поділу трафіку у відповідності з видами сервісів.

Метою роботи є розробка методу визначення ЙЧХ рівня серверів сервісів та додатків IMS з урахуванням різних видів сервісів, котрі спроможна надати IMS.

1 ПОСТАНОВКА ЗАДАЧІ

Нехай задано: архітектура IMS, перелік видів сервісів, на основі якого визначаються структурні блоки РССД; множина вихідних даних для різних блоків $\{ \overline{t'_{\text{обсл}}}, \overline{\rho}', r \}$; припущення та обмеження, а саме – РССД IMS представляє собою окрему накладну мережу, при цьому блоки досліджуваної мережі являють собою одноканальні СМО з буфером необмеженої ємкості $r = \infty$; інтервали часу між заявками на різноманітні сервіси розподілені за експоненційним законом.

Тоді задача визначення ймовірнісно-часових характеристик рівня серверів сервісів та додатків IMS полягає в тому, щоб сформувати математичні вирази для отримання множини результатів: $\{ \overline{L}_i, \overline{T}_{\text{оч}i}, \overline{T}_i \}$.

2 ОГЛЯД ЛІТЕРАТУРИ

Однією з перших робіт напрямку аналізу телекомунікаційних мереж була робота Л. Клейнрока [4], що містить інформацію про основні положення ТМО, в якій обговорюються методи розрахунку ЙЧХ СМО.

Поява нових концепцій – NGN, IMS – викликала необхідність доопрацювання існуючих і розробку нових методів для створення моделей мереж і розрахунку їх ЙЧХ. Даний напрям досліджень розкривається в роботах як вітчизняних, так і іноземних учених. У роботі Д.Ю. Пономарьова [5] розглядається можливість використання методів імітаційного моделювання та тензорного аналізу. В роботі Y. Zhang [6] на основі методів векторної алгебри пропонується рішення для точної оцінки завантаження ліній зв'язку у великих IP мережах. У роботі Y. Jiang, Y. Liu [7] розглядаються конвергентні мережі з технологією QoS; на основі ТМО і теорії ймовірностей пропонуються моделі, які описують функціонування елементів мережі і дозволяють розрахувати їх ЙЧХ.

У роботі [8] показано, що застосування окремих СМО в якості моделей реальних телекомунікаційних мереж призводить до суттєвих обмежень. Реальні інформаційні системи доцільно представляти у вигляді МеМО з відповідною структурою. Показано, що оцінка ЙЧХ МеМО за допомогою методів класичної ТМО є досить трудоємким процесом, а іноді і неможливим.

В низці робіт для оцінки ЙЧХ телекомунікаційних мереж, що представлені у вигляді МеМО, пропонується використовувати підходи тензорного аналізу.

Вперше використання тензорів для аналізу мережних структур було запропоновано Г. Кроном [9]. Подальший розвиток використання тензорного аналізу для задач моделювання телекомунікаційних мереж отримано у роботах В.В. Поповського, О.В. Лемешко [10], Д.Ю. Пономарьова [5] та ін. В роботах В.В. Поповського пропонується використання методології тензорного підходу до аналізу телекомунікаційної системи як складної системи; вирішуються задачі знаходження максимального потоку з обмеженням на час доставки даних з урахуванням тензорного методу розрахунків.

В роботах О. В. Лемешко аналізуються потокові проблеми в області маршрутизації трафіку в мультисервісних мережах. Обґрунтована можливість застосування методів тензорного аналізу мереж для вирішення завдання багатошляхової маршрутизації.

Слід зазначити, що в проаналізованих роботах розглядаються моделі мереж з врахуванням того, що трафік є конвергентним. При цьому мова не йде про поділ трафіку у відповідності з видами сервісів. У той же час архітектура IMS передбачає поділ всього мережного трафіку на різнорідні потоки і різні види через можливість надання низки сервісів з різними характеристиками. Таким чином, задача розробки методу визначення ЙЧХ РССД IMS з врахуванням видів сервісів потребує свого вирішення, що і обумовлює актуальність розробки методу визначення ЙЧХ РССД IMS.

Для розробки методу визначення ЙЧХ РССД IMS слід провести аналіз архітектури IMS, що надасть можливість визначити структурні блоки РССД.

Архітектура IMS розподілена на наступні рівні [3]:

– рівень транспорту;

– рівень управління;

– рівень серверів сервісів і додатків.

Такий підхід дозволяє реалізувати незалежний від технології доступу відкритий механізм доставки сервісів, який дає можливість задіяти в мережі програми сторонніх постачальників сервісів.

Спрощена архітектура IMS та її основні блоки представлена на рис. 1.

Один з основних логічних блоків IMS – блок управління сеансами зв'язку CSCF, або SIP-сервери. Їх основне завдання – обробка SIP-запитів з метою організації сеансів мультимедійного зв'язку між користувачами. Вони «стежать» за виконанням правил безпеки і виділенням необхідних ресурсів для надання різних сервісів. До завдань CSCF входить управління іншими мережними елементами для належного обслуговування користувачів.

Логічно сервери управління сеансами зв'язку діляться на три групи [3]:

– Serving-CSCF;

– Proxy-CSCF;

– Interrogating-CSCF.

DOI 10.15588/1607-3274-2019-4-14

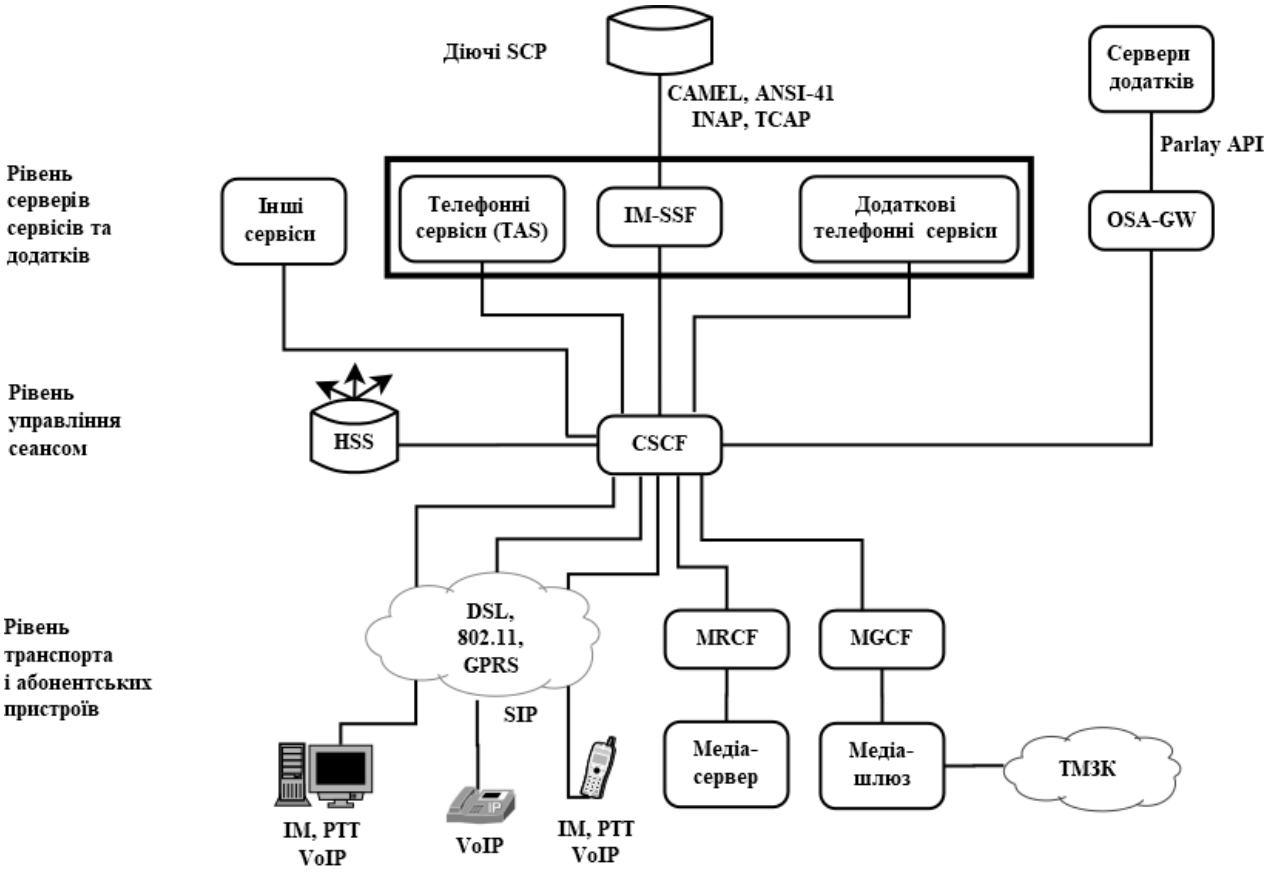


Рисунок 1 – Спрощена схема архітектури IMS

Наступний за важливістю блок IMS – це абонентська база даних HSS. У першому наближенні HSS можна порівняти з використовуваним в стільникових мережах регістром HLR, в якому зберігається інформація про активність абонентів і їх місцезнаходження. Однак функції HSS значно ширше [3]. Це база даних з інформацією не тільки по абонентам мобільних мереж, а й по абонентам мереж фіксованого зв'язку. У ній зберігається інформація про різноманітні вимоги абонентів, наприклад, по переадресації та фільтрації викликів, оповіщенні та повідомленнях голосової пошти, персональна адресна книга (buddy list) для розсилки повідомлень і організації конференцій. Також на сервері HSS є всі необхідні дані для врахування доступності/статусу (presence) і місцезнаходження (location) абонента. Замість застарілого протоколу Radius для взаємодії між HSS і серверами CSCF використовується протокол Diameter. Крім інших удосконалень, в Diameter передбачена підтримка функції тарифікації, в тому числі і для надання популярних послуг з передоплатою (prepaid) [3]. На рис. 1 також показані ще два важливі елементи архітектури IMS: відповідальні за управління медіашлюзами BGCF або MGCF і обробку медіапотоків MRF. Якщо до сеансу зв'язку треба підключити абонента, що знаходиться в мережі з комутацією каналів (мережа стільникового зв'язку або ТМЗК), блок BGCF/MGCF забезпечує доведення до неї відповідної сигнальної інформації. При необхідності він перетворює сигнальні повідомлення з формату SIP в формат ISUP. Подібна функціональність типова для комутаторів Softswitch, але в архітектурі IMS вона виділена в окремий логічний елемент. Системи MRF забезпечують обробку медіапотоків, переданих між серверами додатків і кінцевими пристроями. Їх функції – програвання різних голосових повідомлень, транскодування інформаційних потоків, «змішування» мовних/відеопотоків в конференцію і т. п. [3].

Оскільки дана робота присвячена розробці методу визначення ЙЧХ РССД IMS, розглянемо більш детально архітектуру даного рівня.

РССД містить сервери додатків, які забезпечують обслуговування кінцевих користувачів. Архітектура IMS і сигналізація SIP забезпечують достатню гнучкість для підтримки різноманітних телефонних та інших серверів додатків. Так, розроблені стандарти SIP для сервісів телефонії і сервісів інтелектуальної мережі (IM-SSF, діючі SCP). Верхній рівень еталонної архітектури IMS містить набір серверів додатків, які, в принципі, не є елементами IMS. Ці елементи верхньої площини включають в свій склад як мультимедійні IP-додатки, що базуються на протоколі SIP, так і додатки, які реалізуються в мобільних мережах на базі віртуального домашнього середовища.

Архітектура додатків IMS досить складна, але ключовим моментом тут є висока гнучкість при створенні нових сервісів та додатків і інтеграції їх з традиційними.

DOI 10.15588/1607-3274-2019-4-14

Так, середовище пересилання повідомлень може інтегрувати традиційні властивості телефонного виклику: зворотний виклик і очікування виклику з викликом через Інтернет. Щоб зробити це, архітектура IMS дозволяє запустити безліч сервісів і управляти транзакціями між ними.

РССД містить наступні блоки [3]:

– SCIM − забезпечує управління взаємодією площини додатків і ядра IMS;

– SIP AS − сервер додатків, який слугує для виконання сервісів, що базуються на протоколі SIP. Всі нові сервіси в IMS будуть перебувати саме в сервері SIP AS;

– OSA-SCS − сервер можливих сервісів, який забезпечує інтерфейс до сервісів, що базуються на відкритому доступі послуг OSA;

– IM-SSF − сервер комутації сервісу, служить для з'єднання підсистеми IMS з сервісами в системі пристосованих до користувача додатків для поліпшення логіки мобільної мережі;

– TAS − сервер телефонних додатків, приймає і обробляє повідомлення протоколу SIP, а також визначає, яким чином повинен бути ініційований вихідний виклик. Сервісна логіка TAS забезпечує базові сервіси обробки викликів, включаючи аналіз цифр, маршрутизацію, встановлення, очікування і перенаправлення викликів, конференц-зв'язок і т.д.

У IMS користувачі отримують доступ до сервісів через функціональний компонент CSCF, який динамічно призначається користувачу при його реєстрації в мережі або при отриманні запиту на з'єднання від іншого користувача. Для надання сервісів відповідного класу використовується один або декілька однотипних серверів, що містять логіку обслуговування всіх сервісів даного типу та класу. Користувача буде обслуговувати той сервер, маршрут до якого оптимальний і на якому є логіка даного сервісу. Можна сказати, що на відміну від традиційної інтелектуальної платформи архітектура сервісів на базі IMS орієнтована на користувача та здатна до значного масштабування.

3 МАТЕРІАЛИ І МЕТОДИ

Для розробки методу визначення ЙЧХ РССД IMS запропоновано скористатися підходами ТМО та тензорним аналізом. При виборі математичного апарату враховано, що для дослідження функціональних властивостей мереж традиційно застосовують лише методи ТМО [4]. Використання тензорного аналізу надає додаткові можливості, так як тензор – математичний об'єкт більш загального характеру і має можливості отримання оцінки функціональних характеристик значної кількості мережних вузлів. Тензорний аналіз пропонує математичний апарат перетворення систем координат, розглядаючи мережі МеМО як геометричні об'єкти, проекції яких в різних системах координат різні, але фізичні властивості самих об'єктів при цьому не змінюються.

Розрахунок характеристик РССД IMS, який можна представити у вигляді МеМО великої розмірності і отримання аналітичних рішень для МеМО з урахуванням топології мережі і динамічності інформаційних потоків, є досить складною задачею. Для вирішення такої задачі доцільно використати одночасно підходи ТМО та тензорний аналіз.

Метод визначення ЙЧХ РССД IMS орієнтований на застосування наступних вхідних даних:

– архітектура IMS – для визначення структурних блоків РССД, кожен з яких призначений для управління процесом надання відповідних видів сервісів;

– інтенсивність потоку заявок на надання сервісів відповідних видів;

– середній час обслуговування заявок відповідних видів у кожному структурному блоці РССД;

– середнє завантаження кожного структурного блоку РССД;

– характер трафіку, що формується заявками відповідних видів, який надходить на обслуговування у кожний структурний блок РССД;

– розмір буфера при серверах кожного структурного блоку РССД.

Перелік показників якості – ЙЧХ, які даний метод надає можливість розраховувати, визначено на підставі рекомендацій ITU [11–13], а саме:

– середня довжина черги при серверах кожного структурного блоку РССД, що формується заявками відповідних видів;

– середній час очікування в черзі при серверах кожного структурного блоку РССД, що формується заявками відповідних видів;

– середній час перебування заявки відповідного виду в системі.

Введені наступні припущення та обмеження.

На підставі аналізу архітектури IMS та визначення структурних блоків РССД вважається, що РССД представляє собою окрему накладну мережу, котру можна представити у вигляді МеМО. При цьому блоки досліджуваної мережі являють собою одноканальні СМО з буфером необмеженої ємкості $r = \infty$.

Вважається, що інтервали часу між заявками на різноманітні сервіси, що надходять в РССД IMS, розподілені за експоненційним законом.

Запропонований в даній роботі метод визначення ЙЧХ РССД IMS полягає у виконанні послідовності наступних етапів:

Етап 1. Визначення структурних блоків РССД IMS, які відповідають за надання сервісів різних видів.

Етап 2. Представлення РССД IMS у вигляді окремої накладної мережі (МеМО). В термінах тензорного аналізу дана МеМО матиме назву «вихідна мережа». Для використання контурного методу всі контури мають бути замкнутими. Якщо існують незамкнуті контури, то необхідно ввести уявні гілки, які їх замкнуть.

Етап 3. Введення контурних інтенсивностей. На даному етапі необхідно ввести контурні інтенсивності

DOI 10.15588/1607-3274-2019-4-14

λ_j, $j = \overline{a,z}$ в залежності від кількості контурів. Крім того, для кожного контуру довільним чином обирається їх напрям.

Етап 4. Визначення примітивної мережі. Формується структурна схема примітивної мережі, що представляє собою блоки вихідної мережі у вигляді окремих СМО з зазначенням їх основних характеристик.

Eman 5. Визначення матриці переходу $\overline{C}$ від вихідної мережі до примітивної мережі. Для цього формується таблиця відповідності інтенсивності гілок в примітивній мережі $\overline{\lambda}_i'$ та контурних інтенсивностей вихідної мережі λ_j ($j = \overline{a,z}$). Якщо напрям інтенсивності гілки в примітивній мережі $\overline{\lambda}_i'$ співпадає з напрямом контурної інтенсивності вихідної мережі λ_j даного контуру, то в таблиці ставиться «1», інакше – «–1». Якщо в даному контурі відсутня певна гілка примітивної мережі, то встановлюється значення «0».

Етап 6. Розрахунок показників функціонування МеМО. Для цього розрахунку в якості інваріантного рівняння пропонується використовувати відомий вираз для визначення коефіцієнта завантаження $\overline{\rho}$, що дає зв'язок між інтенсивністю надходження заявок на сервіси і середнім часом обслуговування в блоці [9]:

$$\overline{\rho} = \overline{\lambda}\overline{t_{\text{обсл}}}. \tag{1}$$

Вважатимемо, що потік викликів з однією і тією ж інтенсивністю $\overline{\lambda}$ надходження заявок на сервіси викличе при незмінній інтенсивності обслуговування одне і те ж завантаження $\overline{\rho}$ пристроїв при зміні структури і можна вважати, що буде виконуватися співвідношення (2) [9]:

$$\overline{\rho}\overline{\lambda} = \overline{\rho}'\overline{\lambda}'. \tag{2}$$

Використовуючи матрицю переходів, отримаємо:

$$\overline{\lambda} = \overline{C}\overline{\lambda}', \tag{3}$$

$$\overline{t_{\text{обсл}}} = \overline{C}^T\overline{t_{\text{обсл}}'}\overline{C}. \tag{4}$$

В результаті перетворень для вихідної мережі отримаємо:

$$\overline{C}^T\overline{\rho}' = (\overline{C}^T\overline{t_{\text{обсл}}'}\overline{C})\overline{\lambda}. \tag{5}$$

У виразі (5) вихідна мережа описана в символах примітивної, а отже, відомої мережі. Задаємо значення часу обслуговування заявок на різноманітні сервіси в різних блоках $\overline{t_{\text{обсл}}'}$ та завантаження вузлів (СМО, блоків) $\overline{\rho}'$ для примітивної мережі. Розв'язавши отримане рівняння (5) відносно контурних інтенсивностей $\overline{\lambda}$, визначимо інтенсивності надходження заявок на сервіси в вихідній мережі:

$$\lambda = \overline{\lambda}^T\overline{C}^T. \tag{6}$$

Завантаження вузлів (блоків) можна розрахувати наступним чином:

$$\rho = \overline{\lambda}^T\overline{C}^T\overline{t_{\text{обсл}}'}. \tag{7}$$

У виразах (6) і (7) λ і ρ представляють собою вектори, що містять значення інтенсивності надходження заявок та завантаження для всіх *i* вузлів (блоків) вихідної мережі – РССД IMS.

Етап 7. Розрахунок ймовірнісно-часових характеристик. Існує досить багато ЙЧХ як СМО так і МеМО [14]. Виходячи з рекомендацій ITU щодо найважливіших показників якості сервісів сучасних мереж [11–13], визначимо спосіб розрахунку $\overline{L}_i$, $\overline{T}_{\text{оч}i}$, $\overline{T}_i$. Маючи значення інтенсивності надходження заявок на сервіси до кожного структурного блоку та завантаження структурних блоків, при необхідності можна розрахувати й інші ЙЧХ [14].

Значення обраних ЙЧХ розраховуються за виразами (8–10) [14].

Середня довжина черги:

$$\overline{L}_i = \frac{\rho_i^2}{1-\rho_i}. \tag{8}$$

Середній час очікування в черзі:

$$\overline{T}_{\text{оч}i} = \frac{\rho_i t_i}{1-\rho_i}. \tag{9}$$

Середній час перебування заявки в системі:

$$\overline{T}_i = \overline{T}_{\text{оч}i} + t_i = \frac{t_i}{1-\rho_i}. \tag{10}$$

4 ЕКСПЕРИМЕНТИ

Використовуючи запропонований метод, визначимо ЙЧХ РССД IMS, представленої на рис. 1. Перш за все оберемо необхідні структурні блоки.

До структурних блоків РССД IMS відносяться наступні блоки: Інші сервіси, Телефонні сервіси, IM-SSF, Діючі SCP, Додаткові телефонні сервіси, OSA-GW, Сервери додатків. В перелік блоків необхідно додати блок CSCF, оскільки він перерозподіляє заявки на сервіси між серверами і суттєво впливає на роботу РССД.

РССД і блок CSCF IMS у вигляді МеМО представлено на рис. 2.

DOI 10.15588/1607-3274-2019-4-14

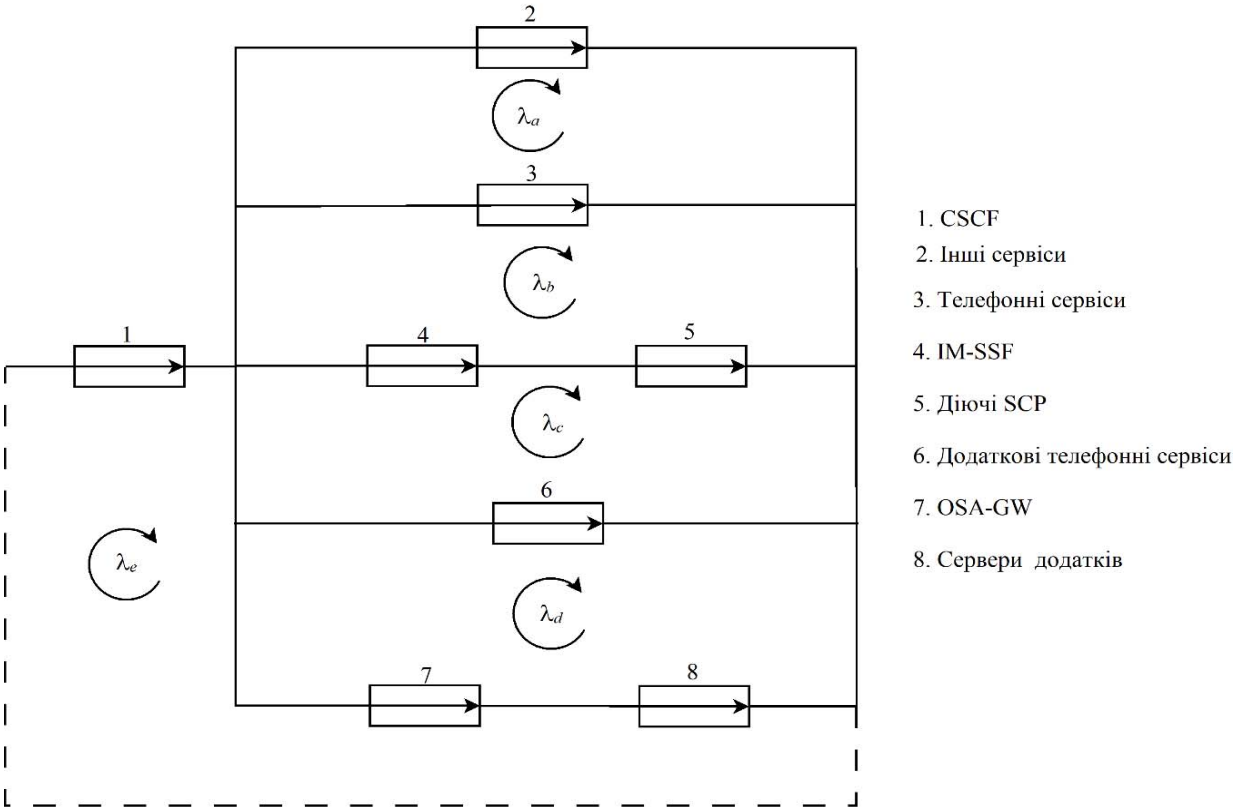


Рисунок 2 – Представлення блоку CSCF та рівня серверів сервісів та додатків у вигляді окремої накладної мережі

Як вже зазначалося, вважатимемо, що блоки досліджуваної мережі представляють собою одноканальні СМО (в даному разі – вісім СМО) з буфером необмеженої ємкості. Інтервали часу між заявками на різноманітні сервіси розподілені за експоненційним законом.

Для використання контурного методу введено уявну гілку (позначена пунктирною лінією), котра створює замкнутий контур. Також на рис. 2 вказані контурні інтенсивності λ_a, λ_b, λ_c, λ_d, λ_e та визначені їх напрямки.

Визначимо примітивну мережу. В даному випадку вона складається з восьми не пов'язаних один з одним вузлів мережі (СМО) (рис. 3).

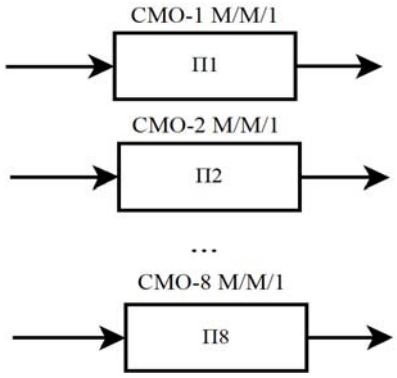


Рисунок 3 – Структурна схема примітивної мережі

Відповідно матриця переходу $\overline{C}$ матиме вигляд (11):

$$\overline{C} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix} \quad (11)$$

Задамо середній час обслуговування заявок в примітивній мережі (12):

$$\overline{t'_{\text{обсл}}} = \begin{pmatrix} t_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & t_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & t_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & t_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & t_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & t_6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & t_7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & t_8 \end{pmatrix} \quad (12)$$

DOI 10.15588/1607-3274-2019-4-14

Завантаження вузлів ρ представимо через середній час обслуговування заявок та інтенсивності гілок. Для примітивної мережі отримаємо наступний вираз (13):

$$\begin{pmatrix}\rho_1'\\ \rho_2'\\ \rho_3'\\ \rho_4'\\ \rho_5'\\ \rho_6'\\ \rho_7'\\ \rho_8'\end{pmatrix}=\begin{pmatrix}t_1&0&0&0&0&0&0&0\\ 0&t_2&0&0&0&0&0&0\\ 0&0&t_3&0&0&0&0&0\\ 0&0&0&t_4&0&0&0&0\\ 0&0&0&0&t_5&0&0&0\\ 0&0&0&0&0&t_6&0&0\\ 0&0&0&0&0&0&t_7&0\\ 0&0&0&0&0&0&0&t_8\end{pmatrix}\begin{pmatrix}\lambda_1'\\ \lambda_2'\\ \lambda_3'\\ \lambda_4'\\ \lambda_5'\\ \lambda_6'\\ \lambda_7'\\ \lambda_8'\end{pmatrix} \quad (13)$$

Для вихідної мережі інваріантне рівняння буде мати вигляд (14):

$$\begin{pmatrix}\rho_a\\ \rho_b\\ \rho_c\\ \rho_d\\ \rho_e\end{pmatrix}=\begin{pmatrix}t_a&0&0&0&0\\ 0&t_b&0&0&0\\ 0&0&t_c&0&0\\ 0&0&0&t_d&0\\ 0&0&0&0&t_t\end{pmatrix}\begin{pmatrix}\lambda_a\\ \lambda_b\\ \lambda_c\\ \lambda_d\\ \lambda_e\end{pmatrix} \quad (14)$$

Транспонована матриця переходу матиме вигляд (15):

$$\overline{C}^T=\begin{pmatrix}0&1&-1&0&0&0&0&0\\ 0&0&1&-1&-1&0&0&0\\ 0&0&0&1&1&-1&0&0\\ 0&0&0&0&0&1&-1&-1\\ 1&0&0&0&0&0&1&1\end{pmatrix} \quad (15)$$

Переходячи від однієї мережі до іншої, для завантаження вузлів ρ отримаємо рівняння (16):

$$\begin{pmatrix}\rho_a\\ \rho_b\\ \rho_c\\ \rho_d\\ \rho_e\end{pmatrix}=\overline{C}^T\overline{\rho}'=$$

$$=\begin{pmatrix}0&1&-1&0&0&0&0&0\\ 0&0&1&-1&-1&0&0&0\\ 0&0&0&1&1&-1&0&0\\ 0&0&0&0&0&1&-1&-1\\ 1&0&0&0&0&0&1&1\end{pmatrix}\begin{pmatrix}\rho_1'\\ \rho_2'\\ \rho_3'\\ \rho_4'\\ \rho_5'\\ \rho_6'\\ \rho_7'\\ \rho_8'\end{pmatrix}=$$

$$=\begin{pmatrix}\rho_2'-\rho_3'\\ \rho_3'-\rho_4'-\rho_5'\\ \rho_4'+\rho_5'-\rho_6'\\ \rho_6'-\rho_7'-\rho_8'\\ \rho_1'+\rho_7'+\rho_8'\end{pmatrix}. \quad (16)$$

Для часу обслуговування заявок отримаємо $\overline{t_{\text{обсл}}}=\overline{C}^T\overline{t_{\text{обсл}}'}\overline{C}$ (рівняння (17)):

$$\overline{t_{\text{обсл}}}=\begin{pmatrix}t_2+t_3&-t_3&0&0&0\\ -t_3&t_3+t_4+t_5&-t_4-t_5&0&0\\ 0&-t_4-t_5&t_4+t_5+t_6&-t_6&0\\ 0&0&-t_6&t_6+t_7+t_6&-t_7-t_8\\ 0&0&0&-t_7-t_8&t_1+t_7+t_8\end{pmatrix}. \quad (17)$$

В результаті для вихідної мережі, виходячи з (5), отримаємо (18):

$$\begin{pmatrix}\rho_2'-\rho_3'\\ \rho_3'-\rho_4'-\rho_5'\\ \rho_4'+\rho_5'-\rho_6'\\ \rho_6'-\rho_7'-\rho_8'\\ \rho_1'+\rho_7'+\rho_8'\end{pmatrix}=$$

$$\begin{pmatrix}t_2+t_3&-t_3&0&0&0\\ -t_3&t_3+t_4+t_5&-t_4-t_5&0&0\\ 0&-t_4-t_5&t_4+t_5+t_6&-t_6&0\\ 0&0&-t_6&t_6+t_7+t_6&-t_7-t_8\\ 0&0&0&-t_7-t_8&t_1+t_7+t_8\end{pmatrix}\begin{pmatrix}\lambda_a\\ \lambda_b\\ \lambda_c\\ \lambda_d\\ \lambda_e\end{pmatrix}. \quad (18)$$

5 РЕЗУЛЬТАТИ

Вхідні дані для розрахунків були отримані в результаті досліджень мережі компанії «Х». Об'єктами вимірювання були апаратні сервери на базі операційної системи Linux, на яких працювали прикладні сервіси: Web-сервер Nginx, сервер IP-телефонії Asterisk, сервер додатків, сервер інтелектуальних сервісів. Характеристики отримувались з журналів стану серверів. Вхідні дані було отримано за період в 24 години – час обслуговування заявок на різноманітні сервіси в різних блоках, інтенсивність вхідних потоків і завантаження вузлів.

Використовуючи для експериментальної частини вхідні дані, отримаємо значення ЙЧХ РССД IMS.

Час обслуговування заявок на різноманітні сервіси в різних блоках (в секундах):

DOI 10.15588/1607-3274-2019-4-14

$$\overline{t'_{\text{обсл}}} = \begin{pmatrix} 0{,}048 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0{,}831 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0{,}482 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0{,}686 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}686 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0{,}507 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0{,}467 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}467 \end{pmatrix}.$$

Завантаження вузлів (СМО, блоків):

$$\begin{pmatrix} \rho'_1 \\ \rho'_2 \\ \rho'_3 \\ \rho'_4 \\ \rho'_5 \\ \rho'_6 \\ \rho'_7 \\ \rho'_8 \end{pmatrix} = \begin{pmatrix} 0.350 \\ 0.195 \\ 0.308 \\ 0.082 \\ 0.082 \\ 0.232 \\ 0.062 \\ 0.062 \end{pmatrix}.$$

Розв'язавши рівняння (18) та використовуючи вирази (8–10), отримаємо значення ЙЧХ блоків РССД, включаючи блок CSCF (табл. 1).

Таблиця 1 – Значення ЙЧХ блоку CSCF та блоків рівня серверів сервісів та додатків

	λ (1/с)	$t_{\text{обсл}}$ (с)	ρ	$\overline{L}$	$\overline{T}_{\text{оч}}$ (с)	$\overline{T}$ (мс)
CSCF	3,027	0,048	0,145	0,025	0,008	56
Інші сервіси	0,481	0,831	0,4	0,266	0,553	1,384
Телефонні сервіси	1,064	0,482	0,513	0,539	0,507	989
IM-SSF	0,269	0,686	0,184	0,042	0,155	841
Діючі SCP	0,269	0,686	0,184	0,042	0,155	841
Додаткові телефоннні сервіси	0,861	0,507	0,437	0,339	0,393	900
OSA-GW	0,352	0,467	0,164	0,032	0,092	559
Сервери додатків	0,352	0,467	0,164	0,032	0,092	559

6 ОБГОВОРЕННЯ

В роботі запропоновано метод розрахунку ЙЧХ РССД для сервісів різних видів (включаючи також блок CSCF).

В сучасних публікаціях щодо ЙЧХ телекомунікаційних мереж [5–10] мова йшла про загальний конвергентний трафік. При цьому не враховувалася специфіка сучасних мультисервісних мереж, а саме – мережі IMS. IMS спроможна надавати різні види сервісів, які відрізняються своїми характеристиками, що потребує врахування особливостей надання різноманітних сервісів при розрахунку ЙЧХ РССД. В даній роботі враховано особливості надання сервісів різних видів, що є розвитком досліджень [5–10]. Окрім того в запропонованому методі визначення ЙЧХ РССД IMS одночасно використовуються підходи класичної ТМО та тензорний аналіз, що надає можливість отримання ЙЧХ для сервісів різних видів.

Для оцінки значень отриманих ЙЧХ для мережі компанії «Х» скористаємося рекомендацією ITU-T Y.1541 [15], а саме – рекомендованими значеннями ЙЧХ для різних класів сервісів.

В нашому випадку можна порівнювати значення IPTD (для різних класів представлена в табл. 2) та розраховані характеристики $\overline{T}_i$, що представлені в табл. 1.

Таблиця 2 – Визначення класів мережної QoS протоколу IP і вимоги до робочих характеристик мережі

Параметр робочої характеристики	Сутність вимоги до робочої характеристики	Класи QoS					
		Клас 0	Клас 1	Клас 2	Клас 3	Клас 4	Клас 5
IPTD	Верхня межа значення IPTD	100 мс	400 мс	100 мс	400 мс	1с	Не визначено

Аналізуючи значення $\overline{T}_i$ (табл. 1) та IPTD (табл. 2), спираючись на дані, представлені в табл. 3, можна стверджувати, що середній час перебування заявки в системі $\overline{T}_i$ для інтелектуальних сервісів, додаткових телефонних сервісів, використання додатків відповідає вимогам класу якості 4. Для телефонних сервісів (VoIP) клас якості повинен бути нульовим або першим і IPTD не повинно перевищувати 400 мс. В мережі компанії «Х» це значення суттєво більше і дорівнює 989 мс. Значення середнього часу перебування заявки в системі $\overline{T}_i$ для інших сервісів – 1,384 мс, що не відповідає вимогам жодного класу якості. Таким чином, компанії «Х» необхідно суттєво поліпшити якість надання телефонних та інших сервісів.

Аналізуючи отримані на основі запропонованого методу результати досліджень мережі компанії «Х», що представлені в табл. 1, також можна стверджувати, що незважаючи на стрімкий розвиток сучасних технологій та мереж, суспільство найчастіше користується звичайними телефонними та додатковими телефонними сервісами (інтенсивності надходження 1,064 1/с та 0,861 1/с, відповідно). Попит на сучасні нові та інтелектуальні сервіси з кожним роком росте, однак досі залишається на незначному рівні (інтенсивності надходження 0,352 1/с та 0,265 1/с, відповідно). Суттєву нішу займають інші сервіси (інтенсивність надходження 0,481 1/с). Значне завантаження телефонних серверів випливає з попередніх міркувань. Суттєве завантаження серверів, що надають Інші сервіси (завантаження 0,4), пояснюється ресурсоємкістю даних сервісів і, відповідно, тривалим часом обслуговування.

DOI 10.15588/1607-3274-2019-4-14

Таблиця 3 – Класи QoS протоколу IP

Клас QoS	Додатки (приклади)	Вузлові механізми	Мережні технології
0	Реального часу, чутливі до тремтіння, з підвищеним ступенем взаємодії (VoIP, VTC)	Окрема черга з привілейованим рівнем обслуговування трафіку	Обмежені маршрутизація і дистанція
1	Реального часу, чутливі до тремтіння, інтерактивні (VoIP, VTC)		Менш обмежені маршрутизація і дистанція
2	Дані транзакцій, з підвищеним ступенем інтерактивності (сигналізація)	Окрема черга, знижений пріоритет	Обмежені маршрутизація і дистанція
3	Дані транзакцій, інтерактивні додатки		Менш обмежені маршрутизація і дистанція
4	Тільки з низькими втратами даних (короткі транзакції, масова передача даних, потоки відео)	Довга черга, знижений пріоритет	Будь-який маршрут/шлях
5	Традиційні додатки стандартних мереж IP	Окрема черга (самий низький пріоритет)	Будь-який маршрут/шлях

Отримані в результаті досліджень значення корелюються з результатами робіт [4–10].

ВИСНОВКИ

В даній роботі досягнута поставлена мета – представлено розроблений метод визначення ЙЧХ рівня серверів сервісів та додатків IMS з урахуванням різних видів сервісів, котрі спроможна надати IMS. Наведено вирази, що надають можливість визначити: середню довжину черги заявок відповідних видів у кожному *i*-му структурному блоці РССД; середній час очікування в черзі заявок відповідних видів у кожному *i*-му структурному блоці РССД; середній час перебування заявок відповідних видів у кожному *i*-му структурному блоці РССД.

Наукова новизна отриманих результатів полягає в тому, що уперше запропоновано метод, який надає можливість визначити ЙЧХ рівня серверів сервісів та додатків IMS з урахуванням різних видів сервісів, котрі спроможна надати IMS.

Практичне значення отриманих результатів полягає в тому, що запропонований метод розрахунку ЙЧХ РССД IMS надасть можливість проектувальникам IMS на ранніх етапах проекту розрахувати ЙЧХ, що дозволить визначити потрібні мережні ресурси для забезпечення необхідного значення якості надання сервісів.

Перспективи подальших досліджень складаються в розвитку запропонованого методу в напрямку урахування самоподібного характеру потоку заявок на сервіси. Крім того, в подальшому слід ураховувати обмеження буферної пам'яті серверів.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Князєва Н.О. Управління інтелектуальними сервісами в мережах наступного покоління / Н. О. Князєва, С. В. Шестопалов. – Одеса : ТОВ Плутон, 2017. – 268 с. – ISBN 978-617-7424-78-8
2. Гольдштейн А. Б. Softswitch / А. Б. Гольдштейн, Б. С. Гольдштейн. – СПб.: БХВ, 2006. – 368 с. – ISBN 5-8206-0117-3
3. Khalid Al'Begain. IMS: A Development and Deployment Perspective / Khalid Al'Begain, Chitra Balakrishna, Luis Angel Galindo, David Moro. – John Wiley & Sons, 2009. – 316 p. Print ISBN:9780470740347 | Online ISBN:9780470750001 | DOI:10.1002/9780470750001
4. Клейнрок Л. Теория массового обслуживания: пер. с англ. / Л. И. Клейнрок, И. Грушко. – М. : Машиностроение, 1979. – 432 с.
5. Пономарев Д. Ю. Программная система для распределения нагрузки информационных систем / Д. Ю. Пономарев // Кибернетика и программирование. – 2013. – № 5. – С. 29–36. DOI: 10.7256/2306-4196.2013.5.9762
6. Fast Accurate Computation of Large-Scale IP Traffic Matrices from Link Loads / [Y. Zhang, M. Roughan, N. Duffield, A. Greenberg] // ACM SIGMETRICS. – 2003. – P. 206–217. DOI: 10.1145/781027.781053
7. Jiang Y. Stochastic Network Calculus / Y. Jiang, Y. Liu. – Springer-Verlag London Limited, 2008. – 229 p. DOI: 10.1007/978-1-84800-127-5
8. Ephremides A. Limitations of Queueing Models in Communication Networks / A. Ephremides // Performance Limits in Communication Theory and Practice, 1988. – P. 143–153. DOI: 10.1007/978-94-009-2794-0
9. Крон Г. Тензорный анализ сетей / Г. Крон – М. : Советское радио, 1978. – 720 с.
10. Lemeshko O. QoS Ensuring over Probability of Timely Delivery in Multipath Routing [Text] / O. Lemeshko, O. Yeremenko, In: Hu Z., Petoukhov S., Dychka I., He M. (eds) // Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, Springer, Cham. – 2019. – Vol. 754. – P. 244–254. DOI: 10.1007/978-3-319-91008-6
11. Глобальная информационная инфраструктура, аспекты протокола интернет и сети последующих поколений: МСЭ-Т Y.3001. – [Действителен от 2011-05-20]. – Женева : Study Group, 2012. – 26 с.
12. Internet protocol data communication service – IP packet transfer and availability performance parameters: ITU-T Recommendation Y.1540. – [Effective from 2016-07-29]. – Geneva : Study Group, 2016. – 51 p.
13. Quality of telecommunication services: concepts, models, objectives and dependability planning – Terms and definitions, related to Quality of Services and network performance including dependability: ITU-R Recommendation E.800. – [Effective from 2008-09-29]. Geneva : Study Group, 2009. – 30 p.
14. Алиев Т. И. Основы моделирования дискретных систем / Т. И. Алиев. – СПб : СПбГУ ИТМО, 2009. – 363 с. ISBN 978-5-7577-0336-7
15. Network Performance Objectives for IP-Based Services: ITU-T Recommendation Y.1541. – [Effective from 2002-05-07]. – Geneva : Study Group, 2002. – 50 p.

Стаття надійшла до редакції 28.07.2019.
Після доробки 17.09.2019.

DOI 10.15588/1607-3274-2019-4-14

УДК 621.391:681.5

МЕТОД ОПРЕДЕЛЕНИЯ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК УРОВНЯ СЕРВЕРОВ СЕРВИСОВ И ПРИЛОЖЕНИЙ IMS

Князева Н. А. – д-р техн. наук, профессор, профессор кафедры Компьютерной инженерии, Одесская национальная академия пищевых технологий, Одесса, Украина.

Шестопалов С. В. – канд. техн. наук, доцент кафедры Компьютерной инженерии, Одесская национальная академия пищевых технологий, Одесса, Украина.

Сиренко А. И. – старший преподаватель кафедры Компьютерной инженерии, Одесская национальная академия пищевых технологий, Одесса, Украина.

АННОТАЦИЯ

Актуальность. Статья посвящена разработке метода определения вероятностно-временных характеристик уровня серверов сервисов и приложений IMS. Показано, что вследствие постоянно растущего разнообразия сервисов, которые способна предоставить IMS, и увеличения спроса на них среди пользователей, а также того, что с развитием телекоммуникаций все большее внимание уделяется качеству предоставления сервисов – QoS, задача оценки качества предоставления сервисов обусловливает актуальность разработки метода определения вероятностно-временных характеристик уровня серверов сервисов и приложений IMS.

Цель. Разработать метод определения вероятностно-временных характеристик уровня серверов сервисов и приложений IMS с учетом различных видов сервисов, которые способна предоставить IMS.

Метод. Рассмотрена архитектура IMS. Основное внимание уделено уровню серверов сервисов и приложений. Для разработки метода определения вероятностно-временных характеристик уровня серверов сервисов и приложений IMS предложено воспользоваться подходами теории телетрафика и тензорным анализом сетей. Предложенный метод представляет последовательность этапов, выполнение которых позволяет определить структурные блоки уровня сервисов и приложений IMS, которые отвечают за предоставление сервисов различных видов; представить блок управления сеансами связи и уровня сервисов и приложений в виде отдельной накладной сети – исходной сети массового обслуживания; для использования контурного метода ввести мнимую ветвь, которая создает замкнутый контур; ввести контурные интенсивности и определить их направления; определить матрицу перехода от исходной сети к примитивной сети; представить инвариантное уравнение для исходной сети; определить контурные интенсивности и на их основе рассчитать интенсивности поступления заявок на сервисы и загрузки серверов в исходной сети. В результате – получить выражения для расчета вероятностно-временных характеристик уровня серверов сервисов и приложений.

Результаты. Предложен метод определения вероятностно-временных характеристик уровня серверов сервисов и приложений IMS на основе подходов теории телетрафика и тензорного анализа сетей, который позволяет учитывать различные виды сервисов, которые способна предоставить IMS.

Выводы. Метод определения вероятностно-временных характеристик уровня серверов сервисов и приложений IMS позволит проектировщикам IMS на ранних этапах проекта рассчитать вероятностно-временные характеристики, что даст возможность определить необходимые сетевые ресурсы для обеспечения требуемого значения качества предоставления сервисов различных видов. В дальнейшем, при развитии предложенного метода, при исследовании уровня сервисов и приложений IMS с целью определения вероятностно-временных характеристик целесообразен учет самоподобия потока заявок на сервисы и ограничения буферной памяти серверов.

КЛЮЧЕВЫЕ СЛОВА: IMS, вероятностно-временные характеристики, уровень серверов сервисов и приложений, подходы теории телетрафика, тензорный анализ, виды сервисов.

UDC 621.391:681.5

METHOD OF DEFINITION OF PROBABILITY-TIME CHARACTERISTICS OF LAYER OF SERVICES AND APPLICATIONS SERVERS OF IMS

Kniazieva N. O. – Dr. Sc., Professor, Professor of Computer Engineering Department, Odessa National Academy of Food Technologies, Odessa, Ukraine.

Shestopalov S. V. – PhD, Senior Lecturer of Computer Engineering Department, Odessa National Academy of Food Technologies, Odessa, Ukraine.

Sirenko O. I. – Senior Instructor of Computer Engineering Department, Odessa National Academy of Food Technologies, Odessa, Ukraine.

ABSTRACT

Context. Article is devoted to development of a method of definition of probability-time characteristics of layer of services and applications servers of IMS. It is shown that constantly growing a variety of services which IMS, and increase in demand for them among users is capable to provide and also the fact that with development of telecommunications the increasing attention is paid to quality of providing services – QoS, the problem of assessment of quality of providing services causes relevance of development of a method of definition of probability-time characteristics of layer of services and applications servers of IMS.

Objective. Develop a method of definition of probability-time characteristics of layer of services and applications servers of IMS taking into account different types of services which IMS is capable to provide.

Method. It is considered architecture of IMS. The main attention is paid to the layer of services and applications servers. For development of a method of definition of probability-time characteristics of layer of services and applications servers of IMS it is offered to use approaches of the queuing theory and the tensor analysis of networks. The offered method represents the sequence of

DOI 10.15588/1607-3274-2019-4-14

stages which execution allows to define structural blocks of layers of services and applications servers of IMS which are responsible for providing services of different types; present call session control function and the layer of services and applications servers in the form of separate laid on network – initial queuing network; for use of a planimetric method to enter the imagined branch which creates the closed circuit; enter planimetric intensity and define their directions; define a transition matrix from initial network to primitive network; present the invariant equation for initial network; define planimetric intensity and on their basis to calculate intensity of receipt of requests for services and loadings of servers in initial network. As a result – to receive expressions for calculation of probability-time characteristics of layer of services and applications servers.

Results. The method of definition of probability-time characteristics of layer of services and applications servers of IMS on the basis of approaches of the queuing theory and tensor analysis of networks which allows to consider different types of services which IMS is capable to provide is offered.

Conclusions. The method of definition of probability-time characteristics of layer of services and applications servers of IMS will allow designers IMS to calculate probability-time characteristics at early stages of the project that will allow to define the necessary network resources for ensuring required value of quality of providing services of different types. Further, at development of the offered method, at a research of layer of services and applications servers of IMS for the purpose of definition of probability-time characteristics accounting of self-similarity of a flow of requests for services and restrictions of a buffer memory of servers is reasonable.

KEYWORDS: IMS, probability-time characteristics, layer of services and applications servers, approaches of the queuing theory, tensor analysis, types of services.

REFERENCES

1. Kniazieva N. O., Shestopalov S. V. Upravlinnia intelektualnymy servisamy v merezhakh nastupnoho pokolinnia. Odesa, TOV Pluton, 2017, 268 p. ISBN 978-617-7424-78-8
2. Goldshteyn A. B., Goldshteyn B. S. Softswitch. SPb, BKhV, 2006, 368 p. ISBN 5-8206-0117-3
3. Khalid Al'Begain, Chitra Balakrishna, Luis Angel Galindo, David Moro IMS: A Development and Deployment Perspective. John Wiley & Sons, 2009, 316 p. Print ISBN:9780470740347 | Online ISBN:9780470750001 | DOI:10.1002/9780470750001
4. Kleynrok L., Grushko I. I. Teoriya massovogo obsluzhivaniya: per. s angl. Moscow, Mashinostroyeniye, 1979, 432 p.
5. Ponomarev D. Yu. Programmnaya sistema dlya raspredeleniya nagruzki informatsionnyih sistem, *Kibernetika i programmirovanie*, 2013, No. 5, pp. 29–36. DOI: 10.7256/2306-4196.2013.5.9762
6. Zhang Y., Roughan M., Duffield N., Greenberg A. Fast Accurate Computation of Large-Scale IP Traffic Matrices from Link Loads, *ACM SIGMETRICS*, 2003, pp. 206–217. DOI: 10.1145/781027.781053
7. Jiang Y., Liu Y. Stochastic Network Calculus. Springer-Verlag London Limited, 2008, 229 p. DOI: 10.1007/978-1-84800-127-5
8. Ephremides A. Limitations of Queueing Models in Communication Networks, *Performance Limits in Communication Theory and Practice*, 1988, pp. 143–153. DOI: 10.1007/978-94-009-2794-0
9. Kron G. Tenzornyy analiz setey. Moscow, Sovetskoye radio, 1978, 720 p.
10. Lemeshko O., Yeremenko O. In Hu Z., Petoukhov S., Dychka I., He M. (eds) QoS Ensuring over Probability of Timely Delivery in Multipath Routing, *Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computting*. Springer, Cham, 2019, Vol. 754, pp. 244–254. DOI: 10.1007/978-3-319-91008-6
11. Globalnaya informatsionnaya infrastruktura. as-pekty protokola internet i seti posleduyushchikh pokoleniy: MSE-T Y.3001. [Deystvitelen ot 2011-05-20]. Zheneva, Study Group, 2012, 26 p.
12. Internet protocol data communication service – IP packet transfer and availability performance parameters: ITU-T Recommendation Y.1540. [Effective from 2016-07-29], Geneva, Study Group, 2016, 51 p.
13. Quality of telecommunication services: concepts, models, objectives and dependability planning – Terms and definitions, related to Quality of Services and network performance including dependability, ITU-R Recommendation E.800. [Effective from 2008-09-29]. Geneva, Study Group, 2009, 30 p.
14. Aliyev T. I. Osnovy modelirovaniya diskretnykh sistem. SPb, SPbGU ITMO. 2009, 363 p. ISBN 978-5-7577-0336-7
15. Network Performance Objectives for IP-Based Services: ITU-T Recommendation Y.1541. [Effective from 2002-05-07]. Geneva, Study Group, 2002, 50 p.

DOI 10.15588/1607-3274-2019-4-14

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

UDC 629.735.051:681.513.5(045)

COMPUTER MODELING OF ACCURACY CHARACTERISTICS OF STRAPDOWN INERTIAL NAVIGATION SYSTEM

Mukhina M. P. – Dr. Sc., Professor, Professor of Department of Aviation Computer-Integrated Complexes, National Aviation University, Kyiv, Ukraine.

Filyashkin M. K. – PhD, Professor, Professor of Department of Aviation Computer-Integrated Complexes, National Aviation University, Kyiv, Ukraine.

ABSTRACT

Context. The problem of correction for operation of strapdown inertial navigation system used for unmanned aerial vehicle is urgent because of further increased requirements to autonomous flight in blackout zones. The object of the study was to simulate the accuracy characteristics of strapdown inertial navigation system based on known (or given) instrument errors of its sensors.

Objective. The goal of the work is to develop a mathematical and computer model of the strapdown inertial navigation system and estimate its accuracy characteristics based on given values of sensor errors.

Method. The mathematical and computer models of the strapdown inertial navigation system based on slow, medium and fast cycles are developed. For the simulation of accuracy characteristics, the strapdown inertial navigation system is represented as a set of dynamic and kinematic equations in local tangent plane coordinate system with the Earth's model taking into account components of gravity acceleration. The models of sensors are developed based on characteristics of low-cost microelectromechanical sensors used onboard. Data fusion algorithms were previously considered and include modified Kalman filter or, for some cases, complimentary filter by compensation scheme, but not considered here in details. Direction cosine matrix for strapdown inertial navigation system algorithms is found by Poisson's method.

Results. The developed models have been realized and simulated in MATLAB+Simulink. Initial parameters (errors of the primary information sensors and the flight conditions) during simulation have been varied: medium, high and low latitudes; direction of flight (along and across the meridian; on and against the direction of rotation of the Earth).

Conclusions. The developed models and their simulations have been compared with actual testing results of strapdown gyrovertical СБКВ-П2А and confirmed the validity. It allow us to recommend them for use in designing strapdown inertial navigation system of unmanned aerial vehicle, as well as for experimental study of innovative data fusion algorithms for integrated satellite and inertial navigation system.

KEYWORDS: strapdown inertial navigation system, satellite navigation system, strapdown gyrovertical, dead reckoning, data fusion.

ABBREVIATIONS

LTP is a local tangent plane;
MEMS are microelectromechanical sensors;
SINS is a strapdown inertial navigation system;
SNS is a satellite navigation system;
UAV is an unmanned aerial vehicle.

NOMENCLATURE

γ is a roll angle;
λ is a longitude;
ϑ is a pitch angle;
Θ is an angle of trajectory inclination;
φ is a geographic latitude;
ψ is a course angle;
Ψ is a track angle;
Ω_0 is an angular speed of the Earth's rotation;
Ω_R, Ω_L, Ω_Φ are the projections of the angular velocity of the Earth's rotation on LTP coordinate axes;
$\omega_{L_\Sigma, R_\Sigma, \Phi_\Sigma}$ are the projections of the angular velocity of the navigation trihedron relative to the inertial space;
$a_{L,R,\Phi}$ are the projections of the apparent acceleration of UAV on the axis of the navigation trihedron;
B is a direction cosine matrix;
$g_{L,R,\Phi}$ are the projections of the acceleration vector of gravity on LTP coordinate axes;
H is a flight altitude;
R is a distance to the Earth's center;
R_m, R_p are the radiuses of meridian and parallels;
V_L, V_R, V_Φ are the components of the flight speed in LTP coordinate system.

INTRODUCTION

Strapdown gyro vertical is related to the class of SINS and outputs main navigation parameters. They are obtained by dead (deduced) reckoning, that is, by continuous integrating signals corresponding to aircraft accelerations. Information about the acceleration comes from accelerometers located on board UAV. The procedure for integrating vector quantities, which are the accelerations and velocities of UAV, is ensured by reproducing (modeling) the corresponding coordinate system on board. The presence of errors in the SINS sensors, in turn, leads to errors in determining the navigational coordinates of UAV movement. That is why while designing SINS it is necessary to reduce the magnitude of the instrument errors in the primary information sensors.

The subsystem of integration of SINS and SNS into one is implemented in the data fusion scheme (usually it is Kalman filter block). This scheme estimates the position and speed of UAV, and this data can come not only to consumers, but also to the delay and phase tracking blocks of SNS receivers. It is necessary to provide high data rate for these blocks so that the time period between measurements in the SNS subsystem can be divided into a large number of subintervals for the purpose of observation correction contour.

DOI 10.15588/1607-3274-2019-4-15

For UAV, sensors of SINS are usually selected to be small and low-cost, and MEMS are almost fully met these requirements. Here there is a problem to develop a mathematical and computer model of the strapdown inertial navigation system and to estimate its accuracy characteristics based on given values of sensor errors.

The object of study is the strapdown inertial navigation systems and its sensors of primary information.

The subject of study is the computer and mathematical model of SINS and its accuracy characteristics depending on instrument errors of primary information sensors.

The purpose of the work is to develop a mathematical and computer model of the strapdown inertial navigation system and estimate its accuracy characteristics based on given values of sensor errors.

1 PROBLEM STATEMENT

As navigation coordinate system, let us use the conditional geographical coordinate system $OLR\Phi$ (Fig. 1). Position of UAV relatively the Earth is determined by geographic longitude λ, latitude φ and distance to the Earth's center R.

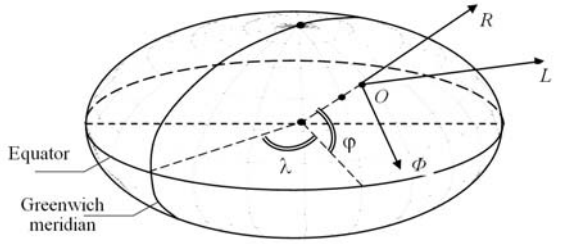


Figure 1 – LTP coordinate system used for navigation

Here there are axes: OR coincides with the vertical; OL is the tangent to the parallel (equator); $O\Phi$ is directed in order to form right-handed coordinate system.

This direction of the axes of the navigation trihedron was chosen taking into account the simplification of the further transition from the geographical to the great-circle coordinate system, since in the great-circle coordinate systems OL axis coincides with the tangent to the great-circle course. It is in this convention of the selected geographical coordinate system. The difference between a conventional geographical and a standard geographical coordinate system is the opposite sign of the latitude value and the course reckoning.

In SINS algorithms, dynamic and kinematic equations are usually distinguished. Dynamic equations realize the three-component SINS scheme in which the coordinates λ, φ_y, H are determined by integration of the following equations:

$$\dot{\lambda} = \frac{V_L}{R_p}; \dot{H} = V_R;$$
$$\dot{\varphi}_y = \frac{V_\Phi}{R_m}; \varphi = -\varphi_y. \quad (1)$$

The components of the flight speed V_L, V_R, V_Φ in the navigation coordinate system are determined by projecting the vector equation on the corresponding axes of the navigation trihedron:

$$\dot{V}_L = a_L + V_R\omega_{\Phi_\Sigma} - V_\Phi\omega_{R_\Sigma} + g_L;$$
$$\dot{V}_R = a_R + V_\Phi\omega_{L_\Sigma} - V_L\omega_{\Phi_\Sigma} + g_R; \quad (2)$$
$$\dot{V}_\Phi = a_\Phi + V_L\omega_{R_\Sigma} - V_R\omega_{L_\Sigma} + g_\Phi,$$

where

$$\omega_{\Phi_\Sigma} = \omega_{\Phi_V} + 2\Omega_\Phi;$$
$$\omega_{R_\Sigma} = \omega_{R_V} + 2\Omega_R;$$
$$\omega_{L_\Sigma} = \omega_{L_V} + 2\Omega_L.$$

In turn, the components of the relative angular velocity of the navigational trihedron and the rotation speeds of the Earth are determined by the relations:

$$\omega_{L_V} = \frac{V_\Phi}{R_m} = \dot{\varphi}_y;$$
$$\omega_{RV} = -\frac{V_L}{R_p}\sin\varphi_y = -\dot{\lambda}\sin\varphi_y; \quad (3)$$
$$\omega_{\Phi_V} = -\frac{V_L}{R_p} = -\dot{\lambda};$$
$$\Omega_L = 0; \Omega_R = \Omega_0\sin\varphi; \Omega_\Phi = -\Omega_0\cos\varphi.$$

Here Ω_0 is equal to $7.27\cdot10^{-5}$ rad/sec.

2 REVIEW OF THE LITERATURE

The inertial navigation systems error models were proposed in [1] which also puts all of the known models in the same framework and shows the equivalence between them. The authors proposed the methodology when any new model which will ever be developed can be added to general one, but such unification had several weak spots like impossibility to get combination of several error sources.

The most significant error source is computational one, namely connected with recalculation of DCM or using quaternions as it is done and analyzed in [2]. Authors adopted dual quaternion algebra, as unified mathematical tool for representing the general displacement of a rigid body, to analyze error characteristics of the strapdown INS. Accuracy characteristics for using Poisson's equation to find DCM is studied in [3], and it is more traditional approach for integrated SINS.

The development of novel miniature sensory of SINS is considered in [4]. It covers the sources of modern MEMS together with [5]. The research of MEMS models is done in [6], where low-cost sensors are represented as error sources with short-term (high-frequency) and long-term (low-frequency) components, via Allan variance, wavelet de-nosing and the selection of the level of decomposition for a suitable combination between these techniques. The same technique (Allan variance analysis)

DOI 10.15588/1607-3274-2019-4-15

is used in [7], where the error model is simply represented in the form of the root mean square random drift error varied with averaging time.

The Earth's model is selected by researcher depending on the given tasks and depends of accuracy requirements to gravity acceleration components like in [8] where for integration SINS with SNS the standard GPS Earth Centred Earth Fixed reference frame was selected together with Earth's model.

Used here models of instrument errors of SINS are previously studied by authors and gathered in book [9].

An integrated SINS-SNS based on the theory of multisensor data fusion is presented in [10]. Error models for the inertial measurement unit are generated and included in the extended Kalman filter for SINS. An improved decentralized Kalman filter is developed to eliminate obvious error of SNS data and reduce the load of calculation. An adaptive federal Kalman filter is used for data fusion between SINS and SNS to provide smoothed and continuous positioning data against the presence of radio blackout or communication dropouts and the unbounded SINS errors growing with time.

3 MATERIALS AND METHODS

Scheme of navigational calculation algorithm is the following.

Performing some transformations and taking into account the equality of the individual components of the initial dynamic and kinematic equations (1)–(3) to zero, the algorithm for performing navigation calculations in the geographic coordinate system can be represented as it is given in [11, 12]. In case of insufficient speed of the airborne processor of the navigation computer, the SINS operation algorithm can be divided by two or even three levels according to the required calculation speed (by the duration of the sampling period), which are characterized the correspondingly fast, medium, and slow calculation cycles.

Fast cycle is described as following:

$$\begin{aligned}\omega_{y_\Sigma} &= \omega_y - \omega_{y_{\Phi LR}};\\ \omega_{x_\Sigma} &= \omega_x - \omega_{x_{\Phi LR}};\\ \omega_{z_\Sigma} &= \omega_z - \omega_{z_{\Phi LR}}.\end{aligned} \tag{4}$$

$$\begin{aligned}\dot\psi &= \left(\omega_{y_\Sigma}\cos\gamma - \omega_{z_\Sigma}\sin\gamma\right)\sec\vartheta;\\ \dot\gamma &= \omega_{x_\Sigma} + \mathrm{tg}\vartheta\,\left(\omega_{z_\Sigma}\sin\gamma - \omega_{y_\Sigma}\cos\gamma\right);\\ \dot\vartheta &= \omega_{y_\Sigma}\sin\gamma + \omega_{z\Sigma}\cos\gamma;\\ \psi_g &= (90^\circ - \psi).\end{aligned} \tag{5}$$

$$B = \begin{bmatrix} \cos\psi\cos\vartheta & \sin\psi\sin\gamma - \cos\psi\sin\vartheta\cos\gamma & \sin\psi\cos\gamma + \sin\psi\cos\vartheta\sin\gamma \\ \sin\vartheta & \cos\vartheta\cos\gamma & -\cos\vartheta\sin\gamma \\ -\sin\psi\cos\vartheta & \cos\psi\sin\gamma + \sin\psi\sin\vartheta\cos\gamma & \cos\psi\cos\gamma - \sin\psi\sin\vartheta\sin\gamma \end{bmatrix} \tag{6}$$

Medium cycle is described as following:

$$\begin{bmatrix} a_L \\ a_R \\ a_\Phi \end{bmatrix} = \mathbf{B}\begin{bmatrix} a_x \\ a_y \\ a_z \end{bmatrix}; \tag{7}$$

$$\begin{aligned}\dot V_L &= a_L + V_R\left(\omega_{\Phi_V} + 2\Omega_\Phi\right) - V_\Phi\left(\omega_{R_V} + 2\Omega_R\right);\\ \dot V_R &= a_R + V_\Phi\omega_{L_V} - V_L\left(\omega_{\Phi_V} + 2\Omega_\Phi\right) + g_R;\\ \dot V_\Phi &= a_\Phi + V_L\left(\omega_{R_V} + 2\Omega_R\right) - V_R\omega_{L_V}.\end{aligned} \tag{8}$$

Slow cycle is described as following:

$$\begin{aligned}\dot\lambda &= -\omega_{\Phi_V} = \frac{V_L}{R_p};\\ \dot H &= V_R;\\ \dot\varphi_y &= \omega_{L_V} = \frac{V_\Phi}{R_m};\end{aligned} \tag{9}$$

$$\begin{aligned}\omega_{RV} &= \omega_{\Phi_V}\sin\varphi_y;\\ \varphi &= -\varphi_y;\\ \Omega_R &= \Omega_0\sin\varphi;\\ \Omega_\Phi &= -\Omega_0\cos\varphi.\end{aligned} \tag{10}$$

$$\begin{bmatrix} \omega_{x_{\Phi LR}} \\ \omega_{y_{\Phi LR}} \\ \omega_{z_{\Phi LR}} \end{bmatrix} = \mathbf{B}^T\begin{bmatrix} \omega_{\Phi_V} + \Omega_\Phi \\ \omega_{R_V} + \Omega_R \\ \omega_{L_V} \end{bmatrix}. \tag{11}$$

The Earth's model is described as following:

$$\begin{aligned}R_p &= \frac{a\cos\varphi}{\sqrt{1 - e^2\sin^2\varphi}} + H\cos\varphi;\\ R_m &= \frac{a\left(1 - e^2\right)}{\left(1 - e^2\sin^2\varphi\right)^{\frac{3}{2}}} + H;\end{aligned} \tag{12}$$

$$g_R = -g\left(1 + 5.2884\cdot10^{-3}\sin^2\varphi\right)\left[1 - \frac{2H}{R_0}\left(1 - e\,\sin^2\varphi\right)\right].$$

The initial parameters for navigational calculations are: strapdown gyrovertical information about the projections of angular velocities and accelerations on the axes of the body-fixed coordinate system, initial values of the geographic course ψ_{g0}, roll γ_0, pitch ϑ_0 obtained as a result of the initial alignment of gyrovertical. Also initial coordinates are used: geographic longitude φ_0, geographic longitude λ_0 and initial flight altitude H_0. In the case of alignment on vehicle, projections of the initial speed of UAV are introduced as initial conditions: V_{L0}, V_{H0}, $V_{\Phi0}$.

The constants in the algorithms of navigation calculations are:

– the Earth's angular velocity: $\Omega_0 = 7.27\cdot10^{-5}$ rad/sec;

– semi-major axis of the ellipsoid of revolution $a = 6378388$ m;

– eccentricity of rotation ellipsoid $e^2 = 6.7227\cdot10^{-3}$;

– acceleration of gravity force at the equator $g = 9.78045$ m/sec^2;

DOI 10.15588/1607-3274-2019-4-15

– radius of a sphere equal to the geoid $R_0 = 6371116$ m.

Initial conditions are calculated as following:

$$R_{p_0} = \frac{a\cos\varphi_0}{\sqrt{1-e^2\sin^2\varphi_0}} + H\cos\varphi_0;$$

$$R_{m_0} = \frac{a\left(1-e^2\right)}{\left(1-e^2\sin^2\varphi_0\right)^{\frac{3}{2}}} + H_0;$$

$$g_{R_0} = -g\left(1+5.2884\cdot10^{-3}\sin^2\varphi_0\right)\left[1-\frac{2H_0}{R_0}\left(1-e\ \sin^2\varphi_0\right)\right];$$

$$\omega_{\Phi_{V0}} = \frac{V_{L0}}{R_{p_0}};\ \ \omega_{L_{V0}} = \frac{V_{\Phi_0}}{R_{m_0}};$$

$$\varphi_{y_0} = -\varphi_0;\ \ \omega_{RV0} = \omega_{\Phi_V 0}\sin\varphi_{y_0};$$

$$\Omega_{R0} = \Omega_0\sin\varphi_0;\ \ \Omega_{\Phi_0} = -\Omega_0\cos\varphi_0.$$

Moreover, the initial transposed direction cosine matrix is calculated by the initial values of the geographic course ψ_{g0}, roll γ_0, pitch ϑ_0. It must be noted that geographic course ψ_g is converted to the yaw angle as $\psi_0 = 90° - \psi_{g0}$.

Initial direction cosine matrix is calculated by (6) and then the initial values of angular speed components can be obtained:

$$\begin{bmatrix} \omega_{x_{\Phi LR_0}} \\ \omega_{y_{\Phi LR_0}} \\ \omega_{z_{\Phi LR_0}} \end{bmatrix} = \mathbf{B}_0^T \begin{bmatrix} \omega_{\Phi_{V0}} + \Omega_{\Phi_0} \\ \omega_{R_{V0}} + \Omega_{R0} \\ \omega_{L_{V0}} \end{bmatrix}.$$

Further, at each step, using the information from strapdown gyrovertical about the projections of angular velocities and accelerations on the axes of the body-fixed coordinate system, equations (4)–(12) given in the algorithm are successively solved.

If necessary, the navigation algorithms can be supplemented by the equations for calculating the ground speed Vg, the track angle Ψ and the angle of trajectory inclination Θ

$$V_g = \sqrt{V_L^2 + V_\Phi^2};$$

$$\Theta = \arcsin\frac{V_R}{\sqrt{V_L^2 + V_\Phi^2 + V_R^2}};$$

$$\Psi = \arccos\frac{V_L}{\sqrt{V_L^2 + V_\Phi^2}}.$$

Also, if necessary, the SINS operation algorithm can be divided according to the required calculation speed into three stages characterizing the fast, medium and slow calculation pace. Strapdown gyrovertical algorithms are carried out at the fast calculation rate (about 200 Hz). Here the updating and precise processing of signals are done for integrating the primary information sensors. SINS algorithms use the already processed information on the projections of angular velocities and accelerations on the axes of the body-fixed coordinate system.

In the above algorithms, the SINS alignment algorithms and algorithms for pre-flight calibration of primary information sensors are not implemented. It is believed that this problem is solved in the strapdown gyrovertical at the stage of pre-flight preparation.

4 EXPERIMENTS

The studies were carried out using Simulink visual modeling program, which is part of the MATLAB universal mathematical programming package.

During the simulation, the following subsystems were created and used: subsystems of the reference (ideal) navigation system "E_HC" and the investigated SINS "BINC", subsystems of the Earth model (reference "E_Zemlya" and simplified "Zemlya"), subsystem of automatic control system and of primary information sensors «САУ-Datchiki». In addition, the subsystem for registering simulation results "Registration" and the subsystem for specifying parameters (initial conditions) of simulation "Start_napametru" were created.

The general interface of simulation block diagram is shown in Fig. 2.

Mathematical models of the reference navigation system and the studied SINS were built on a hierarchical principle. The subsystem "BINC" (Fig. 3a) consists of the several subsystems: "Accelerations" (Fig. 3 b), "Angular speeds" (Fig. 3 c), "Linear speeds" (Fig. 3 d), "Coordinates" (Fig. 3 e).

In the subsystem "Accelerations" equations (5)–(8) of the SINS algorithm are solved, and the transposed matrix **B** is also formed.

The subsystem "Angular speeds" models equation (4) for the components of the angular velocity in equation (9) and equation (12).

The subsystem "Speeds" simulates the equations (9) and projections speed vector components on LTP coordinate system.

The subsystem "Coordinates" solves equations (10) of the SINS algorithm.

The block diagram of ideal navigation system is represented in Fig. 4 without opening the corresponding subsystems since they are much similar to previously explained except including sources of errors (both instrument and measurement-method ones).

The Earth model is simulated in the block "Zemiya". Here the components of the angular velocity of the Earth's rotation Ω_R, Ω_Φ, are calculated together with components of gravity force according to equations (12). Depending on the given assumptions, the Earth can be represented by a sphere or spheroid; rotating or not rotating. These changes are made from the "Start_napametru" subsystem.

DOI 10.15588/1607-3274-2019-4-15

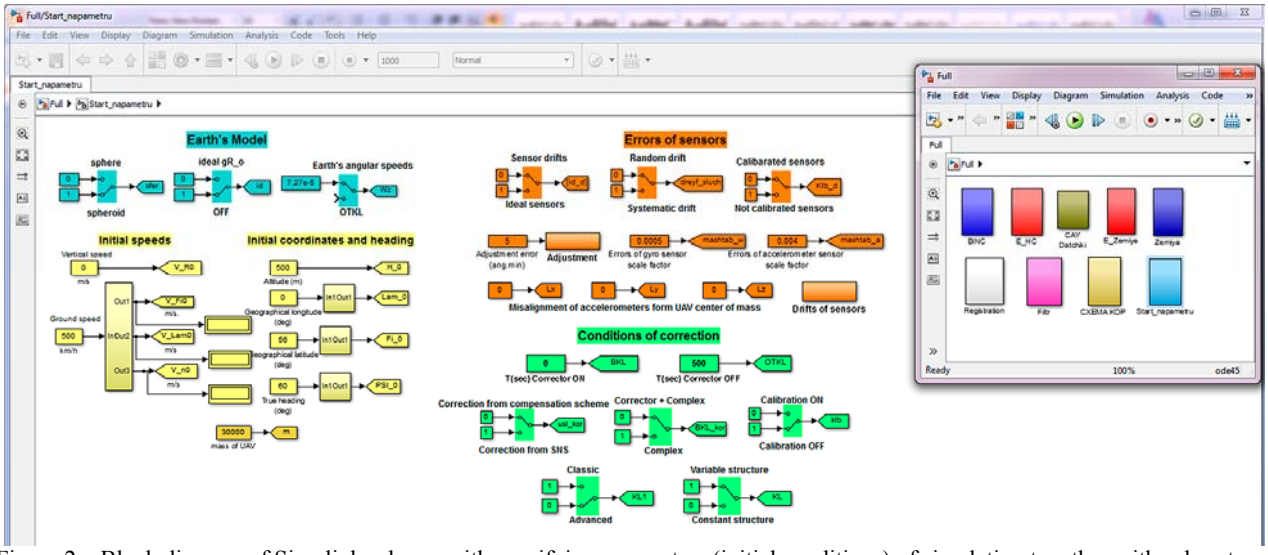
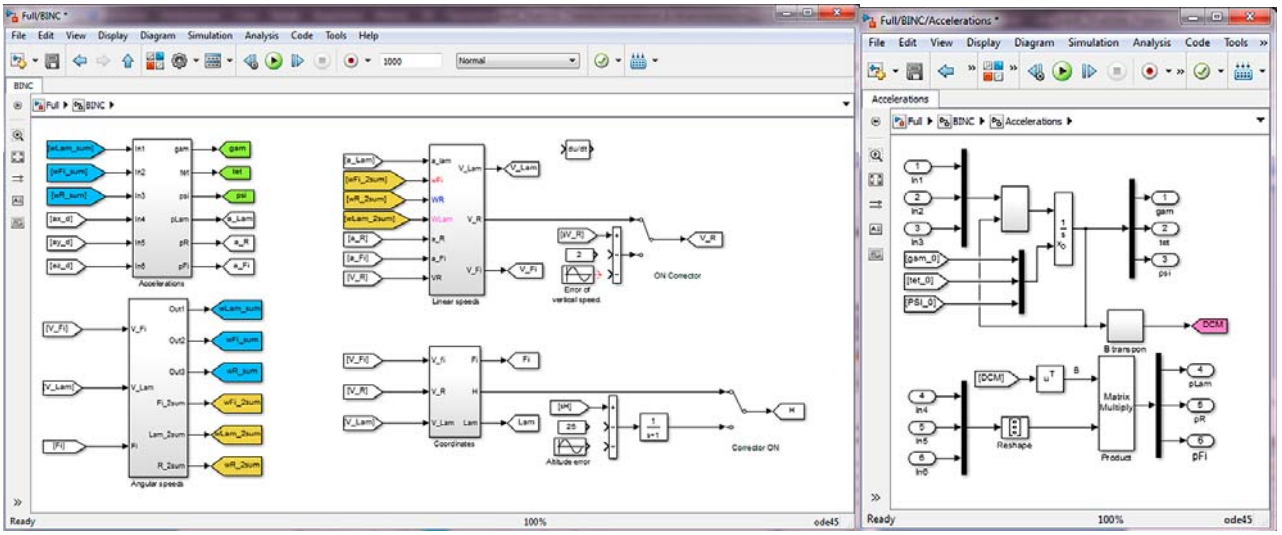
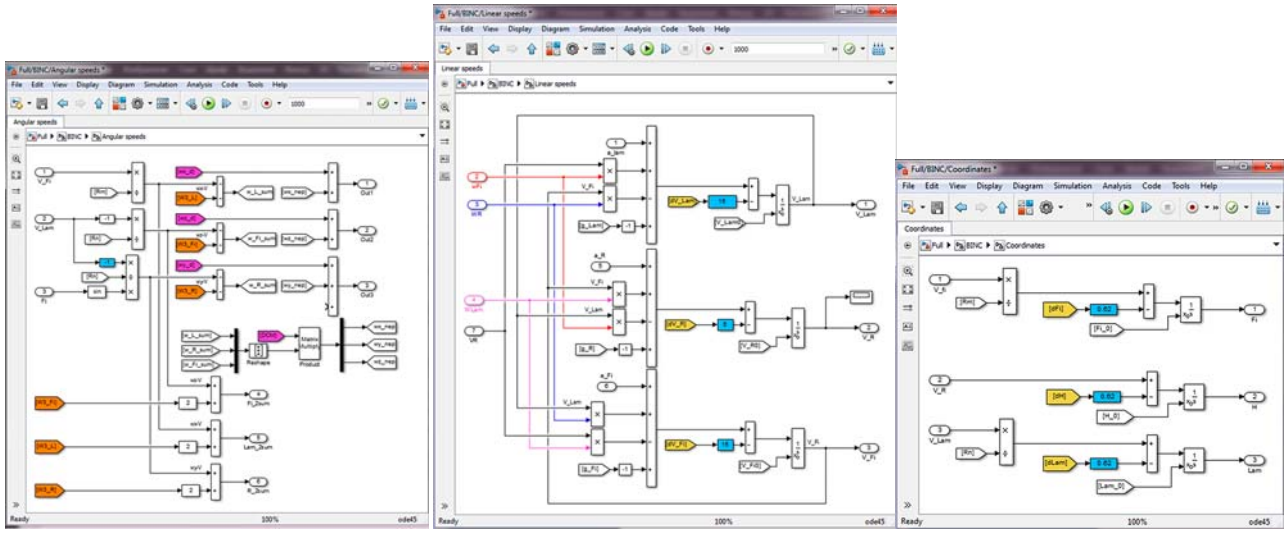


Figure 2 – Block diagram of Simulink scheme with specifying parameters (initial conditions) of simulation together with subsystems



a b



c d e

Figure 3 – Block diagram of Simulink scheme of subsystem "BINC" (with all four subsystems)

DOI 10.15588/1607-3274-2019-4-15

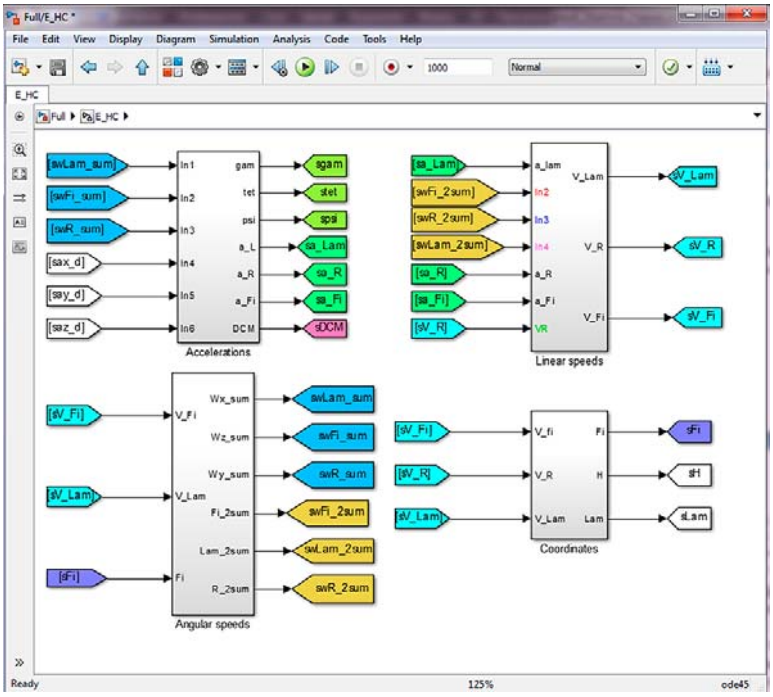


Figure 4 – Block diagram of ideal navigation system in Simulink

5 RESULTS

The main contribution to the dead reckoning errors of the navigation parameters is still made not by the measurement-method errors of the SINS algorithms, but by the instrumental errors of the primary information sensors. The available technical documentation for strapdown gyrovertical СБКВ-П2А (Operation Manual КИНД. 402113.029) contains information on the measurement error of the components of the angular velocity $(\pm 2\sigma) = \pm 0.1$ °/sec and overload $(\pm 2\sigma) = \pm 0.01$ (i.e., errors in acceleration measurement $(\pm 2\sigma) = \pm 0.1$ m/sec^2). Considering the type of sensors used in sensor unit (besides it is thermostated): angular velocity sensors based on dynamically tuned gyroscopes and linear acceleration sensors based on pendulum accelerometers, it can be assumed that the characteristics of such sensors should be three...four orders of magnitude more accurate than declared in manual.

In particular, strapdown gyrovertical СБКВ-П2А has the alignment mode based on gyrocompassing. This mode involves measuring the angular velocity of the Earth s rotation $\Omega_0 = 0.00416$°/sec, i.e. the accuracy characteristics of the angular velocity sensors should allow such a value to be measured. Given that in the course channel, strapdown gyrovertical СБКВ-П2А has two angular velocity sensors, in order to increase the accuracy of measuring small angular velocities, it can be assumed that the accuracy characteristics of the used gyros are at the limit acceptable for systems of this class. In the future, we assume that the measurement error of the components of the angular velocities should be at least an order of magnitude smaller than the angular velocity of the Earth's rotation and be $(\pm 2\sigma) = \pm 0.0001...0.0005$°/sec.

Given that the primary information sensors should be equivalent, i.e. the influence of the errors of the angular velocity sensors and accelerometers on the overall error of the navigation system should be approximately the same; it can be approximately calculated that the error of the accelerometer should be within the range $(\pm 2\sigma) = \pm 0.01 \ldots 0.05$ m/sec^2.

With such maximum values of the errors of the primary information sensors, a series of experiments were carried out to evaluate the accuracy of the calculation of navigation parameters using truncated SINS algorithms. As output parameters, errors in calculating the angular orientation parameters of UAV: roll and pitch angles, course angle, as well as components of the UAV speeds, were estimated. During the research, the errors of the primary information sensors and the flight conditions of the aircraft varied: medium, high and low latitudes; direction of flight (along and across the meridian; on and against the direction of rotation of the Earth), etc.

Figure 5 illustrates the typical behavior of the change in the dead reckoning errors of navigation parameters: heading, roll, pitch by using algorithms of strapdown gyrovertical under for measurement errors of the components of the angular velocity by roll and pitch in 0.0002°/sec, in course 0.0001°/sec (in the course channel of the system, in order to improve the accuracy of course reckoning, two angular velocity sensors are installed). The accelerometer errors were 0.02 m/sec^2 (the error sign was chosen arbitrarily for different sensors). Launch conditions were: 10° of northern latitude, 50° of eastern, initial ground speed was 400 km/h; initial flight altitude was 500 m.

With such errors of the primary information sensors, the strapdown gyrovertical fully meets its functionality as

DOI 10.15588/1607-3274-2019-4-15

attitude-and-heading reference system. The errors in dead reckoning of roll and pitch angles do not exceed 0.4° per hour of flight (the errors declared in the system specification sheet are 0.5°). The dead reckoning errors of course does not exceed 0.25° per hour of flight (the errors declared in the system specification sheet are 0.3°). Such level of accuracy characteristics of the sensors are used for further research.

If the errors in determining the roll and pitch angles, changing with the period of Schuler pendulum, do not exceed the required values, then the error in determining the course has a component that grows proportionally to the flight time. Namely this fact forces the developers to use the magnetometer as a correction device in the course channel.

In addition to estimating the errors in dead reckoning the parameters of the angular orientation, the study was also conducted to investigate the accuracy of the dead reckoning of the navigation parameters of the UAV trajectory motion: coordinates and velocity components under the same errors of the primary information sensors. Errors in dead reckoning the parameters of the UAV trajectory motion substantially depend on the launch conditions, in particular, on the latitude and direction of flight. Moreover, it was revealed that a change in the start condition causes, as it were, "overflowing" of errors from the latitude channel to the longitude channel and vice versa. Figure 6 shows the typical behavior of the change in the errors of dead reckoning coordinates and velocities with an approximately uniform distribution of errors in two channels.

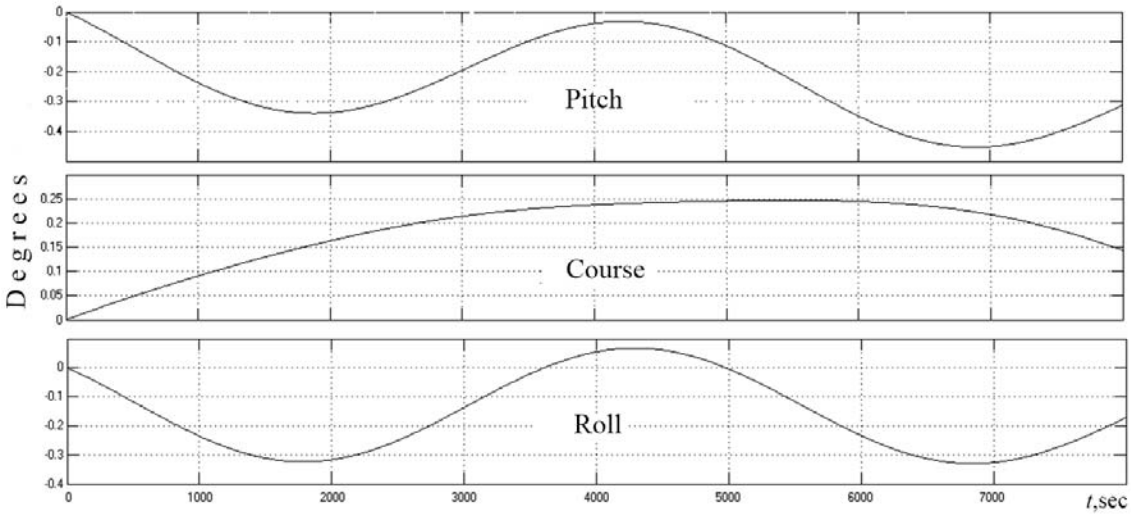


Figure 5 – Errors in pitch, roll and course angles for the given values of errors of primary information sensors

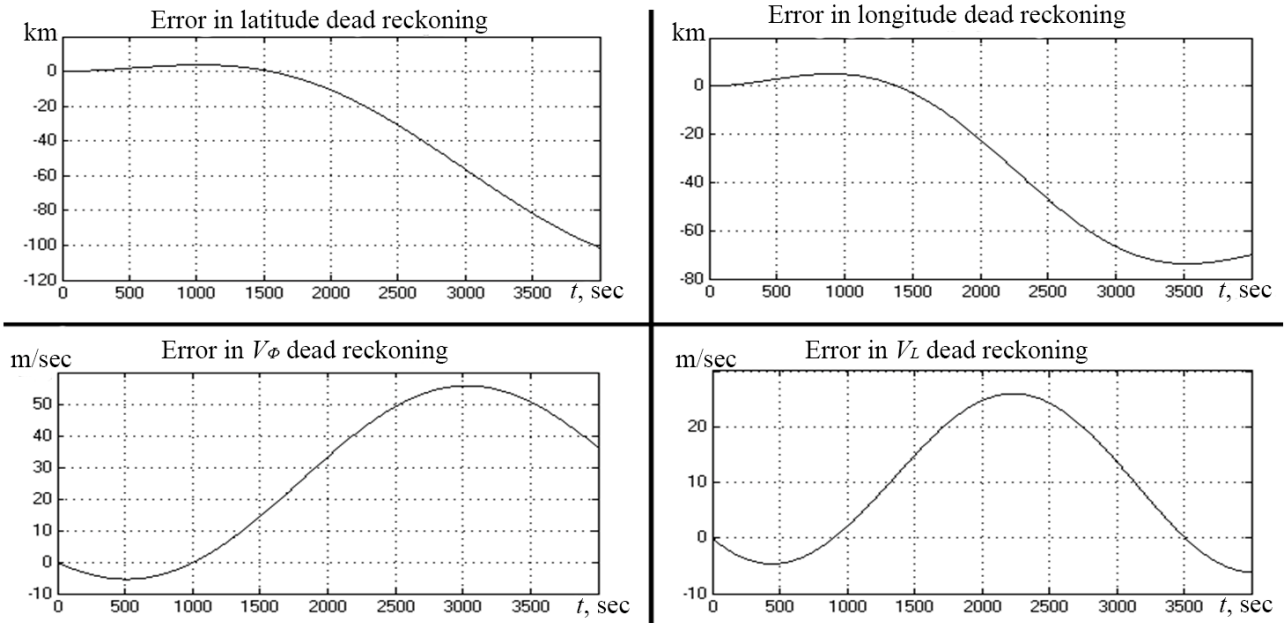


Figure 6 – Errors in coordinates and velocity components

DOI 10.15588/1607-3274-2019-4-15

6 DISCUSSION

Errors of the components of the aircraft speed reach 30...50 m/s per hour of flight and this information is practically not used by consumers (a similar situation occurs in the platform gyrovertical). Errors in the calculation of coordinates with such primary information sensors are generally unacceptable (70...80 km per hour of flight), which once again confirms the impossibility of creating an autonomous SINS on their basis.

Systems of this type can only be used when integrating them with other navigation systems, in particular with SNS. In this case, SINS interpolates the values of the navigation parameters between two adjacent moments of information coming from SNS, and also provides navigation information to consumers with a short-term loss of signals from satellites. With long interruptions in the SNS operation, SINS should be integrate with other navigation systems.

CONCLUSIONS

The urgent problem of mathematical support development is solved to automate the sampling at diagnostic and recognizing model building by precedents.

The scientific novelty is the following. At first the novel approach has been proposed in the using two models of SINS instead one: ideal one, free from all errors, and the real one with selected variants of error sources. Unlike known approach, such technique allows us to estimate accuracy characteristics of SINS and degree of participation of primary information sensor errors in them.

The practical significance of obtained results is that the software realizing the proposed three-level algorithms of SINS operation is developed, as well as simulation to be conducted and proved by comparing with test results of strapdown gyrovertical СБКВ-П2А.

Prospects for further research are the following. The conducted studies confirm the dependence of the accuracy of the dead reckoning navigational parameters on the performance of UAV maneuvers and on other factors, in particular, on the mismatch of the installation location of SINS block with the center of mass of UAV, but with sufficiently vigorous maneuvering. For further research, information is required on the aerodynamic characteristics of a particular type of UAV, as well as on the algorithms of its control system.

ACKNOWLEDGEMENTS

The work is supported by the scientific research project of National Aviation University “Development of algorithms of data processing in inertial system for navigation problem solution” (registration number 04/060-06).

REFERENCES

1. Goshen-Meskin D., Bar-Itzhack I. Y. Unified approach to inertial navigation system error modeling, *Journal of Guidance, Control, and Dynamics,* 1992, Vol. 15, No. 3, pp. 648–653.
2. Wu Y. Strapdown inertial navigation using dual quaternion algebra: error analysis, IEEE Transactions on Aerospace and Electronic Systems, 2006, Vol. 42, No. 1, pp. 259–266.
3. Golovan A. A., Demidov O. V., Vavilova N. B. On GPS/GLONASS/INS tight integration for gimbal and strapdown systems of different accuracy, *IFAC Proceedings Volumes*, 2010, Vol. 43, No. 15, pp. 505–509.
4. Filyashkin M. K. Method of measuring of angular orientation parameters in micromechanical inertial-satellite navigation systems, *Electronics and control systems*, 2014, No. 4, pp. 18–24.
5. Filyashkin M. K., Mukhina M. P. Data fusion schemes in aided navigation systems, *Electronics and control systems*, 2013, No. 4, pp. 11–18.
6. Quinchia A. A comparison between different error modeling of MEMS applied to GPS/INS integrated systems, *Sensors*, 2013, Vol. 13, No. 8, pp. 9549–9588.
7. Zhang X. Allan variance analysis on error characters of MEMS inertial sensors for an FPGA-based GPS/INS system, *Proceedings of the International Symposium on GPS/GNNS*, 2008, pp. 127–133.
8. George M., Sukkarieh S. Tightly coupled INS/GPS with bias estimation for UAV applications, *Proceedings of Australiasian Conference on Robotics and Automation (ACRA),* 2005.
9. Mackison D. L. Review of strapdown inertial navigation technology, *Journal of Guidance, Control, and Dynamics,* 1998, Vol. 21, No. 6, pp. 1018–1018.
10. Shaeffer D. K. MEMS inertial sensors: A tutorial overview, *IEEE Communications Magazine*, 2013, Vol. 51, No. 4, pp. 100–109.
11. Filyashkin M. K., Rogozhyn V.O., Skrypets A.V., Lukinova T.I. Inertial-satellite navigation systems. Kyiv, NAU, 2008, 310 p.
12. Bin W. Study on adaptive GPS/INS integrated navigation system, *Proceedings of the 2003 IEEE International Conference on Intelligent Transportation Systems*, IEEE, 2003. Vol. 2, pp. 1016–1021.

Received 03.08.2019.
Accepted 25.10.2019.

УДК 629.735.051:681.513.5(045)

КОМП’ЮТЕРНЕ МОДЕЛЮВАННЯ ТОЧНІСНИХ ХАРАКТЕРИСТИК БЕЗПЛАТФОРМЕННОЇ ІНЕРЦІАЛЬНОЇ НАВІГАЦІЙНОЇ СИСТЕМИ

Мухіна М. П. – д-р техн. наук, професор кафедри авіаційних комп’ютерно-інтегрованих комплексів Національного авіаційного університету, Київ, Україна.

Філяшкін М. К. – кандидат техн. наук, професор кафедри авіаційних комп’ютерно-інтегрованих комплексів Національного авіаційного університету, Київ, Україна.

АНОТАЦІЯ

Актуальність. Розглядається задача корекції роботи безплатформенної інерціальної навігаційної системи, що використовується на борту безпілотного літального апарату. Завданням дослідження було моделювання точнісних характеристик безплатформенної інерціальної навігаційної системи на основі відомих (або заданих) інструментальних похибок її датчиків.

Мета роботи – розробити математичну та комп’ютерну модель безплатформенної інерціальної навігаційної системи та оцінити точнісні характеристики на основі заданих значень похибок датчика.

Метод. Розроблено математичну та комп’ютерну моделі безплатформенної інерціальної навігаційної системи на основі повільних, середніх та швидких циклів обчислення. Для моделювання точнісних характеристик безплатформенна інерціальна навігаційна система подається у вигляді системи динамічних та кінематичних рівнянь у місцевій геотопічній системи координат із обраною моделлю Землі з урахуванням компонентів прискорення сили тяжіння. Моделі датчиків розроблені на основі характеристик недо-

DOI 10.15588/1607-3274-2019-4-15

рогих мікроелектромеханічних датчиків, що використовуються на борту. Алгоритми синтезу даних раніше вже були розглянуті і включають модифікований фільтр Калмана або, в деяких випадках, компліментарний фільтр за схемою компенсації, але тут детально не розглядаються. Матриця напрямних косинусів для алгоритмів числення шляху інерціальної навігації знайдена за методом Пуассона.

Результати. Розроблені моделі були реалізовані та змодельовані в середовищі MATLAB + Simulink. Початкові параметри (похибки первинних датчиків інформації та умови польоту) під час моделювання були різноманітними: середні, високі та низькі широти; напрям польоту (вздовж і проти меридіану; за та проти напрямку обертання Землі).

Висновки. Розроблені моделі та їх випробування були порівняні з фактичними результатами тестування безплатформенної курсовертикалі СБКВ-П2А та підтвердили свою обгрунтованість. Це дозволяє рекомендувати їх для використання при проектуванні інерціальної навігаційної системи безпілотного літального апарату, а також для експериментального вивчення інноваційних алгоритмів синтезу обробки даних для інтегрованої супутникової та інерціальної навігаційної системи.

КЛЮЧОВІ СЛОВА: безплатформенна інерціальна навігаційна система, супутникова навігаційна система, безплатформенна курсовертикаль, числення шляху, комплексування інформації.

УДК 629.735.051: 681.513.5 (045)

ОЦЕНКА ТОЧНОСТНЫХ ХАРАКТЕРИСТИК БЕСПЛАТФОРМЕННОЙ ИНЕРЦИАЛЬНОЙ НАВИГАЦИОННОЙ СИСТЕМЫ

Мухина М. П. – д-р техн. наук, профессор кафедры авиационных компьютерно-интегрированных комплексов Национального авиационного университета, Киев, Украина.

Филяшкин Н. К. – канд. техн. наук, профессор кафедры авиационных компьютерно-интегрированных комплексов Национального авиационного университета, Киев, Украина.

АННОТАЦИЯ

Актуальность. Рассматривается задача коррекции работы бесплатформенной инерциальной навигационной системы, используемой на борту беспилотного летательного аппарата. Задачей исследования было моделирование точностных характеристик бесплатформенной инерциальной навигационной системы на основе известных (или заданных) инструментальных погрешностей ее датчиков.

Цель работы – разработать математическую и компьютерную модель бесплатформенные инерциальной навигационной системы и оценить точностные характеристики на основе заданных значений погрешностей датчика.

Метод. Разработана математическая и компьютерная модели бесплатформенной инерциальной навигационной системы на основе медленных, средних и быстрых циклов вычисления. Для моделирования точностных характеристик бесплатформенная инерциальная навигационная система представляется в виде системы динамических и кинематических уравнений в местной геотопической системе координат с выбранной моделью Земли и с учетом компонентов ускорения силы тяжести. Модели датчиков разработаны на основе характеристик недорогих микроэлектромеханических датчиков, используемых на борту. Алгоритмы синтеза данных ранее уже были рассмотренные и включают модифицированный фильтр Калмана или, в некоторых случаях, комплиментарный фильтр по схеме компенсации, но здесь подробно не рассматриваются. Матрица направляющих косинусов для алгоритмов исчисления пути инерциальной навигации найдена методом Пуассона.

Результаты. Разработанные модели были реализованы и смоделированы в среде MATLAB + Simulink. Начальные параметры (погрешности первичных датчиков информации и условия полета) при моделировании были разнообразными: средние, высокие и низкие широты; направление полета (вдоль и против меридиана, по и против направления вращения Земли).

Выводы. Разработанные модели и их испытания были сравнены с фактическими результатами тестирование бесплатформенной курсовертикали СБКВ-П2а и подтвердили свою обоснованность. Это позволяет рекомендовать их для использования при проектировании инерциальной навигационной системы беспилотного летательного аппарата, а также для экспериментального изучения инновационных алгоритмов синтеза обработки данных для интегрированной спутниковой и инерциальной навигационной системы.

КЛЮЧЕВЫЕ СЛОВА: бесплатформенная инерциальная навигационная система, спутниковая навигационная система, бесплатформенная курсовертикаль, счисление пути, комплексирование информации.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Goshen-Meskin D. Unified approach to inertial navigation system error modeling / D. Goshen-Meskin, I. Y. Bar-Itzhack // Journal of Guidance, Control, and Dynamics. – 1992. – Vol. 15, № 3. – P. 648–653.
2. Wu Y. Strapdown inertial navigation using dual quaternion algebra: error analysis / Y. Wu // IEEE Transactions on Aerospace and Electronic Systems. – 2006. – Vol. 42, № 1. – P. 259–266.
3. Golovan A. A., On GPS/GLONASS/INS tight integration for gimbal and strapdown systems of different accuracy / A. A. Golovan, O. V. Demidov, N. B. Vavilova // IFAC Proceedings Volumes. – 2010. – Vol. 43, № 15. – P. 505–509.
4. Filyashkin M. K. Method of measuring of angular orientation parameters in micromechanical inertial-satellite navigation systems / M. K. Filyashkin // Electronics and control systems. – 2014. – № 4. – P. 18–24.
5. Filyashkin M. K., Mukhina M. P. Data fusion schemes in aided navigation systems / M. K. Filyashkin, M. P. Mukhina // Electronics and control systems. – 2013. – № 4. – P. 11–18.
6. Quinchia A. A comparison between different error modeling of MEMS applied to GPS/INS integrated systems // Sensors. – 2013. – Vol. 13, No. 8. – P. 9549–9588.
7. Zhang X. Allan variance analysis on error characters of MEMS inertial sensors for an FPGA-based GPS/INS system //Proceedings of the International Symposium on GPS/GNNS. – 2008. – P. 127–133.
8. George M. Tightly coupled INS/GPS with bias estimation for UAV applications / M. George, S. Sukkarieh // Proceedings of Australiasian Conference on Robotics and Automation (ACRA). – 2005.
9. Mackison D. L. Review of strapdown inertial navigation technology / D. L. Mackison // Journal of Guidance, Control, and Dynamics. – 1998. – Vol. 21, № 6. – P. 1018–1018.
10. Shaeffer D. K. MEMS inertial sensors: A tutorial overview / D. K. Shaeffer // IEEE Communications Magazine. – 2013. – Vol. 51, № 4. – P. 100–109.
11. Inertial-satellite navigation systems / M. K. Filyashkin, V. O. Rogozhyn, A. V. Skrypets, T. I. Lukinova. – Kyiv, NAU, 2008. – 310 p.
12. Bin W. Study on adaptive GPS/INS integrated navigation system / W. Bin // Proceedings of the 2003 IEEE International Conference on Intelligent Transportation Systems. – IEEE, 2003. – Vol. 2. – P. 1016–1021.

DOI 10.15588/1607-3274-2019-4-15

УДК 004.932

МЕТОД ПОКРАЩЕННЯ ВИДИМОСТІ НА ЗАТУМАНЕНИХ ЦИФРОВИХ ЗОБРАЖЕННЯХ ТА ЙОГО РЕАЛІЗАЦІЯ У КОМП'ЮТЕРНІЙ СИСТЕМІ ОБРОБКИ ЗОБРАЖЕНЬ

Сердюк М. Є. – канд. техн. наук, доцент, доцент кафедри комп'ютерних технологій Дніпровського національного університету імені Олеся Гончара, м. Дніпро, Україна.

Беркут В. Г. – магістр з прикладної математики, випускник факультету прикладної математики Дніпровського національного університету імені Олеся Гончара, м. Дніпро, Україна.

Сірик С. Ф. – асистент кафедри комп'ютерних технологій Дніпровського національного університету імені Олеся Гончара, м. Дніпро, Україна

АНОТАЦІЯ

Актуальність. Присутність на цифрових зображеннях туману та димки може спричиняти проблеми у процесах розпізнавання, відстеження, класифікації об'єктів. Тому методи видалення туману та покращення розрізнюваності об'єктів на зображеннях, отриманих в умовах поганої видимості, є затребуваними в багатьох задачах комп'ютерного зору. У туманних погодних умовах контраст та колір зображення різко погіршуються. Видалення туману часто супроводжується появою артефактів на зображенні та спотворенням кольорів. Отже актуальним є пошук способів правильної оцінки присутності та видалення туману зі збереженням деталей та кольорів зображення та розробка відповідних методів обробки затуманених зображень.

Мета. Метою роботи є пошук ефективних підходів до розв'язання задачі видалення туману та димки з цифрових зображень та реалізація їх в комп'ютерній системі обробки цифрових зображень [1].

Методи. Основні етапи обробки зображення виконуються на каналі інтенсивності, що сприяє збереженню кольорів. Запропоновано підхід для утримання значень пікселів, які обробляються, у допустимому діапазоні, що дозволяє краще зберегти деталі зображення. Для оцінки карти пропускання використовуються частотні фільтри. В модифікованому методі оцінка щільності туману виконується з використанням нейронної мережі.

Результати. Запропоновано метод видалення туману та димки з одиночних зображень, який ефективно покращує видимість об'єктів, зберігає деталі та кольори на зображенні, а також його модифікація з іншим способом оцінки щільності туману. Представлені методи були реалізовані в комп'ютерній системі [1].

Висновки. Запропонований метод та його модифікація ефективно видаляють туман та димку з одиночних зображень, покращуючи розрізнюваність об'єктів на них. Реалізація цих методів у комп'ютерній системі обробки зображень [1] розширила функціонал системи та збільшила її можливості по підвищенню якості зображень, отриманих в умовах поганої видимості. Система може бути застосована для попередньої обробки зображень з метою запобігання помилкам в подальшій роботі алгоритмів комп'ютерного зору.

КЛЮЧОВІ СЛОВА: обробка зображень, видалення туману та димки, модель туману, покращення видимості, карта пропускання, оцінка атмосферного світла.

АБРЕВІАТУРИ

CUS – запропонований метод видалення туману;

CUSD – модифікація запропонованого методу з використанням нейронної мережі;

dB – децибел;

DCP – метод апріорного темного каналу;

DCP&CLAHE – метод темного каналу з використанням контрастно-обмеженої еквалізації гістограми та адаптивної гамма-корекції;

DFP – дискретне перетворення Фур'є;

DSP – метод видалення туману в реальному часі;

EmguCV – бібліотека комп'ютерного зору;

HSI – колірна модель: Hue – тон, Saturation – насиченість, Intencity – значення інтенсивності;

HSV – колірна модель: Hue – тон, Saturation – насиченість, Value – значення інтенсивності;

MCP – метод апріорного медіанного каналу;

OpenCV – бібліотека комп'ютерного зору;

PSNR – метрика якості, пікове відношення сигналу до шуму;

RGB – колірна модель: R – червоний канал, G – зелений, B – синій;

SSIM – метрика якості: індекс структурної схожості двох зображень;

YUV – колірна модель: Y – компонента яскравості, U та V – компоненти кольору.

НОМЕНКЛАТУРА

A – атмосферне світло;

c – колірний канал в моделі RGB;

$D(u,v)$ – відстань від точки (u, v) до початку координат частотного прямокутника;

D_0 – параметр фільтру Баттерворта;

$F(u,v)$ – результат Фур'є-перетворення в точці (u, v);

$G_н(u,v)$ – результат застосування низькочастотного фільтру в точці (u, v);

$G_в(u,v)$ – результат застосування високочастотного фільтру в точці (u, v);

$H_н(u,v)$ – фільтр низьких частот;

$H_в(u,v)$ – фільтр високих частот;

i – уявна одиниця, $i = \sqrt{-1}$;

DOI 10.15588/1607-3274-2019-4-16

I – вихідне зображення з туманом або димкою;

$I^c(x)$ – інтенсивність колірного каналу c у пікселі x вихідного зображення;

$I^Y(x)$ – значення інтенсивності (Y-складової колірної моделі YUV) у пікселі x вихідного зображення;

$I^в(x)$ – інтенсивність зображення в пікселі x після високочастотної фільтрації;

$I^н(x)$ – інтенсивність зображення в пікселі x після низькочастотної фільтрації;

$\hat{I}(x)$ – інтенсивність зображення в пікселі x після фільтрації;

J – відновлене зображення з покращеною видимістю;

$J^c(x)$ – інтенсивність колірного каналу c у пікселі x відновленого зображення;

$m \times n$ – розмір матриці вихідного зображення;

$M \times N$ – розмір збільшеної матриці зображення;

p – порядок фільтру Баттерворта;

t – карта пропускання;

$t_{\min}$ – мінімальне значення карти пропускання;

$t_{\max}$ – максимальне значення карти пропускання;

$\hat{t}(x)$ – карта пропускання, перерахована на діапазон [0; 255];

t_0 – обмеження карти пропускання знизу;

th – пороговий коефіцієнт для покращення кольорів та контрасту;

(u, v) – координати у частотній області;

V – компонента яскравості вихідного зображення в колірній моделі HSV;

$\hat{V}$ – перерахована компонента яскравості обробленого зображення в колірній моделі HSV;

x – піксель зображення.

ВСТУП

Несприятливі погодні умови, такі як туман, димка, пил, погіршують якість зображень, отриманих поза приміщеннями. Поява артефактів на таких зображеннях призводить до небажаних проблем та помилок в роботі алгоритмів комп'ютерного зору, які використовуються в системах відеоспостереження, розпізнавання, виявлення об'єктів, сегментації зображень тощо. Тому важливим етапом в роботі практично будь-якої системи аналізу зображень або комп'ютерного зору є попередня обробка, яка відіграє ключову роль у підвищенні якості подальшого розпізнавання, аналізу та інтерпретації графічних даних. Однією із задач, яка розв'язується на цьому етапі, є поліпшення розрізнюваності об'єктів на цифрових зображеннях, отриманих в умовах недостатньої видимості, шляхом видалення туману та димки. В туманних погодних умовах контраст та колір зображення різко погіршуються. Рівень погіршення якості збільшується разом з відстанню від камери до об'єкта. Складність задачі видалення туману полягає в тому, що туман залежить від невідомої інформації про глибину сцени. Ефект туману – це функція відстані між камерою та об'єктом. Отже, видалення туману потребує оцінки карти глибини зображення. Крім того, відновлення яскравості пікселів при видаленні туману часто супроводжується спотворенням точності передачі кольорів. Тому актуальною є розробка та вдосконалення підходів до розв'язання даної задачі, які направлені на знаходження способів правильного оцінювання присутності та видалення туману зі збереженням деталей та кольорів зображення.

Об'єктом дослідження є процес покращення видимості на цифрових зображеннях, отриманих в умовах поганої видимості.

Предметом дослідження є математичні моделі та методи для видалення туману та димки з цифрових зображень.

Метою даної роботи є пошук ефективних підходів до розв'язання задачі видалення туману та димки із зображення та використання їх в комп'ютерній системі обробки цифрових зображень.

Дана робота є продовженням проекту з розробки програмного забезпечення для покращення якості цифрових зображень шляхом видалення різного роду плям природного походження на них. На першому етапі були реалізовані функції виявлення та видалення тіней [1].

1 ПОСТАНОВКА ЗАДАЧІ

Основною причиною погіршення якості зображень, що містять сцени на відкритому повітрі в умовах туманних кліматичних умов, є розсіювання більшої частини світла до моменту його досягнення камери через наявність великої кількості розсіяних частинок в повітрі (наприклад, туману, диму або частинок інших речовин). Математично цей процес виражається моделлю формування зображення, яка часто зустрічається в задачах обробки затуманених зображень [2, 3]. Через атмосферні частинки, які поглинають і розсіюють світло, тільки певний відсоток відбитого світла досягає спостерігача. Інтенсивність $I(x)$ пікселя x затуманеного зображення є результатом дії двох основних адитивних компонентів – прямого ослаблення та світла повітря. В кожному колірному каналі $c \in \{R, G, B\}$ такого зображення інтенсивність пікселя може бути представленою у вигляді:

$$I(x) = J(x) \cdot t(x) + A \cdot (1 - t(x)). \quad (1)$$

Перший доданок у правій частині формули (1) є прямим ослабленням, яке описує випромінювання сцени та його загасання в середовищі. Другий доданок – світло повітря, отримується від раніше розсіяного світла, результат його дії – зміщення кольорів.

Карта пропускання $t(x) \in [0;1]$ для кожного пікселя x вихідного зображення описує частину світла, яка не розсіюється і досягає камери. Тобто карта пропускання несе оцінку щільності туману для кожного пікселя затуманеного зображення.

DOI 10.15588/1607-3274-2019-4-16

Задача полягає у відновленні J – вільного від туману зображення – із I.

Складність задачі відновлення J визначається тим, що атмосферне світло A та карта пропускання t є також невідомими.

2 ОГЛЯД ЛІТЕРАТУРИ

Існують різні підходи до розв'язання задачі покращення видимості на зображеннях, спотворених туманом або димкою. Можна виділити дві основні групи методів обробки затуманених зображень: методи, які не використовують фізику процесу передачі світла в атмосфері, та методи, основані на фізичній моделі туману.

Методи першої групи спрямовані на поліпшення зображень шляхом відновлення контрасту. Для цього використовуються просторові фільтри, вирівнювання гістограми та інші перетворення, як покращують візуальне сприйняття зображення. В роботі [4] автор, аналізуючи множину зображень, отриманих зовні приміщень, відзначає, що контраст незатуманених зображень значно вище, ніж зображень з помутніннями, викликаними туманом та димкою, а світло навколишнього середовища, що у великій степені залежить від відстані об'єктів до спостерігача, має схильність бути розмитим. На основі таких спостережень автор пропонує метод видалення туману, який базується на максимізації локального контрасту зображень з помутніннями. Такий метод може забезпечити хороший візуальний ефект, але він не відновлює реальний контраст сцени у відповідності до моделі передачі атмосфери, тому результати можуть бути перенасиченими та неприродними.

В роботі [5] розглядається метод відновлення затуманених зображень, оснований також на підвищенні контрастності. Автори відзначають, що просте підвищення контрастності супроводжується втратою інформації, що є наслідком переповнення або недостатнього заповнення значень пікселів. Тому видалення туману пропонується здійснювати шляхом мінімізації функції вартості, яка враховує контраст і втрату інформації. Такий підхід дозволив оптимальним чином підвищити контраст та зберегти інформацію на зображенні. Крім того, було запропоновано розширення алгоритму видалення туману зі статичних зображень для роботи з відео, що поступає на вхід в режимі реального часу. Проте метод погано адаптується до зображень з різним степенем помутніння та не може ефективно видаляти щільні помутніння у відео.

У роботі [6] автори запропонували метод відновлення видимості на одному зображенні, базуючись на медіанному фільтрі для видалення туману або димки. Метод має високу швидкодію, може працювати в режимі реального часу, видаляє помутніння в значній мірі, але спричиняє появу ореолів та порушення кольорів.

У роботі [7] представлено метод видалення туману, який спирається на загальну закономірність в природних зображеннях, отриманих на відкритому повітрі, де пікселі невеликих ділянок зображення зазвичай мають одномірний розподіл в колірному просторі RGB, відомий як кольорові лінії. Автор представив локальну структурну модель для кольорових ліній в туманних сценах і використав її для відновлення сцени. Для отримання повної і збалансованої карти оцінки шуму і розсіювання була використана марковська модель випадкового поля.

В основі методу покращення розпізнаваності деталей на затуманених зображеннях, представленому в [8], лежить модифікований алгоритм Retinex з автоматичним визначенням декількох рівнів інтенсивності, використовуючи які можна освітлити або затемнити зображення. При обробці зображення, визначаються просторові області з однаковою інтенсивністю та локальним контрастом по кожному колірному каналу. Пікселі, що являються близькими до цих рівнів інтенсивності, особо обробляються для того, щоб виявити деталі, які могли бути невидимими для людського зору. Кожен ідентифікований рівень отримує свою вагу відповідно до його поширеності. Результати демонструють потужність даного підходу на широкому спектрі тестових випадків.

У [9, 10] запропоновано метод, в якому розмиття туману здійснюється за допомогою розрахунку повітряно-світлового потоку. Представлений алгоритм базується на припущенні, що зображення без помутніння добре апроксимуються декількома сотнями різних кольорів, які утворюють щільні кластери у просторі RGB. Алгоритм добре працює на широкому колі зображень, проте він приймає кожен кадр у відео як окреме зображення і повністю базується на методах розмиття зображень.

Є методи, які базуються на порівнянні декількох зображень, отриманих в різних погодних умовах [11, 12]. Такі методи заздалегідь мають отримати прийнятні зображення, що збільшує складність отримання незатуманених зображень.

Існують алгоритми видалення туману, які використовують моделі, що базуються на фізиці розсіювання світла в атмосфері. Для оцінки щільності туману чимало методів використовують явище апріорного темного каналу. Теорія апріорного темного каналу базується на статистиці зображень на відкритому повітрі, що не містять туману. Для більшості локальних областей на зображеннях, які не містять неба, часто деякі пікселі мають дуже низьку інтенсивність хоча б по одному каналу в RGB зображенні. На затуманеному зображенні інтенсивність цих темних пікселів по цьому каналу в основному визначається світлом неба. Тому темні пікселі можуть безпосередньо дати змогу точно оцінити степінь щільності туману. Так, в [2] представлено метод на основі моделі візуалізації туману, який дозволяє оцінити степінь щільності туману та відновити якісне незатуманене зображення. При цьому будується хороша карта глибини. Даний підхід правильний з фізичної точки зору і здатний обробляти віддалені об'єкти навіть на сильно затуманених зо-

DOI 10.15588/1607-3274-2019-4-16

браженнях. Метод не опирається на значні перепади щільності або затінення поверхонь у вхідному зображенні. Однак результат може містити декілька ореолів. Як і будь-який підхід, що використовує строге припущення, цей підхід також має свої власні обмеження. Темний канал може бути непридатним, якщо об'єкт сцени за своєю суттю аналогічний світлу атмосфери на великій локальній області (наприклад, автомобільні фари, засніжена поверхня тощо), і на об'єкти не падають тіні.

В [2] метод темного каналу комбінується з методом м'якого матування для уточнення карти передачі, що викликає велике обчислювальне навантаження. В [13] пропонується метод керуючого фільтра для зменшення обчислювальних витрат. Керований фільтр може використовуватися як оператор розмиття, який зберігає риси границь на зображенні і може краще використовувати структури в оброблюваному зображенні. У [14] запропоновано вдосконалений підхід для видалення туману з одного зображення шляхом комбінування темного каналу та керованої фільтрації зображення. Запропоновано ефективну схему адаптації радіуса локальних областей, що використовується при отриманні темного каналу, та радіуса керованого фільтра. Оброблені зображення мають задовільну якість, однак метод видає помилкові результати у випадку з зображеннями, що мають різкі зміни в глибіні сцени.

У [15] безтуманне зображення отримується через оцінку шарів туману на основі медіанної фільтрації із застосуванням методу темного каналу. Результатом є покращений розмитий шар разом з приглушеними текстурами та збереженими переходами глибини на зображенні. Алгоритм є простим та ефективним способом для «очищення» зображення та покращення контрасту.

Видалення туману з використанням темного каналу часто супроводжується спотворенням кольорів в області неба та яскравих регіонів. Для вирішення цієї проблеми в [16] запропоновано покращений метод, який базується на інверсному зображенні та темному каналі. Інверсне зображення застосовується для оцінки нової карти передачі, яка використовується для зміни вихідної карти, щоб уникнути спотворення кольорів. Потім карта уточнюється з використанням керуючого фільтра.

У роботі [17] розглядається ефективний метод видалення помутніння з одного вхідного зображення, який будує карту передачі шляхом видалення дрібних деталей із мінімального з каналів RGB за допомогою низькочастотного фільтру. Далі карта уточнюється з використанням каналу інтенсивності колірного простору HSI та локального контрасту. На основі моделі розсіювання світла в атмосфері генерується якісне зображення без димки. Проте на зображеннях з щільним туманом помутніння видаляється не повністю.

Аналіз існуючих підходів, які використовують фізику процесу утворення туману, дозволяє виділити основні етапи розв'язання задачі:

1) оцінка карти пропускання;
2) оцінка атмосферного світла;
3) видалення туману.

В деяких підходах для покращення результатів використовується етап попередньої та (або) післяобробки. В цих випадках якість результатів підвищується, але зменшується швидкодія.

3 МАТЕРІАЛИ ТА МЕТОДИ

В даній роботі пропонується метод CUS видалення туману зі збереженням деталей зображення з урахуванням фізичної моделі туману. Затуманене зображення I описується формулою (1). Коли карта пропускання близька до нуля, то перший доданок у формулі (1) теж буде близьким до нуля. Оскільки відновлена інтенсивність сцени J схильна до шуму, то карту пропускання обмежують нижньою границею t_0 та зберігають деяку кількість туману в дуже щільних областях туману, як пропонується у [2]. Зазвичай $t_0 = 0{,}1$. З урахуванням цього з формули (1) випливає, що

$$J(x) = \frac{I(x) - A}{\max(t_0, t(x))} + A. \qquad (2)$$

Для того, щоб відновити шукане зображення J, необхідно отримати оцінку карти пропускання t та оцінку атмосферного світла A. Зауважимо, що A – це константа, яка обчислюється глобально для зображення I.

На практиці застосування формули (2) для видалення туману часто призводить до небажаних артефактів, які з'являються у результаті роботи з неточною картою пропускання. Під неточною картою пропускання розуміється зображення, отримане на основі вихідного зображення, емпіричні значення якого повністю не відповідають теоретичним, тобто не враховується емпірична природа $t(x)$. Наприклад, при розрахунках можна отримати значення інтенсивності поза межами допустимого діапазону [0; 255]. Виникає питання, як скорегувати отримане значення, щоб не спотворити кольорі та саме вихідне зображення. В даній роботі пропонується підхід, який дозволяє плавно зменшити інтенсивність затуманених пікселів та утримати значення зображення у допустимому діапазоні, що дозволяє краще зберегти деталі зображення.

Метод CUS передбачає виконання трьох етапів, визначених вище.

Першим етапом є побудування карти пропускання. Для реалізації оцінки карти пропускання в даній роботі використовуються ідеї із [18]. Процедура побудування карти пропускання складається з таких кроків:

1. У вхідному зображенні виділяється складова інтенсивності за формулою

$$I^Y = 0{,}299R + 0{,}587G + 0{,}114B$$

як Y-складова колірної моделі YUV [19]. Саме на основі аналізу цієї складової будується карта пропускання. Результатом є матриця інтенсивностей $[I^Y_{jk}]$, $j = 1, 2, ..., m$, $k = 1, 2, ..., n$.

DOI 10.15588/1607-3274-2019-4-16

2. Матриця інтенсивностей збільшується за розміром у два рази з використанням лінійної інтерполяції. Новий розмір матриці $M \times N$, де $M = 2m$, $N = 2n$. Парність розмірів матриці необхідна для подальшого застосування DFT та спрощення комп'ютерної реалізації. Всі елементи матриці множаться на $(-1)^{j+k}$ для того, щоб Фур'є-перетворення було центрованим, тобто початок координат (0, 0) знаходився у центрі частотного прямокутника.

3. До збільшеної матриці інтенсивностей застосовується пряме DFT [20]:

$$F(u,v) = \frac{1}{MN} \sum_{j=0}^{M-1} \sum_{k=0}^{N-1} I_{jk}^{Y} e^{-i2\pi(uj/M + vk/N)},$$

де $j = 0,1,...,M-1$, $k = 0,1,...,N-1$, тобто здійснюється перехід до частотної області. Відомо, що частоти у Фур'є-перетворенні зв'язані з варіацією інтенсивності на зображенні. Частотна складова, що змінюється найповільніше (u=0, v=0), співпадає із середньою інтенсивністю зображення. Низькі частоти, що відповідають точкам поблизу початку координат Фур'є-перетворення, визначають компоненти зображення, що змінюються повільно. По мірі віддалення від початку координат більш високі частоти починають відповідати все більш швидким змінам інтенсивності, що уявляють собою межі об'єктів та інші деталі зображення, які характеризуються різкими змінами яскравості, наприклад шум на зображенні.

4. Застосовується фільтр низьких частот Баттерворта порядку p з частотою зрізу на відстані D_0 від початку координат [20]:

$$H_н(u,v) = \frac{1}{1 + [D(u,v)/D_0]^{2p}},$$

в якому відстань від точки (u, v) до початку координат визначається за формулою

$$D(u,v) = [(u-m)^2 + (v-n)^2]^{1/2}.$$

Зауважимо, що в комп'ютерній реалізації даного етапу було використано такі значення параметрів фільтру Баттерворта: p=1, D_0=30.

Результат низькочастотної фільтрації отримується таким чином:

$$G_н(u,v) = H_н(u,v) \cdot F(u,v).$$

Множення матриць $H_н$ і F здійснюється поелементно. Відзначимо, що низькочастотна фільтрація пригнічує високочастотні складові, зокрема шум, та створює згладжене зображення.

5. Застосовується зворотне DFT [20]:

$$I_{jk}^{н} = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} G_н(u,v) e^{i2\pi(uj/M + vk/N)},$$

результатом якого є матриця $[I_{jk}^{н}]$ розміром $M \times N$. Виділяється дійсна частина результату, всі елементи матриці множаться на $(-1)^{j+k}$, щоб компенсувати ефект від множення зображення на ту ж саму величину. Здійснюється повернення до вихідних розмірів матриці, тобто її розміри зменшуються вдвічі.

6. За аналогією до матриці $[I_{jk}^{Y}]$ застосовується фільтр високих частот Баттерворта порядку p з частотою зрізу на відстані D_0 від початку координат [20]:

$$H_в(u,v) = \frac{1}{1 + [D_0/D(u,v)]^{2p}}.$$

Результатом високочастотної фільтрації є матриця:

$$G_в(u,v) = H_в(u,v) \cdot F(u,v).$$

Високочастотна фільтрація пригнічує низькочастотні компоненти та генерує зображення з покращеними краями.

7. До отриманої матриці застосовується зворотне DFT:

$$I_{jk}^{в} = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} G_в(u,v) e^{i2\pi(uj/M + vk/N)},$$

результатом якого є матриця $[I_{jk}^{в}]$ розміром $M \times N$. Аналогічно виділяється дійсна частина результату, всі елементи матриці множаться на $(-1)^{j+k}$, розмір матриці зменшується вдвічі.

8. Результуюча матриця інтенсивностей розраховується як сума двох отриманих матриць:

$$\hat{I}(x) = I^{н}(x) + I^{в}(x).$$

9. Далі із значень матриці $\hat{I}$ отримують карту пропускання

$$t(x) = 1 - \hat{I}(x)/255.$$

Зазначимо, що для візуалізації карти пропускання в комп'ютерній системі було здійснено масштабування $t(x)$ у діапазон [0; 255] з розтягуванням значень на весь відрізок:

$$\hat{t}(x) = \frac{t(x) - t_{\min}}{t_{\max} - t_{\min}} \cdot 255.$$

На наступному етапі оцінюється атмосферне світло. Для цього вхідне зображення спочатку конвертується в колірний простір HSV, в якому компонента V несе інформацію про яскравість пікселя. Метод перетворення зображення із колірної моделі RGB в HSV та навпаки описано, наприклад, в [19]. Далі відбираються 0,1% найяскравіших пікселів в $\hat{I}(x)$. Ці пікселі відповідають найщільнішим областям туману. З отриманих пікселів відбирається один, який відпові-

DOI 10.15588/1607-3274-2019-4-16

дає пікселю на вихідному зображенні з найбільшою яскравістю (канал *V*). Його значення обирається в якості значення атмосферного світла *A*.

Наступним етапом є видалення туману. Для цього пропонується підхід, який дозволяє уникнути виходу значень пікселів за межі допустимого діапазону, що може спричиняти появу артефактів та зміщення кольорів. Будемо застосовувати процедуру видалення туману лише для компоненти яскравості *V* вхідного зображення, а кольори будемо вирівнювати на останньому етапі. Лише для каналу *V* застосуємо формулу, яка побудована емпіричним шляхом з урахуванням (2):

$$\hat{V} = V + (V - A) \cdot (1 - \max(t_0, t)). \qquad (3)$$

Пояснимо сенс другого доданка. Різниця між яскравістю пікселя та атмосферним світлом (*V*–*A*) майже завжди від'ємна. Множник (1–max(t_0 ,*t*)), який по суті є інверсією карти пропускання, дозволяє врахувати щільність туману та додавати до *V* лише частину значення (*V*–*A*). Тобто корегування значення *V* на величину другого доданку формули (3) призводить до вирівнювання яскравості пікселя таким чином: для областей з більш щільним туманом інтенсивність зменшується сильніше, для менш затуменених – слабкіше. Отже, значення (*V*–*A*) можна розглядати як адаптивну величину, на яку слід відкоригувати *V* з урахуванням щільності туману в конкретному пікселі. Якщо результуюче значення яскравості $\hat{V}$ виходить за межі інтервалу [0; 255], другий доданок у формулі (3) зменшується на 25%, поки не буде отримано коректне значення. Таким чином досягається плавне зменшення інтенсивності *V* пікселя у просторі HSV та не допускається вихід цього значення за межі діапазону.

Далі здійснюється повернення до колірного простору RGB. Метод конвертації можна знайти у [19]. Для отримання результуючого зображення виконується ще одне перетворення, спрямоване на покращення кольорів та контрасту, за правилом [21]:

$$J^c = \left(\left(\left(\frac{I^c}{255} - 0{,}5 \right) \left(\frac{100 + th}{100} \right)^2 \right) + 0{,}5 \right) \cdot 255.$$

Поріг *th* є таким, що налаштовується, за замовчуванням *th* = 10.

На основі описаного методу пропонується ще одна модифікація для видалення туману CUSD, яка дозволяє отримати якісні результуючі зображення. В ході аналізу різних методів видалення туману було помічено, що ключову роль в цьому процесі відіграє оцінка товщини туману (карта пропускання), а також післяобробка, яка здатна значно покращити результат. Оскільки, як слідує з моделі формування туману, туман стає щільнішим зі збільшенням відстані від об'єкта до камери, то можна припустити, що в якості оцінки товщини туману можна використовувати карту глибини сцени. Для оцінки глибини сцени на одному зображенні (без залучення додаткових зображень) в даній роботі використовується підхід на основі машинного навчання, описаний в [22]. Автори запропонували нейронну мережу, розроблену на мові Python, з використанням бібліотеки Tensorflow 1.0 для машинного навчання, яка здатна оцінювати глибину сцени з одного зображення. Код для даного методу знаходиться у відкритому доступі на GitHub під ліцензією «UCLB ACP-A», що дозволяє безкоштовне використання даного програмного продукту в некомерційних цілях. Отже, в методі, що розглядається, оцінка глибини сцені здійснюється за допомогою нейронної мережі. Для подальшого видалення туману застосовуються кроки методу CUS, розглянуті вище.

4 ЕКСПЕРИМЕНТИ

Описані вище методи реалізовані в комп'ютерній системі [1] як ще одна група функцій обробки зображень на додаток до виявлення та видалення тіней (різні методи), кластеризації, обробки границь. Програма розроблена на мові C# з використанням бібліотеки комп'ютерного зору EmguCV, яка є кросплатформенною .Net огорткою бібліотеки OpenCV.

Крім запропонованого методу CUS та його модифікації CUSD з використанням нейронної мережі, в комп'ютерній системі були додатково реалізовані такі методи видалення туману:

1) метод апріорного темного каналу (DCP) на основі ідей, викладених у [2];

2) метод апріорного медіанного каналу (MCP), представленому у [3];

3) метод темного каналу з використанням контрастно-обмеженої еквалізації гістограми та адаптивної гамма-корекції (DCP&CLAHE), що описано у [23];

4) видалення туману (DSP), орієнтоване на виконання у реальному часі на цифрових сигнальних процесорах, на основі ідей, викладених у [24].

Реалізація цих методів дозволила провести порівняльний аналіз результатів обробки зображень цими методами з результатами, отриманими запропонованим методом та його модифікацією. Крім того, реалізація багатьох методів розширила функціонал системи.

Програма має віконний інтерфейс та містить декілька меню для вибору способу та методу обробки зображення. Графічні засоби керування програмою згуртовані в панелі відповідно до свого призначення. Основне вікно має три області для відображення вихідного, проміжного та результуючого зображень. Програма надає можливість виводу додаткових вікон з проміжними зображеннями, які отримуються в процесі роботи того чи іншого методу. Таким чином можна побачити, які кроки обробки проходить зображення перед отриманням остаточного результату. Передбачені також додаткові методи обробки, які можуть покращити результати основної обробки.

Порівняння результатів роботи різних методів видалення туману між собою здійснювалось як візуально, так і за допомогою формальних метрик якості. Для розрахунку метрик використовувалась база зображень FRIDA [25], яка була створена для перевірки роботи

DOI 10.15588/1607-3274-2019-4-16

алгоритмів видалення туману та відновлення контрасту. База даних містить набір оригінальних зображень без туману, карту глибини та чотири затуманених зображення з різними видами туману для кожного оригіналу. Отже, для розрахунку формальних метрик якості в роботі використовувались тестові зображення без туману та результати видалення туману різними методами.

5 РЕЗУЛЬТАТИ

Представлені в роботі методи були протестовані на низці зображень. Результат обробки методом CUS із збереженням деталей зображення представлений на рис. 1.

а б в

Рисунок 1 – Приклад обробки зображення методом CUS: а – вихідне зображення, б – карта пропускання, в – результуюче зображення

Результат видалення туману методом CUSD представлений на рис. 2.

На рис. 3 наведено результати видалення туману на трьох тестових зображеннях різними методами.

Для порівняння зображень, отриманих в результаті обробки різними методами видалення туману, з оригінальними зображеннями без туману були використані формальні метрики якості PSNR, SSIM та ентропія Шеннона.

а б в

Рисунок 2 – Приклад обробки зображення методом CUSD: а – вихідне зображення, б – карта пропускання, отримана за допомогою нейронної мережі, в – результуюче зображення

Метрика PSNR – пікове відношення сигналу до шуму, характеризує співвідношення між максимумом можливого значення сигналу та потужністю шуму, що спотворює значення сигналу. Більші значення PSNR відповідають меншим відмінностям зображень, що порівнюються.

Метрика SSIM – індекс структурної схожості двох зображень. Значення SSIM знаходиться в межах від -1 до +1. Значення +1 досягається при повному співпадінні зображень.

Ентропія – це міра невизначеності випадкової величини. Чим більший випадковий характер інтенсивності пікселів, тим більше ентропія у зображення. Низька ентропія означає низьку контрастність зображення. Ентропія розраховується для результуючого зображення, щоб оцінити рівень контрасту для різних методів.

У таблиці 1 наведено результати розрахунків формальних метрик якості для зображень, оброблених різними методами. В таблиці представлені середні значення по набору протестованих зображень.

Таблиця 1 – Результати розрахунків метрик якості

Метод видалення туману	PSNR	SSIM	Ентропія Шеннона
DCP	38,92	0,77	6,65
MCP	38,59	0,74	6,52
DCP&CLAHE	39,17	0,70	6,90
DSP	38,08	0,77	6,67
CUS	36,67	0,76	6,45
CUSD	37,04	0,73	6,52

6 ОБГОВОРЕННЯ

В результаті тестування запропонованих методів на низці зображень з туманом різного характеру було виявлено, що найкраще ці методи справляються з видаленням димки та негустого туману. При цьому результуючі зображення мають досить високу якість, контраст, окремі деталі добре розрізняються. Але при застосуванні цих методів до сильно затуманених зображень часто спостерігаються перепади контрасту та деякі зміщення кольорів сцени.

Візуальне порівняння якості результатів видалення туману запропонованими методами з результатами роботи інших методів демонструє, що найкраще видимість поліпшується при застосуванні методів CUS та DCP&CLAHE. Результуючі зображення часто виходять дуже різкими, з підвищеним контрастом, що дозволяє краще розрізняти об’єкти сцени. Непогані за візуальною якістю результати дає і метод CUSD. Але треба відзначити, що цей метод не підходить для програмних додатків, що працюють в реальному часі, оскільки час роботи нейронної мережі порівняно високий.

Порівняння формальних показників якості розглянутих методів дає неоднозначні результати. Так, за метрикою PSNR запропоновані методи CUS та CUSD демонструють дещо нижчі результати, ніж інші розглянуті методи. Але значення метрики перевищує 30 dB, що є хорошим показником. За метрикою SSIM метод CUS демонструє найкращі результати поряд з методами DCP та DSP. Дещо нижчий показник дає метод CUSD. Варто відзначити, що метрика SSIM більше відповідає візуальному сприйняттю зображення людиною, ніж PSNR. Саме в термінах метрики SSIM запропонований метод CUS показав один з найкращих результатів обробки затуманених зображень.

Якщо порівняти показники ентропії, то методи CUS та CUSD отримали менші у порівнянні з іншими методами значення. Це пояснюється тим, що запропоновані методи виконують «м’яку» обробку зображень зі збереженням деталей на ньому, отже показник контрастності (ентропія) виходить меншим у порівнянні з іншими методами.

DOI 10.15588/1607-3274-2019-4-16

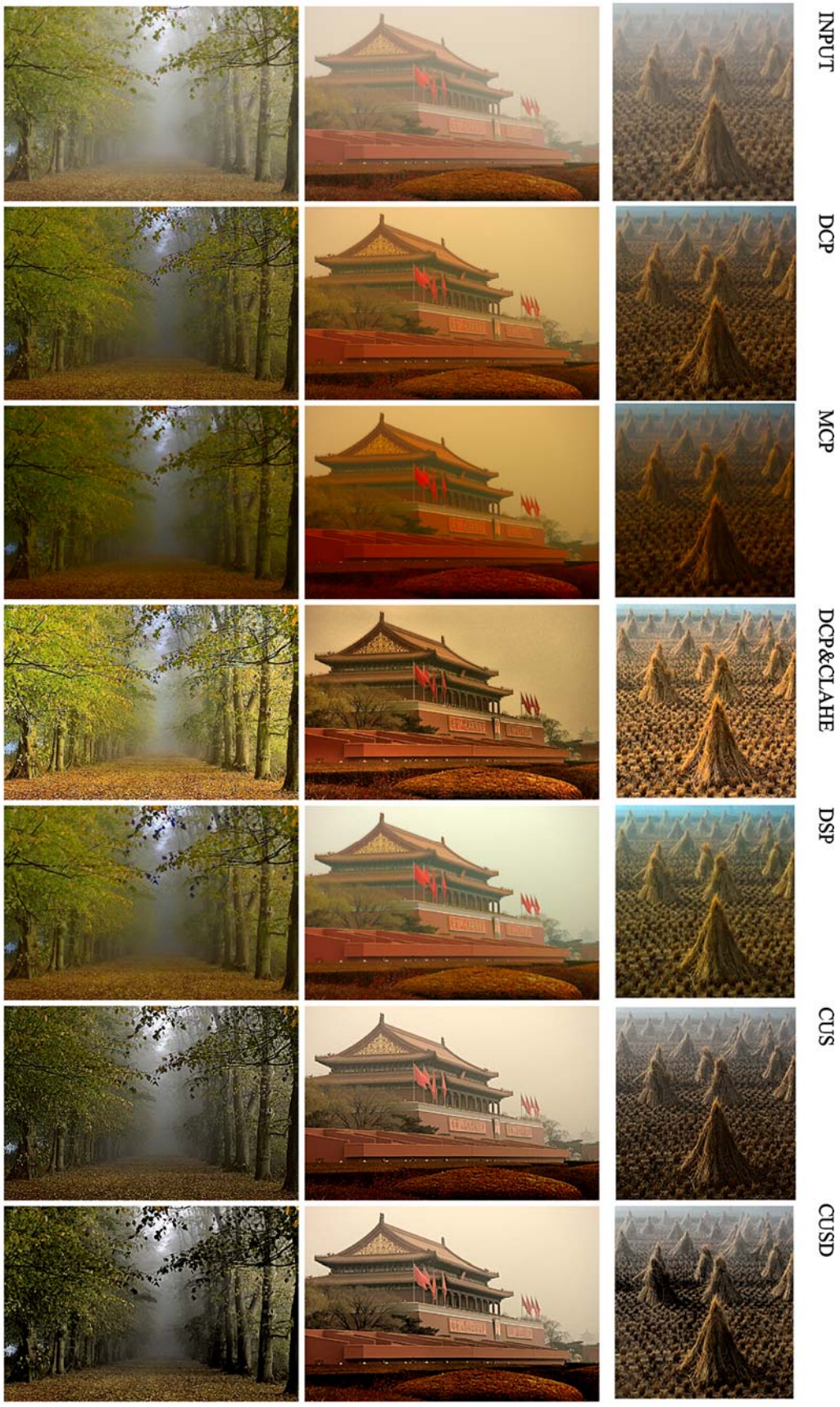


Рисунок 3 – Результати видалення туману різними методами

DOI 10.15588/1607-3274-2019-4-16

Відзначимо, що для об'єктивності аналізу запропонованого методу для результуючих зображень не застосовувались додаткові процедури їх післяобробки. Використання процедур попередньої та післяобробки дозволить ще підвищити якість оброблених зображень.

ВИСНОВКИ

Алгоритми видалення туману із цифрових зображень є затребуваними в багатьох задачах комп'ютерного зору. Аналіз існуючих методів показав, що немає єдиного універсального підходу для покращення видимості, який би однаково добре працював на всіх типах затуманених зображень. В даній роботі запропоновано метод видалення туману з покращенням збереження деталей та кольорів та його модифікація з використанням нейронної мережі.

Запропоновані методи разом з чотирма іншими розглянутими методами були додані в комп'ютерну систему обробки зображень з метою видалення різних плям та спотворень природного походження [1], що значно розширило функціонал системи. В залежності від типу зображення, спотвореного туманом, можна обирати метод, який дасть найкращі результати.

Наукова новизна полягає в розробці методу видалення туману та димки, який зберігає деталі зображення та не спотворює кольори. Запропоновано підхід, який дозволяє плавно зменшити інтенсивність затуманених пікселів та утримати значення зображення у допустимому діапазоні, що сприяє кращому збереженню деталей зображення. Основні етапи обробки виконуються на каналі інтенсивності, що сприяє збереженню кольорів. Запропоновано модифікацію методу, в якій оцінка щільності туману виконується з використанням нейронної мережі.

Практичне значення роботи полягає в тому, що запропонований метод дозволяє отримати якісні зображення після видалення з них туману та димки, зі збереженням деталей та кольорів на зображенні, тому його можна використовувати для попередньої обробки зображень в різних задачах комп'ютерного зору, а також в естетичних цілях, наприклад, у споживчій фотографії.

ПОДЯКИ

Роботу виконано в рамках науково-дослідної роботи кафедри комп'ютерних технологій Дніпровського національного університету імені Олеся Гончара «Дослідження математичних моделей фізичних процесів методами ідентифікації та рекурентного аналізу із застосуванням інформаційних технологій» (шифр 0113U004203, період дії теми: 01.01.2016 – 31.12.2018, шифр 0119U101053, 01.01.2019 – 31.12.2021).

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Сердюк М. Є. Комп'ютерна система локалізації та видалення тіней у цифрових зображеннях / М. Є. Сердюк, В. Г. Беркут // Радіоелектроніка, інформатика, управління. – 2017. – №2(41). – С. 127–133. DOI: 10.15588/1607-3274-2017-2-14
2. He K. Single image haze removal using dark channel prior / K. He, J. Sun, X. Tang // IEEE Trans. Pattern Anal. Mach. Intell. – Dec. 2011. – Vol. 33, No. 12. – P. 2341–2353. DOI: 10.1109/TPAMI.2010.168
3. Kang Hyun-Jin. Fast Removal of Single Image using Pixel-based Median Channel Prior / Hyun-Jin Kang, Young-Hyung Kim, Yong Hwan Lee // I. J. Advanced Science and Technology Letters. – 2015. – Vol. 98. – P. 124–127. DOI: 10.14257/astl.2015.98.31
4. Tan R. T. Visibility in bad weather from a single image / R. T. Tan // Proceedings.of the 26th IEEE Conference on Computer Vision and Pattern Recognition (CVPR '08). – Anchorage, Alaska. – 2008. – P. 1–8.
5. Kim J.-H. Optimized contrast enhancement for real-time image and video dehazing / J.-H. Kim, W.-D. Jang, J.-Y. Sim, C.-S. Kim // Journal of Visual Communication and Image Representation. – 2013. – Vol. 24, No. 3. – P. 410–425. DOI: 10.1016/j.jvcir.2013.02.004
6. Tarel J. P. Fast Visibility Restoration from a Single Color or Gray Level Image / J. P. Tarel, N. Hautiere // Proceedings of the 12th IEEE International Conference on Computer Vision. Kyoto, Japan. – 2009. – P. 2201–2208. DOI: 10.1109/ICCV.2009.5459251
7. Fattal R. Dehazing Using Color-Lines / Raanan Fattal // ACM Transactions on Graphics. – 2014. – Vol. 34, No. 1. – P. 13. DOI: 10.1145/2651362
8. Livingston M. A. Image Processing for Human Understanding in Low-visibility / Mark A. Livingston, Caelan R. Garrett, Zhuming Ai // Information Technology Division, Naval Research Laboratory. – 2011. – P. 1–9.
9. Berman D. Non-Local Image Dehazing / D. Berman, T. Treibitz, S. Avidan // Proceedings of the CVPR Computer Vision and Pattern Recognition; Las Vegas, NV, USA. – 2016. – P. 1674–1682. DOI: 10.1109/CVPR.2016.185
10. Berman D. Air-light Estimation using Haze-Lines / D. Berman, T. Treibitz, S. Avidan // Proceedings of the IEEE 13th International Conference on Intelligent Computer Communication and Processing; Stanford, CA, USA. – 2017. – P. 5178–5191. DOI: 10.1109/ICCPHOT.2017.7951489
11. Narasimhan S. G. Removing weather effects from monochrome images / S. G. Narasimhan, S. K. Nayar // Proceedings of the CVPR Computer Vision and Pattern Recognition; Kauai, HI, USA. – 2001. – P. 186–193. DOI: 10.1109/CVPR.2001.990956
12. Chen G. A Novel Physics-based Method for Restoration of Foggy Day Images / G. Chen, T. Wang, H. J. Zhou // Journal of Image and Graphics. – 2008. – Vol. 13, No. 5. – P. 888–893. DOI: 10.1109/SNPD.2007.350
13. He K. M. Guided image filtering / K. M. He, J. Sun, X. O. Tang // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2010. – Vol. 35, No. 6. – P. 1397–1409. DOI: 10.1109/TPAMI.2012.213
14. Pang J. Improved single image dehazing using guided filter / J. Pang, O. C. Au, Z. Guo // In Proc. APSIPA ASC, Xi'an, China. – 2011. – P. 1–4.
15. Zhang Y.-Q. Visibility enhancement using an image filtering approach / Y.-Q. Zhang, Y. Ding, J.-S. Xiao, J. Liu, Z. Guo // EURASIP Journal on Advances in Signal Processing. – Vol. 2012, Article 220. – 2012. – P. 1–6. DOI: 10.1186/1687-6180-2012-220
16. Shi L. Image Haze Removal Using Dark Channel Prior and Inverse Image / Lei Shi, Xiao Cui, Li Yang, Zhigang Gai, Shibo Chu, Jing Shi // International Conference on Measurement Instrumentation and Electronics 2016 (ICMIE 2016), Munich, Germany. – 2016. – P. 89–93. DOI: 10.1051/matecconf/20167503008
17. Fast Single Image Haze Removal Method based on Atmospheric Scattering Model / [D. Huang, W. Wang, J. Lu, K. Chen]

DOI 10.15588/1607-3274-2019-4-16

// IFAC-PapersOnLine. – 2018. – Vol. 51, Issue. 17. – P. 211–216. DOI: 10.1016/j.ifacol.2018.08.144
18. Kumari A. Real Time Visibility Enhancement for Single Image Haze Removal / A. Kumari, S. K. Sahoo // Proc. Int. Conf. on Information Processing (IMCIP). – 2015. – P. 501–507. DOI: 10.1016/j.procs.2015.06.057
19. Understanding Color Models: A Review / [Noor A. Ibraheem, Mokhtar M. Hasan, Rafiqul Z. Khan, Pramod K. Mishra] // ARPN Journal of Science and Technology, ISSN 2225-7217. – 2012. – Vol. 2, No. 3. – P. 265–275.
20. Гонсалес Р. Цифровая обработка изображений : пер. с англ. / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2005. – 1072 с.
21. Esterhuizen D. C# How to: Image Contrast / D. Esterhuizen [Electronic resource]. – Access mode: https://softwarebydefault.com/2013/04/20/image-contrast/
22. Godard C. Unsupervised Monocular Depth Estimation with Left-Right Consistency / C. Godard, O. M. Aodha, G. Brostow [Electronic resource]. – Access mode: http://zpascal.net/cvpr2017/Godard_Unsupervised_Monocular_Depth_CVPR_2017_paper.pdf.
23. Arora T. Evaluation of a New Integrated Fog Removal Algorithm IDCP with CLAHE / Tarun A. Arora, Gurpadam B. Singh, Mandeep C. Kaur // International Journal of Soft Computing and Artificial Intelligence, ISSN: 2321-404X. – 2014. – Vol. 2, Issue 1. – P. 12–18.
24. Real Time Image Haze Removal on Multi-core DSP/ [L. Bai, Y. Wu, J. Xie, P. Wen] // 2014 Asia-Pacific International Symposium on Aerospace Technology, APISAT2014. – 2014. – P. 244–252. DOI: 10.1016/j.proeng.2014.12.532
25. Improved Visibility of Road Scene Images under Heterogeneous Fog / [J.-P. Tarel, N. Hautière, A. Cord et al.] // Proceedings of IEEE Intelligent Vehicles Symposium (IV'10), San Diego, CA, USA, June 21–24, 2010. DOI:10.1109/IVS.2010.5548128

Стаття надійшла до редакції 13.06.2019.
Після доробки 18.10.2019.

УДК 004.932

МЕТОД УЛУЧШЕНИЯ ВИДИМОСТИ НА ЗАТУМАНЕННЫХ ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ И ЕГО РЕАЛИЗАЦИЯ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Сердюк М. Е. – канд. техн. наук, доцент кафедры компьютерных технологий Днепровского национального университета имени Олеся Гончара, г. Днепр, Украина.

Беркут В. Г. – магистр по прикладной математике, выпускник факультета прикладной математики Днепровского национального университета имени Олеся Гончара, г. Днепр, Украина.

Сирик С. Ф. – ассистент кафедры компьютерных технологий Днепровского национального университета имени Олеся Гончара, г. Днепр, Украина.

АННОТАЦИЯ

Актуальность. Присутствие на цифровых изображениях тумана и дымки может вызывать проблемы в процессах распознавания, отслеживания, классификации объектов. Поэтому методы удаления тумана и улучшения различимости объектов на изображениях, полученных в условиях плохой видимости, востребованы во многих задачах компьютерного зрения. В туманных погодных условиях контраст и цвет изображения резко ухудшаются. Удаление тумана часто сопровождается появлением артефактов на изображении и искажением цветов. Поэтому актуальным является поиск способов правильной оценки присутствия и удаления тумана с сохранением деталей и цветов изображения и разработка соответствующих методов обработки затуманенных изображений.

Цель. Целью работы является поиск эффективных подходов к решению задачи удаления тумана и дымки с цифровых изображений и реализация их в компьютерной системе обработки цифровых изображений [1].

Методы. Основные этапы обработки изображения выполняются на канале интенсивности, что способствует сохранению цветов. Предложен подход для удержания значений обрабатываемых пикселей в допустимом диапазоне, что позволяет лучше сохранить детали изображения. Для оценки карты пропускания используются частотные фильтры. В модифицированном методе оценка плотности тумана выполняется с использованием нейронной сети.

Результаты. Предложен метод удаления тумана и дымки из одиночных изображений, который эффективно улучшает видимость объектов, сохраняет детали и цвета на изображении, а также его модификация с другим способом оценки плотности тумана. Представленные методы были реализованы в компьютерной системе [1].

Выводы. Предложенный метод и его модификация эффективно удаляют туман и дымку из одиночных изображений, улучшая различимость объектов на них. Реализация этих методов в компьютерной системе обработки изображений [1] расширила функционал системы и увеличила ее возможности по повышению качества изображений, полученных в условиях плохой видимости. Система может быть использована для предварительной обработки изображений с целью предотвращения ошибок в дальнейшей работе алгоритмов компьютерного зрения.

КЛЮЧЕВЫЕ СЛОВА: обработка изображений, удаление тумана и дымки, модель тумана, улучшение видимости, карта пропускания, оценка атмосферного света.

UDC 004.932

THE METHOD OF IMPROVING FOGGED IMAGES VISIBILITY AND ITS USING IN THE PROCESSING IMAGES COMPUTER SYSTEM

Serdiuk M. E. – PhD, Associate Professor of Computer Technologies Department, Oles Honchar Dnipro National University, Dnipro, Ukraine.

Berkut V. G. – Master of Applied Mathematics, graduate student of Applied Mathematics Faculty, Oles Honchar Dnipro National University, Dnipro, Ukraine.

Sirik S. F. – Assistant of Computer Technologies Department, Oles Honchar Dnipro National University, Dnipro, Ukraine.

ABSTRACT

Context. Presence of fog and haze on digital images may cause problems in processes of recognition, tracking, classification of objects. Thus methods for removing fog and improving visibility of objects in images obtained under poor visibility conditions are in demand in many computer vision problems. In foggy weather, contrast and color of an image get worse. Fog removal is often accompanied by artifacts in the image and color distortion. Therefore, it is relevant to seek methods for correct assessing presence and removal of fog while preserving image details and colors and developing appropriate methods for blurred images processing.

DOI 10.15588/1607-3274-2019-4-16

Objective. The purpose of this research is to find effective approaches to solving the problem of removing fog and haze from digital images and implementing them in a digital image processing computer system [1].

Method. Main stages of image processing are performed on the intensity channel, which helps to preserve colors. The proposed approach keeps the values of the processed pixels in an acceptable range, which allows better preservation of image details. Frequency filters are used to evaluate the transmission map. In a modified method, fog density is estimated using a neural network.

Results. The method of removing fog and haze from single image is proposed. This method effectively improves the objects visibility, preserves details and colors in the image. A modification of the method with another fog density estimation method is also proposed. The presented methods were implemented in a computer system [1].

Conclusions. The proposed method and its modification effectively remove fog and haze from single image and improve the objects distinguishability in them. The implementation of these methods in a computer image processing system [1] has expanded the functionality of the system and increased its ability to improve the quality of images obtained under poor visibility conditions. The system can be used for preliminary image processing to prevent errors in further operation of computer vision algorithms.

KEYWORDS: image processing, fog and haze removal, fog model, improved visibility, transmission map, atmospheric light evaluation.

REFERENCES

1. Serdiuk M. E., Berkut V. G. Kompiuterna systema lokalizatsii ta vydalennia tinei u tsyfrovykh zobrazhenniakh, Radio Electronics, Computer Science, Control, 2017, №2(41), pp. 127–133. DOI: 10.15588/1607-3274-2017-2-14
2. He K., Sun J., Tang X. Single image haze removal using dark channel prior, IEEE Trans. Pattern Anal. Mach. Intell. Dec. 2011, Vol. 33, No. 12, pp. 2341–2353. DOI: 10.1109/TPAMI.2010.168
3. Kang Hyun-Jin, Young-Hyung Kim, Yong Hwan Lee Fast Removal of Single Image using Pixel-based Median Channel Prior, *I. J. Advanced Science and Technology Letters,* 2015, Vol. 98, pp. 124–127. DOI: 10.14257/astl.2015.98.31
4. Tan R. T. Visibility in bad weather from a single image, *Proceedings.of the 26th IEEE Conference on Computer Vision and Pattern Recognition (CVPR '08)*. Anchorage, Alaska, 2008, pp. 1–8.
5. Kim J.-H., Jang W.-D., Sim J.-Y., Kim C.-S. Optimized contrast enhancement for real-time image and video dehazing, *Journal of Visual Communication and Image Representation*, 2013, Vol. 24, No. 3, pp. 410–425. DOI: 10.1016/j.jvcir.2013.02.004
6. Tarel J. P., Hautiere N. Fast Visibility Restoration from a Single Color or Gray Level Image, *Proceedings of the 12th IEEE International Conference on Computer Vision*. Kyoto, Japan, 2009, pp. 2201–2208. DOI: 10.1109/ICCV.2009.5459251
7. Fattal R. Dehazing Using Color-Lines, *ACM Transactions on Graphics,* 2014, Vol. 34, No. 1, P. 13. DOI: 10.1145/2651362
8. Livingston M. A., Caelan R. Garrett, Zhuming Ai Image Processing for Human Understanding in Low-visibility, *Information Technology Division, Naval Research Laboratory,* 2011, pp. 1–9.
9. Berman D., Treibitz T., Avidan S. Non-Local Image Dehazing, *Proceedings of the CVPR Computer Vision and Pattern Recognition*. Las Vegas, NV, USA, 2016, pp. 1674–1682. DOI: 10.1109/CVPR.2016.185
10. Berman D., Treibitz T., Avidan S. Air-light Estimation using Haze-Lines, *Proceedings of the IEEE 13th International Conference on Intelligent Computer Communication and Processing*. Stanford, CA, USA, 2017, pp. 5178–5191. DOI: 10.1109/ICCPHOT.2017.7951489
11. Narasimhan S. G., Nayar S. K. Removing weather effects from monochrome images, *Proceedings of the CVPR Computer Vision and Pattern Recognition.* Kauai, HI, USA, 2001, pp. 186–193. DOI: 10.1109/CVPR.2001.990956
12. Chen G., Wang T., Zhou H. J. A Novel Physics-based Method for Restoration of Foggy Day Images, *Journal of Image and Graphics,* 2008, Vol. 13, No. 5, pp. 888–893. DOI: 10.1109/SNPD.2007.350
13. He K. M., Sun J., Tang X. O. Guided image filtering, *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2010, Vol. 35, No. 6, pp. 1397–1409. DOI: 10.1109/TPAMI.2012.213
14. Pang J., Au O. C., Guo Z. Improved single image dehazing using guided filter, In Proc. APSIPA ASC. Xi'an, China, 2011, pp. 1–4.
15. Zhang Y.-Q., Ding Y., Xiao J.-S., Liu J., Guo Z. Visibility enhancement using an image filtering approach, *EURASIP Journal on Advances in Signal Processing,* Vol. 2012, Article 220, 2012, pp. 1– 6. DOI: 10.1186/1687-6180-2012-220
16. Shi L., Cui Xiao, Yang Li, Gai Zhigang, Chu Shibo, Shi Jing Image Haze Removal Using Dark Channel Prior and Inverse Image, *International Conference on Measurement Instrumentation and Electronics 2016 (ICMIE 2016)*. Munich, Germany, 2016, pp. 89–93. DOI: 10.1051/matecconf/20167503008
17. Huang D., Wang W., Lu J., Chen K. Fast Single Image Haze Removal Method based on Atmospheric Scattering Model, IFAC-PapersOnLine, 2018, Vol. 51, Issue 17, pp. 211–216. DOI: 10.1016/j.ifacol.2018.08.144
18. Noor A. Ibraheem, Mokhtar M. Hasan, Rafiqul Z. Khan, Pramod K. Mishra Understanding Color Models: A Review, *ARPN Journal of Science and Technology*, 2012, Vol. 2, No. 3, pp. 265–275.
19. Gonsales R., Vuds R. Cifrovaya obrabotka izobrazhenij : per. s angl. Moscow, Texnosfera, 2005, 1072 p.
20. Kumari A., Sahoo S. K. Real Time Visibility Enhancement for Single Image Haze Removal, *Proc. Int. Conf. on Information Processing (IMCIP)*, 2015, pp. 501–507. DOI: 10.1016/j.procs.2015.06.057
21. Esterhuizen D. C# How to: Image Contrast / D. Esterhuizen [Electronic resource]. Access mode: https://softwarebydefault.com/2013/04/20/image-contrast/
22. Godard C., Aodha O. M., Brostow G. Unsupervised Monocular Depth Estimation with Left-Right Consistency, [Electronic resource]. Access mode: http://zpascal.net/cvpr2017/Godard_Unsupervised_Monocular_Depth_CVPR_2017_paper.pdf.
23. Arora T., Gurpadam B. Singh, Mandeep C. Kaur Evaluation of a New Integrated Fog Removal Algorithm IDCP with CLAHE, *International Journal of Soft Computing and Artificial Intelligence*, 2014, Vol. 2, Issue 1, pp. 12–18.
24. Bai L., Wu Y., Xie J., Wen P. Real Time Image Haze Removal on Multi-core DSP, *2014 Asia-Pacific International Symposium on Aerospace Technology, APISAT 2014,* 2014, pp. 244–252. DOI: 10.1016/j.proeng.2014.12.532
25. Tarel J.-P., Hautière N., Cord A., Gruyer D., Halmaoui H. Improved Visibility of Road Scene Images under Heterogeneous Fog, *Proceedings of IEEE Intelligent Vehicles Symposium (IV'10)*. San Diego, CA, USA, June 21–24, 2010. DOI:10.1109/IVS.2010.5548128

DOI 10.15588/1607-3274-2019-4-16

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

UDC 004.056.55

AVALANCHE CHARACTERISTICS OF CRYPTOGRAPHIC FUNCTIONS OF TERNARY LOGIC

Sokolov A. V. – PhD, Senior Lecturer of the Department of Informatics and Control of Information Systems Protection, Odessa National Polytechnic University, Odessa, Ukraine.

Zhdanov O. N. – PhD, Assistant Professor of the IT Security Department, Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia.

ABSTRACT

Context. The development and aplication of cryptographic algorithms based on many-valued logic functions makes it important to research their cryptographic properties and develop effective criteria for the cryptographic quality of their components. The development of efficient methods for the synthesis of high-quality cryptographic primitives based on the functions of many-valued logic is also an important task. The object of this research is the process of improving the efficiency of cryptographic algorithms based on many-valued logic functions.

Objective. The purpose of this paper is to generalize the error propagation criterion and the strict avalanche criterion for the case of functions of three-valued logic.

Method. The emergence of cryptography based on many-valued logic functions led to the understanding that today's dominant cryptographic algorithms based on binary algebraic constructions are only a special case of more general trends. Numerous researches show that the use of cryptographic constructions based on many-valued logic functions leads to the creation of cryptoalgorithms that more fully implement the principles of diffusion and confusion. One of the most important cases of many-valued logic functions are 3-functions, which are also used in quantum cryptography. This article is another step towards developing cryptographic constructions based on many-valued logic functions.

Results. The definition of the propagation criterion was extended to the case of functions of three-valued logic. On the basis of the propagation criterion for the functions of three-valued logic, the definition of a strict avalanche criterion was introduced, which describes the stability of cryptographic constructions against differential cryptanalysis attacks. We experimentally determined the number of 3-functions of length N=9, satisfying the strict avalanche criterion. A method based on three constructive rules is proposed, which allows to synthesize a complete set of 864 S-boxes of length N=9 satisfying strict avalanche criterion. This set of S-boxes is basic for the application of Kim's construction, which allows to recurrently increase the length of the S-box to the required value. The paper shows that using Kim's construction to increase the length preserves the S-box satisfying to a strict avalanche criterion, while allowing to obtain S-boxes with satisfactory non-linearity value as well as small output and input vectors correlation.

Conclusions. The most important criterion of cryptographic quality, which shows the stability of the cryptographic algorithm to attacks of differential cryptanalysis is the propagation criterion that was generalized to the case of 3-functions. The existence of 3-functions of length N=9 satisfying the strict avalanche criterion is shown, and their full set is found. On the basis of the proposed constructive method, a complete set of S-boxes of length N=9 that satisfy the strict avalanche criterion was synthesized. It is shown that the Kim scheme can be applied to recurrently increase the length of S-boxes based on many-valued logic functions. As an actual direction for the continuation of the research, the development of regular and constructive methods for the synthesis of full sets of 3-functions and S-boxes of lengths N=27, 81, 243..., satisfying the strict avalanche criterion can be noted.

KEYWORDS: cryptography, differential properties, ternary logic, Boolean function.

ABBREVIATIONS

SAC is a Strict Avalanche Criterion.

NOMENCLATURE

f, f' are many-valued logic function examples;

x_1, x_2 are arguments of many-valued logic function;

d_1, d_2 are effects on the inputs of many-valued logic function;

N is a length of many-valued logic function or S-box, based on many-valued logic functions;

K^0, K^-, K^+ are numbers of symbols 0, – and + in ternary function;

δ is a transformation of change in ternary function output values;

u is a vector of change in ternary function argument;

$v(u)$ is a number of non-zero values of a vector u;

$D_u f$ is an derivative of ternary logic function;

m is an order of propagation criterion;

X is a vector of ternary function input arguments;

J_1, J_2, J_3 are numbers of S-boxes that can be produced by using Rule 1, Rule 2 and Rule 3 correspondingly;

α is a coding sequence used in Rule 3 to perform sign encodings of ternary functions;

J is a cardinality of the class of S-boxes of length $N = 9$, satisfying strict avalanche criterion;

S, S_{27}, S_{81} are S-box examples;

NL is the nonlinearity distance;

$P = \left\| \rho_{v,\mu} \right\|$ is the matrix of the correlation coefficients between the output y_μ and input x_v vectors of the S-box.

INTRODUCTION

Block symmetric cryptographic algorithms are the very important part of modern information protection systems. A further increase in the computing power of computer systems, as well as the emergence of new methods of cryptanalysis give rise to the need to increase the cryptographic strength of existing and new cryptographic algorithms.

DOI DOI 10.15588/1607-3274-2019-4-17

Further development of existing algorithms and the creation of new ones requires the availability of high-quality cryptographic primitives, in particular, S-boxes.

At the same time, the application of the mathematical apparatus of many-valued logic functions is promising, both from the point of view of quantum cryptography and from the point of view of traditional cryptography.

A special place, especially from the point of view of quantum cryptography, among the functions of many-valued logic is occupied by the functions of three-valued logic.

The creation of new cryptographic primitives based on many-valued logic functions requires the generalization of cryptographic quality criteria, the main of which are: nonlinearity, correlation immunity, propagation criterion and a strict avalanche criterion which is particular case of the propagation criterion.

In this paper, the propagation criterion and strict avalanche criterion are generalized to the case of three-valued logic functions, and effective methods for synthesizing 3-functions and S-blocks of arbitrary length that satisfy the strict avalanche criterion are proposed.

The object of research is the process of improving the efficiency of cryptographic algorithms based on many-valued logic functions.

The subject of research is the synthesis methods of S-boxes based on many-valued logic functions with good avalanche characteristics.

The purpose of the work is to generalize the error propagation criterion and the strict avalanche criterion to the case of functions of three-valued logic that will allow us to develop a recursive method for synthesizing S-boxes satisfying the strict avalanche criterion.

1 PROBLEM STATEMENT

Let the function $f(X)$ of three-valued logic to be given. The scientific problem is to build a method for determining the probability of a change in the output values of a function when its input values change.

Another important task solved in this paper is the development of a method for synthesizing the functions $f(X)$ which the uniform probability of a change in output values when one of the input values is changing (such functions are called as satisfying the strict avalanche criterion).

We also solve the problem of constructing S-boxes on the basis of 3-functions satisfying SAC, that can be used in modern cryptographic algorithms based on the principles of many-valued logic.

2 REVIEW OF THE LITERATURE

The development of methods of many-valued logic, occurring at the present time [1], causes the emergence of new algorithms for the cryptographic data protection [2]. Functions of many-valued logic are the excellent basis for the construction of quantum cryptoalgorithms [3…5].

Although many-valued logic algorithms can have an effective hardware implementation [6], by the reason of better realization of the concepts of diffusion and confusion [7], functions of many-valued logic are of considerable interest from the point of view of implementation on binary computers.

Thus, in [8] a block symmetric cryptoalgorithm based on the methods of ternary logic was synthesized. The researches performed show that the use of these methods of ternary logic for the construction of cryptoalgorithms allows us to obtain a high level of diffusion and confusion even when using the simple block replacement (Electronic Codebook [9]) mode at the cost of a small loss of computational efficiency.

The highly nonlinear many-valued functions, that can be, in particular, used in S-boxes construction schemes like modernized Kim's construction [10] was developed in [11] and [12].

Method for constructing S-boxes of ternary logic satisfying the criterion of zero correlation between the output and input vectors is proposed in [13], and method for constructing highly nonlinear S-boxes based on the Nyberg construction is developed in [14].

A method for estimating the non-linearity distance of many-valued logic functions based on the Vilenkin-Chrestenson transform was proposed in [15].

Nevertheless, such an important criterion of the cryptographic quality of S-boxes, as the propagation criterion and the strict avalanche criterion (SAC) remains outside the framework of modern researches devoted to S-boxes based on functions of many-valued logic.

In the binary case, the strict avalanche criterion as a characteristic of resistance to differential cryptoanalysis is one of the basic in the synthesis of S-boxes [16, 17]. The physical interpretation of the error propagation criterion is to measure the degree of change in the output values of a Boolean function when its input values change [18].

3 MATERIALS AND METHODS

The most important problem is the development of a technique for measuring the differential properties of functions of many-valued logic, in particular, 3-functions.

Let's consider an example. Let the truth table of a 3-function of two variables to be given

$$f = \{012012210\}. \quad (1)$$

In order to research the effect of each of the inputs of the 3-function on its output, we connect the summators (Fig. 1) to the inputs, to which we apply the effects $d_1, d_2 \in \{0,1,2\}$. Obviously, a set of values $d_1, d_2 = 0$, means no effect on the inputs of our 3-function.

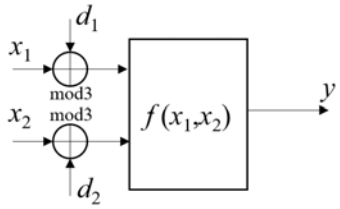


Figure 1 – Example of a scheme for researching the influence of inputs of a 3-function on its output

DOI DOI 10.15588/1607-3274-2019-4-17

Alternately changing the values of the coefficients d_1, d_2, we obtain the rearranged values of the initial 3-function (1), presented in Table 1 (symbol $\oplus$ means addition modulo 3).

Table 1 shows the change in the value of a function when its arguments are changed. Note, that for the binary case this question is trivial, since operating with values from the set $\{0,1\}$ makes it easy to infer the output value: it has changed / has not changed. In the case of ternary logic, obviously, the nature of the change in the output value also plays an important role.

Possible options are:

1. The function value has not changed. Denote this event as 0.

2. The value increased (decreased) by 1 (modulo 3). Denote these events with the symbols "+/–".

We denote this transformation by the symbol δ and introduce the following basic definitions.

Definition 1. Let the $\nu(u)$ to be the number of non-zero values of a vector u. A derivative of a 3-function of k variables in direction of vector u, we call the following 3-function

$$\mathrm{D}_u f = \delta(f(x), f(x+u)). \qquad (2)$$

Definition 2. We say that a 3-function satisfies the propagation criterion in the direction of the vector u if the number of zero values in its derivative $\mathrm{D}_u f$ is equal to the number of positive values and is equal to the number of negative values: $K^0 = K^+ = K^- = N/3$.

In other words, under the influence of the change in input values in direction u the probabilities of events 0, $-$ or $+$ are equal to

$$P_u = \begin{bmatrix} \frac{K^0}{N} & \frac{K^+}{N} & \frac{K^-}{N} \end{bmatrix} = \begin{bmatrix} 0 & + & - \\ 1/3 & 1/3 & 1/3 \end{bmatrix}. \qquad (3)$$

Definition 3. A function is called as satisfying the propagation criterion of order m if it satisfies the propagation criterion in all such directions u that $1 \le \nu(u) \le m$.

Definition 4. A function is said to satisfy a strict avalanche criterion if it satisfies the propagation criterion of order $m = 1$.

Let's continue the example. We find the derivatives of the 3-function (1) and verify its compliance with the strict avalanche criterion (Table 2).

Thus, the researched function does not satisfy the strict avalanche criterion. It is of practical interest to perform the search for 3-functions corresponding to the definition of the strict avalanche criterion that we introduced.

Table 1 – The rearranged values of the initial 3-function (1)

$f(x_1, x_2)$	$f(x_1, x_2 \oplus 1)$	$f(x_1, x_2 \oplus 2)$	$f(x_1 \oplus 1, x_2)$	$f(x_1 \oplus 2, x_2)$
$f(0,0)=0$	$f(0,1)=1$	$f(0,2)=2$	$f(1,0)=0$	$f(2,0)=2$
$f(0,1)=1$	$f(0,2)=2$	$f(0,0)=0$	$f(1,1)=1$	$f(2,1)=1$
$f(0,2)=2$	$f(0,0)=0$	$f(0,1)=1$	$f(1,2)=2$	$f(2,2)=0$
$f(1,0)=0$	$f(1,1)=1$	$f(1,2)=2$	$f(2,0)=2$	$f(0,0)=0$
$f(1,1)=1$	$f(1,2)=2$	$f(1,0)=0$	$f(2,1)=1$	$f(0,1)=1$
$f(1,2)=2$	$f(1,0)=0$	$f(1,1)=1$	$f(2,2)=0$	$f(0,2)=2$
$f(2,0)=2$	$f(2,1)=1$	$f(2,2)=0$	$f(0,0)=0$	$f(1,0)=0$
$f(2,1)=1$	$f(2,2)=0$	$f(2,0)=2$	$f(0,1)=1$	$f(1,1)=1$
$f(2,2)=0$	$f(2,0)=2$	$f(2,1)=1$	$f(0,2)=2$	$f(1,2)=2$

Table 2 – The derivatives of the 3-function (1)

$f(x_1, x_2)$	$f(x_1, x_2 \oplus 1)$	D_{01}	$f(x_1, x_2 \oplus 2)$	D_{02}	$f(x_1 \oplus 1, x_2)$	D_{10}	$f(x_1 \oplus 2, x_2)$	D_{20}
$f(0,0)=0$	$f(0,1)=1$	$-$	$f(0,2)=2$	$+$	$f(1,0)=0$	0	$f(2,0)=2$	$+$
$f(0,1)=1$	$f(0,2)=2$	$-$	$f(0,0)=0$	$+$	$f(1,1)=1$	0	$f(2,1)=1$	0
$f(0,2)=2$	$f(0,0)=0$	$-$	$f(0,1)=1$	$+$	$f(1,2)=2$	0	$f(2,2)=0$	$-$
$f(1,0)=0$	$f(1,1)=1$	$-$	$f(1,2)=2$	$+$	$f(2,0)=2$	$+$	$f(0,0)=0$	0
$f(1,1)=1$	$f(1,2)=2$	$-$	$f(1,0)=0$	$+$	$f(2,1)=1$	0	$f(0,1)=1$	0
$f(1,2)=2$	$f(1,0)=0$	$-$	$f(1,1)=1$	$+$	$f(2,2)=0$	$-$	$f(0,2)=2$	0
$f(2,0)=2$	$f(2,1)=1$	$+$	$f(2,2)=0$	$-$	$f(0,0)=0$	$-$	$f(1,0)=0$	$-$
$f(2,1)=1$	$f(2,2)=0$	$+$	$f(2,0)=2$	$-$	$f(0,1)=1$	0	$f(1,1)=1$	0
$f(2,2)=0$	$f(2,0)=2$	$+$	$f(2,1)=1$	$-$	$f(0,2)=2$	$+$	$f(1,2)=2$	$+$

DOI DOI 10.15588/1607-3274-2019-4-17

4 EXPERIMENTS

It seems to us that for small values of the length it is possible to carry out a exhaustive search for ternary sequences satisfying the strict avalanche criterion. The search of a complete set of ternary sequences of length $N = 9$ allowed us to establish that there are in total 2052 3-functions of the specified length that satisfy the strict avalanche criterion.

For example, we show (Table 3) that the sequence we have found

$$f' = \{001022121\}, \tag{4}$$

satisfies the strict avalanche criterion.

Since all the D_i in Table 3 are balanced, so $K^0 = K^+ = K^-$, the sequence (4) really satisfies the strict avalanche criterion.

We note that such 3-functions possess special practical value, on the basis of which it is possible to construct such important cryptographic primitives as S-boxes. Experimental research carried out with the requirements of the theorem [20] which regulates the conditions of bijectivity of S-boxes, made it possible to discover that from the total set of the 3-functions of length $N = 9$, satisfying the strict avalanche criterion there are only 72 such 3-functions on the basis of which it is possible to construct the S-box. These 3-functions are given in Table 4.

5 RESULTS

Let us determine the possible number of S-boxes of length $N = 9$ satisfying the strict avalanche criterion. A complete set of such S-boxes of length $N = 9$ can be constructed on the basis of a set of generating S-boxes and rules of their reproduction.

We represent the set of generating S-boxes, on the basis of which the full class of S-boxes of length $N = 9$ satisfying the strict avalanche criterion can be obtained

$$\begin{bmatrix} 0\,1\,3\,2\,8\,6\,5\,7\,4 \\ 0\,1\,3\,6\,2\,8\,7\,4\,5 \\ 0\,1\,4\,2\,7\,8\,3\,6\,5 \\ 0\,1\,4\,6\,5\,3\,8\,2\,7 \\ 0\,1\,6\,2\,5\,3\,8\,4\,7 \\ 0\,1\,6\,3\,2\,5\,4\,7\,8 \\ 0\,1\,7\,2\,4\,5\,6\,3\,8 \\ 0\,1\,7\,3\,8\,6\,5\,2\,4 \\ 0\,2\,3\,1\,7\,6\,4\,8\,5 \\ 0\,2\,3\,6\,1\,7\,8\,5\,4 \\ 0\,2\,5\,1\,8\,7\,3\,6\,4 \\ 0\,2\,5\,6\,4\,3\,7\,1\,8 \end{bmatrix} \begin{bmatrix} 0\,2\,6\,1\,4\,3\,7\,5\,8 \\ 0\,2\,6\,3\,1\,4\,5\,8\,7 \\ 0\,2\,8\,1\,5\,4\,6\,3\,7 \\ 0\,2\,8\,3\,7\,6\,4\,1\,5 \\ 0\,4\,1\,2\,8\,7\,3\,5\,6 \\ 0\,4\,1\,6\,3\,5\,8\,7\,2 \\ 0\,5\,2\,1\,7\,8\,3\,4\,6 \\ 0\,5\,2\,6\,3\,4\,7\,8\,1 \\ 0\,5\,3\,1\,2\,8\,7\,4\,6 \\ 0\,5\,3\,2\,8\,1\,6\,7\,4 \\ 0\,8\,2\,1\,4\,5\,6\,7\,3 \\ 0\,8\,2\,3\,6\,7\,4\,5\,1 \end{bmatrix}. \tag{5}$$

Reproduction of S-boxes (5) may be performed by applying the following rules.

Rule 1. Permutation of the second and third triples of elements of the S-box preserves the compliance of S-box with the strict avalanche criterion.

For example, from the first basic S-box obtained by us

$$[0\,1\,3\,2\,8\,6\,5\,7\,4], \tag{6}$$

we can obtain a new S-box by applying the Rule 1

$$[0\,1\,3\,5\,7\,4\,2\,8\,6]. \tag{7}$$

Table 3 – The derivatives of the 3-function (5)

$f'(x_1, x_2)$	$f'(x_1, x_2 \oplus 1)$	D_{01}	$f'(x_1, x_2 \oplus 2)$	D_{02}	$f'(x_1 \oplus 1, x_2)$	D_{10}	$f'(x_1 \oplus 2, x_2)$	D_{20}
$f'(0,0)=0$	$f'(0,1)=0$	0	$f'(0,2)=1$	−	$f'(1,0)=0$	0	$f'(2,0)=1$	−
$f'(0,1)=0$	$f'(0,2)=1$	−	$f'(0,0)=0$	0	$f'(1,1)=2$	+	$f'(2,1)=2$	+
$f'(0,2)=1$	$f'(0,0)=0$	+	$f'(0,1)=0$	+	$f'(1,2)=2$	−	$f'(2,2)=1$	0
$f'(1,0)=0$	$f'(1,1)=2$	+	$f'(1,2)=2$	+	$f'(2,0)=1$	−	$f'(0,0)=0$	0
$f'(1,1)=2$	$f'(1,2)=2$	0	$f'(1,0)=0$	−	$f'(2,1)=2$	0	$f'(0,1)=0$	−
$f'(1,2)=2$	$f'(1,0)=0$	−	$f'(1,1)=2$	0	$f'(2,2)=1$	+	$f'(0,2)=1$	+
$f'(2,0)=1$	$f'(2,1)=2$	−	$f'(2,2)=1$	0	$f'(0,0)=0$	+	$f'(1,0)=0$	+
$f'(2,1)=2$	$f'(2,2)=1$	+	$f'(2,0)=1$	+	$f'(0,1)=0$	−	$f'(1,1)=2$	0
$f'(2,2)=1$	$f'(2,0)=1$	0	$f'(2,1)=2$	−	$f'(0,2)=1$	0	$f'(1,2)=2$	−

Table 4 – The 3-functions suitable for S-boxes constructing

001022121	010112022	020122110	100220121	112010022	122020110	202112100	212200110
001121022	010211220	020221011	101002122	112022010	122101002	202211001	220010211
001202211	010220211	022001121	101122002	112100202	122110020	211001202	220100121
001211202	011002212	022010112	101200221	112202100	200101221	211010220	220121100
002011212	011020221	022112010	101221200	121001022	200110212	211202001	220211010
002101122	011212002	022121001	110020122	121022001	200212110	211220010	221011020
002122101	011221020	100112202	110122020	121100220	200221101	212002011	221020011
002212011	020011221	100121220	110200212	121220100	202001211	212011002	221101200
010022112	020110122	100202112	110212200	122002101	202100112	212110200	221200101

DOI DOI 10.15588/1607-3274-2019-4-17

So, the application of Rule 1 allows to obtaining $J_1 = 2$ new S-boxes based on one.

Rule 2. The permutation of the component 3-functions of the S-box preserves the compliance of S-box with the strict avalanche criterion.

As an example, we again consider the first basic S-box, which can be represented as two component 3-functions

$$\begin{bmatrix} 0\ 1\ 3\ 2\ 8\ 6\ 5\ 7\ 4 \\ 0\ 1\ 0\ 2\ 2\ 0\ 2\ 1\ 1 \\ 0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 1 \end{bmatrix}. \quad (8)$$

By permuting the component 3-functions, we obtain a new S-box, which also satisfies the strict avalanche criterion

$$\begin{bmatrix} 0\ 3\ 1\ 6\ 8\ 2\ 7\ 5\ 4 \\ 0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 1 \\ 0\ 1\ 0\ 2\ 2\ 0\ 2\ 1\ 1 \end{bmatrix}. \quad (9)$$

The application of Rule 2 allows us to obtain on the basis of one S-box $J_2 = k! = (\log_3 N)!$ new S-boxes satisfying the strict avalanche criterion. In the case of length $N = 9$ from one S-box, we obtain two.

Rule 3. All possible $3^k = 3^{\log_3 N} = N$ sign encodings of the component 3-functions of the S-box preserves the compliance of S-box with the strict avalanche criterion.

Let's demonstrate the operation of Rule 3 using as example the first basic S-box and the coding sequence $\alpha = \{\alpha_1 \quad \alpha_2\} = \{12\}$

$$\begin{bmatrix} 0\ 1\ 3\ 2\ 8\ 6\ 5\ 7\ 4 \\ \{0\ 1\ 0\ 2\ 2\ 0\ 2\ 1\ 1\} + \alpha_1 \bmod 3 \\ \{0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 1\} + \alpha_2 \bmod 3 \end{bmatrix} \rightarrow \rightarrow \begin{bmatrix} 7\ 8\ 1\ 6\ 3\ 4\ 0\ 5\ 2 \\ 1\ 2\ 1\ 0\ 0\ 1\ 0\ 2\ 2 \\ 2\ 2\ 0\ 2\ 1\ 1\ 0\ 1\ 0 \end{bmatrix}. \quad (10)$$

The application of Rule 3 allows us to obtain on the basis of one S-box $J_3 = 3^k = 3^{\log_3 N} = N$ new S-boxes satisfying the strict avalanche criterion. In the case of length $N = 9$, we obtain 9 new S-boxes.

Thus, using the basic 24 S-boxes of length $N = 9$ (5), as well as Rule 1, Rule 2 and Rule 3, we can synthesize a class of S-boxes of cardinality $J = 24 \cdot 2 \cdot 2 \cdot 9 = 864$, each of which is satisfying the strict avalanche criterion. This cardinality of class of S-boxes satisfying the strict avalanche criterion is equal to the cardinality of their complete set estimated by the exhaustive search.

6 DISCUSSION

The obtained 3-functions of length $N = 9$ (Table 4), satisfying SAC, as well as S-boxes which are built on their basis are important cryptographic constructions from a theoretical point of view.

We note that, for practical use S-boxes of long length N are necessary. Earlier, to increase the length of the S-boxes, both in the binary case [21] and in the ternary case [13], Kim's scheme was successfully used.

Kim's scheme is presented in general form for ternary case on Fig. 2

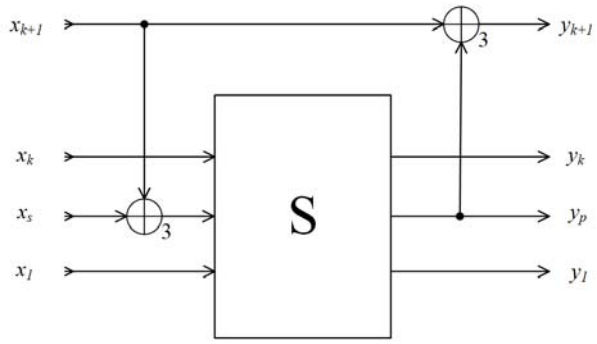


Figure 2 – Kim's scheme for ternary case

Let's consider an example. Suppose the S-box of length $N = 9$ satisfying the strict avalanche criterion is given

$$S = [0 \quad 1 \quad 6 \quad 3 \quad 2 \quad 5 \quad 4 \quad 7 \quad 8], \quad (11)$$

on the basis of which it is necessary to obtain an S-box of length $N = 27$.

We apply to the S-box (11) a Kim's scheme of recurrent increase of length (Fig. 1), which taking into account the length $N = 9$ of the initial S-box and the length $N = 27$ of the required S-box takes the form showed on Fig. 3.

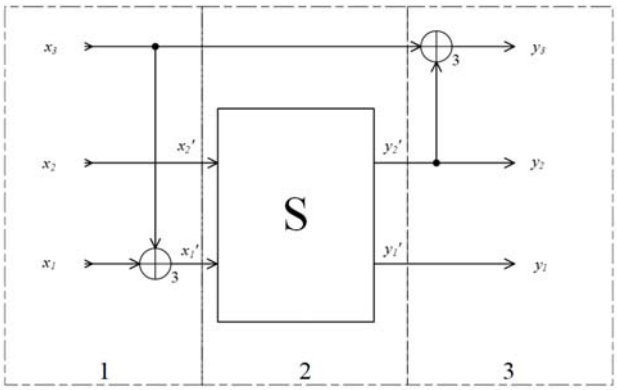


Figure 3 – Kim's scheme for a S-box with two inputs

Suppose, for example, that the vector of the input value of a new S-box of length $N = 27$ has the form

$$X = [x_1 \quad x_2 \quad x_3] = [001]_3. \quad (12)$$

Then, calculating the sum in the first sub-block (Fig. 3), we get the value

$$x_1' = (x_1 + x_3) \bmod 3 = (0+1) \bmod 3 = 1; \quad x_2' = x_2 = 0. \quad (13)$$

In the second sub-block of calculations, in accordance with the small S-box (11) chosen by us, we obtain

$$S(10) = S(1) = 1, \quad y_1' = 1; \quad y_2' = 0. \quad (14)$$

DOI DOI 10.15588/1607-3274-2019-4-17

And, finally, the calculations in the third sub-block

$$\begin{gathered} y_1 = y_1^{'} = 1; \quad y_2 = y_2^{'} = 0; \\ y_3 = (y_2^{'} + x_3) \bmod 3 = (1+0) \bmod 3 = 1 \Rightarrow \\ \Rightarrow Y = [y_1 \quad y_2 \quad y_3] = [101]_3 = 10. \end{gathered} \tag{15}$$

Calculating all the 27 different input values, we get the entire S-box of length $N = 27$

$$\begin{gathered} S_{27} = \big[0\ 1\ 24\ 12\ 2\ 14\ 13\ 25\ 26\ 10\ 6\ 9\ 11 \\ 23\ 21\ 7\ 8\ 22\ 15\ 18\ 19\ 5\ 3\ 20\ 17\ 4\ 16\big]. \end{gathered} \tag{16}$$

In [15] the interconnection between the nonlinearity distance of the S-box component functions and their Vilenkin-Chrestenson transformants was discovered. This interconnection may be described by the formula

$$\mathrm{NL} = \begin{cases} q^k - \max\left\{\left|W_i\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W_i\right|\right\}, & q = 2, \end{cases} \tag{17}$$

where W_i is the vector of S-box i-th component function Vilenkin-Chrestenson (Walsh-Hadamard for the binary case) transformants and $i = 0,1,...,\log_q N - 1$.

From other side, a formula for calculating the matrix $P = \left\|\rho_{\nu,\mu}\right\|$ of the correlation coefficients between the output y_μ and input x_ν vectors of the S-box was introduced in [13]

$$\rho_{\nu,\mu} = \frac{\sum\limits_{t=1}^{N} x_\nu y_\mu - \dfrac{\sum\limits_{t=1}^{N} x_\nu \sum\limits_{t=1}^{N} y_\mu}{N}}{\sqrt{\left[\sum\limits_{t=1}^{N} x_\nu^{\,2} - \dfrac{\left(\sum\limits_{t=1}^{N} x_\nu\right)^2}{N}\right] \cdot \left[\sum\limits_{t=1}^{N} y_\mu^{\,2} - \dfrac{\left(\sum\limits_{t=1}^{N} y_\mu\right)^2}{N}\right]}}, \tag{18}$$

where $\nu,\mu = 0,1,...,\log_q N - 1$.

Using formula (17) we can determine that the distance of nonlinearity of constructed S-box (16)

$$\mathrm{NL} = 11.412, \tag{19}$$

as well as we can calculate its matrix of correlation coefficients according to formula (18)

$$P = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0 \end{bmatrix}. \tag{20}$$

Continuing usage of the Kim's recurrent construction shown in Fig. 2 on the basis of S-box (16) we can get the S-box of length $N = 81$ that also satisfies the strict avalanche criterion

$$\begin{gathered} S_{81} = [0\ 1\ 78\ 39\ 2\ 41\ 40\ 79\ 80 \\ 10\ 60\ 9\ 11\ 50\ 48\ 61\ 62\ 49 \\ 69\ 18\ 19\ 32\ 30\ 20\ 71\ 31\ 70 \\ 28\ 24\ 27\ 29\ 68\ 66\ 25\ 26\ 67 \\ 6\ 36\ 37\ 77\ 75\ 38\ 8\ 76\ 7 \\ 45\ 46\ 15\ 57\ 47\ 59\ 58\ 16\ 17 \\ 51\ 54\ 55\ 14\ 12\ 56\ 53\ 13\ 52 \\ 63\ 64\ 33\ 21\ 65\ 23\ 22\ 34\ 35 \\ 73\ 42\ 72\ 74\ 5\ 3\ 43\ 44\ 4]. \end{gathered} \tag{21}$$

The calculated S-box S_{81} (21) have the nonlinearity distance

$$\mathrm{NL} = 34.235, \tag{22}$$

and the matrix of correlation coefficients

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{23}$$

CONCLUSIONS

The scientific novelty of obtained results is that we generalized such important criteria of cryptographic quality as the propagation criterion and the strict avalanche criterion to the case of functions of three-valued logic. The compliance of the 3-function with the strict avalanche criterion makes it possible to ascertain its resistance to attacks of differential cryptanalysis, which is important for practical cryptoalgorithms.

On the basis of the introduced definition of the strict avalanche criterion for 3-functions, in this paper we found a complete set of cardinality $J = 2052$ of 3-functions satisfying the strict avalanche criterion.

It is established that 72 of these functions can be the basis for constructing bijective S-boxes of length $N = 9$ satisfying the strict avalanche criterion. The cardinality of such S-boxes class is equal to 864.

It is proposed to use the ternary analogue of the Kim's scheme for recurrently increasing the length of the constructed S-boxes. It is shown that in the case of using the Kim's scheme, the resulting S-boxes also satisfies the strict avalanche criterion.

The practical significance of the paper is that the obtained class of 864 S-boxes satisfying the strict avalanche criterion can be used in practical cryptographic algorithm, which are based on the many-valued logic functions. At the same time, using Kim's scheme, S-boxes of any required length can be obtained.

DOI DOI 10.15588/1607-3274-2019-4-17

Prospects for further research are the development of regular and constructive methods for the synthesis of full sets of 3-functions and S-boxes of lengths N=27, 81, 243..., satisfying the strict avalanche criterion as well as consideration of another bases q of many-valued logic functions.

REFERENCES

1. Stankovic R. S., Astola J. T., Moraga C. Representation of Multiple-Valued Logic Functions, *Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems*, 2012, 153 p.
2. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. Springer, Cham, International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018, pp. 331–339.
3. Korchenko O., Vasiliu E., Gnatyuk S. Modern quantum technologies of information security, Aviation. Vilnius, Technika, 2010, No. 14 (2), pp. 58–69.
4. Hnatiuk S., Zhmurko T., Kinzeriavyi V., Seilova N. Method for quality evaluation of trit pseudorandom sequence to cryptographic applications, *Information technology and security,* 2015, Vol. 3, No. 2, pp. 108–116.
5. Vol E. D. Quantum theory as a relevant framework for the statement of probabilistic and many-valued logic, *International Journal of Theoretical Physics*, 2013, 52(2), pp. 514–523.
6. Stakhov A. Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic, *The Computer Journal,* 2002, 45(2), pp. 221–236.
7. Shannon, C.E. A Mathematical Theory of Cryptography, *Bell system technical journal,* 1948, Vol. 27, No. 3, pp. 379–423
8. Zhdanov O.N. Sokolov A.V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic, *Far East Journal of Electronics and Communications*, 2015, Vol. 16, No. 3, pp. 573–589.
9. El Fishawy N. F., Zaid O. M. A. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms, *IJ Network Security*, 2007, 5(3), pp. 241–251.
10. Sokolov, A.V., Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion / A.V. Sokolov. – Radioelectronics and Communications Systems, 2013. – Vol. 56. – No.8. – P. 415–423.
11. Sokolov A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties, *Journal of Telecommunication, Electronic and Computer Engineering,* 2016, Vol. 8, No. 9, pp. 39–43.
12. Mazurkov M. I., Sokolov A. V., Barabanov N. A. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis, *Radioelectronics and Communications Systems,* 2016, Vol. 59, No. 11, pp. 510–517.
13. Zhdanov O. N., Sokolov A. V. Algorithm of construction of optimal according to criterion of zero correlation nonbinary S-boxes, *Problems of physics, mathematics and technics*, 2015, No. 3(24), pp. 94–97.
14. Zhdanov O. N., Sokolov A. V. Extending Nyberg construction on Galois fields of odd characteristic / O.N. Zhdanov, // *Radioelectronics and Communications Systems*, 2017, Vol. 60, No. 12, pp. 538–544.
15. Sokolov A. V., Krasota N. I. Very nonlinear permutations: synthesis method for S-boxes with maximal 4-nonlinearity, *Proceeding of ONAT named after A. S. Popov*, 2017, No.1, pp. 145–154.
16. Webster A. F., Tavares S. E. On the design of S-boxes, *Proc. of CRYPTO'85*. Springer-Verlag, 1985, pp. 523–534.
17. Chandrasekharappa T.G.S., Prema K. V., Kumara Shama S - boxes generated using Affine transformation giving maximum avalanche effect, *Int. J. Comput. Sci. Eng.,* 2011, Vol. 3, No. 9, pp. 3185–3193.
18. Chandrasekharappa T. G. S., Prema K. V., Shama Kumara Possible S-boxes generated from Affine transformation those satisfy Maximum Strict Avalanche Criteria, *Proceedings of World Academy of Science, Engineering and Technology*, 2009, Vol. 60, pp. 880–883.
19. Trakhtman A. M., Trakhtman V. A. Fundamentals of the theory of discrete signals on finite intervals. Moscow, Soviet Radio, 1975, 208 p.
20. Kim K. Construction of DES-like S-boxes based on Boolean functions satisfying the SAC, Lect. Notes Comput. Sci., 1993, pp. 59–72.
21. Kim K., Matsumoto T., Imai H. A recursive construction method of S-boxes satisfying the strict avalanche criterion, *Proc. of CRYPTO90*. Springer-Verlag, 1990, pp. 565–574.

Received 26.06.2019.
Accepted 03.09.2019.

УДК 004.056.55

ЛАВИННІ ХАРАКТЕРИСТИКИ КРИПТОГРАФІЧНИХ ФУНКЦІЙ ТРИЗНАЧНОЇ ЛОГІКИ

Соколов А. В. – канд. техн. наук, старший викладач кафедри інформатики та управління захистом інформаційних систем, Одеський національний політехнічний університет, м. Одеса, Україна.

Жданов О. Н. – канд. физ.-мат. наук, доцент кафедри безпеки інформаційних технологій, Сибірський державний університет науки і технологій імені академіка М. Ф. Решетнева, Красноярськ, Росія.

АНОТАЦІЯ

Актуальність. Розробка і впровадження криптоалгоритмів на основі функцій багатозначної логіки робить актуальною задачу поглибленого вивчення їх криптографічних властивостей, розробки ефективних критеріїв криптографічної якості компонентів, з яких вони складаються. Важливим завданням є також розробка ефективних методів синтезу високоякісних криптографічних примітивів, заснованих на функціях багатозначної логіки. Об'єктом даного дослідження є процеси підвищення ефективності криптоалгоритмів на основі функцій багатозначної логіки.

Мета. Метою статті є узагальнення критерію поширення помилки і суворого лавинного критерію на випадок функцій тризначної логіки.

Метод. Поява криптографії на основі функцій багатозначної логіки привела до розуміння, що домінуючі сьогодні криптографічні алгоритми, засновані на двійкових алгебраїчних конструкціях, є лише окремим випадком більш загальних тенденцій. Численні дослідження показують, що використання криптографічних конструкцій на основі функцій багатозначної

DOI DOI 10.15588/1607-3274-2019-4-17

логіки веде до створення криптоалгоритмів, що більш повно реалізують принципи дифузії і конфузії. При цьому, найважливішим випадком функцій багатозначної логіки є 3-функції, які застосовуються також у квантовій криптографії. Ця стаття є ще одним кроком на шляху освоєння криптографічних конструкцій на основі функцій багатозначної логіки.

Результати. Визначення критерія поширення було узагальнене на випадок функцій тризначної логіки. На основі критерію поширення для функцій тризначної логіки було введено визначення суворого лавинного критерію, який описує стійкість криптографічних конструкцій до атак диференціального криптоаналізу. У статті експериментально визначено кількість 3-функцій довжини N=9, що задовольняють суворому лавинному критерію. Запропоновано метод, заснований на трьох конструктивних правилах, що дозволяє синтезувати повну множину з 864 S-блоків довжини N=9, які задовольняють суворому лавинному критерію. Дана множина S-блоків є базовою для застосування конструкції Кіма, що дозволяє рекурентно збільшити довжину S-блоку до необхідного значення. У статті показано, що використання конструкції Кіма для збільшення довжини зберігає відповідність S-блоку суворому лавинному критерію, при цьому дозволяє отримати S-блоки з задовільними показниками нелінійності та кореляційного зв'язку векторів виходу і входу.

Висновки. Найважливіший критерій криптографічної якості, який показує стійкість криптоалгоритму до атак диференціального криптоаналізу – критерій поширення помилки узагальнено на випадок 3-функцій. Показано існування 3-функцій довжини N=9, що задовольняють суворому лавинному критерію, а також знайдено їх повну множину. На основі запропонованого конструктивного методу синтезовано повну множину S-блоків довжини N=9, які задовольняють суворому лавинному критерію. Показано, що для рекурентного збільшення довжини S-блоків на основі функцій багатозначної логіки може бути застосована схема Кіма. В якості актуального напрямку продовження проведених досліджень можна зазначити побудову регулярних і конструктивних методів синтезу повних множин 3-функцій та S-блоків довжин N=27, 81, 243..., які відповідають суворому лавинному критерію.

КЛЮЧОВІ СЛОВА: криптографія, диференціальні властивості, тризначна логіка, булева функція.

УДК 004.056.55

ЛАВИННЫЕ ХАРАКТЕРИСТИКИ КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ ТРОИЧНОЙ ЛОГИКИ

Соколов А. В. – канд. техн. наук, старший преподаватель кафедры информатики и управления защитой информационных систем, Одесский национальный политехнический университет, г. Одесса, Украина.

Жданов О. Н. – канд. физ.-мат. наук, доцент кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева, Красноярск, Россия.

АННОТАЦИЯ

Актуальность. Разработка и внедрение криптоалгоритмов на основе функций многозначной логики делает актуальной задачу углублённого изучения их криптографических свойств, разработки эффективных критериев криптографического качества составляющих их компонентов. Важнейшей задачей является также разработка эффективных методов синтеза высококачественных криптографических примитивов, основанных на функциях многозначной логики. Объектом данного исследования являются процессы повышения эффективности криптоалгоритмов на основе функций многозначной логики.

Цель. Целью статьи является обобщение критерия распространения ошибки и строгого лавинного критерия на случай функций трехзначной логики.

Метод. Появление криптографии на основе функций многозначной логики, привело к пониманию, что доминирующие сегодня криптографические алгоритмы, основанные на двоичных алгебраических конструкциях, является лишь частным случаем более общих тенденций. Многочисленные исследования показывают, что использование криптографических конструкций на основе функций многозначной логики ведет к созданию криптоалгоритмов, более полно реализующих принципы диффузии и конфузии. При этом, важнейшим случаем функций многозначной логики являются 3-функции, которые применяются также в квантовой криптографии. Настоящая статья является еще одним шагом на пути освоения криптографических конструкций на основе функций многозначной логики.

Результаты. Определение критерия распространения было обобщено на случай функций трехзначной логики. На основе критерия распространения для функций трехзначной логики было введено определение строгого лавинного критерия, который описывает устойчивость криптографических конструкций к атакам дифференциального криптоанализа. В статье экспериментально определено количество 3-функций длины N=9, соответствующих строгому лавинному критерию. Предложен метод, основанный на трех конструктивных правилах, позволяющий синтезировать полное множество из 864 S-блоков длины N=9, удовлетворяющих строгому лавинному критерию. Данное множество S-блоков является базовым для применения конструкции Кима, позволяющей рекуррентно увеличить длину S-блока до необходимого значения. В статье показано, что использование конструкции Кима для увеличения длины сохраняет соответствие S-блока строгому лавинному критерию, при этом позволяет получить S-блоки с удовлетворительными показателями нелинейности и корреляционной связи векторов выхода и входа.

Выводы. Важнейший критерий криптографического качества, показывающий устойчивость криптоалгоритма к атакам дифференциального криптоанализа – критерий распространения ошибки обобщен на случай 3-функций. Показано существование 3-функций длины N=9, соответствующих строгому лавинному критерию, а также найдено их полное множество. На основе предложенного конструктивного метода синтезировано полное множество S-блоков длины N=9, удовлетворяющих строгому лавинному критерию. Показано, что для рекуррентного увеличения длины S-блоков на основе функций многозначной логики может быть применена схема Кима. В качестве актуального направления продолжения проведенных исследований может быть отмечено построение регулярных и конструктивных методов синтеза полных множеств 3-функций и S-блоков длин N=27, 81, 243…, удовлетворяющих строгому лавинному критерию.

КЛЮЧЕВЫЕ СЛОВА: криптография, дифференциальные свойства, троичная логика, булева функция.

DOI DOI 10.15588/1607-3274-2019-4-17

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Stankovic R. S. Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. – 153 p.
2. Sokolov A. V. Prospects for the Application of Many-Valued Logic Functions in Cryptography / A. V. Sokolov, O. N. Zhdanov. – Springer, Cham, International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018. – P. 331–339.
3. Korchenko, O. Modern quantum technologies of information security / O. Korchenko, E. Vasiliu, S. Gnatyuk. – Aviation. Vilnius : Technika, 2010. –No. 14 (2). – P. 58–69.
4. Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань / [С. Гнатюк, Т. Жмурко, В. Кінзерявий, Н. Сейлова]. – Інформаційні технології та безпека. – 2015. – Т. 3, № 2. – С. 108–116.
5. Vol E. D. Quantum theory as a relevant framework for the statement of probabilistic and many-valued logic / E. D. Vol. – International Journal of Theoretical Physics, 2013. – 52(2). – P. 514–523.
6. Stakhov A. Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic / A. Stakhov // The Computer Journal. – 2002. – 45(2). – P. 221–236.
7. Shannon C. E. A Mathematical Theory of Cryptography / C. E. Shannon // Bell system technical journal. – 1948. – Vol. 27, No. 3. – P. 379–423
8. Zhdanov O. N. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O. N. Zhdanov, A. V. Sokolov // Far East Journal of Electronics and Communications. – 2015. – Vol. 16, No. 3. – P. 573–589.
9. El Fishawy N. F. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms / N. F. El Fishawy, O. M. A. Zaid. – IJ Network Security, 2007. – 5(3). – P. 241–251.
10. Sokolov A. V. Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion / A. V. Sokolov // Radioelectronics and Communications Systems. – 2013. – Vol. 56, No. 8. – P. 415–423.
11. Sokolov A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov // Journal of Telecommunication, Electronic and Computer Engineering. – 2016. – Vol. 8, No. 9. – P. 39–43.
12. Mazurkov M. I. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis / M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov // Radioelectronics and Communications Systems. – 2016. – Vol. 59, No. 11. – P. 510–517.
13. Жданов О. Н. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен / О. Н. Жданов, А. В. Соколов // Проблемы физики, математики и техники. – 2015. – № 3 (24). – С. 94–97.
14. Zhdanov O. N. Extending Nyberg construction on Galois fields of odd characteristic / O. N. Zhdanov, A. V. Sokolov // Radioelectronics and Communications Systems. – 2017. – Vol. 60, No. 12. – P. 538–544.
15. Соколов А. В. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью / А. В. Соколов, Н. И. Красота. – Наукові праці ОНАЗ ім. О.С. Попова. – 2017. – № 1. – С. 145–154.
16. Webster A. F. On the design of S-boxes / A. F. Webster, S. E. Tavares // Proc. of CRYPTO'85. – Springer-Verlag, 1985. – P. 523–534.
17. Chandrasekharappa T. G. S. S-boxes generated using Affine transformation giving maximum avalanche effect / T. G. S. Chandrasekharappa, K. V. Prema, Shama Kumara. // Int. J. Comput. Sci. Eng. – 2011. – Vol. 3, No. 9. – P. 3185–3193.
18. Chandrasekharappa T. G. S. Possible S-boxes generated from Affine transformation those satisfy Maximum Strict Avalanche Criteria / T. G. S. Chandrasekharappa, K. V. Prema, Kumara Shama. – Proceedings of World Academy of Science, Engineering and Technology, 2009. – Vol. 60. – P. 880–883.
19. Трахтман А. М. Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. – М. : Советское радио, 1975. – 208 с.
20. Kim, K. Construction of DES-like S-boxes based on Boolean functions satisfying the SAC / K. Kim. – Lect. Notes Comput. Sci., 1993. – P. 59–72.
21. Kim K. A recursive construction method of S-boxes satisfying the strict avalanche criterion / K. Kim, T. Matsumoto, H. Imai // Proc. of CRYPTO90. – Springer-Verlag, 1990. – P. 565–574.

DOI DOI 10.15588/1607-3274-2019-4-17

UDC 004.75

METHODS OF FACTORIAL CODING OF SPEECH SIGNALS

Faure E. V. – Dr. Sc., Associate Professor, Vice-Rector for Research and International Relations, Cherkasy State Technological University, Cherkasy, Ukraine.

Shvydkyi V. V. – PhD, Associate Professor, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine.

Lavdanskyi A. O. – PhD, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine.

Kharin O. O. – Post-graduate student of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine.

ABSTRACT

Context. The paper outlines the methods of factorial coding of speech signals using a factorial code to provide integrated information security and to maintain a receiver and transmitter clock phase. By integrated information security, for the methods proposed in this article, we mean data protection from effects of noise in communication channel and attempts of data unauthorized access in open multiple access telecommunication networks.

Objective. The goal of the research is to provide integrated protection of real-time speech signals based on factorial coding. For this, the methods for factorial coding of speech signals and building speech codecs have been developed. These methods are based on the properties of factorial codes to keep synchronism with the working signal, to detect a significant part of errors caused by the action of noise, natural or created intentionally, to provide the ability to correct all detected errors with a finite accuracy, as well as to provide cryptographic protection against voice message unauthorized listening by hiding the law of converting speech signal samples into a permutation.

Method. The main idea of the proposed methods is to choose permutations for information transferring with a specific set of properties and features that provide the ability to correct errors detected by code and to recover speech signal samples with a finite degree of accuracy (with a nonzero aperture).

Results. The procedures for information coding/decoding have been determined. The results of the experimental evaluation of the model of such systems when working on a communication channel with both independent and multiple bit errors are presented. The magnitude of decoding noise due to the finite accuracy of speech signal samples recovery is determined as a function of bit error probability in a communication channel.

Conclusions. The proposed methods of factorial coding of a speech signal provide integrated information security and recovery with finite accuracy of speech signal samples deformed by noise in communication channel. The requirements to the quality of communication channel (to the value of bit error probability) for comfortable speech perception are determined.

KEYWORDS: factorial code, permutation, speech sample, samples recovery, decoding noise.

ABBREVIATIONS

ADC is an analog-to-digital converter;

BEP is a bit error probability;

DF is a decision feedback;

DTS is a digital transmission system;

FCDR is a factorial code with data recovery by permutation;

PDC is a primary digital channel;

SNR is a signal-to-noise ratio.

NOMENCLATURE

Δ is an interpolation step;

ΔP is a decoder SNR (dB);

ε_j is a decoding error of the j-th sample (the decoding noise, which accompanies the j-th speech signal sample);

$\varepsilon(x)$ is an n-bit error vector that damaged a permutation;

μ_{key} is a key space cardinality;

ν is a code rate;

π is a permutation;

σ is a sum of the permutation π numbers;

A_j is an amplitude of the j-th sample, formed by a source;

$A_j^{\wedge}$ is an amplitude of the j-th sample recovered by a decoder;

$A(x)$ is a data block;

B is a data linear rate;

$d(i)$ is a distance between the receives codeword and the i-th signal vector;

F_{discr} is a speech sampling rate;

h_{dec}^2 is a decoder signal-to-noise ratio;

k is a data block length;

k_{in} is an accumulation coefficient for synchronism entry;

k_{out} is an accumulation coefficient for synchronism exit;

l_r is a permutation symbol code length;

M is a permutation size;

n is a codeword size;

n_{ADC} is an ADC bit depth;

N is a shift register length;

DOI 10.15588/1607-3274-2019-4-18

P_{bg} is a probability of transition from 'bad' to 'good' state;

P_{gb} is a probability of transition from 'good' to 'bad' state;

P_w is a computing unit performance;

p_0 is a bit error probability;

p_{0b} is a bit error probability in a 'bad' state;

p_{0g} is a bit error probability in a 'good' state;

$R(x)$ is a codeword;

$R^{\wedge}(x)$ is a received codeword;

V is a number of samples in a communication session;

W_{noise} is a decoding noise power;

W_{signal} is a signal power;

X is a set of numbers $\{0,1,\ldots,M-1\}$;

Y is a time spent on enumerating all the keys of the key space.

INTRODUCTION

The intensive growth of automation of computer manufacturing equipment and the increasing degree of integration of its element base lead to an acceleration in the rate of increase in productivity and reduction in the cost of computers. The result of these processes is the use of computer systems in all areas of industrial, social and management activities of the global community. These factors generate the development of such opposing trends like the development of the sphere of computer systems application in all departments of human activity, on the one hand, and the equally active introduction of means and methods of unauthorized access of information or its deliberate modification, on the other hand.

Particularly important is the problem of ensuring the confidentiality and integrity of information on the activities of financial agencies and state law enforcement agencies (see, for example [1, 2]). Therefore, the attention of the engineering and scientific community has long been focused on this problem. This explains the interest to the work of recent years [3–16] on creating tools for integrated information security, including protection against the effects of errors in a transmission channel, protection against intentional modification of transmitted messages, and protection against unauthorized access to information.

The object of study is the process of speech data integrated protection.

The subject of study is the methods and means of factorial coding of speech signals.

The purpose of the work is to provide integrated protection of real-time speech signals based on factorial coding. Integrated protection involves:

– correction (with a nonzero aperture) of permutations, carriers of speech signal samples, received with an error and detected by the code;

– protection against unauthorized listening of voice messages.

Using factorial codes for transmission real-time speech signals leads to the need of:

– refusal from exact recovering of samples received with an error;

– transition to recovery of samples received with an error with limited accuracy (i.e., with a non-zero aperture);

– taking into account the psychophysical properties of speech perception.

1 PROBLEM STATEMENT

The task of the research is to develop methods for factorial coding and decoding of speech signals that provide integrated information protection and samples recovery with nonzero aperture.

Choosing the coding with a nonzero aperture inevitably leads to the appearance of a decoder recovery error. This error shows itself in the form of noise accompanying the received signal. The decoding error ε_j of the j-th sample (the decoding noise, which accompanies the j-th speech signal sample) is defined as follows:

$$\varepsilon_j^2 = \left(A_j - A_j^{\wedge}\right)^2.$$

We determine the decoding noise power W_{noise}:

$$W_{noise} = \sum_{j=1}^{V} \varepsilon_j^2 = \sum_{j=1}^{V} \left(A_j - A_j^{\wedge}\right)^2.$$

Note that the signal power in the same communication session will be equal to $W_{signal} = \sum_{j=1}^{V} A_j^2$.

Hence, the decoder SNR in a communication session will be equal to:

$$h_{dec}^2 = W_{signal} / W_{noise} = \sum_{j=1}^{V} A_j^2 \Bigg/ \sum_{j=1}^{V} \left(A_j - A_j^{\wedge}\right)^2.$$

This relation is a random variable. It is influenced by the following components of different physical nature:

– recovery errors due to the properties of the decoding algorithm;

– transformation (by channel noise) of the transmitted permutation into a permutation of the used part of the permutations set [14].

It is often convenient to use the logarithmic decibel scale to express SNR. In this case, decoder SNR (dB) is equal to the difference in levels of signal and decoding noise:

$$\begin{aligned} \Delta P &= P_{signal} - P_{noise} = \\ &= 10\lg\left(W_{signal}/W_{noise}\right) = 10\lg h_{dec}^2\,(dB). \end{aligned} \quad (1)$$

DOI 10.15588/1607-3274-2019-4-18

To solve the designated problem, we will take into account such a psychophysical feature of speech perception as the suppression of a weak signal by a strong signal. This means that if the speech signal is accompanied by low-level noise, then this does not prevent comfortable speech perception (essentially, in these conditions, the noise is imperceptible). Moreover, people experience discomfort in the absence of low-level noise accompanying speech. This is because the mechanism of speech perception has been formed for thousands of years in the conditions of a natural human environment with noises inherent in this environment. Therefore, a person staying in an environment with the absolute lack of interfering noise is unnatural and may cause a negative reaction of the human body. That is why the creation of comfortable speech perception is always in the field of vision of the creators of speech communication systems. Based on this, in this paper we consider a term 'comfort noise' as noise (random, uniformly distributed in amplitude and frequency oscillations. Randomness can be checked by tests and criteria [17–20]) accompanying a speech signal with the upper level of minus 30 dB and the lower level of minus 50 dB. These values define (on average) a threshold of human ear sensitivity.

2 REVIEW OF THE LITERATURE

The methods of combining the functions of cryptography and channel coding began to develop relatively recently. In particular, these include a public-key cryptography method based on error correction codes proposed by McEliece R. J. in [3]. Osmolovskiy S. A. proposed in [4] a stochastic method of integrated information security. This method includes a cascade execution of operations of error-correcting coding and encrypting stochastic transformation. Stakhov A. P. proposed in [5–7] a method of 'golden' cryptography to provide integrated protection. Mazurkov M. I. and Chechelnytskyi V. Ya. in [8–10] proposed to use parametric secrecy of a communication system with noise-like signals in combination with channel coding to provide integrated information security.

The analysis of these works shows that:

– McEliece's cryptosystem provides a slow code speed, requires a very long key length, and is easily decrypted when a key is reused;

– Osmolovskiy's stochastic methods of data protection do not solve the problem of integrating information security functions into a single procedure; they use the XORing operation, which is not always applicable in real data transmission systems with limitations typical for stream ciphers;

– Stakhov's 'golden' cryptography determines only the direction of work and requires additional fundamental research to determine code probability characteristics, evaluate its effectiveness, select an optimal value of the coding matrix degree;

– Mazurkov's and Chechelnytskyi's methods of information security based on perfect algebraic constructions provide parametric secrecy of information transmission and its channel coding, but do not provide message authentication and are limited to use in noise-like signal communication systems.

The factorial codes used in this work are based on the works performed by researchers under the supervision of Borysenko O.A. (see, for example, [11]). They identified some basics of information transfer based on permutations. In particular, they showed that the code built on permutations is an equilibrium with all the properties that follow from this. The use of permutations for information transferring was the starting point for further research on the creation of effective factorial codes [12–16].

The basis for building effective factorial codes consists of the following properties of permutations:

– permutation π on a set of M elements is defined as a bijective function from the set X of cardinality M to itself. Elements of a finite set X are denoted by integers from 0 to $M-1$. Then $X=\{0,1,\ldots,M-1\}$, and we will write a permutation π in the form of a sequence of elements of the set X, where each of the numbers $\{0,1,\ldots,M-1\}$ is applied only once;

– the total number of permutations is equal to $M!$;

– the order of integers $\{0,1,\ldots,M-1\}$ in a permutation π is determined by a transferred information – a data block $A(x)$;

– the sum of the numbers forming a permutation π is equal to $\sigma=0.5\cdot M\cdot(M-1)$.

Given these properties, in [12–16] a number of factorial codes were proposed and their main properties were determined. Among them, we note a factorial code with data recovery by permutation [14], which is the base for the problems solved in this work. FCDR has the following properties:

– checking by the receiving station the fact of the presence in a received sequence of bits of each of the symbols $\{0,1,\ldots,M-1\}$ exactly once ensures detection of all errors of odd multiplicity and a part of errors of even multiplicity, such that create repetitions of symbols and their omissions, i.e. transform the transferred permutation to a non-permutation;

– when choosing M so that $M!\geq 2^k$, creation of replacement tables provides the possibility of bijective mapping of sets $\{A(x)\}\leftrightarrow\pi\leftrightarrow\{R(x)\}$, where $R(x)$ is an n-bit permutation on a set of M elements represented in the binary numeral system (carrier of k-bit word $A(x)$ of source);

– if replacement tables are kept secret, the interception of permutations, carriers of information, by the adversary does not allow reading the transmitted message;

– only 2^k from the full set of $M!$ permutations are used for coding/decoding. The remaining $M!-2^k$ permutations are not used by the code and are redundant. This allows to receiving station detecting errors due to the transformation of the transmitted permutation into permu-

DOI 10.15588/1607-3274-2019-4-18

tations of the unused part of the permutations set. From this it follows that FCDR does not detect only transformations of the permutation, carrier of the transferred sample, into

– another permutation of the allowed part of the set;

– counting an sum in a sliding window of M symbols provides the possibility of finding such a position of the window borders, at which this sum is equal to $\sigma = 0.5 \cdot M \cdot (M-1)$. This position of the window borders corresponds to the in-phase condition of transmitting and receiving stations, i.e. the establishment of frame synchronization of 'transmitter-receiver' tract.

Detection of all errors of odd multiplicity and a part of errors of even multiplicity [12] allows to effectively use factorial codes in data systems with DF, i.e. in systems where error detection is performed by code methods and correction (with zero aperture) is performed by repeated questioning and retransmission of a data block damaged by errors.

In turn, the use of request for error correction leads to the fact that the delivery time of a data block is a random variable. It depends on the intensity of noise in a communication channel and, consequently, on a number of requests of data blocks received with an error. Given these properties, DF systems are effective in non real-time telecommunication systems and cannot be used in real-time telecommunications systems. Such systems, in particular, include voice communication systems organized in an open for general access information transfer environment, for example, in overhead or cable lines, in radio links of any frequency range, etc.

Thus, the listed properties of factorial codes allow building data transmission systems where error correction is performed by requesting data blocks received with an error, but excludes the possibility of their use in real-time speech transmission systems.

3 MATERIALS AND METHODS

First, we will define the main parameters of digitized speech.

It is well known that the main formants of the speech signal are in the range of $\Delta F = 4000\,Hz$. Therefore, according to Kotelnikov's theorem, the speech sampling rate is $F_{discr} \geq 8000\,Hz = 8000\,samples/\sec$, and the sampling interval (the interval between two adjacent samples) is $\tau_{discr} \leq 125\mu s$. The dynamic range of the reproduced speech is at least 40 dB. It follows that the ADC resolution must lie within $n_{ADC} = (13 \div 15)$ to obtain the necessary dynamic range.

Note that the choice of ADC with $n_{ADC} = (13 \div 15)$ corresponds to common practice. We take $n_{ADC} = 15$ as a means of ensuring a better quality of speech reproduction. It follows that to satisfy the condition $M! \geq 2^k$, it is necessary to choose $M \geq 8$. To ensure minimal redundancy, we take $M = 8$. With uniform coding of permutation symbols on a set of cardinality of $M = 8$, the number of bits in each of the symbols is equal to $l_r = 3$. Then the permutation, carrier of a 15-bit sample, will contain $n = l_r \cdot M = 24$ bits, which corresponds to the code rate $\nu = k/n = 0.625$.

We take into account that each sample in a DTS is coded with 8 bits. Therefore, a data transmission rate in a communication line (data linear rate) is equal to $B_{DTS} = F_{discr} \cdot n_{ADC} = 8 \cdot 10^3 \cdot 8 = 64\,Kbit/\sec$. A digital channel with such parameters is called PDC and is the basis of all DTS. With factorial coding, each sample is coded with 24 bits (which is 3 times more than in PDC). So the data linear rate with factorial coding will also be 3 times higher and equal to $B_F = F_{discr} \cdot n = 8 \cdot 10^3 \cdot 24 = 192\,\text{Kbit}/\sec$. An increase in linear rate during factorial coding is a charge for providing integrated information security. Note that if you set the task to provide integrated protection in the end-to-end speech path based on PDC by traditional means, you will have to enter some kind of convolutional error correction code [21–25] with a coding rate (1/2–1/3), as well as use redundancy for providing frame synchronization in a continuous stream of samples. Therefore, it is very likely that the provision of integrated protection in such a tract may require more redundancy than is required in this case. In addition, in PDC, unlike a channel with factorial coding, non-linear compounding is used for coding a speech sample with 8 bits. This reduces the quality of the perceived information.

Now we will evaluate a cryptosystem strength to cracking by the brute-force attack.

The process of bijective mapping of sets $\{A(x)\}$ and $\{R(x)\}$, when the mapping law is kept secret, essentially corresponds to the process of encrypting information. The strength of such a cryptosystem is determined by the key space cardinality. If a replacement table gives the law of sets mapping, the key space cardinality is determined by the cardinality of the set of replacement tables. The redundancy of FCDR (that is equal to $M! - 2^k$ permutations) provides the possibility of creating different permutations (differing from each other in composition and the order of their placement in table). In the problem considered in this paper, the key space cardinality is equal to $\mu_{key} = C_{M!}^{2^k} \cdot (2^k!)$, where the factor $C_{M!}^{2^k}$ determines the key space cardinality due to the change in composition of permutations in the replacement table, and $2^k!$ is the key space cardinality due to the permutation of rows in the replacement table. The presented equality allows determining the cryptosystem strength to its cracking by the brute-force attack, a sequential search of all possible keys of the set μ_{key}. In particular, when $M = 8$, $k = 15$ we get $\mu_{\text{key}} = C_{8!}^{2^{15}} \cdot (2^{15}!) = 7.34 \cdot 10^{142176}$.

DOI 10.15588/1607-3274-2019-4-18

Suppose that the enumeration of keys is performed by a computing unit with a performance of $P_w = 10^{10}$ *keys* / sec. In this case, the time spent on enumerating all the keys of the key space will be $t = \mu_{key} / P_w = 7.34 \cdot 10^{142166}$ sec or $2.33 \cdot 10^{142159}$ years.

Suppose that the performance of the computing unit is increased by 5%, 10% or 15% annually. Then, in accordance with [26], the time spent on enumerating all the keys of the key space μ_{key} taking into account the increase in performance of the computing unit will be

$$Y(5\%) = \log_{\left(1+\frac{5}{100}\right)}\left[\frac{5 \cdot 7.34 \cdot 10^{142166}}{100 \cdot 10^{10} \cdot 365 \cdot 24 \cdot 60 \cdot 60} + 1\right],$$

$$= 6.71 \cdot 10^{6} \; years$$

$$Y(10\%) = 3.43 \cdot 10^{6} \; years,$$

$$Y(15\%) = 2.34 \cdot 10^{6} \; years.$$

The obtained values of strength to the brute-force attack of a voice communication cryptosystem based on data factorial coding make it possible to determine the sufficiency (or insufficiency) of security measures taken.

It should be noted that the FCDR property to ensure the constancy of permutation symbols sum, regardless of the information being transferred, makes it possible to find permutations boundaries in their continuous flow. From the point of view of ensuring the speech exchange security, this property creates the vulnerability of voice communication cryptosystems due to the easy establishment of frame synchronization by an adversary receiver. It is possible to significantly complicate for an adversary the solution of messages interception. To do this, it is enough to perform a bits permutation in a permutation π, carrier of a sample of a speech signal, according to the hidden (from an adversary) rule. This, in essence, denotes the addition of factorial coding system with a second encryption circuit.

Let us now proceed to the basic principles of error correction.

Note that error correction methods with a nonzero aperture are determined by the object to be reconstructed. In this context, it is possible to operate either with speech signal samples or with their permutation-carriers. In any case, to recover the permutations (or samples) deformed by errors, we will use not algebraic, but probabilistic error correction methods. These methods provide the maximum probability of identifying the received permutation (or the sample itself) with their true values. However, different objects of reconstruction require different statistical information about the properties of an error stream in a communication channel and a sensitivity of objects of reconstruction to these factors. This fact determines the difference from each other of the methods of decoding permutations and samples, as well as the composition of the operations performed and the results of their application, including a decoding noise level. Therefore, the main task being solved is decoding noise assessment for different information recovery algorithms. In general, approaches to reconstructing permutations or samples are reduced to replacing a permutation or sample deformed by errors with a most likely permutation or sample.

Now we will consider and analyze two methods for recovering permutations: in the Hamming metric and by linear interpolation.

The essence of the method for recovering permutations in the Hamming metric consists of comparing the permutation received from a communication channel with each of the permutations of the replacement table. For this purpose, Hamming distances from the received sequence are determined to all signal vectors used to transfer information. The result of this operation is to create a catalog of distances between the received *n*-bit sequence $R^{\wedge}(x)$ and each of the signal vectors $R_i(x)$ of the replacement table. This corresponds to the operation:

$$d(i) = R^{\wedge}(x) + R_i(x),$$

$i \in \left[0, 2^k - 1\right]$.

If we consider that $R^{\wedge}(x) = R(x) + \varepsilon(x)$, then we get $d(i) = R(x) + \varepsilon(x) + R_i(x)$ as a result. From this, it follows that with a sequential enumeration of the signal vectors $R_i(x)$ the moment inevitably comes when $R_i(x) = R(x)$ and $d(i) = \varepsilon(x)$. This means that an *n*-bit error vector $\varepsilon(x)$, which damaged the permutation $R(x)$, is necessarily present in a distance catalog.

Thus, a distance catalog can be interpreted as a catalog of error vectors that transform the transferred permutation into a received *n*-bit sequence. Among this set (with a cardinality of 2^k vectors) a real error vector is necessarily present. Now we take into account that with independent bit errors in a block of *n* bits, the probability of an error of a given weight (multiplicity of bit errors in a permutation) obeys the binomial law: $p(t) = C_n^t p_0^t q_0^{n-t}$, $q_0 = 1 - p_0$. In this case, error vectors with small multiplicity are the most likely (if an expected value of a discrete random variable $np_0 \le 1$). It follows that the permutation choosing from the replacement table by the criterion of the minimum distance to the vector of the table is equivalent to the choosing of the most probable noise vector. Based on this, permutations of the minimum distance are selected from the distance catalog and are entered into a catalog of candidates for replacement of the permutation received with an error.

If the minimum distance is provided only to one signal vector, then the received sequence is identified with the permutation corresponding to the given signal vector. A sample is recovered from it and is given to a user.

DOI 10.15588/1607-3274-2019-4-18

If there are at least two signal vectors $R_i(x)$ with the same minimum distance to the received sequence $R^{\wedge}(x)$, then the samples corresponding to these signal vectors are taken as candidates for replacement of the received sequence. The best candidate for replacing a sample received with an error is the closest, in Euclidean space, sample from the list of candidates in relation to the previous sample given to the user. If such a sample is one, then it is taken as a decoded sample. If there are several such samples, then one of the candidates for replacement is chosen randomly as a decoded sample.

The recovering procedure is complete.

The listed operations and the order of their execution ensure the achievement of the following result:

– an increase in the accuracy of speech signal recovery, since all (without exception) permutation, samples carriers, taken with error and detected by the code are subject to correction (with a finite degree of accuracy);

– the possibility of working in real-time is ensured by eliminating the need to request samples received with an error.

The method for recovering permutations by linear interpolation involves:

– selecting permutations in which decoder did not detect errors;

– extracting samples contained in permutations;

– selecting a packet of permutations with detected errors;

– recovering samples by the method of linear interpolation based on the obtained values of samples corresponding to the permutations framing the packet of permutations with detected errors, and the number of permutations in this packet.

To implement this method, an *n*-bit sequence received from a communication channel is checked for correctness. If the results of correctness verification establish that the received sequence is a permutation, then it is checked for belonging to the used subset of permutations (the set of signal vectors). If this check is positive, a sample is retrieved from the permutation obtained. This sample is written to the shift register of the device for recovering erroneous samples, containing N cells of $(k+1)$-bit words. In this case, k bits are retracted to store a sample or to store the current sequence number in a packet of permutations received with an error; and the $(k+1)$-th bit is an indicator defining the storage object in a memory cell.

The first permutation received with an error has the number 1, and the last permutation received with an error has a number corresponding to the length of the packet of signal vectors received with an error.

This allows to identify packets of permutations with detected errors and to recover samples of this packet immediately upon detection of the packet. Sampling recovery is reduced to replacing the $(k+1)$-bit word in the register with the recovered sample and, accordingly, the indicator bit.

As a result, when outputting the contents of the buffer register to the information consumer, the corrected sample stream is output. The service bit follows it. This means that, in contrast to the samples recovery in the Hamming metric, the interpolation method introduces an additional delay corresponding to the accumulation time of N samples. The value of this delay (and, therefore, the length of the package of corrected errors) is determined by several factors. First, we note that this delay should not exceed the speech correlation interval, since error correction by interpolating uncorrelated samples is meaningless. Considering that the speech autocorrelation interval is approximately 0.5 seconds [27, 28], then $N \le 4000$. In reality, the value of N should be substantially less and be determined by the frame synchronization system parameters and properties. This is because frame synchronization of systems with factorial coding is performed by selecting the time position in the window of M symbols. Their sum is $\sigma = 0.5 \cdot M \cdot (M-1)$.

It is obvious that both in the process of searching for synchronism and in the process of its retention within a window of M symbols, there can be both correctly and incorrectly accepted permutations. Therefore, the decision on the achievement or loss of synchronism must be made based on a majority decision, a decision on a majority vote. This number of votes may be different for determining the moment of achieving synchronism in the search (k_{in}) and for determining the moment of loss of synchronism (k_{out}). If the number of errors in the packet exceeds the value of k_{out} in the window of N permutations, then the frame synchronization system will perceive this event as a loss of the clock phase, stop decoding samples, and go into synchronization search mode. From this, it follows that the boundary number of signal vectors N accepted with an error corrected by the interpolation method must satisfy condition $N \le k_{out}$.

Note that a similar situation occurs when correcting errors in the Hamming metric. If the length of the permutation packet received with a detected error exceeds the synchronization system value k_{out}, then the event of clock synchronization loss will be fixed and the transition to the clock phase search mode will occur. Thus, any of the considered methods of speech signal recovery is aimed at correcting errors in the packet of permutations with the length that does not exceed the value of k_{out}. Usually $k_{out} \le 10$ in systems of multiple access with time division of channels.

4 EXPERIMENTS

A software model with tract "speech source – voice encoder – communication channel – speech decoder – speech receiver" has been developed to assess the main technical characteristics of the proposed above methods for recovering samples deformed by noise in a communication channel. The model provides an assessment of the speech tract basic parameters: the probability of error

DOI 10.15588/1607-3274-2019-4-18

detection/non-detection by FCDR decoder, an estimate of the value of sample recovery error. Based on these data, decoding noise power and speech signal security are determined. The main result of the experiment for determining the noise accompanying the decoded speech is the dependence between decoder SNR by (1) and BEP in a communication channel. The model used FCDR with parameters $M = 8$, $k = 15$, $n = 24$, $\nu = 0.625$.

The first version of the codec model implements the decoding algorithm in the Hamming metric. Fig. 1 illustrates a block diagram of such receiving device.

First, we note that binary sequences of digitized speech signal samples transmitted over a communication channel with noise are distorted at a channel output. The fronts of individual packets are randomly shifted from their nominal position; as a result, the duration of packets is a random variable. Therefore, first, it is necessary to restore the time relationship between the elements of a signal, the packets. For this, pre-processing, regeneration, is performed. For this purpose, the receiver contains a clock synchronization system 8. This system ensures synchronization between receiver and transmitter clock generators. Regenerator 1 strobes (polls) the received binary symbol in the least noise susceptible part, in its middle, with synchronous clock cycles. Then regenerator 1 stores it until the next strobing moment. This ensures maximum reliability of bit sequence reception and restores time ratios of packets in their continuous sequence. As a result, a sequence of bits is formed at the output of the regenerator 1. It may contain errors due to the effect of noise in a communication channel at the time of strobing. This sequence is fed to the input of a frame synchronization system 9 and to the input of a selector 2. The frame synchronization system 9 counts in a sliding window the sum of M symbols of the received permutation. If this sum is equal to $\sigma = 0,5 \cdot M \cdot (M-1)$, then, most likely, the permutation boundary is correctly defined; and if not, then, most likely, it is not defined correctly. The clause 'most likely' says that it is impossible to make a decision on the establishment (or loss) of the clock phase in one observation since the sum of symbols in a window is a random value under the influence of noise. The decision can be made on the basis of calculating an expectation of this random process or in the case when most of the samples confirm or refute one of the hypotheses on an observation interval (synchronism is established or synchronism is lost). When a cycle synchronism state is reached, the receiver proceeds to process a sequence of permutations received from a channel carrying speech signal samples. A sample received from a channel and recorded in the selector 2 is checked for correctness. If the received sequence is correct, i.e., it is a permutation, then it is issued to decoder 3 via bus 1. The decoder 3 determine if the permutation belongs to the allowed set of the replacement table. If this check has a positive result, a corresponding sample is extracted from the permutation and sent to the recipient via bus 1 of decoder 3 through connection block 7.

If the received permutation is not contained in the replacement table, i.e., belongs to the non-allowed part of the permutations set, then it is fed via bus 2 of decoder 3 to the first input of the first connection block 4. To the second input of the first connection block 4 the output of selector 2 is connected via bus 2.

As a result, n-bit words of non-permutations and permutations from the non-allowed part of the permutations set are fed to the input of a distance catalog former 5.

The distance catalog former 5 determines Hamming distances between the permutation received from communication channel and each of the permutations of the replacement table. The distance catalog is output to an error correction block 6. In this block, the permutation list is arranged, for example, in the order of decreasing the distance. Permutations with the minimum Hamming distance are separated into a separate list. This list is a list of candidates for replacement received with an error permutation.

If there is only one candidate permutation in this list, then a sample is extracted from it. This sample is output to the consumer through the second connection block 7.

If there are several candidates for a replacement, a sample is extracted from each of them. As a result, a list of candidates for replacement of the sample is formed. A previous sample is extracted from the decoder's memory. An arithmetic difference of the amplitudes of the previous sample and each candidate sample is calculated. The candidate sample with the minimum amplitude difference value is taken as the most probable value of the transmitted sample. It is fed to the consumer. This completes the error correction procedure. The decoder goes into standby mode to receive the next permutation from communication channel. The decoding process is repeated according to the above algorithm.

Decoding of factorial code with recovery of samples received with an error by interpolation is performed using a device, which block diagram is shown in Fig. 2.

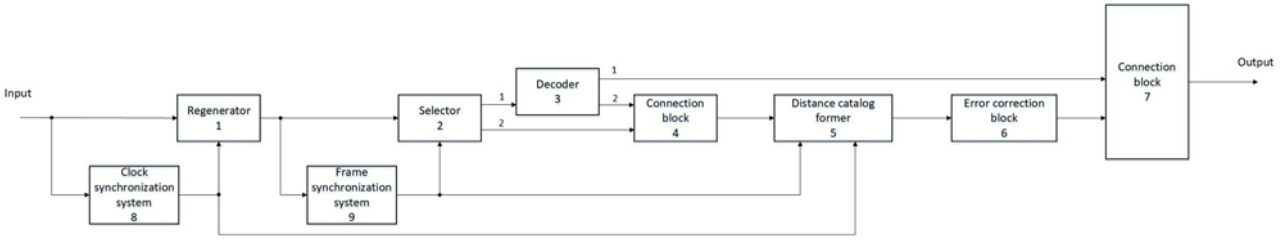


Figure 1 – The block diagram of speech signal receiving device with permutations recovery in the Hamming metric

DOI 10.15588/1607-3274-2019-4-18

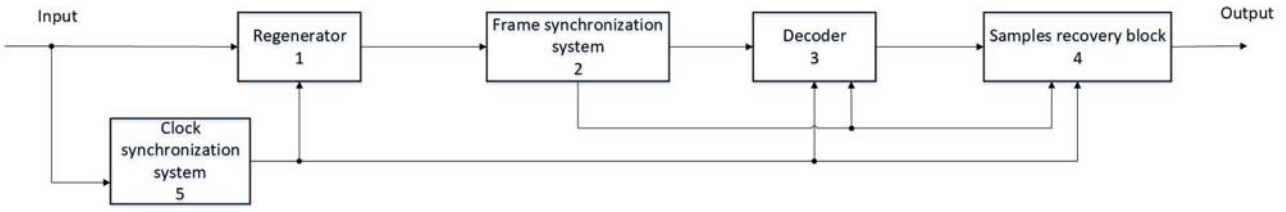


Figure 2 – The block diagram of speech signal receiving device with permutations recovery by interpolation

The receiving device contains a clock synchronization system 5, a regenerator 1, and a frame synchronization system 2, which in this device are made identically with the same device blocks in the Hamming metric and perform the same functions.

After the frame synchronization procedure is completed, 24-bit sequences received from a channel are input to the decoder 3. Decoder 3 performs a validation of the received permutation.

If the received sequence is a signal vector, a sample, a word of 15 bits, is extracted from it. The 16th service bit that is an indicator of the contents of this memory cell is added to the sample (for example, a logical zero).

If the received sequence is not a permutation or a permutation not used for transferring voice information, a word of 15 bits representing the sequence number in a packet of permutations received with errors is entered into the memory cell instead of a sample. The 16th service bit, a content indicator of the memory cell, is assigned to the binary one.

Thus, if several consecutive permutations affected by errors are received, the last number will determine the length of error packet N. This sequence of 16-bit words from the output of the decoder 3 is transmitted to a samples recovery block 4 for correcting error packets. A block diagram of the block 4 is shown in Fig. 3.

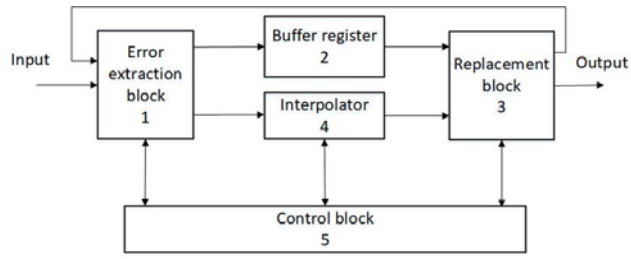


Figure 3 – The block diagram of a samples recovery block

The words coming from the decoder get into the error extraction block 1. The main purpose of this block is to extract the following three words from an incoming stream: samples $A_j^{\wedge}$ and $A_{j-(N+1)}^{\wedge}$ that frame a packet of errors and an error packet length indicator N.

From this data, an interpolation step $\Delta = \left(A_j^{\wedge} - A_{j-(N+1)}^{\wedge}\right) \Big/ (N+1)$ is calculated and transferred to interpolator 4. Thus, after receiving the first permutation without detected error that closes a packet of permutations with detected errors, the values $A_j^{\wedge}$, $A_{j-(N+1)}^{\wedge}$, N, and Δ are loaded into the interpolator 4. This allows to start an interpolation procedure, a procedure for calculating and replacing samples that correspond to error-corrupted permutations. To do this, the procedure of replacing the contents of the cell with a 15-bit word of the recovered sample is performed in the replacement block 3, in the interval between two samples (equal to 125 microseconds), as well as changing a service symbol from a binary one to zero.

Control block 5 controls this process.

Calculating the restored sample involves performing operation $A'_{j-(N+1-i)} = A'_{j-(N+1)} + [i\Delta]$, where $[A]$ denotes rounding to the nearest integer of A.

Thus, the proposed algorithm for the samples recovery using the linear interpolation method ensures the correction of a packet of errors due to the effect of noise in a communication channel with finite accuracy. This means that a decoded speech will be accompanied by additional decoding noise. The presence of decoding noise with a level from minus 30 dB to minus 50 dB corresponds to conditions for speech transmission in an environment with natural noise.

5 RESULTS

The developed software models allow to change the nature of noise in a communication channel. The simulation of voice information transmission for channels with independent bit errors and channels with multiple bit errors caused by multiplicative noise has been performed in order to determine the main parameters of the proposed methods of speech signals factorial coding. The source used a fixed sample of a real speech signal.

The channel model with independent bit errors used a binomial law of their distribution with one parameter p_0.

The channel model with multiple errors used a Gilbert-Elliott model [29, 30]. This model assumes two channel states, ‘good’ and ‘bad’. The law of channel states changing is described by a Markov chain of order one. The simulation was performed for cable channels. In this case, an absolute (average) BEP [31, 32] $p_0 = \left(P_{bg} \Big/ \left(P_{bg} + P_{gb}\right)\right) \cdot p_{0g} + \left(P_{gb} \Big/ \left(P_{bg} + P_{gb}\right)\right) \cdot p_{0b}$ was used to estimate the decoding methods under conditions of multiple errors caused by multiplicative noise.

The results of testing of two models of factorial code decoder show the decoder SNR depending on BEP in communication channel and the nature of noise. Fig. 4–6 graphically illustrates the test results.

DOI 10.15588/1607-3274-2019-4-18

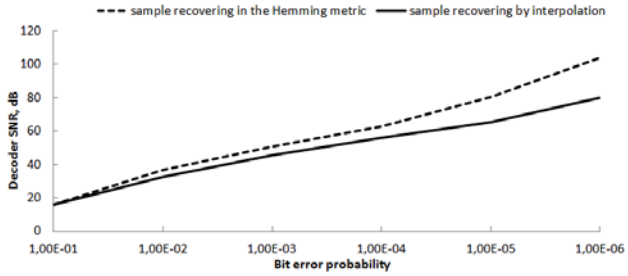


Figure 4 – Decoder SNR vs BEP in channels with independent bit errors

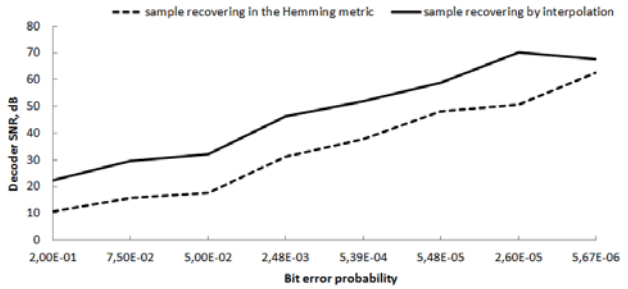


Figure 5 – Decoder SNR vs BEP in channels with multiple errors caused by multiplicative noise

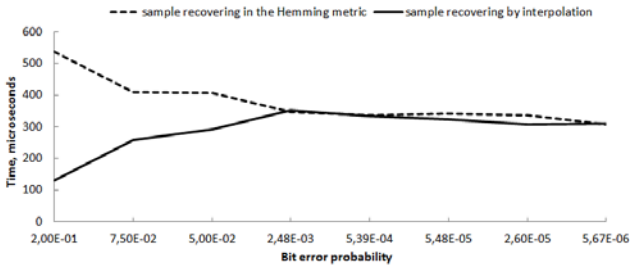


Figure 6 – Graph of average time of samples recovery vs BEP

6 DISCUSSION

It can be concluded, from the above graphs, that each of the decoding methods is oriented to different types of channels in their statistical properties of error appearing.

From Fig. 4, it can be seen that SNR of decoder with samples recovery in the Hamming metric is higher than SNR of decoder with samples recovery by interpolation in the whole range of BEP values in a communication channel with independent bit errors. Channels organized in underground cable lines including fiber-optic belong to this category. It also includes microwave radio lines operating in favorable weather conditions and without applying electronic countermeasures to them.

In turn, from Fig. 5, it can be seen that decoder with samples recovery by interpolation is oriented to channels with multiple bit errors and provides a greater level of SNR in comparison with decoder in the Hamming metric. Radio channels of the short-wave range in normal conditions and radio channels of any radio-frequency range in the conditions of electronic countermeasures can be referred to this category of channels.

We would like also to point out that the sample recovering procedure by interpolation is simpler to implement and requires fewer resources than the recovery in the Hamming metric. From Fig. 6 it can be seen that the performance of decoder with samples recovery by interpolation is significantly higher when $10^{-3} < p_0 \le 10^{-1}$. With the improvement of a channel quality, mostly single errors increasingly begin to occur and the performance of both algorithms becomes identical.

It should be noted that the noise accompanying the recovered speech signal using the recovery algorithm in the Hamming metric for channels with independent errors and the interpolation method for channels with multiple bit errors can be categorized as comfort noise for $10^{-4} \le p_0 \le 10^{-2}$. Decoding noise can be ignored when improving the quality of communication channel.

It follows from this that the threshold value of the transmission reliability at which the specified quality indicators are ensured in terms of the decoding noise level is $p_0 \le 10^{-2}$.

Note also that the proposed coding methods provide better SNR for high BEP compared with turbo codes [33–36]. For example, turbo codes [36] used in the GSM standard have lower SNR when $10^{-3} < p_0 \le 10^{-2}$.

Finally, we would like to admit that the methods proposed in this research provide a code rate of 0.65. Convolutional codes [21–26] as the most widely used codes in speech coding, have a relatively low code rate of 1/2–1/3. In addition, convolutional codes do not provide cryptographic protection, since it contains information bits in a code sequence.

CONCLUSIONS

The urgent problem of integrated protection against unauthorized access and channel errors of real-time speech signals based on factorial coding is solved.

The scientific novelty of obtained results is that two methods of factorial coding of speech information with permutations recovery are firstly proposed. These methods involve converting, for example, by substitution table, samples of speech information into permutations. These permutations after encoding to a binary code are transmitted over a communication channel. The decoding process is to replace a permutation to a speech signal sample. In the case of damage of the received permutation, according to the first method for recovering permutations in the Hamming metric, speech signal is restored by finding the signal vector closest to the permutation in the Hamming metric. If there are several such signal vectors, then one which sample is closest in Euclidean metric to the predecoded sample is selected. The method for recovering permutations by linear interpolation involves restoring a speech signal by linear interpolation based on known adjacent samples. These methods allow to detect and correct errors in real-time with non-zero aperture. This in turn allows using factorial coding for real-time data. The strength to cracking of the protection system by brute-force attack is estimated in millions of years.

The practical significance of the research is that the algorithms and block diagrams of speech signal receiving devices have been developed. This allows their practical

DOI 10.15588/1607-3274-2019-4-18

implementation. 2. The experimental results show that an optimal area of application of the method for recovering permutations in the Hamming metric is communication channels with independent bit errors and BEP $p_0 \le 10^{-2}$. Under these conditions, the Hamming decoder shows the best results, and the decoding noise does not exceed the values of the comfort noise level. An optimal area of use of the method for recovering permutations by linear interpolation is communication channels with multiple bit errors caused by multiplicative noise, in particular, radio channels of the short-range radio band or radio channels of any radio band with an unfavorable noise situation. When using the proposed algorithms in optimal conditions with the BEP $p_0 \le 10^{-2}$, the decoding noise level does not exceed the values of the comfort noise level.

Prospects for further research are to study the effectiveness of the proposed methods in real-world conditions by developing prototype devices.

ACKNOWLEDGEMENTS

The authors express their sincere appreciation to Dc.Sc. Techn., Professor Volodymyr Rudnytskyi and Ph.D., Associate Professor Anatoly Shcherba for the full support of this area of work, constructive comments and suggestions when writing the work, and useful discussion of the results.

REFERENCES

1. Gnatyuk S. Critical Aviation Information Systems Cybersecurity, *Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security*, 2016, Vol. 47, No. 3, pp. 308–316. DOI: 10.3233/978-1-61499-716-0-308
2. Gnatyuk S., Kinzeryavyy V., Kyrychenko K. et al. Secure Hash Function Constructing for Future Communication Systems and Networks, *Advances in Intelligent Systems and Computing*, 2019, Vol. 902, pp. 561–569. DOI: 10.1007/978-3-030-12082-5_51
3. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Theory, *The Deep Space Network Progress Report, DSN PR 42–44,* 1978, pp. 114–116.
4. Osmolovskij S. A. Stoxasticheskaya informatika: innovacii v informacionnyx sistemax. Moscow, Goryachaya liniya-Telekom, 2012, 321 p.
5. Stakhov A. P., Massingue V., Sluchenkova A. Introduction into Fibonacci Coding and Cryptography. Kharkov, Osnova, 1999, 234 p.
6. Stakhov A. P. Fibonacci Matrices, a Generalization of the 'Cassini Formula', and a New Coding Theory, *Chaos, Solitons & Fractals*, 2006, Vol. 30, No. 1, pp. 56–66. DOI: 10.1016/j.chaos.2005.12.054
7. Stakhov A. P. .: The 'Golden' Matrices and a New Kind of Cryptography, *Chaos, Solitons & Fractals*, 2007, Vol. 32, No. 3, pp. 1138–1146. DOI: 10.1016/j.chaos.2006.03.069
8. Mazurkov M. I., Chechel'nitskii V. Ya., Murr P. Information security method based on perfect binary arrays, *Radioelectronics and Communications Systems*, 2008, Vol. 51, No. 11, pp. 612–614. DOI: 10.3103/S0735272708110095
9. Mazurkov M. I., Chechelnytskyi V. Ya., Meleshkevich A. N. et al. Methods of improving information security by integrating multiplexing, ciphering and channel encoding operations, *Radioelectronics and Communications Systems*, 2011, Vol. 54, No. 5, pp. 227–240. DOI: 10.3103/S0735272711050013
10. Mazurkov M. I. Composite matrix cipher based on perfect binary arrays, *Radioelectronics and Communications Systems,* 2013, Vol. 56, No. 3, pp. 133–140. DOI: 10.3103/S0735272713030047
11. Borisenko A. A., Gorjachev A. E., Lopatchenko B. K. et al. Perestanovki v telekommunikacionnyx setyax, *Visnik Sums'kogo derzhavnogo universitet*u, 2013, No. 2, pp. 15–22.
12. Faure E. V., Shvydkyi V. V., Shcherba A. I. Information integrity control based on the factorial number system, *Journal of Baku engineering university – Mathematics and computer science*, 2017, Vol. 1, No. 1, pp. 3–13.
13. Faure E. V., Shvydkyi V. V., Shcherba V. O. Combined factorial coding and its properties, *Radio Electronics, Computer Science, Control,* 2016, No. 3, pp. 80–86. DOI: 10.15588/1607-3274-2016-3-10
14. Faure E. V. Faktorial'noe kodirovanie s vosstanovleniem dannyx, *Visnyk Cherkas'kogo derzhavnogo tehnologichnogo universytetu*, 2016, No. 2, pp. 33–39. DOI: 10.24025/bulletinchstu.v1i2.82932
15. Faure E. V. Factorial coding with error correction, Radio Electronics, Computer Science, Control, 2017, No. 3, pp. 130–138. DOI: 10.15588/1607-3274-2017-3-15
16. Faure E. V., Shcherba A. I., Kharin A. A. Factorial Code with a Given Number of Inversions, Radio Electronics, Computer Science, Control, 2018, No. 2, pp. 143–153. DOI: 10.15588/1607-3274-2018-2-16
17. Marsaglia G. DIEHARD battery of tests of randomness [Electronic resource]. Access mode: http://www.stat.fsu.edu/pub/diehard
18. Rukhin A., Soto J., Nechvatal J. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: Spec. Pub. 800–22 rev. 1a, National Institute of Standards and Technology. Gaithersburg, MD, 2010, 153 p.
19. L'ecuyer P., Simard R. TestU01: A C Library for Empirical Testing of Random Number Generators, *ACM Transactions on Mathematical Software*, 2007, Vol. 33, No. 4, 40 p. DOI: 10.1145/1268776.1268777
20. Faure E. V., Shcherba A. I., Rudnytskyi V. M. The Method and Criterion for Quality Assessment of Random Number Sequences, *Cybernetics and Systems Analysis,* 2016, Vol. 52, pp. 277–284. DOI: 10.1007/s10559-016-9824-3
21. Hagelbarger D. W. Recurrent codes: Easily Mechanized, Burst-Correcting, Binary Codes, The Bell System Technical Journal, 1959, Vol. 38, Issue 4, pp. 969–984. DOI: 10.1002/j.1538-7305.1959.tb01584.x
22. Hagelbarger D. W. Error Detection Using Recurrent Codes, *AIEE Winter General Meeting.* New York, 31 January–5 February 1960. : Proceedings. – New York, IEEE, 1960.
23. Pereira F., Guardia G., Assis F. Classical and Quantum Convolutional Codes De-rived from Algebraic Geometry Codes, *IEEE Transactions on Communications,* 2019, Vol. 67, No. 1, pp. 73–82. DOI: 10.1109/TCOMM.2018.2875754
24. Yang Q., Liew C. Asynchronous Convolutional-Coded Physical-Layer Network Coding, *IEEE Transactions on Wireless Communications*, 2015, Vol. 14, No. 3, pp. 1380–1395. DOI: 10.1109/TWC.2014.2365822
25. Nooraiepour A., Duman T. M. Randomized Convolutional Codes for the Wiretap Channel, *IEEE Transactions on*

DOI 10.15588/1607-3274-2019-4-18

Communications, 2017, Vol. 65, No. 8, pp. 3442–3452. DOI: 10.1109/TCOMM.2017.2704586
26. Lavdanskyi A. O. Time assessment of formation of number sequences under increase of calculation unit performance, *The scientific potential of the present: International Scientific Conference, St Andrews, Scotland, United Kingdom, 1 December 2016 : proceedings*. St Andrews, Scotland, United Kingdom, 2016, pp. 123–126.
27. Rabiner L. R., Schafer R. W. Introduction to Digital Speech Processing. Delft, now Publishers Inc., 2007, 200 p. DOI: 10.1561/2000000001
28. Wang L., Doclo S. Correlation Maximization-Based Sampling RateOffset Estimation for Distributed Microphone Arrays, *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 2016, Vol. 24, No. 3, pp. 571–582. DOI: 10.1109/TASLP.2016.2517326
29. Gilbert E. N. Capacity of a Burst-Noise Channel / E.N. Gilbert // *Bell System Technical Journal*, 1960, Vol. 39, Issue 5, pp. 1253–1265. DOI: 10.1002/j.1538-7305.1960.tb03959.x
30. Elliott E.O. Estimates of Error Rates for Codes on Burst-Noise Channels, *Bell System Technical Journal*, 1963, Vol. 42, Issue 5, pp. 1977–1997. DOI: 10.1002/j.1538-7305.1963.tb00955.x
31. Hasslinger G., Hohlfeld O. The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet, *Measurement, Modelling and Evalutation of Computer and Communication Systems: 14th GI/ITG Conference, Dortmund, Germany, 31 March – 2 April 2008 : proceedings*, VDE VERLAG, 2008.
32. Ellis M., Pezaros D. P., Kypraios T. et al. Modeling of packet loss and delay and their effect on real-time multimedia service quality, *Computer Networks*, 2014, Vol. 70, pp. 384–399. DOI: 10.1016/j.comnet.2014.05.013
33. Heegard C. Turbo Coding / C. Heegard, S.B. Wicker. – Norwell: Kluwer Academic Publishers, 1999. – 476 p. DOI: 10.1007/978-1-4757-2999-3
34. Weithoffer S., Nour C. A., When N. et al. 25 Years of Turbo Codes: From Mb/s to beyond 100 Gb/s, *Turbo Codes and Iterative Information Processing: 10th IEEE International Symposium, Hong Kong, China, 3–7 December 2018 : proceedings.* IEEE Computer Society, 2018. DOI: 10.1109/ISTC.2018.8625377
35. Babar Z., Chandra D., Nguyen H. V. et al.] Duality of quantum and classical error correction codes: Design principles and examples, *IEEE Communications Surveys and Tutorials*, 2019, Vol. 21, Issue 1, pp. 970–1010. DOI: 10.1109/COMST.2018.2861361
36. Panayiotis D. P., Thomas A. S., Prabodh V. et al. Turbo Coded Modulation over GSM Channels, *Third Generation Wireless and Beyond: International Conference, San Francisco, California, 6–8 June 2001, Proceedings.* San Francisco, IEEE, 2001.

Received 19.06.2019.
Accepted 25.09.2019.

УДК 004.75

МЕТОДИ ФАКТОРІАЛЬНОГО КОДУВАННЯ МОВНИХ СИГНАЛІВ

Фауре Е. В. – д-р техн. наук, доцент, проректор з науково-дослідної роботи та міжнародних зв'язків Черкаського державного технологічного університету, Черкаси, Україна.

Швидкий В. В. – канд. техн. наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Лавданський А. О. – канд. техн. наук, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Харін О. О. – аспірант кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

АНОТАЦІЯ

Актуальність. У роботі викладено методи факторіального кодування мовних сигналів, що використовують факторіальний код для забезпечення інтегрованого захисту інформації та підтримки циклової фази розподільників приймання/передавання. Під інтегрованим захистом розуміється захист інформації від впливу завад у каналі зв'язку і спроб несанкціонованого доступу у відкритих телекомунікаційний мережах множинного доступу.

Мета роботи. Метою цієї роботи є забезпечення інтегрованого захисту мовних сигналів реального часу на основі факторіального кодування. Для цього в роботі розроблено методи факторіального кодування мовних сигналів і побудови мовних кодеків, що базуються на властивостях факторіальних кодів утримувати тактовий і цикловий синхронізм за робочим сигналом, виявляти значну частину помилок, обумовлених впливом завад природного походження або створених навмисно, забезпечувати можливість виправлення всіх виявлених кодом помилок зі скінченною точністю, а також забезпечувати криптографічний захист від несанкціонованого прослуховування мовного повідомлення за рахунок приховування закону перетворення вибірок мовного сигналу в сигнал – перестановку.

Метод. Основна ідея запропонованих методів полягає у виборі для перенесення інформації перестановок з певним набором властивостей і ознак, що забезпечують максимальну виявляючу здатність коду, здатність виправлення виявлених кодом помилок і відновлення вибірок мовного сигналу зі скінченним ступенем точності (з ненульовий апертурою).

Результати. Визначено процедури кодування/декодування інформації, що забезпечують виявлення та виправлення на приймальній станції вибірок мовного сигналу з ненульовий апертурою. Викладено результати експериментальної оцінки моделі таких систем під час роботи каналом зв'язку як з незалежними бітовими помилками, так і з пакетуванням помилок. Визначено величину шуму декодування, обумовленого скінченною точністю відновлення прийнятих з помилкою вибірок мовного сигналу, як функції ймовірності помилки в послідовності біт під час передавання інформації каналом зв'язку.

Висновки. Запропоновано методи факторіального кодування мовного сигналу, що забезпечують інтегрований захист інформації і відновлення зі скінченною точністю вибірок мовного сигналу, деформованих завадами в каналі зв'язку. Визначено вимоги до якості каналу зв'язку (до значення ймовірності бітової помилки в каналі зв'язку), за якого забезпечується комфортне сприйняття мови.

DOI 10.15588/1607-3274-2019-4-18

КЛЮЧОВІ СЛОВА: факторіальний код, перестановка, таблиця замін, вибірка мовного сигналу, відновлення вибірок, шум декодування.

УДК 004.75

МЕТОДЫ ФАКТОРИАЛЬНОГО КОДИРОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ

Фауре Э. В. – д-р техн. наук, доцент, проректор по научно-исследовательской работе и международным связям Черкасского государственного технологического университета, Черкассы, Украина.

Швыдкий В. В. – канд. техн. наук, доцент, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Лавданский А. А. – канд. техн. наук, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Харин А. А. – аспирант кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

АННОТАЦИЯ

Актуальность. В работе изложены методы факториального кодирования речевых сигналов, использующие факториальный код для обеспечения интегрированной защиты информации и поддержки цикловой фазы распределителей приема/передачи. Под интегрированной защитой понимается защита информации от воздействия помех в канале связи и попыток несанкционированного доступа в открытых телекоммуникационный сетях множественного доступа.

Цель работы. Целью данной работы является обеспечение интегрированной защиты речевых сигналов реального времени на основе факториального кодирования. Для этого в работе разработаны методы факториального кодирования речевых сигналов и построения речевых кодеков, основанные на свойствах факториальных кодов удерживать тактовый и цикловой синхронизм по рабочему сигналу, выявлять значительную часть ошибок, обусловленных влиянием помех естественного происхождения или созданных искусственно, обеспечивать возможность исправления всех выявленных кодом ошибок с конечной точностью, а также обеспечивать криптографическую защиту от несанкционированного прослушивания речевого сообщения за счет скрытия закона преобразования выборок речевого сигнала в сигнал-перестановку.

Метод. Основная идея предлагаемых методов состоит в выборе для переноса информации перестановок с определенным набором свойств и признаков, обеспечивающих максимальную обнаруживающую способность кода, способность исправления обнаруженных кодом ошибок и восстановления выборок речевого сигнала с конечной степенью точности (с ненулевой апертурой).

Результаты. Определены процедуры кодирования/декодирования информации, обеспечивающие обнаружение и исправление на приемной станции выборок речевого сигнала с ненулевой апертурой. Изложены результаты экспериментальной оценки модели таких систем при работе по каналу связи как с независимыми, так и с пакетирующимися битовыми ошибками. Определена величина шума декодирования, обусловленного конечной точностью восстановления принятых с ошибкой выборок речевого сигнала, как функции вероятности ошибки в последовательности бит при передаче информации по каналу связи.

Выводы. Предложены методы факториального кодирования речевого сигнала, обеспечивающие интегрированную защиту информации и восстановление с конечной точностью выборок речевого сигнала, деформированных помехами в канале связи. Определены требования к качеству канала связи (к значению вероятности битовой ошибки в канале связи), при котором обеспечивается комфортное восприятие речи.

КЛЮЧЕВЫЕ СЛОВА: факториальный код, перестановка, таблица замен, выборка речевого сигнала, восстановление выборок, шум декодирования.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Gnatyuk S. Critical Aviation Information Systems Cybersecurity / S. Gnatyuk // Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. – 2016. – Vol. 47, № 3. – P. 308–316. DOI: 10.3233/978-1-61499-716-0-308
2. Secure Hash Function Constructing for Future Communication Systems and Networks / [S. Gnatyuk, V. Kinzeryavyy, K. Kyrychenko et al.] // Advances in Intelligent Systems and Computing. – 2019. – Vol. 902. – P. 561–569. DOI: 10.1007/978-3-030-12082-5_51
3. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Theory / R. J. McEliece // The Deep Space Network Progress Report, DSN PR 42–44. – 1978. – P. 114–116.
4. Осмоловский С. А. Стохастическая информатика: инновации в информационных системах / С. А. Осмоловский. – М. : Горячая линия-Телеком, 2012. – 321 с.
5. Stakhov A. P. Introduction into Fibonacci Coding and Cryptography / A. P. Stakhov, V. Massingue, A. Sluchenkova. – Kharkov : Osnova, 1999. – 234 p.
6. Stakhov A. P. Fibonacci Matrices, a Generalization of the ‘Cassini Formula’, and a New Coding Theory / A. P. Stakhov // Chaos, Solitons & Fractals. – 2006. – Vol. 30, № 1. – P.56–66. DOI: 10.1016/j.chaos.2005.12.054
7. Stakhov A. P. The ‘Golden’ Matrices and a New Kind of Cryptography / A. P. Stakhov // Chaos, Solitons & Fractals. – 2007. – Vol. 32, № 3. – P. 1138–1146. DOI: 10.1016/j.chaos.2006.03.069
8. Mazurkov M. I. Information security method based on perfect binary arrays / M. I. Mazurkov, V. Ya. Chechel’nitskii, P. Murr // Radioelectronics and Communications Systems. – 2008. – Vol. 51, № 11. – P. 612–614. DOI: 10.3103/S0735272708110095
9. Methods of improving information security by integrating multiplexing, ciphering and channel encoding operations / [M. I. Mazurkov, V. Ya. Chechelnytskyi, A. N. Meleshkevich et al.] // Radioelectronics and Communications Systems. – 2011. – Vol. 54, № 5. – P. 227–240. DOI: 10.3103/S0735272711050013
10. Mazurkov M. I. Composite matrix cipher based on perfect binary arrays / M. I. Mazurkov // Radioelectronics and

DOI 10.15588/1607-3274-2019-4-18

Communications Systems. – 2013. – Vol. 56, № 3. – P. 133–140. DOI: 10.3103/S0735272713030047
11. Перестановки в телекоммуникационных сетях / [А. А. Борисенко, А. Е. Горячев, Б. К. Лопатченко и др.] // Вісник Сумського державного університету. – 2013. – № 2. – С. 15–22.
12. Faure E. V. Information integrity control based on the factorial number system / E. V. Faure, V. V. Shvydkyi, A. I. Shcherba // Journal of Baku engineering university – Mathematics and computer science. – 2017. – Vol. 1, № 1. – P. 3–13.
13. Faure E. V. Combined factorial coding and its properties / E. V. Faure, V. V. Shvydkyi, V. O. Shcherba // Radio Electronics, Computer Science, Control. – 2016. – № 3. – P. 80–86. DOI: 10.15588/1607-3274-2016-3-10
14. Фауре Э. В. Факториальное кодирование с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – № 2. – С. 33–39. DOI: 10.24025/bulletinchstu.v1i2.82932
15. Faure E. V. Factorial coding with error correction / E. V. Faure // Radio Electronics, Computer Science, Control. – 2017. – № 3. – P. 130–138. DOI: 10.15588/1607-3274-2017-3-15
16. Faure E. V. Factorial Code with a Given Number of Inversions / E. V. Faure, A. I. Shcherba, A. A. Kharin // Radio Electronics, Computer Science, Control. – 2018. – № 2 – P. 143–153. DOI: 10.15588/1607-3274-2018-2-16
17. Marsaglia G. DIEHARD battery of tests of randomness [Electronic resource] / G. Marsaglia. – Access mode: http://www.stat.fsu.edu/pub/diehard.
18. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: Spec. Pub. 800-22 rev. 1a / [A. Rukhin, J. Soto, J. Nechvatal et al.] / National Institute of Standards and Technology. – Gaithersburg: MD, 2010. – 153 p.
19. L'ecuyer P. TestU01: A C Library for Empirical Testing of Random Number Generators / P. L'ecuyer, R. Simard // ACM Transactions on Mathematical Software. – 2007. – Vol. 33, № 4. – 40 p. DOI: 10.1145/1268776.1268777
20. Faure E. V. The Method and Criterion for Quality Assessment of Random Number Sequences / E. V. Faure, A. I. Shcherba, V. M. Rudnytskyi // Cybernetics and Systems Analysis. – 2016. – Vol. 52. – P. 277–284. DOI: 10.1007/s10559-016-9824-3
21. Hagelbarger D. W. Recurrent codes: Easily Mechanized, Burst-Correcting, Binary Codes / D. W. Hagelbarger // The Bell System Technical Journal. – 1959. – Vol. 38, Issue 4. – P. 969–984. DOI: 10.1002/j.1538-7305.1959.tb01584.x
22. Hagelbarger D. W. Error Detection Using Recurrent Codes / D. W. Hagelbarger // AIEE Winter General Meeting, New York, 31 January – 5 February 1960 : Proceedings. – New York, IEEE, 1960.
23. Pereira F. Classical and Quantum Convolutional Codes Derived from Algebraic Geometry Codes / F. Pereira, G. Guardia, F. Assis // IEEE Transactions on Communications. – 2019. – Vol. 67, № 1. – P. 73–82. DOI: 10.1109/TCOMM.2018.2875754
24. Yang Q. Asynchronous Convolutional-Coded Physical-Layer Network Coding / Q. Yang, C. Liew // IEEE Transactions on Wireless Communications. – 2015. – Vol. 14, № 3. – P. 1380–1395. DOI: 10.1109/TWC.2014.2365822
25. Nooraiepour A. Randomized Convolutional Codes for the Wiretap Channel / A. Nooraiepour, T. M. Duman // IEEE Transactions on Communications. – 2017. – Vol. 65, № 8. – P. 3442–3452. DOI: 10.1109/TCOMM.2017.2704586
26. Lavdanskyi A. O. Time assessment of formation of number sequences under increase of calculation unit performance / A. O. Lavdanskyi // The scientific potential of the present: International Scientific Conference, St Andrews, Scotland, United Kingdom, 1 December 2016 : proceedings. – St Andrews, Scotland, United Kingdom, 2016. – P. 123–126.
27. Rabiner L. R. Introduction to Digital Speech Processing / L. R. Rabiner, R. W. Schafer. – Delft: now Publishers Inc., 2007. – 200 p. DOI: 10.1561/2000000001
28. Wang L. Correlation Maximization-Based Sampling RateOffset Estimation for Distributed Microphone Arrays / L. Wang, S. Doclo // IEEE/ACM Transactions on Audio, Speech, and Language Processing. – 2016. – Vol. 24, № 3. – P. 571–582. DOI: 10.1109/TASLP.2016.2517326
29. Gilbert E. N. Capacity of a Burst-Noise Channel / E. N. Gilbert // Bell System Technical Journal. – 1960. – Vol. 39, Issue 5. – P. 1253–1265. DOI: 10.1002/j.1538-7305.1960.tb03959.x
30. Elliott E. O. Estimates of Error Rates for Codes on Burst-Noise Channels / E. O. Elliott // Bell System Technical Journal. – 1963. – Vol. 42, Issue 5. – P. 1977–1997. DOI: 10.1002/j.1538-7305.1963.tb00955.x
31. Hasslinger G. The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet / G. Hasslinger, O. Hohlfeld // Measurement, Modelling and Evalutation of Computer and Communication Systems: 14th GI/ITG Conference, Dortmund, Germany, 31 March – 2 April 2008 : proceedings. – VDE VERLAG, 2008.
32. Modeling of packet loss and delay and their effect on real-time multimedia service quality / [M. Ellis, D. P. Pezaros, T. Kypraios et al.] // Computer Networks. – 2014. – Vol. 70. – P. 384–399. DOI: 10.1016/j.comnet.2014.05.013
33. Heegard C. Turbo Coding / C. Heegard, S. B. Wicker. – Norwell: Kluwer Academic Publishers, 1999. – 476 p. DOI: 10.1007/978-1-4757-2999-3
34. 25 Years of Turbo Codes: From Mb/s to beyond 100 Gb/s / [S. Weithoffer, C.A. Nour, N. When et al.] // Turbo Codes and Iterative Information Processing: 10th IEEE International Symposium, Hong Kong, China, 3–7 December 2018 : proceedings. – IEEE Computer Society, 2018. DOI: 10.1109/ISTC.2018.8625377
35. Babar Z. Duality of quantum and classical error correction codes: Design principles and examples / [Z. Babar, D. Chandra, H. V. Nguyen et al.] // IEEE Communications Surveys and Tutorials. – 2019. – Vol. 21, Issue 1. – P. 970–1010. DOI: 10.1109/COMST.2018.2861361
36. Turbo Coded Modulation over GSM Channels / [D. P. Panayiotis, A. S. Thomas, V. Prabodh et al.] // Third Generation Wireless and Beyond: International Conference, San Francisco, California, 6–8 June 2001 : proceedings. – San Francisco, IEEE, 2001.

DOI 10.15588/1607-3274-2019-4-18

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

UDC 004.056

THE INVERSION METHOD OF FOUR-BIT BOOLEAN SAC CRYPTOTRANSFORMS

Fedotova-Piven I. M. – PhD, Assistant Professor, Assistant Professor of the Department of Information Security and Computer Engineering, Cherkassy State Technological University, Cherkassy, Ukraine.

Rudnytskyi V. M. – Dr. Sc., Professor, Head of the Department of Information Security and Computer Engineering, Cherkassy State Technological University, Cherkassy, Ukraine.

Piven O. B. – PhD, Assistant Professor, Professor of the Department of Information Security and Computer Engineering, Cherkassy State Technological University, Cherkassy, Ukraine.

Myroniuk T. V. – PhD, Assistant Professor of the Department of Information Security and Computer Engineering, Cherkassy State Technological University, Cherkassy, Ukraine.

ABSTRACT

Context. Nonlinear systems of Boolean functions play a prominent role in the protection of cryptosystems. The creation and use of new four-bit cryptographic transformations with nonlinear Boolean functions that have the property of strict avalanche criterion is an actual task for increasing the reliability of information protection systems.

Objective. The goal of the work is creating a method for obtaining inverse four-bit cryptographic transformations with the strict avalanche criterion property, which contain balanced Boolean functions only with the operations of inversion and addition modulo two.

Method. A method is proposed for obtaining inverse four-bit cryptographic transformations with the strict avalanche criterion property, each of which contains balanced Boolean functions only with the operations of inversion and addition modulo two. The method simplifies the process of finding inverse cryptographic transformations by creating a class of thirty balanced basic Boolean functions with the required predefined limitations and properties and for finding, within this class, the basic Boolean functions that make up the inverse cryptographic transformation.

Results. The effectiveness of the method is shown for obtaining two inverse four-bit cryptographic transformations with the property of a strict avalanche criterion from two direct four-bit cryptographic transformations with the property of a strict avalanche criterion.

Conclusions. For the first time, there was proposed a method for obtaining inverse four-bit cryptographic transformations with the strict avalanche criterion property for balanced Boolean functions containing two logical operations (inversion and addition modulo two) to ensure reliable information protection. This method is a method of selecting the already existing basic Boolean functions from a predetermined set of balanced basic Boolean functions for direct and inverse cryptographic transformations, whereas the existing methods of searching for inverse cryptographic transformation are methods for calculating each element of the Boolean functions for the inverse cryptographic transformation. The method can be extended to a larger even number of arguments of the balanced Boolean functions of cryptographic transformations to increase the cryptographic resilience.

KEYWORDS: Boolean functions, inverse cryptographic transformation, balancedness, strict avalanche criterion, inversion, addition modulo 2.

ABBREVIATIONS

BBF is a basic Boolean function;
BF is a Boolean function;
CA is a cryptographic algorithm;
CT is a cryptographic transformation;
DCT is a direct cryptographic transformation;
FPBE is a Forward Problem of Boolean equations;
HW is a Hamming weight;
ICT is a inverse cryptographic transformation;
IPBE is a Inverse Problem of Boolean equations;
SAC is a strict avalanche criterion.

NOMENCLATURE

$\neg$ is a sign of the Boolean operation inversion (complementation);

$\oplus$ is a sign of the Boolean operation addition modulo 2 (XOR – exclusive OR);

$B_{n,n}$ is a set of all Boolean functions with n inputs and n outputs;

$f_i(x_1,...,x_n)$ is the i-th Boolean function with n inputs $x_1,...,x_n$ and 1 output;

F is a Boolean function with n inputs and n outputs;

F_{pi}^r is the values of the i-th basic Boolean function of the inverse cryptographic transformation F_1^r;

$f_j(x_1,...,x_4)$ is the j-th basic Boolean function from the set of basic Boolean functions (Table 1);

$wt(f)$ is a Hamming weight of the Boolean function $f(x_1,...,x_n)$.

INTRODUCTION

Nowadays, the number of users of the Internet and digital mobile networks (such as GSM) is more than 4 billions [1], the amount of data transmission is huge. Therefore, data security plays a crucially important role in this data transmission. One of the main ways to ensure the reliability and safety of information is effective methods of encryption/decryption of data [2] with high cryptographic resilience. Today, computationally resilient cryptosystems generally protect information in a satisfactory way, but quantum computers with computing power far beyond the computing power of any classical com-

DOI 10.15588/1607-3274-2019-4-19

puter [3–5] can solve a lot of cryptanalysis tasks that can not be solved by traditional computing systems. The issue of crypto security of information security systems has become extremely acute in connection with the advent of quantum computers.

BFs play a prominent role in the security of cryptosystems [6]. Their most important cryptographic applications include the analysis and design of S-boxes in block ciphers and the construction of filter/combining functions in stream ciphers [7]. Constructing optimal S-boxes has been a prominent topic of interest for security experts [8]. Also, each reversible BF can be implemented as a reversible circuit [9], whereas reversible circuits are indispensable in error correction [10, 11].

Cryptoresistance of a broad class of CAs is determined by their correspondence to some special criteria of bit transform BFs being implemented in these algorithms [12]. One of such criteria is a SAC [12], that is whenever a single input bit is complemented, each of the output bits changes with a probability of one half [13]. This is essential to diminish any correlation between input and output combinations and fails to leak information [14]. This also means that there are no functions with fewer bits, that is a good approximation to the given function and the use of which would significantly reduce the amount of work required to decode the message [15]. That is why the design problem of the Boolean SAC-functions is actually and practically important [16].

The object of study is the process of constructing DCT and ICT of BFs defined by systems for the number of arguments 4 and more.

The subject of study is the methods of constructing ICTs of BFs by given DCTs of BFs that have the property of a SAC and contain only the operations of inversion and addition modulo two.

The purpose of the work is creating a method for obtaining inverse four-bit CTs with the SAC property, which contain balanced BFs only with the operations of inversion and addition modulo two for increasing the reliability of information protection systems. The method must have an applicability property on a larger even number of bits.

1 PROBLEM STATEMENT

It is important to study four-bit, eight-bit BFs in public key cryptography [17, 18]. The formalized procedure for construction of four-bit Boolean SAC-functions with the operations of inversion is proposed in [16]. But CTs with four-bit Boolean SAC-functions with the operations of inversion and addition modulo two are insufficiently investigated and remains relevant. Mathematical statement: we have Boolean multiple-output function $F^d \in B_{4,4}$ with 4 inputs and 4 outputs with the SAC property and bijection property (there are no two or more different sets of input values of $F^d \in B_{4,4}$ that corresponds to the same set of the output values). The function $F^d \in B_{4,4}$ contain balanced BFs only with the operations of inversion and addition modulo two. The function $F^d \in B_{4,4}$ forms a direct four-bit CT. It is required to receive a Boolean multiple-output function $F^r \in B_{4,4}$ with 4 inputs and 4 outputs (an ICT)). All the sets of input values of the function $F^d \in B_{4,4}$ and all the sets of the output values of the function $F^r \in B_{4,4}$ must be the same, and all the sets of the output values of the function $F^d \in B_{4,4}$ and all the sets of the input values of the function $F^r \in B_{4,4}$ also must be the same.

2 REVIEW OF THE LITERATURE

The problem of finding the roots of a system of nonlinear BFs is analytically intractable and therefore provides the basis for many CAs [12]. The FPBE consists of finding all solutions of a system of Boolean equations, whereas the IPBE aims at reconstructing the mathematical formulae of the system of Boolean equations for given the set of solutions. The FPBE has been extensively treated in the literature [19–22] while the inverse problem seems to have received no or little attention [23].

In papers [23–26], various methods for obtaining inverse Boolean functions with *n* inputs and 1 output are described for given direct Boolean functions with *n* inputs and 1 output, but inverse Boolean functions with *n* inputs and *n* outputs for given direct Boolean functions with *n* inputs and *n* outputs in these papers are not considered.

The paper [30] describes invertible Boolean functions of three variables. The papers [27, 28] describe the properties of the Boolean function with *n* inputs and *n* outputs, but the concrete method or algorithm for obtaining the inverse Boolean functions with *n* inputs and *n* outputs for given direct Boolean functions with *n* inputs and *n* outputs is not given. Other publications containing a concrete algorithm for obtaining an ICT using a given DCT containing four or more Boolean functions with four or more Boolean variables and two or more different Boolean operations are unknown to the authors of this article.

The existing methods [23–26] of searching for an inverse Boolean functions are methods for calculating each element of the BFs of the inverse Boolean functions for given direct Boolean functions and this situation needs the development of more effective methods for obtaining ICT for given DCT.

3 MATERIALS AND METHODS

We assume that everywhere in the article $n \geq 1, n \in N$ and $i \in \{1,...,n\}$.

Let $B \overset{def}{=} \{0;1\}$ denote the Boolean values and $B_{n,n}$ [27] denote the set of all BFs with *n* inputs and *n* outputs, where

$$B_{n,n} \overset{def}{=} \{F \mid F : B^n \to B^n\}. \quad (1)$$

DOI 10.15588/1607-3274-2019-4-19

We write $B_n \overset{def}{=} B_{n,1}$ for each n and assume that each $f_i(x_1,...,x_n) \in B_n$ for each i is represented by a propositional formula over the variables $\{x_1,...,x_n\}$ [27]. Conversely, any n-tuple t of BFs over variables $\{x_1,...,x_n\}$ corresponds to a unique BF $F_t \in B_{n,n}$ [27]. We assume that each function $F \in B_{n,n}$ is represented as a tuple $F = (f_1(x_1,...,x_n),..., f_n(x_1,...,x_n))$, where $f_i(x_1,...,x_n) \in B_n$ for each i and hence for each $F(\vec{x}) = (f_1(\vec{x}),..., f_n(\vec{x}))$ for each $\vec{x} \in B^n$ [27].

As known [28], function $F: B^n \to B^n$ is called reversible iff F is bijective, i.e., if each input pattern uniquely maps to an output pattern, and vice versa. Otherwise, it is called irreversible.

Let a DCT and ICT are Boolean multiple-output functions $F^d \in B_{n,n}$ and $F^r \in B_{n,n}$ respectively with n inputs and n outputs. Then not every DCT that satisfies the SAC, has a pertinent ICT. For example, for a DCT $F^d \in B_{n,n}$ that given by the formula (2) and satisfies the SAC, there is no ICT because two different sets (for example, a direct set $x_1 = x_2 = x_3 = x_4 = 0$ and an inverse set $x_1 = x_2 = x_3 = x_4 = 1$) of the input values

$$F^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_3 \\ \neg(x_1 \oplus x_2) \\ \neg(x_2 \oplus x_4) \end{bmatrix}. \quad (2)$$

of the DCT corresponds to the same set of the output values – the results of the operation (2):

$$F^d = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

and therefore, the property of one-to-one correspondence (bijection) of the ICT $F^r \in B_{n,n}$ is lost.

As known [29], the HW $wt(f)$ of the BF $f(x_1,...,x_n) \in B^n$ is the number of the nonzero terms in the truth table of the BF:

$$wt(f) = \sum_i^n x_i.$$

As known [29], the BF $f(x_1,...,x_n) \in B^n$ is balanced if its HW $wt(f) = 2^{n-1}$, i.e. the output column of this BF in the truth table contains equal number of 0's and 1's.

To date, the problem of the total number of balanced Boolean SAC-functions determination for n variables remains open [16]. The search area of the roots of systems of Boolean equations may be decreased significantly by application of different expedients based on taking into account the special features of BFs constructing the system of nonlinear Boolean equations [12].

We will consider four-bit CTs that satisfy a SAC and are constructed using only Boolean operations of the inversion and addition modulo 2. To synthesize both DCT and ICT, we create a set of BBFs $f_j(x_1,...,x_4) \in B^4$, $j \in \{1,...,30\}$ with such restrictions:

1) all the BBFs from Table 1 are balanced, because the HW of each of them is $2^3 = 8$, that is, a half of the number 16 - the length of the vector of values of each BBF;

2) each BBF from Table 1 contains from one to four variables $x_1,..., x_4$, and the same variable is included only once in each BBF of the CT;

3) all the BBFs from Table 1 must have non-coinciding sets of values (see Table 2).

We will assume that the BBFs of an ICT will be selected from the same set of BBFs from Table 1. Functions $f_1(x_1,...,x_4),..., f_{30}(x_1,...,x_4)$ are a superposition of variables and operations of inversion and addition modulo 2. Functions $f_{31}(x_1,...,x_4) = 0$ and $f_{32}(x_1,...,x_4) = 1$ for any values of $x_1,..., x_4$ are not listed in Table 1, because they do not contain operations symbols over variables, that is, there is no explicitly indicated mathematical form of the function.

To construct ICTs that satisfy the SAC, we apply the following method that defines the BBFs of the ICT over

Table 1 – Basic Boolean functions $f_1(x_1,...,x_4),..., f_{30}(x_1,...,x_4)$

1) $f_1 = x_1$;	11) $f_{11} = x_1 \oplus x_4$;	21) $f_{21} = x_1 \oplus x_2 \oplus x_3$;
2) $f_2 = x_2$;	12) $f_{12} = x_2 \oplus x_3$;	22) $f_{22} = x_1 \oplus x_2 \oplus x_4$;
3) $f_3 = x_3$;	13) $f_{13} = x_2 \oplus x_4$;	23) $f_{23} = x_1 \oplus x_3 \oplus x_4$;
4) $f_4 = x_4$;	14) $f_{14} = x_3 \oplus x_4$;	24) $f_{24} = x_2 \oplus x_3 \oplus x_4$;
5) $f_5 = \neg(x_1)$;	15) $f_{15} = \neg(x_1 \oplus x_2)$;	25) $f_{25} = x_1 \oplus x_2 \oplus x_3 \oplus x_4$;
6) $f_6 = \neg(x_2)$;	16) $f_{16} = \neg(x_1 \oplus x_3)$;	26) $f_{26} = \neg(x_1 \oplus x_2 \oplus x_3)$;
7) $f_7 = \neg(x_3)$;	17) $f_{17} = \neg(x_1 \oplus x_4)$;	27) $f_{27} = \neg(x_1 \oplus x_2 \oplus x_4)$;
8) $f_8 = \neg(x_4)$;	18) $f_{18} = \neg(x_2 \oplus x_3)$;	28) $f_{28} = \neg(x_1 \oplus x_3 \oplus x_4)$;
9) $f_9 = x_1 \oplus x_2$;	19) $f_{19} = \neg(x_2 \oplus x_4)$;	29) $f_{29} = \neg(x_2 \oplus x_3 \oplus x_4)$;
10) $f_{10} = x_1 \oplus x_3$;	20) $f_{20} = \neg(x_3 \oplus x_4)$;	30) $f_{30} = \neg(x_1 \oplus x_2 \oplus x_3 \oplus x_4)$;

DOI 10.15588/1607-3274-2019-4-19

the whole set of values at the input and output of the BBFs of DCT.

1. Let's create Table 2 (truth table) of the values of the BBFs from Table 1 for all possible sets of values of the variables $x_1,...,x_4$.

2. Let's create a Table 3 which contains only those BBFs that give the value of 0 for a given set of values $x_1,...,x_4$.

3. Let's create a Table 4 which contains only those BBFs that give the value of 1 for a given set of values $x_1,...,x_4$.

Table 2 – The values of the BBFs from Table 1 for all possible sets of values of the variables $x_1,...,x_4$

x_1 $=f_1$	x_2 $=f_2$	x_3 $=f_3$	x_4 $=f_4$	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{24}	f_{25}	f_{26}	f_{27}	f_{28}	f_{29}	f_{30}
0	0	0	0	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1
0	0	0	1	1	1	1	0	0	0	1	0	1	1	1	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0
0	0	1	0	1	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	1	1	0	1	0	0	0
0	1	0	0	1	0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1	0	1	1	0	0	1	0	0
1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	0	1	0	0	0	1	0
0	0	1	1	1	1	0	0	0	1	1	1	1	0	1	0	0	0	0	1	1	1	0	0	0	0	0	1	1	1
0	1	0	1	1	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0	0	1	0	1	1
1	0	0	1	0	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	0	0	1	1	0	1
0	1	1	0	1	0	0	1	1	1	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	1	0	0	1	1
1	0	1	0	0	1	0	1	1	0	1	1	0	1	0	1	0	0	1	0	0	1	0	1	0	1	0	1	0	1
1	1	0	0	0	0	1	1	0	1	1	1	1	0	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	1
0	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0	1	1	1	1	1	0	0
1	0	1	1	0	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	0	1	1	1	0	1	0
1	1	0	1	0	0	1	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	1	1	0	1	1	0
1	1	1	0	0	0	0	1	0	0	1	0	1	1	1	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0
1	1	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1

Table 3 – The BBFs from the Table 1, that give the value of 0 for a given set of values $x_1,...,x_4$ for each row

x_1 $=f_1$	x_2 $=f_2$	x_3 $=f_3$	x_4 $=f_4$	The value of function	The functions from the set $\{f_1, f_2, ... f_{30}\}$ that gives 0 as a result for the specified values $x_1, ...,x_4$ for each row													
0	0	0	0	0	f_1	f_2	f_3	f_4	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{21}	f_{22}	f_{23}	f_{24}	f_{25}
0	0	0	1		f_1	f_2	f_3	f_8	f_9	f_{10}	f_{12}	f_{17}	f_{19}	f_{20}	f_{21}	f_{27}	f_{28}	f_{29}	f_{30}
0	0	1	0		f_1	f_2	f_4	f_7	f_9	f_{11}	f_{13}	f_{16}	f_{18}	f_{20}	f_{22}	f_{26}	f_{28}	f_{29}	f_{30}
0	1	0	0		f_1	f_3	f_4	f_6	f_{10}	f_{11}	f_{14}	f_{15}	f_{18}	f_{19}	f_{23}	f_{26}	f_{27}	f_{29}	f_{30}
1	0	0	0		f_2	f_3	f_4	f_5	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{24}	f_{26}	f_{27}	f_{28}	f_{30}
0	0	1	1		f_1	f_2	f_7	f_8	f_9	f_{14}	f_{16}	f_{17}	f_{18}	f_{19}	f_{23}	f_{24}	f_{25}	f_{26}	f_{27}
0	1	0	1		f_1	f_3	f_6	f_8	f_{10}	f_{13}	f_{15}	f_{17}	f_{18}	f_{20}	f_{22}	f_{24}	f_{25}	f_{26}	f_{28}
1	0	0	1		f_2	f_3	f_5	f_8	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{22}	f_{23}	f_{25}	f_{26}	f_{29}
0	1	1	0		f_1	f_4	f_6	f_7	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{21}	f_{24}	f_{25}	f_{27}	f_{28}
1	0	1	0		f_2	f_4	f_5	f_7	f_{10}	f_{13}	f_{15}	f_{17}	f_{18}	f_{20}	f_{21}	f_{23}	f_{25}	f_{27}	f_{29}
1	1	0	0		f_3	f_4	f_5	f_6	f_9	f_{14}	f_{16}	f_{17}	f_{18}	f_{19}	f_{21}	f_{22}	f_{25}	f_{28}	f_{29}
0	1	1	1		f_1	f_6	f_7	f_8	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{21}	f_{22}	f_{23}	f_{29}	f_{30}
1	0	1	1		f_2	f_5	f_7	f_8	f_{10}	f_{11}	f_{14}	f_{15}	f_{18}	f_{19}	f_{21}	f_{22}	f_{24}	f_{28}	f_{30}
1	1	0	1		f_3	f_5	f_6	f_8	f_9	f_{11}	f_{13}	f_{16}	f_{18}	f_{20}	f_{21}	f_{23}	f_{24}	f_{27}	f_{30}
1	1	1	0		f_4	f_5	f_6	f_7	f_9	f_{10}	f_{12}	f_{17}	f_{19}	f_{20}	f_{22}	f_{23}	f_{24}	f_{26}	f_{30}
1	1	1	1		f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{25}	f_{26}	f_{27}	f_{28}	f_{29}

Table 4 – The BBFs from the Table 1, that give the value of 1 for a given set of values $x_1,...,x_4$ for each row

x_1 $=f_1$	x_2 $=f_2$	x_3 $=f_3$	x_4 $=f_4$	The value of function	The functions from the set $\{f_1, f_2, ... f_{30}\}$ that gives 1 as a result for the specified values $x_1, ..., x_4$ for each row													
0	0	0	0	1	f_5	f_6	f_7	f_8	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{26}	f_{27}	f_{28}	f_{29}	f_{30}
0	0	0	1		f_4	f_5	f_6	f_7	f_{11}	f_{13}	f_{14}	f_{15}	f_{16}	f_{18}	f_{22}	f_{23}	f_{24}	f_{25}	f_{26}
0	0	1	0		f_3	f_5	f_6	f_8	f_{10}	f_{12}	f_{14}	f_{15}	f_{17}	f_{19}	f_{21}	f_{23}	f_{24}	f_{25}	f_{27}
0	1	0	0		f_2	f_5	f_7	f_8	f_9	f_{12}	f_{13}	f_{16}	f_{17}	f_{20}	f_{21}	f_{22}	f_{24}	f_{25}	f_{28}
1	0	0	0		f_1	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{25}	f_{29}
0	0	1	1		f_3	f_4	f_5	f_6	f_{10}	f_{11}	f_{12}	f_{13}	f_{15}	f_{20}	f_{21}	f_{22}	f_{28}	f_{29}	f_{30}
0	1	0	1		f_2	f_4	f_5	f_7	f_9	f_{11}	f_{12}	f_{14}	f_{16}	f_{19}	f_{21}	f_{23}	f_{27}	f_{29}	f_{30}
1	0	0	1		f_1	f_4	f_6	f_7	f_9	f_{10}	f_{13}	f_{14}	f_{17}	f_{18}	f_{21}	f_{24}	f_{27}	f_{28}	f_{30}
0	1	1	0		f_2	f_3	f_5	f_8	f_9	f_{10}	f_{13}	f_{14}	f_{17}	f_{18}	f_{22}	f_{23}	f_{26}	f_{29}	f_{30}
1	0	1	0		f_1	f_3	f_6	f_8	f_9	f_{11}	f_{12}	f_{14}	f_{16}	f_{19}	f_{22}	f_{24}	f_{26}	f_{28}	f_{30}
1	1	0	0		f_1	f_2	f_7	f_8	f_{10}	f_{11}	f_{12}	f_{13}	f_{15}	f_{20}	f_{23}	f_{24}	f_{26}	f_{27}	f_{30}
0	1	1	1		f_2	f_3	f_4	f_5	f_9	f_{10}	f_{11}	f_{18}	f_{19}	f_{20}	f_{24}	f_{25}	f_{26}	f_{27}	f_{28}
1	0	1	1		f_1	f_3	f_4	f_6	f_9	f_{12}	f_{13}	f_{16}	f_{17}	f_{20}	f_{23}	f_{25}	f_{26}	f_{27}	f_{29}
1	1	0	1		f_1	f_2	f_4	f_7	f_{10}	f_{12}	f_{14}	f_{15}	f_{17}	f_{19}	f_{22}	f_{25}	f_{26}	f_{28}	f_{29}
1	1	1	0		f_1	f_2	f_3	f_8	f_{11}	f_{13}	f_{14}	f_{15}	f_{16}	f_{18}	f_{21}	f_{25}	f_{27}	f_{28}	f_{29}
1	1	1	1		f_1	f_2	f_3	f_4	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{24}	f_{30}

DOI 10.15588/1607-3274-2019-4-19

4. Let's take a DCT with the property of the SAC, for example

$$F_1^d = \begin{bmatrix} \neg(x_1 \oplus x_2 \oplus x_4) \\ \neg(x_1 \oplus x_2 \oplus x_3) \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} f_{27} \\ f_{26} \\ f_1 \\ f_2 \end{bmatrix} \quad (3)$$

and we will find ICT F_1^r for this CT. To do this, create a Table 5 from Table 2. In the left part of Table 5, we write the input values of the variables $x_1,...,x_4$, and in the right part of Table 5 the values of the four BBFs of the DCT. We take functions and their values from Table 2.

Table 5 – Sets of values of variables and their pertinent values of the BBFs of the DCT

The values of variables				The values of the BBFs of a DCT F_1^d			
$x_1=f_1$	$x_2=f_2$	$x_3=f_3$	$x_4=f_4$	f_{27}	f_{26}	$x_1=f_1$	$x_2=f_2$
0	0	0	0	1	1	0	0
0	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0
0	1	0	0	0	0	0	1
1	0	0	0	0	0	1	0
0	0	1	1	0	0	0	0
0	1	0	1	1	0	0	1
1	0	0	1	1	0	1	0
0	1	1	0	0	1	0	1
1	0	1	0	0	1	1	0
1	1	0	0	1	1	1	1
0	1	1	1	1	1	0	1
1	0	1	1	1	1	1	0
1	1	0	1	0	1	1	1
1	1	1	0	1	0	1	1
1	1	1	1	0	0	1	1

5. Since the input values of any DCT are the output values of the pertinent ICT (if it exists), and the output values of the DCT are the input values of the ICT, we will change the places of the left and the right side of Table 5, that is, the set of input and output values of the DCT ($F_{p1}^r, F_{p2}^r, F_{p3}^r, F_{p4}^r$ – known sets of values of the pertinent four unknown BBFs of the ICP). The F_{pi}^r is the *i*-th part of the $F_1^r \in B_{n,n}$. As a result, we obtain Table 6.

Table 6 – Sets of values of variables and their pertinent values of the BBFs of the ICT

The values of variables				The values of unknown BBFs of the ICT F_1^r			
$x_1=f_1$	$x_2=f_2$	$x_3=f_3$	$x_4=f_4$	F_{p1}^r	F_{p2}^r	F_{p3}^r	F_{p4}^r
1	1	0	0	0	0	0	0
0	1	0	0	0	0	0	1
1	0	0	0	0	0	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0
0	0	0	0	0	0	1	1
1	0	0	1	0	1	0	1
1	0	1	0	1	0	0	1
0	1	0	1	0	1	1	0
0	1	1	0	1	0	1	0
1	1	1	1	1	1	0	0
1	1	0	1	0	1	1	1
1	1	1	0	1	0	1	1
0	1	1	1	1	1	0	1
1	0	1	1	1	1	1	0
0	0	1	1	1	1	1	1

6. Let's create a Table 7 where we indicate those BBFs, whose calculation result is equal to the value F_{p1}^r of the first BBF of the ICT F_1^r for each set of values $x_1,...,x_4$.

Table 7 – All possible BBFs that give the values of the first BBF F_{p1}^r of the ICT F_1^r

The values of variables				F_{p1}^r (the values of the first BBF of the ICT F_1^r)	The BBFs from the Table 1 that give the value equal to the value of the first BBF F_{p1}^r of the ICT F_1^r for the specified values $x_1,...,x_4$ for each row														
$x_1=f_1$	$x_2=f_2$	$x_3=f_3$	$x_4=f_4$																
1	1	0	0	0	$\boldsymbol{f_3}$	f_4	f_5	f_6	f_9	f_{14}	f_{16}	f_{17}	f_{18}	f_{19}	f_{21}	f_{22}	f_{25}	f_{28}	f_{29}
0	1	0	0	0	f_1	$\boldsymbol{f_3}$	f_4	f_6	f_{10}	f_{11}	f_{14}	f_{15}	f_{18}	f_{19}	f_{23}	f_{26}	f_{27}	f_{29}	f_{30}
1	0	0	0	0	f_2	$\boldsymbol{f_3}$	f_4	f_5	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{24}	f_{26}	f_{27}	f_{28}	f_{30}
0	0	0	1	0	f_1	f_2	$\boldsymbol{f_3}$	f_8	f_9	f_{10}	f_{12}	f_{17}	f_{19}	f_{20}	f_{21}	f_{27}	f_{28}	f_{29}	f_{30}
0	0	1	0	1	$\boldsymbol{f_3}$	f_5	f_6	f_8	f_{10}	f_{12}	f_{14}	f_{15}	f_{17}	f_{19}	f_{21}	f_{23}	f_{24}	f_{25}	f_{27}
0	0	0	0	0	f_1	f_2	$\boldsymbol{f_3}$	f_4	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{21}	f_{22}	f_{23}	f_{24}	f_{25}
1	0	0	1	0	f_2	$\boldsymbol{f_3}$	f_5	f_8	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{22}	f_{23}	f_{25}	f_{26}	f_{29}
1	0	1	0	1	f_1	$\boldsymbol{f_3}$	f_6	f_8	f_9	f_{11}	f_{12}	f_{14}	f_{16}	f_{19}	f_{22}	f_{24}	f_{26}	f_{28}	f_{30}
0	1	0	1	0	f_1	$\boldsymbol{f_3}$	f_6	f_8	f_{10}	f_{13}	f_{15}	f_{17}	f_{18}	$\boldsymbol{f_{20}}$	f_{22}	f_{24}	f_{25}	f_{26}	f_{28}
0	1	1	0	1	f_2	$\boldsymbol{f_3}$	f_5	f_8	f_9	f_{10}	f_{13}	f_{14}	f_{17}	f_{18}	f_{22}	f_{23}	f_{26}	f_{29}	f_{30}
1	1	1	1	1	f_1	f_2	$\boldsymbol{f_3}$	f_4	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{24}	f_{30}
1	1	0	1	0	$\boldsymbol{f_3}$	f_5	f_6	f_8	f_9	f_{11}	f_{13}	f_{16}	f_{18}	f_{20}	f_{21}	f_{23}	f_{24}	f_{27}	f_{30}
1	1	1	0	1	f_1	f_2	$\boldsymbol{f_3}$	f_8	f_{11}	f_{13}	f_{14}	f_{15}	f_{16}	f_{18}	f_{21}	f_{25}	f_{27}	f_{28}	f_{29}
0	1	1	1	1	f_2	$\boldsymbol{f_3}$	f_4	f_5	f_9	f_{10}	f_{11}	f_{18}	f_{19}	f_{20}	f_{24}	f_{25}	f_{26}	f_{27}	f_{28}
1	0	1	1	1	f_1	$\boldsymbol{f_3}$	f_4	f_6	f_9	f_{12}	f_{13}	f_{16}	f_{17}	f_{20}	f_{23}	f_{25}	f_{26}	f_{27}	f_{29}
0	0	1	1	1	$\boldsymbol{f_3}$	f_4	f_5	f_6	f_{10}	f_{11}	f_{12}	f_{13}	f_{15}	f_{20}	f_{21}	f_{22}	f_{28}	f_{29}	f_{30}

DOI 10.15588/1607-3274-2019-4-19

It can be seen from Table 7 that only the BBF f_3 from the set of functions of the Table 1 satisfies all the values F_{p1}^r from the Table 7. Therefore, $f_3 = F_{p1}^r$ is the first BBF of the ICT F_1^r.

7. Similarly, we create Table 8 for the second BBF F_{p2}^r of the ICT F_1^r.

It can be seen from Table 8 that only the BBF f_4 from the set of functions of the Table 1 satisfies all the values F_{p2}^r from the Table 8. Therefore, $f_4 = F_{p2}^r$ is the second BBF of the ICT F_1^r.

8. Similarly, we create Table 9 for the third BBF F_{p3}^r of the ICT F_1^r.

It can be seen from Table 9 that only the BBF f_{29} from the set of functions of the Table 1 satisfies all the values F_{p3}^r from the Table 9. Therefore, $f_{29} = F_{p3}^r$ is the third BBF of the ICT F_1^r.

9. Similarly, we create Table 10 for the forth BBF F_{p4}^r of the ICT F_1^r.

Table 8 – All possible BBFs that give the values of the second BBF F_{p2}^r of the ICT F_1^r

The values of variables				F_{p2}^r (the values of the second BBF of the ICT F_1^r)	The BBFs from the Table 1 that give the value equal to the value of the second BBF F_{p2}^r of the ICT F_1^r for the specified values $x_1,\ldots,x_4$ for each row													
x_1 =f_1	x_2 =f_2	x_3 =f_3	x_4 =f_4															
1	1	0	0	0	f_3	**f_4**	f_5	f_6	f_9	f_{14}	f_{16}	f_{17}	f_{18}	f_{19}	f_{21}	f_{22}	f_{25}	f_{28}	f_{29}
0	1	0	0	0	f_1	f_3	**f_4**	f_6	f_{10}	f_{11}	f_{14}	f_{15}	f_{18}	f_{19}	f_{23}	f_{26}	f_{27}	f_{29}	f_{30}
1	0	0	0	0	f_2	f_3	**f_4**	f_5	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{24}	f_{26}	f_{27}	f_{28}	f_{30}
0	0	0	1	1	**f_4**	f_5	f_6	f_7	f_{11}	f_{13}	f_{14}	f_{15}	f_{16}	f_{18}	f_{22}	f_{23}	f_{24}	f_{25}	f_{26}
0	0	1	0	0	f_1	f_2	**f_4**	f_7	f_9	f_{11}	f_{13}	f_{16}	f_{18}	f_{20}	f_{22}	f_{26}	f_{28}	f_{29}	f_{30}
0	0	0	0	0	f_1	f_2	f_3	**f_4**	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{21}	f_{22}	f_{23}	f_{24}	f_{25}
1	0	0	1	1	f_1	**f_4**	f_6	f_7	f_9	f_{10}	f_{13}	f_{14}	f_{17}	f_{18}	f_{21}	f_{24}	f_{27}	f_{28}	f_{30}
1	0	1	0	0	f_2	**f_4**	f_5	f_7	f_{10}	f_{13}	f_{15}	f_{17}	f_{18}	f_{20}	f_{21}	f_{23}	f_{25}	f_{27}	f_{29}
0	1	0	1	1	f_2	**f_4**	f_5	f_7	f_9	f_{11}	f_{12}	f_{14}	f_{16}	f_{19}	f_{21}	f_{23}	f_{27}	f_{29}	f_{30}
0	1	1	0	0	f_1	**f_4**	f_6	f_7	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{21}	f_{24}	f_{25}	f_{27}	f_{28}
1	1	1	1	1	f_1	f_2	f_3	**f_4**	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{24}	f_{30}
1	1	0	1	1	f_1	f_2	**f_4**	f_7	f_{10}	f_{12}	f_{14}	f_{15}	f_{17}	f_{19}	f_{22}	f_{25}	f_{26}	f_{28}	f_{29}
1	1	1	0	0	**f_4**	f_5	f_6	f_7	f_9	f_{10}	f_{12}	f_{17}	f_{19}	f_{20}	f_{22}	f_{23}	f_{24}	f_{26}	f_{30}
0	1	1	1	1	f_2	f_3	**f_4**	f_5	f_9	f_{10}	f_{11}	f_{18}	f_{19}	f_{20}	f_{24}	f_{25}	f_{26}	f_{27}	f_{28}
1	0	1	1	1	f_1	f_3	**f_4**	f_6	f_9	f_{12}	f_{13}	f_{16}	f_{17}	f_{20}	f_{23}	f_{25}	f_{26}	f_{27}	f_{29}
0	0	1	1	1	f_3	**f_4**	f_5	f_6	f_{10}	f_{11}	f_{12}	f_{13}	f_{15}	f_{20}	f_{21}	f_{22}	f_{28}	f_{29}	f_{30}

Table 9 – All possible BBFs that give the value of the third BBF F_{p3}^r of the ICT F_1^r

The values of variables				F_{p3}^r (the values of the third BBF of the ICT F_1^r)	The BBFs from the Table 1 that give the value equal to the value of the third BBF F_{p3}^r of the ICT F_1^r for the specified values $x_1,\ldots,x_4$ for each row													
x_1 =f_1	x_2 =f_2	x_3 =f_3	x_4 =f_4															
1	1	0	0	0	f_3	f_4	f_5	f_6	f_9	f_{14}	f_{16}	f_{17}	f_{18}	f_{19}	f_{21}	f_{22}	f_{25}	f_{28}	**f_{29}**
0	1	0	0	0	f_1	f_3	f_4	f_6	f_{10}	f_{11}	f_{14}	f_{15}	f_{18}	f_{19}	f_{23}	f_{26}	f_{27}	**f_{29}**	f_{30}
1	0	0	0	1	f_1	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{25}	**f_{29}**
0	0	0	1	0	f_1	f_2	f_3	f_8	f_9	f_{10}	f_{12}	f_{17}	f_{19}	f_{20}	f_{21}	f_{27}	f_{28}	**f_{29}**	f_{30}
0	0	1	0	0	f_1	f_2	f_4	f_7	f_9	f_{11}	f_{13}	f_{16}	f_{18}	f_{20}	f_{22}	f_{26}	f_{28}	**f_{29}**	f_{30}
0	0	0	0	1	f_5	f_6	f_7	f_8	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{26}	f_{27}	f_{28}	**f_{29}**	f_{30}
1	0	0	1	0	f_2	f_3	f_5	f_8	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{22}	f_{23}	f_{25}	f_{26}	**f_{29}**
1	0	1	0	0	f_2	f_4	f_5	f_7	f_{10}	f_{13}	f_{15}	f_{17}	f_{18}	f_{20}	f_{21}	f_{23}	f_{25}	f_{27}	**f_{29}**
0	1	0	1	1	f_2	f_4	f_5	f_7	f_9	f_{11}	f_{12}	f_{14}	f_{16}	f_{19}	f_{21}	f_{23}	f_{27}	**f_{29}**	f_{30}
0	1	1	0	1	f_2	f_3	f_5	f_8	f_9	f_{10}	f_{13}	f_{14}	f_{17}	f_{18}	f_{22}	f_{23}	f_{26}	**f_{29}**	f_{30}
1	1	1	1	0	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{25}	f_{26}	f_{27}	f_{28}	**f_{29}**
1	1	0	1	1	f_1	f_2	f_4	f_7	f_{10}	f_{12}	f_{14}	f_{15}	f_{17}	f_{19}	f_{22}	f_{25}	f_{26}	f_{28}	**f_{29}**
1	1	1	0	1	f_1	f_2	f_3	f_8	f_{11}	f_{13}	f_{14}	f_{15}	f_{16}	f_{18}	f_{21}	f_{25}	f_{27}	f_{28}	**f_{29}**
0	1	1	1	0	f_1	f_6	f_7	f_8	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{21}	f_{22}	f_{23}	**f_{29}**	f_{30}
1	0	1	1	1	f_1	f_3	f_4	f_6	f_9	f_{12}	f_{13}	f_{16}	f_{17}	f_{20}	f_{23}	f_{25}	f_{26}	f_{27}	**f_{29}**
0	0	1	1	1	f_3	f_4	f_5	f_6	f_{10}	f_{11}	f_{12}	f_{13}	f_{15}	f_{20}	f_{21}	f_{22}	f_{28}	**f_{29}**	f_{30}

DOI 10.15588/1607-3274-2019-4-19

Table 10 – All possible BBFs that give the value of the forth BBF F_{p4}^r of the ICT F_1^r

The values of variables				F_{p4}^r (the values of the forth BBF of the ICT F_1^r)	The BBFs from the Table 1 that give the value equal to the value of the forth BBF F_{p4}^r of the ICT F_1^r for the specified values $x_1,...,x_4$ for each row													
$x_1=f_1$	$x_2=f_2$	$x_3=f_3$	$x_4=f_4$															
1	1	0	0	0	f_3	f_4	f_5	f_6	f_9	f_{14}	f_{16}	f_{17}	f_{18}	f_{19}	f_{21}	f_{22}	f_{25}	$\boldsymbol{f_{28}}$	f_{29}
0	1	0	0	1	f_2	f_5	f_7	f_8	f_9	f_{12}	f_{13}	f_{16}	f_{17}	f_{20}	f_{21}	f_{22}	f_{24}	f_{25}	$\boldsymbol{f_{28}}$
1	0	0	0	0	f_2	f_3	f_4	f_5	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}	f_{17}	f_{24}	f_{26}	f_{27}	$\boldsymbol{f_{28}}$	f_{30}
0	0	0	1	0	f_1	f_2	f_3	f_8	f_9	f_{10}	f_{12}	f_{17}	f_{19}	f_{20}	f_{21}	f_{27}	$\boldsymbol{f_{28}}$	f_{29}	f_{30}
0	0	1	0	0	f_1	f_2	f_4	f_7	f_9	f_{11}	f_{13}	f_{16}	f_{18}	f_{20}	f_{22}	f_{26}	$\boldsymbol{f_{28}}$	f_{29}	f_{30}
0	0	0	0	1	f_5	f_6	f_7	f_8	f_{15}	f_{16}	f_{17}	f_{18}	f_{19}	f_{20}	f_{26}	f_{27}	$\boldsymbol{f_{28}}$	f_{29}	f_{30}
1	0	0	1	1	f_1	f_4	f_6	f_7	f_9	f_{10}	f_{13}	f_{14}	f_{17}	f_{18}	f_{21}	f_{24}	f_{27}	$\boldsymbol{f_{28}}$	f_{30}
1	0	1	0	1	f_1	f_3	f_6	f_8	f_9	f_{11}	f_{12}	f_{14}	f_{16}	f_{19}	f_{22}	f_{24}	f_{26}	$\boldsymbol{f_{28}}$	f_{30}
0	1	0	1	0	f_1	f_3	f_6	f_8	f_{10}	f_{13}	f_{15}	f_{17}	f_{18}	f_{20}	f_{22}	f_{24}	f_{25}	f_{26}	$\boldsymbol{f_{28}}$
0	1	1	0	0	f_1	f_4	f_6	f_7	f_{11}	f_{12}	f_{15}	f_{16}	f_{19}	f_{20}	f_{21}	f_{24}	f_{25}	f_{27}	$\boldsymbol{f_{28}}$
1	1	1	1	0	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{25}	f_{26}	f_{27}	$\boldsymbol{f_{28}}$	f_{29}
1	1	0	1	1	f_1	f_2	f_4	f_7	f_{10}	f_{12}	f_{14}	f_{15}	f_{17}	f_{19}	f_{22}	f_{25}	f_{26}	$\boldsymbol{f_{28}}$	f_{29}
1	1	1	0	1	f_1	f_2	f_3	f_8	f_{11}	f_{13}	f_{14}	f_{15}	f_{16}	f_{18}	f_{21}	f_{25}	f_{27}	$\boldsymbol{f_{28}}$	f_{29}
0	1	1	1	1	f_2	f_3	f_4	f_5	f_9	f_{10}	f_{11}	f_{18}	f_{19}	f_{20}	f_{24}	f_{25}	f_{26}	f_{27}	$\boldsymbol{f_{28}}$
1	0	1	1	0	f_2	f_5	f_7	f_8	f_{10}	f_{11}	f_{14}	f_{15}	f_{18}	f_{19}	f_{21}	f_{22}	f_{24}	$\boldsymbol{f_{28}}$	f_{30}
0	0	1	1	1	f_3	f_4	f_5	f_6	f_{10}	f_{11}	f_{12}	f_{13}	f_{15}	f_{20}	f_{21}	f_{22}	$\boldsymbol{f_{28}}$	f_{29}	f_{30}

It can be seen from Table 10 that only the BBF f_{28} from the set of functions of the Table 1 satisfies all the values F_{p4}^r from the Table 10. Therefore, $f_{28} = F_{p4}^r$ is the forth BBF of the ICT F_1^r.

As a result, the ICT for the DCT (3) has a view:

$$F_1^r = \begin{bmatrix} f_3 \\ f_4 \\ f_{29} \\ f_{28} \end{bmatrix} = \begin{bmatrix} x_3 \\ x_4 \\ \neg(x_2 \oplus x_3 \oplus x_4) \\ \neg(x_1 \oplus x_3 \oplus x_4) \end{bmatrix}. \quad (4)$$

This method provides the construction of ICTs for four variables and two logical operations (inversion and addition modulo 2), but can be extended to a larger even number of variables.

4 EXPERIMENTS

We prove that the resulting CT (4) is indeed the inverse of the CT (3).

As known, the composition $f \circ g$ of BFs $f(x_1,...,x_n) \in B^n$ and $g(x_1,...,x_n) \in B^n$ is a function defined by $(f \circ g)(x_1,...,x_n) = f(g(x_1,...,x_n))$.

As known, the BF with n inputs and n outputs $F(x_1,...,x_n) = (f_1(x_1,...,x_n),..., f_n(x_1,...,x_n))$ has the inverse BF with n inputs and n outputs $F^{-1}(x_1,...,x_n) = (f_1^{-1}(x_1,...,x_n),..., f_n^{-1}(x_1,...,x_n))$, if the following equalities hold: $F^{-1}(F(x_1,...,x_n)) = F(F^{-1}(x_1,...,x_n)) = (x_1,...,x_n)$.

For DCT F_1^d from Table 11 we have $F(x_1,...,x_4) = (\neg(x_1 \oplus x_2 \oplus x_4), \neg(x_1 \oplus x_2 \oplus x_3), x_1, x_2)$ and for ICT F_1^r from Table 11 we have

$F^{-1}(x_1,..., x_4) = (x_3, x_4, \neg(x_2 \oplus x_3 \oplus x_4), \neg(x_1 \oplus x_3 \oplus x_4))$.

Indeed,

$f_1^{-1}(f_1(x_1,...,x_4)) = x_1; \quad f_2^{-1}(f_2(x_1,...,x_4)) = x_2;$

$f_3^{-1}(f_3(x_1,...,x_4)) = \neg(\neg(x_1 \oplus x_2 \oplus x_3) \oplus x_1 \oplus x_2))$

$= x_1 \oplus x_2 \oplus x_3 \oplus \neg x_1 \oplus \neg x_2 = 1 \oplus 1 \oplus x_3 = x_3;$

$f_4^{-1}(f_4(x_1,...,x_4)) = \neg(\neg(x_1 \oplus x_2 \oplus x_4) \oplus (x_1 \oplus x_2)$

$= x_1 \oplus x_2 \oplus x_4 \oplus \neg x_1 \oplus \neg x_2 = 1 \oplus 1 \oplus x_4 = x_4;$

Thus, $F^{-1}(F(x_1,...,x_4)) = (x_1, x_2, x_3, x_4)$.

Conversely,

$f_1(f_1^{-1}(x_1,...,x_4)) = \neg(x_3 \oplus x_4 \oplus \neg(x_1 \oplus x_3 \oplus x_4))$

$= \neg x_3 \oplus \neg x_4 \oplus x_1 \oplus x_3 \oplus x_4 = 1 \oplus 1 \oplus x_1 = x_1;$

$f_2(f_2^{-1}(x_1,...,x_4)) = \neg(x_3 \oplus x_4 \oplus \neg(x_2 \oplus x_3 \oplus x_4))$

$= \neg x_3 \oplus \neg x_4 \oplus x_2 \oplus x_3 \oplus x_4 = 1 \oplus 1 \oplus x_2 = x_2;$

$f_3(f_3^{-1}(x_1,...,x_4)) = x_3; \quad f_4(f_4^{-1}(x_1,...,x_4)) = x_4;$

Thus, $F(F^{-1}(x_1,...,x_4)) = (x_1, x_2, x_3, x_4)$.

Consequently, DCT (3) has ICT (4).

We prove that the ICT F_2^r

$$F_2^r = \begin{bmatrix} x_1 \oplus x_2 \oplus x_4 \\ x_1 \oplus x_3 \oplus x_4 \\ \neg(x_2 \oplus x_3 \oplus x_4) \\ \neg(x_1 \oplus x_2 \oplus x_3) \end{bmatrix}. \quad (5)$$

is indeed the inverse of the DCT F_2^d

DOI 10.15588/1607-3274-2019-4-19

$$F_2^d = \begin{bmatrix} \neg(x_1 \oplus x_2 \oplus x_4) \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_3 \oplus x_4 \\ \neg(x_1 \oplus x_2 \oplus x_3) \end{bmatrix}. \quad (6)$$

For DCT F_2^d we have

$F(x_1,...,x_4) = (\neg(x_1 \oplus x_2 \oplus x_4), (x_1 \oplus x_3 \oplus x_4),$
$(x_2 \oplus x_3 \oplus x_4), \neg(x_1 \oplus x_2 \oplus x_3));$

and for ICT F_2^r we have

$F^{-1}(x_1,...,x_4) = ((x_1 \oplus x_2 \oplus x_4), (x_1 \oplus x_3 \oplus x_4),$
$\neg(x_2 \oplus x_3 \oplus x_4), \neg(x_1 \oplus x_2 \oplus x_3)).$

Indeed,

$f_1^{-1}(f_1(x_1,...,x_4)) = \neg(x_1 \oplus x_2 \oplus x_4)$
$\oplus (x_1 \oplus x_3 \oplus x_4) \oplus \neg(x_1 \oplus x_2 \oplus x_3) = \neg(x_1 \oplus x_2)$
$\oplus \neg(x_1 \oplus x_2) \oplus \neg x_4 \oplus \neg x_3 \oplus (x_4 \oplus x_3 \oplus x_1) =$
$\neg x_4 \oplus \neg x_3 \oplus x_4 \oplus x_3 \oplus x_1 = 1 \oplus 1 \oplus x_1 = x_1;$

$f_2^{-1}(f_2(x_1,...,x_4)) = \neg(x_1 \oplus x_2 \oplus x_4) \oplus (x_2 \oplus x_3 \oplus x_4)$
$\oplus \neg(x_1 \oplus x_2 \oplus x_3) = \neg(x_1 \oplus x_2) \oplus \neg(x_1 \oplus x_2) \oplus \neg x_4$
$\oplus \neg x_3 \oplus (x_4 \oplus x_3 \oplus x_2) = \neg x_4 \oplus \neg x_3 \oplus x_4 \oplus x_3$
$\oplus x_2 = 1 \oplus 1 \oplus x_2 = x_2;$

$f_3^{-1}(f_3(x_1,...,x_4)) = \neg((x_1 \oplus x_3 \oplus x_4) \oplus (x_2 \oplus x_3 \oplus x_4)$
$\oplus \neg(x_1 \oplus x_2 \oplus x_3)) = \neg(x_1 \oplus x_3 \oplus x_4) \oplus \neg(x_2 \oplus x_3$
$\oplus x_4) \oplus (x_1 \oplus x_2 \oplus x_3) = \neg x_1 \oplus \neg x_2 \oplus x_1 \oplus x_2 \oplus x_3 =$
$1 \oplus 1 \oplus x_3 = x_3;$

$f_4^{-1}(f_4(x_1,...,x_4)) = \neg(\neg(x_1 \oplus x_2 \oplus x_4) \oplus (x_1 \oplus x_3 \oplus x_4)$
$\oplus \neg(x_2 \oplus x_3 \oplus x_4)) = x_1 \oplus x_2 \oplus x_4 \oplus \neg x_1 \oplus \neg x_2 =$
$1 \oplus 1 \oplus x_4 = x_4.$

Thus, $F^{-1}(F(x_1,...,x_4)) = (x_1, x_2, x_3, x_4)$.

Conversely,

$f_1(f_1^{-1}(x_1,...,x_4)) = \neg((x_1 \oplus x_2 \oplus x_4) \oplus (x_1 \oplus x_3$
$\oplus x_4) \oplus \neg(x_1 \oplus x_2 \oplus x_3)) = \neg(x_1 \oplus x_2 \oplus x_4) \oplus \neg(x_1$
$\oplus x_3 \oplus x_4) \oplus (x_1 \oplus x_2 \oplus x_3) = \neg(x_1 \oplus x_4) \oplus \neg(x_1 \oplus$
$x_4) \oplus \neg x_2 \oplus \neg x_3 \oplus (x_1 \oplus x_2 \oplus x_3) == \neg x_2 \oplus \neg x_3 \oplus$
$x_1 \oplus x_2 \oplus x_3 == 1 \oplus 1 \oplus x_1 = x_1;$

$f_2(f_2^{-1}(x_1,...,x_4)) = \neg((x_1 \oplus x_2 \oplus x_4) \oplus (x_2 \oplus x_3$
$\oplus x_4) \oplus \neg(x_1 \oplus x_2 \oplus x_3))$
$= \neg(x_1 \oplus x_2) \oplus \neg(x_1 \oplus x_2) \oplus \neg x_4 \oplus \neg x_3 \oplus (x_4 \oplus x_3$
$\oplus x_2) = \neg x_4 \oplus \neg x_3 \oplus x_4 \oplus x_3 \oplus x_2 = 1 \oplus 1 \oplus x_2 = x_2;$

$f_3(f_3^{-1}(x_1,...,x_4)) = (x_1 \oplus x_3 \oplus x_4) \oplus \neg(x_2 \oplus x_3$
$\oplus x_4) \oplus \neg(x_1 \oplus x_2 \oplus x_3))$
$= (x_1 \oplus x_3 \oplus x_4) \oplus \neg(x_2 \oplus x_3) \oplus (x_2 \oplus x_3) \oplus \neg x_4$
$\oplus \neg x_1 = x_1 \oplus x_3 \oplus x_4 \oplus \neg x_4 \oplus \neg x_1 = 1 \oplus 1 \oplus x_3 = x_3;$

$f_4(f_4^{-1}(x_1,...,x_4)) = \neg((x_1 \oplus x_2 \oplus x_4) \oplus (x_1 \oplus x_3$
$\oplus x_4) \oplus \neg(x_2 \oplus x_3 \oplus x_4)) = \neg(x_1 \oplus x_2 \oplus x_4) \oplus \neg(x_1$
$\oplus x_3 \oplus x_4) \oplus (x_2 \oplus x_3 \oplus x_4) = \neg(x_1 \oplus x_4) \oplus \neg(x_1 \oplus$
$x_4) \oplus \neg x_2 \oplus \neg x_3 \oplus x_2 \oplus x_3 \oplus x_4 = 1 \oplus 1 \oplus x_4 = x_4.$

Thus, $F(F^{-1}(x_1,...,x_4)) = (x_1, x_2, x_3, x_4)$.

Consequently, DCT F_2^d (6) has ICT F_2^r (5).

5 RESULTS

The results of the construction by this method of two CTs are given in Table 11.

Table 11 – The results of application of the method to selected four-bit CTs satisfying a SAC. Direct and inverse CTs satisfy the SAC

Direct CT	Inverse CT
$F_1^d = \begin{bmatrix} \neg(x_1 \oplus x_2 \oplus x_4) \\ \neg(x_1 \oplus x_2 \oplus x_3) \\ x_1 \\ x_2 \end{bmatrix}$	$F_1^r = \begin{bmatrix} x_3 \\ x_4 \\ \neg(x_2 \oplus x_3 \oplus x_4) \\ \neg(x_1 \oplus x_3 \oplus x_4) \end{bmatrix}$
$F_2^d = \begin{bmatrix} \neg(x_1 \oplus x_2 \oplus x_4) \\ x_1 \oplus x_3 \oplus x_4 \\ x_2 \oplus x_3 \oplus x_4 \\ \neg(x_1 \oplus x_2 \oplus x_3) \end{bmatrix}$	$F_2^r = \begin{bmatrix} x_1 \oplus x_2 \oplus x_4 \\ x_1 \oplus x_3 \oplus x_4 \\ \neg(x_2 \oplus x_3 \oplus x_4) \\ \neg(x_1 \oplus x_2 \oplus x_3) \end{bmatrix}$

6 DISCUSSION

The existing methods of searching for an ICT are methods for calculating each element of the BBFs of the ICT, whereas proposed by us method is a method of choosing existing BBFs from a predetermined set of BBFs for a DCT and an ICT. The method can be extended to a larger even number of bits.

This method can be used to obtain other ICTs, having DCTs that have the property of SAC and for which there is an ICT.

To date, in the general case, the total number of balanced BFs of any number of variables with different sets of logical operations on these variables and having the property of a SAC remains unknown [16]. Therefore, the problem of finding systems of balanced BFs with an even number of variables greater than four for different sets of logical operations and having the property of SAC is a separate important scientific problem that goes beyond the scope of this article.

The article [23] presents methods that handle the inverse problem for the main types of solutions of Boolean

DOI 10.15588/1607-3274-2019-4-19

equations of the form $f(X) = 0$, where $f(X)$: $B^n \to B$ and B is an arbitrary Boolean algebra. The methods [23] are a mixture of purely-algebraic methods and map methods that utilize the variable entered Karnaugh map: (a) Subsumptive general solutions, in which each of the variables is expressed as an interval by deriving successive conjunctive or disjunctive eliminants of the original function, (b) Parametric general solutions, in which each of the variables is expressed via arbitrary parameters which are freely chosen elements of the underlying Boolean algebra and (c) Particular solutions, each of which is an assignment from the underlying Boolean algebra to every pertinent variable that makes the Boolean equation an identity. But the application of these methods to Boolean functions of the form (1) was not considered in [23].

In the article [31] a mathematical formalism is developed, showing the connection of the inverse Boolean function of the form (1) with its corresponding direct Boolean function of the form (1). But the method of obtaining an inverse Boolean function from a direct Boolean function is not specified in [31], and the conditions for the existence of an inverse Boolean function for a given direct Boolean function are not indicated.

But the method developed in this article makes it possible to effectively find the ICT for any four-bit DCT of BFs containing only the operations of inversion and addition modulo two and satisfying the restrictions 1–3, described in section 3 of this article.

In further studies using the method described in this article, it is possible to increase an even number of variables, which will increase the nonlinearity and cryptographic resilience of CTs.

CONCLUSIONS

The urgent problem of obtaining the inversion method of four-bit Boolean SAC cryptotransforms is solved to ensure reliable information protection..

The scientific novelty of obtained results is that the method for obtaining inverse four-bit CTs with the SAC property for balanced BFs containing two logical operations (inversion and addition modulo two) is proposed for the first time.

The practical significance of obtained results is that this method is a method of selecting the already existing basic four-bit BFs from a predetermined set of balanced BBFs for direct and inverse CTs, whereas the existing methods of searching for ICT are methods for calculating each element of the BFs for the ICT.

Prospects for further research are the modifications of this method to the larger even numbers of arguments of the balanced BFs of CTs to increase the cryptographic resilience.

ACKNOWLEDGEMENTS

The authors would like to thank Vice-Rector for Research of Cherkasy State Technological University Dr. Sc., Faure Emil Vitaliiovych, the Associate Professor of the Department of Information Security and Computer Engineering of Cherkasy State Technological University Ph.D., Associate Professor Shvydkyi Valerii Vasylovych and Head of the Department of Statistics and Applied Mathematics of Cherkasy State Technological University Ph.D., Associate Professor Shcherba Anatolii Ivanovych for fruitful discussions.

REFERENCES

1. Kemp S. Digital 2019. Essential insights into how people around the world use the Internet, mobile devices, social media, and e-commerce. [Electronic resource]. Access mode: https: //wearesocial.com/global-digital-report-2019.
2. Lakhtaria K. I. Protecting Computer Network with Encryption Technique: A Study, *Communications in Computer and Information Science (UCMA 2011)*, 2011, Vol. 151, No. PART 2, pp. 381–390. DOI: 10.1007/978-3-642-20998-7_47.
3. Debnath S., Linke N. M., Figgatt C. et al. Demonstration of a small programmable quantum computer with atomic qubits, *Nature,* 2016, No. 536, pp. 63–66. DOI: 10.1038/nature18648
4. Harrow A. W., Montanaro A. Quantum computational supremacy, *Nature*, 2017, Vol. 549, pp. 203–209. DOI: 10.1038/nature23458
5. Smart S. E., Schuster D. I., Mazziotti D. A. Experimental data from a quantum computer verifies the generalized Pauli exclusion principle, *Communications Physics*, 2019, Vol. 2, No. 1, pp. 1–6. DOI: 10.1038/s42005-019-0110-3
6. Kolokotronis N., Limniotis K., Kalouptsidis N. Best Affine and Quadratic Approximations of Particular Classes of Boolean Functions, *IEEE transactions on information theory*, 2009, Vol. 55, No. 11, pp. 5211–5222.
7. Menezes A. J., Van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. USA, CRC Press, Inc. Boca Raton, 1996, 810 p.
8. Alzaidi A. A., Ahmad M., Doja M. N. at al. A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes, *IEEE Access*, 2018, Vol. 6, pp. 55405–55418. DOI: 10.1109/ACCESS.2018.2871557.
9. Steinbach B. Problems and New Solutions in the Boolean Domain, UK, Cambridge Scholars Publishing, Newcastle upon Tyne, 2016, 480 p. ISBN (10): 1–4438-8947-4 ISBN (13): 978-1-4438-8947-6.
10. Nielsen M., Chuang I. Quantum Computation and Quantum Information, UK, Cambridge University Press, 2000, 676 p. ISBN 978-1-107-00217-3.
11. Golubitsky O., Maslov D. A study of optimal 4–bit reversible toffoli circuits and their synthesis, *IEEE Transactions on Computers*, 2012, Vol. 61, No. 9, pp. 1341–1353. DOI: 10.1109/TC.2011.144.
12. Bardis E. G., Bardis N. G., Markovski A. P. at al. Design of Boolean Functions from a great number of variables satisfying strict avalanche criterion, *Proceedings of the IEEE/WSES/IMACS : 3rd World multiconference on circuits, systems, communications and computers, Athens, July 1999: proceedings*. Athens, World Scientific, 1999, pp. 3111–3116.
13. Tang D., Zhang W., Tang X. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties, *Designs, Codes and Cryptography*, 2013, Vol. 67, No. 1, pp. 77–99 DOI: 10.1007/s10623-011-9587-9
14. Alzaidi A. A., Ahmad M., Doja M. N. at al. A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes, *IEEE Access*, 2018, Vol. 6, pp. 55405–55418. DOI: 10.1109/ACCESS.2018.2871557

DOI 10.15588/1607-3274-2019-4-19

15. Lloyd S. Counting Functions Satisfying a Higher Order Strict Avalanche Criterion, *EUROCRYPT '89 : Workshop on the Theory and Application of Cryptographic Techniques. Advances in Cryptology, 10–13 April 1989: proceedings*. Berlin, Heidelberg, Springer, 1989, Vol. 434, pp. 63–67. DOI: 10.1007/3-540-46885-4_9
16. Bardis N. G. Combinatorial method for Boolean SAC functions designing, *WSEAS Transactions on Communications*, 2004, Vol. 3, No. 2, pp. 746–752.
17. Gupta Brij B., Dharma P. Agraval, Haoxiang Wang Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives. New York, CRC Press, Taylor & Francis Group, Boca Raton, 2019, 665 p. ISBN 9780815371335.
18. Dey S., Ghosh R. Cryptanalysis of 4-Bit Crypto S-Boxes in Smart Applications, *Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure*. Cham, Springer, 2019, P. 211–253. ISBN 978-3-030-01560-2. DOI: 10.1007/978-3-030-01560-2_10.
19. Woods S., Casinovi G. Efficient solution of systems of Boolean equations, *96 Proceedings of the 1996 IEEE/ACM international conference on Computer-aided design, 10–14 November 1996: proceeding.* San Jose, California, ACM Press, 1996, pp. 542–546.
20. Rudeanu S. Boolean sets and most general solutions of Boolean equations, *Information Sciences*, 2010, Vol. 180, No. 12, pp. 2440–2447. DOI: 10.1016/j.ins.2010.01.029.
21. Baneres D., Cortadella J., Kishinevsky M. A Recursive Paradigm to Solve Boolean Relations, *IEEE Transactions on Computers*, 2009, Vol. 58(4), pp. 512–527. http://doi.ieeecomputersociety.org/10.1109/TC.2008.165
22. Rushdi Ali M. A., Motaz H. Amashah Using variable-entered Karnaugh maps to produce compact parametric general solutions of Boolean equations, *International Journal of Computer Mathematics,* 2011, Vol. 88, No. 15, pp. 3136–3149. DOI: 10.1080/00207160.2011.594505.
23. Rushdi A. M. A., H. M. Albarakati The Inverse Problem for Boolean Equations, *Journal of Computer Science*, 2012, Vol. 8, No. 12, pp. 2098–2105. DOI: 10.3844/jcssp.2012.2098.2105
24. Bibilo P. N. Decomposition of Boolean functions based on the solution of logic equations. I. II. III., *Izvestiya Rossijskoj akademii nauk. Teoriya i sistemy upravleniya,* 2002, No. 4, pp. 53–64; 2002, no.5, pp. 57–63.; 2003, no. 6. – P. 88–97.
25. Rudeanu S. On the Decomposition of Boolean Functions via Boolean Equations, *Journal of Universal Computer Science*, 2004, Vol. 10, No. 9, pp. 1294–1301.
26. Primenko É. A. Equivalence classes of invertible Boolean functions, *Cybernetics*, 1984, Vol. 20, No. 6, pp. 771–776. DOI: 10.1007/BF01072161
27. Soeken M., Wille R., Keszocze O. at al. Embedding of Large Boolean Functions for Reversible Logic, *Journal on Emerging Technologies in Computing Systems*, 2016, Vol. 12, № 4, Article No. 41, pp. 41:1–41:26. DOI: 10.1145/2786982.
28. Soeken M. Abdessaied N., De Micheli G. Enumeration of Reversible Functions and Its Application to Circuit Complexity, *Proceedings of the 8th Conference on Reversible Computation (RC 2016), 7–8 July 2016: proceedings*. Bologna: Cham, Springer, 2016, Vol 9720, pp. 255–270. ISBN: 978-3-319-40578-0. DOI: 10.1007/978-3-319-40578-0_19.
29. Kavut S., Maitra S., Tang D. Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile, *Designs, Codes and Cryptography*, 2019, Vol. 87, No. 2–3, pp. 261–276. DOI: 10.1007/s10623-018-0522-1.
30. Lorens C. S. Invertible Boolean functions, *IEEE Transactions on Electronic Computers*, 1964, Vol. EC–13, No. 5, pp. 529–541. DOI:10.1109/pgec.1964.263724.
31. Varadharajan V., Wu C.-K. Public key cryptosystems based on boolean permutations and their applications, *International Journal of Computer Mathematics*, 2000, Vol. 74, No. 2, pp. 167–184. DOI: 10.1080/00207160008804932.

Received 07.05.2019.
Accepted 26.09.2019.

УДК 004.056

МЕТОД ЗНАХОДЖЕННЯ ОБЕРНЕНИХ ЧОТИРЬОХРОЗРЯДНИХ БУЛЕВИХ КРИПТОПЕРЕТВОРЕНЬ ЗІ СТРОГИМ ЛАВИННИМ КРИТЕРІЄМ

Федотова-Півень І. М. – канд. техн. наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Рудницький В. М. – д-р техн. наук, професор, завідуючий кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Півень О. Б. – канд. фіз.-мат. наук, доцент, професор кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна.

Миронюк Т. В. – канд. техн. наук, доцент кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, Черкаси, Україна.

АНОТАЦІЯ

Актуальність. Нелінійні системи булевих функцій грають важливу роль в захисті криптосистем. Створення і використання нових чотирьохрозрядних криптографічних перетворень з нелінійними булевими функціями, що володіють властивістю строгого лавинного критерію, є актуальним завданням підвищення надійності систем захисту інформації.

Метою роботи є створення методу отримання обернених чотирьохбітових криптографічних перетворень з властивістю строгого лавинного критерію, які містять збалансовані булеві функції лише з операціями інверсії і додавання за модулем два.

Метод. Запропоновано метод отримання обернених чотирьохбітових криптографічних перетворень з властивістю строгого лавинного критерію, кожне з яких містить збалансовані булеві функції тільки з операціями інверсії і додавання за модулем два. Метод спрощує процес пошуку обернених криптографічних перетворень шляхом створення класу з тридцяти збалансованих базових булевих функцій з необхідними наперед визначеними обмеженнями і властивостями, а також знаходження в цьому класі базових булевих функцій, що становлять обернене криптографічне перетворення.

DOI 10.15588/1607-3274-2019-4-19

Результати. Показана ефективність методу для отримання двох обернених чотирьохбітових криптографічних перетворень з властивістю строгого лавинного критерію з двох прямих чотирьохбітових криптографічних перетворень з властивістю строгого лавинного критерію.

Висновки. Вперше запропоновано метод отримання обернених чотирьохбітових криптографічних перетворень з властивістю строгого лавинного критерію для збалансованих булевих функцій, що містять дві логічні операції (інверсія і додавання за модулем два) для забезпечення надійного захисту інформації. Цей метод являє собою метод вибору вже існуючих базових булевих функцій з заздалегідь визначеного набору збалансованих базових булевих функцій для прямого і оберненого криптографічних перетворень, тоді як існуючі методи пошуку оберненого криптографічного перетворення є методами обчислення кожного елемента булевих функцій для оберненого криптографічного перетворення. Метод може бути розширений до більшого парного числа аргументів збалансованих булевих функцій криптографічних перетворень для підвищення криптографічного стійкості.

КЛЮЧОВІ СЛОВА: булеві функції, обернене криптографічне перетворення, збалансованість, строгий лавинний критерій, інверсія, додавання за модулем 2.

УДК 004.056

МЕТОД НАХОЖДЕНИЯ ОБРАТНЫХ ЧЕТЫРЕХРАЗРЯДНЫХ БУЛЕВЫХ КРИПТОПРЕОБРАЗОВАНИЙ СО СТРОГИМ ЛАВИННЫМ КРИТЕРИЕМ

Федотова-Пивень И. Н. – канд. техн. наук, доцент, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Рудницкий В. Н. – д-р техн. наук, профессор, заведующий кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Пивень О. Б. – канд. физ.-мат. наук, доцент, профессор кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина.

Миронюк Т. В. – канд. техн. наук, доцент кафедры информационной безопасности и компьютерной инженерии, Черкасский государственный технологический университет, Черкассы, Украина.

АННОТАЦИЯ

Актуальность. Нелинейные системы булевых функций играют важную роль в защите криптосистем. Создание и использование новых четырехразрядных криптографических преобразований с нелинейными булевыми функциями, обладающими свойством строгого лавинного критерия, является актуальной задачей повышения надежности систем защиты информации. Целью работы является создание метода получения обратных четырехбитовых криптографических преобразований со свойством строгого лавинного критерия, которые содержат сбалансированные булевы функции только с операциями инверсии и сложения по модулю два.

Метод. Предложен метод получения обратных четырехбитовых криптографических преобразований со свойством строгого лавинного критерия, каждое из которых содержит сбалансированные булевы функции только с операциями инверсии и сложения по модулю два. Метод упрощает процесс поиска обратных криптографических преобразований путем создания класса из тридцати сбалансированных базовых булевых функций с требуемыми предопределенными ограничениями и свойствами, а также нахождения в этом классе базовых булевых функций, составляющих обратное криптографическое преобразование.

Результаты. Показана эффективность метода для получения двух обратных четырехбитовых криптографических преобразований со свойством строгого лавинного критерия из двух прямых четырехбитовых криптографических преобразований со свойством строгого лавинного критерия.

Выводы. Впервые был предложен метод получения обратных четырехбитовых криптографических преобразований со свойством строгого лавинного критерия для сбалансированных булевых функций, содержащих две логические операции (инверсия и сложение по модулю два) для обеспечения надежной защиты информации. Этот метод представляет собой метод выбора уже существующих базовых булевых функций из заранее определенного набора сбалансированных базовых булевых функций для прямого и обратного криптографических преобразований, тогда как существующие методы поиска обратного криптографического преобразования представляют собой методы для вычисления каждого элемента булевых функций для обратного криптографического преобразования. Метод может быть расширен до большего четного числа аргументов сбалансированных булевых функций криптографических преобразований для повышения криптографической стойкости.

КЛЮЧЕВЫЕ СЛОВА: булевы функции, обратное криптографическое преобразование, сбалансированность, строгий лавинный критерий, инверсия, сложение по модулю 2.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Kemp S. Digital 2019. Essential insights into how people around the world use the Internet, mobile devices, social media, and e-commerce. [Electronic resource] / S. Kemp. – Access mode: https: //wearesocial.com/global-digital-report-2019.
2. Lakhtaria K. I. Protecting Computer Network with Encryption Technique: A Study / K. I. Lakhtaria // Communications in Computer and Information Science (UCMA 2011). – 2011. – Vol. 151, No. PART 2. – P. 381–390. DOI: 10.1007/978-3-642-20998-7_47.
3. Demonstration of a small programmable quantum computer with atomic qubits / [S. Debnath, N. M. Linke, C. Figgatt et al.] // Nature. – 2016. – № 536. – P. 63–66. DOI: 10.1038/nature18648
4. Harrow A. W. Quantum computational supremacy / A. W. Harrow, A. Montanaro // Nature. – 2017. – Vol. 549. – P. 203–209. DOI: 10.1038/nature23458

DOI 10.15588/1607-3274-2019-4-19

5. Smart S. E. Experimental data from a quantum computer verifies the generalized Pauli exclusion principle / S. E. Smart, D. I. Schuster, D. A. Mazziotti // Communications Physics. – 2019. – Vol. 2, № 1. – P. 1–6. DOI: 10.1038/s42005-019-0110-3
6. Kolokotronis N. Best Affine and Quadratic Approximations of Particular Classes of Boolean Functions / N. Kolokotronis, K. Limniotis, N. Kalouptsidis // IEEE transactions on information theory. – 2009. – Vol. 55, № 11. – P. 5211–5222.
7. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. – USA : CRC Press, Inc. Boca Raton, 1996. – 810 p.
8. A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes / [A. A. Alzaidi, M. Ahmad, M. N. Doja at al.] // IEEE Access. – 2018. – Vol. 6. – P. 55405–55418. DOI: 10.1109/ACCESS.2018.2871557.
9. Steinbach B. Problems and New Solutions in the Boolean Domain / B. Steinbach. – UK: Cambridge Scholars Publishing, Newcastle upon Tyne, 2016. – 480 p. ISBN (10): 1–4438-8947-4 ISBN (13): 978-1-4438-8947-6.
10. Nielsen M. Quantum Computation and Quantum Information / M. Nielsen, I. Chuang. – UK: Cambridge University Press, 2000. – 676 p. ISBN 978-1-107-00217-3.
11. Golubitsky O. A study of optimal 4-bit reversible toffoli circuits and their synthesis / O. Golubitsky, D. Maslov // IEEE Transactions on Computers. – 2012. – Vol. 61, № 9. – P. 1341–1353. DOI: 10.1109/TC.2011.144.
12. Design of Boolean Functions from a great number of variables satisfying strict avalanche criterion / [E. G. Bardis, N. G. Bardis, A. P Markovski at al.] // Proceedings of the IEEE/WSES/IMACS : 3rd World multiconference on circuits, systems, communications and computers, Athens, July 1999: proceedings. – Athens: World Scientific, 1999. – P. 3111–3116.
13. Tang D. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties / D. Tang, W. Zhang, X. Tang // Designs, Codes and Cryptography. – 2013. – Vol. 67, № 1. – P. 77–99 DOI: 10.1007/s10623-011-9587-9
14. A New 1D Chaotic Map and β-Hill Climbing for Generating Substitution-Boxes / [A. A. Alzaidi, M. Ahmad, M. N. Doja at al.] // IEEE Access. – 2018. – Vol. 6. – P. 55405 – 55418. DOI: 10.1109/ACCESS.2018.2871557
15. Lloyd S. Counting Functions Satisfying a Higher Order Strict Avalanche Criterion / S. Lloyd // EUROCRYPT ’89 : Workshop on the Theory and Application of Cryptographic Techniques. Advances in Cryptology, 10–13 April 1989: proceedings. – Berlin, Heidelberg: Springer, 1989. – Vol. 434. – P. 63–67. DOI: 10.1007/3-540-46885-4_9
16. Bardis N. G. Combinatorial method for Boolean SAC functions designing / N. G. Bardis // WSEAS Transactions on Communications. – 2004. – Vol. 3, № 2. – P. 746–752.
17. Gupta Brij B. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives / Brij B. Gupta, Dharma P. Agraval, Haoxiang Wang. – London, New York: CRC Press, Taylor & Francis Group, Boca Raton, 2019. – 665 p. ISBN 9780815371335.
18. Dey S. Cryptanalysis of 4-Bit Crypto S-Boxes in Smart Applications / S. Dey, R. Ghosh // Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. – Cham: Springer, 2019. – P. 211–253. ISBN 978-3-030-01560-2. DOI: 10.1007/978-3-030-01560-2_10.
19. Woods S. Efficient solution of systems of Boolean equations / S. Woods, G. Casinovi // 96 Proceedings of the 1996 IEEE/ACM international conference on Computer-aided design, 10–14 November 1996: proceeding. – San Jose, California : ACM Press, 1996. – P. 542–546.
20. Rudeanu S. Boolean sets and most general solutions of Boolean equations / S. Rudeanu // Information Sciences. – 2010. – Vol. 180, № 12. – P. 2440–2447. DOI: 10.1016/j.ins.2010.01.029.
21. Baneres D. A Recursive Paradigm to Solve Boolean Relations / D. Baneres, J. Cortadella, M. Kishinevsky // IEEE Transactions on Computers. – 2009. – Vol. 58(4). – P. 512–527.http://doi.ieeecomputersociety.org/10.1109/TC.2008.165
22. Rushdi Ali M. A. Using variable-entered Karnaugh maps to produce compact parametric general solutions of Boolean equations / Ali M. A. Rushdi, Motaz H. Amashah // International Journal of Computer Mathematics. – 2011. – Vol. 88, № 15. – P. 3136–3149. DOI: 10.1080/00207160.2011.594505.
23. Rushdi A. M. A. The Inverse Problem for Boolean Equations / A. M. A. Rushdi, H. M. Albarakati // Journal of Computer Science. – 2012. – Vol. 8, № 12. – P. 2098–2105. DOI: 10.3844/jcssp.2012.2098.2105
24. Bibilo P.N. Decomposition of Boolean functions based on the solution of logic equations. I. II. III. / P. N. Bibilo // Izvestiya Rossijskoj akademii nauk. Teoriya i sistemy upravleniya. – 2002. – No. 4. – P. 53–64; 2002. – No.5. – P. 57–63.; 2003. – No. 6. – P. 88–97.
25. Rudeanu S. On the Decomposition of Boolean Functions via Boolean Equations / S. Rudeanu // Journal of Universal Computer Science. – 2004. – Vol. 10, № 9. – P. 1294–1301.
26. Primenko É. A. Equivalence classes of invertible Boolean functions / É. A. Primenko // Cybernetics. – 1984. – Vol. 20, № 6. – P. 771–776. DOI: 10.1007/BF01072161
27. Soeken M. Embedding of Large Boolean Functions for Reversible Logic / [M. Soeken, R. Wille, O. Keszocze et al.] // Journal on Emerging Technologies in Computing Systems. – 2016. – Vol. 12, № 4, Article No. 41. – P. 41:1–41:26. DOI: 10.1145/2786982.
28. Soeken M. Enumeration of Reversible Functions and Its Application to Circuit Complexity / M. Soeken, N. Abdessaied, G. De Micheli // Proceedings of the 8th Conference on Reversible Computation (RC 2016), 7–8 July 2016: proceedings. – Bologna: Cham, Springer, 2016. – Vol. 9720. – P. 255–270. ISBN: 978-3-319-40578-0. DOI: 10.1007/978-3-319-40578-0 19.
29. Kavut S. Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile / S. Kavut S. Maitra, D. Tang // Designs, Codes and Cryptography. – 2019. – Vol. 87, № 2–3. – P. 261–276. DOI: 10.1007/s10623-018-0522-1.
30. Lorens C. S. Invertible Boolean functions / C. S Lorens // IEEE Transactions on Electronic Computers – 1964 – Vol. EC–13, № 5. – P. 529–541. DOI:10.1109/pgec.1964.263724.
31. Varadharajan V. Public key cryptosystems based on boolean permutations and their applications / V. Varadharajan, C.-K. Wu // International Journal of Computer Mathematics. – 2000. – Vol. 74, № 2. – P. 167–184. DOI: 10.1080/00207160008804932.

DOI 10.15588/1607-3274-2019-4-19

УПРАВЛІННЯ У ТЕХНІЧНИХ СИСТЕМАХ

CONTROL IN TECHNICAL SYSTEMS

УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

UDC 004.942:656.61.052

AUTOMATIC COLLISION AVOIDANCE WITH MULTIPLE TARGETS, INCLUDING MANEUVERING ONES

Zinchenko S. M. – PhD, Senior Lecturer of Ship Management Department, head of the laboratory of electronic simulators, Kherson State Maritime Academy, Ukraine.

Nosov P. S. – PhD, Associate Professor of Navigation Systems Department, Kherson State Maritime Academy, Ukraine.

Mateychuk V. M. – Assistant of Ship Management Department, head of the laboratory of electronic simulators, Kherson State Maritime Academy, Ukraine.

Mamenko P. P. – Senior Lecturer of Ship Management Department , deep sea captain, Kherson State Maritime Academy, Ukraine.

Grosheva O. O. – Senior Lecturer of Ship Management Department, Kherson State Maritime Academy, Ukraine.

ABSTRACT

Context. There is considered the task of automatic collision avoidance with multiple targets, including maneuvering ones. The object of the research is the process of automatic collision avoidance with multiple targets, including maneuvering ones. The subject of research is the method and algorithms that implement the process of automatic collision avoidance from multiple targets, including maneuvering ones.

Objective. The purpose of the article is development a method and algorithms for automatic collision avoidance from multiple targets, including maneuvering ones, for the module of the onboard controller of the ship control system.

Method. This goal is achieved by periodically measuring the true speed of the vessel and relative speeds of the vessel and targets, averaging the measured information to remove noise, estimating the true speeds of the targets, building, for the obtained estimates of the true speeds of the targets, areas of allowable collision avoidance controls with each targets by numerical iteration of the collision avoidance parameters (speed and course) at the nodes of a given grid in the area of their possible changes, determining the relative speeds at the nodes of the grid ship and target movement and checking that the relative speeds don't belong to sectors of dangerous courses, building a general area of acceptable collision avoidance controls with all targets by combining areas of allowable collision avoidance controls with each target, choosing collision avoidance parameters from the general area of acceptable collision avoidance controls according to specified criteria. This allows to diverge from multiple targets, including maneuvering ones, in a fully automatic mode. Changing the criteria for selecting discrepancy parameters leads to a change in the ship's behavior in case of discrepancy without changing the program code.

Results. The developed method and algorithms are implemented in software and investigated by solving the problem of collision avoidance from multiple targets, including maneuvering ones, in a fully automatic mode in a closed circuit with the simulator Navi Trainer 5000 for various types of ships, targets, navigation areas and weather conditions.

Conclusions. The experiments confirmed the performance of the proposed method and algorithms and allow to recommend them for practical use in the development of modules for automatic collision avoidance with multiple targets, including maneuvering ones, of the onboard controller of the ship control system.

KEYWORDS: ship collision avoidance system, automatic collision avoidance, collision avoidance from maneuvering targets, collision avoidance, area of allowable controls.

ABBREVIATIONS

AIS is a Automatic Identification System;

ARPA is a automatic radar plotting aid;

BCS is a bound coordinate system; is located in the center of rotation of the vessel, the axis OX lies in the center plane and is directed forward, the axis OY is perpendicular to the center plane and directed towards the starboard, the axis OZ complements the system to the "right" one.

COLREG is an international rules for preventing collisions;

ERML is an expected relative movement line;

DOI 10.15588/1607-3274-2019-4-20

GCS is a geographical coordinate system; is located in the center of rotation of the vessel, the axis OXg is directed along the meridian towards the North, the axis

LOG is a device for determining the speed of the vessel;

LSM is a least– squares method;

OYg is directed along the parallel towards the East, the axis OZg complements the system to the "right";

RADAR is a radar station;

RML is a relative movement line;

SDC is a sector of dangerous courses;

NOMENCLATURE

b_j is a linear coefficients of the RML equation for the *j*-target;

D_{mj} is a measured distance to the *j*-target;

D_{sa} is a area of safe collision avoidance;

$\mathbf{E}_{0j}$ is a ort, wich indicates the direction from lead point of *j*-target to the vessel;

$\mathbf{E}_{1j}$ is a ort, wich indicates the direction of $ELRM_1$ for the *j*-target;

$\mathbf{E}_{2j}$ is a ort, wich indicates the direction of $ELRM_2$ for the *j*-target;

k_j is a angular coefficients of the RML equation for the *j*-target;

K_{n1} is a course of safe collision avoidance;

K_{tgj} is a-true course of *j*-target;

K_T is a trial values of course;

k_Ψ is a angle gain factor;

k_ω is a angular speed gain factor;

$k_\int$ is a angle integral gain factor;

N is a number of RADAR measurements for building RML.

N_{tg} is a number of targets;

OE_j is a distance to lead point of *j*-target.

P_{mj} is a measured bearing to the *j*-target;

$\mathbf{U}$ is a flow influence;

$\mathbf{V}_m$ is a measured linear speed vector;

$V_{\max}$ is a maximum ship speeds;

$V_{\min}$ is a minimum ship speed;

$\mathbf{V}_n$ is a linear speed vector;

V_{n1} is a speed of safe collision avoidance;

$\mathbf{V}_T$ is a trial vector of speed;

V_T is a trial values of speed;

$\mathbf{V}_{tgj}$ is a-true speed vector of *j*-target;

V_{tgj} is a module true speed vector of *j*-target;

$\mathbf{W}$ is a wind influence;

$\mathbf{X}_n$ is a state vector of own vessel;

X_n is a absolute ship movement along the axis OX_g in GCS;

$\mathbf{X}_{tgj}$ is a state vector of *j*-target;

X_{tgj} is a-absolute movement of the *j*-target along the OX_g – acis in GCS;

Y_n is a absolute ship movement along the axis OY_g in GCS;

Y_{tgj} is a absolute movement of the *j*-target along the OY_g is a acis in GCS;

δ is a angles deflection of rudder;

ΔT is a period of information processing in the onboard computer;

$\mathbf{\Delta V}_j$ is a relative speed vector of the vessel and *j*-target;

$\mathbf{\Delta V}_{Tj}$ is a trial values of the relative speed of the vessel and the *j*-target;

ΔV_{xj} is a relative speed OX-projection in BCS;

ΔV_{yj} is a relative speed OY-projection in BCS;

ΔX_{mj} is a measured OX-projection of distance between the vessel and the *j*-target in GCS;

ΔY_{mj} is a measured OY-projection of distance between the vessel and the *j*-target in GCS;

θ is a angles deflection of telegraph;

Θ_j is a angle, equal to half the SDC for the *j*-target;

Ψ_m is a measured heading;

Ψ_n is a heading;

Ω_j is a areas of admissible control of collision avoidance with *j*-target;

ω_{mz} is a measured angular speed in BCS;

ω_{nz} is a angular speed in BCS.

INTRODUCTION

The article discusses the issues of automatic collision avoidance with multiple targets, including maneuvering ones. Currently, the main international legal document, regulating the safety of navigation, is the Rules COLREG-72 [1], adopted in 1972 and put into operation since 1977, and the technical equipment of collision avoidance are RADAR / ARPA [2–3].

Recently, the speed of ships and the intensity of navigation have significantly increased, which has caused a significant increase in the flow of information per unit of time. It becomes increasingly difficult for navigators to make the right decisions to prevent the development of dangerous situations. Statistics of accidents in the global maritime industry shows that 75–80% of all accidents occur with the direct participation of a person. The human factor today is the most dangerous element of the ship management system. Analyzing these data, the experts

DOI 10.15588/1607-3274-2019-4-20

concluded that a significant reduction in accidents can be achieved only by reducing the influence of the human factor on the management process. Modern ships have become increasingly equipped with automatic and automated control systems. The use of such systems improves reliability, accuracy and flexibility, and also provides new opportunities through the use of modern mathematical tools. Automatic systems are also much cheaper than traditional ones with the crew.

Technical equipmet of collision avoidance RADAR / ARPA allow to capture, track and diverge with 40 targets at the same time. However, RADAR / ARPA is an automated equipment and involves the participation of man in the collision avoidance. Thus, neither the COLREG-72 Rules nor the RADAR / ARPA technical equipment meet the current trends in the automation of ship traffic control in conditions of increased speeds and traffic flows.

In open sources [5–13], a more detailed analysis of which will be done in the next section, various solutions to the problems of automatic collision avoidance are proposed, but all of them allow to collision avoidance with only a few (from one to three) non-maneuvering targets, despite the fact that the existing RADAR / ARPA equipment allows to capture and accompany a much larger number of targets (up to 40). Therefore, the development of systems of collision avoidance with multiple targets, including maneuvering ones, is an actual scientific and technical problem.

The object of research is the process of automatic collision avoidance with multiple targets, including maneuvering ones.

The subject of research is the method and algorithms that implement the process of automatic collision avoidance from multiple targets, including maneuvering ones.

The purpose of this article is development a method and algorithms for automatic collision avoidance from multiple targets, including maneuvering ones, for the module of the onboard controller of the ship control system.

1 PROBLEM STATEMENT

The are specified a mathematical model of a controlled object (own vessel) in the form of a system of nonlinear differential equations

$$\frac{d\mathbf{X}_n}{dt} = \mathbf{f}_n(\mathbf{X}_n, \mathbf{W}, \mathbf{U}, \theta, \delta),$$
$$\mathbf{X}_n = (\mathbf{V}_n, \omega_n, \Psi_n, X_n, Y_n),$$

models of external influences of wind $\mathbf{W} = \mathbf{f}_w(\mathbf{t})$ and flow $\mathbf{U} = \mathbf{f}_u(\mathbf{t})$. The measured linear speed of the vessel $\mathbf{V}_m$, angular velocity ω_m, yaw angle Ψ_m, bearing P_{mj} and distance D_{mj} to each target take into account the measurement errors determined by the passport data of each sensors. Mathematical models of targets are also specified in the form of a system of nonlinear algebraic equations $\mathbf{f}_{tgj}(X_{tgj}, Y_{tgj}, V_{tgj}, K_{tgj}), j = 1, 2, ..., N_{tg}$ that define the parameters of the movement of targets along a route (speeds and courses), as well as target paths with break points to simulate target maneuvers.

Required for given initial conditions – the position of own vessel $\mathbf{X}_n(0)$, the position of targets $\mathbf{X}_{tgj}(0), j = 1, 2, ..., N_{tg}$, specified parameters of movement of targets on routes, specified routes, external influences, measurement errors of motion parameters, determine such controls that would allow to diverge from specified targets, including maneuvering ones at a safe distance $(X_n - X_{tgj})^2 + (Y_n - Y_{tgj})^2 >= {D_{s.a}}^2, j = 1, 2, ..., N_{tg}$.

2 LITERATURE REVIEW

The main international legal document regulating the safety of navigation today is the COLREG–72. The rules apply only in cases where there is a danger of collision. Rules COLREG–72 are verbal (and therefore sometimes interpreted by navigators differently), are more focused on the intuition of the navigator and not on exact mathematical calculation, consider only the consistent collision avoidance of the two vessels. After installation on ships of the radar, it became possible to measure the parameters of the relative movement of the vessel and targets, as well as to carry out manually graphic constructions on a maneuverable tablet to determine the parameters of collision avoidance [2]. This method of calculating the parameters of the collision avoidance has not high accuracy and is also very labor intensive. To automate calculations, modern radar systems have been installed on modern ships. ARPA [3–4] frees the navigator from a variety of manual operations, and the built-in function “Playback maneuver” provides the navigator with a convenient graphical interface for solving problems of collision avoidance. However, ARPA has significant drawbacks:

–ARPA is an automated system that assumes the presence of a person in the control loop;

“The Replay Maneuver” function of the ARPA provides the navigator with only a convenient graphical interface, but the determination of the parameters of the collision avoidance is still carried out manually “by eye”, rather than relying on an exact mathematical calculation that takes time;

–ARPA function “Playing maneuver”, as with manual radar laying, does not allow to diverge from maneuvering targets, since the task is solved one-time, before the beginning of the diversion maneuver.

A lot of works of authors are also devoted to the issues of automatic collision avoidance.

Thus, in article [5] proposed an automatic collision avoidance system based on deep Q-learning. The advantage of this method is to obtain information from the environment with which the system interacts, which can be used to optimize the behavior of the system. At the

DOI 10.15588/1607-3274-2019-4-20

same time, Q-learning takes time, organizing storage of information, its quick retrieval, as well as database maintenance. In addition, during Q-training, the system may not work optimally or even mistakenly, which is fraught with serious consequences.

The article [6] describes a method for assessing the risk of collision of ships, based on a complex non-linear relationship between the degree of risk of collision and the influencing factors. Collision risk assessments with expert information on collision avoidance experience, are entered into a database for subsequent use. The authors proposed a regression model that is trained on the basis of existing samples, in order to increase the accuracy and speed of prediction. The solution proposed by the authors involves training the system, which is not permissible during ships diverge. In addition, the learning process is associated with a long accumulation of information, the use of databases, the organization of quick retrieval of information from the database as well as the need for additional maintenance of the database.

The article [7] describes the track planning method, taking into account the dynamic characteristics of the control object and the rules of COLREGS-72 to prevent possible collisions. The method takes into account the uncertainty of the trajectory in time. The risk of collision is calculated using the probabilistic method, and the risk zone of collision is adjusted to the predicted trajectory. Also presented are simulation results that demonstrate the feasibility of the proposed approach with examples of shipping. The propoused method allows to estimate the risk of collision with non-maneuvering targets, does not form controls for implementing the collision avoidance in the automatic mode and can only be used in automated decision support systems.

The article [8] describes the use of AIS for tracking the movement of targets through electronic exchange of navigation data between ships with onboard transceivers, ground and / or satellite base stations. The data collected contains a large amount of information useful for safety at sea and is used for: detecting anomalies of movement of targets, route estimation, collision prediction and path planning. The use of AIS data provides great opportunities for ships collision avoidance due to more accurate information about the parameters of their movement, however, this method doesn't allow to diverge from not equipped with AIS ships or ships that hide information about the parameters of their movement.

The article [9] describes the method of support decisions in the case of collision avoidance of ships at sea. The method is based on the use of the COLREG-72 and the accumulated experience of collision avoidance. The described method assumes the presence of a person in the control loop and the use of the Rules of the COLREG-72 for collision avoidance. Since the COLREG-72 Rules regulate collision avoidance with only one non-maneuvering vessel, it cannot be used to automatically diverge with multiple targets, including maneuvering ones.

As a result of the analysis, the authors article [10] came to the conclusion that the collision avoidance algorithms developed over the past decades suppouse the absence of maneuvering targets in the collision avoidance process; collision avoidance from only two targets, simplified dynamics of vessel and targets, etc. A collision avoidance algorithm and a collision avoidance system are proposed. The system visualizes changes course and speed of the vessel, leading to a collision, that can be used in manual control and in decision support systems. Collision avoidance system can also offer evading controls that comply with the Rules and have a minimum number of operations.

This system is closest to the proposed by the authors system of automatic collision avoidance with multiple targets, including maneuvering ones.

A method of collision avoidance using predictive models was described in [11]. Mathematical modeling in the onboard computer predicts the trajectory of the vessel and the target using the measured at the current time parameters of the movement of the vessel and the estimated movement parameters of the target. This forecast, taking into account the rules of the COLREG – 72, is used to determine the optimal collision avoidance management strategy. The disadvantage of this method is the large load on the onboard computer due to the need to implement a variety of forecasts in real time, as well as the possibility of collision avoidance with only one vessel.

The article [12] describes the method of probabilistic obstacle handling based on information from a radar sensor with target tracking, that considers measurement and tracking uncertainties is proposed. A grid based path search algorithm, that takes the information from the probabilistic obstacle handling into account, is then used to generate evasive trajectories.

The article [13] presents a combined Nonlinear Model Predictive Control for position and velocity tracking of underactuated surface vessels, and collision avoidance of static and dynamic objects into a single control scheme with sideslip angle compensation and environmental disturbances counteraction. A three-degree-of-freedom dynamic model is used with only two control variables: namely, surge force and yaw moment. Nonlinear disturbance observer is used to estimate disturbances in order to be fed into the prediction model and enhance the robustness of the computer. Collision avoidance is embedded into the trajectory tracking control problem as a time-varying nonlinear constraint of position states to account for static and dynamic obstacles.

The article [14] describes an approach to real-time collision avoidance that complies with the COLREGS rules for Unmanned Surface Vehicle. The Evidential Reasoning theory is employed to evaluate the collision risks with obstacles encountered and trigger a prompt warning of a potential collision. Then, is extended and adopted the optimal reciprocal collision avoidance algorithm so as to determine a collision avoidance maneuver that is COLREGS compliant. The proposed

DOI 10.15588/1607-3274-2019-4-20

approach takes into consideration the fact that other obstacles also sense their surroundings and react accordingly, conforming to a practical marine situation when making a decision concerning collision-free motion.

3 MATERIALS AND METHODS

This article solves the problem of collision avoidance from multiple targets, including maneuvering ones. The structural diagram of the simulation objects is shown in Fig. 1.

The onboard computer 7 receives the parameters of the state vector of the vessel in the ACS as well as the distances and bearings to each target, measured by the radar 12 and comparator 5.

Block 8 of receiving and converting information reads incoming data with a period of information processing, scales it, translates it into a numeric code and feeds the inputs of modules 7.1–7.n to solve various applied control problems, in particular, in module 7.1. The considered problem of managing the collision avoidance with multiple targets, including maneuvering ones, is solved. The required course values and speeds of collision avoidance from the output of module 7.1 of the calculator are fed respectively to autopilot 3 and to the power energy installation 6, the outputs of which, taking into account the inertia and delays, are controls of the object 4. In addition to the considered controls, the object 4 is also affected by external disturbances 1 in the form of wind and current speeds. The combined effect of controls and disturbances on the control object 4 determines its movement, which at each moment of time is characterized by a state vector. Unit 2 models the movement of targets in the same GCS, in which the movement of the control object 4 itself is modeled. Fig. 2 shows the scheme of collision avoidance of own ship O with two ships – targets O_1 and O_2. The reasoning below is also valid for collision avoidance from any number of targets.

Own ship O (see Fig. 2a) moves with measured speed $\mathbf{V}_m$. Around own ship is drawn the safe area Ds.a. Through the point of the last measurement (p. N) of the target position, the relative movement lines RML_1, RML_2 are drawn, which are built in the onboard computer of the vessel according to a series of observations $1, 2, ..., N$ from the radar, using the least-squares method.

The essence of the LSM is the preliminary accumulation of the measured radar information on the bearing and the distance for each target for 15–30 antenna turns, recalculation of the measured data in the Cartesian coordinate system

$$\Delta X_{mj}(i) = D_{mj}(i)\cos(P_{mj}(i)),$$
$$\Delta Y_{mj}(i) = D_{mj}(i)\sin(P_{mj}(i)), i = 1, 2, ..., N;$$

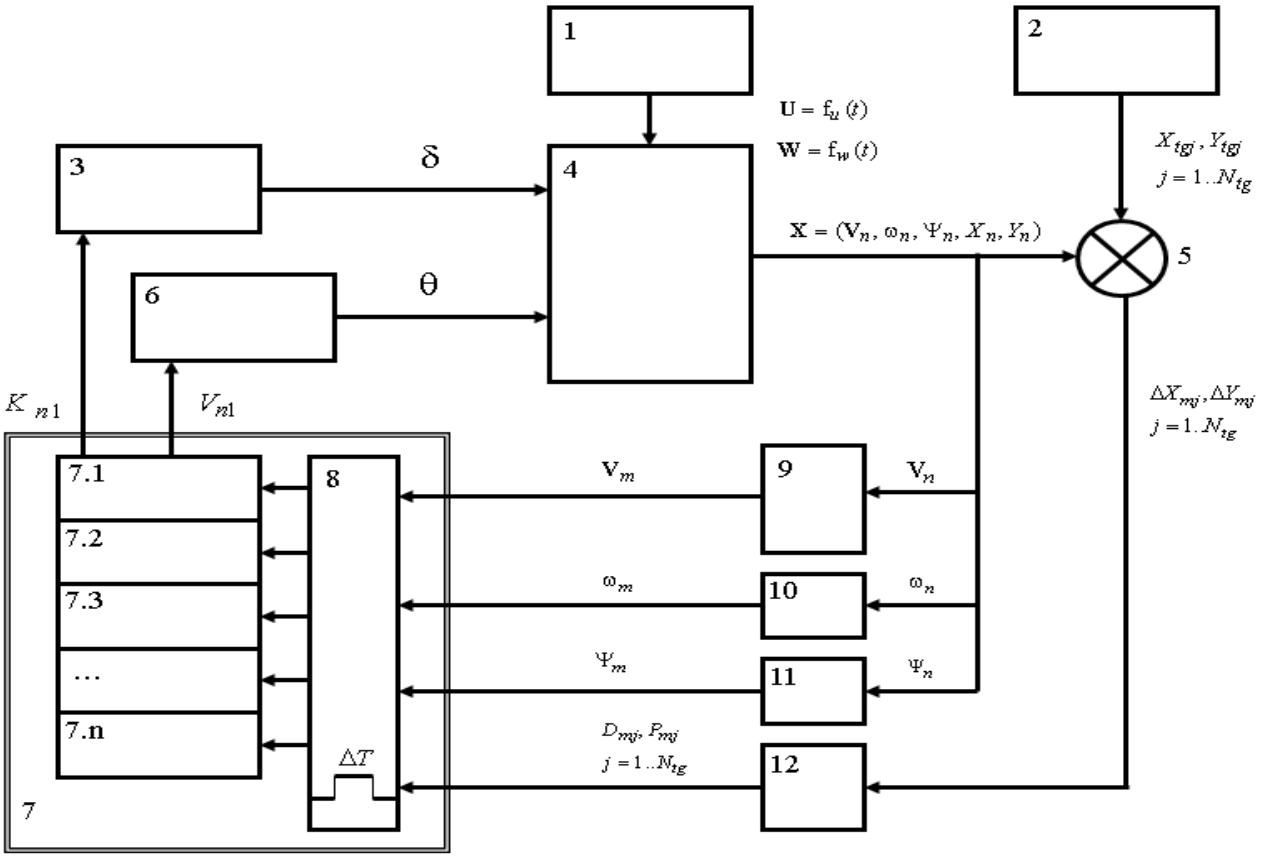


Figure 1 – Structural diagram of the objects of modeling

DOI 10.15588/1607-3274-2019-4-20

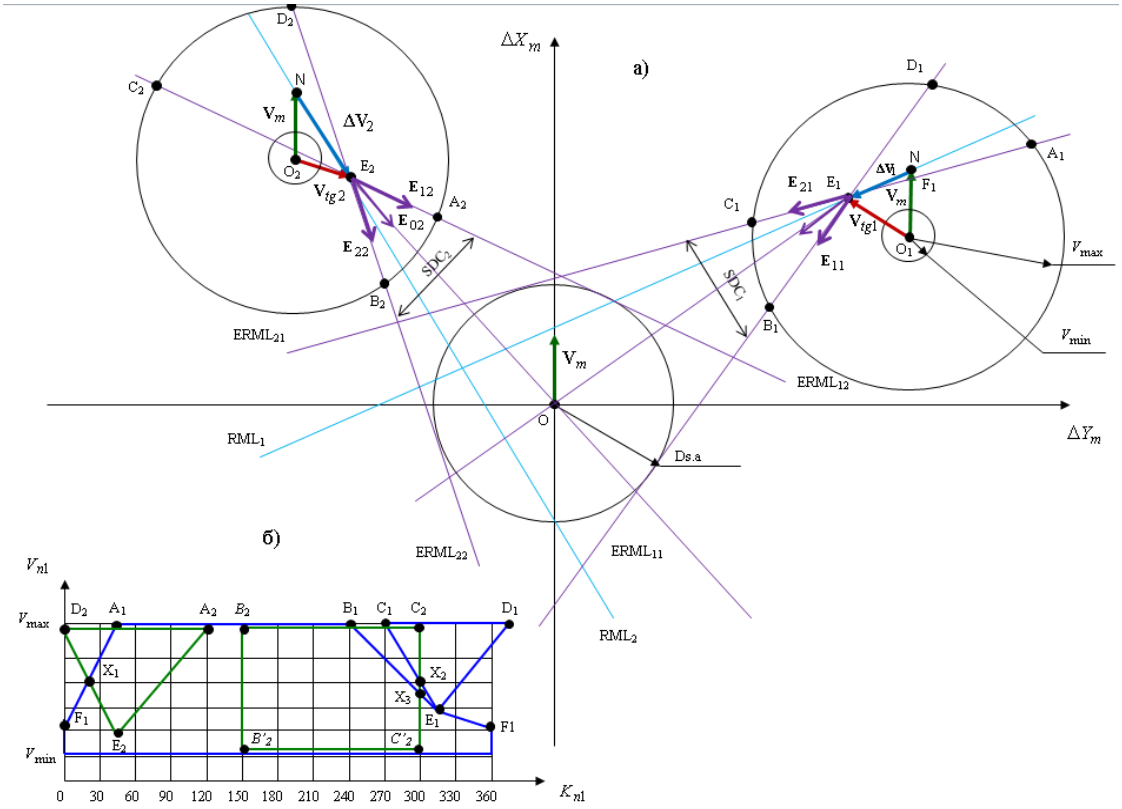


Figure 2 – Diagram of the collision avoidance

with the subsequent approximation of the accumulated data by a RML. This method is currently widely used in ARPA. Further, using the koefficients $k_j, b_j, j = 1,2,....,N_{tg}$ RML equation, the measured coordinates of the target are specified so that they lie on the RML, thus eliminating fluctuation errors in radar measurements

$$\Delta X_{mj}(1) = k_j \Delta Y_{mj}(1) + b_j,$$

$$\Delta X_{mj}(N) = k_j \Delta Y_{mj}(N) + b_j, j = 1,2,...., N_{tg},$$

estimated vector $\mathbf{\Delta V}_j = (\Delta V_{xj}, \Delta V_{yj})$ relative vessel speed and j-target

$$\Delta V_{xj} = (\Delta X_{mj}(N) - \Delta X_{mj}(1))/(\Delta T(N-1)),$$

$$\Delta V_{yj} = (\Delta Y_{mj}(N) - \Delta Y_{mj}(1))/(\Delta T(N-1)),$$

and also computes the true speed vector of the j-target

$$\mathbf{V}_{tgj} = \mathbf{V}_m + \mathbf{\Delta V}_j .$$

In Fig. 2a shows speed triangles $(\mathbf{V}_m, \mathbf{\Delta V}_j, \mathbf{V}_{tgj}, j = 1,2)$, built for 2 targets at last measurement points (p. N). Lead points E_1 (E_2), pushed forward by RML_1 (RML_2) regarding p. N the distance required to change the motion parameters of the vessel in case of collision avoidance (determined by its maneuverability characteristics). $ERML_{11}$, $ERML_{21}$, $ERML_{12}$, $ERML_{22}$ – tangents to the safe area, drawn from points E_1 (E_2). $ERML_{11}$, $ERML_{21}$ and $ERML_{12}$, $ERML_{22}$ form sectors of dangerous courses SDC_1 and SDC_2 accordingly, in which the vector of relative speed of the vessel and targets should not be located in case of collision avoidance. In the Fig. 2 vector $\mathbf{\Delta V_1} \in SDC_1$ and vector $\mathbf{\Delta V_2} \in SDC_2$, both targets are dangerous and collision avoidance is required. Change the direction of vectors $\mathbf{\Delta V_1}$, $\mathbf{\Delta V_2}$ can only be due to a change in the speed vector of the own vessel (the speed vector of the target is not available for control). As can be seen from Fig. 2a, fulfillment of conditions $\mathbf{V}_m \in \Omega_1$ and $\mathbf{V}_m \in \Omega_2$ allows to avoid colission with both targets, where Ω_1 – the area of allowable controls in case of collision avoidance with the first targets, is the area between the circles V_{max} and V_{min}, without SDC_1, and Ω_2 – the area of admissible controls in case of collision avoidance with the second targets, is the area between the circles V_{max} and V_{min}, wthout SDC_2. In Fig. 2b, these areas are also shown in Cartesian coordinates. (Ω_1 bounded by blue lines, and Ω_2 bounded by green lines).

General area $\Omega = \Omega_1 \bigcap \Omega_2$ consists of three subdomains: A1-X1-E2-A2, B2-B2'-C2'-X3-B1, C1-X2-C2 and is an area of allowable controls in case of collision avoidance with two targets at the same time.

As you can see, the area Ω is complex even for two targets and its analytical construction is difficult. In this regard, the authors proposed:

– the area of allowable controls should be built numerically in the onboard computer, which allows obtaining complex forms for any number of targets;

– the area of allowable controls should be built with a period of processing collision avoidance algorithms in the

DOI 10.15588/1607-3274-2019-4-20

onboard computer, which allows to take into account any changes in the mutual movement of the vessel and the targets, and therefore to diverge from the maneuvering targets.

To build the area $\Omega_j, j = 1..N_{tg}$ allowable control of collision avoidance with the j-target are taken trial vectors of collision avoidance $\mathbf{V}_T = (V_T \cos K_T, V_T \sin K_T)$ in the grid nodes of the whole area (in Fig. 2b between $V_{\min}, V_{\max}$ on the speed and between 0 and 360 degrees on the course), for each trial vector, a trial vector of relative motion is calculated with the j-target $\mathbf{\Delta V}_{Tj} = \mathbf{V}_{tgj} - \mathbf{V}_T$, which is checked for belonging SDCj:

$$(\mathbf{\Delta V}_{Tj} \times \mathbf{E}_{1j} \,\&\, \mathbf{\Delta V}_{Tj} \times \mathbf{E}_{2j}) < 0. \qquad (1)$$

Orts $\mathbf{E}_{1j}, \mathbf{E}_{2j}$ are found by turning ort $\mathbf{E_{0j}}$ clockwise and counter-clockwise by an angle $\Theta_j = \arcsin(\frac{D_{sa}}{OE_j})$, equal to half SDCj:

$$\mathbf{E}_{1j} = \mathbf{E}_{0j} \times e^{-i\Theta j}, \mathbf{E}_{2j} = \mathbf{E}_{0j} \times e^{i\Theta j}.$$

Single vector $\mathbf{E}_{0j}$ and distance OEj to p. E_j, used in the above equations, are determined by the formulas:

$$\Delta X_{mj}(E) = \Delta X_{mj}(N) + \Delta V_{xj} \Delta T_m,$$

$$\Delta Y_{mj}(E) = \Delta Y_{mj}(N) + \Delta V_{yj} \Delta T_m,$$

$$OE_j = \sqrt{\Delta X_{mj}{}^2(E) + \Delta Y_{mj}{}^2(E)},$$

$$\mathbf{E}_{0j} = (\frac{\Delta X_{mj}(E)}{OE_j}, \frac{\Delta Y_{mj}(E)}{OE_j}).$$

If condition (1) is not met, trial vector $\mathbf{V}_T = (V_T \cos K_T, V_T \sin K_T)$ belongs to the areas of admissible controls. The area of permissible controls in case of collision avoidance with all targets can be obtained by combining the areas of permissible controls with each target separately.

$$\Omega = \Omega_1 \bigcap \Omega_2 \bigcap ... \bigcap \Omega_{Ntg}.$$

Any pair of collision avoidance parameters $(V_{n1}, K_{n1}) \in \Omega$ is valid for discrepancies with all targets simultaneously. Therefore, further selection of the parameters of the collision avoidance from Ω determined by additional conditions, for example, the conditions for optimizing the collision avoidance, the stability conditions (the invariance of the selected collision avoidance parameters), the Rules of the COLREG –72, etc. The deflection angle of the rudder δ and the deflection angle of the telegraph θ are determined as

$$\delta = k_\Psi(\Psi_m - K_{n1}) + k_\omega \omega_{mz} + k_\int \int (\Psi_m - K_{n1}) dt,$$

$$\theta = \frac{\pi}{2} \frac{V_{n1}}{V_{\max}}.$$

4 EXPERIMENTS

Algorithms for automatic collision avoidance with multiple targets, including maneuvering ones, were checked in a closed circuit with electronic simulators. As an example, the data on the collision avoidance with the five dangerous targets located around the vessel are given below.

Fig. 3 shows a screenshot of the vessel, targets and weather conditions from the visualization channels of the simulator.

Fig. 4 presents a screenshot from the instructor's workplace, which shows the position of the own ship $СС_1$ and the target ships $СЦ_1$-$СЦ_5$ at the time of the start of the collision avoidance. Trajectories of target ships have fractures, i.e. they are supposed to be maneuvered in the course of the task.

Figure 3 – Screenshot of the vessel, targets and weather conditions from the visualization channels of the simulator

DOI 10.15588/1607-3274-2019-4-20

Fig. 5 shows the position of the ships – the targets on the radar screen at the moment of the beginning of the collision avoidance. As you can see, 3 dangerous targets (their relative motion vectors are highlighted in red).

In Fig. 6 shows the areas of permissible controls in the process of collision avoidance at different points in time (at the beginning of the collision avoidance, in the process of collision avoidance and at the end of the collision avoidance). Each time point is represented by a vertical fragment with a common area of collision avoidance with all targets simultaneously, as well as two areas of collision avoidance with the first and second targets separately.

Fig. 7 shows a screenshot from the instructor's workplace at the end of the collision avoidance.

Fig. 8 shows the position of the targets on the radar at the end of the collision avoidance.

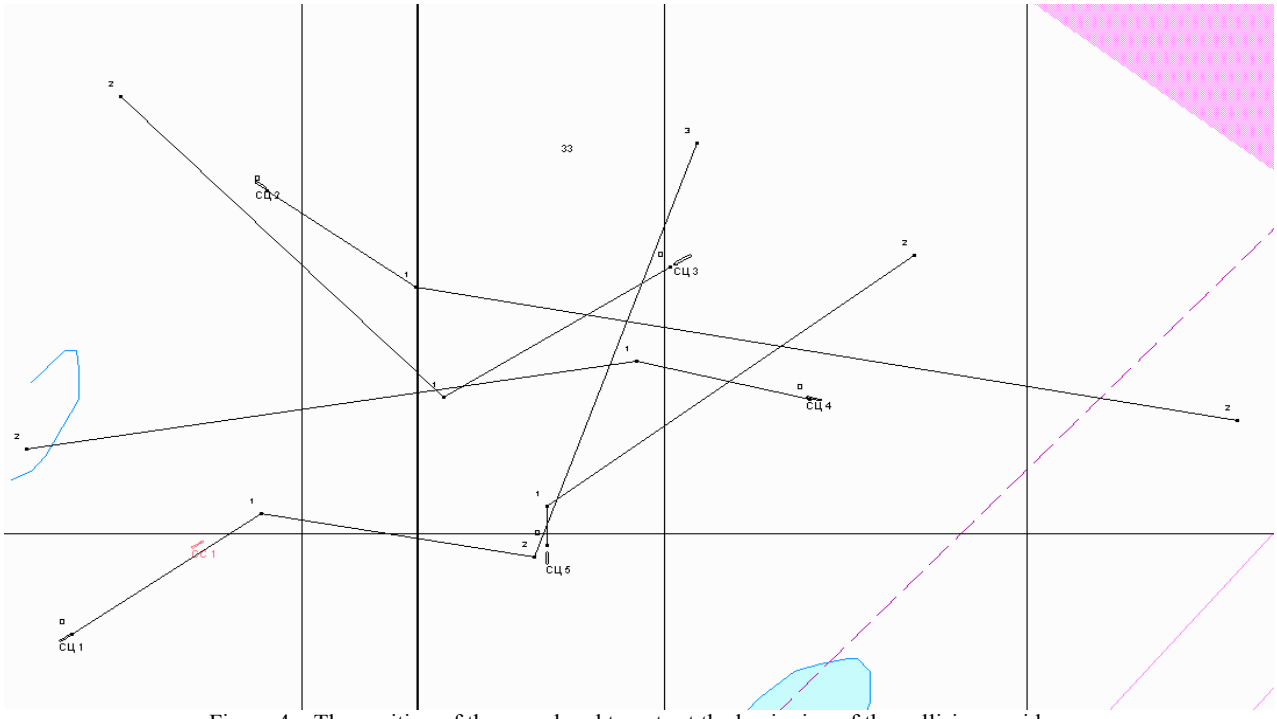


Figure 4 – The position of the vessel and targets at the beginning of the collision avoidance

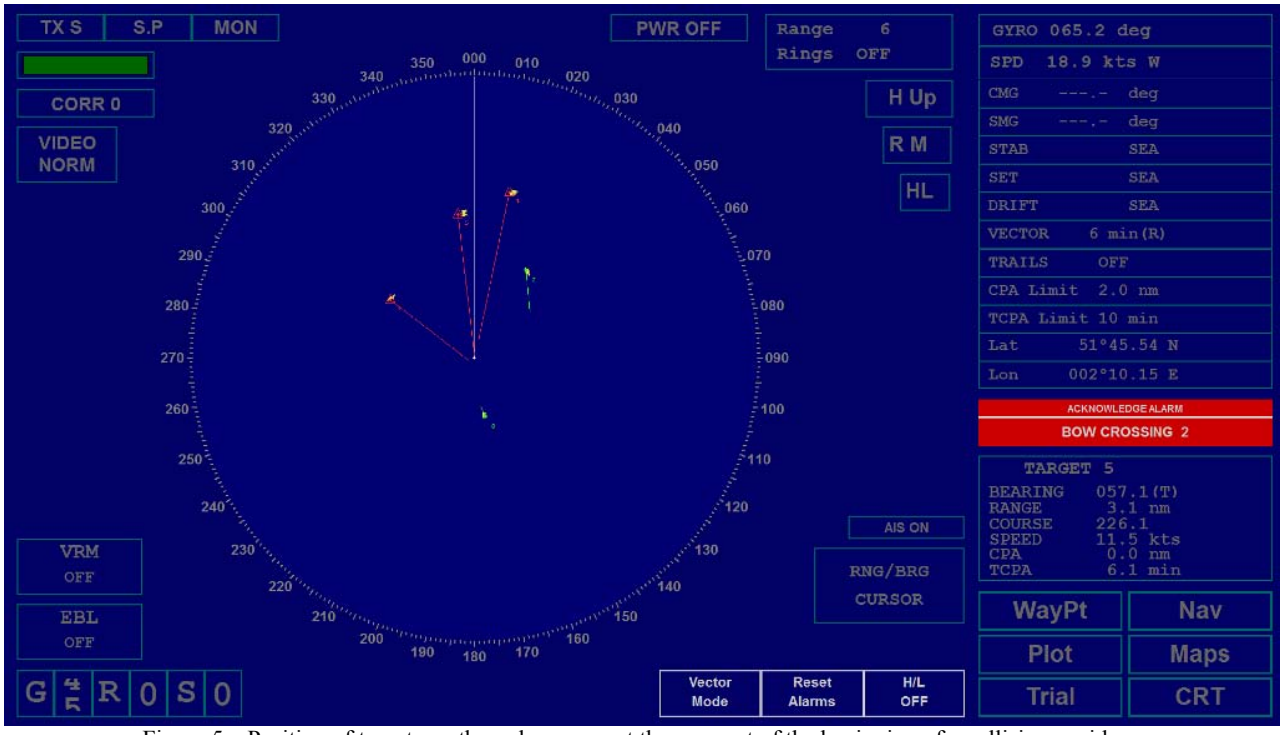


Figure 5 – Position of targets on the radar screen at the moment of the beginning of a collision avoidance

DOI 10.15588/1607-3274-2019-4-20

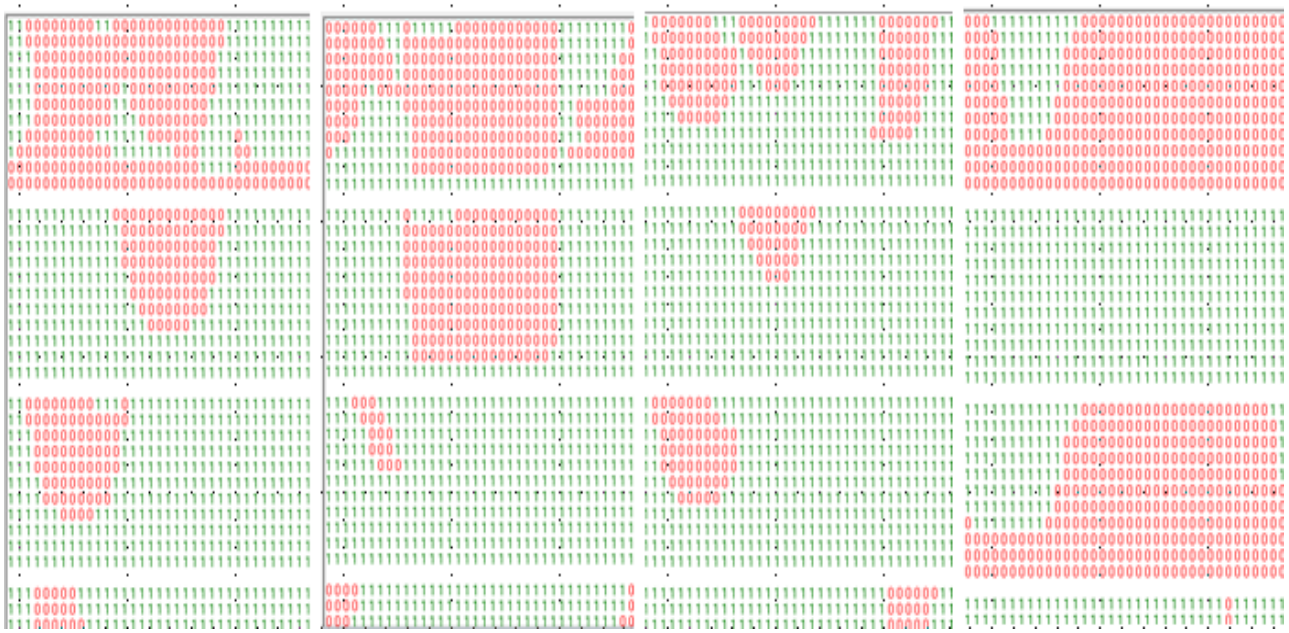


Figure 6 – Areas of permissible controls in the process of collision avoidance

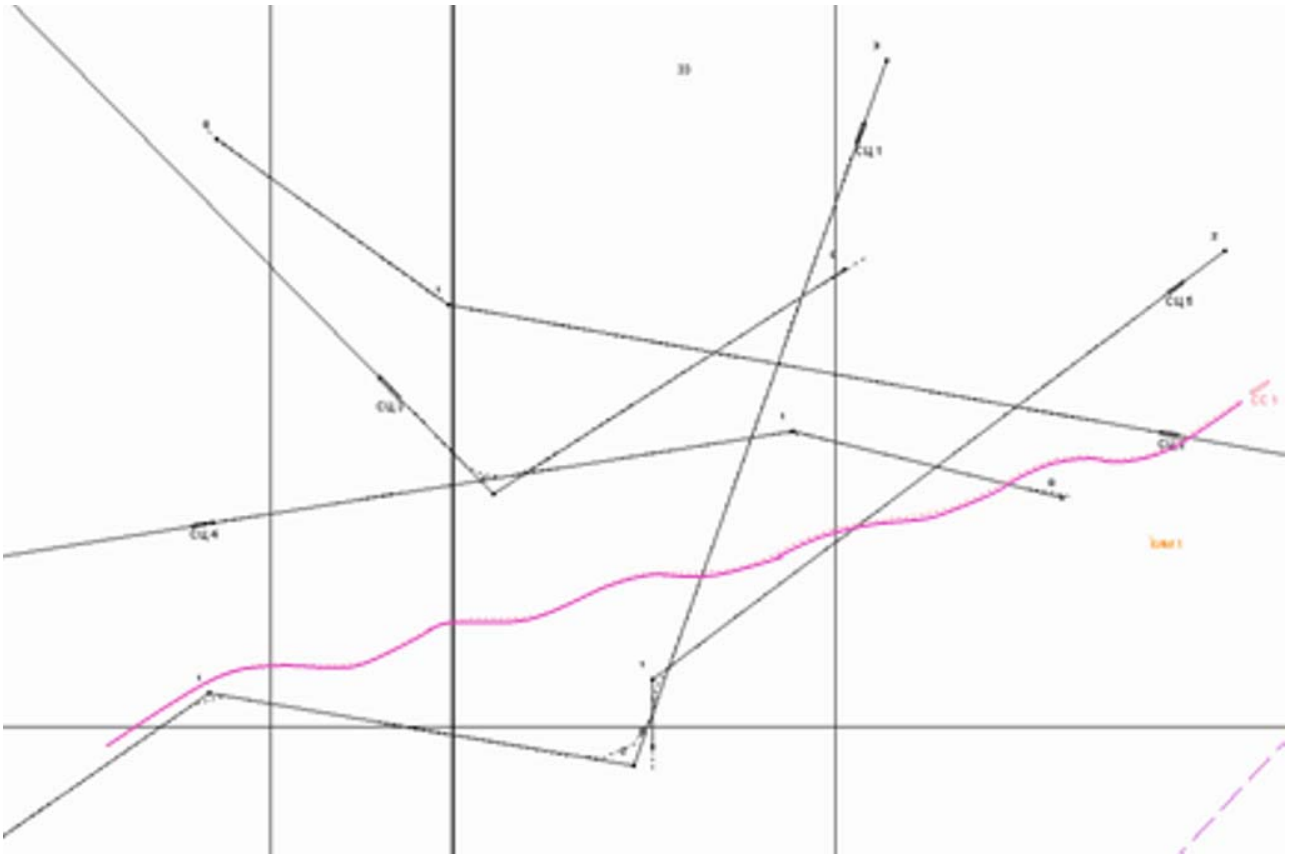


Figure 7 – Screenshot from the instructor's workplace at the end of the collision avoidance

DOI 10.15588/1607-3274-2019-4-20

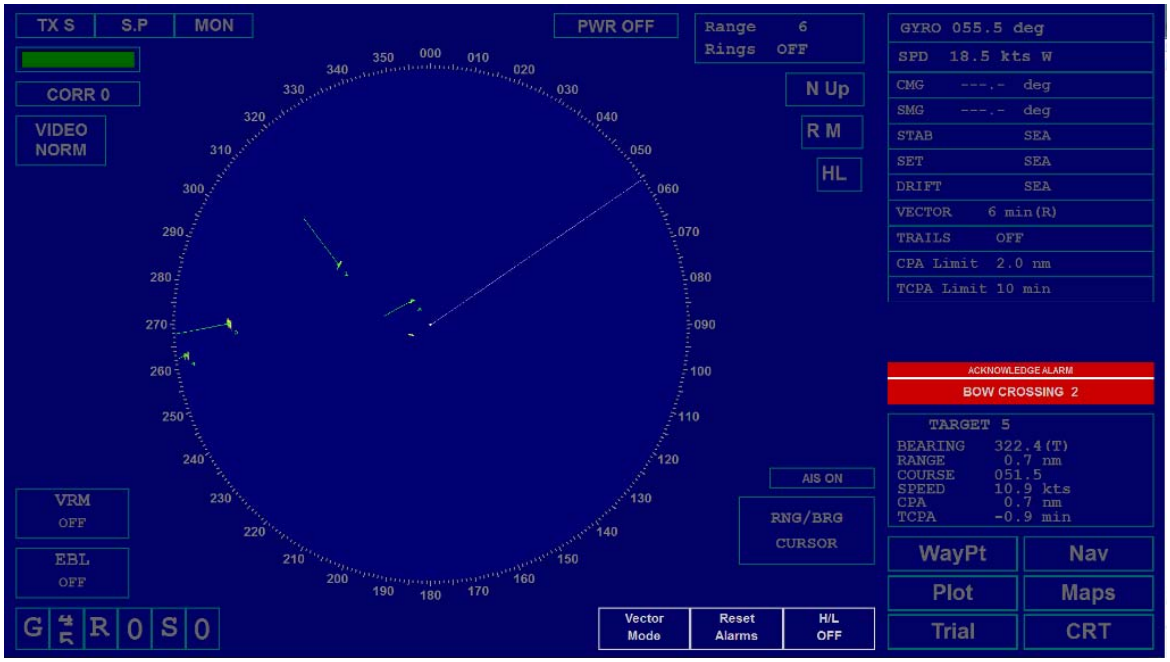


Figure 8 – Position of targets on the radar at the end of the collision avoidance

5 RESULTS

There were considered the issues of collision avoidance with many targets, including maneuvering ones, in a fully automatic mode.

There were analyzed existing methods of automatic collision avoidance of ships, their shortcomings were revealed and the relevance of the solution of this problem was substantiated.

There were developed a method and algorithms, which allow solving the problem of collision avoidance with multiple targets, including maneuvering ones, in onboard computer.

The efficiency of the method and algorithms was tested by mathematical modeling in a closed circuit with an electronic simulator Navi Trainer 5000 for various types of ships, targets, navigation areas and weather conditions.

6 DISCUSSION

The developed method and algorithms make it possible to diverge from multiple targets, including maneuvering ones, and can be used to create the software of the collision avoidance module of the onboard computer of the ship control system.

As shown by the simulation results in a closed circuit with the NTPRO 5000 simulator, the proposed method and algorithms, compared with the previously described solutions [5–14], allow to diverge from multiple targets, including maneuvering ones, in fully automatic mode.

CONCLUSIONS

There are proposed a method and algorithms for automatic collision avoidance with multiple targets, including maneuvering ones.

The scientific novelty of the results obtained is that for the first time a method and algorithms for automatic divergence with many targets, including maneuvering ones, were developed. This one is achieved by periodically measuring the true speed of the vessel and relative speeds of the vessel and targets, averaging the measured information to remove noise, estimating the true speeds of the targets, building, for the obtained estimates of the true speeds of the targets, areas of allowable collision avoidance controls with each targets by numerical iteration of the collision avoidance parameters (speed and course) at the nodes of a given grid in the area of their possible changes, determining the relative speeds at the nodes of the grid ship and target movement and checking that the relative speeds don't belong to sectors of dangerous courses, building a general area of acceptable collision avoidance controls with all targets by combining areas of allowable collision avoidance controls with each target, choosing collision avoidance parameters from the general area of acceptable collision avoidance controls according to specified criteria. This allows to diverge from multiple targets, including maneuvering ones, in a fully automatic mode. Changing the criteria for selecting discrepancy parameters leads to a change in the ship's behavior in case of discrepancy without changing the program code.

The practical value of the obtained results is that the developed method and algorithms are implemented in software and investigated by solving the problem of collision avoidance from multiple targets, including maneuvering ones, in a fully automatic mode in a closed circuit with the simulator Navi Trainer 5000 for various types of ships, targets, navigation areas and weather conditions.

The experiments confirmed the performance of the proposed method and algorithms and allow to recommend them for practical use in the development of modules for automatic collision avoidance with multiple targets, including maneuvering ones, of the onboard controller of the ship control system.

DOI 10.15588/1607-3274-2019-4-20

Prospects for further research may lie in the development of methods for selecting the optimal parameters of the collision avoidance from the area of admissible controls.

ACKNOWLEDGEMENTS

The work is carried out within the framework of "Creation of high-accuracy intellectual systems for military-oriented and commercial ship's navigation" (state registration number 0117U002176), of navigation and ECDIS departments of Kherson State Maritime Academy Navigation Faculty (scientific adviser: PhD, Associate Professor, Deputy Rector for scientific and pedagogical work, Head of the Navigation and Electronic Navigation Systems Department, Kherson State Maritime Academy, Ukraine, Ben A.P.).

REFERENCES

1. COLREGS – International Regulations for Preventing Collisions at Sea [Electronic resource], *Lloyd's Register Rulefinder,* 2005, Version 9.4, 2009. Access mode: http://www.jag.navy.mil/distrib/instructions/COLREG-1972.pdf
2. Radar navigation and ship collision avoidance [Electronic resource], *Nautical Almanac*, 2019. Access mode: https://nauticalalmanac.it/en/navigation-astronomy/radar-navigation-maneuvering-board.html
3. Bole A., Wall A., Norris A. Radar and ARPA manual : Radar, AIS and Target Tracking for Marine Radar Users. Third Editon [Electronic resource], *Elsevir*, 2013, 552 p. Access mode: https://www.amazon.com/Radar-ARPA-Manual-Target-Tracking-ebook/dp/B00GY5XEYO #reader_B00GY5XEYO
4. Pipchenko A. Radar Plotting or... Do we really understand what ARPA does? [Electronic resource], *Learnmarine,* 2018. Access mode: //https://learnmarine.com/blog/Radar-Plotting-or...-Do-we-really-understand-what-ARPA-does?
5. Shen H., Hashimoto H., Matsuda A. et al. Automatic collision avoidance of multiple ships based on deep Q-learning, *Applied Ocean Research Journal,* 2019, Vol. 86. pp. 268–288. DOI: 10.1016/j.apor.2019.02.020.
6. Yishan L., Zhiqiang G., Jie Y. et al. Prediction of ship collision risk based on CART, *IET Intelligent Transport Systems,* 2018, Vol. 12, Issue 10, pp. 1345–1350. DOI: 10.1049/iet-its.2018.5281
7. Park J., Choi J., Choi H. COLREGS-compliant path planning considering time-varying trajectory uncertainty of autonomous surface vehicle, *Electronics Letters*, 2019, Vol. 55, Issue 4, pp. 222–224. DOI: 10.1049/el.2018.6680.
8. Tu E., Zhang G., Rachmawati L. et al. Exploiting AIS date for intelligent maritime navigation: a comprehensive survey, *IEEE Transactions on itelligent transportation system,* 2016, Vol. 19, Issue 5, P. 99. DOI: 10.1109/TITS.2017.2724551.
9. Smeaton G., Coenen F. Developing an intelligent marine navigation system, *Computing & Control Engineering Journal*, 1990, Vol. 1, Issue 2, P. 95–103. DOI: 10.1049/cce:19900024.
10. Huang Y., Chen L., Gelder P. Generalized velocity obstacle algorithm for preventing ship collisions at sea, *Ocean Engineering Journal,* 2019, Vol. 173, pp. 142–156. DOI: 10.1016/j.oceaneng.2018.12.053.
11. Johansen T. A., Cristoforo A., Perez T. Ship Collision Avoidance Using Scenario-Based Model Predictive Control [Electronic resource], *IFAC*, 2016. Access mode: https://pdfs.semanticscholar.org/34a3/c1a0b699774fadab417ca2f5ef422edb1f0b.pdf
12. Blaich M., Kohler S., Reuter J. et al. Probabilistic Collision Avoidance for Vessels, *IFAC – PapersOnLine,* 2015, Vol. 48, Issue 16, pp. 69–74. DOI: 10.1016/j.ifacol.2015.10.260
13. Abdelaal M., Franzle M., Hahn A. Nonlinear Model Predictive Control for trajectory tracking and collision avoidance of underactuated vessels with disturbances, *Ocean Engineering,* 2018, Vol. 160, pp. 168–180. DOI: 10.1016/j.oceaneng.2018.04.026
14. Zhao Yu., Li W., Shi P. A real-time collision avoidance learning system for Unmanned Surface Vessels, *Neurocomputing*, 2016, Vol. 182, pp. 255–266. DOI: 10.1016/j.neucom.2015.12.028

Received 06.02.2019.
Accepted 12.10.2019.

УДК 004.942:656.61.052

АВТОМАТИЧНЕ РОЗХОДЖЕННЯ З БАГАТЬМА ЦІЛЯМИ, ВКЛЮЧАЮЧИ МАНЕВРУЮЧІ

Зінченко С. М. – канд. техн. наук, ст. викладач кафедри управління судном, завідувач лабораторії електронних тренажерів, Херсонська державна морська академія, Україна.

Носов П. С. – канд. техн. наук, доцент кафедри навігаційних систем, Херсонська державна морська академія, Україна.

Матейчук В. М. – асистент кафедри управління судном, завідувач лабораторії електронних тренажерів, Херсонська державна морська академія, Україна.

Маменко П. П. – ст. викладач кафедри управління судном, капітан далекого плавання, Херсонська державна морська академія, Україна.

Грошева О. О. – ст. викладач кафедри управління судном, Херсонська державна морська академія, Україна.

АНОТАЦІЯ

Актуальність. Розглядається задача автоматичного розходження з багатьма цілями, включаючи маневруючі. Об'єктом дослідження є процес автоматичного розходження з багатьма цілями, включаючи маневруючі. Предметом дослідження є метод і алгоритми, що реалізують процес автоматичного розходження з багатьма цілями, включаючи маневруючі.

Мета. Метою статті є розробка методу і алгоритмів автоматичного розходження з багатьма цілями, включаючи маневруючі, для модуля бортового контролера системи управління судном.

Метод. Ця мета досягається періодичним, з тактом роботи бортового контролера, вимірюванням істинної швидкості судна і відносних швидкостей судна і цілей, усередненням виміряної інформації для видалення шумів, оцінкою істинних швидкостей цілей, побудовою, для отриманих оцінок істинних швидкостей цілей, областей допустимих управлінь розходженням з кожною ціллю шляхом чисельного перебору параметрів розходження (швидкості і курсу) на вузлах заданої сітки в області їх можливих змін, визначенням на вузлах сітки відносних швидкостей руху судна і цілей і перевіркою їх на не приналежність секторам небезпечних курсів, побудовою загальної області допустимих управлінь розходженням з усіма цілями шляхом об'єднання областей допустимих управлінь розходженням з кожною ціллю, вибором параметрів розходження із загальної області допустимих управлінь розходженням у відповідності із заданими критеріями. Це дозволяє розходитися з багатьма цілями, включаючи маневруючі, у повністю автоматичному режимі. Зміна критеріїв вибору параметрів розходження призводить до зміни поведінки судна при розходженні без зміни програмного коду.

Результати. Розроблені метод та алгоритми реалізовані в програмному забезпеченні і досліджені шляхом вирішення задачі розходження з багатьма цілями, включаючи маневруючі, у повністю автоматичному режимі у замкнутій схемі з тренажером Navi Trainer 5000 для різних типів суден, цілей, районів плавання і погодних умов.

DOI 10.15588/1607-3274-2019-4-20

Висновки. Експерименти підтвердили працездатність запропонованого способу і алгоритмів і дозволяють рекомендувати їх для практичного використання при розробці модулів автоматичного розходження з багатьма цілями, включаючи маневруючі, бортового контролера системи управління судном.

КЛЮЧОВІ СЛОВА: система розходження суден, автоматичне розходження, розходження з маневруючими цілями, попередження зіткнень, область допустимих управлінь.

УДК 004.942:656.61.052

АВТОМАТИЧЕСКОЕ РАСХОЖДЕНИЕ СО МНОГИМИ ЦЕЛЯМИ, ВКЛЮЧАЯ МАНЕВРИРУЮЩИЕ

Зинченко С. Н. – канд. техн. наук, ст. преподаватель кафедры управления судном, заведующий лабораторией электронных тренажеров, Херсонская государственная морская академия, Украина.

Носов П. С. – канд. техн. наук, доцент кафедры навигационных систем, Херсонская государственная морская академия, Украина.

Матейчук В. Н. – ассистент кафедры управления судном, заведующий лабораторией электронных тренажеров, Херсонская государственная морская академия, Украина.

Маменко П. П. – ст. преподаватель кафедры управления судном, капитан дальнего плавания, Херсонская государственная морская академия, Украина.

Грошева О. А. – ст. преподаватель кафедры управления судном, Херсонская государственная морская академия, Украина.

АННОТАЦИЯ

Актуальность. Рассматривается задача автоматического расхождения со многими целями, включая маневрирующие. Объектом исследования является процесс автоматического расхождения со многими целями, включая маневрирующие. Предметом исследования являются метод и алгоритмы, реализующие процесс автоматического расхождения со многими целями, включая маневрирующие.

Цель. Целью статьи является разработка метода и алгоритмов автоматического расхождения со многими целями, включая маневрирующие, для модуля бортового контроллера системы управления судном.

Метод. Эта цель достигается периодическим, с тактом работы бортового контроллера, измерением истинной скорости судна и относительных скоростей судна и целей, усреднением измеренной информации для удаления шумов, оценкой истинных скоростей целей, построением, для полученных оценок истинных скоростей целей, областей допустимых управлений расхождением с каждой целью путем численного перебора параметров расхождения (скорости и курса) на узлах заданной сетки в области их возможных изменений, определением на узлах сетки относительных скоростей движения судна и целей и проверкой их на не принадлежность секторам опасных курсов, построением общей области допустимых управлений расхождением со всеми целями путем объединения областей допустимых управлений расхождением с каждой целью, выбором параметров расхождения из общей области допустимых управлений расхождением в соответствие с заданными критериями. Это позволяет разойтись со многими целями, включая маневрирующие, в полностью автоматическом режиме. Изменение критериев выбора параметров расхождения приводит к изменению поведения судна при расхождении без изменения программного кода.

Результаты. Разработанные метод и алгоритмы реализованы в программном обеспечении и исследованы путем решения задачи расхождения со многими целями, включая маневрирующие, в полностью автоматическом режиме в замкнутой схеме с тренажером Navi Trainer 5000 для различных типов судов, целей, районов плавания и погодных условий.

Выводы. Эксперименты подтвердили работоспособность предлагаемого способа и алгоритмов и позволяют рекомендовать их для практического использования при разработке модулей автоматического расхождения со многими целями, включая маневрирующие, бортового контроллера системы управления судном.

КЛЮЧЕВЫЕ СЛОВА: система расхождения судов**,** автоматическое расхождение**,** расхождение с маневрирующими целями, предупреждение столкновений, область допустимых управлений.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. COLREGS – International Regulations for Preventing Collisions at Sea [Electronic resource] // Lloyd's Register Rulefinder 2005 – Version 9.4. – 2009. – Access mode: http://www.jag.navy.mil/distrib/instructions/COLREG–1972.pdf
2. Radar navigation and ship collision avoidance [Electronic resource] // Nautical Almanac. – 2019. – Access mode: https://nauticalalmanac.it/en/navigation-astronomy/radar-navigation-maneuvering-board.html
3. Radar and ARPA manual : Radar, AIS and Target Tracking for Marine Radar Users. Third Editon [Electronic resource] / A. Bole, A. Wall, A. Norris. – Elsevir, 2013. – 552 p. – Access mode: https://www.amazon.com/Radar-ARPA-Manual-Target-Tracking-ebook/dp/B00GY5XEYO #reader_B00GY5XEYO
4. Pipchenko A. Radar Plotting or... Do we really understand what ARPA does? [Electronic resource] / A. Pipchenko // Learnmarine. – 2018. – Access mode: //https://learnmarine.com/blog/Radar-Plotting-or...-Do-we-really-understand-what-ARPA-does?
5. Automatic collision avoidance of multiple ships based on deep Q-learning / [H. Shen, H. Hashimoto, A. Matsuda et al.] // Applied Ocean Research Journal. – 2019. – Vol. 86. – P. 268–288. DOI: 10.1016/j.apor.2019.02.020.
6. Prediction of ship collision risk based on CART / [L. Yishan, G. Zhiqiang, Y. Jie et al.] // IET Intelligent Transport Systems. – 2018. – Vol. 12. – Issue 10. – P. 1345–1350. DOI: 10.1049/iet-its.2018.5281
7. Park J. COLREGS-compliant path planning considering time-varying trajectory uncertainty of autonomous surface vehicle / J. Park, J.Choi, H. Choi // Electronics Letters. – 2019. – Vol. 55, Issue 4. – P. 222–224. DOI: 10.1049/el.2018.6680.
8. Exploiting AIS date for intelligent maritime navigation: a comprehensive survey / [E. Tu, G. Zhang, L. Rachmawati et al.] // IEEE Transactions on itelligent transportation system. – 2016. – Vol. 19, Issue 5. – P. 99. DOI: 10.1109/TITS.2017.2724551.
9. Smeaton G. Developing an intelligent marine navigation system / G. Smeaton, F. Coenen // Computing & Control Engineering Journal. – 1990. – Vol. 1, Issue 2. – P. 95–103. DOI: 10.1049/cce:19900024.
10. Huang Y. Generalized velocity obstacle algorithm for preventing ship collisions at sea / Y. Huang, L. Chen, P. Gelder // Ocean Engineering Journal. – 2019. – Vol. 173. – P. 142–156. DOI: 10.1016/j.oceaneng.2018.12.053.
11. Johansen T. A. Ship Collision Avoidance Using Scenario-Based Model Predictive Control [Electronic resource] / T. A. Johansen, A. Cristoforo, T. Perez // IFAC. – 2016. – Access mode: https://pdfs.semanticscholar.org/34a3/c1a0b699774fadab417ca2f5ef422edb1f0b.pdf
12. Probabilistic Collision Avoidance for Vessels / [M. Blaich, S. Kohler, J. Reuter et al.] // IFAC –PapersOnLine. – 2015. – Vol. 48, Issue 16. – P. 69–74. DOI: 10.1016/j.ifacol.2015.10.260
13. Abdelaal M. Nonlinear Model Predictive Control for trajectory tracking and collision avoidance of underactuated vessels with disturbances / M. Abdellal, M. Franzle, A. Hahn // Ocean Engineering. – 2018. – Vol. 160. – P. 168–180. DOI: 10.1016/j.oceaneng.2018.04.026
14. Zhao Yu. A real-time collision avoidance learning system for Unmanned Surface Vessels / Yu. Zhao, W. Li, P. Shi // Neurocomputing. – 2016. – Vol. 182. – P. 255–266. DOI: 10.1016/j.neucom.2015.12.028

DOI 10.15588/1607-3274-2019-4-20

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

УДК 621.391:004.052

АНАЛИЗ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ МЕЖДУ УСТРОЙСТВАМИ СИСТЕМ УПРАВЛЕНИЯ ПРИ ПАКЕТИРОВАНИИ ОШИБОК

Фрейман В. И. – д-р техн. наук, профессор кафедры «Автоматика и телемеханика», Пермский национальный исследовательский политехнический университет, г. Пермь, Россия.

АННОТАЦИЯ

Актуальность. Проведен анализ показателей достоверности передачи информации между элементами систем управления с учетом пакетирования (группирования) ошибок в канале связи. Объектом исследования являются характеристики и параметры помехоустойчивых циклических двоичных и недвоичных кодов, ориентированных на исправление пакетов ошибок. Предмет исследования – теоретический и экспериментальный сравнительный анализ показателей достоверности кодов, исправляющих пакеты ошибок.

Цель работы – определение аналитических зависимостей показателей достоверности выбранных избыточных кодов от их параметров и свойств канала связи, разработка моделей для их экспериментального исследования, формирование рекомендаций по выбору кодов с заданными характеристиками при определенных свойствах и модели описания ошибок.

Методы. Использован математический аппарат и теория построения помехоустойчивых циклических двоичных (БЧХ) и недвоичных (Рида-Соломона) кодов. Получены аналитические соотношения для определения показателей достоверности передачи с учетом возможных искажений символов кода внутри пакета ошибок. Исследованы зависимости корректирующих свойств и вероятности правильной передачи от параметров кода и ошибки, приведены иллюстрирующие примеры. Разработаны имитационные схемотехнические модели системы управления с исследуемыми способами помехоустойчивого кодирования. Проведены экспериментальные исследования, на основании полученных данных сделаны выводы и предложены рекомендации по выбору параметров кодов для заданных показателей достоверности для обеспечения максимальной эффективности (информационной скорости передачи).

Результаты. Получены зависимости показателей достоверности (вероятность правильной передачи) и корректирующих свойств (длина исправляемого пакета ошибок) исследуемых избыточных кодов от их параметров (количества избыточных символов, степени перемежения – для БЧХ-кодов; модуль поля Галуа, кратность исправляемых ошибок – для кодов Рида-Соломона). Даны рекомендации по использованию полученных результатов при выборе параметров кода. Для проведения экспериментальных исследований созданы и настроены модели системы управления в среде MathWorks MatLab Simulink.

Выводы. Проведенные в работе исследования позволяют рассчитать и обоснованно выбрать параметры избыточных кодов для заданных показателей достоверности с учетом модели поведения ошибок в канале передачи. Это дает возможность проектировать и реализовать надежные системы управления с заданными показателями достоверности и максимальной информационной скоростью передачи.

КЛЮЧЕВЫЕ СЛОВА: информационно-управляющие системы, достоверность, помехоустойчивость, избыточность, циклические коды, пакет ошибок, модель.

АББРЕВИАТУРЫ

GF – Galua Field;

IoT – Internet of things;

IPTV – Internet Protocol Television;

PLC – Programmable Logical Controller;

VoIP – Voice over Internet;

Wi-Fi – Wireless Fidelity;

АСУП – Автоматизированная система управления предприятием;

АСУТП – Автоматизированная система управления технологическими процессами;

БЧХ – Боуз, Чоудхури, Хоквингем;

Р-С – Рида-Соломона;

РИУС – распределенные информационно-управляющие системы;

ПЛИС – программируемые логические интегральные схемы.

НОМЕНКЛАТУРА

α – переменная для описания структуры символа;

Δ – приращение;

b – длина пакета исправляемых ошибок;

b^* – количество ошибочных бит в пакете ошибок;

$b_{\max\_p}$ – максимальная потенциальная длина исправляемого пакета ошибок;

$b_{\max\_g}$ – максимальная гарантированная (max_g) длина исправляемого пакета ошибок;

d – минимальное кодовое расстояние Хэмминга;

e – полином ошибки;

f – неприводимый и примитивный полином;

g – порождающий полином кода;

h – параметр БЧХ-кода;

k – длина избыточной части сообщения;

k^* – длина избыточной части исходного БЧХ-кода;

l – количество бит в символе;

m – длина информационной части сообщения;

n – общая длина сообщения;

N_1 – число полных пакетов ошибок;

N_0 – число неполных пакетов ошибок;

p – вероятность ошибочного приема бита;

$P_{\text{пр.}}$ – вероятность правильной передачи сообщения;

$\widetilde{P}_{\text{пр.}}$ – заданная вероятность правильной передачи;

$P_{\text{с}}$ – вероятность ошибочного символа кода;

$P_{\text{тр.}}$ – вероятность трансформации сообщения;

R – информационная скорость передачи;

s – кратность исправляемых ошибок;

t – степень укорочения кода;

u – информационный полином кода;

DOI 10.15588/1607-3274-2019-4-21

V – передаваемый полином кода;

V' – принимаемый полином кода;

x – формальная переменная для описания кода;

XOR – логическая операция «Исключающее ИЛИ».

ВВЕДЕНИЕ

Системы передачи и хранения информации являются важной частью структур систем управления различными объектами и процессами (АСУТП, АСУП, РИУС), а также могут выступать как самостоятельная функциональная система (телекоммуникации – Wi-Fi, Bluetooth, IoT, IPTV, VoIP и т.д.). Одной из их основных эксплуатационно-технических характеристик является достоверность передачи. Она определяется физическими характеристиками источников помех, адекватностью математического описания их поведения, а также корректностью выбранных способов помехоустойчивого кодирования [1].

Из-за распространения коммуникационных технологий (спутниковая связь, беспроводные технологии, кабельные системы и т.п.) устройствам систем управления приходится работать в условиях действия совокупности помех, которые характеризуются малыми соотношениями «сигнал/шум», высокой вероятностью битовых ошибок и т.д. Существенно снижает достоверность пакетирование ошибок, при котором поражаются целые группы символов (от единиц до нескольких сотен) [2]. Поэтому нужны эффективные способы коррекции таких ошибок, при этом необходимо учитывать внесение значительной избыточности и соответствующее снижение пропускной способности и быстродействия. Следовательно, нужно уметь оценить характеристики кодов и выбрать их параметры, гарантирующие требуемую достоверность при максимальной информационной эффективности (минимальной избыточности), задержке, вычислительной сложности реализации алгоритмов кодирования/декодирования и т.д.

Объектом исследования выбраны помехоустойчивые циклические двоичные (БЧХ) и недвоичные (Р-С) избыточные коды, их свойства и параметры.

Предметом исследования является теоретический и экспериментальный сравнительный анализ показателей достоверности выбранных избыточных кодов при пакетировании ошибок при передаче данных по каналам систем управления.

Цель работы – сравнительный анализ характеристик избыточных кодов, корректирующих пакеты ошибок. На основании анализа предлагаются рекомендации по применению кодов с заданными характеристиками при определенных свойствах и модели описания ошибок при передаче.

1 ПОСТАНОВКА ЗАДАЧИ

Корректирующие коды описываются взаимопротиворечащими друг другу характеристиками: достоверностью и эффективностью. За каждый дополнительный бит, улучшающий корректирующие свойства кода и повышающий показатели достоверности, приходится «расплачиваться» снижением быстродействия, увеличением ресурсов, усложнением алгоритмов обработки. Поэтому важно подобрать такие параметры кодов, которые обеспечивают выполнение требований по достоверности при максимальной эффективности [3]. При этом существенным фактором становится адекватная оценка модели поведения помех, которые могут быть описаны как «независимые» или как «пакетирующиеся» («группирующиеся»), что выявляется при тестировании канала передачи [4].

Для коррекции пакетов ошибок разработаны и эффективно применяются двоичные циклические коды, построенные по принципу перемежения, или специальные коды (Файра, Бартона и др.) [5]. Но способы построения, эффективность (избыточность) и алгоритмы декодирования циклических кодов, исправляющих независимые и пакетирующиеся ошибки, существенно отличаются. Поэтому были разработаны и предложены для широкого применения недвоичные циклические коды Рида-Соломона [6]. Особенностью их применения является то, что способы построения и алгоритмы декодирования инварианты к модели ошибок.

Для решения проблемы выбора кода с заданными показателями достоверности при максимальной эффективности выполним математическую постановку задачи.

Пусть имеется совокупность параметров избыточных двоичных и недвоичных кодов, характеризующих их свойства. Общие параметры: длина – m, k, n, t; корректирующие свойства – s, b, а также характеристика канала связи p. Дополнительные параметры: для БЧХ-кодов – i, для кодов Р-С – l. Они задают два основных критерия оценки кодов – достоверность, оцениваемая через $P_{\text{пр.}}$, и эффективность (информационная скорость), оцениваемая через R. Каждый из указанных критериев представляет собой функциональную зависимость от параметров кода и среды передачи:

$$P_{\text{пр.}} = f(n,b,p); R = f(m,n) = f(k,n); P_{\text{пр.}} \sim \frac{1}{R}. \quad (1)$$

Для решения задач синтеза системы управления с заданными показателями достоверности необходимо исследовать зависимости введенных критериев от параметров кода при максимально возможной эффективности (информационной скорости передачи):

$$P_{\text{пр.}} > \widetilde{P}_{\text{пр.}}; R \to \max. \quad (2)$$

Достоверность характеризуется вероятностью правильной передачи сообщения при наличии информации о свойствах (вероятность появления) и характеристиках (степень группирования) ошибок. Эффективность задается коэффициентом полезного использования пропускной способности канала, при этом актуальной задачей является ее максимизация (минимизация символьной избыточности) при соблюдении заданной достоверности. Поэтому далее решаются вопросы по определению и исследованию зависимо-

DOI 10.15588/1607-3274-2019-4-21

стей показателей достоверности и эффективности от параметров кода и свойств среды передачи. Это дает возможность выбрать и реализовать в элементах систем управления способы обеспечения заданной достоверности при максимальной информационной скорости передачи.

2 ОБЗОР ЛИТЕРАТУРЫ

Первоначально для исправления пакетов ошибок использовались двоичные циклические коды (БЧХ-коды) [7]. Они строились двумя способами [1]:

1) перемежением со степенью перемежения i;

2) применением специальных кодов (Файра, Бартона и т.д.).

К их достоинствам можно отнести хорошую проработанность алгоритмов кодирования и декодирования, а также относительную простоту их аппаратурной и программной реализации. Недостатком является отличие алгоритмов декодирования и структур декодеров для разного характера поведения ошибок в канале (независимые или пакетирующиеся), что требует дополнительного анализа и регулярного тестирования канала передачи [8].

Открытие недвоичных циклических кодов (Ирвин Рид и Густав Соломон – Р-С [9]), появление эффективных алгоритмов декодирования и аппаратно-программной реализации способствовало их эффективному применению в информационных системах. К определенным недостаткам указанных способов кодирования можно отнести сложность их математического описания и алгоритмов декодирования. Это компенсируется их высокой эффективностью (достоверностью), а также инвариантностью к характеру поведения помех в канале (способы декодирования независимых и пакетирующихся ошибок одинаковые). Необходимо отметить, что широкое распространение систем передачи информации (промышленные информационно-управляющие системы, системы управления предприятиями, телекоммуникации, системы хранения и обработки данных и т.д.) происходит с учетом существенного снижения достоверности передачи на уровне символов [10]. Это требует более эффективного применения способов и алгоритмов декодирования при сохранении сравнительно низкой избыточности при использовании ресурсов системы.

Теория построения, кодирования и декодирования кодов, исправляющих пакеты ошибок, достаточно подробно представлена в научных публикациях зарубежных и отечественных исследователей [2, 5, 8, 11, 12]. Однако для их анализ показал необходимость исследования получения и исследования зависимостей показателей достоверности и эффективности кодирования с учетом способов их построения. Поэтому далее будут представлены результаты анализа характеристик достоверности и эффективности кодов при пакетировании ошибок. Также построены модели систем передачи и даны практические рекомендации по выбору соответствующих параметров для реализации процедур кодирования и декодирования в современном аппаратно-программном базисе.

3 МАТЕРИАЛЫ И МЕТОДЫ

Перед изложением способов и алгоритмов кодирования и декодирования определим термин «пакет ошибок» [4]. Будем считать, что пакет имеет длину b бит, начинается и заканчивается ошибочным битом, а внутри может содержать и ошибочные, и правильно принятые биты. Таким образом, количество искаженных бит в пакете находится в интервале [2; b], если считать, что искаженных бит в пакете может быть не меньше 2. В работе [1] проиллюстрированы способы определения длины пакета в зависимости от выбранной модели ошибок (Гильберта, Гильберта-Элиота, Пуртова и т.д.).

Рассмотрим краткую теорию построения и применения двоичных циклических кодов для исправления пакетов ошибок. Из границы Рейгера можно определить зависимость длины исправляемого пакета ошибок от количества избыточных символов, представленных через его параметры:

$$b \le \frac{k}{2} = \frac{i \cdot k^*}{2} = \frac{i \cdot s \cdot h}{2}. \qquad (3)$$

Для построения кода используется порождающий полином $g(x^i)$. Структурные схемы и алгоритмы кодирования и декодирования подробно рассмотрены в работе [1].

Исследуем зависимости характеристики b от параметров кода i и k^* и представим их на рис. 1 и 2.

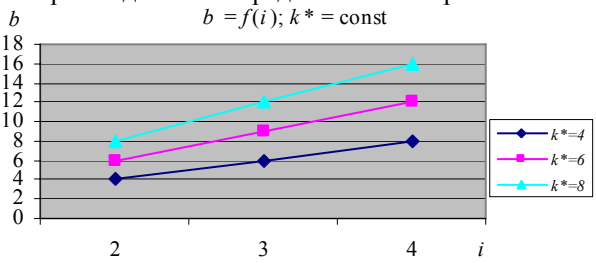


Рисунок 1 – Зависимость длины исправляемого пакета ошибок от степени перемежения

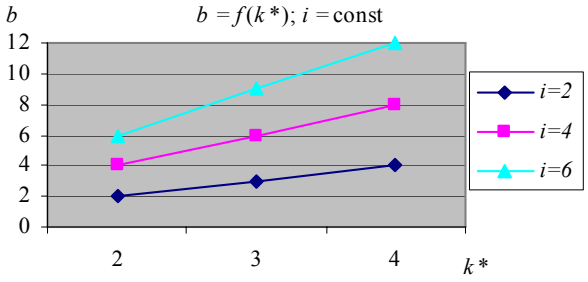


Рисунок 2 – Зависимость длины исправляемого пакета ошибок от числа избыточных символов кода

Выводы по рис. 1 и 2: с увеличением значений параметров кода длина исправляемого пакета ошибок растет линейно. Скорость изменения характеристики b по каждому из параметров определяется соответствующей частной производной, не зависит от данного

DOI 10.15588/1607-3274-2019-4-21

параметра и определяется значениями остальных параметров:

$$\frac{\partial b}{\partial i}=\frac{k^*}{2};\frac{\partial b}{\partial k^*}=\frac{i}{2}. \quad (4)$$

Для оценки вероятности правильной передачи, характеризующей достоверность, сначала нужно определить варианты пакетов ошибок заданной длины $b^* \in [1; b]$. Будем считать пакет ошибок длины b^* комбинацией двоичных символов, крайние значения которой равны 1, а между ними могут быть разные сочетания. Тогда число таких сочетаний равно:

$$\sum_{j=0}^{b^*-2}\binom{b^*-2}{j}. \quad (5)$$

Количество исправляемых пакетов ошибок кратности $b^* \in [1; b]$ определяется так:

$$\sum_{i=1}^{b}\sum_{j=0}^{i-2}\binom{i-2}{j}. \quad (6)$$

Для кода длины n таких пакетов будет:

$$n-b^*+1. \quad (7)$$

Чтобы не делать дополнение для крайних $(b-1)$ символов, используем следующую декомпозицию: отдельно будем рассчитывать N_1 (пакеты, в которых искажаются все символы фрагмента сообщения) и N_0 (пакеты, в которых искажаются не все символы фрагмента сообщения):

$$N_1=\sum_{i=1}^{b}(n-i+1);N_0=\sum_{i=3}^{b}(n-i+1)\sum_{j=0}^{i-3}\binom{i-2}{j}. \quad (8)$$

С учетом биноминального распределения ошибок запишем выражение для вероятности правильной передачи:

$$P_{\text{пр.}}=(1-p)^n+\sum_{i=1}^{b}(n-i+1)p^i(1-p)^{n-i}+ \\ +\sum_{i=3}^{b}(n-i+1)\sum_{j=0}^{i-3}\binom{i-2}{j}p^i(1-p)^{n-i}. \quad (9)$$

Оценим и построим зависимости показателя вероятности правильной передачи от параметров кода и характеристик помехи в канале связи (рис. 3, 4).

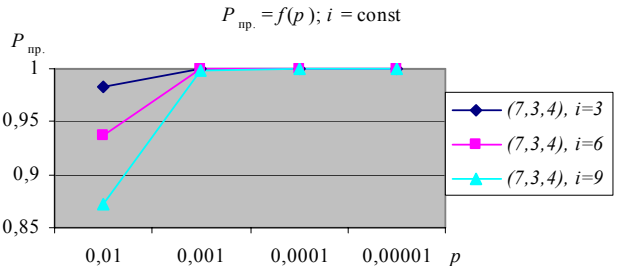


Рисунок 3 – Зависимость показателей достоверности от свойств помехи в канале

Вывод по рис. 3: при низких значениях p, что соответствует сильно «зашумленным» каналам (РИУС, Wi-Fi и т.п.) высокая достоверность достигается при низкой эффективности кода (за счет существенной избыточности). В «хороших» каналах связи заданной достоверности можно добиться при высокой эффективности (низкой избыточности).

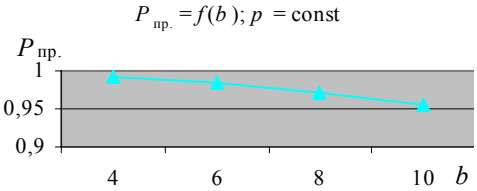


Рисунок 4 – Зависимость показателей достоверности от характеристик поведения ошибки в канале

Вывод по рис. 4: с увеличением длины исправляемого пакета ошибок достоверность снижается за увеличения избыточности. Причем динамика изменения скорости уменьшения достоверности нелинейная – скорость увеличивается.

Рассмотрим краткую теорию построения кодов Р-С [6]. Коды Р-С представляют собой недвоичные циклические коды, построенные над полем Галуа GF(2^l), символы которых строятся путем объединения нескольких (l) бит, описываются полиномом по формальной переменной α и по модулю неприводимого и примитивного полинома $f(\alpha)$ степени l. Полином кода длины n строится из недвоичных символов как коэффициентов по формальной переменной x.

Коды Р-С относятся к блочным кодам и описываются (n,m,d)-формой представления. Их характеристики вычисляются по следующим расчетным соотношениям:

$$d=2s+1;k=2s;n=2^l-1;m=n-k=2^l-1-2s. \quad (10)$$

В соответствии с правилами задания кода Р-С, он может быть укорочен на t символов за счет приравнивания к 0 соответствующего количества старших символов табличного значения информационной части или удлинен, но не более чем на 2 символа [9].

Для описания действий над полиномами кода строятся таблицы представления, сложения и умножения. Для процедур кодирования и декодирования строится порождающий полином $g(x)$.

Процедура кодирования для кодов Р-С как подкласса циклических кодов основывается на делении информационного полинома $u(x)$, домноженного на x^k, на порождающий полином $g(x)$ [6].

Процедура декодирования кодов Р-С содержит три основные этапа: вычисление синдрома, определение места ошибок при помощи полинома локатора ошибки и расчет значений ошибки [3]. После этого вычисленный полином ошибки $e(x)$ складывается с помощью операции XOR с принятым полином $V'(x)$, и ошибки исправляются.

Проанализируем корректирующие свойства кодов Р-С, направленные на исправление пакетов ошибок.

DOI 10.15588/1607-3274-2019-4-21

Очевидно, что коды Р-С, исправляющие однократную ошибку, не могут гарантировано исправлять пакеты ошибок заданной длины b (даже для $b = 2$ есть вероятность расположения пакета ошибок на два соседних символа кода Р-С, значит, нужно исправление как минимум двух символьных ошибок). Оценим максимальную потенциальную (max_p) и максимальную гарантированную (max_g) длины исправляемых пакетов ошибок (без доказательства, оно может быть сделано путем математической индукции – от заданных малых значений к обобщению, а также графически):

$$b_{\max\_p} = l \cdot s;\ b_{\max\_g} = b = l \cdot (s - 1) + 1. \qquad (11)$$

Проанализируем зависимости длины исправляемого пакета ошибок от параметров кода (рис. 5 и 6).

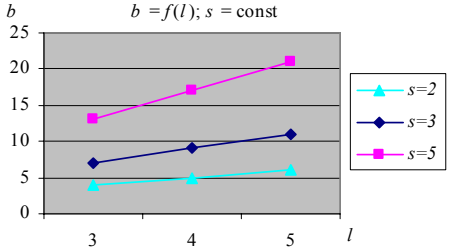


Рисунок 5 – Зависимость длины исправляемого пакета ошибок от параметра кода l

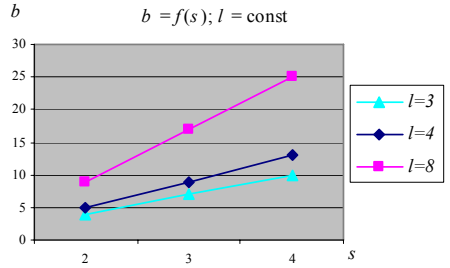


Рисунок 6 – Зависимость длины исправляемого пакета ошибок от параметра кода s

Выводы по рис. 5 и 6: длина исправляемого пакета ошибок линейно зависит от параметров кода и растет тем быстрее, чем лучше корректирующие свойства.

Скорость изменения параметра b по каждому из параметров определяется соответствующей частной производной, не зависит от данного параметра и определяется значением другого параметра:

$$\frac{\partial b}{\partial l} = s - 1; \frac{\partial b}{\partial s} = l. \qquad (12)$$

Для того чтобы оценить, как влияет изменение каждого из параметров на длину исправляемого пакета ошибок b, рассчитаем частные и полное приращения:

$$\begin{aligned} &\Delta_l b = \frac{\partial b}{\partial l}\Delta l = (s-1)\Delta l; \Delta_s b = \frac{\partial b}{\partial s}\Delta s = l\Delta s; \\ &\Delta b \neq \Delta_l b + \Delta_s b; \\ &\Delta b = b(l + \Delta l; s + \Delta s) - b(l; s) = \\ &= [(l + \Delta l)(s + \Delta s - 1) + 1] - \\ &- [l(s-1) + 1] = (s-1)\Delta l + (l + \Delta l)\Delta s. \end{aligned} \qquad (13)$$

Пример 1. Пусть дан код Р-С со следующими параметрами: $l = s = 3$. Зададим для каждого параметра единичное приращение: $\Delta l = \Delta s = 1$ и определим новые значения длины пакета исправляемых ошибок:

$$l = s = 3 : b = l(s-1) + 1 = 3(3-1) + 1 = 7;$$

$$l = s = 4 : \Delta_l b = \frac{\partial b}{\partial l}\Delta l = (s-1)\Delta l = 2; b = b + \Delta_l b = 7 + 2 = 9;$$

$$\Delta_s b = \frac{\partial b}{\partial s}\Delta s = l\Delta s = 3; b = b + \Delta_s b = 7 + 3 = 10;$$

$$\Delta b = (s-1)\Delta l + (l + \Delta l)\Delta s = (3-1)\cdot 1 + (3+1)\cdot 1 = 2 + 4 = 6;$$

$$b = b + \Delta b = 7 + 6 = 13.$$

Для оценки вероятности правильной передачи и трансформации сообщения можно использовать формулу, учитывающую биномиальное распределение ошибок в канале связи:

$$P_{\text{пр.}} = \sum_{i=0}^{s} \binom{n}{i} \cdot P_{\text{с.}}{}^{i} \cdot (1 - P_{\text{с}})^{n-i}; P_{\text{тр.}} = 1 - P_{\text{пр.}}. \qquad (14)$$

$$P_{\text{с.}} = 1 - (1 - p)^{l}. \qquad (15)$$

Поэтому выражение (14) можно представить так:

$$P_{\text{пр.}} = \sum_{i=0}^{s} \binom{n}{i} \cdot [1 - (1-p)^{l}]^{i} \cdot (1-p)^{l\cdot(n-i)}; P_{\text{тр.}} = 1 - P_{\text{пр.}}. \qquad (16)$$

Оценим зависимость показателей достоверности от длины исправляемого пакета ошибок (рис. 7) для кодов Р-С со следующими характеристиками: $l = 8$; $p = 10^{-3}$; $t = \{100; 200\}$; $s = \{2: b = 9;\ 3: b = 17;\ 4: b = 25\}$.

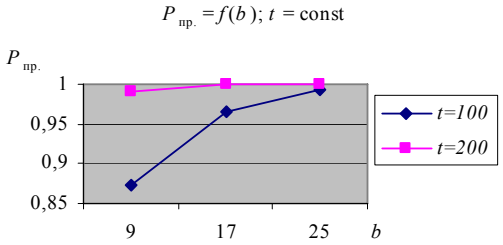


Рисунок 7 – Зависимость показателей достоверности от длины исправляемого пакета ошибок

Вывод по рис. 7: чем короче код, тем лучше показатели достоверности при тех же показателях группирования ошибок в канале передачи.

4 ЭКСПЕРИМЕНТЫ

Для проведения экспериментов были разработаны модели систем управления в среде MathWorks MatLab, пакет расширения Simulink [13] – с применением двоичного циклического кодирования (рис. 8) и кодов Р-С (рис. 9).

Построенные модели позволяют исследовать показатели достоверности в зависимости от свойств среды передачи отношения «сигнал/шум» – рис. 10, а, б.

DOI 10.15588/1607-3274-2019-4-21

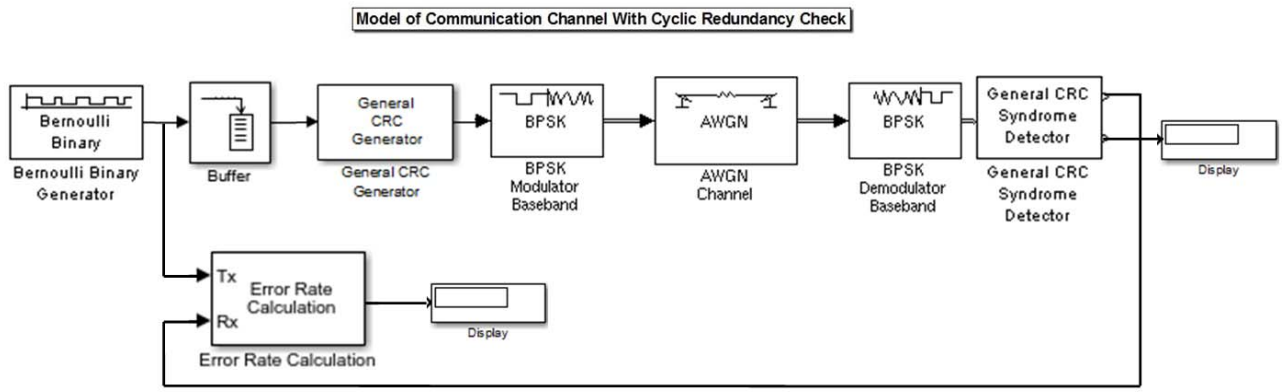


Рисунок 8 – Схемотехническая модель системы управления с двоичным циклическим кодированием

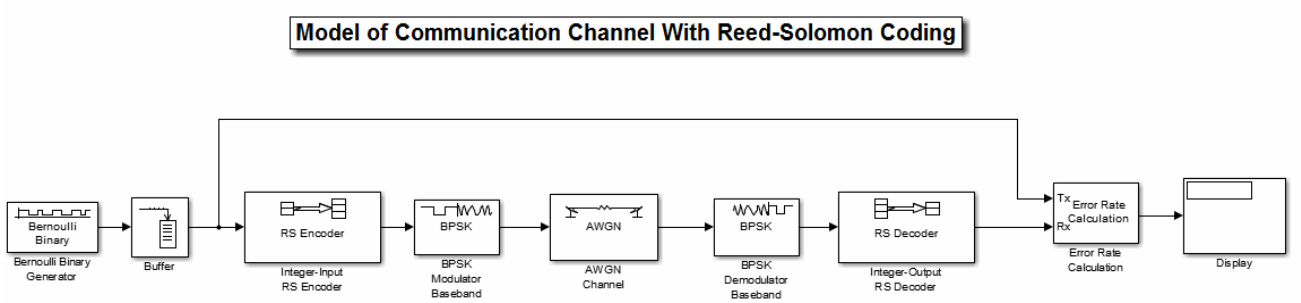
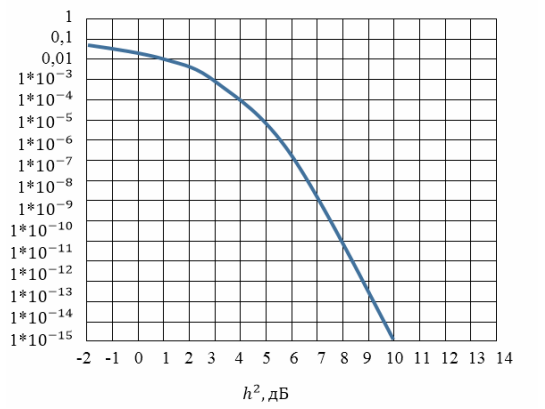
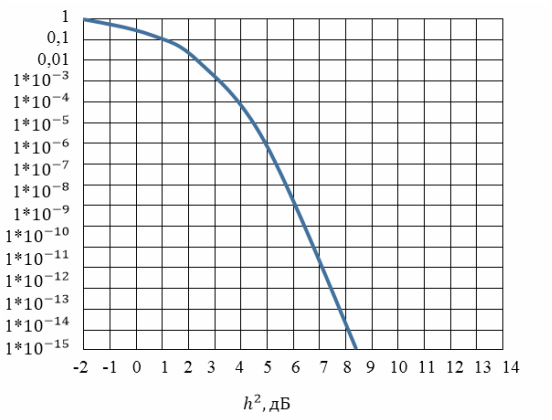


Рисунок 9 – Схемотехническая модель системы управления с недвоичным кодированием Р-С



а



б

Рисунок 10 – Зависимость вероятности ошибки для БЧХ-кодов (*а*) и кодов Р-С (*б*)

Проведенные эксперименты показали, что коды Р-С эффективнее БЧХ, поскольку имеют большую достоверность при меньшей избыточности.

Эксперимент 1.

Р-С: (7, 3, 5) → (21, 9); $l = 3$; $s = 2 \Rightarrow b = 4$;

$P_{\text{пр.}} = 0{,}99999017$.

БЧХ: (7, 3, 4); $i = 3 \rightarrow (21, 9) \Rightarrow b = 6$;

$P_{\text{пр.}} = 0{,}999812$.

Вывод: коды имеют одинаковую длину информационной части в двоичном представлении ($m = 9$) и информационную скорость (9/21). Но достоверность кода Р-С на два порядка лучше (5 «девяток» против 3 после запятой). Это объясняется тем, что код Р-С исправляет еще и независимые ошибки, которые могут отстоять друг от друга больше чем на b (например, в первом и в последнем символах).

Эксперимент 2.

Р-С: (7, 3, 5) → (21, 9); $l = 3$; $s = 2 \Rightarrow b = 4$;

$P_{\text{пр.}} = 0{,}99999017$.

БЧХ: (7, 3, 4); $i = 2 \rightarrow (14, 6) \Rightarrow b = 4$;

$P_{\text{пр.}} = 0{,}99992258$.

Вывод: коды имеют одинаковую длину исправляемого пакета ($b = 4$), но разные показатели достоверности (5 «девяток» против 4 после запятой). Это объясняется тем, что для кода Р-С b – минимальная (гарантированная) длина исправляемого пакета ошибок, а максимальная – $l \cdot s$ (для нашего примера 6), а для БЧХ – максимальная (6).

Построенные модели могут быть использованы для экспериментов с целью подбора параметров кода с заданной достоверностью и максимальной эффективностью. Реализованные в них алгоритмы являются основой для программной реализации процедур коди-

DOI 10.15588/1607-3274-2019-4-21

рования и декодирования в реальном аппаратурно-программном базисе (PLC, ПЛИС, других вычислительных устройствах систем управления) [14].

5 РЕЗУЛЬТАТЫ

В результате проведенных теоретических исследований получены зависимости существенных для проектирования показателей кодов (достоверность и информационная скорость) от структурных параметров кодов и характера поведения ошибок в среде передачи. Были определены аналитические зависимости, исследованы взаимовлияния дифференциальных параметров на интегральные, получены их графические иллюстрации и сделан анализ их характера.

Построены и исследованы имитационные схемотехнические модели системы управления, реализующие рассматриваемые способы кодирования, в пакете моделирования MatLab Simulink. С их помощью проведены экспериментальные исследования, которые подтвердили введенные математические положения. Другое назначение построенных моделей – задачи анализа и синтеза систем управления с заданными показателями достоверности и эффективности.

6 ОБСУЖДЕНИЕ

Проведенные исследования характеристик кодов Р-С и полученные зависимости могут быть использованы при выборе способа помехоустойчивого кодирования для исправления пакетирующихся ошибок. Для заданных технических условий – длина информационной части сообщения (m), показатели достоверности ($P_{\text{пр.}}$) и характеристики среды передачи (p, b) можно подобрать способ кодирования и параметры кода, чтобы обеспечить максимальную информационную скорость (R) для высокой эффективности использования ресурсов системы.

Разработанные модели и программные модули адаптированы для применения в программных модулях построения, расчета, кодирования и декодирования помехоустойчивых кодов при их практической реализации в аппаратурно-программном (ПЛИС) или программном (PLC) базисе.

ВЫВОДЫ

В работе решена задача исследования и выбора способа помехоустойчивого двоичного и недвоичного кодирования в условиях пакетирования ошибок. Были получены и проанализированы зависимости показателей достоверности от параметров кодов и свойств среды передачи для обеспечения их заданных значений при максимальной информационной эффективности.

Научная новизна представленных результатов заключается в том, что предложен способ расчета показателей достоверности для двоичного БЧХ-кода, исправляющего пакет ошибок, особенностью которого является учет всех возможных вариантов распределения ошибочных и правильно принятых бит в пакете. Это позволяет эффективно решать задачи синтеза и анализа систем управления с заданными показателями достоверности и максимальной эффективностью, подбирая структурные параметры кода и ориентируясь на свойства среды передачи информации. Также предложен оригинальный подход к исследованию зависимостей корректирующих свойств кода Р-С, отличием которого от известных является оценивание характера изменений их количественных показателей через частные производные по параметрам кода. Это дает возможность разработки рекомендаций по эффективному подбору параметров кодов для требуемых показателей достоверности и максимальной эффективности с учетом ресурсных ограничений.

Практическая значимость результатов работы заключается в реализации имитационных схемотехнических моделей системы управления, использующей исследуемые способы избыточного двоичного и недвоичного кодирования. Они позволяют выполнить исследования показателей достоверности и оценить эффективность использования пропускной способности системы при различных способах кодирования, структурных параметрах кодов и моделях воздействия помех. Модели является эффективным инструментарием для анализа и синтеза систем управления с заданными показателями достоверности и максимальной информационной скорости передачи.

Перспективы дальнейших исследований предполагаются в разработке алгоритмического и программного инструментария для расчета и сравнительного анализа характеристик избыточных кодов при действии помех различного характера поведения.

БЛАГОДАРНОСТИ

Представленные исследования проведены в рамках совместных научно-исследовательских и опытно-конструкторских работ с одним из ведущих отечественных разработчиков и производителей аппаратуры связи и информационно-управляющих систем – ПАО «Морион» (г. Пермь, Россия). Полученные результаты предназначены для аппаратурно-программной реализации кодирующих и декодирующих устройств, которые обеспечивают надежное взаимодействие модулей проектируемого оборудования по внутриблочной магистрали, также по локальным и транспортным каналам системы управления. Автор выражает глубокую признательность своему учителю и многолетнему руководителю работ профессору Ефиму Львовичу Кону за приобщение к научной тематике.

ЛИТЕРАТУРА / ЛІТЕРАТУРА

1. Кон Е. Л. Теория электрической связи. Помехоустойчивая передача данных в информационно-управляющих и телекоммуникационных системах: модели, алгоритмы, структуры / Е. Л. Кон, В. И. Фрейман. – Пермь : Пермский государственный технический университет, 2007. – 317 с.
2. Blahut R. E. Theory and practice of error control codes / R. E. Blahut. – Massachusetts : Addison-Wesley Publishing Company Incorporated, 1986. – 576 p.
3. Freyman V. Research and application of noise stability providing methods at information and control systems /

DOI 10.15588/1607-3274-2019-4-21

V. Freyman, I. Bezukladnikov // 2017 IEEE Conference of Russian young researchers in electrical and electronic engineering : 1–3 February 2017 : proceedings. – Saint-Petersburg : Saint-Petersburg Electrotechnical University «LETI», 2017. – P. 831–837.
4. Финк Л. М. Сигналы, помехи, ошибки / Л. М. Финк. – М. : Радио и связь, 1984. – 256 с.
5. Viterbi A. J. Principles of digital communication and coding / A. J. Viterbi, J. K. Omura. – New York : McGraw-Hill, 2009. – 584 p.
6. Sklar B. Digital communications. Fundamentals and applications. Second edition / B. Sklar. – New Jersey : Prentice Hall, 2001. – 1079 p.
7. Morelos-Zaragoza R. The art of error correcting / R. Morelos-Zaragoza. – Malden : Wiley, 2006. – 269 p.
8. Kumar A. A. Improved coding-theoretic and subspace-based decoding algorithms for a wider class of DCT and DST codes / A. A. Kumar, A. Makur // IEEE Transactions on Signal Processing. – 2010. – Vol. 58, № 2. – P. 695–708.
9. Freyman V. Research of the Reed-Solomon codes characteristic for realization within control systems devices / V. Freyman // Radio electronics, Computer science, Control. – 2019. – № 3 (50). – P. 143–151.
10. Kon E. L. Soft decoding based fuzzy logic for processing of elementary signals within data transmission channels of distributed control systems / E. L. Kon, V. I. Freyman, A. A. Yuzhakov // 2017 Systems of signal synchronization, generating and processing in telecommunications : 3–4 July 2017 : proceedings. – Moscow : Media-publisher, 2017. – P. 1–6.
11. Freyman V. Application of fuzzy logic for decoding and evaluation of results within the process of information system components diagnosis / V. Freyman, M. Kavalerov // 2017 IEEE Conference of Russian young researchers in electrical and electronic engineering : 1–3 February 2017 : proceedings. – Saint-Petersburg : Saint-Petersburg Electrotechnical University «LETI», 2017. – P. 134–139.
12. Freyman V. Methods and algorithms of soft decoding for signals within information transmission channels between control systems elements / V. Freyman // Radio electronics, Computer science, Control. – 2018. – № 4 (47). – P. 226–235.
13. MATLAB Documentation [Электронный ресурс]. – Режим доступа: http://www.mathworks.com/help/matlab/.
14. Bhargava K. Efficient implementation of error correction coding in a communication system by using VHDL / K. Bhargava // VSRD International Journal of Electrical, Electronics and Communication Engineering. – 2012. – Vol. 2 (6). – P. 359–365.

Статья поступила в редакцию 31.05.2019.
После доработки 01.09.2019.

УДК 621.391:004.052

АНАЛІЗ ДОСТОВІРНОСТІ ПЕРЕДАЧІ МІЖ ПРИСТРОЯМИ СИСТЕМ УПРАВЛІННЯ ПРИ ПАКЕТУВАННІ ПОМИЛОК

Фрейман В. І. – д-р техн. наук, професор кафедри «Автоматика і телемеханіка», Пермський національний дослідницького політехнічний університет, м. Перм, Росія.

АНОТАЦІЯ

Актуальність. Проведено аналіз показників достовірності передачі інформації між елементами систем управління з урахуванням пакетування (групування) помилок в каналі зв'язку. Об'єктом дослідження є характеристики і параметри завадостійких циклічних двійкових і недвійкових кодів, орієнтованих на виправлення пакетів помилок. Предмет дослідження – теоретичний і експериментальний порівняльний аналіз показників достовірності кодів, що виправляють пакети помилок.

Мета роботи – визначення аналітичних залежностей показників достовірності обраних надлишкових кодів від їх властивостей і якостей каналу зв'язку, розробка моделей для їх експериментального дослідження, формування рекомендацій щодо вибору кодів з заданими характеристиками при певних властивостях і моделі опису помилок.

Методи. Використаний математичний апарат і теорія побудови завадостійких циклічних двійкових (БЧХ) і недвійкових (Ріда-Соломона) кодів. Отримано аналітичні співвідношення для визначення показників достовірності передачі з урахуванням можливих спотворень символів коду всередині пакету помилок. Досліджено залежності коригувальних властивостей і ймовірності правильної передачі від параметрів коду і помилки, наведені ілюструвальні приклади. Розроблено імітаційні схемотехнічні моделі системи управління з досліджуваними способами завадостійкого кодування. Проведено експериментальні дослідження, на підставі отриманих даних зроблено висновки і запропоновані рекомендації щодо вибору параметрів кодів для заданих показників достовірності для забезпечення максимальної ефективності (інформаційної швидкості передачі).

Результати. Отримані залежності показників достовірності (ймовірність правильної передачі) і коригувальних властивостей (довжина пакета помилок, що виправляється) досліджуваних надлишкових кодів від їх параметрів (кількості надлишкових символів, ступеня перемеження – для БЧХ-кодів; модуль поля Галуа, кратність виправлених помилок – для кодів Ріда-Соломона). Надано рекомендації щодо використання отриманих результатів при виборі параметрів коду. Для проведення експериментальних досліджень створено і налаштовано моделі системи управління в середовищі MathWorks MatLab Simulink.

Висновки. Проведені в роботі дослідження дозволяють розрахувати і обґрунтовано вибрати параметри надлишкових кодів для заданих показників достовірності з урахуванням моделі поведінки помилок в каналі передачі. Це дає можливість проєктувати і реалізувати надійні системи управління із заданими показниками достовірності та максимальною інформаційною швидкістю передачі.

КЛЮЧОВІ СЛОВА: інформаційно-керуючі системи, достовірність, стійкість, надлишковість, циклічні коди, пакет помилок, модель.

DOI 10.15588/1607-3274-2019-4-21

UDC 621.391:004.052

ANALYSIS OF THE TRANSMISSION RELIABILITY BETWEEN CONTROL SYSTEMS DEVICES WHEN ERRORS ARE PACKAGED

Freyman V. I. – Doctor of Technical Science, Professor of Department «Automatics and telemechanics», Perm National Research Polytechnic University, Perm, Russia.

ABSTRACT

Context. The reliability indicators of information transmission between control systems elements, taking into account the packaging (grouping) of errors in the communication channel, are analyzed. The research object are the characteristics and parameters of noise stability cyclic binary and non-binary codes for the correction of error packets. The research subject is a theoretical and experimental comparative analysis of the reliability indicators of codes for correcting error packets.

Objective. The purpose of the work is to determine the analytical dependencies of the reliability indicators of the selected redundant codes from their parameters and the communication channel properties develop models for their experimental research, formulate recommendations for choosing codes with preset characteristics with certain properties, and an error description model.

Methods. The math methods and building theory of noise stability cyclic binary (BCH) and non-binary (Reed-Solomon) codes are used. The analytic formulas for determination of reliability indicators taking into account bits distortions within error packet are received. The dependencies for corrective properties and correct transmission probability form codes and error parameters are researched, the illustrating examples are shown. The simulation circuit design models for control systems with researched methods of noise stability encoding are developed. The experimental research has been done, based on the results, conclusions and recommendations for choice of code parameters for preset reliability indicators for providing of maximum efficiency (information rate) are made.

Results. The dependencies of the reliability indicators (correct transmission probability) and the corrective properties (the length of corrected errors packet) from its parameters (the number of redundancy symbols, the interleaving degree – for BCH-codes; the Galua field module, number of corrected errors – for Reed-Solomon codes) are received. The recommendations of using the received results for code parameters choice are given.

Conclusions. The performed researches allows calculate and reasonably choose of redundancy codes parameters for preset reliability indicators и the behavior model of errors within the communication channel. It makes possible to design and implement reliable control systems with preset reliability indicators and maximum information rate.

KEYWORDS: information and control systems, reliability, noise stability, redundancy, cyclic codes, error packet, simulation.

REFERENCES

1. Kon E. L., Freyman V. I. The theory of telecommunications. The noise stability data transmission within information and control and telecommunication systems: models, algorithms, structures. Perm, Perm State Technical University, 2007, 317 p.
2. Blahut R. E. Theory and practice of error control codes. Massachusetts, Addison-Wesley Publishing Company Incorporated, 1986, 576 p.
3. Freyman V., Bezukladnikov I. Research and application of noise stability providing methods at information and control systems, *2017 IEEE Conference of Russian young researchers in electrical and electronic engineering : 1–3 February 2017 : proceedings.* Saint-Petersburg, Saint-Petersburg Electrotechnical University «LETI», 2017, P. 831–837.
4. Fink L. M. Signals, noise, errors. Radio and communication, 1984, 256 p.
5. Viterbi A. J., Omura J. K. Principles of digital communication and coding. New York, McGraw-Hill, 2009, 584 p.
6. Sklar B. Digital communications. Fundamentals and applications. Second edition. New Jersey, Prentice Hall, 2001, 1079 p.
7. Morelos-Zaragoza R. The art of error correcting. Malden, Wiley, 2006, 269 p.
8. Kumar A. A., Makur A. Improved coding-theoretic and subspace-based decoding algorithms for a wider class of DCT and DST codes, *IEEE Transactions on Signal Processing*, 2010, Vol. 58, No. 2, pp. 695–708.
9. Freyman V. Research of the Reed-Solomon codes characteristic for realization within control systems devices, *Radio electronics, Computer science, Control,* 2019, No. 3 (50), pp. 143–151
10. Kon E. L., Freyman V. I., Yuzhakov A. A. Soft decoding based fuzzy logic for processing of elementary signals within data transmission channels of distributed control systems, *2017 Systems of signal synchronization, generating and processing in telecommunications, 3–4 July 2017, proceedings.* Moscow, Media-publisher, 2017, pp. 1–6.
11. Freyman V., Kavalerov M. Application of fuzzy logic for decoding and evaluation of results within the process of information system components diagnosis, *2017 IEEE Conference of Russian young re-searchers in electrical and electronic engineering, 1–3 February 2017, proceedings*. Saint-Petersburg, Saint-Petersburg Electrotechnical University «LETI», 2017, P. 134–139.
12. Freyman V. Methods and algorithms of soft decoding for signals within information transmission channels between control systems elements, *Radio electronics, Computer science, Control,* 2018, No. 4 (47), pp. 226–235.
13. MATLAB Documentation [Electronic resource]. Access mode: http://www.mathworks.com/help/matlab/.
14. Bhargava K. Efficient implementation of error correction coding in a communication system by using VHDL, *VSRD International Journal of Electrical, Electronics and Communication Engineering,* 2012, Vol. 2 (6), pp. 359–365.

DOI 10.15588/1607-3274-2019-4-21

Наукове видання

Радіоелектроніка,

інформатика,

управління

№ 4/2019

Науковий журнал

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 10.12.2019. Формат 60×84/8.
Папір офс. Різогр. друк. Ум. друк. арк. 26,97.
Тираж 300 прим. Зам. № 1463.

69063, м. Запоріжжя, НУ «Запорізька політехніка», друкарня, вул. Жуковського, 64

Свідоцтво суб'єкта видавничої справи
ДК № 6952 від 22.10.2019.