МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 10, № 1-2

Volume 10, No. 1-2

Одеса – 2020
Odesa – 2020

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Головний редактор: *А.А. Кобозєва*

Заступник головного редактора:
С.А. Положаєнко

Відповідальний редактор:
О.А.Стопакевич

Редакційна колегія:
І.І. Бобок, Д. Джухар, А.А. Кобозєва, В.Ф. Ложечніков, В.В. Любченко, В.Д. Павленко, В.В. Палагін, С.А. Положаєнко, О.В. Рибальський, А.В. Соколов, В.О. Сперанський, О.А. Стопакевич, О.О. Фомін

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration КВ № 17610 - 6460Р of 04.04.2011

Editor-in-chief: *A. Kobozeva*

Associate editor:
S. Polozhaenko

Executive editor:
O. Stopakevych

Editorial Board:
I. Bobok, J. Juhar, A. Kobozeva, V. Lozhechnikov, V. Liubchenko, V. Pavlenko, V. Palahin, S. Polozhaenko, O. Rybalsky, A. Sokolov, B. Speransky, O. Stopakevych, O. Fomin

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна

Телефон: +38 048 705 8506

Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odesa, 65044, Ukraine

Tel.: +38 048 705 8506

Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

© Одеський національний політехнічний університет, 2020

ЗМІСТ / CONTENTS

ОСОБЛИВОСТІ СТВОРЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ОРІЄНТОВАНИХ НА ДОСЛІДЖЕННЯ ПРОЦЕСІВ ДИФУЗІЇ О.В. Пивовар, С.А. Положаєнко	5	FEATURES OF CREATING INFORMATION TECHNOLOGIES FOCUSED ON THE RESEARCH OF DIFFUSION PROCESSES Pyvovar O., Polozhaenko S.
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ КРИТИЧНИХ ЯВИЩ У ТВЕРДОМУ РОЗЧИНІ НАПІВПРОВІДНИКІВ СПОЛУК A_2B_6 Г.В. Шаповалов, А.І. Казаков, П.П. Москвін, Д.О. Хомутенко, В.М. Петрів	11	MATHEMATICAL MODELING OF CRITICAL PHENOMENA IN SOLID SOLUTION OF SEMICONDUCTORS BASED ON A_2B_6 COMPOUNDS Shapovalov G., Kazakov A., Moskvin P., Khomutenko D., Petriv V.
РОЗРОБКА ПРОГРАМНОЇ ПІДТРИМКИ ДЛЯ СТВОРЕННЯ КОРПУСУ УКРАЇНСЬКОЇ МОВИ І ЙОГО ВИКОРИСТАННЯ О.І. Керпель, В.Г. Пенко	23	DEVELOPMENT OF SOFTWARE FOR THE CREATION OF THE CORPUS OF THE UKRAINIAN LANGUAGE AND ITS USE Kerpel O., Penko V.
ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НОРМОВАНОЇ ВІДОКРЕМЛЕНОСТІ МАКСИМАЛЬНОГО СИНГУЛЯРНОГО ЧИСЛА БЛОКУ МАТРИЦІ ЦИФРОВОГО ЗОБРАЖЕННЯ А.А. Кобозєва, І.І. Бобок	31	RESEARCHING THE PROPERTIES OF THE NORMALIZED SEPARATION OF THE MAXIMUM SINGULAR VALUE OF THE DIGITAL IMAGE MATRIX BLOCK Kobozeva A., Bobok I.
ОПТИМІЗАЦІЯ ІНФОРМАЦІЙНИХ СТРУКТУР ЛОКАЛЬНИХ МЕРЕЖ В.О. Хорошко, Ю.Є. Хохлачова, А. Аясрах, А. Аль-Далваш	45	OPTIMIZATION OF INFORMATION STRUCTURES OF LOCAL NETWORKS Khoroshko V., Khokhlachova Yu., Ayasrah A., Al-Dalwash A.
МОДИФІКАЦІЯ МЕТОДУ ХЕШ-СТЕГАНОГРАФІЇ, ЗАСНОВАНОГО НА ПЕРЕДАЧІ ПОСЛІДОВНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ В.В. Зоріло, О.Ю. Лебедєва, М.В. Бохонько	55	MODIFICATION OF THE HASH-STEGANOGRAPHY METHOD BASED ON THE TRANSFER OF A SEQUENCE OF DIGITAL IMAGES Zorilo V., Lebedeva O., Bokhonko M.

ВИЯВЛЕННЯ «РОЗУМНОГО РОЗМИТТЯ» ЯК ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ
О.Ю. Лебедєва, В.В. Зоріло, О.А. Карпова
61
DETECTING «SMART BLUR» AS A DIGITAL IMAGE INTEGRITY VIOLATION
Lebedeva O., Zorilo V., Karpova O.

МЕТОД ВИБОРУ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ
Ю.М. Ткач
68
METHOD OF SELECTION OF FUNCTIONAL PROTECTION PROFILE
Tkach Y.

РОЗРОБКА МЕТОДУ КОНТРОЛЮ ЦІЛІСНОСТІ ЗОБРАЖЕННЯ НА ОСНОВІ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ
І.С. Чіклікчі, А.А. Смагін, Л.В. Нечитайлова, Н.І. Кушніренко
75
DEVELOPMENT OF A METHOD FOR IMAGE INTEGRITY CONTROL BASEDON DIGITAL WATERMARK
Chiklikchi I., Smagin A., Nechitailova L., Kushnirenko N.

ЖИВУЧІСТЬ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЕРЖАВИ
В.О. Хорошко, Ю.Є. Хохлачова, А. Аясрах, А. Аль-Далваш
84
STABILITY OF THE STATE CYBER SECURITY SYSTEM
Khoroshko V., Khokhlachova Yu., Ayasrah A., Al-Dalwash A.

МАТЕМАТИЧНА МОДЕЛЬ ПЕРВИННОГО ПЕРЕТВОРЮВАЧА СИГНАЛІВ АКУСТИЧНОЇ ЕМІСІЇ ТА ЇЇ ПАРАМЕТРИЧНА ІДЕНТИФІКАЦІЯ
А.Ф. Верлань, С.А. Положаєнко
90
MATHEMATICAL MODEL OF THE PRIMARY CONVERTER OF ACOUSTIC EMISSION SIGNALS AND ITS PARAMETRIC IDENTIFICATION
Verlan A., Polozhaenko S.

ДОСЛІДЖЕННЯ РЕЖИМІВ ШИФРУВАННЯ З ПРОПУСКОМ БЛОКІВ
А.В. Соколов, А.О. Корж
100
STUDY OF BLOCK SKIP ENCRYPTION MODES
Sokolov A., Korzh A.

РОЗРОБКА КОНЦЕПЦІЇ СТВОРЕННЯ ІНТЕРФЕЙСУ ОПЕРАТОРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ УСТАНОВКАМИ ВІДПОВІДНО ДО ПРИНЦИПУ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ
А.О. Стопакевич, О.А. Стопакевич
109
DEVELOPMENT OF THE CONCEPT OF CREATION OF THE OPERATOR INTERFACE OF COMPUTER-INTEGRATED CONTROL SYSTEMS OF TECHNOLOGICAL PLANTS IN ACCORDANCE WITH THE PRINCIPLE OF SITUATIONAL AWARENESS
Stopakevych A., Stopakevych O.

DOI 10.15276/imms.v10.no1-2.5
УДК 004.94

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 5-10

FEATURES OF CREATING INFORMATION TECHNOLOGIES FOCUSED ON THE RESEARCH OF DIFFUSION PROCESSES

O.V. Pyvovar, S.A. Polozhaenko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: sanp277@gmail.com

The need to use information technology is due to many reasons. The current state of computer technology (CT), modern numerical methods make it possible to model objects whose behavior is described by very complex mathematical dependencies, for example, nonlinear systems of differential or integral equations. But complex computational algorithms have their own intrinsic properties, which are far from always analogous, even up to approximation errors, to the properties of the original mathematical model (MM). This can lead to effects of a purely computational nature. Therefore, an important task of the theory of numerical methods is (in relation to the considered structure of information technology (IT)) the development of computational algorithms that exclude or minimize the occurrence of such situations. At the same time, the problem of developing an adequate mathematical model for describing various diffusion processes (DP), as well as methods that implement them, remains very urgent. IT must ensure the "liberation" of a human researcher from performing labor-intensive unproductive operations of the computational process. In this article, issues related to the form of representation of solutions obtained in the course of mathematical modeling are considered. The introduction of the computational experiment method into the practice of theoretical research and a wide range of technologies for processing experimental data made it possible to solve fundamentally new problems, and, in some cases, led to the emergence of new subject areas that could not exist before the advent of modern CT and the development of IT.

Keywords: multimedia information technology, diffusion process, mathematical modeling, computational experiment.

Introduction

The main circle of problems solved in the course of mathematical modeling is the development of mathematical models (MM) of the studied processes, as well as the development of computational and numerical methods for the implementation of these MM. Anomalous diffusion is a diffusion process when the classical Einstein relationship is violated, that is, the standard deviation of the position of a wandering particle is not a linear function of time. In practice, many diffusion processes are actually anomalous. In the existing literature, there are many theoretical calculations for describing anomalous diffusions (the method of reducing partial differential equations to ordinary ones, followed by the numerical solution of modeling and identification problems; the method of quasi-linearization and sweep in a parameter; the method of conjugate functions), as well as descriptions of MM variants, but always large of interest is the most accurate and, in practice, easily used MM of anomalous diffusion.

At the same time, issues related to the form of representation of solutions obtained in the course of mathematical modeling should also be recognized as important. First of all, this aspect concerns the application of information technology (IT) and is associated with the presentation, analysis and implementation of the resulting solutions. It is the implementation in a practical way, as well as the IT requirements for the implementation of MM, that is proposed in this article.

The aim of the work is to identify and analyze the basic requirements for information technology, focused on the presentation of the results of mathematical modeling of diffusion (including the so-called "anomalous") processes.

To achieve this target, it is necessary to solve the following tasks:

- to define and to analyze the tasks facing information technologies in the mathematical modeling of processes;
- to justify the need to use information technology;
- to identify the requirements for information technologies for solving problems of mathematical modeling of the diffusion process.

Main part

The problems arising (as noted above) in the interpretation of the results of mathematical modeling are, in particular, the following. In a number of important applied cases, in the course of mathematical modeling, the investigated diffusion processes (DP) are considered as processes with distributed parameters. The spatial domain of processes with distributed parameters in modeling is represented by a finite-dimensional mesh of nodes [1-3] or finite elements [4, 5], and the state function is an array of values of grid functions at these nodes (or functions in finite elements). Depending on the required accuracy of the solution, the resulting arrays of grid functions (functions in finite elements) have significant sizes ($10^2 \ldots 10^5$ values). With such a number of values, the possibilities for interpreting solutions become of paramount importance (for example, ordering arrays of values and their forms of presentation, methods of storage and handling, transformation, etc.).

In addition, the results of mathematical modeling are often only an intermediate link in the applied problem being solved. In particular, when solving problems of controlling technological or natural processes (technical objects), as a result of mathematical modeling, a function of the state of the object is obtained, according to which the control action is synthesized (taking into account the control law). In this case, as a rule, the synthesis of the control action should be carried out in a real (or even in an accelerated) time scale in the case of solving optimization or multivariate problems. Taking into account the fact that technological or natural processes (technical objects), as noted earlier, are mainly processes with distributed parameters (objects with distributed parameters) (with their inherent features and complexities of mathematical modeling and, above all, significant sizes of arrays that determine the values functions of state), then rational methods of data processing acquire a priority. In these conditions, IT, focused on the creation and application of methods and tools for processing the results of mathematical modeling, constitutes an urgent scientific and applied technical problem.

The formation of a wide class of modern theoretical and applied areas of scientific research (associated, for example, with the atmosphere, the extraction of minerals and other physically complex processes and objects in which a certain kind of diffusion anomalies arise) has become fully possible only thanks to the advent of computer modeling. Examples of the most important areas of research in which mathematical (computer) modeling plays a major role are, in particular, problems of numerical weather prediction, climate change and issues related to pollution of the atmosphere and other components of the environment.

The need to use IT in this case is due to a number of reasons:

- equations describing various processes cannot be solved analytically without using numerical methods, the implementation and interpretation of which is due to the use of IT tools;
- modeling of the specified class of processes is associated with a huge amount of computations, which often requires the use of the most powerful means of CT and developed IT;

- the only experimental data on the state of complex processes are the data of numerous observations (for example, for geological processes, this is drilling wells and measuring reservoir pressures in them; for processes in the atmosphere, this is the determination of the characteristics of its state using ground stations, weather balloons, aviation, various remote control systems sounding based on ground-based radars and orbiting satellites), and the assimilation of such an extensive set of data from various sources is impossible without the use of modern systems for processing, collecting and transmitting information;
- modeling (including mathematical) implies manipulation of significant amounts of intermediate data and analysis (for example, systematization, long-term forecast, etc.) of the results obtained, the effective implementation of which is impossible without the use of certain IT;
- a number of problems of mathematical modeling (especially in the field of studying the regional and global climate; seismic exploration, geodesy and geoecology; variational assimilation of data in complex technological processes) is associated with the need to maintain huge data archives, constant and effective access to which must be provided by IT means.

If we consider mathematical modeling in conjunction with the IT that implements it, then, in this case, it is permissible to talk about information and mathematical modeling (IM modeling) [4, 6]. In this case, the process of IM-modeling includes: collection of the necessary information (in accordance with the set goal), which constitutes (determines) the information model of the process (object) under study; processing of the received data (their organization or structuring) and the algorithm for transforming this data (encapsulation); formation of MM process (object); geometrization of the model or its results of computational implementation (computer visualization by means of computer graphics - the execution of geometric constructions).

Thus, we can conclude that IT provides, in solving problems of mathematical modeling, in the narrow sense, preparation (and, if necessary, collection, as, for example, in the case of modeling atmospheric processes) of the initial data and interpretation of the solution results in a convenient form. or, in a broader sense, IT acts as a toolkit for the implementation of methods and means of mathematical modeling, constituting, in conjunction with the latter, the basis of IM modeling, in which IT and mathematical modeling tools most effectively complement each other in the course of solving applied problems.

The most important factor that determines the effectiveness of IT is its structure (i.e. the elements that make up IT, and the topological connections between them).

Academician AA Samarsky proposed IT [6, 7], the structure of which (Fig. 1) most fully meets the goal of solving problems of mathematical modeling. At the same time, the IT structure is presented in the form of the "MODEL - ALGORITHM - PROGRAM" structure, which defines an unambiguous action plan for the use of mathematical modeling methods:

- choice (or construction) of an "equivalent" of an object, reflecting in mathematical form its most important properties - the laws to which it obeys, the connections inherent in its constituent parts, etc. (in other words, the essence of MM);
- selection (or development) of an algorithm for implementing the model on PC;
- creation of programs that "translate" MM and the algorithm into an accessible PC language.

The following should be noted regarding the properties of this structure. MM - as the most important link in the structure - must be adequate to the object (process) under study. This should be confirmed by an experiment of one kind or another (that is, the “behavior” of a real object (process) and its MM under equal conditions should coincide). After establishing the adequacy of the structure to the original object with MM, various "experiments" are carried out: computational experiments that give all the required qualitative and quantitative properties and characteristics of the object (process).

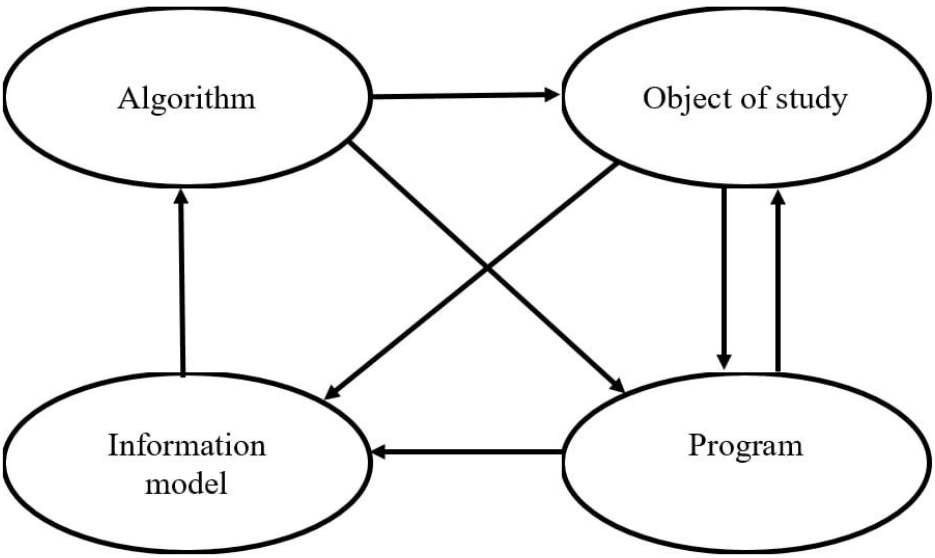


Fig. 1. IT structure focused on solving problems of mathematical modeling (typical structure)

A computational experiment is designed to study, predict, optimize complex (including multiparameter and nonlinear objects (processes)), the theoretical and experimental study of which is difficult by traditional methods.

A computational experiment, in contrast to experiments on natural objects (processes), allows one to accumulate the results obtained in the study of a certain range of problems, and then quickly and flexibly apply them to solving problems in completely different areas. This property is possessed by “universal” MMs that formalize most of the DP. For example, the equation of nonlinear thermal conductivity is suitable for describing not only thermal processes, but also diffusion of matter, movement of groundwater, and gas filtration in porous media. Only the physical meaning of the quantities included in this equation changes. The modeling process is accompanied by the improvement and refinement, as necessary, of all links of the structure.

It should be noted that programs that implement computational algorithms play an important role in the above structure. They must ensure the efficiency of solving a mathematical problem with a minimum of computational costs.

Thus, IT supporting a computational experiment, in their structure, include: methods for constructing MM, support for the latest implementations for finding and selecting algorithms and programs for numerical solution of problems, methods and tools for the accuracy of the calculations performed and the correct operation of the programs used.

Considering the above, the IT structure shown in Fig. 1, can be taken as a typical (generalized) one, which is focused on solving problems of mathematical modeling, since it covers all the main aspects of solving the specified class of problems. On the basis of a typical IT structure, IT structures are formed, designed to solve applied problems of mathematical modeling.

Analysis of the basic requirements for information technology focused on solving problems of mathematical modeling of diffusion processes

It is obvious that IT that provide the solution of a certain class of problems of mathematical modeling (in particular, modeling of diffusion processes) must meet certain requirements. These requirements reflect the relationship between the main (basic) properties of objects, processes; phenomena investigated in the course of mathematical modeling with the means of applied IT and, ultimately, determine the effectiveness of the latter.

Let's analyze the basic requirements for IT, focused on solving problems of mathematical modeling of diffusion processes. The following requirements are considered basic in the mathematical modeling of diffusion processes:

- the ability to process large-scale arrays of numerical information, which are fields of values of the required functions of the state of the DP. Moreover, this processing should provide both operations on multidimensional (mainly two- and three-dimensional) arrays, and the possibility of obtaining a result in real (or even accelerated) time scale, taking into account the subsequent solution of multivariate and optimization control problems;
- the ability to adequately display the qualitative dynamic behavior of the DP at the stage of visualization of the solution of mathematical modeling problems, taking into account the predominantly distributed nature of the processes under study. In other words, when visualizing the received (or displayed) with the help of one or another IT solutions, the latter should be adequate, i.e. with an accuracy to full-scale experiments on a real object (process), reflect its dynamic behavior, taking into account the action on the object (process) of external disturbances and controls;
- creation of effective (from the point of view of computational costs) numerical methods for the implementation of the MM DP in the procedures of IM-modeling. The complexity of the formalization of the problems of mathematical modeling of DP, caused by the finite unrepresentability of the MM of the DP, the nontrivial nature of the spatial regions of modeling and boundary conditions, imposes increased requirements on the computational costs of the computer implementation of the methods used as part of the IT used. Ultimately, the computational costs for the implementation of mathematical modeling methods determine the influence of these methods (as an integral part of the IM-modeling technology) under the conditions of the given criteria;
- the ability to automate the process of mathematical modeling of DP. IT should free the researcher from performing time-consuming operations of the computational process. For example: setting geometry and discretizing spatial areas; determination of parameters of discrete spatial areas; recalculation and re-assignment of these parameters in the course of solving non-stationary and non-linear problems; assignment, recalculation and input of initial and boundary conditions, etc. The human researcher, if necessary, retains the functions of analysis and decision-making based on the results of mathematical modeling.

Conclusion

The basic requirements for IT focused on solving problems of mathematical modeling of diffusion processes are stated. Possible ways of increasing the efficiency of these ITs in the course of applied research are shown, and the possibility of interpreting the typical IT structure for solving scientific and engineering problems is analyzed.

References

1. Верлань А.Ф., Положаенко С.А., Сербов Н.Г. Математическое моделирование процессов аномальной диффузии. Киев: Наукова думка, 2011. 416 с.
2. Бусленко Н.П. Моделирование сложных систем. Москва:Наука, 2001. 374с.
3. Коздоба Л.А. Электрическое моделирование явлений тепломассопереноса. Москва: Энергия, 1972. 296 с.
4. Згуровский М.З., Мельник В.С., Новиков А.Н. Прикладные методы анализа и управления нелинейными процессами и полями. Киев: Наукова думка, 2004. 588 с.
5. Мацевитый Ю.М., Прокофьев В.Е. Моделирование нелинейных процессов в распределенных системах. Киев: Наукова думка, 1985. 302 с.
6. Самарский А.А., Михайлов А.П. Компьютеры и жизнь: Математическое моделирование. Москва: Педагогика, 1987. 157 с.
7. Самарский А.А., Михайлов А.П. Математическое моделирование: Идеи. Методы. Примеры. Москва: Физматлит, 2005. 265 с.

ОСОБЕННОСТИ СОЗДАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ОРИЕНТИРОВАННЫХ НА ИССЛЕДОВАНИИ ДИФФУЗИОННЫХ ПРОЦЕССОВ

О.В. Пивовар, С.А. Положаенко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sanp277@gmail.com

Необходимость использования информационной технологии обусловлена множеством причин. Нынешнее состояние вычислительной техники (ВТ), современных численных методов позволяют осуществлять моделирование объектов, поведение которых описывается весьма сложными математическими зависимостями, например, нелинейными системами дифференциальных или интегральных уравнений. Но сложные вычислительные алгоритмы обладают своими внутренними свойствами, которые далеко не всегда аналогичны, даже с точностью до ошибок аппроксимации, свойствам исходной математической модели (ММ). Это может приводить к появлению эффектов, имеющих чисто вычислительную природу. Поэтому важной задачей теории численных методов является (применительно к рассматриваемой структуре информационной технологии (ИТ)) разработка вычислительных алгоритмов, исключающих или сводящих к минимуму появление подобных ситуаций. При этом проблема разработки адекватных ММ для описания различных диффузионных процессов (ДП), а также методов, их реализующих, остается весьма актуальной. ИТ должна обеспечить «освобождение» человека-исследователя от выполнения трудоемких непроизводительных операций вычислительного процесса. В статье, рассмотрено вопросы, связанные с формой представления получаемых в ходе математического моделирования решений. Внедрение метода вычислительного эксперимента в практику теоретических исследований и широкого спектра технологий обработки экспериментальных данных позволило решить принципиально новые задачи, а, в ряде случаев, привело и к возникновению новых предметных областей, существование которых было невозможно до появления современных средств ВТ и развития ИТ.

Ключевые слова: мультимедийная информационная технология, диффузионный процесс, математическое моделирование, вычислительный эксперимент.

ОСОБЛИВОСТІ СТВОРЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ОРІЄНТОВАНИХ НА ДОСЛІДЖЕННЯ ПРОЦЕСІВ ДИФУЗІЇ

О.В. Пивовар, С.А. Положаєнко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sanp277@gmail.com

Необхідність використання інформаційної технології обумовлена безліччю причин. Нинішній стан обчислювальної техніки (ОТ), сучасних чисельних методів дозволяють здійснювати моделювання об'єктів, поведінка яких описується досить складними математичними залежностями, наприклад, нелінійними системами диференціальних або інтегральних рівнянь. Але складні обчислювальні алгоритми мають свої внутрішні властивості, які далеко не завжди аналогічні, навіть з точністю до помилок апроксимації, властивостям вихідної математичної моделі (ММ). Це може призводити до появи ефектів, що мають чисто обчислювальну природу. Тому важливим завданням теорії чисельних методів є (стосовно аналізованої структурі інформаційної технології (ІТ)) розробка обчислювальних алгоритмів, що виключають або зводять до мінімуму появу подібних ситуацій. При цьому проблема розробки адекватних ММ для опису різних дифузних процесів (ДП), а також методів, їх реалізують, залишається досить актуальною. ІТ повинна забезпечити «звільнення» людини-дослідника від виконання трудомістких непродуктивних операцій обчислювального процесу. У статті, розглянуто питання, пов'язані з формою подання одержуваних в ході математичного моделювання рішень. Впровадження методу обчислювального експерименту в практику теоретичних досліджень і широкого спектру технологій обробки експериментальних даних дозволило вирішити принципово нові завдання, а, в ряді випадків, призвело і до виникнення нових предметних областей, існування яких було неможливо до появи сучасних засобів ОТ і розвитку ІТ.

Ключові слова: мультимедійна інформаційна технологія, дифузійний процес, математичне моделювання, обчислювальний експеримент.

DOI 10.15276/imms.v10.no1-2.11
УДК 004.94

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 11-22

MATHEMATICAL MODELING OF CRITICALl PHENOMENA IN SOLID SOLUTION OF SEMICONDUCTORS BASED ON A_2B_6 COMPOUNDS

G.V. Shapovalov[1], A.I. Kazakov[1], P.P. Moskvin[2], D.O. Khomutenko[2], V.M. Petriv[2]

[1] Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: shapovalovhennady@gmail.com
[2] Zhytomyr State Technological University,
103, Chudnivska Str., 10005 Zhytomyr, Ukraine

Mathematical modeling of critical phenomena in multicomponent solid solutions of semiconductors was carried out on the basis of the theory of phase transitions and the theory of catastrophes. A mathematical method is proposed for calculating the spaces of coexistence of phases in solid solutions of semiconductors of II – VI groups of the periodic system. An algorithm for calculating the zero contours of the free energy function of the system, critical spaces and spaces of phase coexistence is presented. For calculating spaces of coexistence of phases of order two in ternary solid solutions based on semiconductors of II – VI groups of the periodic system the differential topological approach was used. The calculations were carried out in the framework of the regular solution model. Interactions both of the first and the second nearest neighbor pairs of atoms and also the temperature dependence of the interaction parameter were considered additionally. Modern methods of computer simulation are used for analyzing processes of occurrence of self-organizations ordered structures. Multicomponent phase diagrams, taking into account the possibility of existence of bifurcation spaces and critical spaces and spaces of coexistence of phases of different orders were obtained. The positions of the spaces of coexistence of second-order phases for the Zn-Cd-Te system are calculated using the mathematical method proposed in this work. Multicomponent phase diagrams have been obtained, taking into account the possibility of the existence of bifurcation spaces, critical spaces and spaces of coexistence of phases of different orders, makes it possible to predict the processes of loss of stability in three-component semiconductor solutions based on compounds II - V and groups of the periodic system with different modes of their synthesis and operation.

Keywords: Computer simulation, phase diagrams, solid solutions, alloys, semiconducting II–VI materials.

Introduction

The development of modern methods of computer modeling led to the possibility of predicting the properties of multicomponent semiconductor materials. One of the promising areas is the mathematical modeling of processes leading to degradation of the properties of semiconductor compounds. Some progress has been made in this area; however, some directions in the modeling of processes in semiconductors remain poorly studied. In particular, there are practically no papers related to the modeling of spaces in which two or more phases can coexist simultaneously in solid solutions of semiconductors. This circumstance is a significant omission, since in many solid solutions, for example, obtained on the basis of A_2B_6 semiconductor compounds [1-5], metastable states associated with the formation of phases of coexistence spaces are observed. The problem of creating and investigating A_2B_6 materials, which has optimal properties for tasks of electronics, is increasingly important today. Moreover crystal properties

play the most important part for characteristic of created devices. The researches of A_2B_6 multicomponent materials received have shown that homogeneous solid solutions of semiconductors occur unstable. This leads to spinodal ordering and forming periodical structures with modulated composition. The loss of thermodynamic stability with respect to composition fluctuations, which is possible in a multicomponent solid phase, can lead to the appearance of metastable or unstable states of multicomponent solid solutions. The appearance of critical phenomena in unstable solid phases leads to the degradation of the properties of optoelectronic devices. However, the problem of predicting the possibility of appearing spaces of the coexistence of fazes in A_2B_6 solid solutions was studied not enough. In this paper, a thermodynamic model is considered in which the temperature dependences of the interaction parameter between the atoms of the first two coordination spheres are taken into account. One of the promising solid solutions based on A_2B_6 is $Zn_XCd_{1-X}Te$. On the basis of the model considered and using a differential topological approach, a spaces of coexistence of phases of order two for the Zn-Cd-Te system is obtained.

Main part

Modern computer models describe the properties of semiconductor compounds based on A_2B_6 quite correctly. In [6] within the framework of the polyassociative model, a satisfactory description of the phase diagram was obtained and the thermodynamic functions of the dissociation of complexes in the Cd-Hg-Te system were found. A good agreement with the experimental data was obtained in the modeling of phase equilibrium for the Zn-Cd-Te system in [7]. Attempts are made [8, 9] to construct models for explaining intrinsic ferromagnetism in $Zn_{1-x}Cr_xTe$. The first steps have been taken to model the appearance of an additional geometric phase in semiconductor systems with a strong spin-orbit coupling [10, 11]. The static model of the formation of an exciton condensed phase with allowance of the nonequilibrium effects in a two-dimensional system is presented in [12, 13]. Modeling based on the variational approach makes it possible to study the influence of the magnetic field on the energy of the ground state of exciton-donor complexes [14]. Mixing models for studying the effective dielectric permittivity of alloys was considered in [15]. A model was proposed [16] that allows one to explain the characteristic features of the photoluminescence spectra of single quantum dots of CdMnSe/ZnSe. A model is obtained for studying the process of self-assembly of tetrahedral cells in alloys [17]. Attempts were made to construct models for explaining ferromagnetism in ZnMnO on the basis of assumptions about its intrinsic nature [18] or as a consequence of some metastable phase [19]. A model is known [20] that quantitatively describes the processes of passivity of defects in a polycrystalline CdTe:Cl. The article [21] describes a model based on a completely microscopic theory, which allows one to demonstrate the effect of high-order optical nonlinearities in the coherent control signal for ZnSe. The [22] proposed a model that allows one to explain of laser shock waves impact on a defect system in narrow-gap HgCdTe alloys. Modelling proposed in the article [23] provides calculations of internal tensions in the ZnBeSe alloys. A model has been developed [24] that makes it possible to describe the photoluminescence spectra of localized excitons of $CdS_{1-x}Se_xS$ with a hexagonal structure and alloys in which regions with a hexagonal structure and a structure with stacking faults coexist. Work continues on improving the models that explain the mechanism of the transition from 2D to 3D growth in the CdSe / ZnSe system [25]. There are contradictory models on the basis of which attempts are made to describe the growth of ZnO films on GaAs substrates by pulsed laser

deposition [26 – 30]. Model representations [31] make it possible to better understand the photoluminescence spectra of an (Cd,Mn)Te in the presence of a spin-polarized two-dimensional hole gas and can now be useful in elucidating certain properties of the magnetic phase in a quantum well.

Thermodynamic modeling of critical phenomena in solid solutions of A_2B_6 semiconductors. Simulation of the process of formation of critical spaces and spaces of coexistence of phases in multicomponent and multiphase systems may be carried out on the basis of a differential topological approach [32, 33, 37 – 42]. According to Maxwell's principle, the space of coexistence of phases arises when two (or more) global minima of potential functions of system have the same depth. The appearance of such a space corresponds to the classical phase transition of the first kind. At some points in this space, the existing phase may become unstable, creating a bifurcation subspace. Two phases in some space may be identical under certain conditions, creating a critical space of the second order. When there is three or four identical phases having critical spaces of third order or fourth respectively.

Modeling of critical phenomena for A_2B_6 we will show on an example of Zn-Cd-Te system that is of great interest as a buffer material in the formation of heterostructures strictly matched for a period of crystal lattices for infrared devices and X-ray sensors To obtain a thermodynamic model to predict of the ordering in a triple system, it is necessary to construct an expression for the free energy of the system as a potential function dependent on the system parameters. In the framework of this paper, the expression for the free energy of a $Zn_XCd_{1-X}Te$ solid solution was constructed as a function of the component concentrations and temperature of the system $F=F(X_{AB},X_{AC},T)$, where X_{AB} and X_{AC} are understood to mean the concentration of atomic pairs $Zn-Te$ and $Cd-Te$ in a quasi-binary approximation. To analyze the existence of a stable phase need conditions [32] under which the first derivative of the free energy of the system by the concentrations of the corresponding components x will be equal to zero, and the second derivative will have positive values:

$$\frac{dF}{dx}=0\,;\quad \frac{d^2F}{dx^2}>0\,. \tag{1}$$

The space of instability that is bifurcation space is calculated on the conditions of zero first and second derivatives, and the positive value of the third derivative:

$$\frac{dF}{dx}=\frac{d^2F}{dx^2}=0\,;\quad \frac{d^3F}{dx^3}>0\,. \tag{2}$$

The condition for the existence of a critical space of the second order is the correspondence with the zero values of the first, second and third derivatives simultaneously and the positive value of the fourth derivative:

$$\frac{dF}{dx}=\frac{d^2F}{dx^2}=\frac{d^3F}{dx^3}=0\,;\quad \frac{d^4F}{dx^4}>0\,. \tag{3}$$

In formulas (1–3) there are complete derivatives, which in the case of $Zn_XCd_{1-X}Te$ alloy means differentiation by X_{AB} and X_{AC}.

Thus, for calculating the positions of the boundaries of phase stability, it is necessary to construct an analytical expression for free energy. The application of the above mathematical

procedures will allow analytically obtain the position of the boundaries of the critical spaces of the required order. At the same time, the expressions (2) correspond to the spinodal curves indicating the thermodynamic position of a completely unstable state of the phase. To calculate the positions of the boundaries of the metastable states (binodals of decay), it is necessary to compare the expressions (1) that need to be written for each of the coexisting phases.

Thermodynamic modeling of free energy of a solid phase of $Zn-Cd-Te$ system. The free energy of the triple zinc system can be looked at as the sum of free energy contributions for pure binary solids components, i.e., zinc and cadmium systems, the free energy of the ideal mixture, without taking into account the interaction between the components and the component taking into account the deviation of the value of the free energy from the energy of the ideal solution [34, 35]:

$$F = \sum_{i=1}^{2} F_i + F^{id} + \Delta F^{ex} , \tag{4}$$

where F_i is the free energy for pure binary components with F_{Zn-Te} and F_{Cd-Te} constituents; F^{id} is the free energy of the ideal mixture without taking into account the interaction between the components; ΔF^{ex} – deviation of the value of free energy from the energy of the ideal solution. The Bethe grid, taking into account the interaction of the first and second nearest adjacent atoms, is depicted in Fig. 1. For convenience, different types of atoms, i.e. atom Te, Zn, and Cd, are indicated by the numbers 1, 2 and 3, respectively. Mark 2, 3 denotes the location of an atom of type 2 or 3.

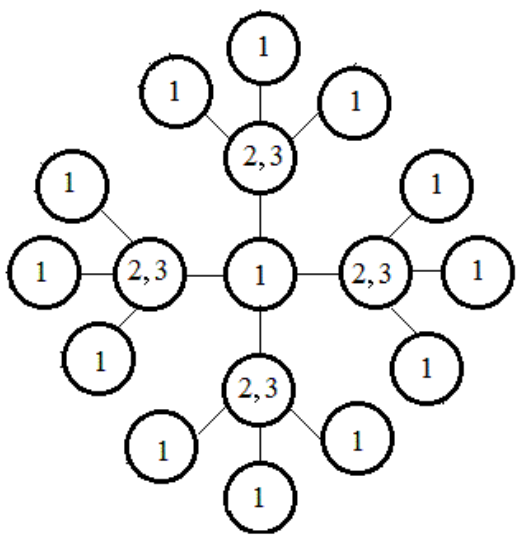


Fig. 1. Bethe grid for a triple $Zn_X Cd_{1-X} Te$ solid solution. The number 1 denotes the atom Te, 2 is the atom Zn, and 3 is the atom Cd

Then, taking into account the interactions of the atoms of the first and second coordination spheres, the components of free energy for pure binary constituents can be represented as:

$$F_{12} = \left\{ w_{12} + \frac{z_2}{z_1}(w_{11}^2 + w_{22}^1) \right\} , \tag{5}$$

$$F_{13} = \left\{ w_{13} + \frac{z_2}{z_1}(w_{11}^3 + w_{33}^1) \right\} , \tag{6}$$

where w_{12} is the binding energy between atoms Te and Zn, provided that they are the first closest neighbors. Accordingly, w_{13} denotes the binding energy between the nearest adjacent atoms of Te and Cd. The denotations w_{11}^2 and w_{11}^3 in (5) and (6) correspond to the binding energy between the second nearest neighboring atoms of Te on the condition that atom of Zn or atom of Cd is located between them respectively. Accordingly, w_{22}^1 and w_{33}^1 is the binding energies between the second nearest neighboring atoms of Zn and atoms of Cd on the condition that the Te atom is between them. Constants z_1 and z_2 in (5) and (6) are respectively the number of nearest neighboring atoms for each of the atoms (z_1=4) and second nearest neighboring atoms (z_2=12) in a zinc grid. It should be noted quite complicated problems associated with the calculation of energy connections, but in the process of obtaining derivatives, already at the stage of finding the second derivative, in connection with the linearity of expressions (5) and (6) this part of the expression (2) is completely degenerate and does not affect the verification of conditions (2) – (3).

The free energy for a mixture of ideal components of a solution, that is, the second term in (4) can be found by the classical expression:

$$F^{id} = -TS^{id} ,$$

where S^{id} is the entropy of an ideal solution, in which the atoms are randomly located. The value of the configurationally entropy S^{id} can be expressed in terms of the total number of atoms in the solution N_0 and the concentration parameter x:

$$S^{id} = -R \cdot ((1-x)\ln x + x\ln x) , \tag{7}$$

where R - gas constant. Taking into account the connection of the concentration parameter x with the number of pairs of atoms N_{12} and N_{13}:

$$x = N_{12} / N_0$$
$$1 - x = N_{13} / N_0$$

and the number of pairs of atoms with corresponding moles of X_{12} and X_{13}:

$$N_{12} = z_1 N_0 X_{12}$$
$$N_{13} = z_1 N_0 X_{13}$$

the expression (7) can be represented as:

$$S^{id} = -z_1 R \cdot (X_{12}\ln X_{12} + X_{13}\ln X_{13}) . \tag{8}$$

The formula (8) is most convenient for differentiation.

The deviation of the value of the free energy from the energy of the ideal solution is expressed by the difference between the configuration entropy and the entropy of the ideal solution, the temperature and the mixing energy:

$$F^{ex} = -T(S - S^{id}) + \Delta E \,. \tag{9}$$

According to the theory of simple solutions, the mixing energy ΔE can be expressed through the interaction parameter and mole fractions of the solution components in the form:

$$\Delta E = \alpha_{12-13} \frac{X_{12} X_{13}}{X_{12} + X_{13}} ,$$

where α_{12-13} – interaction parameter. In the approximation $S = S^{id}$, the expression (4) taking into account (9) takes the form:

$$F = \sum_{i=1}^{2} F_i - TS^{id} + \Delta E \,. \tag{10}$$

Note that for the analysis of higher derivatives in terms of composition concentrations starting from the second one, in the framework of the regular approximation it suffices to consider only two last terms in (10):

$$\begin{aligned} -TS^{id} + \Delta E = z_1 TR(X_{12}\ln X_{12} + X_{13}\ln X_{13}) + \\ + \alpha_{12-13} \frac{X_{12} X_{13}}{X_{12} + X_{13}} \end{aligned} .$$

The interaction parameter α_{12-13} within the framework of work was considered as a function of temperature T [37]:

$$\alpha_{TeZn-TeCd} = (17230 - 14{,}83\mathrm{T})\ \mathrm{J/Mole}.$$

Prediction of critical phenomena in ternary system $Zn - Cd - Te$**.** In order to analyze the probability of occurrence of critical spaces and spaces of coexistence of phases in the system $Zn - Cd - Te$, the analytical expressions of higher derivatives according to the order parameters X_{ij} for the free energy of the system were obtained and investigated. Derivatives by concentrations from the first to fourth inclusive for the free energy (4) of the solid solution $Zn_X Cd_{1-X} Te$ were calculated using the methods of matrix-vector differentiation of multidimensional systems. To obtain matrices of higher derivatives, the method of direct sums [34] was used. The algorithm for calculating the higher derivatives of free energy consisted of successive calculations of components of derivatives by corresponding concentrations, compilation of matrices from components of derivatives, calculation of their determinants and calculation of positions of zero contours. As a result of calculating the first derivative of free energy (4), components of the derivative F_i $(i = 1, 2)$ of the function of two variables was obtained as two partial derivatives by X_{12} and X_{13}:

$$F_i = \begin{pmatrix} F_1 \\ F_2 \end{pmatrix},$$

where F_1 and F_2 are partial derivatives of free energy by X_{12} and X_{13}, respectively. The obtained analytical expressions were used to calculate the components of the second derivative of the free energy of the investigated system:

$$F_i = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix}, \tag{11}$$

where the element of the matrix F_{11} is the analytic expression of the partial derivative of F_1 by X_{12} concentration, F_{12} is the corresponding derivative of F_1 by X_{13} concentration, F_{21} is the derivative of F_2 by X_{12} concentrations and F_{22} is the derivative of F_2 by X_{13}. The analytical expression of the determinant of the second derivative was obtained for the components of the matrix (11) and its value was calculated according to the concentration parameter x with the given step for $x \in (0;1)$. The values found were used to obtain the null contours of the second derivative and to analyze the stable phases of the $Zn - Cd - Te$ system in accordance with (1). To obtain the highest free energy derivatives, the Maxima system's calculation tools were used [43]. The results of calculations are shown in Fig. 2.

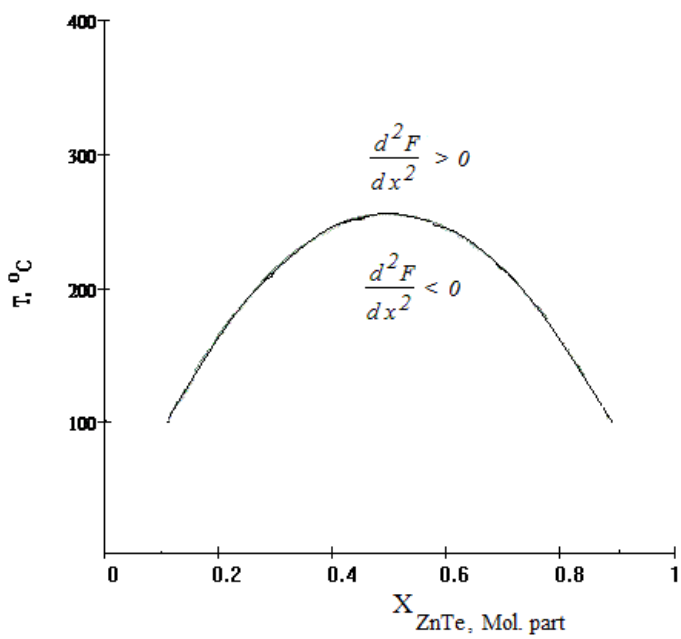


Fig. 2. The cross section of the existence of solid solutions phase diagram of $Zn - Cd - Te$ system. The results of numerical calculations of the zero contour of the second derivative of the free energy of the system are shown

The points satisfying the condition $\det F_i = 0$ were reflected on the cross section for the existence of solid solutions of the state diagram of the $Zn - Cd - Te$ system. After that, areas were determined in which the values of the respective determinants were positive or negative. In

the next step, each of the elements F_{ij} of the matrix (1.3.2) differentiated by concentrations X_{ij}. As a result of the differentiation, two matrices of partial derivatives were obtained. The first of them consisted of the components of the F_{ij} obtained by differentiation by X_{12}, the second one from the components obtained by differentiation in X_{13}:

$$F_{ij1} = \begin{pmatrix} F_{111} & F_{121} \\ F_{211} & F_{221} \end{pmatrix}, \quad F_{ij2} = \begin{pmatrix} F_{112} & F_{122} \\ F_{212} & F_{222} \end{pmatrix}. \tag{12}$$

The expression for the determinant of the third derivative was obtained on the basis of the direct sum method as the sum of the determinants of the matrices (12):

$$DetF_{ijk} = DetF_{ij1} + DetF_{ij2}\,. \tag{13}$$

The calculations of the values of the determinants (13) were used to calculate the instability spaces, that is, the bifurcation spaces under the conditions (2). The results of calculations of zero contour are shown in Fig. 3.

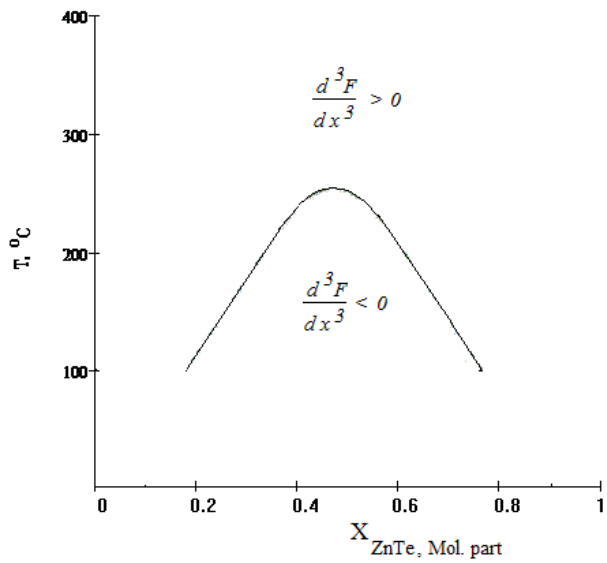


Fig. 3. The cross section of the existence of solid solutions phase diagram of $Zn-Cd-Te$ system. The results of numerical calculations of the zero contour of the third derivative of the free energy of the system are shown

To obtain the analytical expression of the determinant of the fourth derivative of free energy, the matrices of the partial derivatives of the components (12) were calculated:

$$F_{ij11} = \begin{pmatrix} F_{1111} & F_{1211} \\ F_{2111} & F_{2211} \end{pmatrix}, \quad F_{ij12} = \begin{pmatrix} F_{1112} & F_{1212} \\ F_{2112} & F_{2212} \end{pmatrix} \quad F_{ij21} = \begin{pmatrix} F_{1121} & F_{1221} \\ F_{2121} & F_{2221} \end{pmatrix}, \tag{14}$$

$$F_{ij22} = \begin{pmatrix} F_{1122} & F_{1222} \\ F_{2122} & F_{2222} \end{pmatrix}.$$

The determinant of the complete fourth derivative of free energy was obtained as the sum of the determinants of the matrices (14):

$$DetF_{ijkl} = DetF_{ij11} + DetF_{ij12} + DetF_{ij11} + DetF_{ij22}$$

The results of the calculation of the zero contours of the complete fourth derivative of the free energy of the system are shown in Fig. 4.

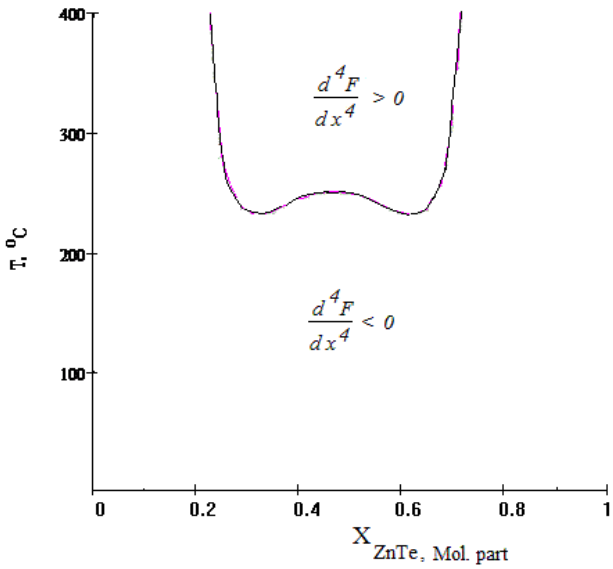


Fig. 4. The cross section of the existence of solid solutions phase diagram of $Zn-Cd-Te$ system. The results of numerical calculations of the zero contour of the fourth derivative of the free energy of the system are shown

In order to verify the condition (3) and calculate the domains of the second-order critical space were used the results of calculating the values of the determinants of the matrices (11), (12) and (14), as well as the positions of the zero contours depicted on Fig.2. - 4. The region in which the most probable occurrence of critical spaces of the second order is shown in Fig. 5:

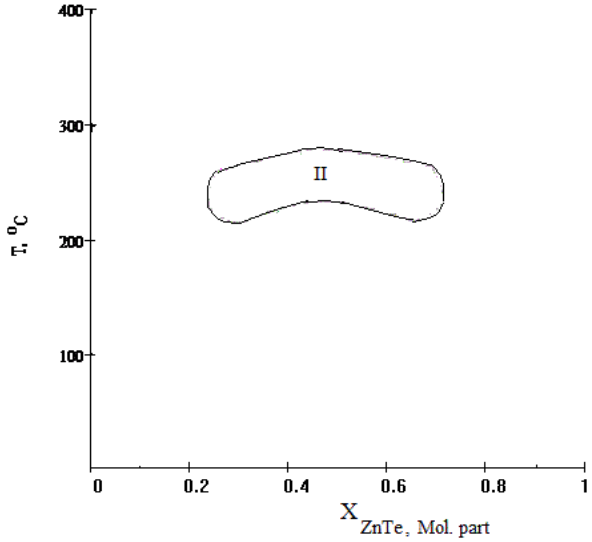


Fig. 5. The cross section of the existence of solid solutions phase diagram of $Zn-Cd-Te$ system. The results of numerical calculations of the region of the conditions for forming the spaces of coexistence of phases of order two are shown (the region found is indicated by the mark II)

Conclusion

Within the framework of thermodynamic modelling, the zero contours of the free energy derivatives from the first to the fourth inclusive was calculated and plotted for the $Zn_X Cd_{1-X} Te$ solid solution on the diagrams of the state of the $Zn - Cd - Te$ system. The space in which the simultaneous occurrence of two kinds of solid phases is most probable was found for the $Zn - Cd - Te$ system. The results are obtained for temperatures in the range from 100 to 400 degrees Celsius. From the results of the calculations, it follows that the most probable region of the concentration space in which space of coexistence of phases of the order of two can form corresponds to concentrations in the range of 0.25 – 0.75 at temperatures of the 210-290 degrees Celsius. The data obtained during the simulation are important from a practical point of view, since they are related to the difficulties in the synthesis of $Zn_X Cd_{1-X} Te$ layers and allow the development of recommendations for the process of their growing under different conditions. The study of the obtained positions of the zero contours of higher derivatives of free energy in the framework of the considered model opens the possibility of estimating the occurrence of periodic oscillations of the composition. The proposed model allows us to analyze the processes of formation of concentration domains in the volume of material while providing the necessary conditions for the synthesis of $Zn_X Cd_{1-X} Te$ solid solutions.

The results obtained in this paper open up the possibility of studying the possibility of the emergence in a solid solution of spaces of coexistence of phases of higher orders [40, 41], when three or more simultaneously coexisting spaces may arise in the solid phase.

References

1. Romcevic M., Kulbachinskii V.A., Romcevic N., Maryanchuk P.D., Churilov I.A. Optical Properties of $Hg_{1-x}Mn_xTe_{1-y}Se_y$. *Infrared Physics & Technology*. 2005. V.46, P. 379-387.
2. Romcevic N., Romcevic M., Golubovic A., Khoi L., Mycielski A. Far-infrared and Raman spectroscopy of $Cd_{1-x}Mn_xTe_{1-y}Se_y$: Phonon properties. *Journal of Alloys and Compunds*. 2005. V.397. P. 52-57.
3. Hsieh C.H., Huang Y.S., Ho C.H. et al. Temperature dependence of the band-edge transitions of ZnCdBeSe. *Jpn. J. Appl. Phys*. 2004. V.43, 459.
4. Maksimov O., Guo S.P., Tamargo M.C. Be-Chalcogenide alloys for improved R-G-B LEDs: Be[x]Zn[y]Cd[1-x-y] Se on InP, *Phys. Stat. Sol.* 2002. V.229. 1005.
5. Sorokin V.S., Sorokin S.V., Kaygorodov V.A. et al. The Instability and Immiscibility Regions in $Mg_xZn_{1-x}S_ySe_{1-y}$ *Alloys, J. Cryst. Growth.* 2000. V.214/215. 130 p.
6. Moskvin P.P., Khodakovsky V., Rashkovetskii L., Stronski A.J. *Crystal Growth*. 2008. V.310(10). 2617.
7. Singh A.K., Sharma R.C. *CALPHAD*. 1992. V.16(2). 161.
8. Saito H. et al. *Phys. Rev. Lett.* 2003. V.90. 207202.
9. Bergqvist L. et al. *Phys. Rev. Lett.* 2004. V.93, 137202.
10. Morpurgo A.F., Heida J.P., Klapwijk T.M., Wees B.J., Borghs G. *Phys. Rev. Lett.* 1998. 80(5). 1050.
11. Yau J.B., Poortere E.P., Shayegan M. *Phys. Rev. Lett*. 2002. V.88(14). 146801.
12. Sugakov V.I. *Physics of the Solid State*. 2004. V. 46, 1496.
13. Sugakov V.I. *Sol. St. Comm*. 2005. V.134, 63 p.
14. Avetisyan A.A., Djotyan A.P. Kazaryan E.M. *Phys. Stat. Sol.* 2003. 734.
15. Karkkainen K., Sihvola A., Nikoskinen K. IEEE GRSS V.39. 2001.
16. Nawrocki M., Rubo Yu.G., Lascaray J.P., Coquillat D. *Phys. Rev. B.* 1995. V.52. 2241.
17. Elyukhin V.A, Sanchez V.M., Elyukhina O.V. *Appl. Phys. Lett.* 2004. V.85. 1704 p.
18. Jung S.W., An S.J., Gyu-Chul Y. *Appl. Phys. Lett*. 2002. V.80. 4561.
19. Kundaliya D.C., Ogale S.B. et al. *Nature Materials*. 2004. №3. 709.
20. Yanfa Y, Al-Jassim M.M., Jones K.M. *J. Appl. Phys.* 2004. V.96. 320.
21. Voss T. et al., *Phys. Rev. B.* 2002. V.66. 155301.

22. Yakovyna V., Berchenko N., Kurbanov K., Virt I., Kurilo I., Nikiforov Yu. P*hys. Stat. Sol. 2*003. 1019.
23. Postnikov A.V., Pages O., Hugel J., *Phys. Rev. B 71*. 2005. 115206.
24. Novikov B.V., Grigorieva N.R., Grigoriev R.V., et all. *Phys. Stat. Sol.* B. V.229. 69.
25. Kim C.S. et al. *Phys. Rev. Lett.* 2000. V.85. P.1124-1127.
26. Ryu et al. *J. Crystal Growth.* 2000. V.216. 330.
27. Hwang et al., *J. Crystal Growth*, 2003. V.254, P.449
28. Look et al., *Appl. Phys. Lett.* 2004. V.85. 5269.
29. Morhain et al. *Phys. Status Solidi B.* 2002. V.229. 881.
30. Almamun Ashrafi et al.: *Appl. Phys. Lett.* 2000. V.76. 550.
31. Kossacki P., Boukari H., Bertolini M. et al. *Phys. Rev.* 2004. V.70. 195337.
32. Okada K., Suzuki I. Classical calculations on the phase transition I. Phase diagram in four-dimensional space for the system with one order parameter. *J. Phys. Soc. Jap.* 1982. V.51(10). P. 3250-3257.
33. Magnus J.R., Neudecker H. Matrix Differential Calculus with Applications in Statistics and Econometrics. Wiley Series in Probability and Statistics. Wiley,1999. P. 171-173.
34. Laugier A. Thermodynamics and phase diagram calculations in II-VI and IV-VI ternary systems using an associated solution model. *Revue De Physique Applique*. 1973. V.8(9). P. 259-26.
35. Onabe K. Thermodynamics of the type $A_{1-x}B_xC_{1-y}D_y$, III-V quaternary solid solutions. *J.Phys.Chem.Solids*, 1982. V.43(11). P. 1071-1086.
36. Moskvin P.P. The polyassocompatible model of the melt and p-T-x equilibrium in the Zn-Cd-Te system. *Journal of Physical Chemistry*. 2010. №11. P. 210-215.
37. Gogunskii V., Piterska V., Kolesnikov O., Lukianov D., Kolesnikova K., Development of the markovian model for the life cycle of a project's benefits. *Eastern-European Journal of Enterprise Technologies*. 2018. V.5(4). 95 p.
38. Kazakov A., Kishmar I. Computer simulation for stability of quaternary solid solutions. *J. Crystal Growth*. 1991. V.110. P. 803-814.
39. Kazakov A., Kishmar I. Stability analysis of quaternary alloys including the lattice mismatch strain energy. *J. Crystal Growth.* 1992.V. 125. P. 509 – 518.
40. Kazakov A., Burtnyi D., Shapovalov G. Calculation of the phases coexistence spaces in the system Hg-Mn-Te-Se. *Proceedings of Odessa Polytechnic University*. 2018. V.54(1). P. 69-73.
41. Kazakov A.I., Shapovalov G.V., Moskvin P.P. Computer simulation for formation of critical spaces in II–VI solid solutions. *Journal of Crystal Growth.* 2019. V.506. P. 201-205.
42. Moskvin P., Skurativskyi S., Kravchenko O., Skyba G., Shapovalov H. Spinodal decomposition and composition modulation effect at the lowtemperature synthesis of $A_xB_{1-x}C_x$ semiconductor solid solutions. *Journal of Crystal Growth*. 2019. V.510. P. 40-46.
43. Maxima, a Computer Algebra System. URL: http://maxima.sourceforge. Netcomputer.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ КРИТИЧЕСКИХ ЯВЛЕНИЙ В ТВЕРДЫХ ПОЛУПРОВОДНИКОВЫХ РАСТВОРАХ СОЕДИНЕНИЙ A_2B_6

Г.В. Шаповалов[1], А.И. Казаков[1], П.П. Москвин[2], Д.А. Хомутенко[2], В.М. Петров[2]

[1] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: shapovalovhennady@gmail.com
[2] Житомирский государственный технологический университет,
ул. Чудновская, 103, Житомир, 10005, Украина

Математическое моделирование критических явлений в многокомпонентных твердых растворах полупроводников было проведено на основе теории фазовых переходов и теории катастроф. В работе разработан метод математического моделирования для вычисления пространств сосуществования фаз второго порядка в тройных твердых растворах на основе соединений II - V групп периодической системы. Представлен алгоритм расчета нулевых контуров функции свободной энергии системы, критических пространств и пространств сосуществования фаз. Нулевые контуры функции свободной энергии системы находились с использованием дифференциально-топологического подхода. Вычисления положений пространств сосуществования фаз проводились в рамках приближения регулярного раствора с помощью свободного пакета компьютерной

алгебры Maxima. Математическое моделирование пространств сосуществования фаз были выполнены в приближениях взаимодействия как первой, так и второй ближайших соседних пар атомов, а также температурной зависимости параметра взаимодействия. Для анализа процессов возникновения самоорганизованно упорядоченных структур используются современные методы компьютерного моделирования. Рассчитаны положения пространств сосуществования фаз второго порядка для системы полупроводников с использованием предложеного в работе математического метода. Получено многокомпонентные фазовые диаграммы с учетом возможности существования бифуркационных пространств, критических пространств и пространств сосуществования фаз различных порядков, дает возможность прогнозировать процессы потерю стабильности в трехкомпонентных полупроводниковых растворах на основе соединений II - V и групп периодической системы с различными режимами их синтеза и эксплуатации.

Ключевые слова: математическое моделирование, фазовые диаграммы, твердые растворы полупроводников II – VI групп.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ КРИТИЧНИХ ЯВИЩ У ТВЕРДОМУ РОЗЧИНІ НАПІВПРОВІДНИКІВ СПОЛУК A_2B_6

Г.В. Шаповалов[1], А.І. Казаков[1], П.П. Москвін[2], Д.О. Хомутенко[2], В.М. Петрів[2]

[1] Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: shapovalovhennady@gmail.com
[2] Житомирський державний технологічний університет,
вул. Чуднівська, 103, Житомир, 10005, Україна

Математичне моделювання критичних явищ у багатокомпонентних твердих розчинах напівпровідників було проведено на основі теорії фазових переходів і теорії катастроф. В роботі розроблено метод математичного моделювання для обчислення просторів співіснування фаз другого порядку у потрійних твердих розчинах на основі сполук II – VI груп періодичної системи. Надано алгоритм обчислення нульових контурів функції вільної енергії системи, критичних просторів і просторів співіснування фаз. Нульові контури функції вільної енергії системи знаходились за використанням диференціально-топологічного підходу. Обчислення положень просторів співіснування фаз проводились у рамках наближення регулярного розчину за допомогою вільного пакету комп’ютерної алгебри Maxima. Математичне моделювання просторів співіснування фаз було виконано у наближеннях взаємодії як першої, так і другої найближчих сусідніх пар атомів, а також температурної залежність параметра взаємодії. Для аналізу процесів виникнення самоорганізовано впорядкованих структур використовуються сучасні методи комп'ютерного моделювання. Обчислено положення просторів співіснування фаз другого порядку для системи напівпровідників з використанням запропонованого в роботі математичного методу. Отримано багатокомпонентні фазові діаграми з урахуванням можливості існування біфуркаційних просторів, критичних просторів та просторів співіснування фаз різних порядків, що надає змогу прогнозувати процеси втрату стабільності у трьохкомпонентних напівпровідникових розчинах на основі сполук II – VI груп періодичної системи за різними режимами їх синтезу та експлуатації.

Ключові слова: математичне моделювання, фазові діаграми, тверді розчини напівпровідників II – VI груп.

DOI 10.15276/imms.v10.no1-2.23
УДК 004.912

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 23-30

DEVELOPMENT OF SOFTWARE FOR THE CREATION OF THE CORPUS OF THE UKRAINIAN LANGUAGE AND ITS USE

O.I. Kerpel, V.G. Penko

Odessa I.I.Mechnikov National University,
2, Dvoryanskaya St., Odessa, 65026, Ukraine, e-mail: alexeykerpel15@gmail.com, vpenko@onu.edu.ua

The relevance of the work lies in the need to analyze Ukrainian texts in order to study the Ukrainian language and the lack of appropriate information and software resources. The object of research is the variety of tools for the task of POS tagging of Ukrainian texts. The subject of the research is the process of developing software for creating corpora of Ukrainian texts, in particular, POS tagging algorithms. The purpose of the work is to research and develop software for creating an annotated corpus of the Ukrainian language. To achieve this goal, following tasks were solved: analysis of the subject area; selection of suitable software tools; creating a training set; system implementation; system training; system testing. An approach to the generation of a training sample was designed and implemented. The approach is based on the use of an already implemented tagger of the Russian language and the similarity of the morphological structure of words in the Russian and Ukrainian languages. The search for an effective combination of the feature space and the training algorithm was made. The most successful machine learning models for this task turned out to be stochastic gradient descent and decision trees. K-fold cross-validation was used to achieve an acceptable level of generalization. As a result of this work, a trained tagger of the Ukrainian language was obtained, which, for a sample of literary Ukrainian texts, provides the quality of classification at the level of 0.892 according to the weighted F-measure. A distributed application with a client-server architecture has been implemented, which allows clients to tag their own texts. With the regular use of this application by linguistic experts, the training set used can be improved, which will lead to higher rates of classification carried out by the tagger.

Keywords: POS tagging, text corpus, machine learning algorithms, feature space.

Introduction

At the moment, processing of the natural texts is becoming more and more demanded in different contexts. Among them are speech recognition systems (Cortana, Siri), search engines (Google, Yandex, Yahoo), etc. Also, computer processing of natural texts is necessary to detect plagiarism which is present in the works of various authors by identifying certain patterns in the texts of different genres. Word processing can be useful in tasks such as organizing search in search engines, speech recognition, automatic detection of topics on web pages, translation of texts, and in many similar tasks that require advanced word processing.

Within text analysis research area, text corpora (plural form of corpus notion) are commonly used. Corpora are collections of various texts that allow you to study the language from different angles and contain different types of markup (meta-data, such as morphological, semantic, syntactic, etc.). Until recently, the only possible way to compose such a corpus was to tag texts manually, but the development of information technologies opened up new opportunities by enabling markup process automation and significantly reducing (or completely eliminating) the need for human (expert) intervention in the word recognition area.

Unfortunately, for the Ukrainian language there is still lack of marked-up corpora and software resources sufficient for practical use, which would allow the natural text markup automation.

Up till now, there is only one corpus of the Ukrainian language developed by the KNU. T. Shevchenko. Despite the declared presence of part-of-speech markup, in fact, the search for parts of speech on the official website does not work [1], and the search is available exclusively in legislative texts. There is also a project according to which the development of the corpus of the Ukrainian language from NU Ostrozka Academy is underway. Work on the project started in 2010. However, there is essentially no progress in the development of the project [2].

The goal of this work is to create an automated system that allows you to generate text markup as a basis for creating corpora of Ukrainian texts in future.

Given the variety of tagging types, construction of universal tools of this kind is hardly possible. Due to this limitation, it was decided to focus on obtaining part-of-speech markup or POS tagging.

To achieve defined goal, following tasks were accomplished:

- analysis of the POS tags system used in the Ukrainian language;
- investigation of the possibility of building simple automatic taggers (usually based on regular expressions). Evaluation the effectiveness of such taggers for the Ukrainian language;
- investigation of the approaches to building an automated tagger based on machine learning methods in terms of their applicability to the Ukrainian language;
- implementation of the automated tagger and analysis of the effectiveness of its performance;
- implementation of the distributed system to provide access to the classification system based on the automated tagger.

Main Part

At the first stage, there is a need to clarify the system of the Ukrainian tags. The system of parts of speech of the Ukrainian language is generally accepted [3]. In the process of implementing the POS tagger, it was decided to use standard tag notation, shown on the table 1.

Table 1.

List of the Ukrainian POS-tags

Independent POS		Tag	Auxiliary POS	Tag
Іменник		S	сполучник	CONJ
Прикметник		A	прийменник	PR
Числівник		NUM	частка	PART
Займенник		A-PRO		
Дієслово		V		
Прислівник		ADV		

Simple taggers.POS-tagging is a well-known problem in the field of natural text processing problems. To date, a wide range of diverse approaches to solving this problem have been proposed [4]. There are two relatively simple possibilities for building taggers: based on dictionaries or regular expressions.

In the case of a dictionary usage, it will be necessary to create a dictionary consisting of all the words of the language, as well as all their forms, which will require a huge waste of resources and is an extremely difficult and time-consuming task. And still, there are many ambiguity cases.

A regex-based tagger is simpler, but has a disadvantage of being not suitable for all languages. Regular expression tags are very different depending on a languages. Building such taggers requires deep expertise in the grammar of a particular language. It has a fairly low tagging accuracy (even for English - about 85% on average versus machine learning-based taggers - 97%). To improve accuracy, it is necessary to continuously increase the number of regular expressions, which is highly complex and effort-consuming task, and it is also less effective than analogs based on machine learning. A regular expression tagger is barely suitable for tagging Slavic languages due to the high number of different cases and word forms, which, in its turn, leads to extremely low accuracy of tag recognition in the text.

In connection with the above, systems based on machine learning have been selected as the most effective means for solving the problem of POS-tagging of the Ukrainian language.

Training set. The absence of tagged Ukrainian texts is an obstacle to obtaining a training set within the framework of the problem being solved. To solve this problem in this work, it was decided to use the scheme involving the combination of Russian and Ukrainian languages, as languages belonging to the same Slavic group. One of the features of this similarity is the similar word order in the sentence. Due to this similarity, as well as the presence of the Russian language POS tagger in the NLTK library, it became possible to take Ukrainian texts, split them into words, translate them into Russian words and tag them as the Russian text, and then match the tags to the Ukrainian words as shown on the figure 1. Thus, it was possible to automatically obtain a sufficiently large and high-quality sample base which can be used as training set in machine learning experiments.

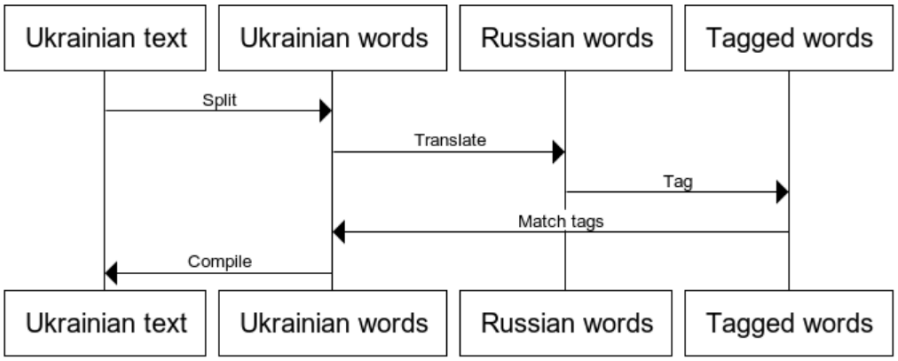


Fig. 1. Training set construction

The training set contains the fiction texts as shown on the table 2.

Table 2.

Training set texts

Texts (Ukrainian translation)	Words
Dead Souls, by Nikolai Gogol	3114
The Master and Margarita by Mikhail Bulgakov	2101
War and Peace by Leo Tolstoy	2283

Note that Ukrainian translations of famous literature works were chosen as the source texts. At this stage, relatively small fragments of these texts have been used.

Features. One of the most elaborate operations in creation of an effective automated tagger based on classifiers is the determination of a set of entity attributes. These attributes affect its compliance with certain classes. In the field of machine learning these entity attributes are called features. Determining the appropriate feature sets is critical. In this case, the most effective features can be present in the text in an implicit form. Research toward finding successful feature sets and their subsequent use represents an important subsection of machine learning, commonly referred to as feature engineering [5,6].

Due to the importance of identifying an effective set of features, a study was conducted to identify the optimal set of features. The task of identifying the best features is tightly associated with the task of determining the most appropriate learning algorithm. However, an exhaustive computational experiment in this two-dimensional space is extremely time-consuming. In this work, a simplified approach is used. The SGD classifier was chosen as a basic classifier to determine the effectiveness of certain features, shown in table 3.

The feature search strategy is based on the idea of revealing the most intuitive possible features and then checking their compatibility with each other.

Table 3.

Class features

Features	Meaning	Weighted F-score
word	The word itself	0.78
word + is_first	If the word is first in sentence	0.78
word + is_last	If the word is last in sentence	0.775
word + position	The position of the word in sentence	0.76
word + capitalized	If the word is capitalized	0.776
word + is_all_caps	If all the letters are uppercase	0.778
word + is_all_lower	If all the letters are lowercase	0.7785
word + prefix-1	First letter	0.72
word + prefix-2	First 2 letters	0.733
word + prefix-3	First 3 letters	0.77
word + suffix-1	Last letter	0.73
word + suffix-2	Last 2 letters	0.8
word + suffix-3	Last 3 letters	0.82
word + suffix-4	Last 4 letters	0.82
word + all suffixes	All suffixes	0.845
word + all prefixes	All prefixes	0.766
word + all suffixes and prefixes	All suffixes and prefixes	0.89
word + prev_word	The word before the current	0.76
word + next_word	The word after the current	0.75
word + has_hyphen	If the word has hyphen	0.78
word + is_numeric	If the word consists of digits	0.78
word + capitals_inside	If the word has capitals inside	0.78
All the above	All the features	0.89
All the above – capitalized	All the features except capitalized	0.892
All the above – capitalized – prev_word – next_word	All the features except capitalized, previous and next words	0.892

Machine learning algorithms. Another important aspect that affects the performance and efficiency of classification is the type of machine learning algorithms. Machine learning scientists have developed a huge number of these algorithms. Our practical choice was limited to a basic set of algorithms that are implemented in the popular scikit_learn programming tool [7].

Stochastic Gradient Descent (SGD) is a simple yet very efficient approach to fitting linear classifiers and regressors under convex loss functions such as (linear) Support Vector Machines and Logistic Regression.

Decision Trees (DTs) are a non-parametric supervised learning method used for classification and regression.

A multilayer perceptron (MLP) is a type of artificial neural network.

An MLP consists of at least three layers of nodes: an input layer, a hidden layer and an output layer. Except for the input nodes, each node is a neuron that uses a nonlinear activation function. MLP utilizes a supervised learning technique called backpropagation for training.

K-neighbours. Classification is computed from a simple majority vote of the nearest neighbors of each point: a query point is assigned the data class which has the highest number of representatives within the nearest neighbors of the point.

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operate by constructing a multitude of decision trees at training time and outputting the class that is the mode of the classes or mean/average prediction of the individual trees.

The output of the other learning algorithms ('weak learners') is combined into a weighted sum that represents the final output of the boosted classifier. AdaBoost is adaptive in the sense that subsequent weak learners are tweaked in favor of those instances misclassified by previous classifiers.

The mentioned above classifiers were compared on the selected set of features on different training set range. To obtain better generalization, K-block cross validation was used [8]. The results are shown on figure 2.

As we can see on the figure. 2, the best classifiers, according to the weighted F-score is SGD classifier. So we can choose it for the following application implementation.

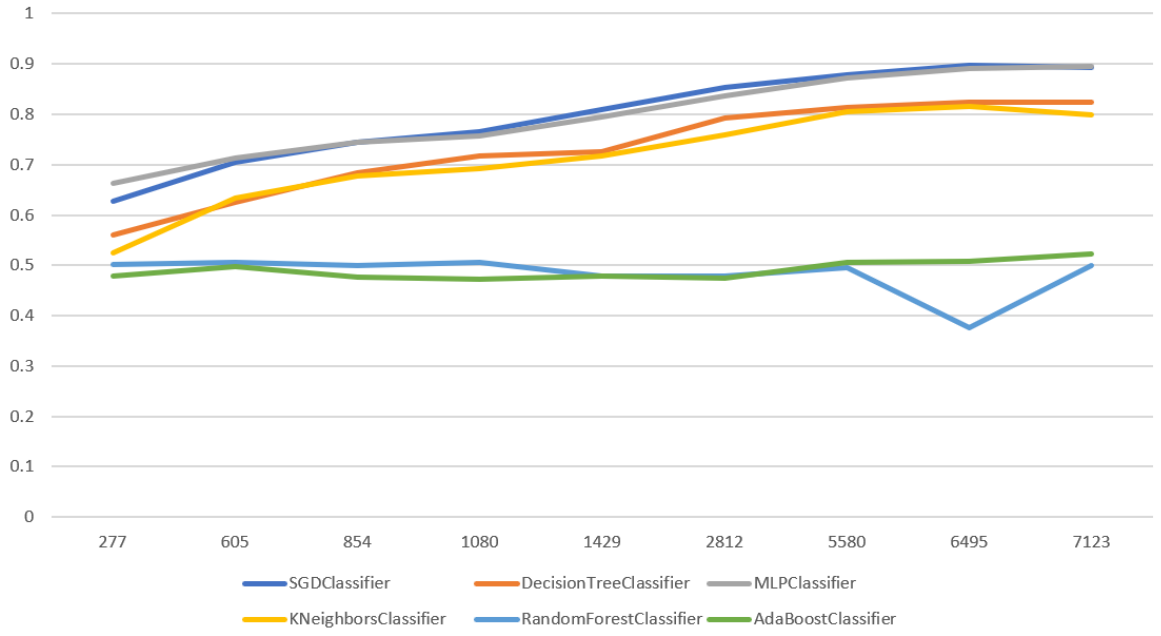


Fig. 2. Weighted F-score classifiers comparison

Client-server architecture. The task of the implementation of this work is to create the system that would provide accurate POS predictions for the user, but at the same time the goal of this work implies the facilitation for the linguists that would use it to create the Ukrainian text corpus.

It was decided to create the distributed system that would consist of the client and the server to provide the ability of using the tagger remotely. The Electron app was chosen as the client platform, as it can run on any operating system [9]. The server was written in Python same as the main learning application as it is efficient enough to handle the simple http requests.

As shown on the figure 3, the client is displaying the input field where the user can type any word combination or text he wants to tag and the “POS-tag” button that sends the request for tagging to the server. The server responses with the tagged words which get displayed in the application interface.

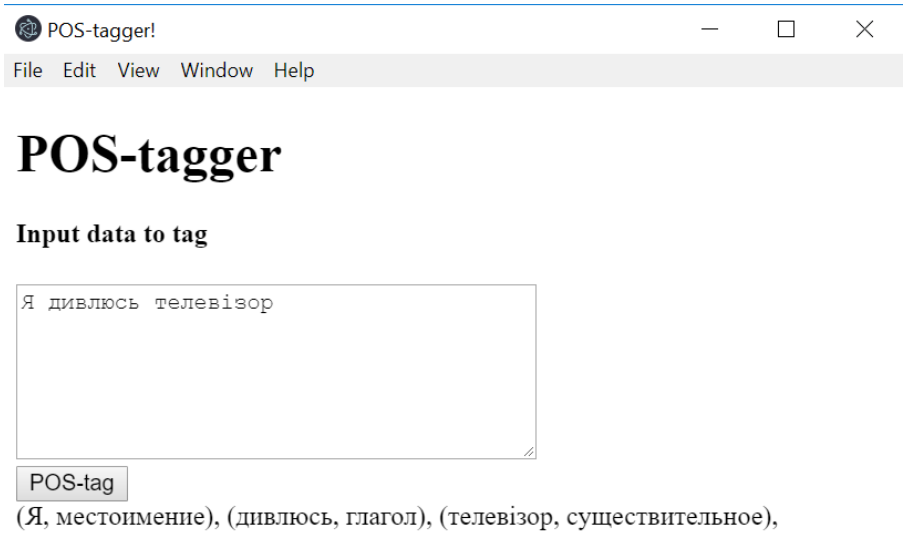


Fig. 3. Application interface

As the result of this work, training set was created, set of the class features was composed, classifier was chosen, trained and tested. The final and most efficient classifier is SGD classifier. The final tagger performance according to weighted F-score is 0.892 [10]. The client and the server are implemented for the client use.

Conclusions

The system that performs automatic markup of Ukrainian texts by parts of speech was designed, implemented and tested.

The main classification mechanism is based on supervised machine learning methods implemented in the de facto standard scikit-learn package. Effective use of the functions of this package involves the implementation of several research procedures.

In particular, for the implementation of the system, the search for the optimal set of class features and their construction from the training set was conducted. Also, the performance of various classification models was analyzed and the optimal classification model was selected, which turned out to be the SGD classifier. To obtain a high generalizing ability of the classifier, the K-block cross-validation technique was used.

The implemented POS tagger allows users to POS-tag large amounts of information in a short time and with high efficiency. Thus, the presented tagger can be used to create a corpus of the Ukrainian language, which will provide linguists with additional opportunities to study the Ukrainian language.

To improve the classification quality indicators, it seems promising to include contextual information in the feature space, consisting of information about tags of neighboring words.

References

1. Корпус української мови. URL: http://www.mova.info/syntaxis_search.aspx.
2. Проект створення корпусів текстів.Національний університет «Острозька академія» URL: https://www.oa.edu.ua/ua/departments/filologist/filol_literature/lexilab/project3.
3. Кочерган М.П. Вступ до мовознавства. К.: Академія, 2001. 368 с.
4. Manning C., Schütze H. Foundations of Statistical Natural Language Processing, Cambridge, MA: MIT Press, 1999. 717 p.
5. Zheng A., Casari A. Feature Engineering for Machine Learning. O'Reilly Media. 2018. 456 p.
6. Indurkhya N., Damerau F.J. Handbook of Natural Language Processing. Chapman and Hall. 2010. 702 p.
7. Scikit-learn: machine learning in Python – scikit-learn 0.23.2 documentation. URL: https://scikit-learn.org.
8. Refaeilzadeh P., Tang L., Liu H. Cross-Validation. Encyclopedia of Database Systems. Springer, 2009. P. 532-538.
9. Build cross-platform desktop apps with JavaScript, HTML, and CSS. URL: https://www.electronjs.org
10. Sokolova M., Japkowicz N., Szpakowicz S. Beyond Accuracy, F-Score and ROC: A Family of Discriminant Measures for Performance Evaluation. *Advances in Artificial Intelligence, Lecture Notes in Computer Science*. 2006. V.4304. P. 1015-1021.

РОЗРОБКА ПРОГРАМНОЇ ПІДТРИМКИ ДЛЯ СТВОРЕННЯ КОРПУСУ УКРАЇНСЬКОЇ МОВИ І ЙОГО ВИКОРИСТАННЯ

О.І. Керпель, В.Г. Пенко

Одеський національний університет ім. І.І.Мечникова,
вул. Дворянська, 2, Одеса, 65000, Україна; e-mail: alexeykerpel15@gmail.com, vpenko@onu.edu.ua

Актуальність роботи полягає в необхідності аналізу українських текстів з метою вивчення української мови і нестачі відповідних інформаційних і програмних ресурсів. Об'єкт дослідження - засоби складання POS-тегованих корпусів українських текстів. Предмет дослідження - процес розробки програмних засобів для створення корпусів українських текстів, зокрема, алгоритмів POS тегування. Мета роботи - дослідження і розробка програмних засобів для створення анотованого корпусу української мови. Для досягнення поставленої мети були вирішені наступні завдання: аналіз предметної області; вибір відповідних підходів і програмних засобів; створення навчальної множини; реалізація системи; навчання системи; тестування системи. Спроектовано та реалізовано підхід до генерації навчальної вибірки. Підхід заснований на використанні вже реалізованого тегера російської мови і схожості морфологічної будови слів російської та української мови. Для підвищення ефективності класифікації проведений пошук вдалої комбінації простору ознак і навчального алгоритму. Найбільш вдалими моделями машинного навчання для даного завдання виявилися стохастичний градієнтний спуск і дерева прийняття рішень. Для досягнення прийнятного рівня

узагальнення використана перехресна перевірка. В результаті проведеної роботи було отримано навчений тегер української мови, який для вибірки літературних українських текстів забезпечує якість класифікації на рівні 0.892 по зваженій F-мірі. Реалізовано розподілений додаток з клієнт-серверною архітектурою, що дозволяє клієнтам здійснювати тегування власних текстів. При регулярному використанні цього додатку експертами-лінгвістами використану навчальну множину може бути покращено, що дозволить отримувати більш високі показники класифікації, що здійснює тегер.
Ключові слова: POS-тегування, корпус текстів, алгоритми машинного навчання, простір ознак.

РАЗРАБОТКА ПРОГРАММНОЙ ПОДДЕРЖКИ ДЛЯ СОЗДАНИЯ КОРПУСА УКРАИНСКОГО ЯЗЫКА И ЕГО ИСПОЛЬЗОВАНИЯ

А.И. Керпель, В.Г. Пенко

Одесский национальный университет им. И.И.Мечникова,
ул. Дворянская, 2, Одесса, 65000, Украина; e-mail: alexeykerpel15@gmail.com,
vpenko@onu.edu.ua

Актуальность работы заключается в необходимости анализа украинских текстов с целью изучения украинского языка и недостатке соответствующих информационных и программных ресурсов. Объект исследования – средства составления POS-тегированных корпусов украинских текстов. Предмет исследования – процесс создания программных средств для создания корпусов украинских текстов, в частности, алгоритмов POS тегирования. Цель работы – исследование и разработка программных средств для создания аннотированного корпуса украинского языка. Для достижения поставленной цели были решены следующие задачи: анализ предметной области; выбор подходящих подходов и программных средств; создание обучающего множества; реализация системы; обучение системы; тестирование системы. Спроектирован и реализован подход к генерации обучающей выборки. Подход основан на использовании уже реализованного теггера русского языка и сходстве морфологического строения слов русского и украинского языка. Для повышения эффективности классификации произведен поиск эффективной комбинации признакового пространства и обучающего алгоритма. Наиболее удачными моделями машинного обучения для данной задачи оказались стохастический градиент спуск и деревья принятия решений. Для достижения приемлемого уровня обобщения использована перекрестная проверка. В результате проведеной работы был получен обученный теггер украинского языка, который для выборки литературных украинских текстов обеспечивает качество классификации на уровне 0.892 по взвешенной F-мере. Реализовано распределенное приложение с клиент-серверной архитектурой, позволяющей клиентам осуществлять тегтрование собственных текстов. При регулярном использовании данного приложения экспертами-лингвистами использованное обучающее множество может быть улучшено, что позволит получать более высокие показатели классификации, осуществляемой теггером.
Ключевые слова: POS-тегирование, корпус текстов, алгоритмы машинного обучения, пространство признаков.

DOI 10.15276/imms.v10.no1-2.31
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 31-44

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ НОРМОВАНОЇ ВІДОКРЕМЛЕНОСТІ МАКСИМАЛЬНОГО СИНГУЛЯРНОГО ЧИСЛА БЛОКУ МАТРИЦІ ЦИФРОВОГО ЗОБРАЖЕННЯ

А.А. Кобозєва, І.І. Бобок

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

На сьогоднішній день одним з найпоширеніших і затребуваних стеганографічних методів є метод модифікації найменшого значущого біта - LSB-метод. Це залишає актуальними задачі виявлення наявності й декодування прихованої інформації, вбудованої в контейнер з використанням цього методу, зокрема в умовах малої пропускної спроможності прихованого каналу зв’язку. Існуючі стеганоаналітичні алгоритми, розроблені для LSB-методу, вирішують, як правило, основну задачу стеганоаналізу - детектування прихованого каналу зв'язку, залишаючи невирішеною задачу декодування (відновлення) додаткової інформації, для якої важливою складовою є визначення/оцінка пропускної спроможності прихованого каналу. *Метою* роботи є додаткові дослідження властивостей нормованої відокремленості максимального сингулярного числа блоків матриці оригінальних цифрових зображень, які розглядаються як контейнери, та побудованих на їх основі LSB-методом стеганоповідомлень, результати якого дадуть змогу для оцінки пропускної спроможності прихованого каналу зв’язку. В роботі досліджуються властивості дискретної функції $y(QF)$, яка визначає кількість блоків зображення, в яких відбувається збільшення нормованої відокремленості максимального сингулярного числа в результаті перезбереження зображення в формат з втратами з коефіцієнтом якості QF. Виявлені особливості зміни функції $y(QF)$ при стеганоперетворенні досліджуваного зображення в залежності від того, контейнером чи стеганоповідомленням воно є; досліджені властивості $y(QF)$ залежно від формату цифрового зображення та коефіцієнта якості для зображення в форматі з втратами, від величини пропускної спроможності прихованого каналу зв’язку, при одноразовому та дворазовому стеганоперетворенні. В результаті проведених досліджень отримані однобічні (зверху) оцінки величини пропускної спроможності прихованого каналу зв’язку, побудованого за допомогою LSB-методу на основі контейнера в форматі з втратами.

Ключові слова: стеганоаналітичний метод, цифрове зображення, пропускна спроможність прихованого каналу, LSB-метод, нормована відокремленість сингулярного числа.

Вступ

Стеганографія сьогодні – один з наймогутніших і широко використовуваних напрямів в області захисту інформації. Стеганографічні системи дають можливість приховати сам факт наявності секретної інформації шляхом організації прихованого каналу зв'язку всередині каналу загального користування. Одним з основних питань тут є питання про те, у чиїх руках перебуває такий потужний засіб захисту, оскільки використання стеганографії, на жаль, може приводити до прихованої комунікації, цілі якої є антидержавними, протизаконними, антигуманними [1,2]. У таких випадках критично важливим є якнайшвидше виявлення прихованої комунікації, що має місце. Основною «зброєю» для цього є стеганоаналіз [3]. Потужні зусилля вчених усього світу спрямовані сьогодні на розв'язок основної задачі стеганоаналізу – виявлення наявності прихованої (додаткової) інформації (ДІ) в інформаційному контенті [4], однак в умовах інформаційного протиборства, яке має місце в сучасному світі [2], цього виявляється

недостатньо. Лише декодування прихованої інформації, її відновлення дозволить повністю досягти мету стеганоаналізу. Задача витягу прихованої інформації, її декодування є найбільш складною, розв'язку якої сприяє визначення/оцінка пропускної спроможності організованого стеганографічного каналу зв'язку [3,5], на забезпечення чого й спрямована дана робота.

Аналіз досліджень та публікацій

На сьогоднішній день одним з найпоширеніших і затребуваних стеганографічних методів залишається метод модифікації найменшого значущого біта (LSB-метод) [3], хоча останнім часом його використання має певні нетипові особливості – малу пропускну спроможність прихованого каналу зв'язку (ПСПК), що організується (≤0.1 біт/піксель), на яку, як правило, не розраховані існуючі стеганоаналітичні методи, що залишає актуальною задачу виявлення наявності прихованої інформації, вбудованої з використанням LSB-методу. Крім того, сучасні стеганоаналітичні методи, як правило, не визначають/не оцінюють ПСПК, що є важливою складовою процесу декодування (відновлення) додаткової інформації. Так в [6] запропонований метод виявлення LSB-вкладень в цифровому зображенні (ЦЗ), заснований на врахуванні значення кореляції між довжиною додаткової інформації й регресією кількості ідентичних по яскравості пікселів, при цьому кожний піксель ЦЗ аналізується окремо. Цей метод дає можливість для використання нової стеганоаналітичної функції для виміру подібності між вагою пікселів, що, як стверджують автори, дозволяє забезпечити значну чутливість стеганоаналізатора. Однак метод не є дієздатним при ПСПК менше, ніж 0.125 біт/піксель, як і метод, запропонований в [7]. Для методу, розробленого в [8], нижня межа ПСПК склала лише 0.1 біт/піксель. Оцінка ПСПК в жодному методі не відбувається.

В [9] був запропонований стеганоаналітичний метод, орієнтований на виявлення прихованого каналу зв’язку з малою пропускною спроможністю, заснований на властивостях нормованої відокремленості максимального сингулярного числа (НВМСЧ) блоку матриці зображення, а саме на врахуванні кількості блоків досліджуваного ЦЗ, отриманих шляхом стандартної розбивки матриці [10], в яких збільшується НВМСЧ в результаті перезбереження ЦЗ в формат з втратами з різними коефіцієнтами якості *QF*. Цю кількість відображала дискретна функція $y(QF)$ ($QF \in \{1,2,...,100\}$ для формату Jpeg, $QF \in \{1,2,...,20\}$ для формату Jpeg2000), яка будувалась для ЦЗ, що піддавалось експертизі.

Якщо позначити через *F* матрицю ЦЗ, яка в процесі аналізу розбивається стандартним чином на непересічні $l \times l$-блоки з сингулярними числами (СНЧ) [11]

$$\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0, \tag{1}$$

які утворюють вектор $\sigma = (\sigma_1, \sigma_2, ..., \sigma_l)^T$, то нормований вектор СНЧ $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, ..., \bar{\sigma}_l)^T$ визначиться як $\bar{\sigma} = \sigma / \|\sigma\|$, де $\|\sigma\|$ норма вектора σ. Тоді нормована відокремленість СНЧ $\sigma_i, i = \overline{1,l}$, визначається наступним чином [9]:

$$svdgap_n(i) = \min_{i \neq j} \left| \bar{\sigma}_j - \bar{\sigma}_i \right|. \tag{2}$$

З (2) з урахуванням (1) випливає, що НВМСЧ – це

$$svdgap_n(1) = \bar{\sigma}_1 - \bar{\sigma}_2,$$

при цьому $0 < svdgap_n(1) \le 1$.

Алгоритмічна реалізація запропонованого в [9] методу виявилася такою, що перевищує по ефективності виявлення наявності прихованого каналу зв'язку сучасні аналоги в умовах малої ПСПК, тобто математичний базис методу, заснований на властивостях НВМСЧ та дискретної функції $y(QF)$, забезпечує чутливість до малих збурень контейнера в процесі стеганоперетворення, а тому може вважатися перспективним для використання з метою розв'язку задачі визначення/оцінки пропускної спроможності прихованого каналу, яка є важливою для процесу декодування ДІ, але в методі, запропонованому в [9], не передбачена. Для забезпечення можливості визначення/оцінки ПСПК необхідні додаткові дослідження властивостей НВМСЧ блоків ЦЗ та функції $y(QF)$.

Мета і задачі дослідження

Метою роботи є подальше дослідження властивостей НВМСЧ блоків та функції $y(QF)$ оригінальних ЦЗ та побудованих на їх основі стеганоповідомлень, результати якого будуть корисними для оцінки ПСПК, сформованого за допомогою LSB-методу.

Для досягнення мети в роботі розв'язуються наступні *задачі*:

- виявити особливості зміни дискретної функції $y(QF)$ при стеганоперетворенні досліджуваного ЦЗ в залежності від того, контейнером чи стеганоповідомленням воно є;
- дослідити властивості функції $y(QF)$ залежно від формату ЦЗ та коефіцієнта якості для зображення в форматі з втратами;
- дослідити властивості функції $y(QF)$ залежно від величини ПСПК;
- дослідити властивості функції $y(QF)$ при одноразовому та дворазовому стеганоперетворенні за допомогою LSB-методу.

Основна частина

В [9] основною ознакою для виявлення стеганоповідомлення (СП), сформованного на основі ЦЗ-контейнера, що зберігалося в форматі з втратами, було порушення монотонності дискретної функції $y(QF)$, значення якої визначаються кількістю блоків досліджуваного зображення, в яких збільшується НВМСЧ при перезбереженні з втратами з коефіцієнтом якості *QF*. При цьому перезбереження оригінального ЦЗ в форматі без втрат приводило до монотонно спадаючої функції $y(QF)$.

Нехай є оригінальне Jpeg-ЦЗ, збережене з коефіцієнтом якості QF_1. Згадану вище дискретну функцію для оригінального зображення позначимо $y_0(QF)$. Вона не тільки не є монотонною, але в точці $QF = QF_1$, як правило, буде мати локальний мінімум [9].

Параметри й вид кривої, що є графіком $y_0(QF)$, для оригінальних ЦЗ в форматі з втратами з коефіцієнтом якості QF_1 буде залежати від QF_1: чим менше QF_1, тем нижче вздовж осі ординат буде розташована крива $y_0(QF)$ в координатній площині (рис.1), хоча для значних *QF* (для формата Jpeg для *QF*>75), використовуваних при перезбереженні ЦЗ в ході експертизи, ця картина може порушуватися. Дійсно, чим нижче коефіцієнт якості оригінального ЦЗ, тем менше його високочастотна

складова [10], тим більша кількість СНЧ блоків будуть порівнянні з нулем [12], тим більше в таких блоках оригінального ЦЗ буде НВМСЧ, тим у меншій кількості блоків вона збільшиться при перезбереженні у формат із втратами. Коли при перезбереженні в ході експертизи будуть використовуватися значні коефіцієнти якості (*QF*>75), кількість блоків, у яких відбувається збільшення НВМСЧ, різко знижується (через зменшення елементів матриці квантування [10]), і тут уже значну роль будуть відігравати обчислювальні похибки в процесі округлень до цілих значень частотних коефіцієнтів після квантування. Це приводить до деякого «змішання» кривих $y_0(QF)$ в області *QF*>75, що ілюструє рисунок 1.

Раніше показано [12], що при стеганоперетворенні Jpeg-контейнера за допомогою методу модифікації найменшого значущого біта властивості СНЧ блоків ЦЗ із втратами починають «прямувати» до властивостей СНЧ блоків ЦЗ без втрат, зокрема, зростає швидкість зміни найменших СНЧ, мінімальні СНЧ, які в блоці оригінального ЦЗ порівнянні з нулем, після вбудови ДІ вже такими не будуть, причому, чим більше буде ПСПК, за допомогою якої отримано СП, тим більше зростуть значення найменших СНЧ блоків матриці контейнера та швидкість їх зміни. Взагалі існують стеганографічні методи, які в результаті вбудови ДІ дають стеганоповідомлення, матриця якого практично не відрізняється від матриці оригінального відповідного ЦЗ у форматі без втрат [13]. При цьому відповідними будемо називати такі ЦЗ, які відрізняються лише форматом (з/без втрат) збереження [9]. Поведінка функції $y(QF)$ змінюється аналогічним чином: чим більше ПСПК, тим «ближче» крива $y(QF)$ для СП, сформованого на основі контейнера в форматі з втратами, до $y(QF)$ для відповідного оригінального ЦЗ у форматі без втрат, тобто чим більше ПСПК, тим вище вздовж осі ординат крива $y(QF)$ на координатній площині для відповідного СП, тим менше відмінність між значеннями відповідних функцій для СП і «чистого» відповідного ЦЗ без втрат, що проілюстровано на рисунку 2 для оригінального ЦЗ в форматі Jpeg, отриманого з *QF*=75. Зауважимо, що із зростанням ПСПК для функції $y(QF)$ локальний мінімум в *QF*=75 стає все менш вираженим (рис.2). Для деяких ЦЗ він взагалі може стати відсутнім.

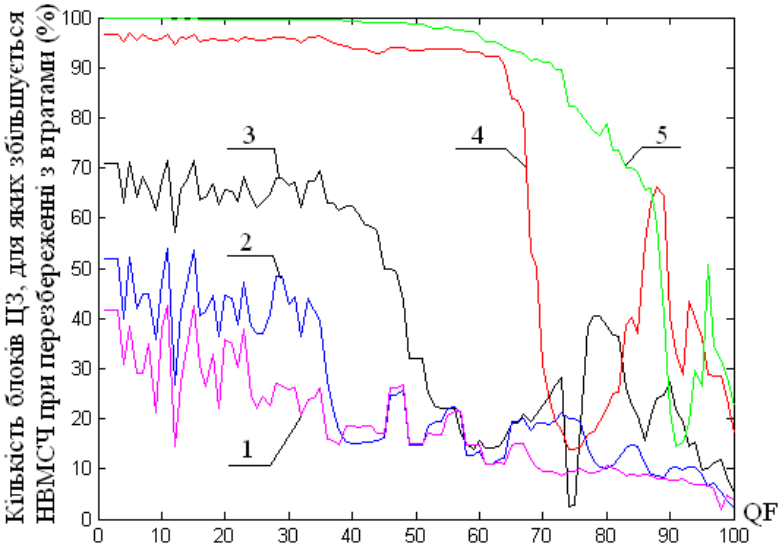


Рис. 1. Графіки функції $y(QF)$ для оригінальних ЦЗ в форматі Jpeg з коефіцієнтом якості *QF*, який дорівнює: 1 – 55; 2 – 65; 3 – 75; 4 – 85; 5 – 95

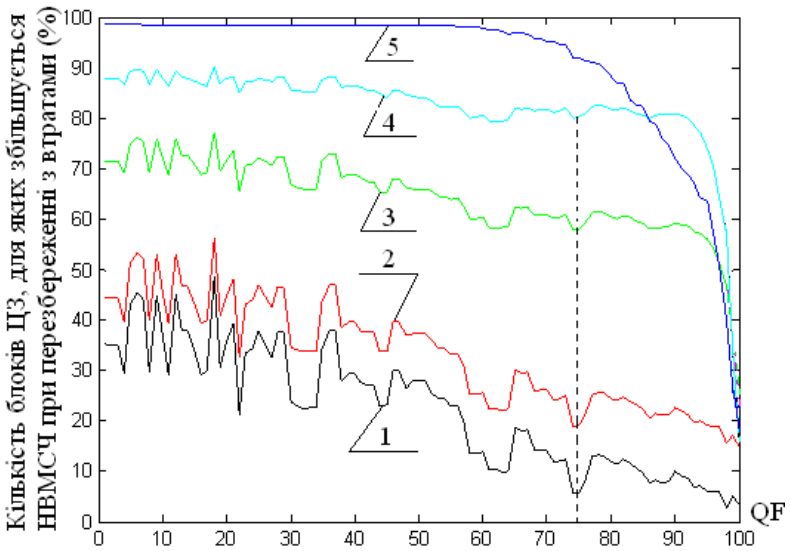


Рис. 2. Зміна властивостей $y(QF)$ залежно від ПСПК, яка використовується при отриманні стеганоповідомлення: 1 – оригінальне ЦЗ-контейнер в форматі Jpeg (*QF*=75); 2 – СП з ПСПК=1%; 3 – СП з ПСПК=5%; 4 – ПСПК=10%; 5 – оригінальне відповідне ЦЗ без втрат

Описані зміни СНЧ при вбудові ДІ в контейнер у форматі із втратами приведуть до збільшення кута між нормованим вектором СНЧ $\bar{\sigma}$ $l \times l$-блоку і першим вектором e_1 стандартного базису простору R^l, у порівнянні з кутом в оригінальному Jpeg-ЦЗ, тобто НВМСЧ у більшості блоків стеганоповідомлення буде не більше, чим у блоках контейнера. Якщо тепер перезберігати із втратами контейнер і СП, то кількість блоків, у яких буде збільшуватися НВМСЧ, у СП буде більше, чим у контейнері для одного *QF*, оскільки в загальному випадку можна стверджувати, що чим менше НВМСЧ у блоці ЦЗ, тим більше ймовірність її збільшення при перезбереженні зображення із втратами, тому що збереження із втратами в більшості блоків збільшує НВМСЧ [9].

Нехай ДІ вбудовується в ЦЗ-контейнер у форматі без втрат. У цьому випадку якісні зміни СНЧ, що відбуваються в блоках матриці контейнера, передбачити складно, вони не будуть тут настільки явними, оскільки тут немає таких характерних рис СНЧ, як для ЦЗ у форматі із втратами, зокрема, порівнянності з нулем найменших СНЧ блоків. Хоча при вбудові ДІ й тут збільшується кількість блоків при перезбереженні СП у формат з втратами, у порівнянні з перезбереженням контейнера, тобто графік $y(QF)$ для СП буде вище вздовж осі ординат, ніж $y(QF)$ для контейнера. Дійсно, у загальному випадку вбудова LSB-методом ДІ, яка розглядається як випадково сформована матриця відповідного зображенню розміру, елементи якої належать множині $\{-1,0,1\}$, не зменшує високочастотну складову ЦЗ [10], тобто приводить до незбільшення, а на практиці до зменшення НВМСЧ. Тому кількість блоків у ЦЗ-СП, для яких зросте НВМСЧ при перезбереженні із втратами з коефіцієнтом якості *QF*, буде більше, чим у ЦЗ-контейнера при перезбереженні з тим самим *QF*. Виключення тут може становити перезбереження з $QF \approx 100$. Якщо $QF \approx 100$, то кількості блоків, для яких збільшиться НВМСЧ при перезбереженні із втратами, і ЦЗ-СП, і ЦЗ-контейнера у форматі без втрат, будуть незначними й такими, що практично не відрізняються одна від іншої (що є наслідком використовуваних для таких коефіцієнтів якості *QF* матриць квантування, що мають незначні елементи [10]) (рис.3).

Таким чином, встановлено, що крива $y(QF)$ для контейнера завжди нижче вздовж осі ординат на координатній площині, ніж для СП, сформованого на його основі, тобто кількість блоків ЦЗ-СП, для яких зросте НВМСЧ при перезбереженні з

втратами, є більшою, ніж у ЦЗ-контейнері, незалежно від формату (з/без втрат) контейнера.

Зауважимо, що оскільки LSB-метод є нестійким до атак проти вбудованого повідомлення, зокрема, до стиску із втратами, то стеганоповідомлення, як правило, буде зберігатися у форматі без втрат.

Нехай розглядається ЦЗ, що формально збережене у форматі без втрат. Це може бути: оригінальне ЦЗ; СП, яке сформовано на основі контейнера у форматі з втратами й збережене без втрат; СП, сформоване на основі контейнера без втрат, збережене без втрат. Будемо припускати, що СП формуються в умовах малої ПСПК, а саме: ПСПК $\leq 10\%$. Побудувавши для досліджуваного ЦЗ функцію $y(QF)$, можна відокремити оригінальне ЦЗ у форматі без втрат або СП, побудоване на основі контейнера без втрат, від ЦЗ, яке зазнало перезбереження з формату із втратами у формат без втрат (з/без стеганоперетворення), досліджуючи монотонність $y(QF)$ [9].

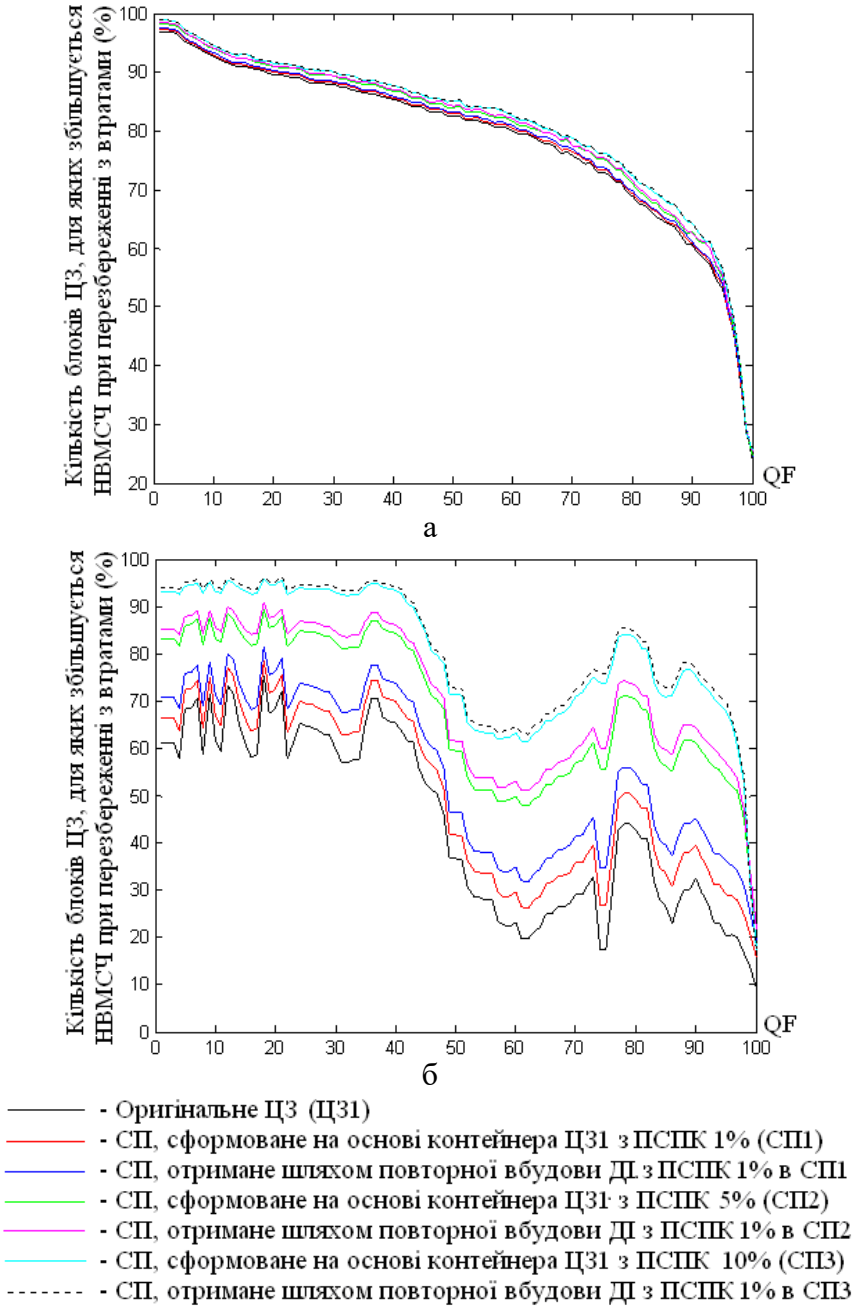


Рис. 3. Графіки функції $y(QF)$: а – ЦЗ без втрат, б – ЦЗ з втратами (Jpeg (QF=75))

Однак наступні задачі залишаються тут невирішеними:

- відокремити спочатку збережене у форматі із втратами цз, що піддалося стеганоперетворенню, від такого, яке не зазнало вбудову ді, а просто було перезбережено у формат без втрат;
- відокремити оригінальне цз без втрат від сп, побудованого на основі контейнера без втрат.

Розглянемо в даній роботі детально задачу 1. Нехай ЦЗ спочатку зберігалися в форматі з втратами; F_1 – матриця ЦЗ, яке піддається експертизі. Формально воно збережено в форматі без втрат. Якщо F_1 – це СП, то будемо вважати, що воно отримане на основі Jpeg-контейнера з матрицею F. Піддамо F_1 стеганоперетворенню з малою ПСПК (наприклад, 1%), формальним відображенням якого є співвідношення [14]:

$$F_{1,1} = F_1 + \Delta F, \tag{3}$$

де ΔF – матричне представлення ДІ, $F_{1,1}$ – матриця ЦЗ-СП. Визначимо функції $y\left(QF\right)$ для F_1 і $F_{1,1}$, перезберігаючи їх з втратами з усіма можливими значеннями коефіцієнта якості QF. З вищенаведеного випливає, що для конкретного QF, як правило, значення $y\left(QF\right)$ для $F_{1,1}$ буде більше, ніж для F_1, що геометрично відобразиться в тому, що графік $y\left(QF\right)$ для $F_{1,1}$ буде вище вздовж осі ординат, ніж графік $y\left(QF\right)$ для F_1, незалежно від того, СП чи контейнеру відповідає матриця F_1. Однак відмінність між значеннями функції $y\left(QF\right)$ (між відповідними графіками) буде різною залежно від того, оригінальному ЦЗ чи СП відповідає матриця F_1.

Нехай F_1 – матриця контейнера, тоді стеганоперетворення (3) для нього буде першим і єдиним. Якщо F_1 відповідає СП, то для нього (3) – повторне стеганоперетворення. Покажемо, що первинне перетворення (3) за допомогою матриці ΔF «підніме» графік функції $y\left(QF\right)$ вздовж осі ординат відносно побудованого для F_1 більше, ніж повторне перетворення за допомогою тієї ж матриці ΔF.

Стеганоперетворення Jpeg-контейнера, як згадано вище, практично завжди приводить до збільшення найменших СНЧ (оскільки від'ємними вони стати не можуть у силу (1), а до вбудови ДІ є порівнянними з нулем), зменшення НВМСЧ у блоках, задіяних у стеганоперетворенні, збільшуючи тим самим імовірність зростання НВМСЧ при перезбереженні ЦЗ у формат із втратами. Якщо ж вбудова ДІ відбувається в ЦЗ-СП, то там вже НВМСЧ у блоках, задіяних у первинному стеганоперетворенні, менше, ніж в відповідних блоках оригінального контейнеру. Після вбудови ДІ в СП найменші СНЧ відповідних блоків, задіяних у повторному стеганоперетворенні, які вже не порівнянні з нулем у тих блоках, що були задіяні в первинному стеганоперетворенні, можуть як зменшитися, так і збільшитися, що може привести як до збільшення, так і до зменшення НВМСЧ. Повторна вбудова ДІ в СП у загальному випадку збільшить результуючу ПСПК, додатково збурюючи СНЧ, але відносна зміна найменших СНЧ блоків контейнера буде більше, ніж найменших СНЧ блоків СП при однаковій збурній дії. Таким чином, кількість блоків, у яких зросте НВМСЧ при перезбереженні із втратами СП, отриманого в результаті послідовного дворазового стеганоперетворення, хоча й буде більше, чим при перезбереженні первинного СП, але ступінь цього збільшення буде менше, ніж ступінь збільшення при такому ж (що характеризується матрицею ΔF), але первинному стеганоперетворенні щодо порожнього контейнера. Більше того, ступінь збільшення буде тим менше, чим більше ПСПК первинного стеганоперетворення. Дійсно, чим більше ПСПК первинного стеганоперетворення, тим більше кількість блоків контейнера, у яких зменшиться НВМСЧ у результаті

стеганоперетворення, тим менше НВМСЧ у блоках F_1, задіяних у стеганоперетворенні, тим «вище» буде графік функції $y\left(QF\right)$, отриманої при перезбереженні F_1 з втратами. При повторній вбудові ДІ в СП, сформоване з порівнянно значною первинною ПСПК, буде значна кількість блоків, де після повторного стеганоперетворення НВМСЧ збільшиться, а не зменшиться, у порівнянні із НВМСЧ у блоці вхідного СП, що приведе до того, що при перезбереженні СП, отриманого в результаті дворазового стеганоперетворення, хоча графік функції $y\left(QF\right)$ буде вище, ніж графік аналогічної функції для вхідного СП (отриманого в результаті однократного стеганоперетворення), але ця різниця буде тим менше, чим більше була ПСПК первинного стеганоперетворення, що практично підтверджується результатами обчислювального експерименту, докладно описаного нижче, наведеними в табл.1 (використані позначення введені нижче) і проілюстрованими на рис.3.

Описану вище картину, що полягає в тому, що чим більша ПСПК первинного стеганоперетворення, тим менше відмінність між відповідними функціями $y\left(QF\right)$ для СП, отриманих одноразовим і дворазовим стеганоперетворенням, складно відстежити для ЦЗ-контейнера у форматі без втрат, де це не буде вже так строго виконуватися, хоча для середніх по експерименту значень має місце (табл.1).

Таблиця 1.

Середні по експерименту значення $T_{i,1}$, $i \in \{0,1,5,10\}$

Множина, з якої обирався контейнер	$T_{0,1}$	$T_{1,1}$	$T_{5,1}$	$T_{10,1}$
M_{Tif}	1.95	1.90	1.82	1.68
$M_{Jpeg,70}$	60.44	51.40	26.14	12.19
$M_{Jpeg,75}$	46.16	39.54	20.81	10.08
$M_{Jpeg,80}$	33.12	28.29	15.49	8.16

Для цього є дві причини. По-перше, у блоках ЦЗ в форматі без втрат практично відсутні нульові/порівнянні з нулем СНЧ [15], внаслідок чого зміни, які відбуваються в ЦЗ без втрат при вбудові ДІ, можуть приводити як до зменшення, так і до збільшення СНЧ блоків, незалежно від їхнього порядкового номера. По-друге, кількість блоків, у яких відбувається збільшення НВМСЧ при перезбереженні у формат із втратами, при малих і середніх значеннях *QF* близько до 100% (див. рис.3). Зростання цієї кількості при вбудові ДІ в цьому випадку взагалі не може бути значним. Крім того, у силу малої зміни оцінюваної кількості блоків тут критичну роль відіграє накопичення обчислювальної похибки. У силу цього для більшості протестованих ЦЗ спостерігалося порушення монотонності для величини, що характеризує зміну значень дискретної функції $y\left(QF\right)$, із зростанням ПСПК первинного стеганоперетворення (табл.2), причому порушення монотонності могло спостерігатися на будь-якому кроці збільшення ПСПК первинного стеганоперетворення (рис.4 – тут ПСПК первинного стеганоперетворення вважається рівною 0 для ЦЗ-контейнера).

Таблиця 2.

Кількість ЦЗ, використаних у якості контейнерів, для яких порушувалася монотонна залежність відмінності між значеннями функцій $y\left(QF\right)$ для СП, отриманих одноразовим і дворазовим стеганоперетворенням, із зростанням ПСПК первинного стеганоперетворення (в % від загального числа ЦЗ в експерименті)

Формат ЦЗ-контейнера			
без втрат (Tif)	з втратами (Jpeg, QF=80)	з втратами (Jpeg, QF=75)	з втратами (Jpeg, QF=70)
84.7	6.3	3.8	2.5

Наведені таблиці 1, 2, рисунки 3, 4 частково відображають результати обчислювального експерименту, який підтверджує висновки, теоретично отримані вище. В обчислювальному експерименті були задіяні наступні множини ЦЗ: M_{Tif} – 500 ЦЗ в форматі без втрат (Tif) (150 ЦЗ з бази 4cam_auth [16], 275 ЦЗ з бази img_Nikon_D70s [17], 75 ЦЗ отриманих непрофесійною відеокамерою); $M_{Jpeg,70}$, $M_{Jpeg,75}$, $M_{Jpeg,80}$ – по 500 ЦЗ, отриманих з ЦЗ з множини M_{Tif} шляхом перезбереження у формат Jpeg з *QF*=70, 75, 80 відповідно (значення *QF* обрані як такі, що найбільш часто використовуються на практиці).

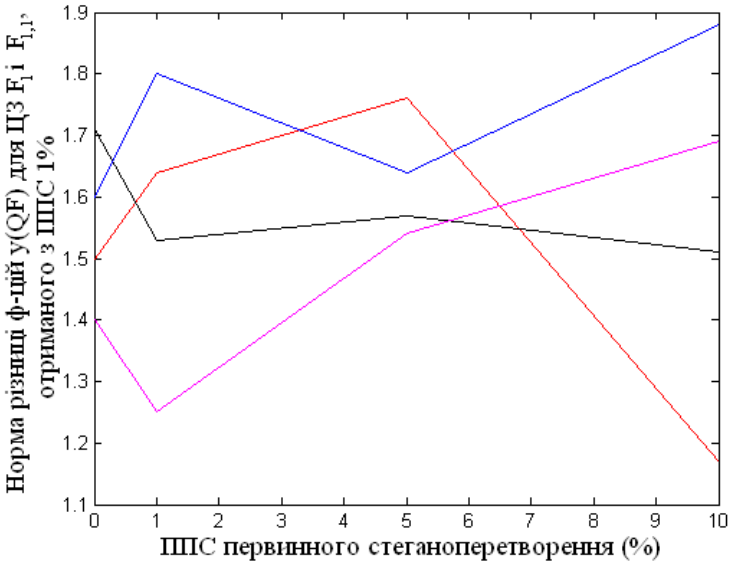


Рис. 4. Залежність для 4-х конкретних ЦЗ в форматі без втрат норми вектора різниці значень дискретних функцій $y\left(QF\right)$ для досліджуваного ЦЗ і ЦЗ, отриманого вбудовою ДІ з ПСПК=1% в досліджуване, від ПСПК первинного стеганоперетворення

На першому етапі в оригінальне ЦЗ (з втратами або без втрат) вбудовувалася ДІ з ПСПК 1, 5, 10%. Оригінальне ЦЗ-контейнер і отримані СП перезберігалися у формат із втратами (Jpeg) з усіма коефіцієнтами якості $QF \in \{1,2,...100\}$. В результаті визначалися дискретні функції $y_0(QF)$ (для контейнера), $y_1(QF)$, $y_5(QF)$, $y_{10}(QF)$, $QF \in \{1,2,...100\}$ для СП відповідно, що визначають для кожного $QF \in \{1,2,...100\}$ кількість блоків ЦЗ, для яких зростає НВМСЧ у результаті перезбереження у формат із втратами з коефіцієнтом якості *QF*. У якості кількісної характеристики змінення ЦЗ в результаті первинного стеганоперетворення розглядалася величина, що характеризує змінення функції $y_0(QF)$:

$$T_{0,i} = \left(\sum_{1}^{100} \left| y_0(QF) - y_i(QF) \right|^2 \right)^{\frac{1}{2}}, \quad i \in \{1,5,10\}. \tag{4}$$

Співвідношення (4) являє собою евклідову норма вектора різниці векторів значень функцій $y_0(QF)$ і $y_1(QF)/y_5(QF)/y_{10}(QF)$ в відповідних аргументах.

На другому етапі в сформовані на першому етапі СП повторно вбудовувалася ДІ з ПСПК=1% (матриця ДІ ΔF тут формувалася випадковим чином і використовувалася одна й та сама для СП з ПСПК 1, 5, 10%, сформованих на основі одного контейнера). Отримані після повторного стеганоперетворення СП перезберігалися із втратами (формат Jpeg) з $QF \in \{1,2,...100\}$. У результаті були отримані дискретні функції $y_{1,1}(QF)$, $y_{5,1}(QF)$, $y_{10,1}(QF)$, $QF \in \{1,2,...100\}$ для СП з ПСПК первинного стеганоперетворення 1, 5, 10% відповідно. У якості кількісної характеристики зміни ЦЗ-СП після повторного стеганоперетворення за аналогією з (4) розглядалася величина:

$$T_{i,1} = \left(\sum_{1}^{100} \left| y_i(QF) - y_{i,1}(QF) \right|^2 \right)^{\frac{1}{2}}, \quad i \in \{1,5,10\}. \tag{5}$$

Результати експерименту для оригінальних ЦЗ у форматі з втратами, крім таблиць і рисунків, наведених вище, знайшли своє відображення для випадку формату Jpeg з коефіцієнтом якості *QF*=75 на рис.5 і в табл.3, де наочно виражена загальна тенденція якісної зміни значень оцінок (4), (5) із зростанням ПСПК первинного стеганоперетворення зображення: зменшення моди гістограми значень $T_{i,1}$ з одночасним збільшенням значення в моді; зменшення довжини інтервалу можливих значень $T_{i,1}$ за рахунок зменшення максимального значення $T_{i,1}$. Отримані якісні результати є типовими для ЦЗ в форматі з втратами, незалежно від конкретики формату (Jpeg) та використаного коефіцієнта якості (*QF*=75), оскільки базуються на отриманих в роботі теоретичних висновках і підтверджують їх. Використання іншого формату з втратами (наприклад, Jpeg2000) чи іншого коефіцієнту якості змінить лише кількісні показники гістограм.

Таблиця 3.

Максимальні й мінімальні по експерименту значення $T_{i,1}$, $i \in \{0,1,5,10\}$ для ЦЗ-контейнерів, спочатку збережених в форматі Jpeg з *QF*=75

$T_{0,1}$		$T_{1,1}$		$T_{5,1}$		$T_{10,1}$	
макс.	мін.	макс.	мін.	макс.	мін.	макс.	мін.
146	2.1	124	2.4	61	1.7	26	2

Аналіз числових значень величин (4), (5) з використанням отриманих гістограм (рис.5) дозволяє зробити висновки, важливі для оцінки величини ПСПК, де використовувалося у якості контейнера ЦЗ у форматі Jpeg (*QF*=75):

- якщо для досліджуваного ЦЗ значення $T_{i,1} \geq 125$, то воно не зазнавало стеганоперетворення;
- якщо $61 < T_{i,1}$, то для аналізованого ЦЗ ПСПК<5%, у тому числі ЦЗ може бути «чистим» контейнером;

- якщо $26 < T_{i,1}$, то для аналізованого ЦЗ ПСПК<10%.

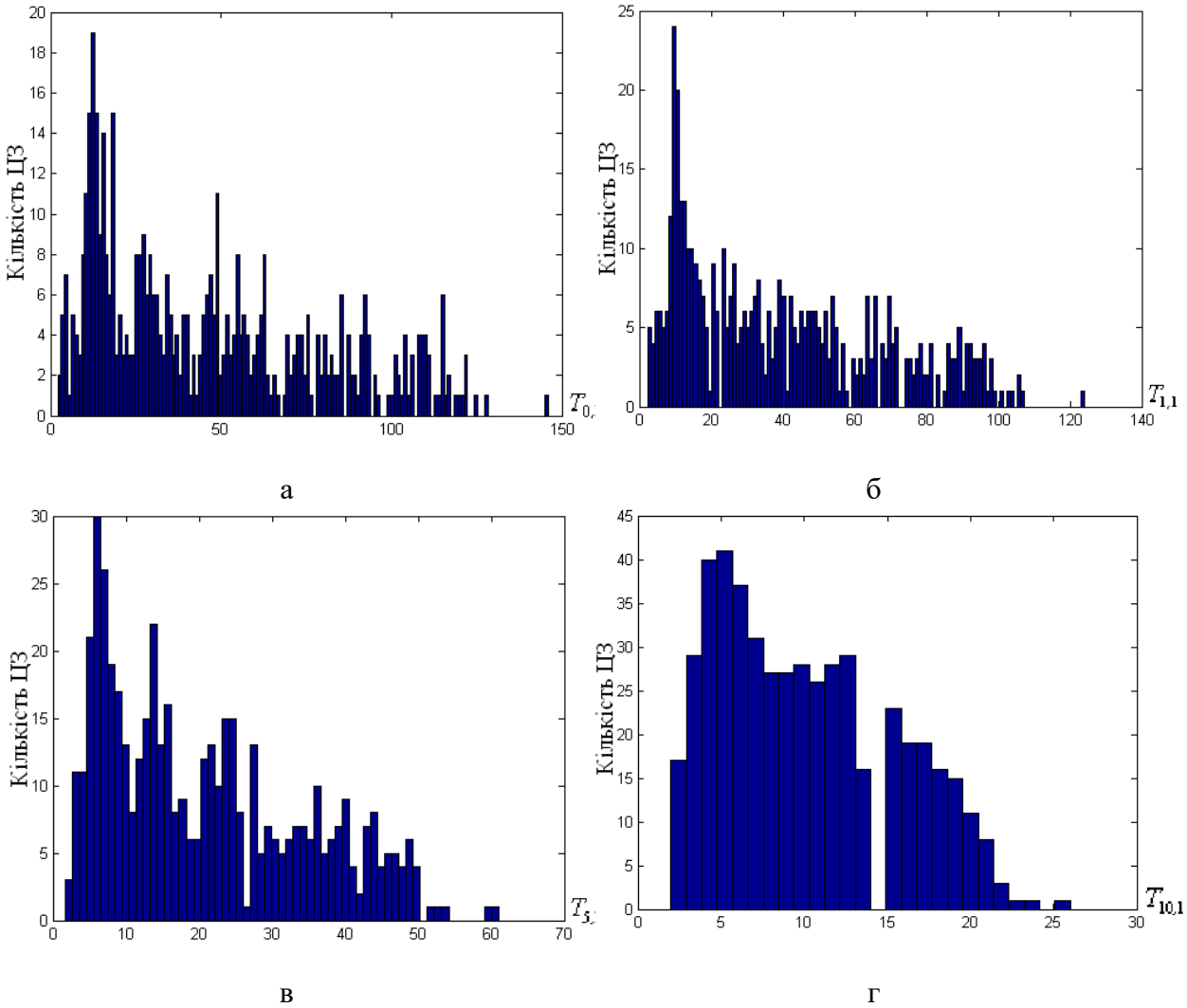


Рис. 5. Гістограми значень $T_{i,1}$, $i \in \{0,1,5,10\}$, для оригінального ЦЗ-контейнера, збереженого у форматі Jpeg з QF=75: а – $T_{0,1}$ (мода дорівнює 13, значення в моді 19); б – $T_{1,1}$ (мода 10, значення в моді 24); в – $T_{5,1}$ (мода 6, значення в моді 30); г – $T_{10,1}$ (мода 5, значення в моді 41)

Отримані результати на даному етапі досліджень не є остаточними, отримані для ПСПК кількісні оцінки є однобічні (оцінки зверху), такі, що залежать від величини ПСПК первинного стеганоперетворення ЦЗ в форматі Jpeg (QF=75). Розширюючи обчислювальний експеримент, збільшуючи різноманітність значень ПСПК для первинного стеганоперетворення (наприклад, від 1 до K% з кроком h%), отримані результати можна уточнити, що буде зроблено при розробці безпосередньо методу оцінки ПСПК. Використання іншого формату з втратами (наприклад, Jpeg2000) чи іншого коефіцієнту якості QF змінить кількісні показники гістограм, тому розробка методу потребує отримання кількісних характеристик для всіх можливих (самих використовуваних) значень коефіцієнта якості. Враховуючи їх можливу різноманітність, необхідним попереднім кроком перед використанням методу оцінки ПСПК повинен бути крок визначення QF для контейнера в форматі з втратами, що можливо зробити за допомогою, наприклад, методу, запропонованому в [18].

Висновки

У роботі проведені дослідження властивостей НВМСЧ блоків матриці ЦЗ, дискретної функції $y(QF)$, яка ставиться у відповідність ЦЗ в умовах його перезбереження із втратами з різними коефіцієнтами якості й відображає кількість блоків, у яких у результаті перезбереження збільшується НВМСЧ.

Встановлено теоретично й підтверджено практично шляхом обчислювального експерименту:

- чим більше коефіцієнт якості оригінального ЦЗ в форматі з втратами, тим більше значення функції $y(QF)$ для конкретного $QF \le 75$; установлені причини, по яких дане твердження може порушуватися для QF>75;
- чим більше ПСПК, що використовувалася для отримання СП, тим більше значення $y(QF)$ для конкретного QF, тобто, чим більше ПСПК, тим вище крива $y(QF)$ для відповідного СП, тим «ближче» графік функції $y(QF)$ для СП, сформованого на основі контейнера в форматі з втратами, до $y(QF)$ для відповідного оригінального ЦЗ у форматі без втрат;
- кількість блоків ЦЗ-СП, для яких зросте НВМСЧ при перезбереженні з втратами, є більшою, ніж у ЦЗ-контейнері незалежно від формату (з/без втрат) контейнера;
- первинне стеганоперетворення ЦЗ за допомогою матриці ΔF змінює («піднімає» графік) функцію $y(QF)$ більше, ніж повторне стеганоперетворення за допомогою тієї ж матриці ΔF;
- чим вище ПСПК первинного стеганоперетворення, тим менше відмінність між відповідними функціями $y(QF)$ для СП, отриманих шляхом одноразового й дворазового стеганоперетворення, при цьому для повторної вбудови ДІ використовується одна й та сама матриця ΔF незалежно від ПСПК первинного стеганоперетворення.

У результаті проведених досліджень отримані однобічні оцінки (зверху) величини ПСПК в умовах ЦЗ-контейнера в форматі Jpeg (QF=75). Проведені дослідження не є завершеними, але говорять про перспективність обраного шляху для оцінки величини ПСПК первинного стеганоперетворення ЦЗ і в даний час продовжуються авторами.

Список літератури

1. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures / W. Mazurczyk et al. Hoboken: Wiley, 2016. 296 p.
2. Информационное противоборство в современных условиях / Л.Г. Пирцхалава и др. К.: ЦП «Компринт», 2019. 226 с.
3. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский и др. М.: Вузовская книга, 2009. 220 с.
4. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications.* 2018. V.40. P. 217–235.
5. Метод оценки величины скрытой пропускной способности стеганографического канала связи. Информационные системы в управлении, образовании, промышленности: монография / под ред. В.С. Пономаренко. Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. С.190–203
6. Chaeikar S.S., Ahmadi A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. *Signal Processing: Image Communication*. 2019. 70. P. 233–245.
7. PSW statistical LSB image steganalysis / S. Shojae Chaeikar et al. *Multimedia Tools and Applications*. 2018. V.77. P. 805–835.
8. Veena S.T., Arivazhagan S. Universal secret payload location identification in spatial LSB stego images. *Annals of Telecommunications*. 2019. V.74. P. 273–286.

9. Bobok I.I., Kobozeva A.A. Steganalysis method efficient for the hidden communication channel with low capacity. *Радіотехніка*. 2019. V.198. С. 19–31
10. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
11. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.
12. Бобок И.И. Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями. *Сучасний захист інформації*. 2011. V.2. С. 50–60.
13. Кобозева А.А., Альфалуджи С.А. Стеганографический алгоритм, обеспечивающий большую пропускную способность канала скрытой связи. *Вестник Нац. техн. ун-та "ХПИ": сб. науч. тр. Темат. вып.: Системный анализ, управление и информационные технологии*. 2012. V.29. С. 30–41.
14. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности: монография. К.: ГУИКТ, 2009. 251 с.
15. Бобок И.И., Кобозева А.А. Общий стеганоаналитический подход, основанный на матричном анализе. *Вісник Національного технічного університету «ХПІ».* 2011. V.35. С. 12–20.
16. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. *2006 IEEE International Conference on Multimedia and Expo*, Toronto, 2006. P. 549–552
17. Gloe T., Böhme R. The “Dresden Image Database” for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC ’10)*. New York, 2010. P. 1585–1591.
18. Кобозева А.А., Бобок И.И., Батиене Л.Е. Стеганоаналитический метод, основанный на анализе сингулярных чисел блоков матрицы цифрового изображения. *Problemele Energeticii Regionale*. 2018. V.3(38). URL: http://journal.ie.asm.md/ru/contents/electronni-jurnal-338-2018.

ИССЛЕДОВАНИЕ СВОЙСТВ НОРМИРОВАННОЙ ОТДЕЛЕННОСТИ МАКСИМАЛЬНОГО СИНГУЛЯРНОГО ЧИСЛА БЛОКА МАТРИЦЫ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

А.А. Кобозева, И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

На сегодняшний день одним из самых распространенных и востребованных стеганографических методов является метод модификации наименьшего значащего бита – LSB-метод, оставляя актуальной задачу выявления наличия и декодирования скрытой информации, погруженной в контейнер с использованием этого метода, в частности в условиях малой пропускной способности скрытого канала связи. Существующие стеганоаналитические алгоритмы, разработанные для LSB-метода, решают, как правило, основную задачу стеганоанализа – детектирование скрытого канала, оставляя нерешенной задачу декодирования (восстановления) дополнительной информации, для которой важной составляющей является определение/оценка пропускной способности скрытого канала. *Целью* работы являются дополнительные исследования свойств нормированной отделенности максимального сингулярного числа блоков матрицы оригинальных цифровых изображений, которые рассматриваются в качестве контейнеров, и построенных на их основе стеганосообщений, результаты которого дадут возможность для оценки пропускной способности скрытого канала связи. В работе исследуются свойства дискретной функции $y(QF)$, которая определяет количество блоков изображения, в которых происходит увеличения нормированной отделенности максимального сингулярного числа в результате пересохранения изображения в формат с потерями с коэффициентом качества QF. Определены особенности изменения функции $y(QF)$ при стеганопреобразовании исследуемого изображения в зависимости от того, контейнером или стеганосообщением оно является; исследованы свойства $y(QF)$ в зависимости от формата цифрового изображения и коэффициента качества для

изображения в формате с потерями; от величины пропускной способности скрытого канала связи; при однократном и двукратном стеганопреобразовании. В результате проведенных исследований получены односторонние оценки (сверху) величины пропускной способности скрытого канала связи, построенного с помощью LSB-метода на основе контейнера в формате с потерями.
Ключевые слова: стеганоаналитический метод, цифровое изображение, пропускная способность скрытого канала, LSB-метод, нормованнная отделенность сингулярного числа.

RESEARCHING THE PROPERTIES OF THE NORMALIZED SEPARATION OF THE MAXIMUM SINGULAR VALUE OF THE DIGITAL IMAGE MATRIX BLOCK

A.A. Kobozeva, I.I. Bobok

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

The least significant bit modification method is one of the most widespread and demanded steganographic methods. Today this method is often used for the hidden communication channel with low capacity. Therefore, the problem of detecting and decoding LSB-embedding with low capacity is actual. Existing steganoanalytical algorithms for the LSB-method, as a rule, solve the main problem of steganoanalysis. This task is to detect a hidden channel. The problem of decoding (restoring) additional information remains unsolved. It is important to determine/to estimate the capacity of the hidden channel for decoding information. The article considers a digital image as a container. The aim of this article is additional research of the properties of the normalized separation of the maximum singular value of the blocks of the matrix of original digital images and stego. The research results will be used to assess the capacity of the hidden communication channel. The article examines the properties of the discrete function $y(QF)$. This function determines the number of image blocks in which the normalized separation of the maximum singular value increases as a result of resaving the image into a lossy format with a quality factor QF. The features of the change in the function $y(QF)$ during the steganotransformation of the image are determined. These features are different for an empty container and a stego. The properties of $y(QF)$ are investigated depending on the digital image format, on the quality factor for the image in the lossy format; on the value of the capacity of the hidden communication channel; with single and double steganotransformation. As a result of the studies, one-sided estimates (from above) of the capacity of the hidden communication channel constructed using the LSB-method were obtained.
Keywords: steganoanalytical method, digital image, capacity of the hidden channel, LSB-method, normal singularity separation.

DOI 10.15276/imms.v10.no1-2.45
УДК 681.51:519.876

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 45-54

ОПТИМІЗАЦІЯ ІНФОРМАЦІЙНИХ СТРУКТУР ЛОКАЛЬНИХ МЕРЕЖ

В.О. Хорошко, Ю.Є. Хохлачова, А. Аясрах, А. Аль-Далваш

Національний авіаційний університет,
пр. Любомира Гузара, 1, Київ, 03058, Україна; e-mail: post@nau.edu.ua

Широкомасштабне використання обчислювальної техніки та комунікаційних (інформаційних) мереж, перехід до збільшення об'ємів оброблювальної інформації та розширення кола користувачів в усіх сферах життя сучасного суспільства (політичній, військовій, економічній, соціальній та фінансовій) приводять до якісно нових можливостей. Сучасний процес в області інформаційних мереж привів до розробки численних методів, призначених для оптимізації структур інформаційних мереж. При розробці трафіків передачі інформації в мережах необхідно враховувати побудову структур інформаційних потоків, які визначаються кількісними, топологічними, якісними і часовими факторами. Основним критерієм є максимізація суми відношень ефектів взаємодії локальних мереж до затрат на їх взаємодію. *Метою* є кількісна оптимізація інформаційних структур локальних мереж. Пропонується основний критерій подати у вигляді ієрархії локальних критеріїв, а задачу розробки декомпозувати на ряд локальних задач. Основи декомпозиції складає залежність між локальними критеріями оптимізації та факторами, які приховуються. Оптимізація структур за кількісним фактором здійснюється в локальній задачі обчислення раціональних об'єктів інформації. Раціональний об'єм повинен відповідати вимогам повноти інформації, що стає важливою задачею для споживача. Отримані в роботі результати дозволяють виконати кількісну оптимізацію інформаційних структур локальних мереж. Для її виконання розв'язана задача максимізації суми відношень ефектів взаємодії локальних мереж до затрат на їх взаємодію та розроблений порядок її обчислення.

Ключові слова: локальні мережі, кількісна оптимізація, інформаційні структури, трафік передачі інформації, ієрархія локальних критеріїв, декомпозиція.

Вступ

Процес впровадження інформаційних технологій в усі сфери життя сучасного суспільства, що вступає в сучасний період свого розвитку, не можливий без рішення питань оптимізації інформаційних структур мереж в різних сферах: політичній, військовій, економічній, соціальній та фінансовій. Широкомасштабне використання обчислювальної техніки та комунікаційних (інформаційних) мереж, перехід до збільшення об'ємів оброблювальної інформації та розширення кола користувачів приводять до якісно нових можливостей. Незважаючи на те, сучасний процес в області інформаційних мереж привів до розробки численних методів, призначених для оптимізації структур інформаційних мереж.

При розробці трафіків передачі інформації в мережах необхідно враховувати побудову структур інформаційних потоків, які визначаються раціональними факторами: кількісними, топологічними, якісними і часовими [1,2]. Основним критерієм є максимізація суми відношень ефектів взаємодії локальних мереж до затрат на їх взаємодію. Оскільки виникають труднощі, пропонується основний критерій подати у вигляді ієрархії локальних критеріїв, а задачу розробки декомпозувати на ряд локальних

задач. Основи декомпозиції складає залежність між локальними критеріями оптимізації та факторами, які приховуються [2, С.253].

Метою є кількісна оптимізація інформаційних структур локальних мереж.

Основна частина

Виконання задачі розробки структур і трафіків передачі інформації починається з побудови початкових інформаційних структур $G_n^1, (n=\overline{1,n_0})$, що являють собою зв'язані орієнтовані графи [3, С.183]. Вершинами графів є задачі взаємодії макрорівня $M_i^{\mu_i}, (i=\overline{1,\iota_0}, \mu_i=\overline{1,(\mu_\iota)_0})$, що здійснюють інформаційний обмін між елементами локальної мережі та локальними мережами, а дугами – спрямовані інформаційні повідомлення, які назвемо впливами або атаками. Зміст кожного впливу (атаки) визначає локальна мережа, що його використовує.

Задачі $M_i^{\mu_i}$, в свою чергу, представляють зв'язані орієнтовані підграфи, вершинами яких служать задачі взаємодії мікрорівня $U_i^{\lambda_i}, \lambda_i=\overline{1,(\lambda_\iota)_0}$, що перетворюють і передають інформацію елементам локальної мережі S_i, а дугами – інформацію цій локальній мережі.

Задачі взаємодії макрорівня і мікрорівня поділимо на три типи [1,4].

$$M_i^{\mu_i}=A_i^{\alpha_i}\vee B_i^{\beta_i}\vee D_i^{\beta_i}; \tag{1}$$

$$(\alpha_i,\beta_i,\delta_i)=\overline{1,(\mu_i)}_0; \alpha_i\neq\beta_i\neq\delta_i;$$

$$U_i^{\varphi_i}=X_i^{\varphi_i}\vee Y_i^{\psi_i}\vee Z_i^{\xi_i};$$

$$(\varphi_i,\psi_i,\xi_i)=\overline{1,(\lambda_1)}_0; \varphi_i\neq\psi_i\neq\xi_i,$$

Де $(A_i^{\alpha_i}, X_i^{\varphi_i})$ – джерела, що виконують збір підготовку та передачу інформації; $(B_i^{\beta_i}; Y_i^{\psi_i})$ – споживачі, в результаті обробки інформацією, якими формуються рішення або здійснюються дії в мережі S_i. Позначену задачу $X_i^{\varphi_i}$ або $Y_\iota^{\psi_\iota}$ через $(U^\iota)_\iota^{\lambda_\iota}$, а задачу $Y_\iota^{\psi_\iota}$ або $Z_i^{\xi_i}$ через $(U'')_i^{\lambda_i}$. Аналогічно $(M')_i^{\mu_i}$ ідентифікує задачу $A_i^{\alpha_i}$ або $B_i^{\beta_i}$, а $(M'')_i^{\mu_i}$ – задачу $B_i^{\beta_i}$ або $D_i^{\delta_i}$.

Використовуючи позначення задач взаємодії, можна виразити інформацію, якою обмінюються елементи мережі, наприклад,

$$S_k \text{ і } S_i\ W_{k_i}^{M'_{\mu k}U'_{\lambda k}\overline{M''_{\mu k}U''_{\iota k}}}(k=\overline{1,\iota_0}, \mu_k=\overline{1,(\mu_k)_0}, \lambda_k=\overline{1,(\lambda_k)_0}),$$

що функціонує всередині локальної мережі $S_i, W_{ii}^{M_{\mu_i}U'_{\lambda_i}U''_{\lambda_i}}, (\gamma_i=\overline{1,(\lambda_i)_0}, \gamma_i\neq\lambda_i)$.

У зв'язку з тим, що вихідні структури зовнішньої інформації і задачі взаємодії макрорівня необхідно розглядати як в напрямку від джерел до споживачів інформації, так і навпаки, то вони можуть бути подані у вигляді (2) і (3):

$$G_n^{(1)} = \left\{ \begin{array}{l} \left(A_k^{\alpha_k}\right)\left[W_{k_i}^{A_{\lambda k}U'_{\lambda k}M''_{\mu_i}U''_{\lambda_i}}\right], \\ A_k^{\alpha_k}\left(U'\right)_k^{\lambda k} I^*\left(M''\right)_i^{\mu_i}\left(U''\right)_i^{\lambda_i} \times \\ \times\left[\wedge W_{k_i}^{A_{\lambda k}U'_{\lambda k}M''_{\mu_i}U''_{\lambda_i}}\right]\left(B_i^{\beta_i}\right), \\ \left(M'\right)_k^{\mu k}\left(U'\right)_k^{\lambda k} I^* B_i^{\beta_i}\left(U''\right)_i^{\lambda_i} \times \\ \times\left[\wedge W_{ij}^{B_{\beta_i}U'_{\lambda_i}M''_{\mu j}U''_{\lambda j}}\right], \\ B_i^{\beta_i}\left(U'\right)_{i_1}^{\lambda_i} I_1^*\left(M''\right)_j^{\mu_j}\left(U''\right)_i^{\lambda_i} \times \\ \times\left[\wedge W_{ij}^{M_{\mu_i}U'_{\lambda_i}D_{\delta_j}U''_{\lambda j}}\right]\left[\left(D_j^{\delta_j}\right)\right] \end{array} \right\}, \quad (2)$$

$$\left(k,i,j\right)=\overline{1,l_0};\left(\mu_i,\delta_j\right)=\overline{1,\left(\mu_j\right)_0};\lambda_j=\overline{1,\left(\lambda_j\right)_0}, k\neq i\neq j.$$

$$M_i^{\mu_i} = \left\{ \begin{array}{l} \left(X_{\varphi_i}\right)\left[\wedge U''_{\lambda_i}\right],\left[\wedge U'_{\varphi_i}\right]\left(Y_{\psi_i}\right)\times \\ \times X_i^{\varphi_i} I^*\left(U''\right)_i^{\lambda_i}\left(U'\right)_i^{\gamma_i} I * Y_i^{\psi_i} \times \\ \times\left[\wedge U''_{\lambda_i}\right],\left[\wedge U'_{\gamma_i}\right]\left(Z_{\xi_i}\right) \end{array} \right\}, \quad (3)$$

$$Y_i^{\psi_i} I*\left(U''\right)_i^{\lambda_i}\left(U'\right)_i^{\gamma_i} I * Z_i^{\xi_i},$$

де I^* позначає оператор безпосереднього інформаційного зв'язку. Наприклад, в (2) задача $A_k^{ak}(U!)_k^{\lambda_i}$, а задача $(M'')_i^{\mu_i}(U'')_i^{X_i}$ безпосередньо йде за задачею $A_k^{ak}(U')_k^{\lambda k}$. В $G_n^{(1)}$ індекс (1) вказує порядковий номер локальної задачі.

Задачі взаємодії мікрорівня, що розглядаються в (2), будемо називати екзогенними, так як вони безпосередньо видають або отримують інформацію від інших елементів мережі. Решта задач мікрорівня є ондогененними , оскільки вони формують, переробляють або використовують інформацію, що функціонує в середині однієї мережі[5, С.89].

Припустимо, що структури $G_n^{(1)}$ перетворені в структури $G_n^{(3)}$, в результаті видалення в них і задачах $M_i^{\mu_i}$ елементарних контурів і мінімізації кількості дубльованої інформації.

Оптимізація структур за кількісним фактором здійснюється в локальній задачі обчислення раціональних об'єктів інформації [2,5].

Під об'єктом інформації будемо розуміти кількість елементарних символів. Слід відзначити, що мова йде про об'єми інформації, що складається з базових, а не синтетичних показників.

Раціональний об'єм повинен відповідати вимогам повноти інформації, що становиться важливою задачею для споживача.

Якщо об'єм інформації менше потрібного, то елемент мережі, споживач або вся мережа відчуватиме недостачу в інформації. У випадку надлишку потрібного об'єму

виникають непродуктивні затрати на формування, обробку та передачу інформації або результатів рішення задач [4,5].

Позначимо через $\theta_{k_i}^{M'_{\lambda_k}U'_{\lambda_k},M''_{\mu_i}U''_{\lambda_i}}$, $\theta_{ij}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}$, $\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i}M''_{\mu_j}U''_{\lambda j}}$, $\theta_{ii}^{M''_{\mu_k}U''_{\gamma_i}U'_{\lambda_i}}$ об'єми відповідної інформації $W_{ki}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}$, $W_{ii}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}$, $W_{ij}^{M''_{\mu_i}U'_{\lambda_i},M''_{\mu_j}U''_{\lambda j}}$, $W_{ii}^{M'_{\mu_i}U'_{\lambda_i}U''_{\nu_i}}$ $(v_i=\overline{1,(\lambda_i)_0}, v_i \neq \lambda_i)$. Нехай $(Q_{BX})^{M''_{\mu_i}U''_{\lambda_i}}$ або $(Q_{BX})^{B_{\beta_i}Y_{\psi_i}}$ визначають об'єми даних, що необхідні для виконання відповідних задач $(M'')_i^{\mu_i}(U'')_i^{\lambda_i}$, $B_{\beta_i}Y_{\psi_i}$, а $(\theta_{\text{вих}})_i^{M'_{\mu_i}U'_{\lambda_i}}$ і $(\theta_{\text{вих}})_i^{B_{\beta_i}Y_{\psi_i}}$ ідентифікують об'єми результатів рішення задач $(M'')_i^{\mu_i}(U'')_i^{\lambda_i}$ і $B_{\beta_i}Y_{\psi_i}$.

Використовуючи введені позначення, сформулюємо математичну постанову локальної задачі. Тобто, необхідно отримувати структуру $G_n^{(3)}$ за кількісним фактором θ, який характеризує об'єм інформації: необхідний споживачу

$$G_n^{(4)} = optG_n^{(3)},$$

Отже, кількісний критерій K_Q буде мати такий вигляд:

$$K_\theta = \left[\forall_{G_n^{(4)}} \left(M''\right)_i^{\mu_i} \left(U''\right)_i^{\lambda_i} \left(\vartheta_g \sum_{(M')_k^{\mu_k}(U')_i^{\lambda_i}(M'')_i^{\mu_i}(U'')_i^{\lambda_i}} \frac{\left(\theta_{k_i}^{M'_{ik}U'_{\lambda k}M''_{\mu i}U''_{ki}}\right)^{\vartheta_n}}{\left(\theta_{\upsilon\lambda}\right)_i^{M''_{\mu i}U''_{\lambda i}}} + \sum_{(U')_i^{\gamma_i} I*(U'')_i^{\lambda_i}} \frac{\left(\theta_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right)^{\vartheta_n}}{\left(\theta_{вх}\right)^{M''_{\mu_i}U''_{\lambda_i}}} \right) \to 1 \right],$$

де ϑ_g – коефіцієнт достовірності інформації $(\vartheta_g \leq 1)$, ϑ_n – коефіцієнт повноти інформації $(\vartheta_n \leq 1)$. Крім того вони дійсні при врахуванні накладених обмежень.

$$\left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} \geq \left[\left\{ \vartheta_g \left(\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}} \right)^{\vartheta_n} \right\}, \left\{ \left(\theta_{ii}^{M'_{\mu_i}U'_{\lambda_i}U''_{\upsilon_i}} \right)^{\vartheta_n} \right\} \right], \tag{4}$$

$$\begin{gathered} \left(\theta_{вх}\right)_i^{B_{\beta_i}Y_{\psi_i}} = \left(\theta_{вих}\right)_i^{B_{\beta_i}Y_{\psi_i}}, \\ \left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} \geq \left[\left\{ \vartheta_g \left(\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}} \right)^{\vartheta_n} \right\}, \left\{ \left(\theta_{ii}^{M'_{\mu_i}U'_{\lambda_i}U''_{\upsilon_i}} \right)^{\vartheta_n} \right\} \right] \end{gathered} \tag{5}$$

Обмеження (4) вказує на те, що задачам $(M'')_i^{\mu_i}(U'')_i^{\lambda_i}$ і $(M')_i^{\mu_i}(U'')_i^{v_i}$, що використовують інформацію відповідно $W_{ij}^{M''_{\mu_i}U'_{\lambda_i},M''_{\mu_j}U''_{\lambda j}}$ та $W_{ii}^{M'_{\mu_i}U'_{\lambda_i}U''_{v_i}}$, можуть передаватися всі або частина результатів рішення задачі $(M')_i^{\mu_i}(U')_i^{\lambda_i}$. Обмеження (5) характеризує рівність вхідних і вихідних об'ємів даних задач – транзитів.

Коефіцієнт достовірності ϑ_g і коефіцієнт повноти ϑ_n визначаються на основі статистичних матеріалів як наступні відношення:

$$\vartheta_g = \left(\frac{\left(\theta_{ф}^{p}\right)_{k_i}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}}{\left(\theta_{пр}\right)_{k_i}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}U''_{\lambda_i}}} \right)^{y_i},$$

$$\vartheta_n = \left(\frac{\left(\theta_{\phi}\right)_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}}{\left(\theta_{пр}\right)_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}} \right)^{y_i}.$$

Тут використані позначення $W_{ki}^{M'_{\mu_i}U'_{\lambda_i}, M''_{\mu_i}U''_{\lambda_i}}$, $(\theta_{\text{пр}})_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}$ ідентифікують проектний об'єм інформації, фактичний об'єм позначений $(\theta_{\phi})_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}$, $(\theta_{\phi}^{p})_{k_i}^{M'_{\mu_i}U'_{\lambda_i}, M''_{\mu_i}U''_{\lambda_i}}$ – кількість релевантних символів у фактичному об'ємі інформації, а y_i є коефіцієнтом нелінійності, що залежить від цілі H_i системи S_i та вибирається евристично.

Для обчислення раціональних об'ємів інформації, що функціонує всередині задачі взаємодії макрорівня $M_i^{\mu_i}$, критерій K_θ доцільно представити у наступному вигляді:

$$K_\theta = \left[\forall_{M_i^{\mu_i}} \left(U''\right)_i^{\lambda_i} \times \sum_{(U')_i^{\gamma_i} I^* (U'')_i^{\lambda_i}} \frac{\left(\theta_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right)^{\vartheta_n}}{\left(\theta_{вх}\right)^{M''_{\mu_i}U''_{\lambda_i}}} \to 1 \right].$$

Обмеження (4) і (5) можна перетворити у наступні вирази:

$$\left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} \geq \left\{ \left(\theta_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right)^{\vartheta_n} \right\},$$

$$\left(\theta_{вх}\right)_i^{M_{\mu_i}Y_{\psi_i}} = \left(\theta_{вих}\right)_i^{M_{\mu_i}Y_{\psi_i}}.$$

Вихідними даними локальної задачі є об'єми інформації $(\theta_в)_i^{M_{\mu_i}Z_{\xi_i}}, (e = \overline{1, e\xi\iota})$, що використовуються для вироблення тих або інших керуючих рішень або здійснення будь-яких керуючих дій в мережі S_i, та коефіцієнти об'ємів $h_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}$, $h_{ii}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}$, $\left[\left(h_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}, h_{ii}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right) \leq 1\right]$, відповідної інформації $W_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}$, $W_{ii}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}$.

Значення $(\theta_в)_i^{M_{\mu_i}Z_{\xi_i}}$, $h_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}}$, $h_{ii}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}$ визначаються так, щоб для кожної екзогенної задачі $(M')_i^{\mu_i}(U')_i^{\lambda_i}$ виконувалася наступна рівність:

$$\sum_{(M')_k^{\mu_k}(U')_k^{\lambda_k} I^* (M'')_i^{\mu_i}(U'')_i^{\lambda_i}} h_{k_i}^{M'_{\mu_k}U'_{\lambda_k}, M''_{\mu_i}U''_{\lambda_i}} + \sum_{(U')_k^{\gamma_i} I^* (U'')_i^{\lambda_i}} h_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}} = 1,$$

а для ендогенної задачі $(M')_i^{\mu_i}(U')_i^{\lambda_i}$ виконується рівність:

$$\sum_{(U')_k^{\gamma_i} I^* (U'')_i^{\lambda_i}} h_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}} = 1.$$

В загальному випадку значення об'єму $(\theta_{вх})_i^{M_{\mu_i}Z_{\xi_i}}$ знаходиться в інтервалі між найбільшим значенням із $\{(\theta_в)_i^{M_{\mu_i}Z_{\xi_i}}\}$ і сумою всіх $(\theta_в)_i^{M_{\mu_i}Z_{\xi_i}}$:

$$\max\left\{\left(\theta_e\right)_i^{M_{\mu_i}Z_{\xi_i}}\right\} \le \left(\theta_{вх}\right)_i^{M_{\mu_i}Z_{\xi_i}} \le \sum_{e=1}^{e_{\xi_i}}\left(\theta_e\right)_i^{M_{\mu_i}Z_{\xi_i}} .$$

Однак при подальшому розгляді обмеження повинні бути наступними:

$$\left(\theta_{вх}\right)_i^{M_{\mu_i}Z_{\xi_i}} = \max\left\{\left(\theta_e\right)_i^{M_{\mu_i}Z_{\xi_i}}\right\}, \tag{6}$$

$$\left(\theta_{вх}\right)_i^{M_{\mu_i}Z_{\xi_i}} \le \sum_{e=1}^{e_{\xi_i}}\left(\theta_e\right)_i^{M_{\mu_i}Z_{\xi_i}}, \tag{7}$$

при цьому $(\theta_{вх})_i^{M_{\mu_i}Z_{\xi_i}}$ визначається за цими виразами в залежності від значення коефіцієнта релевантності $\theta_i^{M_{\mu_i}Z_{\xi_i}}$.

В результаті рішення локальної задачі необхідно знайти раціональні об’єми:

$$\theta_{k_i}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}U''_{\lambda_k}},\ \theta_{ii}^{M'_{\mu_k}U'_{\gamma_i}U''_{\lambda_i}} \text{ та } (\theta_{\text{вих}})_i^{M'_{\mu_i}U'_{\lambda_i}} .$$

Алгоритм обчислення об’ємів інформації починається з послідовного аналізу задач $M_i^{\mu_i}$ і пошуку в них задач-споживачів Z_{ξ_i} [4,5]. Використовуючи опис задачі макрорівня в (3) і коефіцієнтів об’ємів, обчислюємо раціональні об’єми інформації $W_{ii}^{M'_{\mu_i}U'_{\gamma_i}Z_{\xi_i}}$. Припустимо, що

$$\left(\theta_{ii}^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}}\right)^{\vartheta_1} = h_{ii}^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}}\left(\theta_{вх}\right)_i^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}},$$

Тоді

$$\theta_{ii}^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}} = \left[h_{ii}^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}}\left(\theta_{вх}\right)_i^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}}\right]^{\frac{1}{\vartheta_1}}. \tag{8}$$

Якщо задача Z'_{ξ_i} отримує також інформацію $W_{k_i}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}Z'_{\xi_i}}$ із зовнішнього середовища, то за описом $G_n^{(3)}$ в (3) знаходимо ці впливи і визначаємо їх раціональні об’єми:

$$\vartheta_g\left(\theta_{k_i}^{M'_{ik}U'_{\lambda k},M''_{\mu i}Z_{\xi_i}}\right)^{\vartheta_n} = h_{ii}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}Z_{\xi_i}}\left(\theta_{вх}\right)_i^{M''_{\mu_i}Z_{\xi_i}}, \tag{9}$$

$$\theta_{k_i}^{M'_{ik}U'_{\lambda k},M_{\mu i}Z''_{\xi_i}} = \left[\frac{h_{ik}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}Z_{\xi_i}}\left(\theta_{вх}\right)_i^{M''_{\mu_i}Z_{\xi_i}}}{\vartheta_g}\right]^{\frac{1}{\vartheta^n}}. \tag{10}$$

Оскільки інформація $W_{k_i}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}Z_{\xi_i}}$ передається між елементами мережі, то в (9) і (10) враховується коефіцієнт достовірності ϑ_g, тип задачі $M_i^{\mu_i}$ у цьому випадку рівний B або D.

Далі переходимо, до обчислення об'ємів $(\theta_{\text{вих}})_i^{M'_{\mu_i}U'_{\lambda_i}}$ та $(\theta_{\text{вих}})_k^{M'_{\mu_k}U'_{\lambda_k}}$. Послідовно розглядаємо задачі $D_i^{\delta_i}Z_i^{\xi_i}$ і визначаємо:

$$D_i^{\sigma_i}(U')_i^{\gamma_i}\, I * D_i^{\delta_i}Z_i^{\xi_i}\ ,$$

$$(M')_k^{\mu_k}(U')_k^{\lambda_k}\, I * D_i^{\delta_i}Z_i^{\xi_i}\ .$$

За задачами $D_i^{\sigma_i}(U')_i^{\gamma_i}$ або $(M')_k^{\mu_k}(U')_k^{\lambda_k}$ безпосередньо можуть іти не тільки задачі-споживачі, але й задачі-транзити. Тоді зафіксувавши задачі $D_i^{\sigma_i}(U')_i^{\gamma_i}$ або $(M')_k^{\mu_k}(U')_k^{\lambda_k}$, слід обчислити об'єми результатів виконання задач-транзитів аналогічно (8) і (10). Якщо за цими задачами-транзитами, в свою чергу безпосередньо ідуть інші задачі-транзити, то процес фіксування і аналізу вихідних об'ємів повторюється до тих пір, доки за задачею, що розглядається, не будуть іти задачі типу Z. Вихідні об'єми задач обчислюються як в (6) і (7) на основі заданого значення коефіцієнта релевантності $a_i^{M_{\mu_i}}$

$$\left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} = \max\left[\left\{\vartheta_g\left(\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}\right)^{\vartheta_n}\right\}\left\{\left(\theta_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right)^{\vartheta_n}\right\}\right],$$

$$\left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} = \sum\nolimits_{(M')_i^{\mu_i}(U')_i^{\lambda_i}\, I*(M'')_i^{\mu_i}(U'')_i^{\lambda_i}} \vartheta_g\left(\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}\right)^{\vartheta_n} + \sum\nolimits_{(U')_i^{\lambda_i}\, I*(U'')_i^{\lambda_i}}\left(\theta_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right)^{\vartheta_n};$$

для екзогенних задач $(U')_i^{\lambda_i}$ і згідно

$$\left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} = \max\left\{\vartheta_g\left(\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}\right)^{\vartheta_n}\right\},$$

$$\left(\theta_{вих}\right)^{M'_{\mu_i}U'_{\lambda_i}} = \sum\nolimits_{(U')_i^{\lambda_i}\, I*(U'')_i^{\lambda_i}}\left(\theta_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}}\right)^{\vartheta_n},$$

для екзогенних задач $(U')_i^{\lambda_i}$. Враховуючи (5) і (13) знаходимо об'єми інформації $(\theta_{вх})_i^{B_{\beta_i}Y_{\psi_i}}$ та $(\theta_{вх})_i^{M_{\mu_i}Y_{\psi_i}}$.

Послідовно розглядаючи всі зафіксовані задачі, можна визначити раціональні об'єми інформації:

$$\theta_{k_i}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}U''_{\lambda_i}} = \left[\frac{h_{k_i}^{M'_{\mu_k}U'_{\lambda_k},M''_{\mu_i}U''_{\lambda_i}}\left(\theta_{вх}\right)^{M''_{\mu_i}U''_{\lambda_i}}}{\vartheta_A}\right]^{\frac{1}{\vartheta_1}};$$

$$\theta_{ii}^{M'_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}} = \left[h_{ii}^{M''_{\mu_i}U'_{\gamma_i}U''_{\lambda_i}} \left(\theta_{вх}\right)_i^{M''_{\mu_i}U''_{\lambda_i}} \right]^{\frac{1}{\vartheta_1}}.$$

В порядку обчислення раціональні об'єми вносимо в опис задачі взаємодії макрорівня (3). Після закінчення процедури визначення раціональних об'ємів інформації вирази (2) і (3) приймуть відповідно такий вигляд:

$$G_n^{(4)} = \left\{ \begin{array}{l} \left(A_k^{\alpha_k}\right)\left[\vee\left(W_{k_i}^{A_{\alpha_i}U'_{\lambda_k},M''_{\mu_i}U''_{\lambda_i}}\theta_{k_i}^{A_{\alpha_k}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}\right)\right], \\ A_k^{\alpha_k}\left(U'\right)_k^{\lambda k} I*\left(M''\right)_i^{\mu_i}\left(U''\right)_i^{\lambda_i} \\ \left[\wedge W_{k_i}^{M'_{\mu_k}U'_{\lambda_k},B_{\beta_i}U''_{\lambda_i}}\theta_{k_i}^{M'_{\mu_k}U'_{\lambda_k}B_{\beta_i}U''_{\lambda_i}}\right]\left(B_i^{\beta_i}\right) \\ \left(M'\right)_k^{\mu k}\left(U'\right)_k^{\lambda k} I*B_i^{\beta_i}\left(U''\right)_i^{\lambda_i} \\ \left[\vee\left(W_{ij}^{B_{\beta_i}U''_{\lambda_i},M'_{\mu_i}U'_{\lambda_i}}\theta_{k_i}^{B_{\beta_i}U'_{\lambda_i},M''_{\mu_i}U''_{\lambda_i}}\right)\right], \\ B_i^{\beta_i}\left(U'\right)_i^{\lambda_i} I*\left(M''\right)_j^{\mu_j}\left(U''\right)_i^{\lambda_i} \\ \left[\wedge W_{ij}^{M'_{\mu_i}U'_{\lambda_i}D_{\delta_j}U''_{\lambda_j}}\theta_{ij}^{M'_{\mu_i}U'_{\lambda_i}D_{\delta_j}U''_{\lambda_j}}\right]\left(D_j^{\delta_j}\right) \end{array} \right\},$$

$$\left(M'\right)_i^{\mu_i}\left(U'\right)_i^{\lambda_i} I*D_j^{\delta_j}\left(U''\right)_j^{\lambda_j}$$

$$M_i^{\mu_i} = \left\{ \begin{array}{l} \left(X_{\varphi_i}\right)\left[\wedge U''_{\lambda_i}\theta_{ii}^{M_{\mu_i}X_{\varphi_i}U''_{\lambda_j}}\right] \\ X_i^{\varphi_i} I*\left(U''\right)_i^{\lambda_i} \\ \left[\wedge U'_{\lambda_i}\theta_{ii}^{M_{\mu_i}U'_{\gamma_i}Y_{\psi_i}}\right]\left(Y_{\psi_i}\right)\left[\wedge\left(U''_{\gamma_i}\theta_{ii}^{M_{\mu_i}Y_{\psi_i}U''_{\lambda_i}}\right)\right], \\ \left(U'\right)_i^{\gamma_i} I*Y_i^{\psi_i} \\ Y_i^{\psi_i} I*\left(U''\right)_i^{\lambda_i} \\ \left[\wedge\left(U'_{\gamma_i}\theta_{ii}^{M_{\mu_i}U'_{\gamma_i}Z_{\xi_i}}\right)\right]\left(Z_{\xi_i}\right) \end{array} \right\}$$

$$\left(U'\right)_i^{\gamma_i} I*Z_i^{\xi_i}$$

На цьому оптимізація інформаційних структур локальних мереж закінчена.

Висновки

Приведені викладки на отримані результати дозволяють виконати кількісну оптимізацію інформаційних структур локальних мереж. Для її виконання розв'язана задача

максимізації суми відношень ефектів взаємодії локальних мереж до затрат на їх взаємодію та розроблений порядок обчислення її.

Список літератури

1. Брахман Т.Р. Многокритериальность и выбор альтернативы в техник. Москва: Радио и связь, 1984. 308 с.
2. Штойер Р. Многокритериальная оптимизация. Теория вычислений и приложения. Москва: Радио и связь, 1992. 504с.
3. Оре О. Теория графов. Москва: Наука, 1980. 336 с.
4. Майника Э. Алгоритмы оптимизации на сетях и графах. Москва: Мир, 1981. 323с.
5. Козюра В.Д., Шелест М.Є., Ткач Ю.М. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. Ніжин: ТПК «Орхідея», 2019. 144с.

ОПТИМИЗАЦИЯ ИНФОРМАЦИОННЫХ СТРУКТУР ЛОКАЛЬНОЙ СЕТИ

В.О. Хорошко, Ю.Є. Хохлачова, А. Аясрах, А. Аль-Далваш

Национальный авиационный университет,
пр. Любомир Гузар, 1, Киев, 03058, Украина; e-mail: post@nau.edu.ua

Широкомасштабное использование вычислительной техники и коммуникационных (информационных) сетей, переход к увеличению объемов обрабатывающей информации и расширение круга пользователей во всех сферах жизни современного общества (политической, военной, экономической, социальной и финансовой) приводят к качественно новым возможностям. Современный процесс в области информационных сетей привел к разработке многочисленных методов, предназначенных для оптимизации структур информационных сетей. При разработке трафиков передачи информации в сетях необходимо учитывать построение структур информационных потоков, которые определяются количественными, топологическими, качественными и временными факторами. Основным критерием является максимизация суммы отношений эффектов взаимодействия локальных сетей к затратам на их взаимодействие. Целью является количественная оптимизация информационных структур локальных сетей. Предлагается основной критерий представить в виде иерархии локальных критериев, а задачу разработки декомпозировать на ряд локальных задач. Основы декомпозиции составляет зависимость между локальными критериями оптимизации и факторами, которые скрываются. Оптимизация структур по количественному фактору осуществляется в локальной задачи вычисления рациональных объектов информации. Рациональный объем должен соответствовать требованиям полноты информации, становится важной задачей для потребителя. Полученные в работе результаты позволяют выполнить количественную оптимизацию информационных структур локальных сетей. Для ее выполнения решена задача максимизации суммы отношений эффектов взаимодействия локальных сетей к затратам на их взаимодействие и разработан порядок ее исчисления.

Ключевые слова: локальные сети, количественная оптимизация, информационные структуры, трафик передачи информации, иерархия локальных критериев, декомпозиция.

OPTIMIZATION OF INFORMATION STRUCTURES OF LOCAL NETWORKS

V.O. Khoroshko, Yu.Ye. Khokhlachova, A. Ayasrah, A. Al-Dalwash

National Aviation University,
1, Lubomyr Guzarv Ave, Kyiv, 03058, Ukraine; e-mail: post@nau.edu.ua

Large-scale use of computers and communication (information) networks, the transition to increasing the amount of processing information and expanding the range of users in all spheres of modern society (political, military, economic, social and financial) lead to qualitatively new opportunities. The modern process in the field of information networks has led to the development of numerous methods designed to optimize the structures of information networks. When developing traffic for information transmission in networks, it is necessary to take into account the construction of information flow structures, which are determined by quantitative, topological, qualitative and time factors. The main criterion is to maximize the sum of the ratios of the effects of interaction of local networks to the cost of their interaction. The aim is to quantitatively optimize the information structures of local networks. It is proposed to present the main criterion in the form of a hierarchy of local criteria, and to decompose the development task into a number of local tasks. The basis of decomposition is the relationship between local optimization criteria and hidden factors. The optimization of structures by a quantitative factor is carried out in the local problem of calculating rational objects of information. Rational volume must meet the requirements of completeness of information, which becomes an important task for the consumer. The results obtained in this work allow to perform quantitative optimization of information structures of local networks. To perform it, the problem of maximizing the sum of the ratios of the effects of interaction of local networks to the cost of their interaction is solved and the procedure for its calculation is developed.

Keywords: local networks, quantitative optimization, information structures, traffic of information transfer, hierarchy of local criteria, decomposition.

DOI 10.15276/imms.v10.no1-2.55
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 55-60

МОДИФІКАЦІЯ МЕТОДУ ХЕШ-СТЕГАНОГРАФІЇ, ЗАСНОВАНОГО НА ПЕРЕДАЧІ ПОСЛІДОВНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ

В.В. Зоріло, О.Ю. Лебедєва, М.В. Бохонько

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: whiteswanhelena@gmail.com

Захист електронної інформації криптографічними та стеганографічними методами, а також їх комбінацією сьогодні є дуже затребуваним. Проте новий вид стеганографії – хеш-стеганографія, принципово відрізняється від класичної стеганографії тим, що не потрібно вбудовувати повідомлення в контейнер, не потрібно хвилюватись про кількість інформації, яку можна передати в одному контейнері, не порушивши візуальну стійкість зображення. Певна послідовність звичайних цифрових зображень – це і є повідомлення. Метою даної роботи є підвищення ефективності передачі секретного повідомлення шляхом модифікації метода хеш-стеганографії. Раніше алгоритми отримання хеш-функцій цифрових зображень не використовували для передачі повідомлень, проте вони знайшли своє застосування в хєш-стеганографії. В даній роботі виконано порівняння двох алгоритмів отримання хеш-кодів та запропоновано метод їх застосування для перетворення текстового повідомлення на послідовність цифрових зображень. Саме певний порядок файлів, що передаються, і є вирішальним при розшифруванні повідомлення. Символам повідомлення ставиться у відповідність частина хеш-коду цифрового зображення. Таким чином утворюється необхідна комбінація файлів, кількість яких дорівнює кількості символів повідомлення. В роботі проведено порівняльний аналіз двох алгоритмів методу. Отримані результати підтвердили ефективність використання алгоритму отримання хеш-кодів, заснованого на аналізі коефіцієнтів ДКТ цифрового зображення. Даний алгоритм робить метод стійким до атак стисненням, зміною яскравості та контрастності, масштабуванням та обертанням.

Ключові слова: хеш-стеганографія, цифрове зображення, хеш-код.

Вступ

Використання різних технологій приховування процесу інформаційної взаємодії з метою приховування інформації при її подальшої передачі по відкритих каналах зв'язку є не новим в нинішніх реаліях повсякденного життя людини. Для забезпечення скритності повідомлення, що міститься в носії (контейнері), використовуються різні стеганографічні методи. При цьому поряд з конфіденційністю набуває все більшої актуальності забезпечення цілісності переданих по незахищеним каналам даних. В якості основного методу захисту інформації від нелегітимних користувачів при організації інформаційної взаємодії застосовується криптографічний захист, який має високу ефективність через гарантовану стійкість сучасних систем шифрування [1]. Також сучасні методи захисту інформації неможливо уявити без стеганографічних методів, які, на відміну від криптографічних, приховують сам факт передачі повідомлення. Однак, коли ми вбудовуємо повідомлення в стеганографічні контейнери, завжди є ризик модифікації чи втрати повідомлення в результаті атаки. Також важливою проблемою в даній області є пропускна здатність, тобто кількість інформації, яку можна непомітно вбудувати в контейнер. Для того, аби уникнути цих проблем, винайшли альтернативний вид стеганографії – хеш-стеганографія. В роботі [2] запропоновано не вбудовувати в зображення-контейнери інформацію, а використовувати послідовність зображень, а саме безпосередньо хеш-код зображень

для побудови секретного повідомлення. Тобто хеш-стеганографія заснована на тому, що певна послідовність цифрових сигналів, зокрема цифрових зображень, і є повідомленням. Встановлюється відповідність між хеш-кодами зображень та певними символами, які в визначеній послідовності формують секретне повідомлення. В роботі [3] запропоновано метод хеш-стеганографії, заснований на використанні цифрових зображень та їх хеш-кодів для передачі секретного повідомлення. Дана стаття є продовженням попередньої роботи. В ній описано доповнений хеш-стеганографічний метод, заснований на передачі послідовності цифрових зображень.

Мета роботи

Метою роботи є підвищення ефективності передачі секретного повідомлення шляхом модифікації метода хеш-стеганографії.

Матеріали та методи

Модифікація методу, описаного в [3], полягає в наступному. Отримання хеш-коду пропонується виконувати алгоритмом Perceptual Hash (далі pHash) [4], який має певні переваги перед алгоритмом Average Hash (далі aHash), використаним в [3], а саме стійкість хешкоду до певних афінних перетворень за рахунок використання ДКП.

У зображеннях є відповідність між частотним спектром та інформаційною наповненістю. Високі частоти зображення відповідають деталям, контурам, зміні функції яскравості пікселів тощо. Низькі частоти відповідають фоновим частинам, несуть основну інформацію. Високі частоти чутливі до багатьох атак: стиснення, зміна чіткості зображення розмиттям чи підвищенням різкості тощо. Низькі частоти більш стійкі до подібних змін. Логічно використовувати низькочастотну складову сигналу для передачі секретного повідомлення. Тобто необхідно виконати певні перетворення цифрового зображення, перш ніж генерувати його хеш-код.

Найшвидший спосіб видалити високі частоти та деталі – зменшити зображення. Алгоритм aHash має одним з кроків зменшення зображення до розмірів 8×8, щоб загалом було 64 пікселі. Збереження пропорцій не є важливим у даному випадку. Таким чином, хеш буде відповідати будь-яким варіаціям зображення, незалежно від масштабу або співвідношення сторін. Далі рисунок розміром 8×8 необхідно перевести у градації сірого. Це змінює хеш із 64 пікселів (64 червоних, 64 зелених та 64 синіх) на 64 загальні кольори. Потім обчислюємо середнє значення N для 64 кольорів. Перетворюємо зображення в бінарну послідовність наступним чином. Порівнюємо значення кожного пікселя зображення із значенням N. Якщо значення пікселя менше за N, то ставимо йому у відповідність значення 0, інакше – 1. Формуємо вектор із значень 0 та 1. Отриману послідовність шифруємо за допомогою шифру MD5. Даний алгоритм генерує хешкоди, стійкі до масштабування та зміни співвідношення сторін, до стиснення зображення, проте нестійкий до таких афінних перетворень як повороти ЦЗ та корекції яскравості кольорів.

Розглянемо перцептивний алгоритм (pHash). За аналогією з попереднім алгоритмом зменшуємо розмір зображення до 32×32. Переходимо до зображення в градаціях сірого. Обчислюємо ДКП. Для роботи нам потрібні низькі частоти, як було зазначено вище, тому в даному алгоритмі використовують коефіцієнти ДКП верхнього лівого блоку 8×8. Вони відповідають найнижчим частотам зображення. Обчислюємо середнє значення коефіцієнтів ДКП за виключенням першого коефіцієнта, оскільки він може значно відрізнятися від інших значень і буде відкидати середнє значення. Поставимо у відповідність коефіцієнтам ДКП бінарну послідовність, де 0 відповідає

коефіцієнтам, значення яких менше за середнє, 1 – більше. Переводимо 64-бітову послідовність у 64-бітове ціле число.

Основні етапи модифікованого методу хеш-стеганографії представлено далі.

На першому етапі створюються бази даних (далі БД) хеш-кодів зображень. Для коректної роботи даного методу необхідна велика кількість унікальних зображень. На даному етапі розраховуються хеш-коди усіх зображень за допомогою вищезазначеної хеш-функції (рис.1). Будемо використовувати перші два символи хеш-коду.

```
e84014ff8666378de4f997e4536950f3
aed21eb87010e8dcd8f77d5ef2b3b64b
388bb38e38db9d3474d076e92154e178
bf0c959a017a46abe942dc47a2f96843
e0a952358b03def495fe558da26f208b
a76b210b02bc63050a0943cd25edc2ed
ec1ad6716c85a93c3164223ba978f2e1
cf097b964ab7ca0b3d48b19f64e1eb94
0f8c3ecb62a71ee6a4f3ac862acb180a
2eb87b2767e836e9792c0dfcac762212
6ebec9533947729d4fd61d8954df2c9c
```

Рис. 1. Хеш-коди деяких зображень

Зображення підбираються таким чином, щоб одному символу повідомлення відповідали чотири зображення. Символи повідомлення кодуються в системі ASCII. Код символу повинен відповідати першим двом символам хеш-кодів зображень (рис. 2).

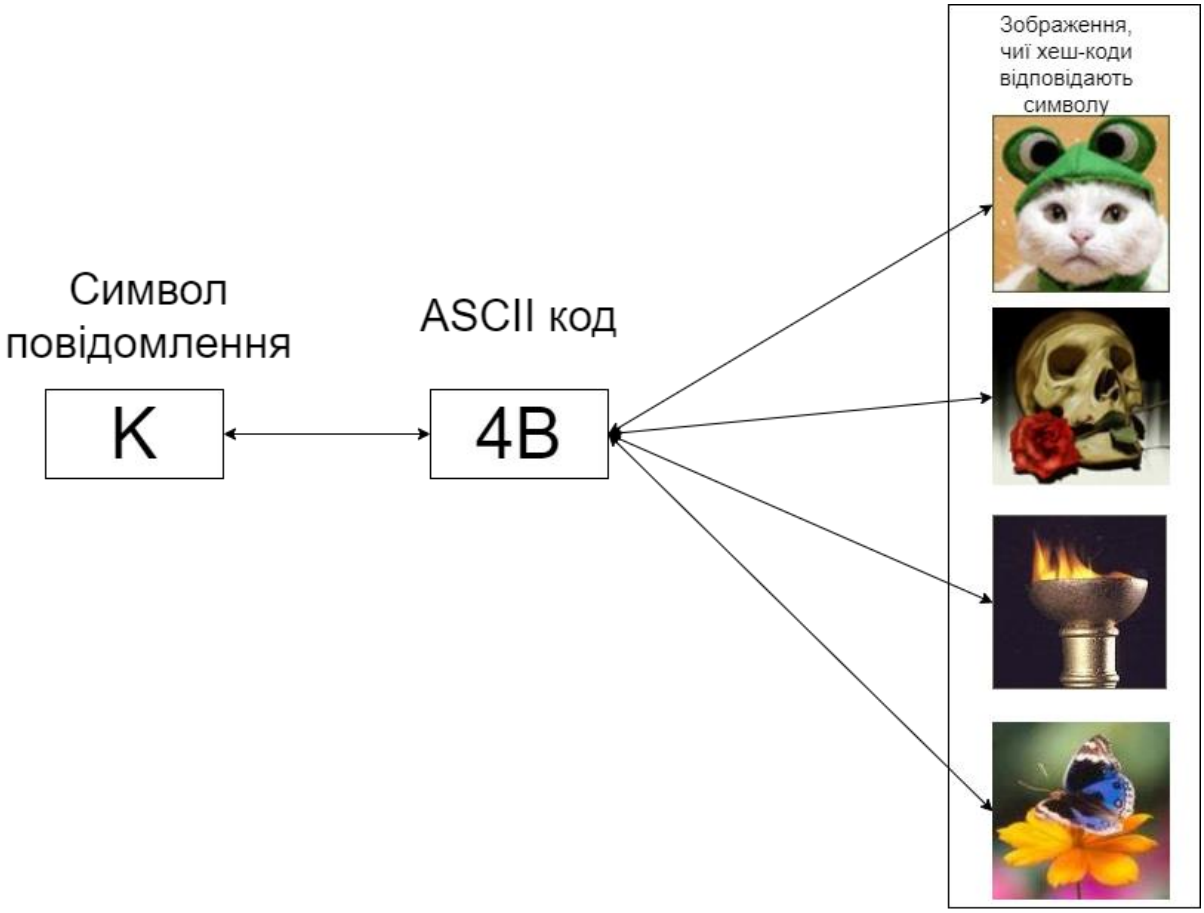


Рис. 2. Схема відповідності «символ-зображення»

На другому етапі вводимо повідомлення для передачі. Переводимо повідомлення в систему ASCII та розбиваємо на рівні частини по 2 символи [5]. Для кожного символу повідомлення відбираємо відповідне зображення перше в черзі. Якщо зображення було використано раніше, беремо наступне зображення у черзі. Якщо всі зображення були використані, цикл починається з початку.

На третьому етапі отримуємо послідовність зображень, яка є контейнером стеганоповідомлення та готова для відправлення.

Приклад результату роботи метода показано на рисунку 3, де закодовано повідомлення «Bad company».

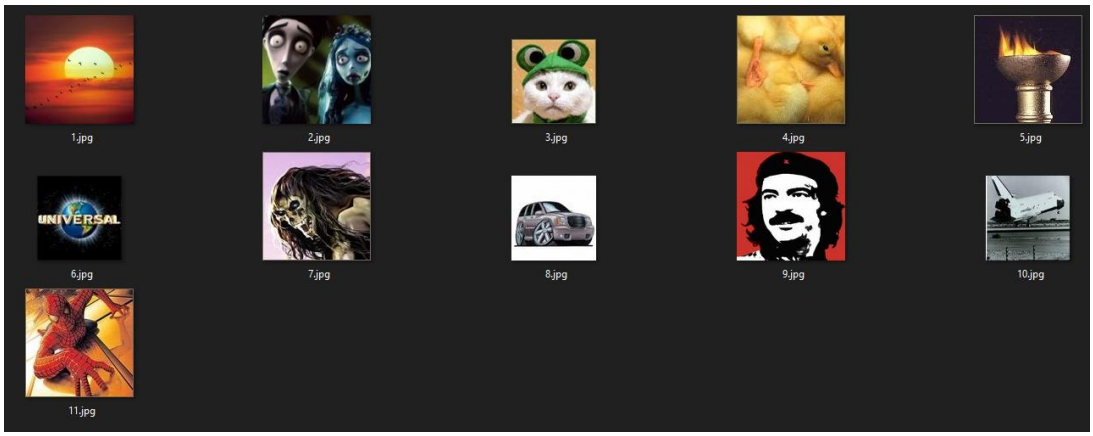


Рис. 3. Відібрані зображення, які шифрують словосполучення «Bad company»

Результати та обговорення. Одержувач після отримання зображень зберігає їх у тому ж порядку, генерує їх хеш-коди, з перших двох символів кожного хеш-коду формує ASCII-код. Далі одержувач переводить ASCII код в символи латинського алфавіту і отримує початковий текст повідомлення.

Основна ідея методу полягає у використанні перцептивних хеш-функцій aHash та pHash, за допомогою яких отримуються стійкі хеш-коди зображень до різних видів атак, таких як: масштабування, стиснення, зміна яскравості або контрасту. Порівняємо ефективність відновлення повідомлень, переданих подібним шляхом (табл.1).

Таблиця 1.

Порівняння ефективності алгоритмів методу хеш-стеганографії

Алгоритм / Вид атаки	aHash	pHash
Обертання (не більше 30°)	87	94
Зміна контрастності	85	95
Масштабування	92	97
Стиснення JPG	96	96
Зміна яскравості	91	95

Як бачимо з таблиці, використання pHash дало кращі результати в порівнянні з aHash, що дозволило підвищити ефективність передачі секретних повідомлень.

Висновки

В результаті даної роботи виконано модифікацію методу хеш-стеганографії. Отримані результати обчислювального експерименту показали, що використання

алгоритму pHash, заснованого на ДКП, дає кращі результати відновлення повідомлення з послідовності цифрових зображень в порівнянні з алгоритмом aHash, який працює зі значеннями яскравості пікселів напряму.

Список літератури

1. Pfitzmann B. Information hiding terminology, information hiding. *First international workshop of lecture notes in computer science*. Berlin: Springer-Verlag, 1996. P. 347-350.
2. Shin N. One-Time Hash Steganography. Heidelberg: Springer-Verlag, 2000. P.17-28.
3. Бохонько М.В, Зоріло В.В. Модифікація методу хеш-стеганографії. VII *Міжнародна науково-практична інтернет-конференція «Сучасний рух науки», 6-7 червня 2019 р*. Дніпро, 2019. С.605-608.
4. Looks Like It. URL: www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html.
5. ASCII Code – The extended ASCII table. URL: www.ascii-code.com.

МОДИФИКАЦИЯ МЕТОДА ХЕШ-СТЕГАНОГРАФИИ, ОСНОВАННОГО НА ПЕРЕДАЧЕ ПОСЛЕДОВАТЕЛЬНОСТИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

В.В. Зорило, Е.Ю. Лебедева, М.В. Бохонько

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: whiteswanhelena@gmail.com

Защита электронной информации криптографическими и стеганографическими методами, а также их комбинацией сегодня является очень востребованной. Однако новый вид стеганографии – хэш-стеганография, принципиально отличается от классической стеганографии тем, что не нужно встраивать сообщение в контейнер, не нужно волноваться о количестве информации, которую можно передать в одном контейнере, не нарушив визуальную устойчивость изображения. Определенная последовательность обычных цифровых изображений – это и есть сообщение. Целью данной работы является повышение эффективности передачи секретного сообщения путем модификации метода хеш-стеганографии. Ранее алгоритмы получения хэш-функций цифровых изображений не использовались для передачи сообщений, однако они нашли свое применение в хеш-стеганографии. В данной работе выполнено сравнение двух алгоритмов получения хэш-кодов и предложен метод их применения для преобразования текстового сообщения в последовательность цифровых изображений. Именно определенный порядок передаваемых файлов и является решающим при расшифровке сообщения. Символам сообщения ставится в соответствие часть хэш-кода цифрового изображения. Таким образом образуется необходимая комбинация файлов, количество которых равно количеству символов сообщения. В работе проведен сравнительный анализ двух алгоритмов метода. Полученные результаты подтвердили эффективность использования алгоритма получения хэш-кодов, основанного на анализе коэффициентов ДКП цифрового изображения. Данный алгоритм делает метод устойчивым к атакам сжатием, изменением яркости и контрастности, масштабированием и вращением.

Ключевые слова: хеш-стеганография, цифровое изображение, хеш-код.

MODIFICATION OF THE HASH-STEGANOGRAPHY METHOD BASED ON THE TRANSFER OF A SEQUENCE OF DIGITAL IMAGES

V.V. Zorilo, O.Yu. Lebedeva, M.V. Bokhonko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: whiteswanhelena@gmail.com

The protection of electronic information by cryptographic and steganographic methods, as well as their combination, is in great demand today. However, the new type of steganography – hash-steganography, fundamentally differs from classical steganography in that there is no need to embed messages in a container, no need to worry about the amount of information that can be transmitted in one container without compromising the visual stability of the image. A certain sequence of ordinary digital images is a message. The purpose of this work is to increase the efficiency of transmitting a secret message by modifying the hash-method of steganography. Previously, algorithms for obtaining hash functions of digital images have not been used to transmit messages, but they have found their application in hash-steganography. This paper compares two algorithms for obtaining hash codes and suggests a method of their application for transforming a text message into a sequence of digital images. It is a certain order of files transferred that is decisive in the decryption of a message. The symbols of the message are put in correspondence with the part of the hash code of the digital image. Thus, the necessary combination of files is formed, the number of which is equal to the number of symbols in the message. A comparative analysis of the two algorithms of the method has been performed. The results obtained have confirmed the effectiveness of the hash code algorithm based on the analysis of digital image DCT coefficients. This algorithm makes the method resistant to attack by compression, changing brightness and contrast, magnification and rotation.
Keywords: hash-steganography, digital image, hash-code.

DOI 10.15276/imms.v10.no1-2.61
УДК 004.02

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 61-67

ВИЯВЛЕННЯ «РОЗУМНОГО РОЗМИТТЯ» ЯК ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

О.Ю. Лебедєва, В.В. Зоріло, О.А. Карпова

Одеський національний політехнічний університет,
просп.Шевченка, 1, Одеса, 65044, Україна; e-mail:whiteswanhelena@gmail.com

Виявлення порушень цілісності цифрового зображення – одна з важливих задач захисту інформації. При підробці зображення часто використовують розмиття, зокрема фільтр «розумне розмиття», який впливає на фон і залишає контури чіткими. Відомими методами виявлення розмиття обробку даним фільтром важко виявити, що спонукає шукати нове рішення. Метою роботи є виявлення обробки цифрового зображення фільтром «Розумне розмиття» шляхом модифікації методу, заснованого на аналізі сингулярних чисел блоків матриці цифрового зображення. Методи досліджень базуються на використанні загального підходу до аналізу стану та технології функціонування інформаційної системи. Розроблено метод виявлення «розумного» розмиття, отримано кількісні оцінки ефективності методу в термінах помилок першого та другого роду: помилки 1 роду – 3%, 2 роду – 1,5%. Розроблений у даній роботі метод може бути використано при розробці комплексної системи захисту інформації для перевірки цифрових зображень на наявність їх постобробки після можливої фальсифікації або при виявленні стеганографічної атаки.Можливим напрямком подальших досліджень є продовження роботи з аналізу впливу інших видів розмиття цифрового зображення на властивості його матриці для розширення області застосування модифікованого методу.

Ключові слова:цифрове зображення, фальсифікація цифрового зображення, «розумне розмиття», матриця цифрового зображення, сингулярні числа.

Вступ

Поширеність, доступність та простота у використанні різноманітного програмного забезпечення для обробки та редагування цифрових зображень призвела до їх фальсифікації у великих масштабах. Через це виникла необхідність у вдосконаленні вже існуючих та розробці новихалгоритмів та методів для виявлення порушення цілісності цифрових зображень (ЦЗ), щоє невід’ємною складовою сучасних комплексних систем захисту інформації.

Наукові дослідження та розробки у цьому напрямку ведуться багатьма вченими у всьому світі. Проте відомі з відкритих джерел сучасні методи та алгоритми виявлення порушень цілісності зображень не завжди є ефективними, а також мають великі недоліки. Наприклад, існує багато методів, де використовуються цифрові водяні знаки, але більшість технічних засобів для отримання цифрових зображень та відео не мають можливості попереднього занурення цифрового водяного знаку, що частіш за все робить нереальним використання цих методів [1]. Досить активними у розвитку є методи виявлення фальсифікації ЦЗ, які виконують аналіз exif-даних, але вони лише констатують факт можливого редагування ЦЗ та не локалізують область фальсифікації [2].

Практика та відомі з відкритих джерел факти показують, що для обробки цифрового зображення часто використовують такий інструмент, як розмиття. Ефективним методом виявлення розмиття наразі є метод, заснований на аналізі сингулярних чисел (СНЧ) блоків матриці цифрового зображення [3]. Даний метод використовує швидкість росту найменших сингулярних чисел для виявлення таких

видів розмиття як розмиття за Гаусом, розмиття в русі. Дані види розмиття, реалізовані, наприклад, в графічному редакторі AdobePhotoshop, впливають головним чином на контури зображення, що впливає головним чином на найменші сингулярні числа: швидкість їх росту зменшується. Проте є ще один популярний фільтр зазначеного графічного редактору – «розумне» розмиття. Даний фільтр розмиває фон, залишаючи контури чіткими. Виявлення даного виду розмиття відомим методом частіше дає хибні результати у вигляді помилок першого роду (до 30%), що спонукає дослідити детально вплив «розумного» розмиття на математичні параметри (матриці) цифрового зображення.

Мета роботи

Метою даної роботи є виявлення «розумного» розмиття цифрового зображення шляхом модифікації методу, заснованого на аналізі сингулярних чисел блоків матриці цифрового зображення.

Основна частина

Оскільки в основі фільтру «розумне» розмиття лежить розмиття усього окрім контурів, то частка фону в цифровому зображенні після обробки стане більшою за рахунок розмиття нечітких контурів. В цей самий час контури, що були чіткими до розмиття, лишатимуться такими і після. Обчислювальний експеримент показав, що після обробки деякі сингулярні числа збільшуються. На прикладі цифрового зображення, представленого на рисунку 1, розглянемо вплив «розумного» розмиття на сингулярні числа блоків 8×8, отриманих за допомогою стандартної розбивки його матриці [4].

Рис. 1. Оригінальне зображення

Як бачимо на рисунку 2, дійсно, деякі сингулярні числа збільшуються в результаті обробки. Щоб зручніше було бачити даний ефект, від матриці сингулярних чисел оригінального ЦЗ віднімемо матрицю сингулярних чисел обробленого зображення (рис.3).

Як бачимо, не можна сказати певно, які саме сингулярні числа збільшуються в блоках, проте очевидно, що дану особливість можна використати для виявлення даного виду розмиття цифрового зображення.

531,229	469,503	413,725	397,678	396,182	423,854	426,249	450,652
8,96193	12,5403	10,5984	10,3551	11,9294	10,0598	10,4218	12,1709
7,46241	9,46935	9,17458	8,47127	10,8741	9,79565	8,28681	8,07548
5,11614	6,16596	6,27723	4,03754	7,65027	8,4415	6,53117	7,93263
3,65982	4,61563	4,72728	2,73436	6,59548	5,05442	4,62604	4,62407
3,06919	2,08904	3,69734	1,81966	1,89974	2,97611	3,42039	2,10065
0,94862	1,5846	3,10196	0,91867	1,22273	1,10224	1,38946	2,0158
0,31321	0,41385	0,29524	0,49634	0,37428	0,1205	0,02824	1,09677

а

530,732	472,035	412,403	398,396	395,635	421,992	428,274	451,695
8,312	11,9481	11,4658	10,7214	12,7472	11,5827	11,0423	14,6338
7,22052	9,20825	8,44183	9,1371	9,36465	9,64593	8,04784	8,24214
4,90431	4,75626	5,80179	4,12288	8,30317	8,28432	5,80664	7,53503
4,06288	3,92507	3,80482	2,32577	3,51018	3,30399	4,00838	4,02028
1,64489	0,98372	3,16109	2,08293	1,45145	1,48103	1,33101	2,05103
0,79551	0,80007	0,29485	0,69469	0,66738	0,36165	1,12076	0,89356
1,16E-14	9,54E-16	3,46E-15	1,66E-14	3,90E-15	2,02E-14	5,32E-15	1,37E-15

б

Рис. 2. Фрагмент матриці сингулярних чисел блоків ЦЗ: а – оригінального ЦЗ; б – розмитого

0,4964	-2,5321	1,3222	-0,7179	0,5471	1,8621	-2,0251	-1,0421
0,6499	0,5922	-0,8674	-0,3663	-0,8178	-1,5229	-0,6205	-2,4629
0,2419	0,2611	0,7328	-0,6658	1,5095	0,1497	0,2390	-0,1667
0,2118	1,4097	0,4754	-0,0853	-0,6529	0,1572	0,7245	0,3976
-0,4031	0,6906	0,9225	0,4086	3,0853	1,7504	0,6177	0,6038
1,4243	1,1053	0,5362	-0,2633	0,4483	1,4951	2,0894	0,0496
0,1531	0,7845	2,8071	0,2240	0,5554	0,7406	0,2687	1,1222
0,3132	0,4139	0,2952	0,4963	0,3743	0,1205	0,0282	1,0968

Рис. 3. Фрагмент матриці різниці

Для встановлення порогового значення виявлення первинного розмиття було використано 300 цифрових зображень у форматі без втрат розміром 1000×1000 пікселів та 300 ЦЗ у форматі без втрат розміром 2000×2000 пікселів. У зв'язку з тим, що розмір досліджуваного зображення може виявитися будь-яким, розглянемо відсоткове відношення кількості сингулярних чисел, які збільшилися після розмиття, до загальної кількості сингулярних чисел матриці.

У таблиці 1 представлені дані про кількість збільшених сингулярних чисел після розмиття.

Також цікаво, як повторне розмиття вплине на збільшення сингулярних чисел. Результати представлено в таблиці 2.

Таблиця 1.

Фрагмент таблиці з кількістю збільшених СНЧ після розмиття оригінального ЦЗ

№	ЦЗ 1000×1000 пікселів		ЦЗ 2000×2000 пікселів	
	Кількість збільшених СНЧ, шт.	Кількість збільшених СНЧ, %	Кількість збільшених СНЧ, шт.	Кількість збільшених СНЧ, %
1	50851	40,6808	214300	42,86
2	46490	37,192	186281	37,2562
3	51949	41,5592	194225	38,845
4	42512	34,0096	196004	39,2008
5	52064	41,6512	193492	38,6984
6	49666	39,7328	186730	37,346
7	43323	34,6584	188486	37,6972
8	49117	39,2936	211104	42,2208
9	48260	38,608	162081	32,4162
10	50506	40,4048	201943	40,3886
11	47155	37,724	181876	36,3752
12	48080	38,464	208652	41,7304
13	49763	39,8104	202762	40,5524
14	50745	40,596	215581	43,1162
15	47852	38,2816	198265	39,653

Таблиця 2.

Кількість СНЧ, що зросли після повторного розмиття

№	Первинне розмиття з R=1, P=1		Первинне розмиття з R=2, P=1		Первинне розмиття з R=2, P=2	
	Кількість збільшених СНЧ, шт	Кількість збільшених СНЧ, %	Кількість збільшених СНЧ, шт	Кількість збільшених СНЧ, %	Кількість збільшених СНЧ, шт	Кількість збільшених СНЧ, %
1	43150	34,52	39228	31,3824	32472	25,9776
2	33473	26,7784	31884	25,5072	33802	27,0416
3	41013	32,8104	38044	30,4352	33666	26,9328
4	28391	22,7128	28520	22,816	34697	27,7576
5	34420	27,536	33051	26,4408	36638	29,3104
6	35851	28,6808	33380	26,704	32245	25,796
7	43508	34,8064	40185	32,148	33061	26,4488
8	32185	25,748	30689	24,5512	32795	26,236
9	38325	30,66	36132	28,9056	33215	26,572
10	28966	23,1728	28381	22,7048	34371	27,4968
11	36715	29,372	34294	27,4352	36465	29,172
12	33390	26,712	31759	25,4072	34082	27,2656
13	26882	21,5056	26309	21,0472	34724	27,7792
14	24718	19,7744	24789	19,8312	33206	26,5648
15	40841	32,6728	37733	30,1864	31193	24,9544

Завдяки аналізу отриманих даних було встановлено, що у якості порогового значення, що дозволяє відділити більшість розмитих експертом вперше ЦЗ від повторно розмитих, доцільно використовувати значення – 32,95%, що підтверджено експериментально. На основі даного аналізу розробимо алгоритм методу виявлення «розумного» розмиття.

Нехай I – $N \times M$ -матриця цифрового зображення, що було обрано для перевірки.

Крок 1. Виділити із матриці I підматрицю R, що відповідає червоному колірному каналу. Виділити матрицю C $k \times l$-розміру, де k та l – найближчі значення до N та M, які діляться на 8.

Крок 2.Розбити матрицю C стандартним чином на блоки 8×8:

$$C_{ij}, i = 1, 2, ...k/8, \quad j = 1, 2, ..., l/8 .$$

Крок 3. Скласти матрицю сингулярних чисел: побудувати сингулярне розкладання [5] для кожного блоку C_{ij} :

$$C_{ij} = U_{ij} \sum_{ij} V_{ij}^T ,$$

Де U_{ij}, V_{ij} – ортогональні матриці лівих та правих сингулярних векторів C_{ij} відповідно, розміром 8×8; $\sum_{ij} = diag\left(\sigma_1, ..., \sigma_8\right)$ – матриця сингулярних чисел, для якої виконується:

$$\sigma_1 \geq ... \geq \sigma_8 \geq 0 .$$

Крок 4. Отримане на перевірку ЦЗ розмити у AdobePhotoshop фільтром «Розумне розмиття» з наступними параметрами: радіус = 1, порогове значення = 1, якість = «Висока».

Повторити дії пунктів 1-3 для розмитого експертом зображення. R_{ij} – отримана матриця сингулярних чисел.

Крок 5. Знайти різницю матриць СНЧ оригінального та розмитого ЦЗ:

$$RAZN = \sum_{ij} - R_{ij} .$$

Крок 6. Обчислити кількість $count$ від'ємних значень матриці $RAZN$.

Крок 7. Обчислити кількість усіх СНЧ:

$$s = \left(h + \frac{w}{8} \right).$$

Крок 8. Знайти відношення $count / s$ та виконати порівняння:

Якщо

$$\frac{count}{s} * 100 < 32.95$$

то зображення розмите

інакше – зображення оригінальне.

Аналіз ефективності даного методу в таблиці 3.

Таблиця 3.

Ефективність методу виявлення «розумного розмиття»

Помилки першого роду	Помилки другого роду
3%	1.5%

Висновки

В даній роботі на основі виявленої особливості поведінки сингулярних чисел блоків, отриманих за допомогою стандартного розбиття матриці цифрового зображення, при «розумному розмитті» розроблено метод виявлення обробки цифрового зображення даним фільтром. Кількість помилок 1 роду розробленого методу складає 3%, кількість помилок 2 роду – 1.5%.

Предметом подальшого розвитку розробленого методу є проведення досліджень для вдосконалення точності відокремлення оригінальних цифрових зображень від таких, цілісність яких порушена, а також розширення спектру досліджуваних параметрів розмиття.

Список літератури

1. Yeung M.M.,Mintzer F.,Yeung M.M. An Invisible Watermarking Technique for Image Verification. *ICIP 1997: Proceedings of IEEE International Conference on Image Processing*, 26-29 October 1997. Santa Barbara, California, USA, 1997. №2. P. 680-683.
2. Грибунин В.Г.,Оков И.Н.,Туринцев И.В. Цифровая стеганография. Москва: СОЛОН-Пресс, 2002. 272 с.
3. Зорило В.В. Методы повышения эффективности выявления нарушения целостности цифрового изображения.*Інформаційнабезпека.* 2013. № 2.С. 34-41.
4. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.
5. Деммель Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.

ВЫЯВЛЕНИЕ «УМНОГО РАЗМЫТИЯ» КАК НАРУШЕНИЯ ЦЕЛОСТНОСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Е.Ю. Лебедева, В.В. Зорило, А.А. Карпова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail:whiteswanhelena@gmail.com

Выявление нарушений целостности цифрового изображения - одна из важных задач защиты информации. При подделке изображения часто используют размытие, в частности фильтр «умное размытие», который влияет на фон и оставляет контуры четкими. Известными методами выявления размытия обработку данным фильтром трудно обнаружить, что побуждает искать новое решение. Целью работы является выявление обработки цифрового изображения фильтром «Умное размытие» путем модификации метода, основанного на анализе сингулярных чисел блоков матрицы цифрового изображения. Методы исследований базируются на использовании общего подхода к анализу состояния и технологии функционирования информационной системы. Разработан метод выявления «умного» размытия, получена количественная оценка эффективности метода в терминах ошибок первого и второго рода: ошибки 1 рода - 3%, 2 рода - 1,5%. Разработанный в данной работе метод может быть использован при создании комплексной системы защиты информации для проверки цифровых изображений на наличие

их постобработки после возможной фальсификации или при обнаружениистеганографическойатаки. Возможным направлением дальнейших исследований является продолжение работы по анализу влияния других видов размытия цифрового изображения на свойства его матрицы для расширения области применения модифицированного метода.
Ключевые слова: цифровое изображение, фальсификация цифрового изображения, умное размытие, матрица цифрового изображения, сингулярные числа.

DETECTING «SMART BLUR» AS A DIGITAL IMAGE INTEGRITY VIOLATION

O.Yu. Lebedeva, V.V. Zorilo, O.A. Karpova

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail:whiteswanhelena@gmail.com

Detection of violations of the integrity of the digital image is one of the important tasks of information protection. Blurring is often used when forging images, in particular the "smart blur" filter, which affects the background and leaves the outlines clear. Known methods of blur detection treatment with this filter is difficult to detect, which encourages the search for a new solution. The aim of this work is to detect the processing of digital images by the filter "Smart Blur" by modifying the method based on the analysis of singular numbers of blocks of the matrix of the digital image. Research methods are based on the use of a general approach to the analysis of the state and technology of the information system. The method of detection of "reasonable" blur is developed, quantitative estimations of efficiency of a method in terms of errors of the first and second kind are received: errors of the 1st kind - 3%, 2nd kind - 1,5%. The method developed in this work can be used in the development of a comprehensive information security system to check digital images for the presence of their post-processing after possible falsification or in the detection of steganographic attack. A possible area of further research is to continue work on the analysis of the impact of other types of blurring of the digital image on the properties of its matrix to expand the scope of the modified method.
Keywords: digital image, falsification of digital image, smart blur, digital image matrix,singular values.

DOI 10.15276/imms.v10.no1-2.68
УДК 004.056:351.861

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 68-74

МЕТОД ВИБОРУ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ

Ю.М. Ткач

Національний університет «Чернігівська політехніка»,
вул. Шевченка, 95, м. Чернігів, 14035, Україна; e-mail: tkach_ym@ukr.net

Запропоновано метод вибору функціонального профілю захищеності. Функціональний профіль захищеності є мінімальним набором необхідних послуг для визначеного рівня та для забезпечення обраного рівня захищеності, але вибір способів їх реалізації залишається за розробником (експертом). За рахунок реалізації обраного функціонального профілю захищеності забезпечується зменшення збитку, який може бути нанесений об’єкту захисту. У статті формалізовано завдання вибору функціонального профілю захищеності. Метод складається з таких кроків: відбір експертів для визначення та оцінки показників відповідних ймовірностей; збір інформації та її обробка; обчислення показника вірогідності появи і-ої загрози; обчислення показника вірогідності відвернення і-ої загрози, обчислення показника вірогідності використання j-ої вразливості v_{ij}; обчислення показника відверненого збитку; оцінка оптимальності функціонального профілю захищеності за умови виконання $S(F_0) = \max_{F \in \bar{F}} S(F)$ при обмеженні $C(F) \le C_r$. Таким чином, метод вибору функціонального профілю захищеності дозволяє здійснити оптимальний вибір при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту. Розроблений метод може бути використаним при створенні системи захисту інформації в кіберпросторі.

Ключові слова: функціональний профіль захищеності, система захисту інформації.

Постановка проблеми

Створення будь-якої системи захисту інформації (СЗІ) в усіх сферах інформаційної діяльності в державі включає обов'язкову процедуру вибору і подальшу розробку та реалізацію системи функціонування профілю захисту [1]. У завдання розробки системи входить обстеження властивостей конкретного об'єкту захисту (ОЗ) і вибір необхідного функціонального профілю захищеності з приведеного списку ФПЗ. Дана робота присвячена саме проблемі розробці методу вибору оптимального функціонального профілю захищеності об'єкту захисту.

Аналіз останніх досліджень і публікацій

Дослідженню питання розвитку систем захисту інформації, зокрема, розробці теоретичного та методологічного підґрунтя оцінки їх ефективності присвячені роботи як вітчизняних науковців, так і закордонних (Л.М. Артюшин, Д.С.Берестов, В.Ю. Гайкович, О.Г. Корченко, Л.М. Осинский, О.О. Скопа, О.В. Потій, В.О. Хорошко, В.Л. Шевченко, Ю.В. Щеглов, Andrew Blyth, Peter Eden, Gyunyoung Heo, Hanseong Son, Pete Burnap, Rahman Khalilur, Hugh Soulsby, Kristan Stoddart та ін.). Публікації [2-7] підтверджують актуальність наявних загроз в інформаційній сфери, серед яких вже котрий рік поспіль перші позиції займають питання інформаційної безпеки держави.

Мети та завдання статті

Метою статті є підвищення рівня захищеності інформаційної системи як окремого державного органу, так і держави в цілому. Основними завданнями є аналіз процесу вибору функціонування профілю захищеності, віднаходження процедури оптимізації цього вибору.

Виклад основного матеріалу дослідження

Згідно із НД ТЗІ 2.5-005-99 [1] метою введення класифікації АС і стандартних функціональних профілів захищеності є полегшення задачі співставлення вимог до комплексу засобів захисту (КЗЗ) обчислювальної системи автоматизованої системи (АС) з характеристиками самої АС. Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС. Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред’являються.

Загально відомо, що інформація, з точки зору безпеки, характеризується такими властивостями: конфіденційністю, цілісністю і доступністю. При чому, кожний підклас деякого класу складається з певної кількості ієрархічних стандартних функціональних профілів. Ця кількість може бути різною від профілю до профілю. Стандартні функціональні профілі є ієрархічними, оскільки їх реалізація забезпечує наростаючу захищеність. Загрози кіберпростору за впливом на базові характеристики безпеки інформаційних ресурсів (конфіденційність, цілісність, доступність) у відповідності з джерелом [1] поділяють на: К-тип (загроза конфіденційності); Ц-тип (загроза цілісності); Д-тип (загроза доступності); КЦ-тип; КД-тип; ЦД-тип; КЦД-тип.

Природа джерела загроз та стан джерела загроз розділяють на:

- об'єктивна (загроза, виникнення якої не залежить від прямої діяльності людини і пов'язана з різними стихійними природними явищами, такими, як пожежі, блискавки, землетрусу, радіоактивне випромінювання, нападу гризунів і т.п.);
- суб'єктивна (загроза, виникнення якої залежить від діяльності людини).

Суб’єктивну загрозу за мотивом поділяють на активну, таку що пов’язана з діями людини, які направленні на отримання певної вигоди та пасивну, тобто ту, яка виключає вказану складову і пов’язана з помилками людини. Пасивні загрози - це помилки системи (пошкодження окремих компонентів обладнання, тобто апаратного забезпечення підприємства) та катастрофи. Також зазначають, що пасивна загроза - несанкціонований доступ до інформації без зміни стану самої системи, активна - несанкціонована зміна системи, яка вносить певні зміни в стан самої системи [8].

Для прикладу, представимо в таблиці 1 множину профілів та послуг, якими характеризується АС класу 1.

Примітка: 0 – ставився у випадку, якщо певна послуга в профілі взагалі відсутня, 1,2,3 – рівні захисту у відповідному СФПЗ.

З таблиці 1 видно, що до всіх профілів включені послуги НР, НИ,НК, НО, НЦ, НТ, проте відсутні НВ, НА та НП, в сукупності всі вони характеризують у СФПЗ спостереженість. Також жодного разу не зустрічались деякі характеристики і інших властивостей інформації (конфіденційність, цілісність), зокрема, КД, КК, КВ, ЦД, ЦВ.

Зауважимо, що наявність спостереженості у всіх СФПЗ обумовлюється тим, що спостереженість є властивістю системи, яка стосується її керованості, а тому має бути

притаманна всім системам, що реалізуються функції захисту інформації (ЗІ). Аналогічне явище щодо спостереженості присутнє і в СФПЗ АС класу 2 та АС класу 3.

Таблиця 1.

Стандартні функціональні профілі захищеності

Послуги		Типи загроз та рівні захисту																					
		К		Ц		Д				КЦ		КД				ЦД				КЦД			
		1	2	1	2	1	2	3	4	1	2	1	2	3	4	1	2	3	4	1	2	3	4
Конфіденційність	КА	0	1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1
	КО	0	1	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	1	1
	КК	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Цілісність	ЦА	0	0	0	2	0	0	0	0	0	2	0	0	0	0	1	1	1	1	1	1	1	1
	ЦО	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1
Достовірність	ДР	0	0	0	0	1	2	2	2	0	0	1	2	2	2	1	2	2	2	1	2	2	2
	ДС	0	0	0	0	0	1	2	3	0	0	0	1	2	2	0	1	2	3	0	1	2	3
	ДЗ	0	0	0	0	0	1	2	3	0	0	0	1	2	3	0	1	2	3	0	1	2	3
	ДВ	0	0	0	0	1	2	2	3	0	0	1	2	2	3	1	2	2	3	1	2	2	3

Під час створення нових функціональних профілів необхідно дотримуватись описаних в НД ТЗІ 2.5-004-99 [2] умов для кожної із послуг, що включаються до профілю. Послуги можуть включати декілька рівнів захисту (1 – мінімальний, 2 – базовий, 3 – повний, 4 – абсолютний). Рівні розпочинаються з першого і зростають до рівня n, де n - визначене для кожного виду послуг число. Чим вище рівень послуги, тим більш складно забезпечується захист від різного типу загроз. Отже, послуга є набором функцій, що дозволяють забезпечити захист від певної сукупності загроз.

Розглянувши загальні питання формування стандартного функціонального профілю захищеності (ФПЗ), перейдемо до його вибору та оптимізації цього рішення.

У НД ТЗІ 2.5-005 -99 налічується 22 послуги, які забезпечують захист від чотирьох основних типів загроз (конфіденційності, цілісності, доступності та їх всі можливі комбінації) [1].

ФПЗ є мінімальним набором необхідних послуг для визначеного рівня та для забезпечення обраного рівня захищеності, але вибір способів їх реалізації залишається за розробником (експертом). За рахунок реалізації обраного ФПЗ забезпечується зменшення збитку, який може бути нанесений ОЗ.

Формалізуємо завдання вибору оптимального ФПЗ. Для цього побудуємо математичну модель ФПЗ.

Нехай $\overline{F}$ множина усіх можливих ФПЗ заданих рівнів, які визначаються вимогами до захищеності інформації, F – вектор розмірності 22 (нормативно

визначена кількість). Компонентами вектора F є булеві змінні $f_i \in \{0,1\}$. Розмірність вектора F введена для зручності і уніфікації опису СФПЗ, оскільки відомо, що до складу багатьох ФПЗ входять не усі послуги. У разі відсутності якої-небудь послуги відповідна компонента дорівнює нулю. $S(F)$ – загальний відвернений збиток.

Тоді, формальна постановка задачі має вигляд:

$$S(F_0) = \max_{F \in \bar{F}} S(F) \tag{1}$$

при обмеженні

$$C(F) \le C_r , \tag{2}$$

де F – деякий вектор, що описує ФПЗ, $\bar{F}$ сукупність усіх допустимих профілів, F_0 – оптимальне значення вектора F, а C_r – допустимі витрати на ФПЗ.

Таким чином, нас перш за все буде цікавити значення F_0, який визначає оптимальний при даній постановці задачі набір послуг, що будуть влючені до ФПЗ.

Відмітимо, що допустима інша постановка задачі, а саме:

$$C(F_0) = \min_{F \in \bar{F}} C(F) ,$$

$$S(F) \ge F_{kr} .$$

У даному випадку знаходимо F_0, при якому витрати на СФПЗ будуть мінімальними, і при цьому відвернений можливий збиток складатиме не менше F_{kr}.

Припустимо, що може бути реалізований деякий набір вразливостей, внаслідок чого може виникнути ряд загроз t_i, $i = 1,...,n$ $(n = 4)$. При цьому, кожну *i*-у загрозу характеризуватиме ймовірність її появи P_{it}, можливий збиток інформаційного середовища – S_i, тоді P_i - ймовірність відвернення *i*-ої загрози, а відвернений збиток за рахунок запобігання *i*-ої загрози через $r_i = P_i P_{it} S_i$.

Загрози нейтралізуються за рахунок реалізації функціональних послуг, тобто відповідними засобами і механізмами СЗІ. Тоді, P_i – вірогідність нейтралізації кожної *i*-ої загрози, буде основною характеристикою СЗІ. Очевидно, що ймовірність нейтралізації *i*-ої загрози: $P_i = g_i(F) = g_i(f_1, f_2,..., f_m)$, де $m = 22$.

Позначимо p_{ij} – ймовірність відвернення *i*-ої загрози за рахунок включення до ФПЗ компоненти f_j, $I_i(f_j)$ – індикатор f_j, тобто, випадкова величина, значення якої дорівнює 1, якщо f_j входить до профілю, і дорівнює нулю у протилежному випадку. Уважаючи випадкові величини $I_i(f_j)$ незалежними, маємо:

$$P_i = \sum_{j=1}^{m} p_{ij} I_i(f)_j - \sum_{l<j} p_{ij} p_{il} I_i(f_j) I_i(f)_l + ... + (-1)^{m-1} \prod_{j=1}^{m} p_{ij} I_i(f_j) . \tag{3}$$

Ймовірності p_{ij} можна визначити за допомогою експертів. Тоді загальний відвернений збиток виражається співвідношенням:

$$S(F) = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} P_i P_{it} S_i .$$

Таким чином, (3) є явним видом цільової функції $S(F)$ задачі математичного програмування (1)-(2). Однак, функція $S(F)$ нелінійна і визначена на булевій множині, тому проблема пошуку оптимального розв'язку є досить складною.

З метою спрощення задачі розглянемо дещо інший підхід до побудови цільової функції. Цілком природньо серед усіх можливих послуг f_j, які дозволяють усунути *i*-ту загрозу вибрати таку, для якої ймовірність p_{ij} є максимальною, тоді

$$S(F) = \sum_{i=1}^{n} P_{it} S_i \max_{f_i} \{ p_{ij} f_j \}.$$

Вірогідність появи *i*-ої загрози P_{it} визначається таким чином. Як було вказано раніше, кожна загроза залежить від вірогідності використання деякої множини вразливостей $V_{ij} = \{v_{ij}, i = 1,...,n\}$, тобто $P_{it} = f_i(v_{ij},...,v_{in})$. Даний показник також можна визначити на основі експертного методу.

Вірогідність використання *j*-ої вразливості v_{ij} можна визначити, за допомогою обчислення відносної частоти їх появи. А саме,

$$v_{ij} = \frac{\lambda_{ij}}{\sum_{k=1}^{n} \lambda_{ik}}$$

де λ_{ij} – частота виникнення *j*-ої вразливості, а *i* - відповідний номер загрози.

Отже, запропоновано метод, який складається з наступних кроків:

- відбір експертів для визначення та оцінки показників відповідних ймовірностей;
- збір інформації та її обробка;
- обчислення показника вірогідності появи *i*-ої загрози;
- обчислення показника вірогідності відвернення *i*-ої загрози,
- обчислення показника вірогідності нейтралізації *i*-ої загрози;
- обчислення показника вірогідності використання *j*-ої вразливості v_{ij};
- обчислення показника відверненого збитку;
- оцінка оптимальності ФПЗ за умови виконання $S(F_0) = \max_{F \in \bar{F}} S(F)$ при обмеженні $C(F) \le C_r$.

Висновки

Розроблений метод може бути використаним для здійснення вибору оптимального функціонального профілю захищеності при створенні системи захисту інформації та передбачає виконання умови максимізації відверненого збитку та не перевищення допустимих витрат.

Список літератури

1. Класифікація автоматизованих систем та стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. URL: http://www.dstszi.gov.ua/ dstszi/doccatalog/ document?id=41648.
2. Берестов Д.С. Гульков М.О., Козачок В.А. Побудова парето-оптимальних функціональних профілів захищеності. *Збірник наукових праць*. 39(1). К.: ЦВСД НУОУ, 2009. С. 89-94. URL: http://www.nbuv.gov.ua/ old_jrn /Soc_Gum/Znpcvsd/2009_1/12.pdf.

3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. URL: http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=41649.
4. Лєншин А.В., Буслов П.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу. *Радіоелектрон-ні і комп'ютерні системи : науч. тр.* Харків.: Нац. аэрокосм. ун-т ХАИ, 2010. V.48(7). С.77-81. URL: http://nbuv.gov.ua/UJRN/recs_2010_7_15.
5. Паламарчук Н.А., Хлапонін Ю.І., Овсянніков В.В. Сучасний стан нормативно-правової бази в галузі технічного захисту інформації. *Збірник наукових праць ВІТІ НТУУ "КПІ"*. К.: ВІТІ НТУУ "КПІ", 2011. №3. С.78-82. URL: http://viti.edu.ua/ files/ zbk/ 2011/11_3_2011.pdf.
6. Потій О.В., Лєншин А.В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу. *Прикладная радиоэлектроника*. Харків, 2010. 9(3). С.479-488. URL: http://openarchive.nure.ua/handle/document/ 410.
7. Шевченко В.Л., Берестов Д.С. Метод пошуку проектних альтернатив системи захисту інформації. *Сучасний захист інформації* К.: ДУТ, 2015. №3. С.22-27. URL: http://journals.dut.edu.ua/index.php/ dataprotect/ article/viewFile/386/358

МЕТОД ВЫБОРА ФУНКЦИОНАЛЬНОГО ПРОФИЛЯ ЗАЩИЩЕННОСТИ

Ю.Н. Ткач

Национальный университет «Черниговская политехника»,
ул. Шевченко, 95, Чернигов, 14035, Украина; e-mail: tkach_ym@ukr.net

Предложен метод выбора функционального профиля защищенности. Функциональный профиль защищенности является минимальным набором необходимых услуг для определенного уровня и для обеспечения выбранного уровня защищенности, но выбор способов их реализации остается за разработчиком (экспертом). За счет реализации выбранного функционального профиля защищенности обеспечивается уменьшение ущерба, который может быть нанесен объекту защиты. В статье формализована задача выбора функционального профиля защищенности. Метод состоит из следующих шагов: отбор экспертов для определения и оценки показателей соответствующих вероятностей; сбор информации и ее обработка; вычисления показателя вероятности появления i-й угрозы; вычисления показателя достоверности предотвращения i-й угрозы, вычисления показателя достоверности использования j-й уязвимости v_{ij}; вычисления показателя отвлеченного ущерба; оценка оптимальности функционального профиля защищенности при условии выполнения $S(F_0) = \max_{F \in \bar{F}} S(F)$ при ограничении $C(F) \le C_r$. Таким образом, метод выбора функционального профиля защищенности позволяет осуществить оптимальный выбор при выполнении условия максимизации отраженного ущерба и не превышения допустимых расходов за счет вероятно-стоимостной оценки показателей количества и частоты появления угрозы, вероятных убытков от реализации найденных угроз и стоимости услуги защиты. Разработанный метод может быть использован при создании системы защиты информации в киберпространстве.

Ключевые слова: функциональный профиль защищенности, система защиты информации.

METHOD OF SELECTION OF FUNCTIONAL PROTECTION PROFILE

Y.N. Tkach

National University "Chernihiv Polytechnic",
95, Shevchenko St., Chernihiv, 14035, Ukraine; e-mail: tkach_ym@ukr.net

A method for selecting a functional security profile is proposed. The functional security profile is the minimum set of necessary services for a certain level and to ensure the selected level of security, but the choice of ways to implement them remains with the developer (expert). The implementation of the selected functional security profile reduces the damage that may be caused to the object of protection. The article formalizes the task of choosing the Functional Security Profile. The method consists of the following steps: selection of experts to determine and evaluate the indicators of the relevant probabilities; information collection and processing; calculation of the probability of the i-th threat; calculation of the probability of averting the i-th threat, calculating the probability of using the j-th vulnerability v_{ij}; calculation of the averted loss indicator; estimation of the optimality of functional security profile under the condition of $S(F_0) = \max_{F \in \bar{F}} S(F)$ under the restriction of $C(F) \le C_r$. Thus, the method of choosing the functional profile of security allows to make the optimal choice when fulfilling the condition of maximizing the averted damage and not exceeding the allowable costs for account of probabilistic cost estimation of indicators of quantity and frequency of occurrence of threat, probable losses from realization of the defined threats and cost of service of protection. The developed method can be used to create a system of information security in cyberspace.

Keywords: functional security profile, information security system.

DOI 10.15276/imms.v10.no1-2.75
УДК 004.056.6

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 75-83

РОЗРОБКА МЕТОДУ КОНТРОЛЮ ЦІЛІСНОСТІ ЗОБРАЖЕННЯ НА ОСНОВІ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

І.С. Чіклікчі, А.А.Смагін, Л.В. Нечитайлова, Н.І. Кушніренко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: infsec2011@gmail.com

Розробка засобів та методів захисту інформаційної цілісності документів, зокрема цифрових зображень, залишається традиційно актуальною задачею. Популярність отримали методи контролю цілісності контенту з використанням прихованих цифрових водяних знаків. Цілісність тут може гарантуватися шляхом хешування файлу. Хеш-суми зображень можуть зберігатися у окремій захищеній базі даних. Для зручності роботи системи бажано, щоб хеш або інший модифікатор, який гарантує цілісність, був вбудований безпосередньо у зображення. Переважна більшість цифрових фотографій зберігається в стисненому вигляді з використанням алгоритмів групи JPEG. Оскільки алгоритм не зберігає точні значення пікселів, додавання цифрового водяного знаку (ЦВЗ) в файли такого типу передбачає додавання інформації в просторі перетворень, іншими словами, зміні підлягають квантовані коефіцієнти дискретного косинусного перетворення (ДКП), саме ті дані, які залишаються незмінними в процесі стиснення зображення. У ролі ЦВЗ виступатиме хеш-сума зображення, яка отримується шляхом використання хеш-функції. В алгоритмах, які працюють з зображенням такого формату, зазвичай змінюються молодші значущі біти (LSB), і інформація впроваджується послідовно. У даній статті розроблено метод контролю цілісності зображення на основі цифрового водяного знаку, який базується на вбудовуванні хеш-суми в найменш помітні місця зображення і дозволяє оцінити психовізуальну помітність впровадження. На етапі перед вбудовуванням проводиться аналіз статистики зображення з метою виявлення найбільш вдалих місць для вбудовування додаткової інформації. Наведені результати обчислювального експерименту.

Ключові слова: контроль цілісності зображень, дискретне косинусне перетворення, цифровий водяний знак, вбудовування секретної інформації, хеш-сума.

Вступ

В еру стрімкого розвитку інформаційних технологій дані, які зберігаються і передаються у цифровому форматі, все частіше потребують захисту від модифікації, несанкціонованого копіювання та використання. Одним із основних видів цифрового контенту на сьогоднішній день є цифрове зображення. Протидія копіюванню зображень, захист авторських прав власників на зображення, захист торгової марки продукції [1] – це далеко не повний перелік напрямків, які сьогодні існують. Крім того, виникає необхідність перевірки інформаційної цілісності зображень з метою виявлення присутності несанкціонованих змін і фальсифікації. Тому на сьогоднішній день розробка засобів та методів перевірки інформаційної цілісності зображення є актуальною задачею. Існуючі методи базуються на різних підходах, кожен з яких має свої переваги та недоліки. Популярність отримали методи контролю цілісності контенту з використанням прихованих цифрових водяних знаків. В такому випадку цілісність зображення може гарантуватися шляхом хешування файлу. Хеш-суми зображень можуть зберігатися у окремій захищеній базі даних. Але для зручності роботи системи бажано, щоб хеш або

інший модифікатор, який гарантує цілісність, був вбудований безпосередньо у зображення.

Мета та задачі роботи

Метою роботи є розробка метода контролю цілісності зображення, який ґрунтується на вбудовування в зображення ЦВЗ, який містить його хеш-значення.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз моделей і методів контролю цілісності зображень;
- запропонувати власний метод контролю цілісності зображень з вбудовування хеш значення;
- розробити програмне забезпечення, яке реалізує запропонований метод контролю цілісності;

Об'єкт дослідження – процеси забезпечення достовірності джерела поширення та контролю цілісності зображення на основі цифрових водяних знаків.

Предмет дослідження – методи контролю цілісності зображень, що ґрунтуються на використанні цифрових водяних знаків.

Основна частина

Для впровадження хеш-значення в зображення існує 4 основних методи[2], три з яких досить прості у реалізації, проте не є надійними. Четвертий метод базується на використані цифрового водяного знаку, що робить цього більш надійним, але і більш складним у реалізації.

Перші три методи контролю цілісності зображень: зберігання хеш-суми поруч з зображенням, зберігання хеш-суми у віддаленій базі даних, поєднання хеш-суми та зображення (наприклад її додавання в кінець зображення не використовуючи жодних стенографічних методів). Мінусом цих методів є надійність. Використовуючи кожен з них, можна легко отримати хеш-суму зображення і в підсумку змінити її, а так само і саме зображення. Таким чином, вони ніяк не можуть гарантувати цілісність зображення, а цей критерій є головним для алгоритму, що розробляється.

Четвертий спосіб контролю цілісності використовує стенографічний метод на основі вбудовуванні непомітного ЦВЗ. В даному випадку зловмисник не зможе зрозуміти, що зображення може підлягати контролю цілісності і будь-яка його модифікація може бути з легкістю виявлена. В даному методі так само використовується хеш-сума зображення, однак пропонується використання самого зображення в якості сховища для хеш-суми (рис.1). Для того щоб вбудувати хеш-суму використовують молодший розряд обраних частотних компонентів зображення. Метод заміни молодших біт (LSB-метод) заснований на тому, що молодші розряди графічних, аудіо та відеоформатів несуть мало інформації і їх зміна практично не позначається на якості переданих зображення [3]. Це дає можливість використовувати їх для приховування конфіденційної інформації. Однак за рахунок введення додаткової інформації спотворюються статистичні характеристики зображення-контейнера і приховане повідомлення легко виявити за допомогою статистичних методів стеганоаналіза, таких як оцінка ентропії і коефіцієнтів кореляції [4].

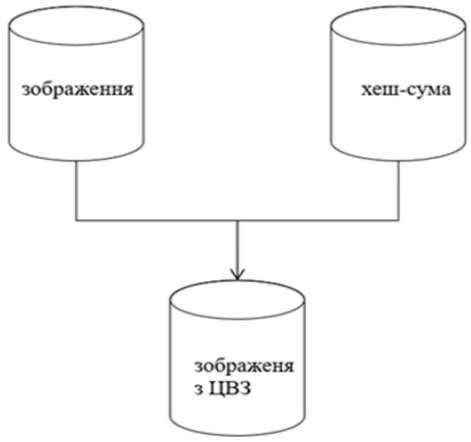


Рис. 1. Використання цифрового водяного знаку

Недолік даного методу полягає в тому, що не завжди можливо помістити у зображення хеш певної довжини. Щоб уникнути цього можна обчислювати кількость пікселів в зображені і підбирати потрібну довжину хешу.

Хеш-функція – це функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованої довжини, так званий «дайджест». Якщо дані зміняться, то і дайджест, також зміниться.

Позначимо хеш-функцію через H, вихідні дані – через *T*, вхідні дані – через *T'*. Контроль цілісності даних зводиться до перевірки рівності[5]:

$$H(T') = H(T).$$

Якщо воно виконано, вважається, що $T' = T$.

Збіг дайджестів для різних даних називається колізією – $H(T) = H(Y)$. Колізіїможливі, оскільки потужність множини дайджестів менше, ніж потужність безлічі даних, що підлягає хешуванню. Однак те, що H –одностороння функція, означає, що за прийнятний час спеціально організувати колізію неможливо.

SHA-1, SHA-2 і SHA-3 –це сімейство криптографічних хеш-функції, які відносяться до алгоритмів безпечного хешу (“Secure hash algorithms”)[6]. Вони відрізняються між собою довжиною хеш-суми, яка покращує стійкість до атак. В SHA-1 це 160 бітів, в SHA-2 це 256 бітів і в SHA-3 це 512 бітів, крім довжини хеш-суми у них також різні внутрішні дизайни. Метод контролю цілісності зображення, який пропонується в даній роботі буде використовуватиSHA-1 з довжиною хеш-значення 160 бітів, через наступні переваги:

- складність генерування хеш-суми протягом найближчих років буде неприступною для підбору хеш-суми методом «грубої сили»: завдання знаходження колізій вимагає $2^{160/2} = 2^{80}$ операцій, а завдання знаходження прообразу - початкового повідомлення - по його хешу, вимагає $2^{160/2}$ операцій[7],
- впроваджувальна кількість бітів є оптимальною, тому що лише 160 бітів будуть змінені і це буде збільшувати помилку другого роду для статичних аналізаторів, так як вони залежать від кількості змінених бітів у зображенні.

Стеганографічні методи, що діють в частотної області, зазвичай ховають дані в коефіцієнтах ортоганального перетворення контейнера. Для цього найчастіше

використовуються перетворення, що застосовуються в сучасних алгоритмах стиснення з втратами (дискретне косинусне перетворення в стандарті JPEG і вейвлет-перетворення - в JPEG2000). Розглянемо докладно алгоритм стиснення зображення JPEG на рисунку2.

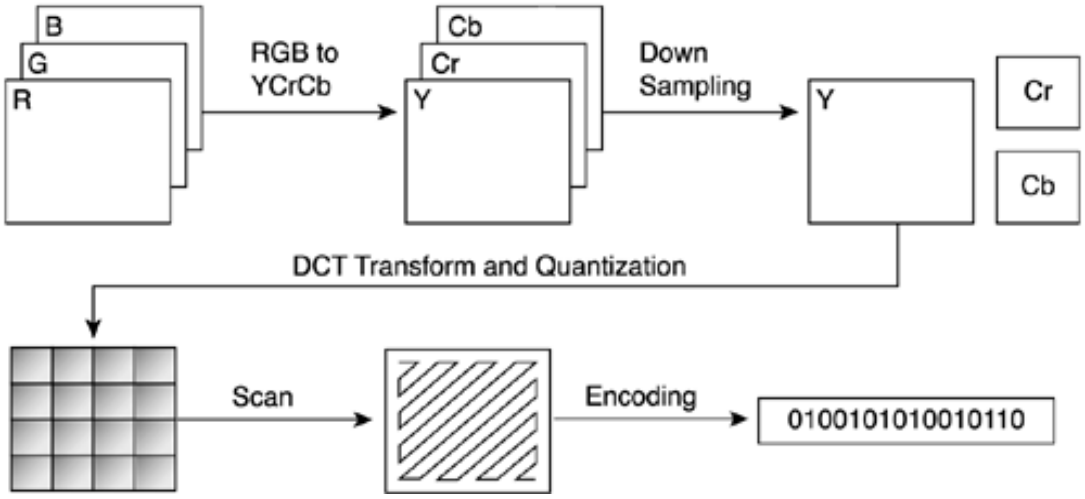


Рис. 2. Алгоритм стиснення зображення формату JPEG

У цьому алгоритмі зображення перетворюється з колірного простору RGB в YCbCr, де Y – компонента яскравості, а Cb і Cr - компоненти кольоровості. Тому важливіше зберегти більшу точність при передачі Y, ніж при передачі Cb і Cr. Значення каналів розбиваються на блоки 8x8. Кожен блок піддається дискретному косинусному перетворенню (ДКП)[8]. Таким чином, при перетворенні виходить матриця, елементи якої відповідають інтенсивності різних просторових частот вихідного блоку. Для кожного елемента матриці дискретного косинусного перетворення існує відповідний елемент матриці квантування. Отримуємо матриця розподілом кожного елемента матриці дискретного косинусного перетворення на відповідний елемент матриці квантування і наступним округленням результату до найближчого цілого числа. Отримана матриця перетворюється в 64-елементний вектор таким чином, що на початку вектора розташовуються коефіцієнти матриці, що відповідають низьким частотам, а в кінці - високим. Отриманий вектор згортається за допомогою алгоритму групового кодування RLE[9], а потім кодується кодами Хаффмана.

Для того щоб записати хеш-суму в зображення спочатку необхідно вибрати для впровадження такі ДКП-компоненти блоків зображення, які будуть найменш помітні. Для того що б їх визначити ми будемо використовувати псіховізуальну модель JPEG, яка заснована на особливостях сприйняття зображень людиною. Зазвичай використовується грубе квантування високочастотної складової зображення і більш акуратне квантування низькочастотної складової, знижуючи тим самим точність передачі різких переходів яскравості і відтінків кольору.

На основі матриці квантування, ми створюємо матрицю індексів, в якій ставимо у відповідність кожному з компонентів ДКП індекс прихованості цього компонента. Таким чином ми отримаємо вектор з цих індексів і їх розташування, вибираємо 160 елементів з найбільшими індексами прихованості, щоб записати хеш-суму.

Основні кроки можна побачити на рисунку 3:

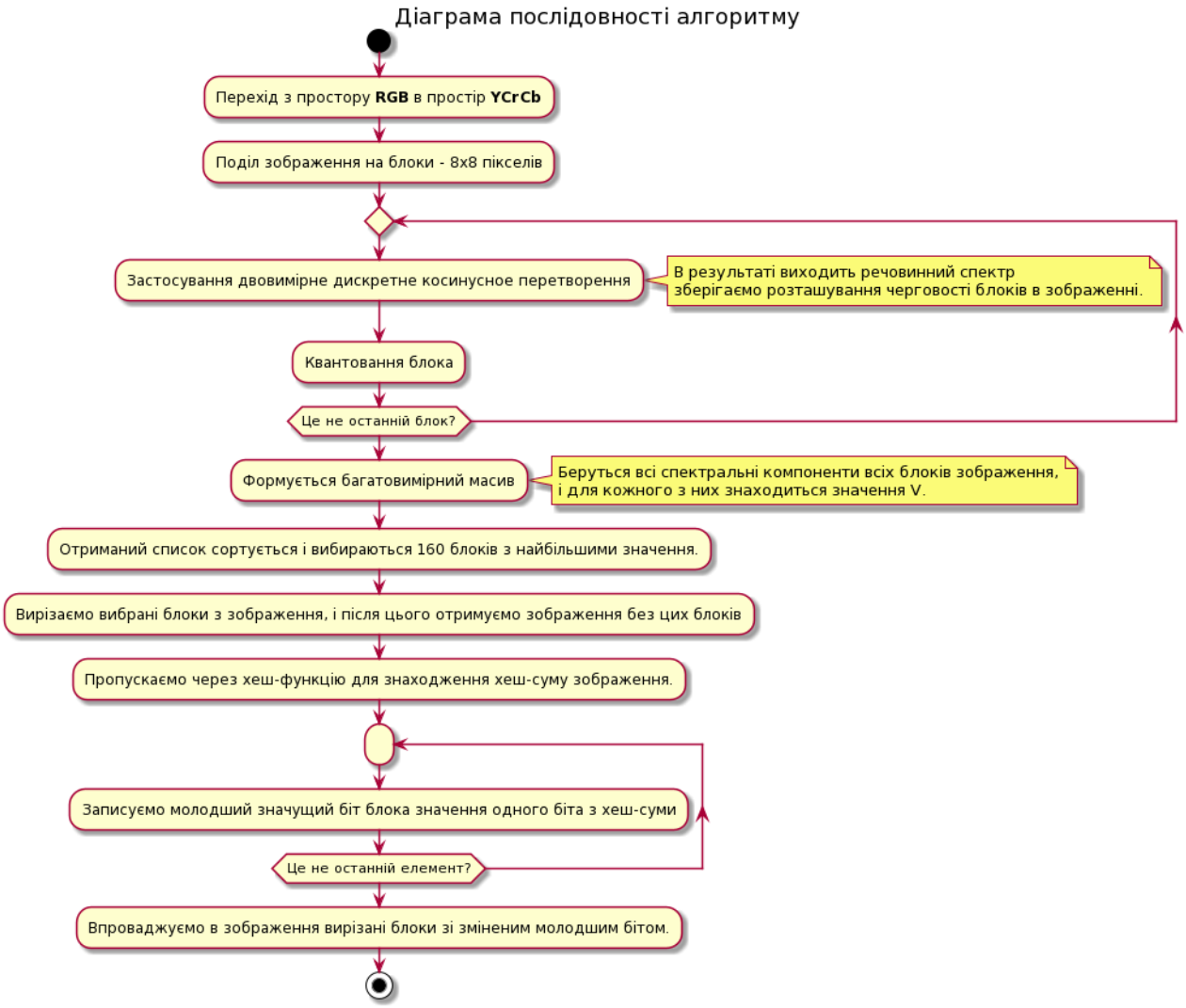


Рис. 3. Алгоритм методу контролю цілісності зображення.

Основні кроки розробленого методу контролю цілісності зображення.

Крок 1. Перехід з простору RGB в простір YCrCb.

Крок 2. Поділ зображення на блоки - 8x8 пікселів.

Крок 3. До кожного блоку застосовується двовимірне дискретне косинусное перетворення. В результаті виходить речовинний спектр.

Крок 4. Сформовані блоки піддаються квантуванню. Далі з них формується багатовимірний масив.

Таким чином, беруться всі спектральні компоненти всіх блоків зображення, і для кожного з них знаходиться значення прихованості. Отриманий список сортується і вибираються 160 блоків з найбільшими значеннями.

Крок 5. Вирізаємо вибрані блоки з зображення, пам'ятаючи їх місце розташування тачерговість блоків в зображенні і після цього отримуємо зображення без цих блоків, яке пропускаємо через хеш-функцію для знаходження хеш-суми зображення.

Крок 6. Знаючи черговість блоків записуємо в кожен молодший значущий біт блока значення одного з бітів хеш-суми. Таким чином ми впроваджуємо хеш-суму в зображення в найбільш непомітні місця.

Крок 7. Додаємо назад змінені вирізані блоки в зображення.Завершується стиснення зображення.

Виконаємо тестування та аналіз результатів роботи розробленого методу. Для експерименту було обрано зображення з роздільною здатністю 340x487 пікселів (рис. 4(а)). Зображення-результат наведені на рисунку 4(б).

а

б

Рис. 4. Порівняння оригінального та результуючого зображень: а – оригінальне зображення; б – зображення з вбудованим ЦВЗ

Як видно, на перший погляд, зображення ідентичні. Однак, при виділенні і посилення різниці між зображеннями, можна помітити незначні, відмінності (рис. 5).

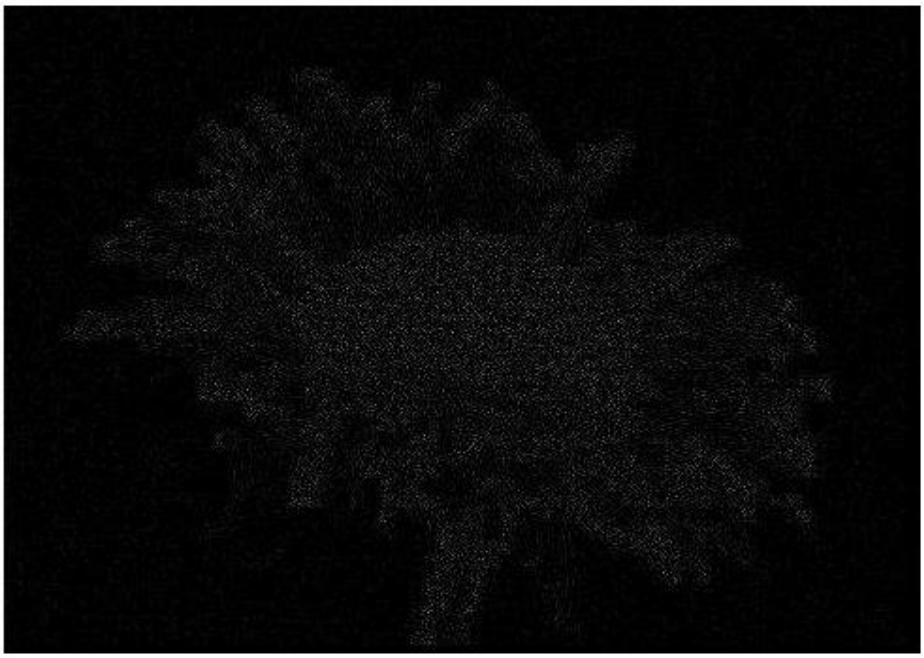


Рис. 5. Різниця між зображеннями

Програмна реалізація запропонованого методу здійснювалася в середовищі Python IDLE.

Для оцінки якості зображення використаємо такі об'єктивні критерії як середньоквадратичний критерій (MSE) та співвідношення «сигнал/шум» - SNR.Для експерименту буде використовуватися група з 10-ти зображень в яких був вже введений

значення хешу. Значенням критерії оцінки буде медіана для цих зображень. MSE для цих зображень складає 3.676. Параметр SNR дозволяє провести аналіз рівня спотворень, які вносяться в контейнер під час приховування в ньому інформації. SNR для цих зображень складає 18.410.

Так само зрівняємо MSE та SNRдля групи початкових зображення в яких не було введено значення хешу. Зменшимо коефіцієнти компресії на 10% від початкової. MSE для цих зображень складає 4.012, SNR – 17.203.

Висновки

У роботі розглянуті основні методи контролю цілісності зображень на основі хеш-значення та проведено їх аналіз. Наведені основні принципи формування зображень формату JPEG. Розроблено метод контролю цілісності зображення на основі цифрового водяного знаку, який використовує у якості ідентифікатора цілісності хеш-значення, отримане шляхом застосування функції SHA-1 до оригінального зображення. На етапі перед вбудовуванням проводиться аналіз статистики зображення з метою пошуку найбільш вдалих місць для вбудовування. Таким чином, впроваджене хеш-значення залишається непомітнім для людського ока.

Список літератури

1. Грібунін В.Г. Кайданів І.М., Туринців І.В. Цифрова стеганографія. Москва: Солон-Прес, 2009. 272 с.
2. Yang C.N., Lin C.C., Chang C.C. Steganography and Watermarking. Nova Science Publishers, 2013. 200 p.
3. Таранчук А.А. Гальпер Л.Г. Стеганографічній метод пріховування даних до області частотних перетворень зображення. *Вісник Хмельницького національного університету*. 2009. № 2. С. 197-201.
4. Wang Y., Moulin P. Steganalysis of block-DCT image steganography Urbana, USA: University of Illinois at Urbana-Champaign,2010.172 p.
5. Хеш-функція – картка даних терміну. Українське агентство зі стандартизації. URL:uas.org.ua/ua/bank-danih/natsionalniy-bank-terminiv/znachennya-termina/?term-id=38741.
6. Stevens M., Bursztein E., Karpman P., Albertini A, Markov Y., Katz J., Shacham H. The First Collision for Full SHA-1. 2017. 76c. URL: web.archive.org/web/20180515222208/ http:/shattered.io/static/shattered.pdf.
7. NIST Comments on Cryptanalytic Attacks on SHA-1. URL: csrc.nist.gov/groups/ST/hash/ statement.html.
8. Фисенко В.Т., Фисенко Т.Ю. Компьютерная обработка и распознавание изображений. СПб: Санкт-Петербургский государственный университет информационных технологий, механики и оптики, 2009. 192 с.
9. Haines R.F., Chuang S.L. The effects of video compression on acceptability of images for monitoring life sciences experiments1992. 45c. URL: ntrs.nasa.gov/search.jsp?R=19920024689.

РАЗРАБОТКА МЕТОДА КОНТРОЛЯ ЦЕЛОСТНОСТИ ИЗОБРАЖЕНИЯ НА ОСНОВЕ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

И.С. Чикликчи, А.А. Смагин, Л.В. Нечитайлова, Н.И. Кушниренко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail:infsec2011@gmail.com

Разработка средств и методов защиты информационной целостности документов, в частности цифровых изображений, остается традиционно актуальной задачей. Известность получили методы контроля целостности контента с использованием скрытых цифровых водяных знаков. Целостность здесь может гарантироваться путем хеширования файла. Хеш-суммы изображений могут храниться в отдельной защищенной базе данных. Для удобства работы системы желательно, чтобы хеш или другой модификатор, который гарантирует целостность, был встроен непосредственно в изображение. Подавляющее большинство цифровых фотографий хранится в сжатом виде с использованием алгоритмов группы JPEG. Поскольку алгоритм не хранит точные значения пикселей, добавление цифрового водяного знака (ЦВЗ) в файлы такого типа предусматривает добавление информации в пространстве преобразований, то есть, изменении подлежат квантованные коэффициенты дискретного косинусного преобразования (ДКП), именно те данные, которые остаются неизменными в процессе сжатия изображение. В качестве ЦВЗ выступать хеш-сумма изображения, получаемого путем использования хэш-функции. В алгоритмах, работающих с изображением такого формата, обычно меняются младшие значащие биты (LSB), и информация внедряется последовательно. В данной статье разработан метод контроля целостности изображения на основе цифрового водяного знака, который базируется на встраивании хеш-суммы в менее заметные места изображения и позволяет оценить психовизуальную заметность внедрения. На этапе перед встраиванием проводится анализ статистики изображения с целью выявления наиболее удачных мест для встраивания дополнительной информации. Приведенные результаты вычислительного эксперимента.

Ключевые слова: контроль целостности изображений, дискретное косинусное преобразование, цифровой водяной знак, встраивание секретной информации, хеш-сумма.

DEVELOPMENT OF A METHOD FOR IMAGE INTEGRITY CONTROL BASEDON DIGITAL WATERMARK

I.S. Chiklikchi, A.A. Smagin, L.V. Nechitailova, N.I. Kushnirenko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: infsec2011@gmail.com

The development of tools and methods to protect the information integrity of documents, in particular digital images, remains a traditionally important task. Methods for controlling the integrity of content using hidden digital watermarks have become popular. Integrity here can be guaranteed by hashing the file. Image hashes can be stored in a separate secure database. For the convenience of the system, it is desirable that the hash or other modifier that guarantees integrity, was embedded directly in the image. The vast majority of digital photos are stored in compressed form using JPEG group algorithms. Because the algorithm does not store exact pixel values, adding a digital watermark (DWC) to files of this type involves adding information in the transformation space, in other words, quantized discrete cosine transform coefficients (DCTs) are subject to change, namely those data that remain unchanged during compression. image. The hash sum of the image obtained by using the hash function will act as the CEV. Algorithms that work with an image of this format usually change the least significant bits (LSB), and the information is implemented sequentially. This article develops a method of image integrity control based on a digital watermark, which is based on embedding a hash sum in the least visible places of the image and allows you to assess the psycho-visual visibility of the implementation. At the stage before embedding, the analysis of image statistics is performed in order to identify the most successful places for embedding additional information. The results of a computational experiment are given.

Keywords: image integrity control, discrete cosine transformation, digital watermark, embedding of secret information, hash sum.

DOI 10.15276/imms.v10.no1-2.84
УДК 004. 681.3

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 84-89

ЖИВУЧЕСТЬ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВА

В.А. Хорошко, Ю.Е. Хохлачева, А. Аясрах, А. Аль-Далваш

Национальный авиационный университет,
пр. Любомир Гузар, 1, Киев, 03058, Украина; e-mail: post@nau.edu.ua

В настоящее время стремительно развивающиеся информационные технологии, динамично растущие объемы информации и увеличение ее значимости в жизни современного общества и государства в целом ставит вопрос информационной и кибербезопасности в ряд наиболее актуальных, а проблемам защиты информации и киберзащиты уделяется все большее внимание, что обуславливает растущее количество публикаций по данной тематике во всем мире. Практически все авторы так или иначе считают проблему надежной и живучей системы защиты информации наиболее острой, при этом сама проблема защиты информации и киберзащиты трактуется в широком смысле – как проблема предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования информации и т.п. Влияние случайных факторов на процессы защиты информации делает практически непригодными методы классической теории систем применительно к решению задач создания, организации и обеспечения функционирования системы защиты. Количество (и виды) воздействий и процессов, связанных с несанкционированным (а возможно и случайным) доступом к информации определить практически невозможно. Одним из важнейших вопросов при проектировании и эксплуатации систем защиты информации является вопрос обеспечения и оценки ее живучести. В работе было проведено исследования, которые показали, что критерии вероятностной оценки качества функционирования средств защиты и оценки надежности (живучести) системы защиты в целом можно использовать. К обобщенному процессу защиты применены критерии теории надежности, позволяющие в ходе проектирования и эксплуатации систем защиты оперативно оценивать ее надежность (живучесть, готовность).

Ключевые слова: кибербезопасность государства, живучесть системы защиты, надежность системы защиты, готовность.

Введение

Динамично растущие объемы информации и увеличение ее значимости в жизни современного общества и государства в целом, ставит вопрос информационной и кибербезопасности в ряд наиболее актуальных в настоящее время.

Сегодня проблемам защиты информации и киберзащиты уделяется все большее внимание, чем обусловлено растущее количество публикаций по данной тематике. Практически все авторы так или иначе считают проблему надежной и живучей защиты информации наиболее острой, при этом сама проблема защиты информации и киберзащиты трактуется в широком смысле – как проблема предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования информации и т.п.

Однако, как растущее количество публикаций, ни увеличивающееся число специализированных фирм и организаций, осуществляющих деятельность, так или иначе связанную с кибербезопастностью (которая является составной частью информационной безопасности), не могут не только решить проблему, но и зачастую прийти к согласию по частным вопросам. И объяснить это можно довольно просто – неопределенностью (либо многообразием) исходных для проектирования систем защиты данных: объектов защиты-множество; видов и количества угроз – множество;

пользователей информации (ПИ) и источников информации (ИИ) – множество; возможностей взаимодействий ПИ с ИИ – множество и т.д. Действительно, при проектировании комплексной системы защиты (составной частью, которой является система киберзащиты), связанной с конкретным объектом, можно получить количественную информацию по объектам защиты, ПИ, и ИИ. Но количество (и виды) воздействий и процессов, связанных с несанкционированным (а возможно и случайным) доступом к информации определить практически невозможно. И это неоспоримо, иначе возможным было бы построение абсолютной системы защиты информации, что, как известно, не является возможным.

Основная часть

Таким образом, влияние случайных факторов на процессы защиты информации делает практически непригодными методы классической теории систем применительно к решению задач создания, организации и обеспечения функционирования системы защиты [1, Т.1 С.50, Т.2, С.13].

В условиях конкретной задачи можно попытаться применить эмпирический подход. Однако, он не может претендовать на моделирование абсолютно всех возможных ситуаций, а кроме этого, может быть связан со значительными материальными затратами, неадекватными к стоимости самой защищаемой информации. И здесь незаменимыми оказываются методы теории вероятностей [2, С.25] и теории принятия решений. [3, С.201].

В этом плане работа [4, С.192] является базовой, обобщающей и дающей основы вероятностной модели системы защиты. Анализ преимуществ и недостатков такой модели дает работа [4, С.93]. В ней рассматривается модель, которая привлекательна своей простотой. Причем, для определения показателей защищенности информации достаточно знать вероятностные характеристики дестабилизирующих воздействий на информацию и эффективность функционирования системы защиты. Кроме того, можно делать вывод, что такую модель целесообразно использовать при оценке надежности и живучести системы защиты на этапе проектирования и эксплуатации ее, а также при оперативной оценке возможностей проектируемой и эксплуатируемой системы.

Однако, вероятностные методы могут быть эффективными не только при построении модели самой системы защиты, но и при разработке критериев функционирования средств защиты информации, согласно с работой [5, С.187], качество функционирования определяется вероятностной мерой, значение которой соответствует доверию к конкретному средству защиты со стороны потребителя. Такую оценку можно проводить путем оценки двух показателей- целостности средства защиты и непрерывности обслуживания (вероятность живучести средств защиты в произвольный момент времени и безотказной работы с этого момента в течении заданного интервала). Оценка качества по данным критериям позволяет выбрать оптимальные средства защиты в рамках конкретной задачи.

Предлагаемые критерии можно применять к средствам защиты информации, однако применять их к оценке системы защиты не представляется возможным хотя бы потому, что задачу придется рассматривать в общем, абстрагировавшись от этапов построения конкретной системы защиты и выбора конкретных средств защиты информации.

Несмотря на важность количественной оценки качества, можно утверждать, что одним из важнейших вопросов при проектировании и эксплуатации является именно вопрос обеспечения и оценки живучести системы защиты. Применительно к системе защиты от несанкционированного действия живучесть – это свойство системы защиты обеспечивать защиту от несанкционированных действий в течение заданного

промежутка времени. Под отказом системы защиты понимается обнаружение злоумышленником канала несанкционированных действий к информации [2].

Подход работы [2, С.221], где аналогично теории надежности вычислительных систем в качестве двух важнейших параметров, характеризующих систему защиты, вводятся интенсивность отказов (среднее число возможных отказов в единицу времени α) и время восстановления системы после отказа ($T_в$), является перспективным в плане применения этих критериев и вероятностной модели [4] и в последствии модели [5], которая не имеет недостатков, присущих вероятностным моделям и является более общей.

Итак, согласно [2, С.23], под интенсивностью отказов системы защиты от несанкционированных действий будем понимать интенсивность обнаружения каналов несанкционированных действий по отношению к информации в единицу времени. При расчете надежности и живучести принимаем, что интенсивность отказов постоянная во времени величина. Если предположить, что угрозы несанкционированных действий взаимно независимы и любая *i*-я $(i = 1, 2, ..., I)$ угроза носит катастрофический характер, то интенсивность отказов системы защиты равна сумме интенсивностей угроз несанкционированных действий к соответствующей системе защиты:

$$\lambda = \sum_{i=1}^{I} \lambda_i .$$

Тогда вероятность непрерывной работы системы защиты в течение произвольного интервала времени определяется следующим образом:

$$p(t) = e^{-\lambda \cdot t} .$$

Соответственно, обратная величина интенсивности отказов системы равна среднему промежутку времени между двумя отказами и называется [2, С.315] временем наработки на отказ:

$$T = 1/\lambda .$$

Интенсивность отказов системы определяется различными параметрами, в том числе сложностью исследования механизмов защиты, реализованных в системе, квалификацией злоумышленника, временным интервалом эксплуатации системы защиты.

Второй составляющей надежности системы защиты, как уже отмечалось, является время восстановления. Под этим понятием понимается интервал времени, в течение которого после возникновения отказа системы защиты обнаруженный канал несанкционированных действий на информацию устраняется. Время восстановления характеризуется двумя компонентами: временем установления соответствующего канала несанкционированных действий на информацию разработчиком системы защиты (T_y), и временем внедрения на защищаемый объект исправлений $(T_{ИС})$. Можно принять среднее время восстановления определяющимся средним временем устранения канала несанкционированных действий к информации:

$$T_B = T_y + T_{ИС} .$$

Можно считать в течение всего времени восстановления систему защиты отказавшей, а защищаемый объект – незащищаемым. Однако следует учитывать тот фактор, что живучесть системы защиты не позволяет оставить объект не защищенным. Считается, что выход параметров системы защиты за границы допусков все-таки

обеспечивает какой-то уровень защиты и она противодействует несанкционированным действиям злоумышленников.

С точки зрения теории надежности, эксплуатационные свойства системы защиты могут быть охарактеризованы коэффициентом готовности [2, С.172]:

$$K_r = T / \left(T + T_B\right).$$

Коэффициент готовности характеризует не только долю времени, в течение которого система защиты работоспособна, а вероятность того, что в любой произвольный момент времени система защиты работоспособна.

Для того, чтобы проиллюстрировать смысл такой характеристики, как коэффициент готовности и его связь с временем восстановления, можно рассматривать вопрос следующим образом.

Примем интенсивность обнаружения ошибки, которая может привести к несанкционированным действиям к информации, равной 1 в месяц [5]. В таблице 1 показано изменение коэффициента готовности системы при различных значениях времени восстановления. Полученные результаты наглядно свидетельствуют о том, что, следуя требованиям к надежности системы (определяемым обычно коэффициентом готовности 0,99), время восстановления системы должно определяться часами.

Таблица 1.

Изменение коэффициента готовности системы при различных значениях времени восстановления

Время восстановления	2 недели	1 неделя	3 дня	1 день	12 часов
Коэффициент готовности	0,682	0,811	0,909	0,968	0,984

Теперь рассмотрим два основных критерия оценки надежности (живучести) системы защиты на базе обобщенной модели процесса защиты информации [1,5] и общей модели системы, построенной в [4,5]. Вероятность нейтрализации несанкционированных действий с учетом введенного выше коэффициента готовности системы будет определяться выражением (для системы защиты, обладающей свойствами контроля в обнаружении несанкционированных действий):

$$P_{ЗН} = P_{обн} \cdot K_Г \cdot P_{ФМ} \cdot e^{-\lambda \cdot t} \cdot \left(\left(1 - P_{обх1}\right) \vee \left(1 - P_{обх2}\right) \vee \ldots \vee \left(1 - P_{обхn}\right)\right),$$

где $P_{обн} = 1 - t_{пр} / t_{обн}$ - вероятность обнаружения нарушителя; $t_{пр}$ - время преодоления системы защиты; $t_{обн}$ - время обнаружения злоумышленника; $K_Г$ - коэффициент готовности системы защиты; $P_{ФМ}$ - вероятность отказа системы защиты в результате наступления форс-мажорных обстоятельств; $P_{обхi}$ - вероятность обхода системы защиты по *i*-ому возможному пути ($i = \overline{1,n}$).

Данное соотношение можно использовать и для оценки многозонной или многорубежной системы защиты, тогда по этой формуле будет определяться вероятность предотвращения несанкционированных действий конкретным злоумышленником в конкретном звене или на конкретном рубеже.

Выводы

Проведенные исследования показали, что критерии вероятностной оценки качества функционирования средств защиты и оценки надежности (живучести) системы защиты в целом можно использовать. К обобщенному процессу защиты применены критерии теории надежности, позволяющие в ходе проектирования и эксплуатации систем защиты оперативно оценивать ее надежность (живучесть, готовность).

Список литературы

1. Ленков С.В., Перегудов Д.А, Хорошко В.А. Методы и средства защиты информации: в 2-х томах. К: Арий, 2008.
2. Креденцер Б.П. Расчет показателей надежности технических систем с избыточностью. К: Феникс, 2019. 520 с.
3. Тарасов В.А., Герасимов Б.М., Левик Н.А., Корнейчук В.А. Интеллектуальные системы поддержки принятия решений: теория, синтез, эффективностью. К: МАКНС, 2007. 336 с.
4. Павлов І.М., Хорошко В.О. Проектування комплексних систем захисту інформації. К: ВІТІ – ДУІКТ, 2011. 245 с.
5. Кобозєва А.А., Мачалін І.О, Хорошко В.О. Аналіз захищеності інформаційних систем. К: ДУІКТ, 2010. 316 с.

ЖИВУЧІСТЬ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

В.О. Хорошко, Ю.Є. Хохлачова, А. Аясрах, А. Аль-Далваш

Національний авіаційний університет,
пр. Любомира Гузара, 1, Київ, 03058, Україна; e-mail: post@nau.edu.ua

В даний час стрімко розвиваються інформаційні технології, динамічно зростаючі обсяги інформації і збільшення її значущості в житті сучасного суспільства і держави в цілому ставить питання інформаційної та кібербезпеки в ряд найбільш актуальних, а проблемам захисту інформації і кіберзахисту приділяється все більша увага, що обумовлює зростаюча кількість публікацій з даної тематики у всьому світі. Практично всі автори так чи інакше вважають проблему надійної і живучої системи захисту інформації найбільш гострою, при цьому сама проблема захисту інформації і кіберзахисту трактується в широкому сенсі - як проблема попередження її спотворення або знищення, несанкціонованої модифікації, зловмисної отримання і використання інформації і т.п . Вплив випадкових факторів на процеси захисту інформації робить практично непридатними методи класичної теорії систем стосовно до вирішення завдань створення, організації та забезпечення функціонування системи захисту. Кількість (і види) впливів і процесів, пов'язаних з несанкціонованим (а можливо і випадковим) доступом до інформації визначити практично неможливо. Одним з найважливіших питань при проектуванні і експлуатації систем захисту інформації є питання забезпечення і оцінки її живучості. У роботі було проведено дослідження, які показали, що критерії ймовірнісної оцінки якості функціонування засобів захисту і оцінки надійності (живучості) системи захисту в цілому можна використовувати. До узагальненому процесу захисту застосовані критерії теорії надійності, що дозволяють в ході проектування і експлуатації систем захисту оперативно оцінювати її надійність (живучість, готовність).

Ключові слова: кібербезпека держави, живучість системи захисту, надійність системи захисту, готовність.

STABILITY OF THE STATE CYBER SECURITY SYSTEM

V.O. Khoroshko, Yu.Ye. Khokhlachova, A. Ayasrah, A. Al-Dalwash

National Aviation University,
1, Lubomyr Guzarv Ave, Kyiv, 03058, Ukraine; e-mail: post@nau.edu.ua

Currently, rapidly developing information technologies, dynamically growing volumes of information and the increase in its importance in the life of modern society and the state as a whole puts the issue of information and cybersecurity among the most urgent, and increasing attention is paid to the problems of information security and cyber protection, which leads to a growing number of publications on this topic all over the world. Almost all authors in one way or another consider the problem of a reliable and tenacious information protection system to be the most acute, while the problem of information protection and cyber protection itself is interpreted in a broad sense - as the problem of preventing its distortion or destruction, unauthorized modification, malicious acquisition and use of information, etc. ... The influence of random factors on information security processes makes the methods of classical systems theory practically unsuitable for solving the problems of creating, organizing and ensuring the functioning of a security system. The number (and types) of impacts and processes associated with unauthorized (and possibly accidental) access to information is almost impossible to determine. One of the most important issues in the design and operation of information security systems is the issue of ensuring and assessing its survivability. In the work, studies were carried out, which showed that the criteria for the probabilistic assessment of the quality of the functioning of protection means and the assessment of the reliability (survivability) of the protection system as a whole can be used. The criteria of the theory of reliability have been applied to the generalized process of protection, which make it possible to quickly assess its reliability (survivability, readiness) during the design and operation of protection systems.

Keywords: state cybersecurity, survivability of the protection system, reliability of the protection system, readiness.

DOI 10.15276/imms.v10.no1-2.90
УДК 519.87:004(043)

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 90-99

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПЕРВИЧНОГО ПРЕОБРАЗОВАТЕЛЯ СИГНАЛОВ АКУСТИЧЕСКОЙ ЭМИССИИ И ЕЕ ПАРАМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ

А.Ф. Верлань[1], С.А. Положаенко[2]

[1]Институт проблем моделирования в энергетике НАН Украины,
ул. Генерала Наумова,15, Киев, 02000, Украина; e-mail: a.f.verlan@gmail.com
[2]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sanp277@gmail.com

При обработке сигналов акустической эмиссии (АЭ) в системе контроля с целью исследования диагностических признаков сигналов, статистической обработки результатов измерений, оценки степени опасности различных дефектов конструкций должны обеспечиваться запись и долговременное хранение результатов измерения, а также полученных оценок общей активности АЭ; распределения роста активности по зонам изделия; амплитудного распределения; временных интегральных и спектральных характеристик сигналов. Полную и качественную информационную картину источника АЭ при этом должен обеспечить первичный преобразователь сигналов АЭ, от корректности функционирования которого, в конечном итоге, зависит достоверность оценки исследуемого физического явления, формируемой системой регистрации в целом. В практических приложениях основную диагностическую ценность представляет ряд временных характеристик импульсов АЭ, из которых, прежде всего, наиболее информативным являются: амплитуда, длительность импульса и крутизна его переднего фронта. Информативной, по результатам первичных измерений, также является картина распределения факторов АЭ в изделии, позволяющая делать выводы о возможных механизмах динамических процессов, оценить уровень релаксации напряжений и возможных повреждений, прогнозировать вероятность трещинообразования, а также ухудшения прочностных свойств материала изделия от наличия примесей и продуктов износа. Сложность задачи выбора и разработки способов, программных и аппаратных средств регистрации АЭ-сигналов определяется большим разнообразием принципов организации соответствующих измерительных приборов и систем, недостаточной изученностью явления АЭ и, как следствие, отсутствием общепризнанной концепции АЭ-контроля и диагностики.

Ключевые слова: акустическая эмиссия (АЭ), первичный преобразователь (датчик) сигналов АЭ, математическая модель, параметрическая идентификация математической модели.

Введение

Задача обработки сигналов АЭ возникает в ряде практических приложений, например, при оценке степени опасности различного рода дефектов конструкций с целью исследования диагностических признаков сигналов, а также статистической обработки результатов измерений. Особая роль при этом отводится первичным преобразователям сигналов АЭ (датчикам), которые должны обеспечить полную и достоверную регистрацию как качественных, так и количественных характеристик указанных сигналов.

В известных работах, посвященных вопросам регистрации сигналов АЭ (в том числе и импульсных) [1–3], отмечается, что из временных характеристик последних наиболее информативными являются амплитуда A и длительность T импульса, а также крутизна $S_ф$ его переднего фронта. Кроме того, информативным следует считать

распределение АЭ в элементах деформируемой (или имеющей дефекты, например, трещины) конструкции, которое (распределение) позволяет различать механизмы динамических явлений, оценить темп и масштаб накопления деформаций (разрушений), отличать пластическую деформацию от собственно трещин ηT, отсутствие трещинообразования от скопления неметаллических включений и т.д.

На основе аппроксимации плотности распределения амплитуд, например, усеченным релеевским или экспоненциальным распределениями могут быть предложены новые информативные параметры АЭ [4]. Для характеристик механических дефектов зарождения и развития магистральных трещин используется связь (коэффициент корреляции, в частности) между амплитудой огибающей импульсов АЭ и интервалов между ними. Энергетические и временные параметры физических проявлений АЭ используются во всех акустико-эмиссионных системах (примером может служить метод восстановления потока повреждений по сигналам АЭ, разработанный на основе кинетической концепции прочности). Значительное число работ посвящено использованию в акустико-эмиссионных системах спектральных характеристик сигналов АЭ [5]. В частности, одной из самых информативных признается спектральная плотность сигналов [5, 6].

Высокое качество регистрации сигналов АЭ обеспечивает возможность формирования диагностического портрета сигнала, который представляет собой определенный набор диагностических признаков, вычисленных либо по дискретным значениям сигнала, поступающего с выхода устройства регистрации сигнала, либо на основе модельных сигналов. Сюда следует включить координаты источника сигнала акустической эмиссии, а также порядковый номер и время регистрации сигнала.

Очевидно, что формируемый датчиком сигнал $y(t)$ должен позволять оценить все из указанных выше характеристик (параметров) первичного сигнала АЭ $x(t)$. При этом, в максимальной степени обеспечить желаемые качественные показатели датчику сигналов АЭ можно в ходе математического моделирования, задавшись тем или иным критерием.

Цель работы

Формирование математической модели (ММ) первичного преобразователя сигналов АЭ, обеспечивающей адекватное представление исходного акустического воздействия $x(t)$ в виде выходного отклика $y(t)$ в условиях ограничений на вычислительные ресурсы при ее численной реализации.

Основная часть

Математическая модель первичного преобразователя. Первичный измерительный преобразователь (датчик) можно рассматривать как динамическую систему и применять для его описания, анализа и моделирования соответствующий математический аппарат. Будем рассматривать класс линейных и стационарных первичных преобразователей (датчиков). На этом основании, в качестве (ММ) первичного преобразователя, можно использовать обыкновенное линейное дифференциальное уравнение (ОДУ) с постоянными коэффициентами и соответствующими начальными условиями (НУ)

$$\sum_{i=0}^{n}\alpha_i \frac{d^i}{dt^i} y(t) = \sum_{j=0}^{m} b_j \frac{d^j}{dt^j} x(t); \quad n \ge m, \frac{d^i}{dt^i} y(0) = 0; \quad i = 0,...,n-1; \quad \alpha_0 = 1, \tag{1}$$

где $x(t)$ – входной, а $y(t)$ – выходной сигналы; t – независимая координата времени; α_i, b_i – постоянные коэффициенты, которые являются параметрами ММ датчика, причем, по известным параметрам α_i, b_i можно произвести качественную и количественную оценку свойств датчика.

Представление ММ в виде эквивалентных интегральных уравнений во многих случаях повышает эффективность их компьютерной реализации. Представим дифференциальное уравнение (1) в области изображений по Лапласу:

$$\sum_{i=0}^{n}\alpha_i p^i Y(p) = \sum_{j=0}^{m} b_j p^j X(p) \text{ или } \sum_{i=0}^{n}\alpha_{n-i} p^{-i} Y(p) = \sum_{j=0}^{m} b_{n-j} p^{-j} X(p), \tag{2}$$

$$\alpha_0 = 1,\ b_j = 0, \text{ при } j > m.$$

Умножение изображения функции на p^{-1} соответствует операции ее интегрирования в области оригиналов, а умножение изображения функции на p^{-i} соответствует i-кратному интегрированию в области оригиналов. С другой стороны, произведению изображений двух функций соответствует, их свертка в области оригиналов. В частности, изображению p^{-i} соответствует функция-оригинал $\left\{\left(t^{n-1}\right)/\left[(n-1)!\right]\right\}$ [7]. Таким образом, (2) можно представить в области оригиналов в виде:

$$\alpha_n y(t) + \sum_{i=1}^{n}\frac{\alpha_{n-i}}{(i-1)!}\int_0^t (t-s)^{i-1} y(s)\,ds = b_n x(t) + \sum_{j=1}^{m}\frac{b_{n-j}}{(j-1)!}\int_0^t (t-s)^{j-1} x(s)\,ds, \tag{3}$$

$$\alpha_0 = 1,\ b_j = 0, \text{ при } j > m.$$

Дифференциальному уравнению (1) в области изображений соответствует понятие дробно-рациональной передаточной функции [8], которая, для рассматриваемого случая примет вид:

$$W(p) = \frac{Y(p)}{X(p)} = \frac{\sum_{j=0}^{m} b_j p^j}{\sum_{i=0}^{n}\alpha_i p^i}, \quad n \ge m. \tag{4}$$

Дробно-рациональную передаточную функцию (4) можно представить в виде суммы элементарных дробей [8], применив, например, метод неопределенных коэффициентов [9]:

$$W(p) = k_1 + (1-k_1)\left(\sum_{g=1}^{r}\sum_{\alpha=1}^{\mu g}\frac{k_{g,\alpha}}{\left(T_g p+1\right)^{\alpha}} + \sum_{\nu=1}^{u}\frac{p k_{\nu,1} + k_{\nu,0}}{\left(T_{\nu,2}p^2 + T_{\nu,1}p + 1\right)}\right), \tag{5}$$

где k_1, $k_{g,\alpha}$, $k_{\nu,1}$, $k_{\nu,0}$ – вещественные коэффициенты; T_g – постоянные времени инерционных звеньев; $\sqrt{T_{\nu,2}}$ – периоды колебаний; $T_{\nu,1}$ – постоянные времени затухания колебательных звеньев (T_g, $T_{\nu,1}$, $T_{\nu,2}$ определяются корнями полинома знаменателя дробно-рациональной передаточной функции); r – число простых корней полинома; μ_g – кратность g-го корня, u-число комплексно-сопряженных корней полинома.

Переходя в (3.5) от изображений к оригиналам, получим аналитическое выражение интегральной динамической модели в форме интегрального уравнения Вольтеры II рода относительно выходного сигнала:

$$y(t)=k_1x(t)+(1-k_1)\int_0^t K(t-s)x(s)ds \tag{6}$$

с ядром (весовой функцией) вида

$$K(t)=\sum_{g=1}^{r}\frac{1}{T_g}\exp\left(-\frac{t}{T_g}\right)\cdot\sum_{\alpha=1}^{\mu g}\frac{k_{g,\alpha}}{(\alpha-1)!}\left(\frac{t}{T_g}\right)^{\alpha-1}+$$
$$+\sum_{\nu=1}^{u}\frac{1}{T_{\nu,1}}\exp\left(-\frac{t}{T_{\nu,1}}\right)\cdot\left(k_{s,\nu}\sin\left(\frac{2\pi\nu t}{T_\nu}\right)+k_{c,\nu}\cos\left(\frac{2\pi\nu t}{T_\nu}\right)\right), \tag{7}$$

где $k_{s,\nu}$, $k_{c,\nu}$, $T_\nu=T_{0;2}^{1/2}$ аналитически связаны с $k_{\nu,1}$, $k_{\nu,0}$, $T_{\nu,1}$, $T_{\nu,2}$.

Процесс разложения дробно-рациональной функции на элементарные дроби включает в себя поиск корней полинома знаменателя для определения постоянных величин, составление и решение системы литейных алгебраических уравнений (СЛАУ) для определения весовых коэффициентов. Интегральная модель с весовой функцией вида (7) соответствует представлению линейной стационарной динамической системы комбинацией масштабных, инерционных, колебательных и других звеньев. Из условия физической реализуемости системы ($K(t-s)=0$ при $s>t$) и состояния покоя до момента времени $t_0\left(y(t)=0 \text{ при } t<t_0\right)$ следует, что $k_1=0$. Параметры α_i, b_j дробно-рациональной передаточной функции $W(p)$ (4) соответствуют параметрам аналитического выражения весовой функции $K(t)$.

Акустические датчики являются динамическими системами с колебательными звеньями [10]. Поэтому, с учетом $k_1=0$ весовая функция интегральной динамической модели акустического датчика имеет вид

$$K(t)=\sum_{\vartheta=1}^{u}\frac{1}{T_{\vartheta,1}}\exp\left(-\frac{t}{T_{\vartheta,1}}\right)\cdot\sum_{\beta=1}^{\nu\vartheta}\left(\frac{t}{T_\vartheta}\right)^{\beta}\cdot\left(k_{s,\vartheta,\beta}\sin\left(\frac{2\pi\nu t}{T_\vartheta}\right)+k_{c,\vartheta,\beta}\cos\left(\frac{2\pi\nu t}{T_\vartheta}\right)\right).$$

Для исследования акустических датчиков применяются упрощенные модели [6] в пределах допустимой погрешности. Например, для заданной переходной функции акустического датчика вида

$$V(t) = A\left(1 - \exp\left(-\frac{t}{T_\vartheta}\right)\cos(\omega t + \phi)\right),$$

где A – масштабный коэффициент, $T_{v,1}$ – постоянная времени затухания колебательного процесса, ω — угловая частота, ϕ – начальный сдвиг фазы – импульсная переходная (весовая) функция в модели (6) может быть записана следующим образом:

$$K(t) \equiv V'(t) = A\exp\left(-\frac{t}{T_\vartheta}\right)\cdot\left(\frac{1}{T_\vartheta}\cos(\omega t + \phi) + \omega\sin(\omega t + \phi)\right). \tag{8}$$

Использование модели с ядром вида (8) позволяет исследовать колебательные системы без привлечения больших вычислительных ресурсов.

Для повышения устойчивости модели (6) при $k = 0$ вводится малый регуляризирующий параметр [6]. Тогда модель (6) будет иметь вид:

$$\alpha x(t) + \int_0^t K(t-s)x(s)ds = y(t) \tag{9}$$

Для удобства компьютерного моделирования представим (8) в дискретной форме (в виде решетчатой функции):

$$K(nh) \equiv A\exp\left(-n\frac{h}{T_\vartheta}\right)\cdot\left(\frac{1}{T_\vartheta}\cos(n\omega h + \phi) + \omega\sin(n\omega h + \phi)\right), \tag{10}$$

где h – шаг дискретизации независимой переменной. Воспользовавшись таблицей Z-преобразований [7], определяем Z-изображение модели (9) с учетом (10):

$$Y(z) = X(z)\cdot A\left(\frac{h}{T_\vartheta}\frac{z^2\gamma^{-2}\cos\phi - z\gamma^{-1}\cos(\beta - \phi)}{z^2\gamma^{-2} - 2z\gamma^{-1}\cos\beta + 1} + \right.$$

$$\left. + h\omega\frac{z^2\gamma^{-2}\sin\phi + z\gamma^{-1}\sin(\beta - \phi)}{z^2\gamma^{-2} - 2z\gamma^{-1}\cos\beta + 1} + \alpha\right),$$

где $\beta = \omega h$, $\gamma = \exp\left(-\frac{h}{T_\vartheta}\right)$.

После проведения алгебраических преобразований получаем разностную схему моделирования колебательной системы:

$$y_n = 2\gamma\cos\beta y_{n-1} - \gamma^2 y_{n-2} + A\left(\left(\frac{h}{T_\vartheta}\cos\phi + h\omega\sin\phi\right)x_n + \right. \tag{11}$$

$$+\left(h\omega\sin\left(\beta-\phi\right)-\frac{h}{T_{\vartheta}}\cos\left(\beta-\phi\right)-\alpha\cos\beta\right)\gamma x_{n-1}+\alpha\gamma^{2}x_{n-2},$$

где $y_i = y\left(ih\right)$, $x_i = x\left(ih\right)$.

Разностная модель более удобна для компьютерной реализации и, кроме того, естественным образом учитывает «предысторию» входного сигнала, в отличие от прямой дискретизации.

Идентификация характеристик первичного преобразователя. Для адекватного моделирования динамической системы необходимо знание параметров $\alpha_i\left(i=1...n\right)$, $b_j\left(j=1...m\right)$ ее ММ (1). Для модели акустического датчика (11) параметры α_i, b_j однозначно определяют характеристики колебательной системы A, $T_{\vartheta,1}$, ω, ϕ. Для определения значений параметров воспользуемся одним из методов идентификации.

Методы идентификации характеристик датчиков можно разделить на три группы: временные, частотные и статистические. Использование методов двух последних групп, как правило, требует использования дорогостоящей прецизионной аппаратуры и продолжительного времени проведения эксперимента (например, для сбора необходимых статистических данных). Во многих практических случаях для оценки динамических характеристик датчиков оказывается вполне достаточно зарегистрировать одну реализацию реакции датчика на широкополосной входной сигнал, например, прямоугольный импульс (т.е. суть весовую функцию [8, 9]).

Определение параметров весовой функции элемента системы, обычно [8] осуществляют путем решения задачи интерпретации кривых переходных процессов, вызванных детерминированными входными тестовыми сигналами.

Чрезвычайно важной является задача оценки параметров передаточной функции при построении корректирующих устройств, для компенсации искажений, вносимых измерительными преобразователями (датчиками). Довольно часто может возникать необходимость в повторной идентификации датчика в связи с его старением или изменением условий эксплуатации. Это обстоятельство обуславливает целесообразность построения компактных специализированных устройств для идентификации характеристик первичных преобразователей.

Для однозначного определения линейного стационарного объекта необходимо знать конкретные величины параметров его ММ: α_i, b_j (для случая дробно-рациональной передаточной функции вида (3.4)). Параметры α_i, b_j $\left(i=0,...,n,\ j=0,...,m\right)$ определяются путем анализа отклика системы $y\left(t\right)$ на детерминированное входное воздействие $x\left(t\right)$.

Экспериментально можно зафиксировать сигналы $x\left(t\right)$ и $y\left(t\right)$ в $n+m+1$ различные моменты времени, что позволяет сформировать СЛАУ относительно неизвестных параметров α_i, b_j:

$$\sum_{i=0}^{n}\alpha_i\frac{d^i}{dt^i}y\left(t_k\right)-\sum_{j=0}^{m}b_j\frac{d^j}{dt^j}x\left(t_k\right)=0,\ k=1,...n+m+1,\ \alpha_0=1,\ n\geq m. \qquad (12)$$

Для формирования СЛАУ (12) по экспериментальным данным $x\left(t_k\right)$, $y\left(t_k\right)$ необходимо численно определять производные высших порядков. Известные алгоритмы характеризуются большим числом операций и невысокой точностью, что практически исключает возможность прямого использования (12) для идентификации.

Более эффективные алгоритмы идентификации можно получить, используя в области оригиналов эквивалентные математические модели в виде интегральных уравнений, в частности, в свертках со степенными рядами (3). Экспериментально зафиксировав не менее $k=1,...,n+m+1$ значений входного $x(t_k)$ и выходного $y(t_k)$ сигналов в различные моменты времени можно получить СЛАУ относительно неизвестных (искомых) параметров α_i, b_j:

$$\alpha_n y(t_k)+\sum_{i=1}^{n}\frac{\alpha_{n-1}}{(i-1)!}\int_0^{t_k}(t_k-s)^{i-1}y(s)ds-b_n x(t_k)-\sum_{j=1}^{n}\frac{b_{n-j}}{(j-1)!}\int_0^{t_k}(t_k-s)^{j-1}x(s)ds=0, \tag{13}$$

$$\alpha_0=1,\ \text{при}\ j>m,\ n\geq m;\ k=1,...,n+m+1.$$

В случае переменного шага дискретизации времени для вычисления свертки можно воспользоваться свойством разделяемости степенного разностного ядра, осуществляя разделение свертки на простые интегралы по одной переменной интегрирования путем представления степенного разностного ядра в виде биномиального многочлена. Однако такой алгоритм может потребовать дополнительные вычислительные ресурсы, так как предполагает вычисление линейных комбинаций степенных функций с существенно различными величинами аргументов.

С точки зрения более экономичной аппаратурной реализации целесообразно вычислять эквивалентные свертке кратные интегралы:

$$\int_0^t\ldots\int_0^t b(t)\,dt^n=\frac{1}{(n-1)!}\int_0^t(t-s)^{n-1}b(s)ds.$$

Тогда (13) запишется в виде:

$$\alpha_n y(t_k)+\sum_{i=1}^{n}\alpha_{n-1}\int_0^{t_k}\ldots\int y(s)ds^n-b_n x(t_k)-\sum_{j=1}^{m}b_{n-j}\int_0^{t_k}\ldots\int x(s)ds^n=0,$$

$$\alpha_0=1,\ b_j=0\ \text{при}\ j>m,\ n\geq m;\ k=1,...,m+n+1.$$

Одним из существенных достоинств интегральных методов идентификации является получение искомых параметров в явном виде, удобном для количественного анализа. Кроме того, найденные параметры инвариантны относительно шага дискретизаций. Важным достоинством интегральных методов является их высокая устойчивость, обусловленная усреднением (сглаживанием) высокочастотных помех при вычислении кратных интегралов. С другой стороны, точность интегрального метода ограничивается методической погрешностью численного интегрирования.

Интегральный метод идентификации дает возможность получить коэффициенты дробно-рациональной передаточной функции (4) динамической системы, которые используются для анализа динамики исследуемых процессов. Разложение передаточной функции (3.4) на элементарные дроби (5) позволяет легко переходить от изображений к оригиналам. Разложение дробно-рациональной передаточной функции на простые дроби можно осуществить, например, воспользовавшись методом неопределенных коэффициентов [8]. После разложения можно получить передаточную функцию в форме простых дробей вида (5), причем коэффициенты дробей, определяющие характеристики отдельных звеньев ММ динамической системы,

определяются найденными в процессе идентификации коэффициентами α_i, b_j дробно-рациональной передаточной функции (4).

Выводы

Получена ММ первичного преобразователя сигналов акустической эмиссии (датчика) в виде интегрального уравнения Вольтерры II рода. Отличительной особенностью данной модели является ее очевидный физический смысл с представлением в виде весовой функции измеряемого акустического сигнала, а также простота компьютерной реализации при относительно невысоких вычислительных затратах. Кроме того, предложенная ММ легко может быть записана в терминах теории автоматического управления в форме передаточной функции, что позволяет, с одной стороны, исследовать ее с привлечением хорошо разработанного обширного аналитического аппарата указанной теории, а с другой – в удобной форме применять при синтезе соответствующих систем регистрации и управления.

Разработана действенная процедура параметрической идентификации предложенной ММ первичного преобразователя акустической эмиссии, цель которой состоит в определении постоянных коэффициентов исходного ОДУ, описывающего динамическое поведение первичного преобразователя. Процедура сводится к вычислению кратных интегралов, эквивалентных свертке изображений входного сигнала первичного преобразователя и отклика на него в области оригиналов.

Корректность предложенной ММ первичного преобразователя подтверждена решениями ряда тестовых задач, показавших отклонение от реальных измерений не более чем на $(3...5)\%$, что вполне допустимо при построение практических систем регистрации сигналов акустической эмиссии.

Список литературы

1. Ермолов И.Н., Алешин Н.П., Потапов А.И. Неразрушающий контроль: в 5 кн. Кн. 2. Акустические методы контроля. Москва: Высшая школа, 1991. 283 с.
2. Андрейкив А.Е., Лысак Н.В. Метод акустической эмиссии в исследовании процессов разрушения. К. : Наукова думка, 1989. 176 с.
3. Baldev R. Fundamentals of acoustic emission. *British Journal of NDT*. 1994. V.36(1).
4. Носов В.В., Бураков И.Н. Использование параметров амплитудного распределения сигналов акустической эмиссии для оценки прочности конструкционных материалов. *Дефектоскопия*. 2004. №3. С. 15-21.
5. Boczar T., Zmarzly D. Analysis of the acoustic emission pulses generated by partial electrical discharges. *Insight*. 2008. V.45(7). P. 488-492.
6. Верлань А.Ф., Горошко И.О., Карпенко Е.Ю., Королев В.Ю., Мосенцова Л.В. Методы и алгоритмы восстановления сигналов и изображений: монография. К: НАН Украины, ИПМЭ им. Г.Е. Пухова, 2011. 368 с.
7. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. Москва: Наука, 1979. 831 с.
8. Бессекерский В.А., Попов Е.П. Теория систем автоматического регулирования. Москва: Наука, 1975. 768 с.
9. Цыпкин Я.З. Теория линейных импульсных систем. Москва: Наука, 1973. 265 с.
10. Гуменюк В.А., Сульженко В.А., Яковлев А.В. Современные возможности и тенденции развития акустико-эмиссионного метода. *В мире неразрушающего контроля*. 2000. V.9(3). С. 8-12.

МАТЕМАТИЧНА МОДЕЛЬ ПЕРВИННОГО ПЕРЕТВОРЮВАЧА СИГНАЛІВ АКУСТИЧНОЇ ЕМІСІЇ ТА ЇЇ ПАРАМЕТРИЧНА ІДЕНТИФІКАЦІЯ

А.Ф. Верлань[1], С.А. Положаєнко[2]

[1]Інститут проблем моделювання в енергетиці НАН України,
вул. Генерала Наумова, 15, Київ, 02000, Україна; e-mail: a.f.verlan@gmail.com
[2]Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sanp277@gmail.com

При обробці сигналів акустичної емісії (АЕ) в системі керування з метою дослідження діагностичних ознак сигналів, статистичної обробки результатів вимірювань, оцінки ступеня небезпеки різних дефектів конструкцій повинні забезпечуватися запис і довготривале зберігання результатів вимірювання, а також отриманих оцінок загальної активності АЕ; розподілу зростання активності по зонам виробу; амплітудного розподілу; тимчасових інтегральних і спектральних характеристик сигналів. Повну і якісну інформаційну картину джерела АЕ при цьому повинен забезпечити первинний перетворювач сигналів АЕ, від коректності функціонування якого, в кінцевому підсумку, залежить достовірність оцінки досліджуваного фізичного явища, що формується системою реєстрації в цілому. У практичних застосуваннях основну діагностичну цінність представляє ряд тимчасових характеристик імпульсів АЕ, з яких, перш за все, найбільш інформативним є: амплітуда, тривалість імпульсу і крутизна його переднього фронту. Інформативною, за результатами первинних вимірювань, також є картина розподілу факторів АЕ у виробі, яка дозволяє робити висновки про можливі механізми динамічних процесів, оцінити рівень релаксації напружень і можливих пошкоджень, прогнозувати ймовірність утворення тріщин, а також погіршення характеристик міцностних властивостей матеріалу виробу від наявності домішок і продуктів зносу. Складність задачі вибору та розробки способів, програмних і апаратних засобів реєстрації АЕ-сигналів визначається значною різноманітністю принципів організації відповідних вимірювальних приладів та систем, недостатньою вивченістю явища АЕ і, як наслідок, відсутністю загальновизнаної концепції акустико-емісійного контролю та діагностики.

Ключові слова: акустична емісія (АЕ), первинний перетворювач (датчик) сигналів АЕ, математична модель, параметрична ідентифікація математичної моделі.

MATHEMATICAL MODEL OF THE PRIMARY CONVERTER OF ACOUSTIC EMISSION SIGNALS AND ITS PARAMETRIC IDENTIFICATION

A.F. Verlan[1], S.A. Polozhaenko[2]

[1]Institute for Modeling Problems in Power Engineering, NAS
15, General Naumov Str., Kyiv, 02000, Ukraine; e-mail: a.f.verlan@gmail.com
[2]Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: sanp277@gmail.com

When processing acoustic emission (AE) signals in the control system in order to study diagnostic signs of signals, statistically process measurement results, assess the degree of danger of various structural defects, recording and long-term storage of measurement results and obtained estimates of the total AE activity, distribution of activity growth over product zones should be provided, amplitude distribution, time integral and spectral characteristics of signals. In this case, a complete and high-quality information picture of the AE source should be provided by the primary converter of the AE signals, the correct functioning of which ultimately determines the reliability of the assessment of the physical phenomenon under study, formed by the registration system as a whole. In practical applications, the main diagnostic value is a number of temporal characteristics of AE pulses, of which, first of all, the most informative are: amplitude, pulse duration, and steepness of its leading edge. According to the results of primary measurements, the picture of the distribution of AE factors in the product is also informative, which makes it possible to draw conclusions about the possible mechanisms of dynamic processes, assess the level of stress relaxation and possible damage, predict the probability of cracking, as well as the deterioration of the strength properties of the product material from the presence of impurities and wear products. The complexity of the problem of choosing and developing methods, software and hardware for recording AE signals is determined by a wide variety of principles for organizing the corresponding measuring instruments and systems, insufficient knowledge of the AE phenomenon and, as a consequence, the lack of a generally recognized concept of AE control and diagnostics.

Keywords: acoustic emission (AE), primary transducer (sensor) of AE signals, mathematical model, parametric identification of the mathematical model.

DOI 10.15276/imms.v10.no1-2.100
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 100-108

ИССЛЕДОВАНИЕ РЕЖИМОВ ШИФРОВАНИЯ С ПРОПУСКОМ БЛОКОВ

А.В. Соколов, А.О. Корж

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: radiosquid@gmail.com

Блочные симметричные шифры являются неотъемлемой частью любой современной комплексной системы защиты информации. Сегодня внимание исследователей сосредоточено на повышении эффективности и быстродействия блочных симметричных шифров, тем не менее, как показывает практический опыт реализации реальных систем шифрования данных, большое значение для обеспечения высокой криптографической стойкости и быстродействия современных систем шифрования имеет также режим шифрования, с помощью которого применяется тот или иной криптографический алгоритм. В настоящей статье предлагаются новые режимы шифрования: с пропуском блоков, а также с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей. Предложенные режимы шифрования позволяют обеспечить экономию примененных в программе операций шифрования данных с помощью блочного симметричного шифра. Для разработанных режимов шифрования вычислены параметры, позволяющие обеспечить высокий уровень стохастического качества, полученного на выходе шифротекста, что подтверждается проведенными испытаниями в соответствии с набором стохастических тестов NIST. При этом установлено, что режим шифрования с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей обеспечивает значительное повышения числа уровней защиты применяемого криптопреобразования, а также показывает наилучшие результаты при прохождении набора стохастических тестов NIST. Разработанные режимы шифрования являются обоснованным решением для использования в приложениях, работающих на платформах с ограниченными вычислительными и энергетическими ресурсами, в первую очередь, на мобильных устройствах. При этом предпочтительным является выбор режима с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей. Отметим также, что представленные режимы шифрования позволяют объединить воедино преимущества блочных симметричных шифров и генераторов псевдослучайных ключевых последовательностей.

Ключевые слова*:* криптография, режим шифрования, блочный симметричный шифр.

Введение

Построение современных систем передачи, обработки и хранения информации сегодня во многом сопряжено с задачами обеспечения её защиты. Одним из важнейших компонентов практически любой системы защиты информации являются блочные симметричные шифры (БСШ) [1].

Стремительное развитие методов криптоанализа, а также наращивание вычислительных мощностей современных компьютеров диктует необходимость совершенствования современных БСШ для повышения их криптографической стойкости, что является основной задачей большинства современных криптографических исследований.

С другой стороны, многие используемые современные вычислительные системы, например, распространенные сегодня мобильные устройства, обладают очень ограниченным уровнем вычислительных и энергетических ресурсов, что накладывает значительные ограничения на разрабатываемые приложения. В частности, желание

разработчиков увеличить быстродействие своих приложений, а также повысить общее время автономности вычислительного устройства зачастую приводит к необходимости отказаться от применения БСШ, например, для передачи файловых вложений большого размера в ущерб кибербезопасности.

Данный аспект практического использования методов криптографии органично ставит перед исследователями не только задачу повышения криптографической стойкости шифров, но и задачу повышения их быстродействия.

В работе [2] была предложена концепция шифрования с переменной фрагментацией блоков, позволяющая значительно снизить количество необходимых итераций основного шага криптопреобразования, таким образом снижая вычислительные затраты на шифрование одного блока входной информации. Данная концепция стала основой для разработки криптографического алгоритма, адаптированного для работы на мобильных устройствах [3]. Тем не менее, практический опыт использования данного БСШ показывает, что даже он достаточно сильно снижает быстродействие приложений при передаче больших файлов. Данный момент приводит к необходимости исследования не только вопросов повышения быстродействия самих БСШ, но и методов их применения к шифруемым данным – режимов шифрования. В частности, актуальным является построение режимов шифрования, в которых небольшие объемы чувствительной информации шифруются с применением режимов шифрования, обеспечивающих высокий уровень криптостойкости, в то время как более значительные объемы менее критичной информации шифруются с применением режимов шифрования, обладающих большим быстродействием.

Цель и задачи

Целью настоящей статьи является разработка режимов шифрования с пропуском блоков.

Для достижения цели статьи необходимо решить следующие задачи:

- разработать новые режимы шифрования с пропуском блоков, которые бы обеспечивали экономию операций применения БСШ при приемлемом уровне качестве шифрования;
- исследовать параметры режимов шифрования с пропусками блоков, обеспечивающие на практике высокий уровень криптографического качества операции шифрования.

Основная часть

Помимо криптографической стойкости самого используемого БСШ, в контексте безопасности и быстродействия применяемого криптографического алгоритма имеет огромное значение также и режим, с помощью которого он применяется к шифруемым данным.

Определение 1 [4]. Режим шифрования – это метод применения блочного шифра (алгоритма), позволяющий преобразовать последовательность блоков открытых данных в последовательность блоков зашифрованных данных.

Простейшим из существующих режимов шифрования является режим Electronic Codebook (ECB), который предусматривает разбиение открытого текста на N блоков, размер каждого из которых определяется параметрами используемого шифра. Далее происходит их последовательное шифрование без установления какой-либо взаимосвязи между ними (рис. 1).

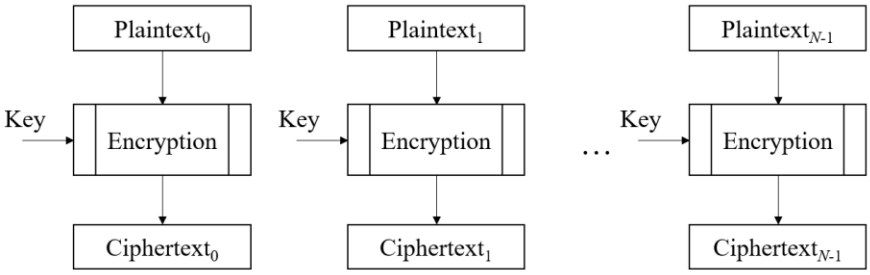
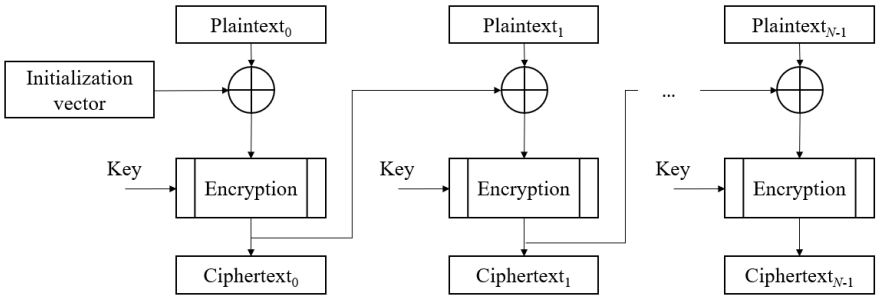


Рис. 1. Схема шифрования в режиме ECB

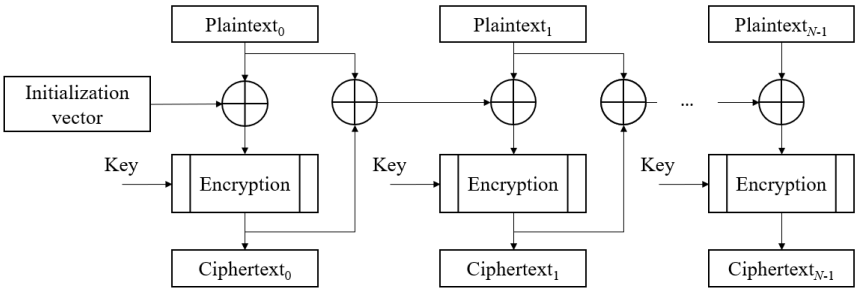
Данный режим шифрования характеризуется крайне низким уровнем криптографического качества при использовании любого, даже самого качественного БСШ, в виду сохранения статистических особенностей блоков открытого текста. Данный режим строго не рекомендуется применять на практике [4].

Отметим также, что классическим подходом к оценке качества криптограмм является использование в отношении них пакета стохастических тестов NIST [5]. Эксперименты показывают, что применение данного пакета тестов к последовательностям, полученным с помощью применения криптоалгоритма AES [6] в режиме ECB приводит к провалу в прохождении указанного пакета стохастических тестов. В частности, рассмотренный пример шифрования файлов показал, что криптограммы не проходят тесты Binary matrix rank test (показатель $P-value = 0.00019$) и Linear complexity test (показатель $P-value = 6.85 \cdot 10^{-6}$).

Следующими, более совершенными режимами шифрования являются режимы сцепления блоков (CBC) и распространяющегося сцепления блоков (PCBC), схемы которых представлены на рисунке 2.



а



б

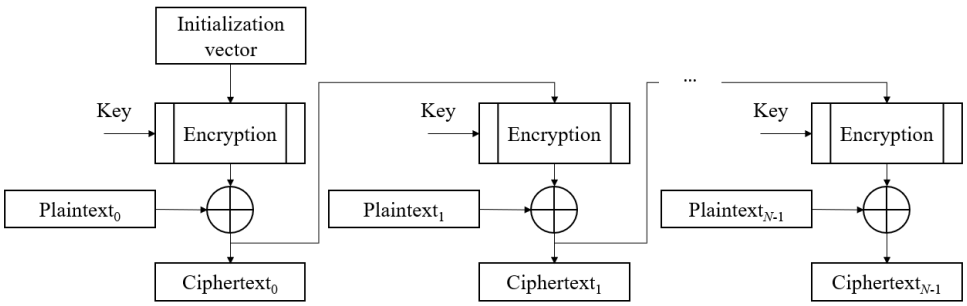
Рис. 2. Режимы шифрования CBC и PCBC: а – режим шифрование CBC; б – режим шифрование PCBC

В данных режимах предусмотрено использование вектора инициализации, который складывается с первым блоком отрытого текста, после чего происходит

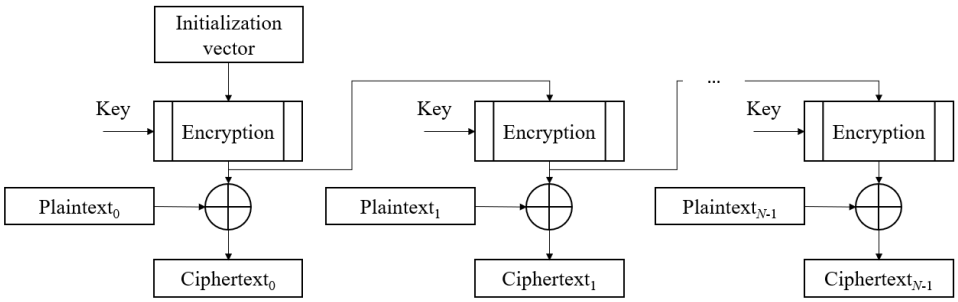
шифрование полученной суммы. Для последующих блоков данный вектор инициализации представляет собой либо предыдущий блок зашифрованного текста (CBC), либо сумму предыдущих блоков зашифрованного и открытого текста (PCBC).

Шифрование данных в представленных режимах обеспечивает высокий уровень криптографического и стохастического качества зашифрованных последовательностей, что экспериментально подтверждается прохождением пакета стохастических тестов NIST.

Еще двумя часто используемыми на практике режимами шифрования являются режим обратной связи по шифротексту (CFB) и режим обратной связи по выходу (OFB), схемы которых представлены на рисунке 3.



а



б

Рис. 3. Режимы шифрования CFB и OFB: а – режим шифрование CFB; б – режим шифрование OFB

Данные режимы предусматривают маскировку входного текста путем сложения его по модулю 2 с результатом шифрования векторов инициализации, в качестве которых используется шифротекст предыдущего блока (CFB) или гамма из предыдущего блока до сложения с вектором открытого текста (OFB). Указанные режимы шифрования также обеспечивают высокий уровень криптографического и стохастического качества получаемых криптограмм, достаточный для прохождения набора стохастических тестов NIST.

Помимо перечисленных основных режимов шифрования существуют и некоторые другие, например, с аутентификацией данных [4].

Отметим, что шифрование во всех перечисленных режимах предполагает применение процедуры шифрования выбранным криптоалгоритмом ко всем без исключения блокам входных данных. Тем не менее, как показывают исследования, данное действие не является обязательным для достижения достаточного уровня криптографического и стохастического качества.

В настоящей работе предлагается модификация перечисленных основных режимов шифрования, позволяющая сократить количество необходимых операций «шифрование блока», необходимых для зашифрования файла. Так, на этапе подготовки

к процедуре шифрования выбираются константы M и C. В начале процедуры шифрования значением 0 инициализируется переменная i. Перед применением блока шифрования выполняется проверка условия $i \bmod M \in \{0,1,...,C\}$ и, если условие ложно – шифрование данного блока не выполняется. По завершении обработки блока значение переменной i увеличивается на 1.

В зависимости от конкретных значений M и C происходит пропуск операции шифрования для того или иного блока открытого текста. Так, например, если $M = 2$ и $C = 0$ происходит пропуск операции шифрования для каждого второго блока открытого текста.

При этом указанная модификация может быть применена к любому из рассмотренных нами режимов шифрования (рис. 1–3). Для краткости изложения материала, в качестве примера мы приводим на рис. 4 схему режима шифрования с пропуском блоков на примере модификации режима CBC.

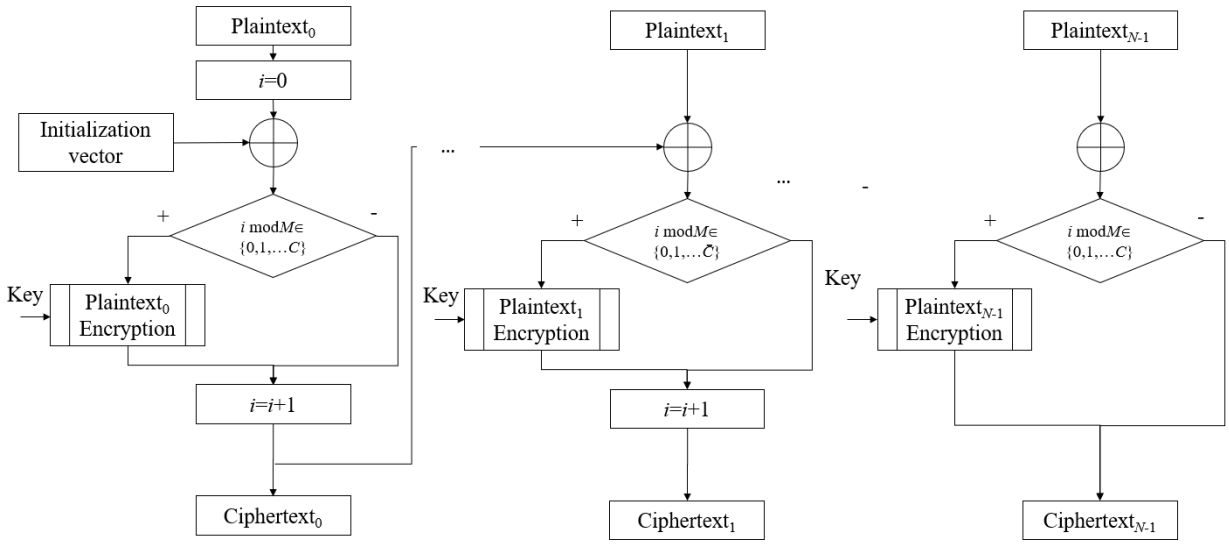


Рис. 4. Модификация режима шифрования CBC с пропуском блоков

При этом схема расшифрования строится аналогично схеме шифрования (рисунке 4).

В настоящей работе были проведены вычислительные эксперименты, в рамках которых шифровались файлы различного размера и содержания с помощью криптоалгоритма AES в различных режимах шифрования с пропуском блоков при различных значениях M и C. После выполнения шифрования к полученным криптограммам применялся набор стохастических тестов NIST.

Полученные в данных вычислительных экспериментах результаты свидетельствуют, что при шифровании информации при значениях $M = 25$ и $C = M - 2$ (данные значения обеспечивают пропуск шифрования каждого 25-го блока отрытого текста) для полученных криптограмм выполняются все стохастические тесты из набора NIST. Таким образом, для реализации операции шифрования файла требуется на $(1/25) \cdot 100\% \simeq 4\%$ меньшее количество блоков шифрования.

Тем не менее, полученного выигрыша в количестве необходимых операций шифрования с помощью БСШ, например, AES может оказаться недостаточно для шифрования крупных файлов.

Далее мы предлагаем еще один режим шифрования (рис. 5), позволяющий значительно сократить необходимое количество блоков шифрования БСШ. Для реализации этой схемы используется такой криптографический примитив как генератор псевдослучайных ключевых последовательностей (ГПКП), который может

быть построен, например, в соответствии со схемами [7] или [8]. При этом быстродействие данных криптографических примитивов значительно превышает быстродействие блочных симметричных криптоалгоритмов [8].

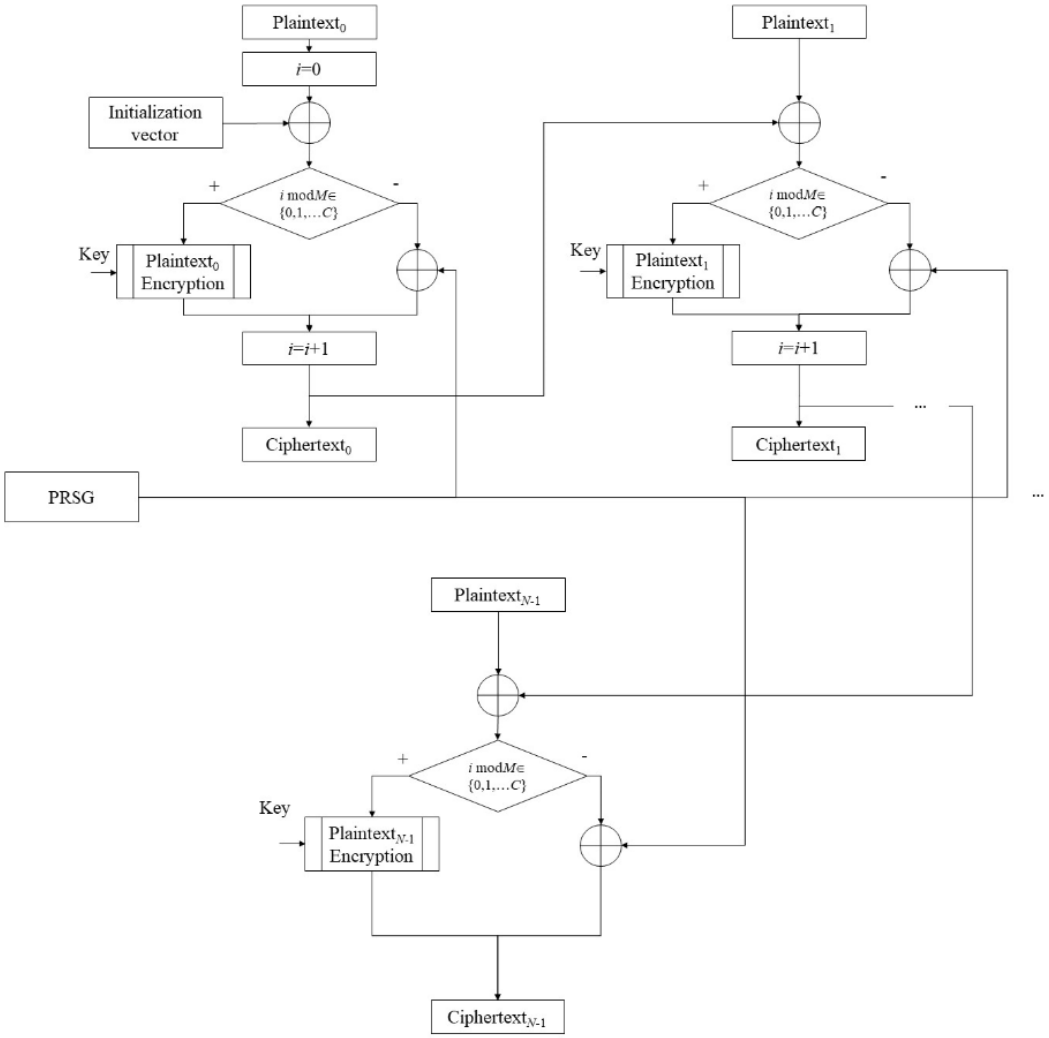


Рис. 5. Режим шифрования CBC с пропуском блоков и применшеним ГПКП

Перед началом операции шифрования выбранная схема ГПКП инициализируется с помощью дополнительного фрагмента ключа. Аналогично модифицированному режиму шифрования с пропуском блоков (рис. 4), в данном режиме шифрования вводятся параметры M и C. В начале процедуры шифрования значением 0 инициализируется переменная i. Перед применением блока шифрования выполняется проверка условия $i \bmod M \in \{0,1,...,C\}$ и, если условие ложно – вместо шифрования данного блока выполняется его гаммирование с помощью очередного сегмента гаммы, полученного с помощью ГПКП. По завершении обработки блока значение переменной i увеличивается на 1.

Отметим, что схема расшифрования строится аналогично схеме шифрования (рис. 5).

Эмпирические исследования показали, что наилучшим образом себя показывает применение данного режима шифрования с режимом CFB, в то время как оптимальными являются значения параметров $M = 2$ и $C = 0$, т.е. сложение с гаммой ГПКП происходит для каждого второго шифруемого блока открытого текста.

Отметим также, что число уровней защиты получившейся схемы определяется произведением числа уровней защиты выбранного БСШ и ГПКП. Например, при

использовании БСШ AES-256 и ГПКП на основе дуальных пар бент-последовательностей [7] общее число уровней защиты получившейся криптографической системы достигает значения $\Psi \simeq 2^{256} \cdot 2^{165} = 2^{421}$, что является очень значительной величиной. Перспективным является также применение генераторов псевдослучайных ключевых последовательностей на основе совершенных алгебраических конструкций многозначной логики [9].

В таблице 1 приведены результаты выполнения стохастических тестов для шифрования исходных данных до шифрования, после шифрования в режимах CFB, CFB с пропуском блоков, CFB с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей.

Таблица 1.

Результаты стохастических тестов NIST

№	Тест	Открытый текст		CFB		CFB с пропуском блоков		CFB с пропуском блоков и ГПКП	
		P-value	Pass rate	P-value	Pass rate	P-value	Pass rate	P-value	Pass rate
1	Monobit test	0	✗	0.71	✔	0.49	✔	0.8	✔
2	Frequency within block test	0	✗	0.4	✔	0.18	✔	0.99	✔
3	Runs test	0	✗	0.7	✔	0.32	✔	0.84	✔
4	Longest run ones in a block test	10^{-191}	✗	0.64	✔	0.31	✔	0.54	✔
5	Binary matrix rank test	0	✗	0.68	✔	0.18	✔	0.7	✔
6	DFT test	0	✗	0.9	✔	0.09	✔	0.96	✔
7	Non overlapping template matching test	0.125	✔	1	✔	0.99	✔	1	✔
8	Overlapping template matching test	0	✗	0.91	✔	0.85	✔	0.84	✔
9	Maurers universal test	0	✗	0.73	✔	0.16	✔	0.38	✔
10	Linear complexity test	10^{-11}	✗	0.22	✔	0.11	✔	0.03	✔
11	Serial test	0	✗	0.25	✔	0.12	✔	0.68	✔
12	Approximate entropy test	0	✗	0.34	✔	0.19	✔	0.9	✔
13	Cumulative sums test	0	✗	0.81	✔	0.34	✔	0.55	✔
14	Random excursion test	0.22	✔	0.2	✔	0.04	✔	0.31	✔
15	Random excursion variant test	0.11	✔	0.1	✔	0.02	✔	0.02	✔

Анализ данных, показанных в таблице 1 позволяет установить высокий уровень стохастического качества криптограммы, полученной в режиме CFB с пропуском блоков и использованием ГПКП.

Выводы

Отметим основные результаты проведенных исследований. В статье предложены новые режимы шифрования: с пропуском блоков, а также с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей. Применение данных режимов шифрования позволяет уменьшить количество применяемых в программе операций шифрования данных с помощью блочного симметричного шифра, что является особенно актуальным для использования в приложениях, работающих на требовательных к вычислительным и энергетическим ресурсам платформах. При этом предпочтительным является выбор режима с пропуском блоков и использованием генератора псевдослучайных ключевых последовательностей.

Для предложенных режимов шифрования вычислены параметры, обеспечивающие высокий уровень стохастического качества криптограмм при оптимальном уровне экономии применяемых в программе операций шифрования данных с помощью блочного симметричного шифра. Так, для режима шифрования с пропуском блоков количество сэкономленных операций шифрования данных с помощью блочного симметричного шифра составляет $\sim 4\%$ и 50% для режима с пропуском блоков и использованием ГПКП.

Число уровней защиты информации в случае применения режима с пропуском блоков и использованием ГПКП составляет $\Psi \simeq 2^{256} \cdot 2^{165} = 2^{421}$, что значительно превосходит число уровней защиты, обеспечиваемых другими режимами шифрования.

Проведенные в статье исследования органично ставят задачу дальнейшего повышения криптографической стойкости и быстродействия генераторов псевдослучайных ключевых последовательностей, в частности, на основе совершенных алгебраических конструкций.

Список литературы

1. Knudsen L.R., Robshaw M. The Block Cipher Companion. Springer, 2011. 284 p.
2. Жданов О.Н., Соколов А.В. Алгоритм шифрования с переменной фрагментацией блока. *Проблемы и достижения в науке и технике: сб. материалов науч.-практ. конф., 1 июня 2015 г.* Омск. 2015. № 2. С. 153-159.
3. Соколов А.В., Корж А.О., Лопуленко О.В. Модифікований алгоритм шифрування зі змінною фрагментацією блоків. *WayScience: матеріали VII міжнародної наук.-практ. конф., 6-7 червня 2019*, Дніпро. 2019. С. 1592-1596.
4. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley. 2015. 784 p.
5. Rukhin A., Soto J., Nechvatal J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology Special Publication. 2010. 131 p.
6. FIPS 197. Advanced encryption standard. 2001. URL: http://csrc.nist.gov/publications/.
7. Мазурков М.И., Соколов А.В., Барабанов Н.А. Генератор ключевых последовательностей на основе дуальных пар бент-функций. *Праці Одеського політехнічного університету*. 2013. №3. С. 150-156.
8. Соколов А.В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов. *Праці Одеського політехнічного університету,* 2014.43(1). С. 180-186.
9. Соколов А.В., Жданов О.Н., Барабанов Н.А. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций. *Проблемы физики, математики и техники*. 2016. V.26(1). С. 85-91.

ДОСЛІДЖЕННЯ РЕЖИМІВ ШИФРУВАННЯ З ПРОПУСКОМ БЛОКІВ

А.В. Соколов, А.О. Корж

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Блокові симетричні шифри є невід'ємною частиною будь-якої сучасної комплексної системи захисту інформації. Сьогодні увага дослідників зосереджена на підвищенні ефективності і швидкодії блокових симетричних шифрів, проте, як показує практичний досвід реалізації реальних систем шифрування даних, велике значення для забезпечення високої криптографічної стійкості і швидкодії сучасних систем шифрування має також режим шифрування, за допомогою якого застосовується той або інший криптографічний алгоритм. У цій статті пропонуються нові режими шифрування: з пропуском блоків, а також з пропуском блоків і використанням генератора псевдовипадкових ключових послідовностей. Запропоновані режими шифрування дозволяють забезпечити економію застосованих в програмі операцій шифрування даних за допомогою блокового симетричного шифру. Для розроблених режимів шифрування обчислені параметри, що дозволяють забезпечити високий рівень стохастичної якості, отриманого на виході шифротекста, що підтверджується проведеними тестами відповідно до набору стохастичних тестів NIST. При цьому встановлено, що режим шифрування з пропуском блоків і використанням генератора псевдовипадкових ключових послідовностей забезпечує значне підвищення числа рівнів захисту застосовуваного криптоперетворення, а також показує найкращі результати при проходженні набору стохастичних тестів NIST. Розроблені режими шифрування є обґрунтованим рішенням для використання в додатках, що працюють на платформах з обмеженими обчислювальними і енергетичними ресурсами, в першу чергу, на мобільних пристроях. При цьому переважним є вибір режиму з пропуском блоків і використанням генератора псевдовипадкових ключових послідовностей. Відзначимо також, що представлені режими шифрування дозволяють об'єднати воєдино переваги блокових симетричних шифрів і генераторів псевдовипадкових ключових послідовностей.

Ключові слова: криптографія, режим шифрування, блоковий симетричний шифр.

STUDY OF BLOCK SKIP ENCRYPTION MODES

A.V. Sokolov, A.O. Korzh

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: radiosquid@gmail.com

Block symmetric ciphers are an integral part of modern complex information security systems. Today, the attention of researchers is focused on increasing the efficiency and performance of block symmetric ciphers. However, it is shown by the practical experience of implementation of data encryption systems, that block cipher modes of operation are also of great importance for the efficiency and performance of encryption systems. In this paper we propose new block cipher modes of operation: with block skipping, as well as with block skipping and the use of pseudo-random key sequence generator. The proposed block cipher modes of operation make it possible to reduce the amount of used in the program data encryption operations (i.e. the amount of the block symmetric cipher runs). For the developed block cipher modes of operation, the parameters are calculated to ensure a high level of stochastic quality of the obtained ciphertext, which is confirmed by the tests carried out in accordance with the NIST stochastic test suite. At the same time, it was found that the block cipher mode of operation with skipping of blocks and the use of a pseudo-random key sequence generator, provides a significant increase in the number of information protection levels of the applied cryptographic transformation, and also shows the best results when passing the NIST stochastic tests suite. The developed block cipher modes of operation are a reasonable solution for use in applications running on platforms with limited computing and power resources, primarily on mobile platforms. In this case, it is preferable to select a block cipher mode of operation with skipping of blocks and use of pseudo-random key sequence generator. Note also that the presented block cipher modes of operation allow to combine the advantages of block ciphers and generators of pseudo-random key sequences.

Keywords: cryptography, encryption mode, block symmetric cipher.

DOI 10.15276/imms.v10.no1-2.109
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 109-118

РАЗРАБОТКА КОНЦЕПЦИИ СОЗДАНИЯ ИНТЕРФЕЙСА ОПЕРАТОРА КОМПЬЮТЕРНО-ИНТЕГРИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ УСТАНОВКАМИ В СООТВЕТСТВИИ С ПРИНЦИПОМ СИТУАЦИОННОЙ ОСВЕДОМЛЕННОСТИ

Ан.А. Стопакевич[1], А.А. Стопакевич[2]

[1]Одесская национальная академия связи,
ул. Кузнечная, 14, Одесса, 65029, Украина; e-mail: stopakevich@gmail.com
[2]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: stopakevich@opu.ua

Важной проблемой, определяющей безопасность функционирования современного автоматизированного производства на основе компьютерно-интегрированных систем управления технологическими установками, является учет психологических аспектов восприятия компьютерных интерфейсов человеком-оператором автоматизированного технологического процесса. Большинство разработанных компьютерных интерфейсов для операторов созданы в соответствии с идеей предоставления максимального количества информации о технологическом процессе. Но, эта идея противоречит основам инженерной психологии, которая акцентирует внимание разработчиков на особенности восприятия информации человеком. С одной стороны, в ситуации стресса, связанного с аварийностью и опасностью производства, оператор не способен проанализировать большой объем информации для принятия верного решения. С другой стороны, длительное наблюдение за мало изменяющимся набором данных о состоянии технологического процесса приводит к деконцентрации внимания оператора, что, в свою очередь, увеличивает вероятность неверного решения в нештатной, аварийной или предаварийной ситуации. Для борьбы с этими явлениями предлагается следовать принципам ситуационной осведомленности при создании компьютерных интерфейсов. Концепция использования указанного принципа при создании ряда интерфейсов компьютерно-интегрированной системы управления ректификационной установкой производства спирта разработана в статье. На основе результатов моделирования необходимой деятельности оператора в аварийных ситуациях разработан многоуровневый графический интерфейс оператора ректификационной установки, который отвечает не только принципам ситуационной осведомленности, но и современным требованиям в области эргономики компьютерных интерфейсов, что позволяет его реализовать в любой SCADA-системе, как с поддержкой сенсорного экрана, так и без такой поддержки.

Ключевые слова: Ситуационная осведомленность, человеко-машинный интерфейс, безопасность технологического процесса.

Введение

Имеющиеся методики и стандарты, регламентирующие различные аспекты разработки интерфейсов компьютерно-интегрированных систем управления (КИСУ) технологическими процессами, в значительной мере устарели не только ввиду значительного прогресса в области возможностей технических средств отображения информации, но и в виду введенных в сферу профессионального рассмотрения современных концепций проблемно-ориентированного подхода к разработке человеко-машинного интерфейса [1] и ситуационной осведомленности оператора [2]. Именно использование этих концепций позволяет качественно и безаварийно вести современные технологические процессы. В то же время, анализ внедренных в системы управления, например, ректификационными установками спиртового производства,

человеко-машинных интерфейсов показывает [3], что их разработка ведется традиционно, без научного обоснования, и, соответственно, получено профессионально неудовлетворительное качество интерфейсов, хотя для непрофессионалов такие интерфейсы выглядят привлекательными.

В качестве прототипа для развития предложенного подхода к решению задачи выбран международный стандарт ANSI/ISA-101.01-2015. На основе адаптированного применения рекомендаций этого стандарта разработан пример современного интерфейса оператора КИСУ ректификационной установки спиртового производства. Отметим, что корректно разработанный интерфейс влечет за собой повышение эксплуатационных характеристик системы управления, отражается на производительности и качестве продукции, влияет на снижение ошибок оператора в ходе управления технологическим процессом и помогает не допустить аварии, особенно на таком взрыво - пожароопасном производстве, как спиртовое.

Упрощенная структурная схема типовой трехколонной установки косвенного действия приведена на рисунке 1. С деталями технологического процесса и его автоматизации можно ознакомиться в работах [4, 8].

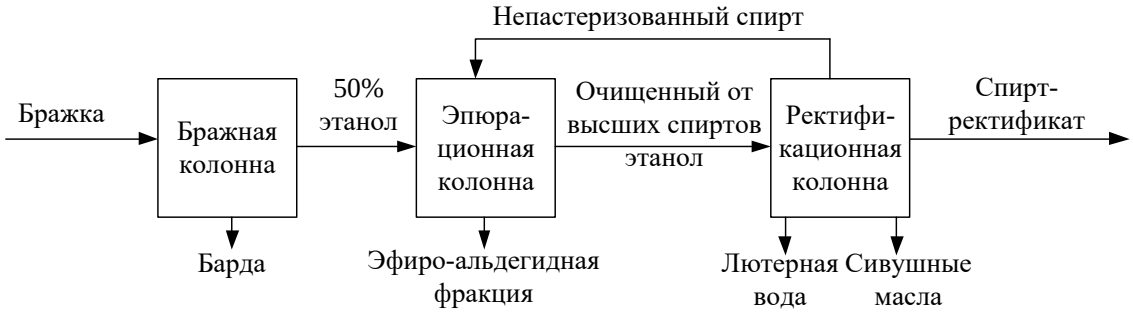


Рис. 1. Принципиальная схема технологической установки

Установка производит спирт-ректификат, соответствующий требованиям ДСТУ по концентрации и составу. В каждую тарельчатую колонну подается пар и происходит тепло- и массообменный процесс. Верхний продукт каждой колонны охлаждается водой.

Основными функциями оператора КИСУ установки являются:

- ведение технологического процесса в соответствии с инструкциями;
- предупреждение и устранение отклонения процесса от заданного режима;
- анализ факторов, влияющих на ход процесса и качество продукции;
- регулировка подачи и ведение учета расходов пара и воды;
- регулировка производительности установки с учетом норм расхода сырья;
- осуществление пуска, вывода установки на режим, остановки установки;
- переключение работающего оборудования на резервное при необходимости;
- контроль состояния оборудования, выявление неполадок и аварий.

Во время работы оператор подвержен ряду отвлекающих факторов. Такими факторами, например, являются посторонняя речь, шумы на производстве, температура и т.п. Оператор может вовремя не заметить аварийную ситуацию потому, что довольно длительное время на его мониторе не изменялась картина. Это приводит к своего рода «торможению» реакции на изменение.

Основная часть

Задачей работы является создание комплекса проблемно-ориентированных интерфейсов оператора КИСУ по модели ситуационной осведомленности Эндсли [2, 5].

Ситуационная осведомленность достигается тогда, когда оператор способен с помощью интерфейса без дополнительных операций оценить прошлое, текущее и будущее (хотя-бы методом экстраполяции) состояние процесса и выполнить предусмотренные операции.

Используя существующие рекомендации, представленные в стандартах ISA 101, ISO 9241, ISO 13407, можно сформулировать следующие принципы построения интерфейсов:

- использование как можно меньшей цветовой палитры;
- цвет должен нести в себе смысловую нагрузку;
- не использовать цветовые градиенты;
- детерминированность и унификация индикации типовых элементов;
- отображение небольшого количества параметров, или их группировка;
- отображение допустимых границ отклонения параметров;
- иерархическая организация экранов.

Критерием эффективности разработки интерфейса является достижение максимальной ситуационной осведомленности оператора [2,5] при наличии функциональных возможностей воздействия на ход технологического процесса в широком спектре предполагаемых ситуаций.

Исходя из анализа инструкции по ведению процесса и моделирования действий оператора сформулируем требования к содержимому экранов каждого уровня (L1, L2, L3) и список задач, которые должен выполнять оператор. Результаты анализа приведены в таблице 1.

Таблица 1.

Иерархия экранов оператора установки

Тип	Содержимое	Задача
L1 Обзорный	1. Основные показатели производства 2. Объем произведенного спирта ректификата за фиксированные временные промежутки. 3. Состояние основных показателей энергоэффективности. 4. Состояние основных параметров ТП 5. Состояние регуляторов. 6. Тренды производительности установки и концентрации спирта-ректификата.	1. Оценить эффективность проведения ТП. 2. Оценить соответствие основных параметров регламенту. 3. Оценить и спрогнозировать динамику производства.
L2 Основной	1. Условное обозначение установки. 2. Температуры и давления в колоннах. 3. Расходы пара, бражки. 4. Тренды концентрации и производительности по этанолу. 5. Температуры воды и пара.	1. Оценка и прогноз параметров агрегатов. 2. Обобщенный анализ качества регулирования 3. Локализация места. превышения параметров.
L3 Детальный	1. Задания. 2. Параметры регуляторов. 3. Переключатель режима работы.	1. Изменение задания. 2. Переключение режимов работы. 3. Ручное изменение управлений.

Рассмотрим, насколько недавно разработанные интерфейсы, удовлетворяют перечисленным выше принципам на примере обзорного экрана установки.

Как можно увидеть, проанализировав экраны на рисунках 2–3, при разработке х интерфейсов был допущен ряд ошибок:

- на экранах используется избыточное количество цветов, использованы объемные изображения аппаратов, а, следовательно, присутствуют цветовые градиенты;
- цвета не несут смысловой нагрузки, а служат только в качестве декорации;
- вентили, приводы и другие исполнительные механизмы не имеют единой системы индикации;
- отсутствуют аналоговые шкалы или полосы с отображением допустимых норм отклонений, что усложняет для оператора прогнозирование протекания технологического процесса;
- при цифровой индикации параметров оператору необходимо постоянно производить математические и логические операции для сравнения показателя с нормальным, который должен быть извлечен из памяти человека, что утомляет оператора, особенно если параметров много.

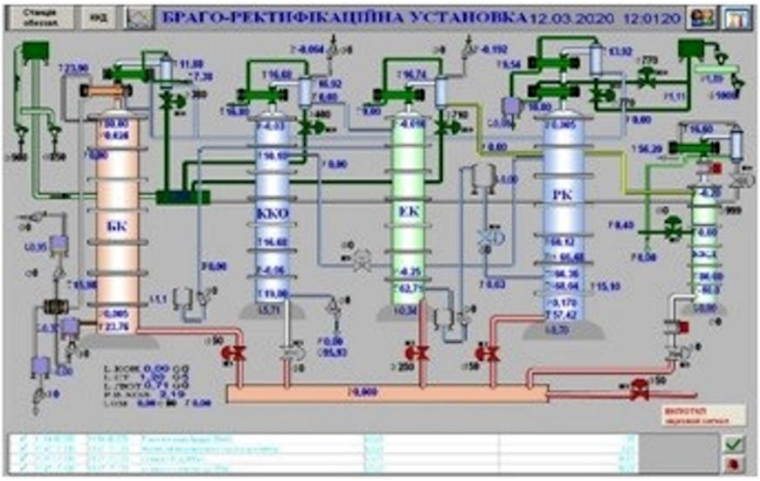


Рис. 2. Экран SCADA/HMI Proficy iFIX для БРУ

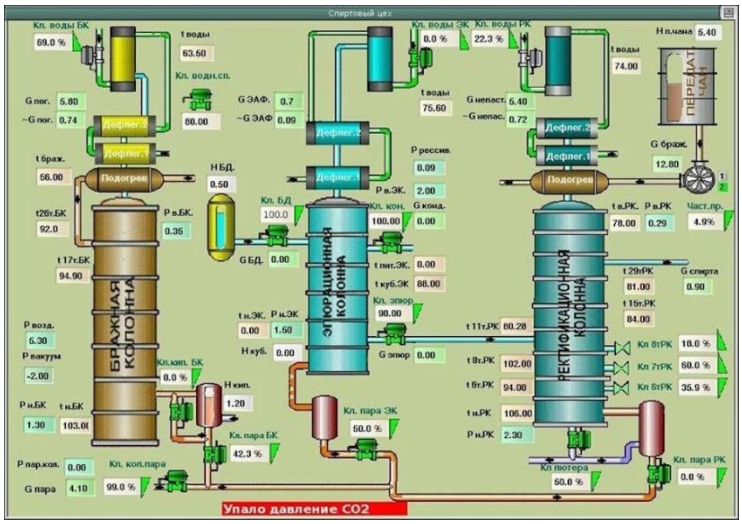


Рис. 3. Экран для ГП «Козловский спиртзавод» [6]

Экран на рисунке 4 лишен ряда недостатков, однако использование объемных фигур по-прежнему усложняет наблюдение за процессом.

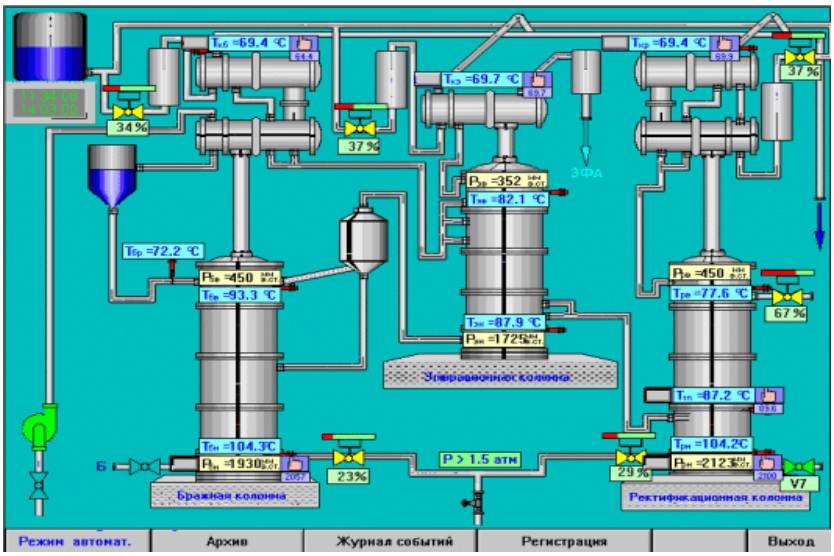


Рис. 4. Экран для спиртового производства ЗАО “РТСофт” [7]

Рассмотренные экраны используют подход, моделирующий размещение приборов на щитах предыдущих поколений АСУТП: рисуется мнемосхема установки и на ней отображаются параметры в цифровом виде. Выбор параметров для отображения является необоснованным, поскольку интерфейс не разрабатывается исходя из предварительного анализа задач оператора, а только из анализа технологического регламента и мнемосхемы. Оператор с помощью цветовой индикации узнает о проблеме уже тогда, когда технологический процесс нарушен. Таким образом, экраны, отображенные на рисунках 2–4, не соответствуют требованиям ситуационной осведомленности.

Согласно ISA 101, все типовые элементы должны быть детерминированы и выдержаны в едином представлении на всех экранах. Исходя из рекомендаций данного стандарта, предложен набор типовых элементов, приведенный на рисунке 5.

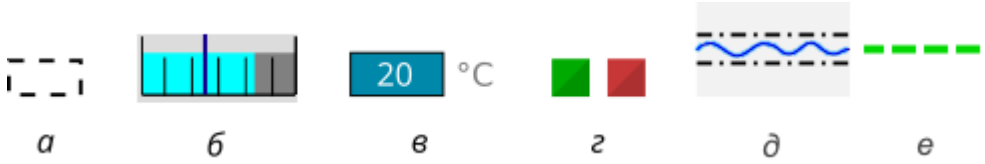


Рис. 5. Типовые элементы интерфейсов: а – группировка; б – аналоговая шкала отклонения; в – цифровое отображение параметра: фон привычный для технолога, единица измерения известна и отображается почти незаметной; г – индикаторы состояния показателя; д – тренд с указанием зон отклонения; е – связь (например, регулятора с вентилем и местом отбора сигнала)

Опираясь на определенный в работе путь решения задачи, были разработаны экраны трех уровней.

Внешний вид экрана первого уровня при технологической ситуации превышения давления в первой колонне изображен на рисунке 6.

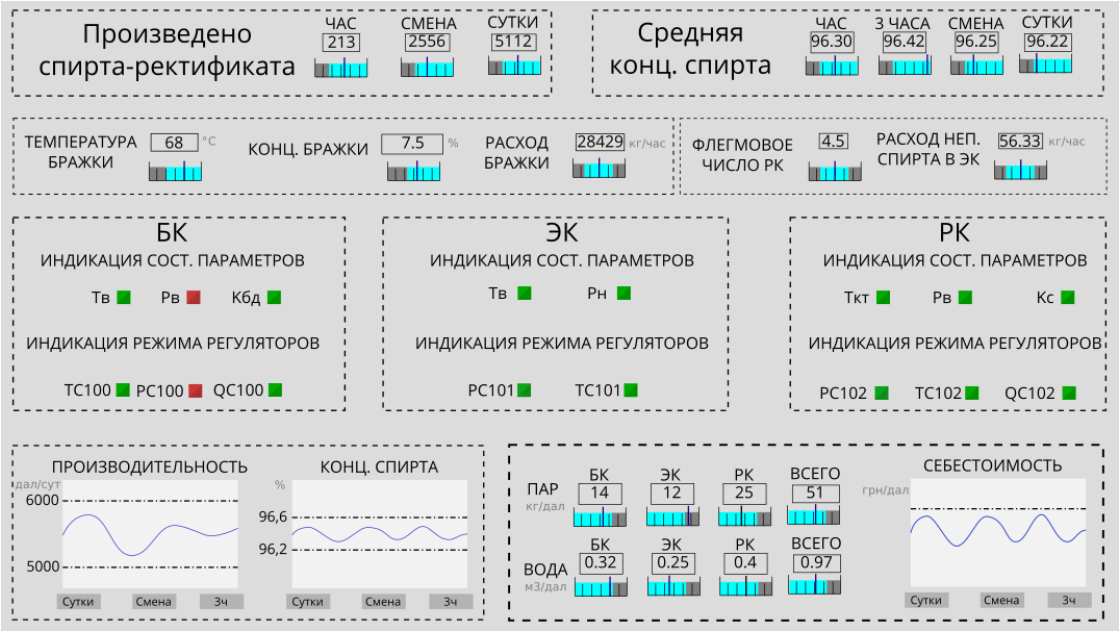


Рис. 6. Экран первого уровня

На экране сразу видны основные показатели производства и их динамика в заданный временной промежуток. Также они приведены в виде трендов. Показатели сырья важны, поскольку их долговременное отклонение приведет нарушению хода ТП [4,9]. Флегмовое число и расход непастеризованного спирта – прямые показатели эффективности процессов разделения. От расхода пара и воды зависит себестоимость производства, которую целесообразно отображать в виде тренда. В заданном месте (снизу экрана или на отдельном мониторе) должны отображаться сообщения, связанные с возникновением предаварийных и аварийных ситуаций (на экранах условно не показаны). При появлении сообщения оператор должен его подтвердить и переместить внимание на другие экраны.

Первый экран второго уровня, предназначенный для наблюдения при нормальном ходе процесса, изображен на рисунке 7.

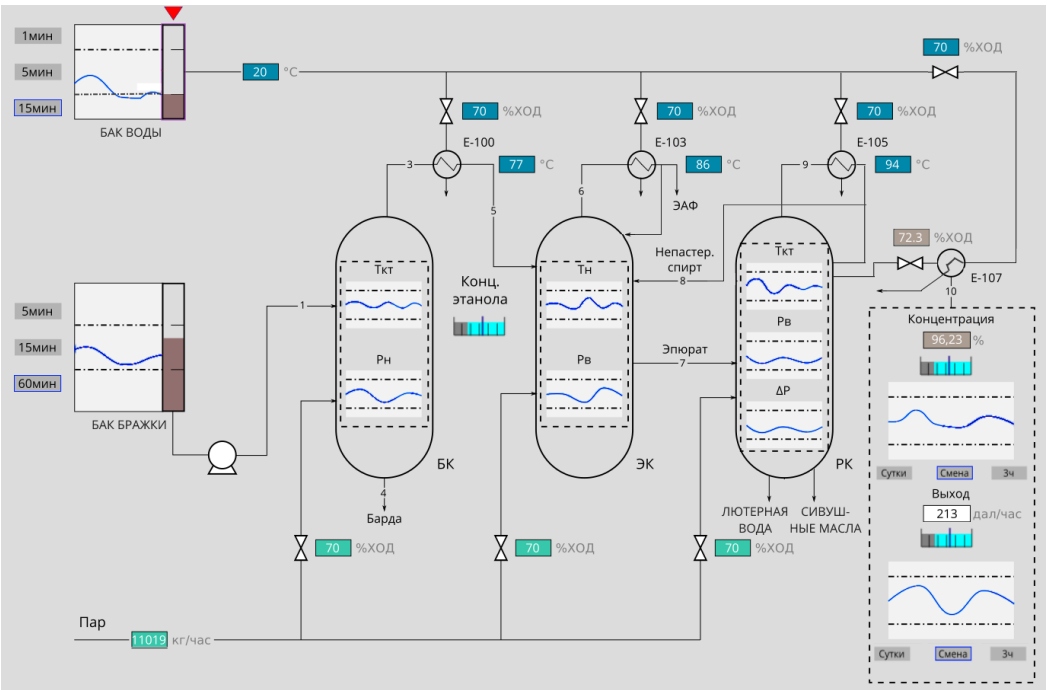


Рис. 7. Основной экран второго уровня

На рисунке показана технологическая ситуация падения уровня воды для охлаждения продуктов колонн в накопительном баке ниже допустимой зоны. Внимание оператора привлекается появляющимся индикатором и сообщением (не показано, появляется снизу экрана). Информации на показанном первичном экране достаточно для нормального наблюдения, но число параметров сведено к минимуму, чтобы не утомлять оператора. Привлечение внимания к нарушению параметров сырья, продукта, работы регуляторов, отказу оборудования и т.п. производится с помощью аварийных сообщений (внизу экрана или на отдельном мониторе) и цветовой сигнализации, привязанной к мнемосхеме (рис. 5г).

На рисунке 8 показан дополнительный экран второго уровня, предназначенный для работы при нестандартных технологических ситуациях. Локализация места нарушения процесса ректификации проводится по двум параметрам: температуре и давлению. Отображение температурного профиля по колоннам, давления верха и низа колонн и основных показателей материального и энергетического баланса установки позволяет локализовать место нарушения. Например, внезапное нарушение температурного профиля при постоянном составе сырья чаще всего говорит о наличии испорченных тарелок; изменение перепада давления – о засорении колонны и т.д. Так, на рисунке показана технологическая ситуация отклонение температурного профиля первой колонны, внимание к которой привлекается предупредительной (желтой) сигнализацией.

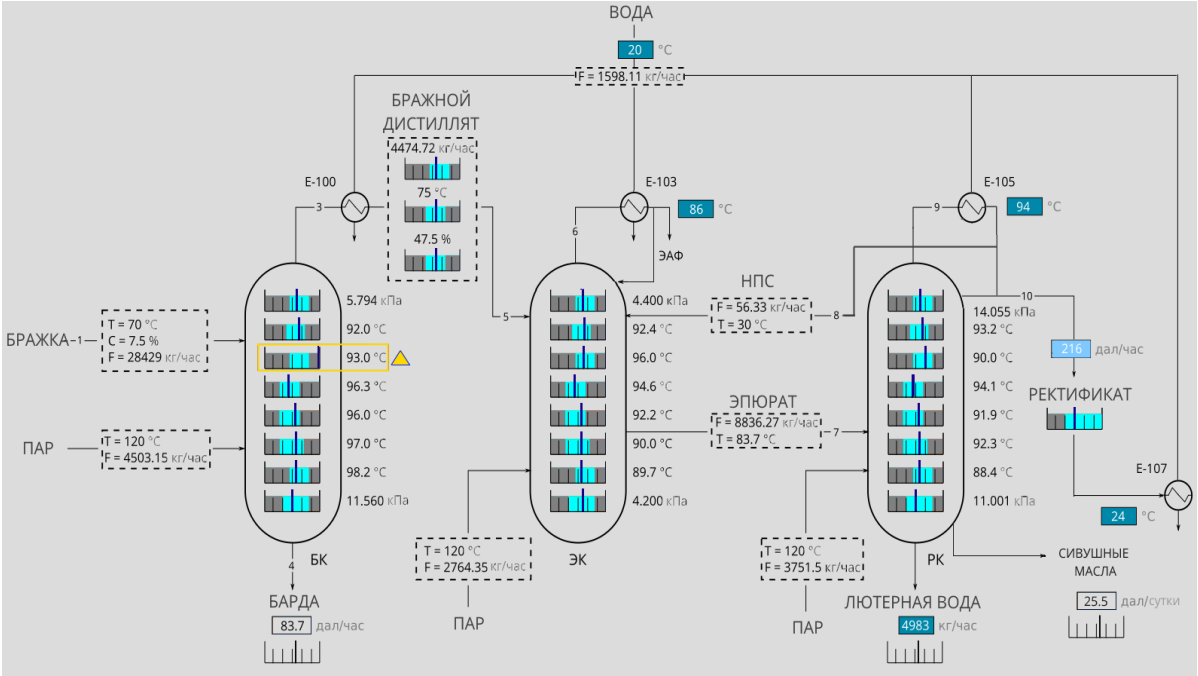


Рис. 8. Дополнительный экран второго уровня

На рисунке 9 показан экран третьего уровня для последней колонны.

Этот экран предназначен для изменения заданий регуляторов (SP) и перевода регуляторов в ручной режим при их ненормальной работе. Ручное управление проводится введением значения процента открытия регулирующего органа (OV) на основании текущего значения управляемой переменной (PV) с помощью стрелок или текстового ввода. В случае текстового ввода и значительного изменения значения OV должно проводиться подтверждение операции с помощью всплывающего диалогового окна. На рисунке отображена технологическая ситуация – регулятор не справился со стабилизацией температуры контрольной тарелки. Оператор отключил регулятор и задал 65% открытия вентиля пара, что вернуло параметр в регламентную зону.

При нарушении работы системы управления ректификационной колонны может произойти захлебывание колонны, потеря спирта с лютерной водой, выход некачественного продукта [6]. Для обеспечения возможности исправить ситуацию после отключения регуляторов для оператора предусмотрена функция открытия и закрытия продуктовых потоков, которые не задействованы при регулировании.

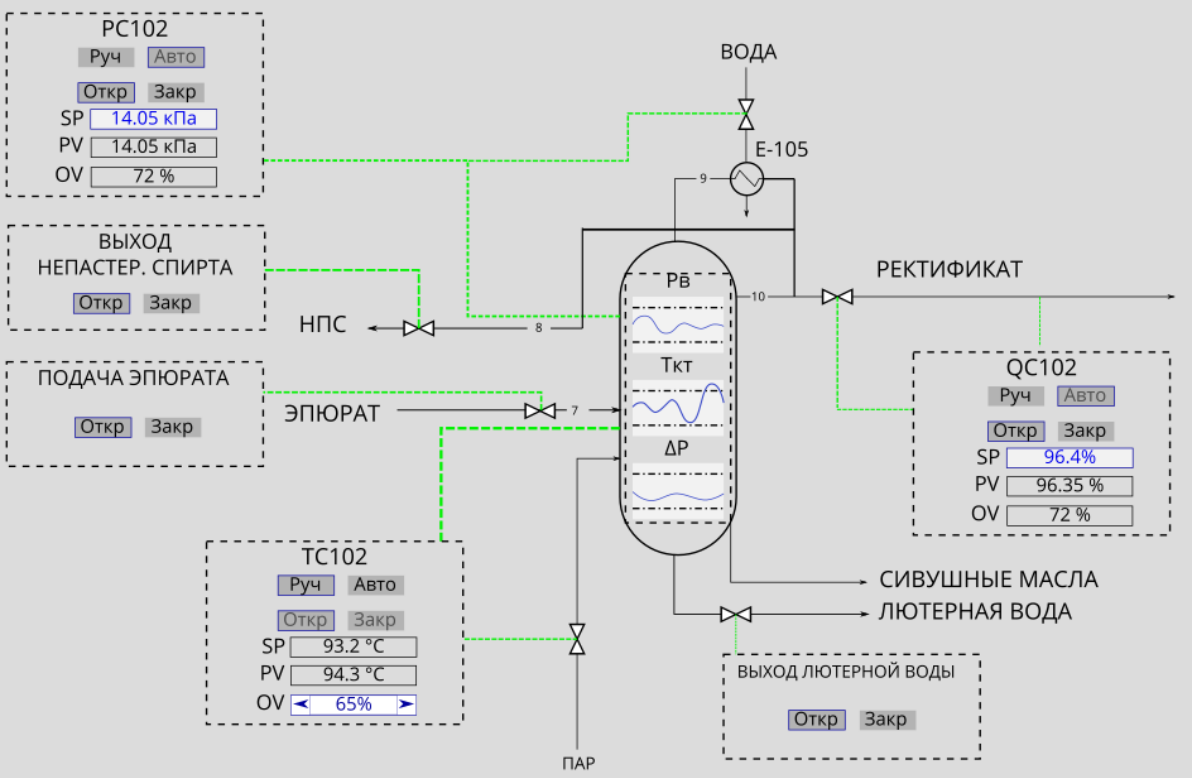


Рис. 9. Экран третьего уровня

Выводы

Разработан подход к созданию интерфейса оператора КИСУ на примере управления ректификационной установкой спиртового производства. Подход основан на использовании концепции ситуационной осведомленности. Разработаны примеры экранов трех уровней человеко – машинного интерфейса, которые включают:

- первый уровень, обзорный экран технологической установки;
- второй уровень, первичный экран, который отображает состояние технологического процесса в установке без средств воздействия на ход процесса и предназначен для привлечения внимания оператора к ситуации выхода параметров процесса за регламентные нормы;
- второй уровень, дополнительный экран, который позволяет точно локализовать проблему, выявленную на первичном экране;
- третий уровень, предназначенный для корректировки хода технологического процесса с помощью изменения заданий регуляторам или ручного управления.

Использование приведенного подхода рекомендуется для разработки современных человеко-машинных интерфейсов в АСУТП различных технологических процессов.

Список литературы

1. Юрчук Л.Ю. Міжнародні нормативні засади людино-машинного інтерфейсу систем управління технологічними процесами. *Summer infocom advanced solutions 2017. Матеріали IV Міжнародної науково-практичної конференції,* Київ, 2017. С. 66-68.
2. Endsley M. Designing for situation awareness: an approach for user-centered design. USA, NW: CRC Press 2011.
3. Стопакевич А.О. Основи комп'ютерного управління. Одеса: ОНАЗ, 2017. 38 с.
4. Стабников В.Н., Николаев А.П., Мандельштейн М.Л. Ректификация в пищевой промышленности. Теория процесса, машины, интенсификация. Москва: Легкая и пищевая промышленность, 1982. 232 с.
5. Endsley M.R., Garland D.J. Situation awareness analysis and measurement. Mahwah, NJ: LEA, 2000.
6. АСУ ТП производства спирта для ГП Козловский спиртзавод. URL: www.rts.ua/rus/got/610/0/18/.
7. Кириллов Е.А. Система автоматического управления и регулирования технологическими процессом брагоректификации. *Промышленные контроллеры и АСУ*. 2001. №1. С.17-23.
8. Стопакевич А.А., Тодорцев Ю.К. Анализ современного состояния систем управления брагоректификационной установки спиртового производства. *Автоматика. Автоматизация. Электротехнические комплексы и системы*. 2009. V.23(2). С. 180-184.
9. Рожнов Е.Д., Каменская Е.П., Обрезкова М.В. Технология отрасли. Производство спирта и ликероводочных изделий. Бийск: Алтайский гос. техн. ун-т, 2013. 162 с.

РОЗРОБКА КОНЦЕПЦІЇ СТВОРЕННЯ ІНТЕРФЕЙСУ ОПЕРАТОРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ УСТАНОВКАМИ ВІДПОВІДНО ДО ПРИНЦИПУ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ

А.О. Стопакевич[1], О.А. Стопакевич[2]

[1]Одеська національна академія зв'язку,
вул. Кузнечна, 14, Одеса, 65029, Україна; e-mail: stopakevich@gmail.com
[2]Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: stopakevich@opu.ua

Важливою проблемою, яка визначає безпеку функціонування сучасного автоматизованого виробництва на основі комп'ютерно-інтегрованих систем управління технологічними установками, є врахування психологічних аспектів сприйняття комп'ютерних інтерфейсів людиною-оператором автоматизованого технологічного процесу. Більшість розроблених комп'ютерних інтерфейсів для операторів створені відповідно до ідеї надання максимальної кількості інформації про технологічний процес. Але, ця ідея суперечить основам інженерної психології, яка акцентує увагу розробників на особливості сприйняття інформації людиною. З одного боку, в ситуації стресу, пов'язаного з аварійністю і небезпекою виробництва, оператор не здатний проаналізувати великий обсяг інформації для прийняття вірного рішення. З іншого боку, тривале спостереження за набором даних про стан технологічного процесу, який мало змінюється, призводить до деконцентрації уваги оператора, що, в свою чергу, збільшує ймовірність неправильного рішення в нештатної, аварійної або передаварійної ситуації. Для боротьби з цими явищами пропонується слідувати принципам ситуаційної обізнаності при створенні комп'ютерних інтерфейсів. Концепція використання зазначеного принципу при створенні ряду інтерфейсів комп'ютерно-інтегрованої системи управління ректифікаційної установкою виробництва спирту розроблена в статті. На основі результатів моделювання необхідної діяльності оператора в аварійних ситуаціях розроблений багаторівневий графічний інтерфейс оператора ректифікаційної установки, який відповідає не тільки принципам ситуаційної обізнаності, а й сучасним вимогам в області ергономіки комп'ютерних інтерфейсів, що дозволяє його реалізувати в будь-який SCADA-системі, як з підтримкою сенсорного екрану, так і без такої підтримки.

Ключові слова. Ситуаційна обізнаність, людино-машинний інтерфейс, безпека технологічного процесу.

DEVELOPMENT OF THE CONCEPT OF CREATION OF THE OPERATOR INTERFACE OF COMPUTER-INTEGRATED CONTROL SYSTEMS OF TECHNOLOGICAL PLANTS IN ACCORDANCE WITH THE PRINCIPLE OF SITUATIONAL AWARENESS

A.O. Stopakevych[1], O.A. Stopakevych[2]

[1]Odessa National Academy of Telecommunications,
14, Kuznechna, Odessa, 65029, Ukraine; e-mail: stopakevich@gmail.com
[2]Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: stopakevich@opu.ua

An important problem that determines the safety of the functioning of modern automated plants based on computer-integrated control systems for technological processes is taking into account the psychological aspects of the perception of computer interfaces by a human operator of an automated technological process. Most of the developed computer interfaces for operators are created in accordance with the idea of providing the maximum amount of information about the technological process. But this idea contradicts the foundations of engineering psychology, which focuses the attention of developers on the peculiarities of human perception of information. On the one hand, in a situation of stress associated with accidents and industrial hazards, the operator is not able to analyze a large amount of information to make the right decision. On the other hand, long-term monitoring of a slightly changing set of data on the state of the technological process leads to deconcentration of the operator's attention, which, in turn, increases the probability of a wrong decision in an emergency or pre-emergency situation. To cease these phenomena, it is proposed to follow the principles of situational awareness when creating computer interfaces. The concept of using this principle when creating a number of interfaces of a computer-integrated control system for a rectification plant for alcohol production is developed in the article. Based on the results of simulating the necessary operator activities in emergency situations, a multi-level graphical interface for the operator of the rectification plant has been developed. The interface meets not only the principles of situational awareness, but also modern requirements in the field of ergonomics of computer interfaces, which makes it possible to implement it in any SCADA system, as with support for a sensor screen, and without such support.

Keywords. Situational awareness, human-machine interface, technological process safety.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 10, номер 1-2, 2020. Одеса – 120 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 10, номер 1-2, 2020. Одесса – 120 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 10, No. 1-2, 2020. Odesa – 120 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №5 від 28.01.2020)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали

© Одеський національний політехнічний університет, 2020