МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 5, № 1

Volume 5, No. 1

Одеса – 2015
Odesa – 2015

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.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

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

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., Odessa, 65044, Ukraine

Tel.: +38 048 705 8506

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

ЗМІСТ / CONTENTS

УДК 004.82:681.18

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 5-9

МОДЕЛЬ ВИЗНАЧЕННЯ РІВНЯ ЕФЕКТИВНОСТІ ВИКОНАННЯ СПІЛЬНОГО ПРОЕКТУ В МЕРЕЖЕВИХ WEB-РЕСУРСАХ НА ОСНОВІ КОМУНІКАТИВНИХ ПОКАЗНИКІВ

Ю. Є. Яремчук, Л. О. Нікіфорова, А. А. Шиян, В. Х. Касіяненко

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: yurevyar@vntu.net

Поставлено задачу моделювання рівня ефективності виконання спільного проекту в мережевих web-ресурсах з використанням комунікативних показників. Введено систему комунікативних показників, які характеризують інтегрально весь колектив у цілому. Вони вимірюють інтегральний рівень емоційного стану колективу, що впливає на ефективність його діяльності.

Ключові слова: моделювання, web-ресурс, спільна діяльність, комунікативні показники, колектив.

Вступ

Мережеві web-ресурси все частіше використовуються для здійснення практичної діяльності. Вже давно стали нормою так звані віртуальні фірми, а соціальні мережі успішно використовуються для здійснення соціальних проектів. Важливим фактором при виконанні спільної діяльності в рамках виробничого чи соціального проекту є та обставина, що окремі люди згуртовуються у колектив внаслідок свого власного вибору. При цьому стабільність та ефективність такого колективу залежить, внаслідок цього, передовсім від інформаційно-психологічного клімату.

У колективі, який сформовано на основі мережевого web-ресурсу, ефективність виконання проекту залежить від загального рівня психологічного комфорту, що відчуває кожен учасник. Причому цей показник, у свою чергу, залежить від рівня комфортності спілкування за допомогою телекомунікаційної мережі, на базі якої й сформовано такий віртуальний проектний колектив.

Аналіз останніх досліджень та публікацій

В [1, 2] розглядається широке коло задач моделювання діяльності людей у соціальних мережах, проте увага зосереджена на описі мереж у вигляді графів, вузли яких (люди) характеризуються тільки кількістю зв’язків між ними. В рамках таких підходів практично неможливо здійснити моделювання спільної діяльності людей.

В [3] розглянуто широке коло задач з моделювання інформаційного впливу в соціальних мережах. Але використані моделі не враховують особливості довготривалої комунікації людей в умовах спільної діяльності.

Робота [4] доводить, що діяльність людей є важливим фактором структурування соціальної групи, яка зв'язана за допомогою телекомунікаційної мережі.

В [5] розроблено математичний апарат для мультиагентних мереж, в яких в якості агентів виступають люди, що приймають рішення або здійснюють вибір, та побудована топологічна класифікація соціальних мереж. Класифікація основана на розробленій класифікації людей за типами ефективності спільної діяльності. Однак в цій топології не враховують індивідуальні психологічні характеристики людини, які проявляються, наприклад, у рамках емоційного зафарбування відносин до того чи іншого комуніканта.

Таким чином, проблема врахування емоційної складової комунікацій при виконанні спільного проекту в мережевих web-ресурсах залишається все ще актуальною в науковому плані. Практична цінність її розв'язання полягає в тому, що її результати дозволять прогнозувати рівень ефективності виконання спільного проекту.

Мета статті

Метою статті є розробка моделі визначення ефективності виконання спільного проекту в мережевих Web-ресурсах на основі комунікативних показників.

Основна частина

Розглянемо обмін повідомленнями, якими обмінюються комуніканти в процесі виконання спільного проекту. Ці повідомлення можуть бути віднесені до трьох полюсів: схвальні, несхвальні, нейтральні.

Схвальні повідомлення у своїй переважній більшості відображають позитивний емоційний стан автора повідомлення і свідчать про його емоційне схвалення діяльності отримувача. Несхвальні повідомлення свідчать про негативне емоційне відношення до отримувача. Нарешті, нейтральні повідомлення – це, найчастіше, або повідомлення – коментарії щодо роботи, або ж свідчення байдужості до отримувача.

Введемо такі показники. Нехай X_{ij}^{+} – наявність схвального (позитивного) повідомлення, а X_{ij}^{-} – наявність несхвального (негативного) повідомлення, які отримує i - та людина від свого j -го комуніканта через мережевий web-ресурс. Тепер для опису виконавців спільного проекту можна застосувати методи соціометрики, введені Дж.Морено в [6]. Але ці показники описують лише конкретну людину, а не весь колектив у цілому. Більш того, інтерпретація цих показників іноді не є достатньо прозорою [7, 8].

В [7, 8] для опису колективу в цілому було запропоновано нижченаведене узагальнення ряду соціометричних показників. Так, для i -тої людини можна ввести показник, який відображує сприйняття його колективом, за такою формулою [7, 8]:

$$C_i = \frac{1}{2}\left(\left(\sum_j X_{ij}^{+} - \sum_j X_{ij}^{-}\right)\Big/(N-1)+1\right). \tag{1}$$

Тут N – кількість людей у колективі.

Для опису стану у всьому колективі (1) потрібно усереднити по всім працівникам:

$$C = \frac{1}{N}\sum_i C_i \,. \tag{2}$$

Значення показника, розрахованого за формулою (2), приймає лише додатні значення і обіймає інтервал $[0,1]$. При цьому значення показника $C \to 1$ є позитивними, що свідчить про те, що, «в середньому», члени виробничого колективу позитивно відносяться один до одного (схвалюють діяльність одне одного).

Аналогічно можна ввести ще такі показники, які характеризують відношення i-тої людини до свого j-го комуніканта. Нехай Z_{ij}^{+} – є наявність схвального (позитивного) повідомлення від i-тої людини до свого j-го комуніканта через мережевий web-ресурс, а Z_{ij}^{-} – наявність несхвального (негативного) повідомлення, відповідно. Тоді, аналогічно (1) та (2), отримуємо такі формули:

$$E_i = \frac{1}{2}\left(\left(\sum_j Z_{ij}^{+} - \sum_j Z_{ij}^{-}\right)\Big/(N-1)+1\right), \tag{3}$$

$$E = \frac{1}{N}\sum_i E_i . \tag{4}$$

Показники, розраховані за формулами (2) та (4), відносяться до всього проектного колективу та інтерпретуються аналогічним чином.

При прямуванні показників $C \to 0$ та $E \to 0$ можна зробити висновок, що міжособові відносини у досліджуваному колективі є «негативними» і не сприяють ефективності праці. Прямування обох показників до 0,5 свідчить, що міжособові відносини є «байдужими» або «нейтральними». Коли ж обидва показники прямують до 1, то це свідчить, що міжособові відносини у виробничому колективі є «позитивними» та сприяють підвищенню ефективності праці.

Використовуючи наведену вище інтерпретацію, можна запропонувати таку формулу для єдиного інтегрованого показника, який буде характеризувати ділові характеристики виробничого колективу як єдиного цілого:

$$W = p_1 \cdot C + p_2 \cdot E , \tag{5}$$

p_1, p_2 - параметри, знайдені експериментальним шляхом (наприклад, із опитування експертів). Як правило, часто можна покладати $p_1 + p_2 = 1$.

Цей показник можна назвати «показником ділового комфорту». Його інтерпретація є такою. Коли $W \to 0$, то в даному колективі склалися такі відносини між його членами, які негативно впливають на результати діяльності колективу. Його працівники не вважають свій колектив достатньо професійним. Коли $W \to 0{,}5$, то у колективі панує байдужість як одне до одного, так і до діяльності колективу в цілому. Нарешті, коли $W \to 1$, то професійна та економічна діяльність колективу високо оцінюється його членами, високий рівень взаємопідтримки нових ідей тощо.

В [8] введено ще два інтегральні показники, які характеризують спільну роботу співробітників колективу. Вони можуть служити для оцінки ступеня згуртованості колективу, а також для оцінки наявного рівня корпоративної культури у колективі. Це індекс взаємності G та індекс конфліктності Y. Величина індексу взаємності G розраховується як частка таких пар комунікантів у колективі, яким приємно працювати один з одним. Чим більша кількість позитивних пар у колективі, тим вищим є рівень позитивної згуртованості та взаємності колективу. На відміну від попереднього показника, індекс конфліктності Y визначає частку негативних пар, тобто пар таких співробітників, які не хочуть працювати разом.

Враховуючи ще ці два показники, в [7, 8] запропоновано об'єднати їх у єдиний інтегральний «показник психологічного комфорту» за такою формулою:

$$P = (G - Y + 1)/2\,. \qquad (6)$$

Інтерпретація цього показника є такою.

Коли $P \to 1$, це відповідає тому, що кожен співробітник колективу згоден працювати та спілкуватися із кожним іншим його членом, що є ідеальним з точки зору опису колективу як єдиного цілого. Також це свідчить про високий рівень корпоративної культури у виробничому колективі. Якщо $P \to 0$, то це відповідає ситуації, коли кожен працівник колективу активно не згоден працювати та спілкуватися ні з яким іншим членом колективу. Звичайно, це є найгіршою можливою ситуацією. Коли ж $P \to 0.5$, це відповідає ситуації, коли колектив «у середньому» є байдужим до колективної співпраці, що, звичайно, є небажаним для виробничого колективу.

Порівнюючи (5) та (6) та спираючись на тотожність їх інтерпретацій, можна ввести єдиний «інтегральний показник ефективності спільної діяльності колективу»:

$$I = q_1 \cdot W + q_2 \cdot P\,. \qquad (7)$$

Тут q_1 та q_2 – ваги, які відповідають впливу кожного із цих показників. Ці ваги можна або визначити експериментально, або ж знайти за допомогою експертів. Як правило, при розрахунках використовується таке співвідношення: $q_1 + q_2 = 1$.

Значення $I \to 1$ буде відповідати високому рівню ефективності спільної діяльності колективу і свідчити про те, що даний виробничий колектив являє собою єдине ціле, є згуртований і пристосований до спільної роботи. Значення $I \to 0.5$ характеризує несформований колектив, а $I \to 0$ відповідає колективу, який є непрацездатним.

Обговорення результатів

Комунікативний показник I (або, в залежності від поставленої задачі, окремі показники C, E, W та P) можна використовувати для різних задач з управління ефективністю виконання спільного проекту в мережевих web-ресурсах. Наприклад, можна виділяти (за методом перебору) в колективі тих людей, видалення яких приводить до зростання того чи іншого комунікативного показника. В [8] це було виявлено на прикладі реальних трудових колективів та було розроблено метод для розрахунку економічної ефективності від покращення комунікативної комфортності в колективі. В [9] описано метод розрахунку наслідків із здійснення інформаційного впливу на певних людей в соціальній мережі. Отримані вище результати дають можливість як виявити тих людей, які якнайсильніше впливають на соціальну групу, що обмінюється повідомленнями через телекомунікаційну мережу, так і спрогнозувати наслідки від видалення цих людей із групи (або від їх тимчасової ізоляції від неї).

Висновки

На основі використання комунікативних показників вирішено задачу моделювання визначення рівня ефективності виконання спільного проекту в мережевих web-ресурсах. Введено систему комунікаційних показників, які характеризують інтегрально весь колектив у цілому. Вони вимірюють інтегральний рівень емоційного стану колективу, що впливає на ефективність його діяльності.

Список літератури

1. Easley, D. Networks, Crowds, and Markets: Reasoning about a Highly Connected World / D. Easley, J. Kleinberg. – Cambridge: Cambridge University Press, 2010. – 833 p.
2. Jackson, M.O. Social and Economic Networks / M. O. Jackson. – Princeton : Princeton University Press, 2010. – 520 p.
3. Губанов, Г.А. Социальные сети: моделирование информационного влияния, управления и противоборства / Г.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили. – М.: Физматлит, 2010. – 228 с.
4. Hong-Han Shuai. Willingness Optimization for Social Group Activity [Електронний ресерс] / Hong-Han Shuai, De-Nian Yang, Philip S. Yu, Ming-Syan Chen. – 16 p. Режим доступу: http://arxiv.org/abs/1305.1502
5. Шиян, А.А. Про один клас мультиагентних мереж для оптимального управління організаційними структурами / А.А. Шиян // Проблеми інформатизації та управління. – 2013. – Вип. 4(44). – С. 86–92.
6. Морено, Дж. Социометрия: Экспериментальный метод и наука об обществе / Дж. Морено. – М.: Иностр.лит., 2008. – 289 с.
7. Шиян, А.А. Метод оцінювання ефективності економічної діяльності колективу підприємства на основі інтегральних показників / А.А. Шиян, Л.О. Нікіфорова // Збірник наукових праць «Економічний простір». – 2008. – №17.– С. 157–165.
8. Мороз, О.В. Соціально-психологічні чинники мотивування працівників приладобудівних підприємств / О.В. Мороз, Л.О. Нікіфорова, А.А. Шиян. – Вінниця: ВНТУ, 2011. – 252 с.
9. Пелещишин, А.М. Визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти / А.М. Пелещишин, Р.О. Корж, Р.В. Гумінський // Безпека інформації. – 2014. – Т.20, №3. – С. 264–273.

МОДЕЛЬ ОПРЕДЕЛЕНИЯ УРОВНЯ ЭФФЕКТИВНОСТИ ВЫПОЛНЕНИЯ ОБЩЕГО ПРОЕКТА В СЕТЕВЫХ WEB-РЕСУРСАХ НА ОСНОВЕ КОММУНИКАТИВНЫХ ПОКАЗАТЕЛЕЙ

Ю. Е. Яремчук, Л. А. Никифорова, А. А. Шиян, В. Х. Касияненко

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

Поставлена задача моделирования уровня эффективности выполнения общего проекта в сетевых web-ресурсах с использованием коммуникативных показателей. Введено систему коммуникативных показателей, которые характеризуют интегрально весь коллектив в целом. Они измеряют интегральный уровень эмоционального состояния коллектива, что влияет на эффективность его деятельности.

Ключевые слова: моделирование, web-ресурс, общая деятельность, коммуникативные показатели, коллектив.

SIMULATION TO DETERMINE THE EFFICIENCY OF DEVELOPMENT OF A COMMON PROJECT IN NETWORK WEB-RESOURCES BASED ON COMMUNICATIVE INDICES

Yu.Ye.Yaremchuk, L.A. Nikiforova, A.A. Shiyan, V.Kh. Kasiyanenko

Vinnitsa National Technical University
95, Khmelnytske roadway, Vinnytsya, 21021, Ukraine; e-mail: yurevyar@vntu.net

The problem was stated as follows: to simulate the efficiency of the development of a common project in network web-resources based on communicative indices. A system of communicative indices was introduced to characterize integrally the whole team. These indices were used to measure the emotional status of the team influencing the efficiency of the team.

Keywords: simulation, web-resource, common activity, communicative indices, team

УДК 004.415.056.5(075)

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 10-18

EVALUATING METHODS OF THE PROJECT SOLUTION EFFECTIVENESS IN INFORMATION SECURITY SYSTEM DEVELOPING BASED ON RESOURCE MAPS

I. Pavlov

State University of Telecommunications,
7, Solomenskaya str., Kiev, 03680, Ukraine; e-mail: pavlov@ukr.net

The article presents methods of quantitative valuation of project decision effectiveness in information security system development.

Keywords: absolute efficiency, relative efficiency, methods, project, resource maps, information security systems, the effectiveness of the project (design) decision.

Problem

Determination of the design decision effectiveness is a non-trivial task. In most cases, the assessment of effectiveness is made subjectively, as a rule on the basis of experts' assessments by known methods. It is based on narrow area experts' opinions in the field of information security and it's not carried out a systematic analysis of the efficiency of decision-making process upon information security system creating.

In most cases, when creating information security systems the rating systems are used. On their basis the calculation of quantitative factor of decision-making process is fulfilled. In practice, such systems are quite specific and often mostly persecute motivational goals than the real purpose.

Indeed, determining the effectiveness of decisions is based on the principle of comparative characteristics of some standard set of actions, decisions or results. But wrong decisions, taken at the design stage, lead to information leakage due to detected during operation protection mechanism vulnerabilities.

Therefore, the search of a common approach to determine the quantitative methods of evaluating the effectiveness of the design decisions during creating information security systems is a challenging problem.

Analysis of research publications and reports

Analysis of research publications and reports confirms that publications describing the procedure for evaluation the effectiveness of the systems is not determined by quantification of total project solutions, and available estimates do not allow us to determine the requirements for information security systems as complex systems.

So in [1-4] there is a general formal approach to the creation of information security systems, but the quantitative evaluation performances of the decision in the design of information security systems have not been revealed.

In [5] there is a common approach to determine the quantitative approach for evaluating the effectiveness of project management, but the peculiarities of information security system design are not defined.

In [6] the requirements for complex systems, which are the systems of information security, are determined. But the problem for the developer is how to take these requirements for information security systems into consideration.

In [7] a general methodology of requirements for information security systems is shown, but it is necessary to define the quality requirements of the decision-making with such approach as resource maps. This approach allows a more careful approach to assessing the quality of the decision.

Thus, the purpose of the article is a method for assessment the effectiveness of project decisions during creating information security systems based on resource maps.

Main part

In design methodology we often use the terms "management efficiency", "effectiveness of management decisions". These terms reflect the efficiency of interaction between subsystems and systems that transform inputs into outputs and job management system as a whole. One of the main requirements to management is a quality requirement, that must necessarily be considered from the standpoint of a systematic approach. This requirement involves consideration of quality management system from the standpoint of a higher level inherently complex systems, which are information security system [6].

In [5] it is given an attempt to determine the range of tasks associated with the general approach of determining the effectiveness of complex systems, which indicates the need to partition the concepts of "effect" and "efficiency" and, to the author's view, it is given the correct research vector, where the "effect" should be understood as a result or consequence of certain actions, and "efficiency" – as a property of actions that lead to the effect.

That is the efficiency is determined by some function of several parameters of the system, and the effect – by the integral sum of the function of time.

For project management, as a result of which a quality solution must be formed, we'll define efficiency, as defined property of management project, which is objectively reflected as the degree of achievement of the objectives' tree taking into account the cost of resources.

Let's show the following definitions: properties of information security system - some functional, that combines a set of functions of information security system for their further conversion into function of efficiency. Efficiency function can be built only in a system with adequate control mechanism (e.g. intrusion detection system), which provides an objective assessment of management results. Under the information security systems design management results we have to understand the timely and qualitative implementation of the planned design works with expected quality.

In fact, the efficiency function is a function with delay, as a result of management can be assessed by the certain time only, and therefore it is necessary to further define the mechanism of timely response. The mechanisms of deviation from the expected value range earlier inform stimulation are called preventive self-control mechanisms (5).

Highlighting the above, we can come to the conclusion, that the effectiveness of project management solution is a function of time, which objectively reflects the degree of adequacy between the expectation and the actual state of affairs. This is the essence of performance indicator and determines the nature of the phenomenon.

In practice information security management systems regularly take partial solution to use various security mechanisms, each of them brings its contribution to the final effect.

So, let's divide the concept of "efficiency of design decisions" on absolute E_a and relative E_r terms.

The absolute indicator E_a means the effectiveness of the decision about extreme limits, for example, a particular phase of work:

$$E_a(t) = f_r \cdot f_q \cdot f_c, \tag{1}$$

where f_r – resource absorption factor for the mentioned period, which is the ratio of the planned resource to realized resource values; f_q – the quality factor, which characterizes the value of customer responsiveness for the mentioned period; f_c – the completion factor, which characterizes the completion magnitude of the process in relation to the planned project time.

The resource absorption factor plays a key role in making design decisions, its reflection can be found in the method [5], therefore this figure is taken as the main performance indicator in the calculation of the efficiency of design decisions. For example, as a resource the financial costs may be taken, in this case this factor reflects the index of the value:

$$f_r = \frac{C_p}{C_a}, \tag{2}$$

where C_p – project costs, which are incorporated in the said time t; C_a – actual costs at a specified time t.

In one line with the coefficient of resource absorption is an important indicator of the quality of performed work. In practice, it's not always possible objectively to assess the quality of non-completed works and the results of the performed individual works from the total work. Therefore, in the planning process checkpoints are assigned, which help to check the quality of performed works, as a rule in a percentage.

Completion factor (f_c) considers the degree of completion of the transaction in relation to a given period:

$$f_c = \frac{\tau_p(t) \cdot (T_p + \Delta\tau(t))}{T_p \cdot \tau_a(t)}, \tag{3}$$

where $\tau_p(t)$ – the total duration of the planned project work for mentioned time (t); $\tau_a(t)$ – the total duration of the actually performed project work on the time (t); T_p – the total duration of all the planned works of the project; $\Delta\tau(t)$ – the factor that characterizes the time change of the project implementation.

In a case when the work or a work package is on the critical path, then this value (factor) is the time difference between actually carried out works and planned ones:

$$\Delta\tau(t) = \tau_a(t) - \tau_p(t). \tag{4}$$

For example, if the value of the project work is 800 hours, and the complex planned work – 150 hours, and by the time (t) the value factor $\Delta\tau(t) = 230$ hours, then the completion factor of this work package is:

$$f_c = \frac{150 \cdot (800 + (230 - 150))}{800 \cdot 230} = 0.72.$$

This formula reflects the link of two factors: the completion factor as planned $f_{c(plan)}$ and the actual completion factor $f_{c(actual)}$:

$$f_{c(plan)} = \frac{\tau_p(t)}{T_p};$$

$$f_{c(actual)} = \frac{\tau_a(t)}{T_p + \Delta\tau(t)}; \quad (5)$$

$$f_c = \frac{f_{c(plan)}}{f_{c(actual)}}.$$

A relative performance of design decision efficiency E_r means a part of efficiency and its contribution to the overall efficiency of design decision making, which in its turn, is calculated as a part of absolute effectiveness factor of the design decision in general:

$$E_r(t) = E_a(t) \cdot f_i, \quad (6)$$

where $E_r(t)$ – a relative efficiency factor of design decisions; f_i – importance factor or scope of decision, which characterizes the importance of the decision as for the general project.

The importance factor can be defined both by experts and the ratio of two values, one of them determines the scope of impact of made decision and the other a scope of project. For example, if efficiency of project phase management is determined, the project time of mentioned phase realization can be chosen as the first value, and the second value – the project time of a general project implementation:

$$f_i = \frac{T_i}{T_{phase}}, \quad (7)$$

where T_i - the time of implementation of the project; T_{phase} – the time of implementation of the project phase.

In this example, we can determine the phase’s budget as the first value, and the second value – the project’s budget. The main requirement when determining importance factor is a common scope for the project.

Let’s examine the calculating of efficiency of design decision factor as an example (Table 1).

In this table “a type of operations” is classified by the manner, which proposed in [5], where operations are divided into dependent, independent and dependent in small ranges of increasing resource. That is, if for the independent operation of increase resource, 6 man-hours were allocated, then the increase in manpower of performers won’t lead to a decrease of the total time of the operation. The column “type of resource allocation capacity” shows the nature of allocation of load on a command of performers during operation.

On the upper part of the Fig. 1, in circles with numbers from 1 to 9, breakpoints of quality control are shown. The circles with list elements (6.1, 8.1) denote additional points to clarify the process of the project. Overlay figures shows planned and actual works of the project, and their volume – the required amount of resources. Also on the right and below the picture, in the form of numerical values, according to intervals, the planned and actual number of resources is reflected.

Table 1.

Project settings

№ з/п	Process	Type of operation	Possible actions	Type of resource allocation capacity	Duration (h-s)	Used resource (monetary unit)
1	Process 1				15	47.5
1.1	Operation 1	Which depends on small range	The increase in intensity; the use of additional performers	Uniform distribution	6	24
1.2	Operation 2	Depending on small range	The increase in intensity; the use of additional performers	The increase by the end of the operation	4	16
1.3	Operation 3	Independent of increasing resource	Stimulating performers	The eduction by the end of the operation	5	7.5
2	Process 2				15	50
2.1	Operation 4	Independent of increasing resource	Stimulating performers Increasing the intensity of work	The lowest rate in the middle of the operation	8	15
2.2	Operation 5	Depending on small range	Increasing the intensity of work	Uniform distribution	7	35

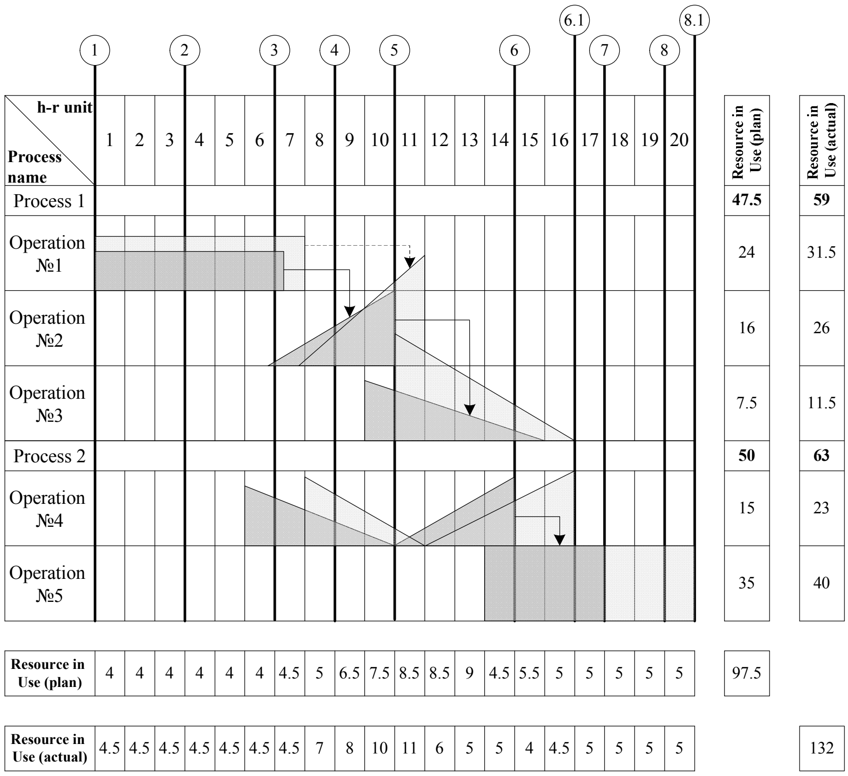


Figure 1. The resource map of decision-making fragment

Table 2.

Efficiency parameters

Time unit	1	2	3	4	5	6	7	8	9	10	11	12	13
Completion factor (plan)	0.04	0.08	0.12	0.16	0.21	0.25	0.29	0.34	0.41	0.49	0.52	0.56	0.59
Completion factor (actual)	0.03	0.07	0.1	0.14	0.17	0.2	0.24	0.29	0.35	0.48	0.51	0.56	0.59
Completion factor on this time range	0.83	0.83	0.83	0.83	0.83	0.83	0.82	0.85	0.86	0.88	0.98	1.0	1.0
Quality %	83	83	83	89	89	89	95	95	92	92	97	97	97
Absolute efficiency	0.69	0.69	0.69	0.74	0.74	0.74	0.78	0.81	0.79	0.81	0.95	0.97	0.98
Relative effectiveness	0.03	0.03	0.03	0.03	0.03	0.03	0.04	0.04	0.05	0.06	0.08	0.08	0.03
Time unit	14	15	16	17	18	19	20	21	22	23	24	25	26
Completion factor (plan)	0.64	0.69	0.74	0.79	0.85	0.9	0.95						
Completion factor (actual)	0.63	0.66	0.7	0.75	0.77	0.83	0.85	0.89					
Completion factor on this time range	0.99	0.96	0.94	0.92	0.91	0.9	0.89	0.89					
Quality %	97	97	97	95	91	91	95	95	93	93	93	92	92
Absolute efficiency	0.96	0.95	0.91	0.86	0.83	0.82	0.85	0.84					
Relative efficiency	0.04	0.05	0.05	0.05	0.04	0.04	0.04	0.04					

At the Fig.1 we can see that for the actual project works it took more resources than planned, with the quality, to reach the end of each work, is within (tab. 2).

The table 2 shows the necessary parameters to calculate absolute and relative efficiency of decision making. In the first line the time scale from 1 to 26 is given . The second line - the completion factor of the project according to the plan $f_{c(plan)}$, the third line – the completion factor of the actual works $f_{c(actial)}$, the fourth line – the completion factor f_c, the fifth line – the quality factor in percentage, in the sixth line – the absolute efficiency E_a, in the seventh line – the relative efficiency E_r .

Fig. 2 – the planned and actual resources' graph.

Fig. 3 – the relative efficiency of decision making changes. The relative efficiency e_r is marked with the dotted line. This index is the ratio of the planned effect Θ_p to the project fulfillment time:

$$e_r = \frac{\Theta_p}{T_p}, \tag{8}$$

where e_r – the relative efficiency boundary, Θ_p – planned effect (is taken as a unit).

Analysis of the resulting function allows to determine the importance of the decision to retain project performance within certain limits.

Fig.4. shows the function of absolute efficiency changes , where the dotted line is the border of the absolute efficiency, which in its turn, is equal to a predictable effect.

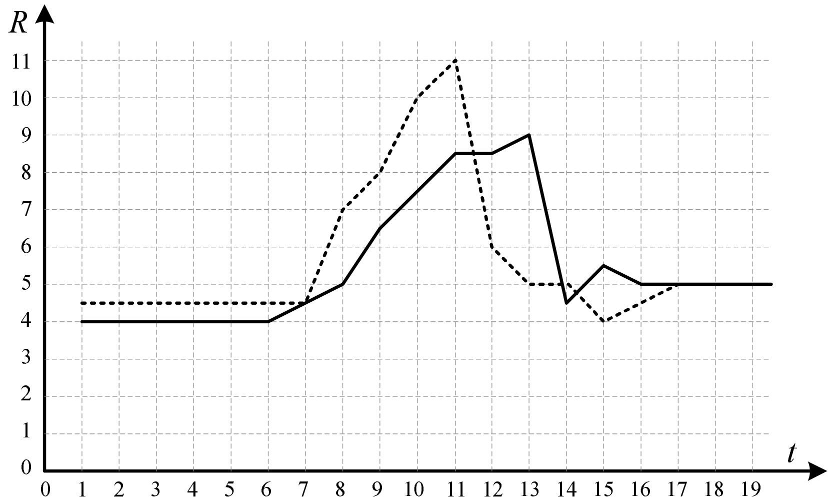


Figure 2. The resource in use graph: as planned – a solid line; under actual use – a dotted line

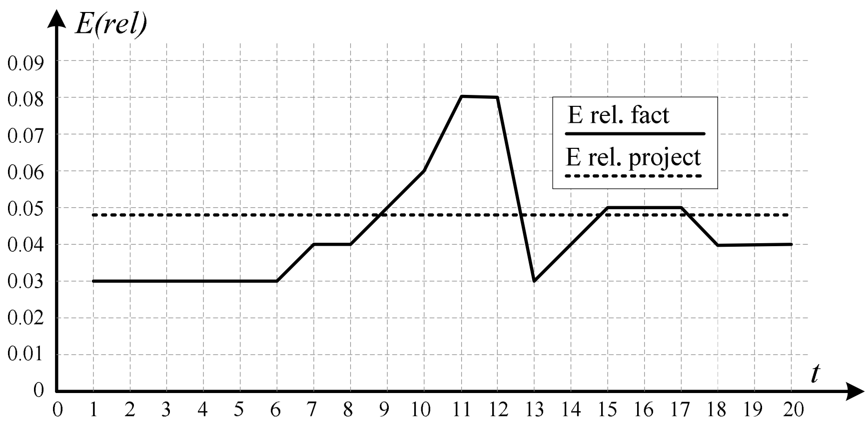


Figure 3. Relative efficiency of design decisions

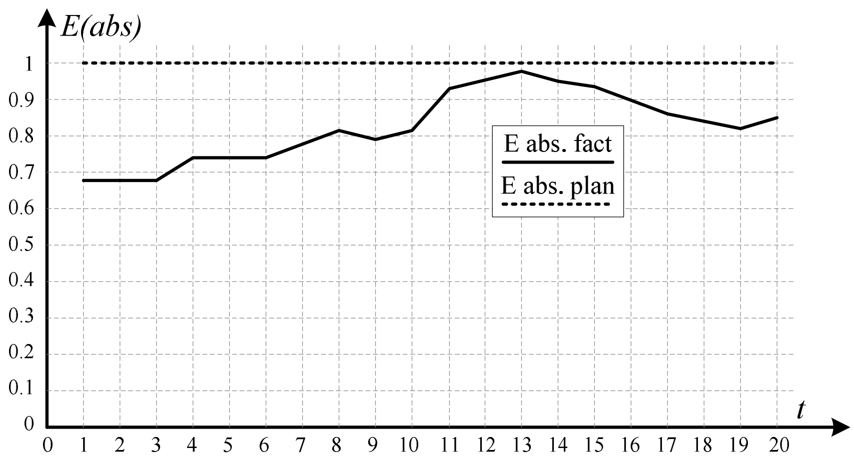


Figure 4. The absolute efficiency design decision performances' graph

As can be seen in Fig. 4, the indicators of absolute efficiency design decisions increase and come nearer to the absolute performances in a certain period of time (in this case from 10 to 13), and then the results decrease with their further growth.

This is due to the following: initially the project manager has boundary data and the imagination of a draft, and only with quantitative and qualitative growth of output data, the solution may be as close to optimum quality of a specific project. But over time, the leader must constantly adjust their actions and decisions as a whole to determine the right approach during the final project result creating.

For the decision making, during the information security systems development, it's necessary a lot of work in the resources analysis to do. These resources are needed for making the right decision to create the optimal information security structure.

When designing information security systems, resources mean the division on types: economic – organizational, labor (labor costs), financial; information (data collection for effective obtain reliable data: individual documents and individual files of documents in libraries, funds, banks and databases, information systems), which in their turn may be network or Internet resources; computing resources and time resources. All this imposes on the process of designing information security systems an additional leverage to take into account certain resources, that must be considered when developing a specific project.

A used resource is determined on the stage of conceptual design project with a prerequisite of design protection (the principle of "golden mean"): the cost of creating information security system should not be more than the value of the information, which this security system protects.

Conclusion

The analysis of the design process of information security has been established, that there is no unitary system of quantitative performances of efficiency of adopted project solution. The formalization of a proposed number of factors has a local character. The proposed technique is general for determining the general evaluating approaches of the effectiveness of information security systems, and partial – to assess the decision-making quality in the assessment methodology of requirements for information security systems [7].

References

1. Павлов, І.М. Формалізація проектних показників якості захисту інформації комплексної системи захисту інформації [Текст] / І.М. Павлов, В.О. Бірюков // Захист інформації. – 2011. – № 2(51). – С. 15–21.
2. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі / НД ТЗІ 3.7 – 003 – 05. – К.: 2005. – 35 с.
3. Широчин, В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / В.П. Широчин, В.Е. Мухин. – К.: ВЕК, 2000. – 111 с.
4. Щеглов, А.Ю. Проблемы и принципы проектирования систем защиты информации от НСД [Текст] / А.Ю. Щеглов // Сборник «Экономика и производство». – М.: НиТ, 2001. – № 3. – С. 34–46.
5. Чимшир, В.И. Методика построения ресурсных карт в проектном управлении [Текст] / В.И. Чимшир // Журн. Восточно-Европейский журнал передовых технологий. –2012. – № 4/8(58). – С. 49–53.
6. Потьомкін, М.М. Загальний підхід до формування вимог до складних систем [Текст] / М.М. Потьомкін, А.А. Седляр // Збірник наукових праць ЦНДІ ЗСУ. – 2013. – № 3 (65). – С. 267–281.
7. Павлов, І.М. Методологія обґрунтування основних загальносистемних вимог до проектування систем захисту інформації на об'єктах критичної інфраструктури [Текст] / І.М. Павлов. // Інформатика та математичні методи в моделюванні. – 2014. – т.1, №3. – С. 263–271.

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ ПРОЕКТНИХ РІШЕНЬ ПРИ РОЗРОБЦІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ РЕСУРСНИХ КАРТ

І.М. Павлов

Державний університет телекомунікацій,
вул. Солом’янська, 7, Київ, 03680, Україна; e-mail: pavlov@ukr.net

У статті представлена методика кількісної оцінки ефективності проектних рішень при розробці систем захисту інформації.

Ключові слова: абсолютна ефективність, відносна ефективність, методика, проект, ресурсні карти, системи захисту інформації,ефективність проектного рішення.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОЕКТНЫХ РЕШЕНИЙ ПРИ РАЗРАБОТКЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ РЕСУРСНЫХ КАРТ

И.Н. Павлов

Государственный университет телекоммуникаций,
ул. Соломенская, 7, Киев, 03680, Украина; e-mail: pavlov@ukr.net

В статье представлена методика количественной оценки эффективности проектных решений при разработке систем защиты информации.

Ключевые слова: абсолютная эффективность, методика, проект, оптимальная эффективность, ресурсные карты, система защиты информации, эффективность проектных решений.

УДК 004.621.3:681.324

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 19-27

АНАЛИЗ ТОПОЛОГИИ СЕТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Е.А. Скоробогатько, Н.П. Тимченко, В.А. Хорошко, Ю.Е. Хохлачёва

Национальный авиационный университет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

В работе рассматривается оптимизация структур программно-моделирующего комплекса и системы передачи информации с анализом устойчивости топологии систем передачи информации на основе понятия двойственности, а также оперативность прохождения конфиденциальной информации по этапам обработки. Выработаны рекомендации по пропускной способности этих этапов и систем в целом.

Ключевые слова: информационная безопасность, оптимизация, сети передачи информации, программно-моделирующий комплекс, пропускная способность.

Введение

Актуальной стороной вопроса информационного обеспечения государственных структур является решение проблемы информационной безопасности и технологической независимости рынка информационных технологий Украины от зарубежных поставщиков или максимальное уменьшение этой зависимости. Одновременному решению данной проблемы по всем направлениям препятствуют экономические факторы и общее отставание Украины от зарубежных разработчиков и производителей в области информационных технологий. В подобных условиях цели национальной доктрины информационной безопасности Украины в части развития отечественных информационных технологий должны реализовываться поэтапно, т.е. ориентироваться на стандарты (топологии и архитектуры) и учитывать пути эволюции технологии [1]. Одним из приоритетных направлений информационных технологий в Украине являются отечественные телекоммуникационные средства построения распределенных корпоративных сетей, систем электронного документооборота и сетей передачи информации различных служб. Режим передачи и обработки характеризуется наличием в сети пользователей, потенциально не допущенных к обрабатываемой и передаваемой информации, составляющей государственную и служебную тайну. В виду этого таким сетям и системам свойственны многочисленные функциональные требования, а также ограничения по обработке и передачи информации, которые частично определены нормативными и руководящими документами [1].

Известно, что в этих сетях для повышения надежности, оперативности и достоверности конфиденциальной информации (КИ) применяются специальные средства вычислительной техники, так называемые программно-моделирующие комплексы (ПМК). При этом эффективность применения ПМК зависит от его комплектации входными и выходными модулями, а также количества оконечных рабочих станций (ОРС). Обычно при разработке таких сетей комплектация ПМК выбирается интуитивно на основании имеющегося опыта у разработчиков или волевого решения руководителя, вытекающего из экономической целесообразности затрат. Такой подход не всегда оправдан с точки зрения пропускной способности сети, оперативности и достоверности приема КИ. Поэтому научно обоснованный выбор структуры ПМК и сетей передачи информации (СПИ) для различных систем передачи информации с учетом нагрузки на корпоративную сеть является весьма актуальной задачей.

Кроме того, в ряде математических моделей, описанных в [2,3] и используемых до исследования СПИ, содержится параметр, который представляет интенсивность информационного обмена между ОРС. Изменение величин интенсивностей информационного обмена может приводить к изменениям в топологии сети. Для сетей, в которых осуществляется перекоммутация, разработаны алгоритмы, предусматривающие случаи возможного изменения топологии [4].

Анализ математических модулей, содержащих изменяемый параметр, на устойчивость топологии СПИ является важным на начальном этапе системной интеграции ПКМ сети.

Цель работы

Решение задачи оптимизации структуры ПМК, СПИ и анализ устойчивости топологии СПИ на основе использования понятий двойственности.

Основная часть

В соответствии с целью работы для оптимизации структуры ПМК достаточно рассмотреть последовательную цепь основных операций, непосредственно участвующих в обработке входящей КИ, для чего ПМК можно разбить на три уровня иерархии:

1. Подсистема ОРС;
2. Подсистема коммутатор-сервер;
3. Подсистема входных устройств.

Используя системный подход, составляется аналитическая модель автоматизированной обработки входящей КИ в ПМК.

Подсистема ОРС находится на высшей ступени иерархии, и поэтому обобщенный критерий на этом уровне будет обрабатывать оптимальную комплексную структуры ПМК в целом. В качестве такого критерия целесообразно выбрать время обработки КИ, не превышающее заданного нормативного значения.

Подсистема коммутатор-сервер находится ниже. Пропускная способность данного уровня существенно влияет на пропускную способность выше стоящей подсистемы ОРС. Следовательно, на этом уровне в качестве обобщенного критерия целесообразно выбирать пропускную способность λ_2.

Самой низшей системой иерархической цепи является подсистема входных устройств. Как и в предыдущем случае, в качестве обобщенного критерия на этом уровне целесообразно выбирать пропускную способность λ_1.

Согласно системному подходу критерии эффективности должны быть связаны функциональными зависимостями, представляющими собой аналитические модели функционирования подсистем и ПМК в целом, т.е. комплект математических моделей ПМК должен строиться таким образом, чтобы модели и критерии чередовались между собой: модель-критерий-модель-критерий и так далее.

Подсистемы ПМК можно описать последовательной n-фазой системы массового обслуживания [5]. Решая дифференциальные уравнения состояний, можно определить такие внутренние характеристики подсистем, как, например, количество сообщений в очереди S_i, среднее время ожидания сообщения в очереди $t_{оч_i} (i = 0,1,2,...)$, позволяющие оценить технические возможности отдельных устройств и подсистемы в целом.

В качестве обобщенного критерия на высшем уровне иерархии ОРС выступает $\bar{t}_{об}$ – время обработки КИ в ПМК, которое не должно превышать заданное $\bar{t}_{зад}$:

$$\bar{t}_{об} \le \bar{t}_{зад}. \tag{1}$$

Левую часть неравенства (1) можно разложить на следующие интервалы времени:

1. Среднее время обработки КИ в адаптере мультиплексора передачи данных − $\bar{t}_{ад}$;
2. Среднее время обработки КИ в специализированном блоке − $\bar{t}_{р}$;
3. Среднее время обработки КИ в принтере − $\bar{t}_{пр}$;
4. Среднее время устранения общих искажений − $\bar{t}_{он}$;
5. Среднее время считывания и корректировки обработанного текста по экрану дисплея − $\bar{t}_{k}$;
6. Среднее время ожидания КИ в очереди на передачу по каналу связи − $\bar{t}_{оч}$;
7. Среднее время ожидания КИ в очереди на обработку в специализированном блоке $\bar{t}_{оч_1}$;
8. Среднее время ожидания обработанного текста в очереди на печать − $\bar{t}_{оч_2}$.

В результате получаем:

$$\bar{t}_{об} = \bar{t}_{ад} + \bar{t}_{р} + \bar{t}_{пр} + \bar{t}_{оп} + \bar{t}_{к} + \bar{t}_{оч} + \bar{t}_{оч_1} + \bar{t}_{оч_2}. \tag{2}$$

Проанализируем правую часть выражения (2). Параметры $\bar{t}_{ад}, \bar{t}_{р}, \bar{t}_{пр}$ определяются техническими возможностями соответственно адаптера канала, специализированного блока и принтера, поэтому в каждом конкретном случае они будут заданы и равны

$$\bar{t}_{ад} = \frac{1}{\mu}, \;\; \bar{t}_{р} = \frac{1}{\mu_1}, \;\; \bar{t}_{пр} = \frac{1}{\mu_2},$$

где μ_i − техническая производительность i-го устройства.

Значения параметров $\bar{t}_{оп}$ и $\bar{t}_{к}$ зависят от квалификации и опыта работы обслуживающего персонала. В качестве их количественной оценки можно взять показатели «среднего» сотрудника, которые определяются статистическим путем, и их можно считать заданными величинами.

Параметр $\bar{t}_{оч_i}$ $(i = 0,1,2,...)$ полностью определяется техническими возможностями комплекса, и поэтому может служить переменной величиной, по которой оптимизируется обобщенный показатель $\bar{t}_{об}$ при заданной производительности устройств ПМК.

Время пребывания КИ в очереди $\bar{t}_{оч_i}$ можно уменьшить путем повышения производительности соответствующих устройств подсистем либо путем увеличения числа обслуживающих устройств. Очевидно, при оптимизации ПМК по обобщенному критерию (1) необходимо использовать оба эти пути. При этом наиболее эффективным с точки зрения уменьшения $\bar{t}_{об}$ является первый путь, поскольку, повышая производительность устройств ПМК, тем самым одновременно уменьшаем все слагаемые выражения (2), кроме $\bar{t}_{оп}$ и $\bar{t}_{к}$. А увеличивая число обслуживающих устройств, уменьшаем только непосредственно величины $\bar{t}_{оч_i}$.

На практике возникает необходимость определения распределения времени обработки КИ по этапам прохождения в ПМК.

Общее время обработки $\bar{t}_{об}$ представляется по этапам следующим образом:

$$\bar{t}_1 = \bar{t}_{ад} + \bar{t}_{оч};\ \bar{t}_2 = \bar{t}_{т} + \bar{t}_{оп} + \bar{t}_{оч1} + \bar{t}_{оч2};\ \bar{t}_3 = \bar{t}_{к};\ \bar{t}_4 = \bar{t}_{пр}.$$

При этом среднее время пребывания КИ в очередях на соответствующих этапах обработки легко определяется: очередь перед принтером, очередь за счет печати будет решением динамических уравнений состояний на каждом из этапов и будет иметь вид:

$$\bar{t}_{оч} = \frac{P(m,\alpha(\dfrac{\tilde{\beta}}{(1-\tilde{\beta})^2}}{\left[R(m,\alpha) + P(m,\alpha(\dfrac{\tilde{\beta}}{1\text{-}\tilde{\beta}}\right]\lambda}, \tag{3}$$

где $R(m,\alpha) = \sum\limits_{k=0}^{m} \dfrac{\alpha^k}{k!} l^{-\alpha}$; $\tilde{\beta} = \dfrac{\alpha}{m} = \dfrac{\alpha}{m\mu}$; $\alpha = \dfrac{\lambda}{\mu}$:

$$\bar{t}_{оч1} = \frac{P(n,\alpha_1)\dfrac{\tilde{\beta}_1}{(1-\tilde{\beta}_1)^2}}{\left[R(n,\alpha_1) + P(n,\alpha_1)\dfrac{\tilde{\beta}_1}{1\text{-}\tilde{\beta}_1}\right]\lambda_1}, \tag{4}$$

где $\alpha_1 = \dfrac{\lambda_1}{\mu_1}$; $\tilde{\beta}_1 = \dfrac{\lambda_1}{\mu_1 n} = \dfrac{\lambda_1}{n}$;

$$\bar{t}_{оч2} = \frac{P(1,\alpha_2)\dfrac{\tilde{\beta}_2}{(1-\tilde{\beta}_2)^2}}{\left[R(1,\alpha_2) + P(1,\alpha_2)\dfrac{\tilde{\beta}_2}{1\text{-}\tilde{\beta}_2}\right]\lambda_2}, \tag{5}$$

где $R(1,\alpha_2) = \alpha_2 e^{-\alpha_2}$; $\tilde{\beta}_2 = \dfrac{\alpha_2}{\mu_2}$; $\alpha_2 = \dfrac{\lambda_2}{\mu_2}$.

Полученные выражения (1) – (5) легко программируются на ПЭВМ, что позволяет оценить оптимальность выбранной структуры.

Вторая решаемая задача заключается в определении диапазонов изменения величин интенсивностей информационного обмена, в которых топология СПИ рассчитывается с помощью математической модели. Предполагается, что варианты топологии отображаются регулярным графом, где между каждой парой ОРС иметься одинаковое количество маршрутов. Маршруты передачи информации представляются набором значений булевых переменных $\{\delta_{ijz}^{rq}, i, j, z, q = \overline{1,v}, s = \overline{1,p}\}$, ν − число ОРС; z – число типов сообщений, передаваемых в СПИ; $\delta_{ijz}^{rq} = 1$ означает наличие линий передачи топологии z-того типа между ОРС i и j в маршруте $(r,q) \in W$ (W – множество маршрутов). Для СПИ регулярной топологии характерно свойство достижения минимальных значений среднего времени задержки и вероятности отказа [6].

Рассмотрим математическую модель, описывающую задачу оптимизации топологии СПИ в классе регулярных графов по критерию среднего времени задержки $\overline{T}$ [2,3].

Математическая модель имеет следующий вид:

$$[PIH]\overline{T} = \frac{1}{y}\sum_{i=1}^{v}\sum_{j=1}^{v}\sum_{z=1}^{p}\frac{f_{ijz}}{d_{ij} - f_{ijz}} \tag{6}$$

$$\sum_{i=1}^{v}\sum_{j=1}^{v}\sum_{=1}^{\rho} C_{ijz}(f_{ijz}) \le C_{доп} \tag{7}$$

$$\sum_{\mathrm{j=1}}^{v}\delta_{\mathrm{ijz}}^{\mathrm{iq}} = \sigma, i, q = \overline{1,k},\ i \ne q,\ s = \overline{1,\rho} \tag{8}$$

$$\delta_{ilz}^{rd} = \{0,1\}, \sigma \ge 2,\ i, j, \sigma, q = \overline{1,k}\ ,\ z = \overline{1,\rho}\ . \tag{9}$$

Здесь f_{ijz}, d_{ij} − трафик в линии передачи информационного сообщения z-типа между i-м и j-м ОРС и пропускная способность соответственно; γ − суммарный трафик сообщений, передаваемых в СПИ; C_{ijz} − стоимость передачи сообщения z-го типа между i-м и j-м ОРС; h_{rqz} − интенсивность информационного обмена между z-м и q-м ОРС; σ − число линий передачи в ОРС; $C_{доп}$ − допустимое значение стоимости передачи информации в СПИ.

В связи с наличием нелинейности в математической модели (6)-(10) исследование устойчивости топологии сети предлагается проводить на основе необходимых и достаточных условий Куна-Таккера оптимальности задачи нелинейного программирования [7]. Для этого случая справедлива следующая теорема.

Теорема 1. Пусть δ_{ijz}^{rq} − оптимальное значение переменных, определяющих сообщение z-го типа между i-м и j-м ОРС в маршруте СПИ $(r,q) \in W$ (W − множество маршрутов). Оптимальная топология, представляемая множеством W, устойчива, если выполняются условия вида

$$0 \le h_{rqz} \le \frac{\sigma}{C^0\delta_{ijz}^{rq}}\left[C доп - \sum_{\substack{i_1=1 \\ i_1\ne i}}^{v}\sum_{\substack{f_1=1 \\ j_1\ne j}}^{v} C_{i_1 j_1} z(f_{i_1 j_1 z})\right] - \sum_{\substack{r_1=1 \\ r_1\ne r}}^{v}\sum_{\substack{q_1=1 \\ q_1\ne q}}^{v} h_{r_1 q_1} z\,\delta_{ijz}^{r_1 q_1}, \tag{10}$$

$$i, j, r, q = 1,,\ z = \overline{1,\rho}\,.$$

Доказательство теоремы 1. Необходимые условия оптимальности решения задачи, описываемой математической моделью (6)-(10), записывается в следующем виде:

$$\frac{h_{rqz}\,d_{ij}}{\gamma\sigma\left(d_{ij} - \sum\limits_{r_1 q_1}^{v}\frac{h_{r_1 q_1} z\,\delta_{ijz}^{r_1 q_1}}{\sigma}\right)^2} - \lambda_1 C^0\frac{h_{rqs}}{\sigma} = 0; \tag{11}$$

$$i, j, r, q = \overline{1,v};\ i \ne r\ ;$$

$$\lambda_1\left[\sum_{i=1}^{v}\sum_{j=1}^{v}\sum_{z=1}^{\rho}C_{ijz}(f_{ijz})-C_{доп}\right]=0;$$

$$\lambda_2 iqz\left(\sum_{j=1}^{v}\delta_{ijz}^{iq}-\sigma\right)=0,\ i,q=\overline{1,v},\ i\neq q,\ z=\overline{1,\rho};$$

$$\sum_{i=1}^{v}\sum_{j=1}^{v}\sum_{z=1}^{\rho}C_{ijz}(f_{ijz})\le C_{доп},$$

$$\sum_{j=1}^{v}\delta_{ijz}^{iq}=\sigma,\ i,q=\overline{1,v},\ i\neq q,\ s=\overline{1,\rho};$$

$$f_{ijz}=\sum_{r=1}^{v}\sum_{q=1}^{v}\frac{h_{rqz}\delta_{ijz}^{rq}}{\sigma},\ i,j,q=\overline{1,v},\ z=\overline{1,\rho};$$

$$\delta_{ijz}^{\delta q}=\{0,1\},\sigma\ge 2,i,j,r,q=\overline{1,v},\ z=\overline{1,\rho};$$

$$\lambda_1\ge 0,\lambda_2\ge 0,\ i,q=\overline{1,v},\ z=\overline{1,\rho}.$$

Здесь λ_1, $\lambda_{2iqz}(i,q=\overline{1,v},s=\overline{1,\rho})$ определяют переменные задачи, двойственной к (6)-(10), характеризуют удельный информационный поток сообщений и число линий передачи i-го ОРС i,j; C^0 − стоимость единицы пропускной способности линии передачи сообщений.

Из равенства (12) получаем $h_{rqz}^{\min}=0$, а из неравенства (7) выражение для $h_{rqz}^{\min}$ принимает вид

$$h_{rgz}^{\max}=\frac{\sigma}{C^0\delta_{ijz}^{rq}}\left[C_{доп}-\sum_{\substack{i_1=1\\ i_1\neq i}}^{v}\sum_{\substack{f_1=1\\ j_1\neq j}}^{v}\sum_{z=1}^{p}c_{i_1j_1z}(f_{i_1j_1z})\right]-\sum_{\substack{r_1=1\\ r_1\neq r}}^{v}\sum_{\substack{q_1=1\\ q_1\neq q}}^{v}h_{r_1q_1z}\delta_{ijz}^{rq},\ i,j,r,q=\overline{1,v},\ z=\overline{1,\rho}.$$

Соотношения, определяющие диапазоны $\left\lfloor h_{rqz}^{\min},h_{rqz}^{\max}\middle| r,q=\overline{1,v},z=\overline{1,p}\right\rfloor$ изменения величин интенсивностей информационного обмена между ОРС, представляют собой необходимые условия устойчивости регулярной топологии СПИ. Покажем, что данные соотношения определяют достаточные условия устойчивости топологии. Для этого исследуем угловые детерминанты $H_t^{(1)},H_t^{(2)}$,.. матрицы $\nabla^2 H_t$ вторых производных функции (1). В результате преобразований и расчетов получено $H_t^{(1)}>0,H_t^{(2)}>0$,.., что обеспечивает положительную определенность матрицы $\nabla^2 H_t$ и выпуклость функции (6). Ограничения (7) - (9) определяют выпуклое множество. Таким образом, соотношения, определяющие диапазоны $\left\lfloor h_{rqz}^{\min},h_{rqz}^{\max}\middle| r,q=\overline{1,v},z=\overline{1,p}\right\rfloor$, представляют собой также достаточные условия устойчивости топологии. Теорема доказана.

Теперь необходимо оценить оптимальность трафиков передачи информационных сообщений. Представим СПИ в виде неориентированного взвешенного графа $G=(V,C,F)$, где V − множество вершин (ОРС), $|V|=H,C$ − множество ребер (стоимость каналов или линий связи) [8,9].

Пусть на графе G в некоторый момент времени уже решена задача канала поиска оптимальных маршрутов к всем ОРС множества $V_{\hat{s}}=V\setminus\{v_s\}$ из начальной ОРС v_s, т.е.

построено дерево оптимальных маршрутов с корнем в ОРС v_s. Обозначим это дерево как ОРС T_∂.

Для каждого канала связи $e_{ij} \in E$ на шкале значений весов определены точки вхождения в дерево $f_{i,j}^t$ и точки вхождения во множество замены $f_{i,j}^s$, причем $f_{i,j}^t \le f_{i,j}^s$, под которыми понимается максимально возможный вес канала $e_{i,j}$ при его вхождении в множество каналов дерева $E_T \in T_\partial$ в множество каналов замены для дерева $E_S \in T_\partial$ соответственно.

Обозначим $f_{i,j}$ − вес канала, содержащего ОРС v_i и v_j. ОРС v_i располагается шире по иерархии в дереве оптимальных маршрутов относительно v_j. Множество E_T − множества каналов, каждый элемент которого входит, по крайней мере, в один оптимальный маршрут связи из начального ОРС, E_R − множество остальных каналов. $E_R \cup E_T = \mathrm{E}, E_R \cap E_T = \phi$. Обозначим V_{T} − множество ОРС, к которым найден оптимальный маршрут связи из начального ОРС, V_{R} − множество остальных ОРС, $V_R \cup V_{\mathrm{T}} = V, V_R \cap V_{\mathrm{T}} = \phi$.

Исходя из этого, можно сформулировать задачу динамического управления трафиком СПИ следующим образом. Для каждого класса трафика ($s = \overline{1,\eta}$) необходимо установить определенный маршрут ω, и построить для него закон управления $u^s(t)$ на интервале $[t_1;t_2]$, где модель динамики трафика имеет вид динамической системы:

$$x^s(k+1) = A^s x^s(k) + B^s u^s(k) + L[x^s(k)],$$

$$d^s = D^s L[x^s(k)],$$

при заданных критериях:

$$\sum_{k=t_1}^{t_2} \left[\hat{d}^s(k) - d^s(k)\right]^2 \to \min$$

$$n_1 \le d^s(k) \le n_2,$$

где $x^s \in R^n$ − n-мерный вектор состояний системы; $u^s \in U^s \subset R$ − управление; k − дискретное время; $A^s u\, B^s$ − матрицы; $L[x^s(k)]$ − нелинейная функция; $\hat{d}^s(k)$ − необходимая пропускная способность маршрута; $d^s(k)$ − необходимая пропускная способность маршрута в условиях ограничений; n_1, n_2 − заданные ограничения на маршруте. Следовательно, для этого случая справедливы следующие теоремы.

Теорема 2. Если $nf_{i,j} > f_{i,j}$ и $e_{i,j} \in E_T$, то изменению могут подвергнутся оптимальные маршруты и оценки их длины для ОРС $V_T^{(V_i)}$.

Доказательство теоремы 2. Пусть увеличится вес канала связи $e_{ij} \in E_T$, который входит, по крайней мере, в один оптимальный маршрут ψ_{k}, допустим в $\psi_{\mathrm{k,p}}$. ОРС v_{k}, оптимальные маршруты, в которые канал связи e_{ij} не входит, будут составлять множество V_T ОРС. Пусть существует оптимальный маршрут $\psi_{\mathrm{k}} = \psi_{\mathrm{k,p}}$ к ОРС v_{k} и известно, что канал связи e_{ij} не входит в этот маршрут. Тогда увеличение стоимости этого канала со значениями $f_{i,j}$ до $nf_{i,j}$ не изменит маршрута этого пути и не повлияет на величину длины маршрута $y_{k,p}$. Еще до увеличения стоимости рассматриваемого канала включение этого канала в оптимальный маршрут приводило к увеличению длины маршрута. Все ОРС, не вошедшие в множество V_T, будут составлять множество V_R. Оптимальные маршруты к ОРС множества $v \in V_R$ станут «недействительными», т.е. невозможно будет без дополнительного расчета сказать, останутся они такими же или оптимальный маршрут к ним не будет включать изменившийся канал связи. Теорема доказана.

Терема 3. Если $nf_{i,j} < f_{i,j}$ и $\mathrm{e}_{\mathrm{i,j}} \in E_T$, то без изменения останутся оптимальные маршруты для ОРС множества $v \in \overline{V}_T^{(v_j)} \cup V^{(V_i)}$, а для ОРС множества $V^{(V_i)}$ неизменными останутся и оценки длин оптимальных маршрутов.

Доказательство теоремы 3. Пусть уменьшилась стоимость канала связи $\mathrm{e}_{\mathrm{i,j}} \in E_T$, входящего в оптимальный маршрут $\psi_{\mathrm{k}} = \psi_{\mathrm{k,p}}$ к ОРС $v_{\mathrm{k}} \in V$. Канал связи $\mathrm{e}_{\mathrm{i,j}}$ после изменения также будет входить в оптимальный маршрут ψ_{k} к ОРС v_{k}. Поскольку стоимость канала связи $f_{i,j}$ изменилась, то измениться должны длины всех маршрутов $\psi_{\mathrm{t},\tau}$, в которые входит этот канал связи. Действительно, если канал связи $\mathrm{e}_{\mathrm{i,j}}$ входит в какой-либо оптимальный маршрут, и стоимость этого канала уменьшиться, то это изменение не потребует изменения оптимального маршрута $\psi_{\mathrm{k,p}}$ (последовательности каналов) и длина маршрута $y_{\mathrm{k,p}}$ изменится на величину изменения стоимости канала. Маршруты $\psi_{\mathrm{s}}, v_s \notin V_T^{(V_j)} \cup V^{(V_i)}$ станут «недействительными», т.е. невозможно будет без дополнительного расчета сказать, останутся они такими же, или оптимальный маршрут к ним будет включать изменившейся канал связи. Следовательно, теорема доказана.

Выводы

Полученные соотношения позволяют оценить оптимальность выбранной структуры программно-моделирующего комплекса и системы передачи информации, а также оперативность прохождения конфиденциальной информации по этапам обработки и выработать рекомендации по оптимизации пропускной способности самих этапов и системы в целом. Кроме того, соотношения, которые получены в результате параметрического исследования системы математических моделей оптимизации регулярной топологии сети передачи информации, позволяют получить обоснованные решения на начальном этапе системной интеграции информационных ресурсов.

Список литературы

1. Хорошко, В.А. Кибертерроризм и информационная безопасность / В.А. Хорошко, М.Е. Шелест // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2014. – Вип. 1(27). – С. 9–14.
2. Шарейко, Л.А. Комплексный анализ сетей передачи данных / Л.А. Шарейко – Винница: УНІВЕРСУМ, 1998. – 183 с.
3. Дудикевич, В.Б. Інформаційна модель безпеки технологій зв’язку / В.Б. Дудикевич, Т.В. Микитин, Р.І. Банах, А.І. Ребець, В.О. Хорошко // Інформатика та математичні методі в моделюванні. – 2014. – Т. 4, №2. – С.137–149.
4. Abu-Amara, H. Self-stabiliziting topology maintenance protocols for high-speed networks / H. Abu-Amara, B.A. Coan, A. Kanevsky, J.I. Welch // IEEE/ACM Trans.Networking. – 2006. – Volume 4, №6. – PP. 902–912.
5. Анисимов, В.В. Элементы теории массового обслуживания и асимптотического анализа систем / В.В. Анисимов, О.К. Закусило, В.С. Донченко. – К: Вища школа, 1987. – 248 с.

6. Егоров, Ф.И. Математическое моделирование процессов передачи и обработки информации в телекоммуникационных сетях / Ф.И. Егоров, Е.А. Скоробогатько, В.И. Степаненко, В.А. Хорошко // Інформатика та математичні методи в моделюванні. – 2012. – Т.2, №3. – С. 210–221.
7. Штойер, Р. Многокритериальная оптимизация. Теория, вычисления и приложения / Р. Штойер. – М: Радио и связь, 1992. – 504 с.
8. Хорари, Ф. Теория графов / Ф. Хорари. – М: Мир, 1973. – 300 с.
9. Оре, О. Теория графов / О. Оре. – М: Наука, 1980. – 336 с.

АНАЛІЗ ТОПОЛОГІЇ МЕРЕЖІ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Скоробогатько Е.А., Тимченко Н.П., Хорошко В.О., Хохлачёва Ю.Є.

Національний авіаційний університет,
пр. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

У роботі розглядається оптимізація структур програмно-моделюючого комплексу та системи передачі інформації з аналізом стійкості топології систем передачі інформації на основі поняття подвійності, а також оперативність проходження конфіденційної інформації по етапах обробки та вироблені рекомендації щодо пропускної спроможності цих етапів і систем в цілому.

Ключові слова: інформаційна безпека, оптимізація, мережі передачі інформації, програмно-моделюючий комплекс, пропускна здатність.

ANALYSIS OF NETWORK TOPOLOGY INFORMATION

Skorobogatko E.A, Timchenko N.P, Khoroshko V.A, Hohlachëva Y.E

National Aviation University,
pr. Komarova, 1, Kiev, 03058, Ukraine; e-mail: professor_va@ukr.net

The paper deals with the optimization of structures and software modeling complex systems and information transfer with the analysis of the stability of the topology information transmission systems based on the concept of duality, as well as the efficiency of transmission of confidential information processing steps and recommendations on the capacity of these steps and systems in general.

Keywords: information security, optimization, network information, software and modeling complex, bandwidth.

УДК 621.396.931

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 28-37

О ВЛИЯНИИ ВИДА ОРТОГОНАЛЬНОГО ПРЕОБРАЗОВАНИЯ НА ПИК-ФАКТОР СПЕКТРА СИГНАЛОВ В СИСТЕМАХ С CDMA

М.И. Мазурков, А.В. Соколов, Н.А. Барабанов

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина, e-mail:alart@stream.com.ua

В статье исследуется влияние вида ортогонального преобразования на пик-фактор сигналов в системах с технологией кодового разделения каналов. Рассматриваются все пять классов ортогональных преобразований порядка N=16, построенных на основе функций Уолша, а также дискретное преобразование Фурье и преобразования, основанные на ортогональных функциях Виленкина-Крестенсона. Найдено семейство троичных последовательностей, обладающих равномерным спектром Виленкина-Крестенсона.

Ключевые слова: CDMA, пик-фактор, ортогональное преобразование.

Введение

В настоящее время широкое распространение получили системы радиосвязи поколений 3G, 4G, а также проводится активная разработка перспективной технологии 5G, которые основаны на технологии кодового разделения каналов MC-CDMA (Multi-Carrier Code Division Multiple Access). Технология CDMA обладает множеством неоспоримых преимуществ, среди которых гибкость распределения ресурсов, бóльшая защищенность каналов связи, более рациональное использование мощности передатчика [1].

Данные преимущества является следствием механизма разделения каналов, основанного на применении системы ортогональных сигналов, в качестве которых чаще всего используются функции Уолша. Так, биты исходных данных d_i, поступающих по каждому каналу изменяют знак одной из ортогональных функций W_i. Далее происходит умножение на некоторую константу g_i (чаще всего принимают $g_i = 1$), суммирование, модуляция и передача трансформант в канал связи (рис.1) [2]. Таким образом, передаваемый в канал связи сигнал является, по сути, последовательностью коэффициентов преобразования Уолша-Адамара.

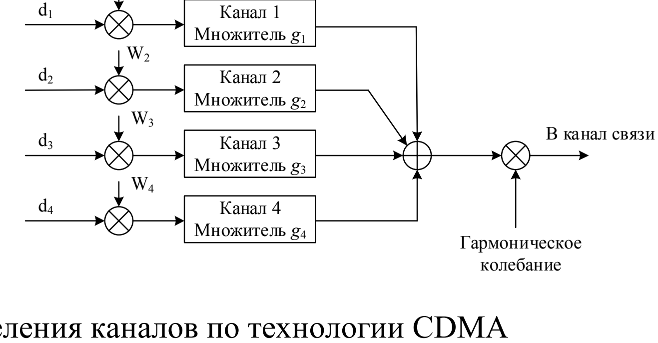


Рис. 1. Схема разделения каналов по технологии CDMA

Пусть, например, $d_1 = [1,1]$, $d_2 = [-1,-1]$, $d_3 = [-1,1]$, $d_4 = [1,-1]$, а в качестве системы ортогональных функций выбраны функции Уолша длины $N = 2^k$, упорядоченные по Адамару [3]

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \tag{1}$$

где $H_1 = 1$.

Для нашего случая $k = 4$, таким образом, имеем систему функций

$$\begin{bmatrix} W_1 = +1,+1,+1,+1; \\ W_2 = +1,-1,+1,-1; \\ W_3 = +1,+1,-1,-1; \\ W_4 = +1,-1,-1,+1; \end{bmatrix}$$

Выполняя преобразование (рис. 1) получаем результирующий сигнал, который подается на устройство модуляции

$$\begin{array}{cccc} +1 & +1 & +1 & +1 \\ -1 & +1 & -1 & +1 \\ -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 \\ \hline 0 & 0 & 0 & 4 \end{array} \qquad \begin{array}{cccc} +1 & +1 & +1 & +1 \\ -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 \\ -1 & +1 & +1 & -1 \\ \hline 0 & 4 & 0 & 0 \end{array} \ . \tag{2}$$

Полученная последовательность $S = [0,0,0,4,0,4,0,0]$ после модуляции подается в канал связи, и далее, на приемной стороне возможно выделение сигнала каждого из каналов связи в соответствии с формулой [1] $d_a = \sum_{i=0}^{N} S \cdot W_a \Big/ \left(g_a N\right)$.

Например, можем выделить исходное сообщение, переданное по второму каналу

$$\times\begin{array}{cccc} 0 & 0 & 0 & 4 \\ +1 & -1 & +1 & -1 \\ \hline 0 & 0 & 0 & -4 \end{array} \quad \times \quad \begin{array}{cccc} 0 & 4 & 0 & 0 \\ +1 & -1 & +1 & -1 \\ \hline 0 & -4 & 0 & 0 \end{array}$$

Вычисляя сумму, и разделив её на $g_2 N$, получаем исходный сигнал $d_2 = [-1,-1]$.

Анализ примера работы системы кодового разделения каналов (рис. 1) приводит к выводу, что передаваемый в канал связи сигнал S является набором коэффициентов преобразования Уолша-Адамара, которые обладают высоким значением пик-фактора

$$k = \frac{P_{\max}}{P_{cp}} = \frac{1}{N} \max_t \left\{ \left| S(T) \right|^2 \right\}, \tag{3}$$

что приводит к таким недостаткам применяемой технологии CDMA как нерациональное использование мощности передатчика, возрастание нелинейных искажений.

Для преодоления данного недостатка может быть использован особый класс кодов, называемый С-кодами, каждое кодовое слово которых обладает минимальным значением пик-фактора $к$. При использовании в качестве ортогональной системы сигналов функций Уолша наилучшим значением пик-фактора $k=1$ обладают бент-последовательности, которые могут быть использованы в качестве кодовых слов С-кода.

Бент-последовательности [4] — бинарные последовательности $B=[b_0, b_1, ..., b_j, ..., b_{n-1}]$, где коэффициенты $b_i \in \pm 1$, четной длины $N=2^{2m}$, которые обладают равномерным по модулю спектром Уолша-Адамара, представимым в матричной форме $W_B(\omega)=B\cdot H_n, \cdot\ \omega=\overline{0, N-1}$.

Общая схема применения C-кода для снижения пик-фактора к представлена на рис. 2 [1].

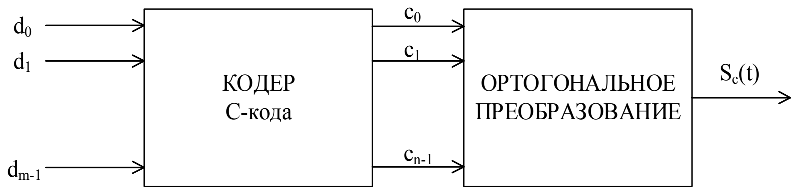


Рис. 2. Схема кодирования информации на основе C-кода

Таким образом, в нашем примере для кодирования первого бита передаваемой по всем каналам информации $[d_1, d_2, d_3, d_4]=[1,-1,-1,1]$ может быть применено некоторое кодовое слово С-кода, представляющее собой, например, бент-последовательность $[d_1, d_2, d_3, d_4]=[1,-1,-1,1]\rightarrow[c_1, c_2, c_3, c_4]=[-1\ \ 1\ \ 1\ \ 1]$, тогда, проведя вычисления в соответствии со схемой (рис. 1), подобно (2) получаем сигнал в канале связи $S=[2\ \ -2\ \ -2\ \ -2]$, обладающий пик-фактором $k=1$.

Задача построения множеств С-кодов является очень актуальной, тем не менее, как показывают проведенные исследования пик-фактор передаваемого по технологии CDMA сигнала также во многом зависит и от выбранного вида ортогональных функций.

Целью настоящей статьи является исследование влияния применяемого набора ортогональных функций на пик-фактор сигналов в технологии CDMA.

Чаще всего, при реализации технологии кодового разделения каналов CDMA применяют функции Уолша упорядоченные по Адамару, построенные в соответствии с выражением (1).

Ортогональные коды на основе эквивалентных классов матриц Адамара

Определение 1. Матрицей Адамара H порядка N называется матрица, размера $N\times N$, такая, что все её элементы равны $\{\pm 1\}$ и выполняется тождество

$$H_N \cdot H_N^T = N\,E_N, \tag{4}$$

где T — оператор транспонирования, E — единичная матрица.

Определение 2. Матрицы Адамара, получаемые друг из друга многократным применением операций умножения строк или столбцов на -1 и перестановок строк или столбцов местами называются эквивалентными.

Известно, что для порядков матрицы Адамара $N=1,2,4,8$ существует только один неэквивалентный класс матриц Адамара, полностью определяемый рекуррентным выражением (1). Тем не менее, как показывают проведенные в [5] исследования уже для порядка $N=16$ существует 5 эквивалентных классов матриц Адамара, представители которых приведены на рис.3. Представители эквивалентных классов матриц Адамара порядка $N = 16$, приведенные на рис. 3 не могут быть получены друг из друга путем применения простейших операций умножения строк или столбцов на -1 и перестановок строк или столбцов местами, тем не менее все удовлетворяют определению (4), что делает возможным их применение в технологии CDMA.

Тем не менее, проведенные исследования показывают, что структура каждой неэквивалентной матрицы $H_1, H_2, ..., H_5$ приводит к различным свойства конструируемого для неё С-кода.

$H_1 =$

```
++++++++++++++++
++++++++--------
++++----++++----
++++--------++++
++--++--++--++--
++--++----++--++
++----++++----++
++----++--++++--
+-+-+-+-+-+-+-+-
+-+-+-+--+-+-+-+
+-+--+-++-+--+-+
+-+--+-+-+-++-+-
+--++--++--++--+
+--++--+-++--++-
+--+-++-+--+-++-
+--+-++--++-+--+
```

$H_2 =$

```
++++++++++++++++
++++++++--------
++++----++++----
++++--------++++
++--++--++--++--
++--++----++--++
++----++++----++
++----++--++++--
+-+-+-+-+-+-+-+-
+-+-+-+--+-+-+-+
+-+--+-++-+--+-+
+-+--+-+-+-++-+-
+--++--++--+-++-
+--++--+-++-+--+
+--+-++-+--++--+
+--+-++--++--++-
```

$H_3 =$

```
++++++++++++++++
++++++++--------
++++----++++----
++++--------++++
++--++--++--++--
++--++----++--++
++----++++----++
++----++--++++--
+-+-+-+-+-+-+-+-
+-+-+-+--+-+-+-+
+-+--+-++--++--+
+-+--+-+-++--++-
+--++--++--+-++-
+--++--+-++-+--+
+--+-++-+-+--+-+
+--+-++--+-++-+-
```

$H_4 =$

```
++++++++++++++++
++++++++--------
++++----++++----
++++--------++++
++--++--++--++--
++--++----++--++
++----++++----++
++----++--++++--
+-+-+-+-+-+-+-+-
+-+-+--++--+-+-+
+-+--++--+-++--+
+-+--+-+-++--++-
+--++-+--+-+-++-
+--++--+-++-+--+
+--+-++-+-+--+-+
+--+-+-++--++-+-
```

$H_5 =$

```
++++++++++++++++
++++++++--------
++++----++++----
++++--------++++
++--++--++--++--
++--++----++--++
++----+++-+-+-+-
++----++-+-+-+-+
+-+-+-+-++----++
+-+-+-+---++++--
+-+--+-++--+-++-
+-+--+-+-++-+--+
+--++--++-+--+-+
+--++--+-+-++-+-
+--+-++-+--++--+
+--+-++--++--++-
```

Рис. 3. Эквивалентные классы матриц Адамара

Так, пусть на вход схемы (рис. 2) подаются кодовые слова полного кода, а в качестве ортогонального преобразования используются поочередно представители неэквивалентных классов матриц Адамара (рис. 3). Тогда мощности классов последовательностей, обладающих заданным значением пик-фактора для каждой из матриц Адамара приведены в табл. 1.

Таблица 1.

Распределение пик-фактора для векторов полного кода

№ п / п	Абсолютное значение пика P_{max}	Пик-фактор κ	Число векторов для матрицы H_1	Число векторов для матрицы H_2	Число векторов для матрицы H_3	Число векторов для матрицы H_4	Число векторов для матрицы H_5
1	16	1	896	384	128	0	0
2	36	2,25	14336	14336	14336	14336	14336
3	64	4	28000	28512	28768	28896	28896
4	100	6,25	17920	17920	17920	17920	17920
5	144	9	3840	3840	3840	3840	3840
6	196	12,25	512	512	512	512	512
7	256	16	32	32	32	32	32
Σ			65536	65536	65536	65536	65536

Таким образом, изучение данных табл. 1 показывает большую зависимость возможности построения С-кодов, обладающих оптимальным значением пик-фактора $k=1$ от вида выбранного набора ортогональных функций, ортогонального преобразования.

Так, наибольшей мощности С-кода позволяет достичь матрица Адамара, построенная по рекуррентному правилу (1), тогда как матрицы H_4 и H_5 вовсе не допускают построения бент-последовательностей, обладающих оптимальным значением пик-фактора $k=1$.

Проведенные исследования классов оптимальных последовательностей, обладающих пик-фактором $k=1$ относительно матриц H_2 и H_3 позволили установить, что все эти последовательности являются подмножеством множества бент-последовательностей для матрицы H_1, регулярные методы построения которых приведены в [6].

Ортогональные коды на основе функций Виленкина-Крестенсона и Фурье

Ясно, что в качестве ортогонального преобразования могут быть использованы системы ортогональных функций Виленкина-Крестенсона [7], которые являются обобщением функций Уолша на многоуровневый случай.

Функции Виленкина-Крестенсона могут быть определены, в частности, через определение аффинного кода функций многозначной логики.

Определение 3. Функцией q-значной логики (далее q-функция) k переменных называется отображение $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

Пологая значение $q=2$ получаем функции трехзначной логики — отображение $\{0,1,2\}^k \to \{0,1,2\}$, т. е. правило, однозначно сопоставляющее вектору из k координат, принадлежащему алфавиту $\{0,1,2\}$, значение из множества $\{0,1,2\}$.

Подобно булевым функциям 3-функции также могут быть однозначным образом представлены в алгебраически нормальной форме, т.е. в виде полинома, содержащего операции умножения и сложения в поле $GF(3)$, которые определяются следующими таблицами

$$\begin{array}{cccc} + & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 2 & 0 & 0 & 1 \end{array} \qquad \begin{array}{cccc} \cdot & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}.$$

Например, для значения $k=2$, общий вид алгебраически-нормальной формы 3-функции будет иметь вид $f(x_1,x_2)=a_0+a_1x_1+a_2x_2+a_3x_1x_2+a_4x_1^2+a_5x_2^2+a_6x_1^2x_2+a_7x_1x_2^2+a_8x_1^2x_2^2$, где $a_i \in \{0,1,2\}$.

Определение. Для произвольного натурального k, аффинным $A(N,k)$-кодом длины $N=3^k$ называется множество всех строк Ω_f тех булевых функций, степень нелинейности которых не превышает 1, то есть $A(N,k)=\{\Omega_f \,|\, f \in F_q, \deg f \le 1\}$ [9].

Другими словами, аффинными являются все 3-функции имеющие вид: $f(x_0,...,x_{k-1})=a_0x_0+a_1x_1+...+a_{k-1}x_{k-1}(\mathrm{mod}\,3)=\sum_{i=0}^{k-1}a_ix_i(\mathrm{mod}\,3)$, где $a_i \in \{0,1,2\}$.

Так, для случая $k=2$ могут быть выписаны все аффинные функции

$$
\begin{array}{lll}
\varphi_1 = 0; & \varphi_{10} = x_2; & \varphi_{19} = 2x_2; \\
\varphi_2 = 1; & \varphi_{11} = x_2 + 1; & \varphi_{20} = 2x_2 + 1; \\
\varphi_3 = 2; & \varphi_{12} = x_2 + 2; & \varphi_{21} = 2x_2 + 2; \\
\varphi_4 = x_1; & \varphi_{13} = x_2 + x_1; & \varphi_{22} = 2x_2 + x_1; \\
\varphi_5 = x_1 + 1; & \varphi_{14} = x_2 + x_1 + 1; & \varphi_{23} = 2x_2 + x_1 + 1; \\
\varphi_6 = x_1 + 2; & \varphi_{15} = x_2 + x_1 + 2; & \varphi_{24} = 2x_2 + x_1 + 2; \\
\varphi_7 = 2x_1; & \varphi_{16} = x_2 + 2x_1; & \varphi_{25} = 2x_2 + 2x_1; \\
\varphi_8 = 2x_1 + 1; & \varphi_{17} = x_2 + 2x_1 + 1; & \varphi_{26} = 2x_2 + 2x_1 + 1; \\
\varphi_9 = 2x_1 + 2; & \varphi_{18} = x_2 + 2x_1 + 2; & \varphi_{27} = 2x_2 + 2x_1 + 1.
\end{array},
$$

Указанные функции могут быть представлены в виде своих таблиц истинности

$$
\begin{Bmatrix}
000000000 & 111111111 & 222222222 \\
012012012 & 120120120 & 201201201 \\
021021021 & 102102102 & 210210210 \\
000111222 & 111222000 & 222000111 \\
012120201 & 120201012 & 201012120 \\
021102210 & 102210021 & 210021102 \\
000222111 & 111000222 & 222111000 \\
012201120 & 120012201 & 201120012 \\
021210102 & 102021210 & 210102021
\end{Bmatrix},
$$

Подобно двоичному случаю, на основе трети кодовых слов аффинного кода, а также однозначного преобразования $0 \to e^{j0^\circ}, 1 \to e^{j120^\circ}, 2 \to e^{j240^\circ} = e^{-j120^\circ}$ может быть построена ортогональная матрица, каждая строка которой представляет собой функцию Виленкина-Крестенсона

$$
\begin{bmatrix}
e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} \\
e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} \\
e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} \\
e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j240^\circ} \\
e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} \\
e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} \\
e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j120^\circ} \\
e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} \\
e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ}
\end{bmatrix}, \qquad (5)
$$

На основе матрицы (5) также может быть построена система связи с кодовым разделением каналов по принципу, подобному (рис.1). Например, пусть 9 абонентов одновременно передают сообщения $\{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9,\} = \{0,1,0,2,2,0,0,2,2,\} \to \{e^{j0^\circ}, e^{j120^\circ}, e^{j0^\circ}, e^{j240^\circ}, e^{j240^\circ}, e^{j0^\circ}, e^{j0^\circ}, e^{j240^\circ}, e^{j240^\circ},\}$.

Выполняя преобразование подобное (2) находим результирующий сигнал, который подается в канал связи

$$S = \{3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j60^\circ}, 3 \cdot e^{-j180^\circ}, 3 \cdot e^{-j60^\circ},\}. \quad (6)$$

В соответствии с (3) вычисляем пик-фактор сигнала (6), который равен $\kappa = 3/3 = 1$, т.е. исходная последовательность, состоящая из сообщений в каждом канале является оптимальной.

В целях изучения возможностей построения оптимальных С-кодов для работы с преобразованием Виленкина-Крестенсона в технологии CDMA подадим на вход преобразования (5) полный код над алфавитом $e^{j0^\circ}, e^{j120^\circ}, e^{-j120^\circ}$ мощности $J = 3^9$. Результаты проведенного эксперимента позволяют установить, что всего существует 486 таких оптимальных последовательностей, которые, говоря в общем случае, могут быть названы бент-последовательностями относительно преобразования Виленкина-Крестенсона.

Подробный анализ полного класса данных оптимальных последовательностей позволил установить их весовую структуру, по которой они могут быть разделены на шесть подмножеств

$$\begin{array}{cccc} K_0 & K_1 & K_2 & (J_i) \\ 1 & 4 & 4 & (54); \\ 2 & 2 & 5 & (108); \\ 2 & 5 & 2 & (108); \\ 4 & 1 & 4 & (54); \\ 4 & 4 & 1 & (54); \\ 5 & 2 & 2 & (108), \end{array} \quad (7)$$

где K_0, K_1, K_2 — количество 0, 1, 2 в троичной последовательности соответственно, с учетом однозначного отображения $0 \to e^{j0^\circ}, 1 \to e^{j120^\circ}, 2 \to e^{j240^\circ} = e^{-j120^\circ}$:

J_i — количество последовательностей с заданной структурой.

В качестве примера, приведем полный класс оптимальных троичных последовательностей, обладающих первой структурой

011122122	110122212	121022112	122122011	211202112	220112112
011212221	110212122	121112022	122212110	211211022	220121211
011221212	110221221	121121202	122221101	211220121	220211121
022112121	112022121	121202121	202112211	212011221	221011212
022121112	112112220	121211220	202121121	212101212	221101122.
022211211	112121022	121220211	202211112	212110122	221110221
101122221	112202211	122011122	211022211	212122110	221122101
101212212	112211202	122101221	211112202	212212101	221212011
101221122	112220112	122110212	211121220	212221011	221221110

Анализ (7) показывает, что подобно дуальным парам двоичных бент-функций существует 2 тройственных набора оптимальных троичных последовательностей, которые в сумме являются уравновешенными, соответственно наборы $\{1,4,4\}, \{4,1,4\}, \{4,4,1\}$ и $\{2,2,5\}, \{2,5,2\}, \{5,2,2\}$.

Отметим, что дальнейшие изучение методов построения С-кодов, обладающих оптимальным значением пик-фактора к трансформант Виленкина-Крестенсона является актуальной задачей и может быть предметом дальнейших исследований.

Другим широко используемым в технологии CDMA видом ортогонального преобразования является Дискретное Преобразования Фурье (ДПФ), ортогональная матрица порядка N которого в обобщенном виде [7]

$$F = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^{2} & \dots & w^{N-1} \\ 1 & w^{2} & w^{4} & \dots & w^{2(N-1)} \\ 1 & w^{3} & w^{6} & \dots & w^{2(N-1)} \\ \vdots & & & & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \dots & w^{(N-1)2} \end{bmatrix}, \tag{8}$$

где $w = \cos(2\pi/N) + j\sin(2\pi/N)$, $j = \sqrt{-1}$.

Методом перебора может быть легко установлено, что для практически ценных длин векторов $N = 8$ и $N = 16$ алфавита $\{+1,-1\}$ для матрицы (8) не существует оптимальных последовательностей, т.е. построение С-кода, обладающего значением пик-фактора $k = 1$ является невозможным.

Тем не менее, как показали исследования, оптимальные последовательности длины $N = 9$ могут быть найдены для алфавита $\{e^{j0^\circ}, e^{j120^\circ}, e^{-j120^\circ}\}$, которых существует $J = 162$ штуки.

Аналогично табл. 1 сведем в табл. 2 данные о распределении пик-фактора для векторов полного кода относительно преобразования Виленкина-Крестенсона и ДПФ.

Таблица 2.

Распределение пик-фактора для векторов полного кода длины $N = 9$

№ п/п	Абсолютное значение пика $P_{\max}$	Пик-фактор к	Число векторов для матрицы (5)	Число векторов для матрицы ДПФ
1	9	1	486	162
2	14.638	1.626	—	486
3	18.679	2.075	—	486
4	19.237	2.137	—	972
5	19.598	2.177	—	972
6	20.638	2.293	—	972
7	21.003	2.333	10692	3564
8	22.231	2.47	—	1458
9	24.870	2.763	—	2430
10	26.998	2.999	4104	1476
11	27.321	3.035	—	486
12	29.833	3.314	—	972
13	30.869	3.429	—	972
14	31.787	3.531	—	324
15	34.786	3.865	—	324
16	36	4	1944	648
17	36.505	4.056	—	972
18	37.908	4.212	—	324

Продолжение таблицы 1.

19	39	4.333	1944	648
20	41.1	4.566	—	486
21	51.696	5.744	—	324
22	57.002	6.333	486	162
23	57.699	6.411	—	54
24	81	9	27	9
Σ			19683	65536

Анализ данных табл.2 приводит к выводу, что матрица преобразования Виленкина-Крестенсона допускает построение большего числа оптимальных троичных последовательностей, обладающих пик-фактором $k=1$, чем матрица ДПФ. Данное свойство является практически ценным с точки зрения реализации технологии кодового разделения каналов.

Выводы

Установлено, что структура и мощность бинарного C-кода, обладающего оптимальным значением пик-фактора к коэффициентов преобразования Уолша-Адамар сильно зависит от вида выбранной матрицы преобразования. Так, уже при порядке матрицы $N=16$ существуют структуры матриц Адамара для которых вовсе не существует бент-последовательностей.

Исследована возможность использования преобразования Виленкина-Крестенсона для реализации технологии кодового разделения каналов. Обнаружено, что существует класс оптимальных троичных последовательностей мощности $J=486$, которые подобным бент-функциям образом обладают равномерными амплитудами спектра и таким образом могут быть использованы в качестве кодовых слов C-кода.

Проведенный сравнительный анализ распределения пик-фактора векторов полного кода для матрицы Виленкина-Крестенсона и матрицы ДПФ показывает, что преобразование Виленкина-Крестенсона допускает построение большего числа векторов, обладающих оптимальным значением пик-фактора $k=1$, что может быть привлекательным CDMA.

Список литературы

1. Paterson, K.G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory / K.G. Paterson // Sequences and their applications. – Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. – PP. 46–71.
2. Schwengler, T. TLEN 5510 – Wireless & Cellular Communications [Электронный ресурс] / T. Schwengler. – Режим доступа: http://morse.colorado.edu/~tlen5510/text/classweb.html .
3. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков. – Одесса: Наука и Техника, 2010. – 340 с.
4. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. – 2009. – Сер. №1(3). – С. 15–37.
5. Hall, M.Jr. Hadamard matrices of order 16 / M. Hall // Research Summary. – 1961. – Volume I, No. 36–10. – PP. 21–26.
6. Мазурков, М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов // Труды Одес. нац. политехн. ун-та. – 2013. – №2 (41). – 227–231.
7. Трахтмаи, А.М. Основы теории дискретных сигналов на конечных интервалах / А.М. Трахтман, В.А. Трахтман. – М.: Сов.радио, 1975. – 208 с.
8. Амбросимов, А.С. Свойства бент-функций q-значной логики над конечными полями / А.С. Амбросимов // Дискрет. матем. – 1994. – Т.6, Вып. 3. – С. 50–60.

ПРО ВПЛИВ ВИДУ ОРТОГОНАЛЬНОГО ПЕРЕТВОРЕННЯ НА ПІК-ФАКТОР СПЕКТРУ СИГНАЛІВ У СИСТЕМАХ CDMA

М. В. Мазурків, А. В. Соколов, Н.А. Барабанів

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна, e-mail: alart@stream.com.ua

У статті досліджується вплив виду ортогонального перетворення на пік-фактор сигналів в системах з технологією кодового розділення каналів. Розглядаються всі п'ять класів ортогональних перетворень порядку N=16, побудованих на основі функцій Уолша, а також дискретне перетворення Фур'є і перетворення, засновані на ортогональних функціях Віленкіна-Крестенсона. Знайдено сімейство трійкових послідовностей, що володіють рівномірним спектром Віленкіна-Крестенсона.
Ключові слова: CDMA, пік-фактор, ортогональне перетворення.

ON THE EFFECT OF THE TYPE OF ORTHOGONAL TRANSFORM ON PAPR OF SIGNAL SPECTRUM IN CDMA SYSTEMS

M.I. Mazurkov, A.V. Sokolov, N.A. Barabanov
Odessa National Polytechnic University,
1 Shevchenko Str., Odessa, 65044, Ukraine; e-mail: alart@stream.com.ua

This paper is devoted to research of the impact of the type of orthogonal transform on the PAPR of signals in systems with CDMA technology. We consider all five classes of orthogonal transforms of order N=16 that are based on Walsh functions, as well as discreet Fourier transform and transform based on orthogonal Vilenkin-Christenson functions. A set of ternary sequences having uniform Vilenkin-Christenson spectrum is discovered.
Keywords: CDMA, peak factor, orthogonal transform

УДК 621.317

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 38-43

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА ПРОЯВЛЕНИЯ СЛЕДОВ МОНТАЖА В ЦИФРОВЫХ ФОНОГРАММАХ

О.В. Рыбальский, В.И. Соловьев

Национальная академия внутренних дел,
пл. Соломенская, 1, Киев, 03035, Украина; e-mail: rybalsky_ol@mail.ru

Рассмотрены результаты экспериментальных исследований проявления следов цифрового монтажа в цифровых фонограммах. Экспериментально доказано, что как вырезание фрагментов фонограммы в паузах между речевыми сигналами, так и вставка вырезанных фрагментов в паузах, приводит к изменениям спектрального состава сигналов в точках монтажа. Предложено разработать программу и методику для экспертизы цифровых фонограмм.

Ключевые слова: запись звука, пауза, речевой сигнал, спектр сигнала, цифровая фонограмма, файл.

Введение

При проведении экспертизы материалов звукозаписи одной из самых сложных задач является задача выявления признаков и мест монтажа. Но до последнего времени эта задача не поддавалась всеобъемлющему решению, поскольку всегда оставались способы монтажа, признаки которого не удавалось выявить существующими методами.

Разработанные нами ранее частные методы выявления монтажа основаны на предположении, что монтаж фонограммы проводится в паузах между речевыми сигналами [1]. Решение задачи выявления его признаков в случае проведения монтажа из записей, сделанных на разной аппаратуре, было предложено реализовать путем разделения каждой паузы на части и сравнения характеристик паразитных параметров аппаратуры записи, зафиксированных в разных частях паузы [2]. Но решение задачи значительно усложняется в случае проведения монтажа из записей, сделанных на одной аппаратуре. Еще более сложно выявить монтаж, если вся его процедура проводилась с одной записью (вырезка части сигнала, вставка в другое место части ранее вырезанной записи).

Мы предположили, что экспериментальную проверку возможности решения этих задач должен обеспечить предложенный ранее метод сравнения двух (или более) частей одной паузы. В результате нами была разработана программа и методика эксперимента, позволяющая, с нашей точки зрения, выявлять следы монтажа, оставленные при обработке записи, сделанной на одной аппаратуре.

Программа, позволяющая реализовать данный эксперимент, построена на неортогональном вейвлет-преобразовании с использованием вейвлета Морле. Практически идеология построения ее вычислительной части основана на идеологии, основанной на теории каркасов, изложенной, например, Стефаном Малла [3], и незначительно отличается от метода, предложенного в одной из наших статей, описывающей построение вычислительной части программы, предназначенной для идентификации диктора [4]. Разумеется, в этой программе предусмотрен другой интерфейс, предназначенный для обеспечения удобства работы исследователя при решении новой задачи, и предусмотрены небольшие изменения, связанные с выделением и разделением пауз на части и выделения, обработки и сравнения полученных характеристик аппаратуры записи. Однако описание этой программы и реализуемых методов исследования пауз не является предметом данной публикации. Но следует отметить, что ее применение обеспечило высокоточное вычисление вейвлет-спектров сигналов на интервалах от 30 до 100 мс.

Целью исследований, результаты которых приведены в данной статье, была экспериментальная проверка возникновения отличий сигналов в точках монтажа на паузах речи в смонтированных фонограммах, выполненного путем вырезания и вставки информации, содержащейся в цифровой фонограмме, записанной на одной аппаратуре, относительно фонограмм, не подвергавшихся монтажу. Кстати, теоретически наличие таких отличий впервые были обоснованы в работе [5].

Проведенный эксперимент должен дать ответ на вопрос о целесообразности разработки метода выявления такого монтажа, удовлетворяющего требованиям экспертизы.

Основная часть

Эксперименты проводились в следующем порядке. Сначала записывались отдельные файлы на различных типах и экземплярах аппаратуры цифровой звукозаписи (АЦЗЗ). Эти файлы загружались в компьютер и запоминались с пометкой «без монтажа». Затем каждый из этих файлов открывался в звуковом редакторе и подвергался монтажу. Монтаж файлов проводился по одному алгоритму:
по временной шкале окна редактора определялось и записывалось время начала паузы, затем выделялась часть фонограммы с речевым сигналом;

1. Определялась длительность выделенного участка фонограммы, после чего он из нее вырезался;
2. Далее по временной шкале редактора выбиралась другая пауза, и ее изображение растягивалось во времени;
3. Устанавливался курсор на нулевое (по уровню) значение сигнала в паузе, записывалось его временное положение в фонограмме, и вставлялся ранее вырезанный участок фонограммы;
4. Определялось место окончания вставки сигнала и записывалось ее временное положение в фонограмме;
5. Участок вставки растягивался во времени и, при необходимости, устранялся фазовый набег.

Таким образом, монтаж производился в предположении, что он выполнен опытным оператором, умеющим скрывать следы своей “деятельности”. При этом не проводилась подборка монтируемых участков по смыслу произведенных перестановок (что при экспертизе обязательно проверяется экспертом). Это делалось для упрощения задачи создания экспериментального материала, т.к. прослушивание смонтированных фонограмм не входило в задачи эксперимента.

Ниже приводятся иллюстрации к проведенным экспериментам, которые проводились на фонограммах, записанных на различной АЦЗЗ при разных частотах дискретизации.

Всего были использованы записи, сделанные на 9 различных цифровых диктофонах и 5 мобильных телефонах при частотах дискретизации 8 кГц, 11.025 кГц, 16 кГц, 32 кГц и 44.1 кГц. Во всех случаях были обнаружены отличия между сигналами пауз, содержащих точки монтажа, относительно сигналов в паузах, не содержащих точек монтажа.

На рис. 1 приведены сигнал паузы во временной (верхнее окно) и время-частотной области для фонограммы, не подвергавшейся монтажу. Эта пауза выбрана потому, что при изготовлении смонтированной фонограммы в этой точке был вырезан фрагмент длительностью примерно в 2 с. На рис. 2 приведен сигнал этой же паузы для фонограммы, подвергшейся монтажу.

Из визуального сравнения время-частотных графиков видно различие частотного состава сигналов на одном временном интервале для смонтированной и не смонтированной фонограмм (в области значения 6.625 с.), что свидетельствует об изменении частотного состава сигнала на этом участке.

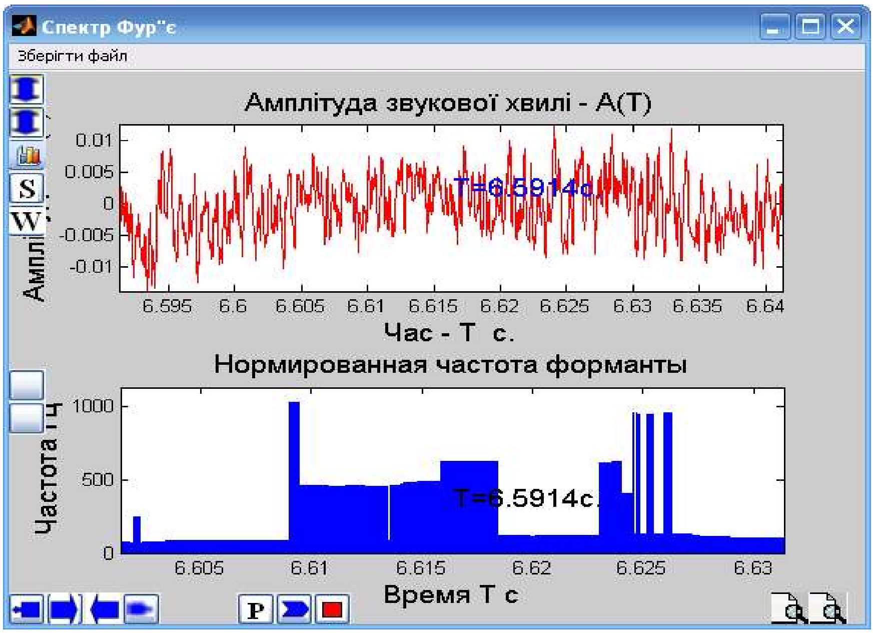


Рис. 1. Сигнал паузы фонограммы, не подвергавшейся монтажу на временном отрезке от 6.594 с. до 6.63 с.

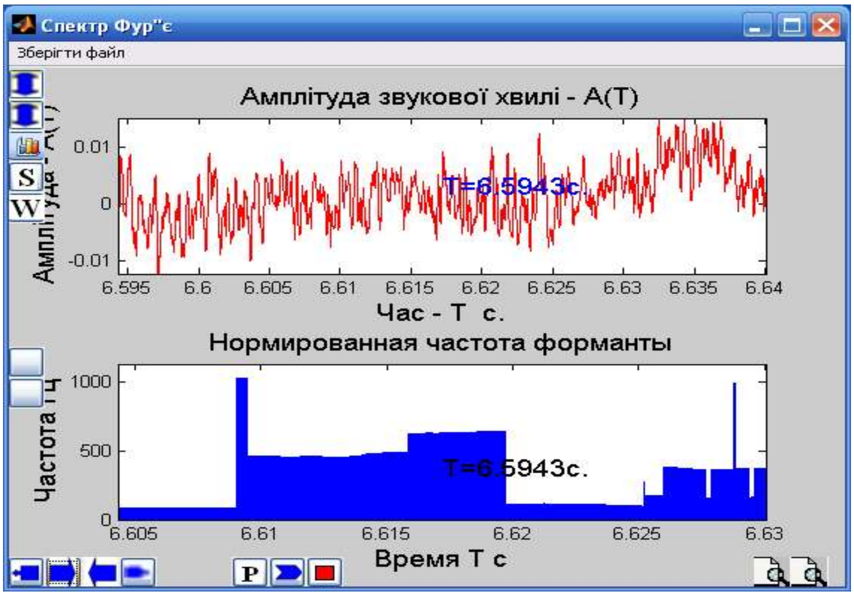


Рис. 2. Сигнал паузы фонограммы, подвергшейся монтажу (вырезка фрагмента) на временном отрезке от 6.594 с. до 6.63 с.

На рис. 3 и рис. 4 аналогично показаны паузы, соответствующие началу вставки вырезанного фрагмента фонограммы длительностью примерно 2 с. Из сравнения время-частотных характеристик сигналов в этой паузе также видно, что спектральный состав пауз изменяется при проведении монтажа методом вставки фрагмента.

Рис. 3. Сигнал паузы фонограммы, не подвергавшейся монтажу методом вставки фрагмента (момент начала вставки) на временном отрезке от 18.9585 с. до 19 с.

На рис. 5 и рис. 6 показаны паузы, соответствующие окончанию вставки вырезанного фрагмента фонограммы длительностью примерно 2 с. Из сравнения время-частотных характеристик сигналов в этой паузе также видно, что спектральный состав пауз изменяется при проведении монтажа методом вставки фрагмента.

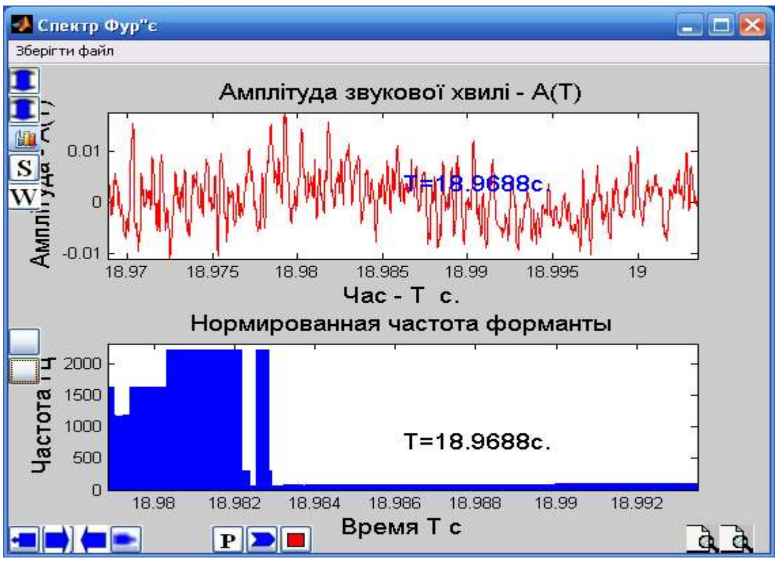


Рис. 4. Сигнал паузы фонограммы, подвергшейся монтажу методом вставки фрагмента (момент начала вставки) на временном отрезке от 18.9688 с. до 18.994 с.

Рис. 5. Сигнал паузы фонограммы, не подвергавшейся монтажу методом вставки фрагмента (момент завершения вставки) на временном отрезке от 21.5898 с. до 21.3 с.

Рис. 6. Сигнал паузы фонограммы, подвергшейся монтажу методом вставки фрагмента (момент завершения вставки) на временном отрезке от 21.5968 с. до 21.622 с.

Проведенные эксперименты показали, что следствием монтажа, производимого методом вырезки или перестановки (вставки фрагмента) в паузах речевой информации в файле, записанном на одной АЦЗЗ, является изменение спектрального состава сигнала в паузах, где производился монтаж. Данное свойство наблюдалось при исследовании всех цифровых файлов, записанных на всех аппаратах, использованных при проведении эксперимента. Однако при этом не выявлена какая-либо устойчивость характеристик изменения спектра пауз для файлов, записанных на разных аппаратах.

Выводы

Из этого следует, что хотя проведенные исследования и доказали изменяемость спектра сигналов в точках монтажа, но прямое использования примененного при эксперименте метода и программы непригодно для построения рабочей программы для проведения экспертиз материалов цифровой звукозаписи.

Наиболее целесообразно строить программу и методику экспертизы на основе метода, позволяющего выделять устойчивые идентификационные признаки монтажа. Но методы построения такой программы не являются предметом рассмотрения данной статьи.

Список литературы

1. Рыбальский, О.В. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе / О.В. Рыбальский, Ю.Ф. Жариков. – К.: НАВСУ, 2003. – 300 с.
2. Соловьев, В.И. Локализация следов обработки сигнала в задачах монтажа аудиозаписи / В.И. Соловьев, О.В. Рыбальский, В.К. Железняк // Вестник Полоцкого государственного университета. – 2013. – Серия С: фундаментальные науки, Т. 4. – С. 5–12.
3. Малла, С. Вэйвлеты в обработке сигналов / С. Малла: Пер. с англ. – М.: Мир, 2005. – 671 с.
4. Соловьев, В.И. Спектральный анализ и современные речевые технологии / В.И. Соловьев, О.В. Рыбальский, В.К. Железняк // Вестник Полоцкого государственного университета. – 2014. – Т. 4. – С. 2–6.
5. Рыбальский, О.В. К вопросу о фрактальности аналоговых сигналов, подвергнутых цифровой обработке / О.В. Рыбальский // Вісник Східноукраїнського національного університету ім В. Даля. – 2006. – № 9, ч. 1. – С. 21–25.

ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ПРОЯВУ СЛІДІВ МОНТАЖУ В ЦИФРОВИХ ФОНОГРАМАХ

О.В. Рибальський, В.І. Соловйов

Національна академія внутрішніх справя
пл. Солом'янська, 1, Київ, 03035, Україна; e-mail: rybalsky_ol@mail.ru

Розглянуті результати експериментальних досліджень прояву слідів цифрового монтажу в цифрових фонограмах. Експериментально доведено, що як вирізування фрагментів фонограми в паузах між мовними сигналами, так і вставка вирізаних фрагментів у паузах, призводить до змін спектрального складу сигналів у точках монтажу. Запропоновано розробити програму та методику для експертизи цифрових фонограм.

Ключові слова: запис звуку, пауза, мовний сигнал, спектр сигналу, цифрова фонограма, файл.

EXPERIMENTAL DETECTION OF EDITING TRACES IN DIGITAL AUDIO RECORDS

O.V. Rybalsky, V.I. Solovyev

National Academy of Internal Affairs,
1, Solomenskaya sq., Kiev, 03035, Ukraine; e-mail: rybalsky_ol@mail.ru

The paper discusses the results of experimental detection of editing traces in digital audio records. It was proved experimentally that both cutting of the pause fragments from voice records and adding the pre-cut fragments into pauses results in the changes in signal spectrum at editing locations. It was proposed to develop a methodology for the expertise of digital audio records.

Keywords: audio recording, pause, voice signal, signal spectrum, digital audio record, file.

УДК 519.92:002.5:303.442.3

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp.44-56

КОНСОЛІДАЦІЯ КЛАСИФІКАЦІЇ В МОДЕЛЯХ КОМПЕТЕНЦІЇ ТА УМІНЬ В ГАЛУЗЕВИХ СТАНДАРТАХ ВИЩОЇ ОСВІТИ

А.А. Кобозєва[1], В.Г. Кононович[1], І.В. Кононович[2], О.В. Ніколаєнко[1]

[1] Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net
[2] Одеська національна академія харчових технологій,
вул. Канатна, 112, м. Одеса, 65039, Україна; e-mail: kononovich@mail.ru

Розглядається проблема класифікації та кодифікації умінь фахівців у зв’язку з виявленими колізіями у практиці формування стандартів вищої освіти в технічних та економічних галузях в умовах застосування компетентнісного підходу. Знайдені колізії, причини яких полягають у тому, що: а) відсутня методика формування єдиного переліку фахових умінь з умінь вирішувати типові завдань діяльності та умінь, що забезпечують формування компетенції; б) відсутні моделі зворотних зв’язків та модель постачальника компетенції на ринок праці. Застосовано методи шкалювання, інформаційної аналітики та кореляційний кластер-аналіз. Запропоновано варіант моделі діяльності навчання. Сформовані принципи консолідації класифікації фахових умінь, яка придатна, принаймні, у технічних, економічних і природничих галузях вищої освіти. Консолідована класифікація простіша, враховує сучасні тенденції техніки і науки до конвергенції, міждисциплінарності, що дозволить підвищити якість освітніх стандартів.

Ключові слова: класифікація, кластери, галузеві стандарти, консолідація інформації, компетенції, фахові уміння, задачі діяльності, класи задач діяльності, кореляція, коди (шифри) умінь.

Вступ

У вік значного прискорення науково-технічного й технологічного прогресу виростають нові галузі і напрями науки, потреби в нових кваліфікаціях фахівців та розвитку нових галузей і спеціальностей вищої освіти. У процесах стандартизації вищої освіти забезпечення компетентнісного підходу до змісту й оцінки якості освіти стало провідним принципом. Основою логічної структури та якості складових галузевих стандартів вищої освіти є вирішення проблеми спрощення класифікації компетенції та умінь фахівців і зворотних зв’язків із виробничими галузями.

Серед величезного різноманіття літератури, пов’язаної з цією проблемою, відмітимо наступні. Теорія класифікації та кластер-аналіз представлені у фундаментальній книзі [1]. Її авторами є відомі вчені Л. Заде, С. Рао, К. Фу та ін. У цій роботі, зокрема підкреслюється, що «Класифікація – один із фундаментальних процесів у науці. Факти і явища повинні бути впорядковані попри ніж ми їх зможемо зрозуміти та розробити загальні принципи, які пояснюють їх появу та видимий порядок». Із періодичних видань відмітимо роботу [2], яка торкається ієрархічно організованих класифікацій. Методи аналізу можуть опиратись на досягненнях сучасного напряму інформаційно-аналітичної діяльності, який отримав назву «консолідована інформація» [3]. Прикладом всебічного обґрунтування компетентнісного підходу до підготовки сучасного фахівця може служити колективна монографія [4]. Результатом плідної багатопланової роботи стала методика розроблення складових галузевих стандартів вищої освіти з використанням компетентнісного підходу [5]. Для аналізу відібрані три типічні стандарти із різних напрямів вищої освіти [6 – 8].

В результаті їх аналізу виявлені колізії у системі класифікації умінь та компетенції фахівців. Класифікація характеризується складністю внаслідок нестиковок між класифікаціями кластеру умінь і кластеру компетенції. Крім того, відсутня методика формування єдиного переліку фахових умінь із умінь виконувати типові завдання діяльності та умінь, які складають компетенції фахівця. В результаті класифікація стала складною і її незручно застосовувати для формування стандарту. Між тим, провідні вчені вказують на доцільність простих підходів до вирішення проблем. Наприклад, за словами Д. У. Гіббса, «одною з головних цілей теоретичного дослідження – знайти точку зору, з якої предмет представляється найбільш простим [9; епіграф до § 1.2]». А в роботі Г.Г. Малінецького підкреслюється, що: «Як показує історія, в житті можуть стійко працювати лише прості ідеї. … Тому при вирішенні багатьох питань стратегічного характеру так важливо опиратись на прості, ясні, оглядові та доступні розумінню моделі [10]». З цих поглядів задача дослідження проблеми класифікації фахових умінь, які визначають логічну структуру галузевих стандартів, виглядає актуальною.

Метою даної роботи є підвищення якості класифікації в складових галузевих стандартах вищої освіти України (ГСВОУ) та стандартах вузів в природничих і технічних галузях за рахунок усунення виявлених колізій (колізія: відсутність методики формування єдиного переліку умінь та її наслідки), явного подання моделі діяльності навчання, як постачальника компетенції на ринок праці, організації зворотних зв’язків у процесі формування стандарту та за рахунок консолідації класифікації компетенції та умінь фахівців, більш зручної для застосування при формуванні стандартів освіти.

Згідно існуючої методики розроблення складових галузевих стандартів вищої освіти система класифікації фахових умінь та компетенції [5], що визначає структуру цих стандартів, базується на таксономії, в якій кожній з операційних таксономічних одиниць (ОТО) відповідають наступні вектори дескрипторів у просторі ознак:

1. Види типових задач діяльності: ПФ – професійна, СВ – соціально-виробнича, СП – соціально-побутова.
2. Класи задач діяльності: С – стереотипна, Д – діагностична, Е – евристична.
3. Види уміння: ПП – предметно-практичне, ПР – предметно-розумове, ЗП – знаково-практичне, ЗР – знаково-розумове.
4. Рівні сформованості уміння: О – здатність виконувати дію, спираючись на матеріальні носії інформації щодо неї; Р – здатність виконувати дію, спираючись на постійний розумовий контроль без допомоги матеріальних носіїв інформації, Н – здатність виконувати дію автоматично, на рівні навички.
5. Компетенції: КСО – соціально-особистісні, КЗН – загальнонаукові, КІ – інструментальні, КЗП – загально-професійні, КСП – спеціалізовано-професійні.

Розроблена відповідна система форматів для шифрування (далі «кодування») умінь. Краще говорити «кодування», бо шифрування і кодування є різними розділами науки. За способом кодування коди уміння поділені на:

1. Код уміння виконувати типову задачу діяльності з форматом

<u>XX. XX. X. XX</u>. <u>XX</u>. <u>X</u>. <u>XX</u>

номер уміння, наскрізний для типової задачі діяльності

рівень сформованості уміння

вид уміння

код типової задачі діяльності

2. Код уміння, яке є складовою компетенції за форматом

КХХ. ХХ. ХХ. Х. ХХ

номер уміння, наскрізний для даної компетенції

рівень сформованості уміння

вид уміння

код компетенції

Відразу помічаємо, що коди відрізняються префіксами. У випадку а) префіксом являється код типової задачі діяльності, формат якого виглядає так:

Х. ХХ. Х. ХХ

номер задачі, наскрізний для даної виробничої функції

клас типової задачі діяльності

вид типової задачі діяльності

номер виробничої функції

Побудовані таким чином формати кодів можуть приводити до різних процедур їх використовування.

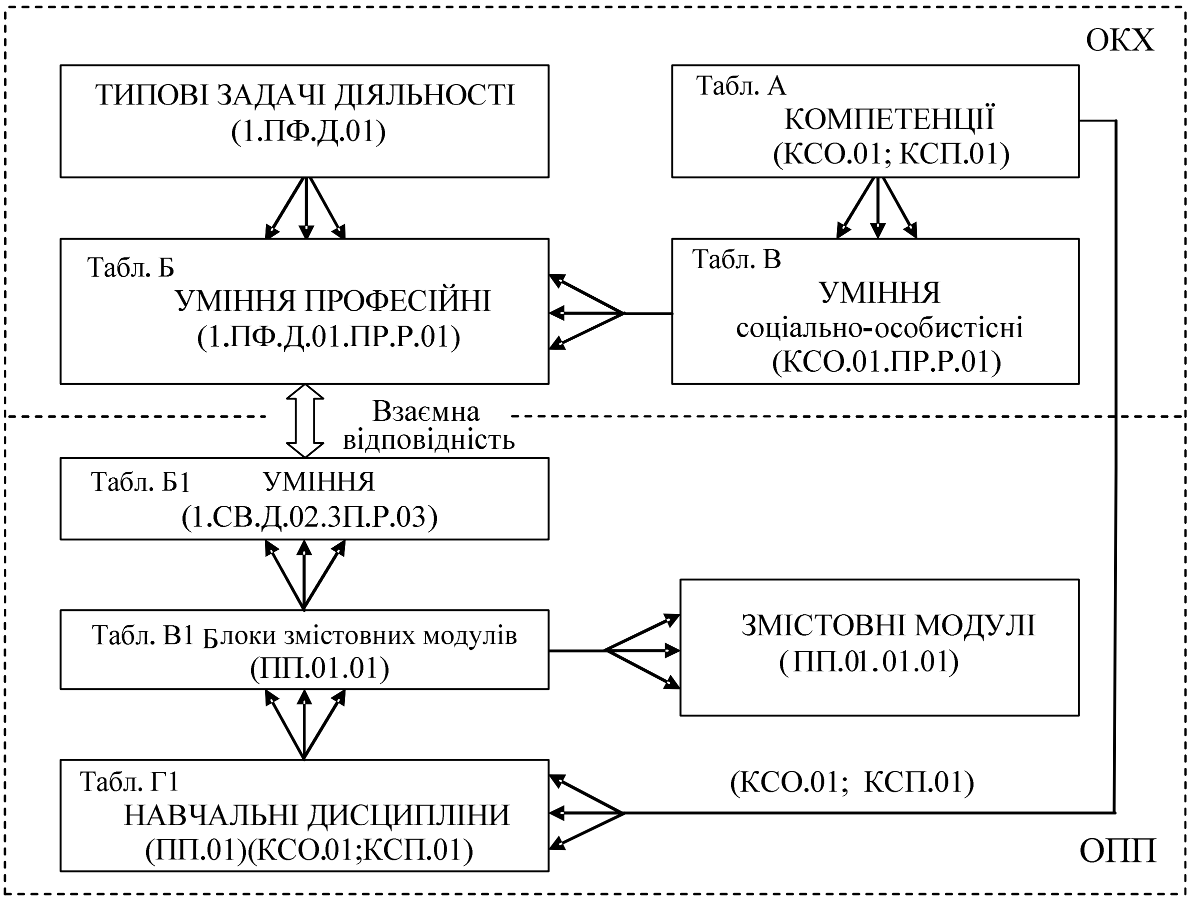


Рис. 1. Процедура формування ГСВОУ 8.05100304-13 магістра за спеціальністю прилади і системи екологічного моніторингу

Аналіз практики формування ГСВОУ дозволяє виділити три групи процедур формування переліку компетенції, умінь, змістовних навчальних модулів та навчальних дисциплін в освітній кваліфікаційній характеристиці (ОКХ) та освітньо-професійній програмі підготовки (ОПП). Дамо характеристику цих груп.

Перша група процедур формування переліків показана на рис. 1.

Ця процедура характеризується: наскрізним застосуванням коду умінь типу а); обмеженим використанням коду умінь типу б); із ОКХ в ОПП передається перелік умінь для кожного з яких формується змістовний навчальний модуль; введенням коду «ПП» – професійної і практичної підготовки в кодах дисциплін та змістовних модулів; коди компетенції використовуються на заключному етапі формально, як переліки складових сформованої компетенції кожною з дисциплін, а також в переліках умінь, де відмічається, яку складову компетенції формує кожне з умінь. При цьому, одне уміння може формувати декілька складових компетенції. Можна припустити, що процедура є циклічною. Спочатку формуються переліки умінь виконувати типові задачі діяльності та переліки компетенції. Далі формується перелік умінь, які формуються навчальними дисциплінами. Потім ці переліки узгоджуються на взаємну відповідність. Якщо переліки не узгоджені, то процедури повторюються до повного узгодження. За такого підходу забезпечується повнота переліку умінь виконувати типові задачі діяльності.

Друга група процедур формування переліків наведена на рис. 2 (без блоків, що показані пунктиром). Ця процедура характеризується: наскрізним застосуванням коду умінь типу б); код умінь типу а) має обмежене застосування; вся процедура в цілому має послідовний деревовидний характер; уміння виконувати типові задачі діяльності однозначно узгоджуються за кодами з уміннями що формують компетенції; замість кодів професійних умінь далі використовуються коди компетенції, які однозначно узгоджені з ними; уміння сформульовані так, що кожному умінню відповідає одна складова компетенції, що її формує; в результаті складається консолідований перелік умінь; із ОКХ в ОПП передається перелік умінь, для кожного з яких формується не один змістовний навчальний модуль, а блок змістовних модулів, що дає більшу свободу при формуванні навчальних дисциплін. За такого підходу забезпечується повнота переліків як відносно умінь виконувати типові задачі діяльності, так і переліку умінь, що формують компетенції.

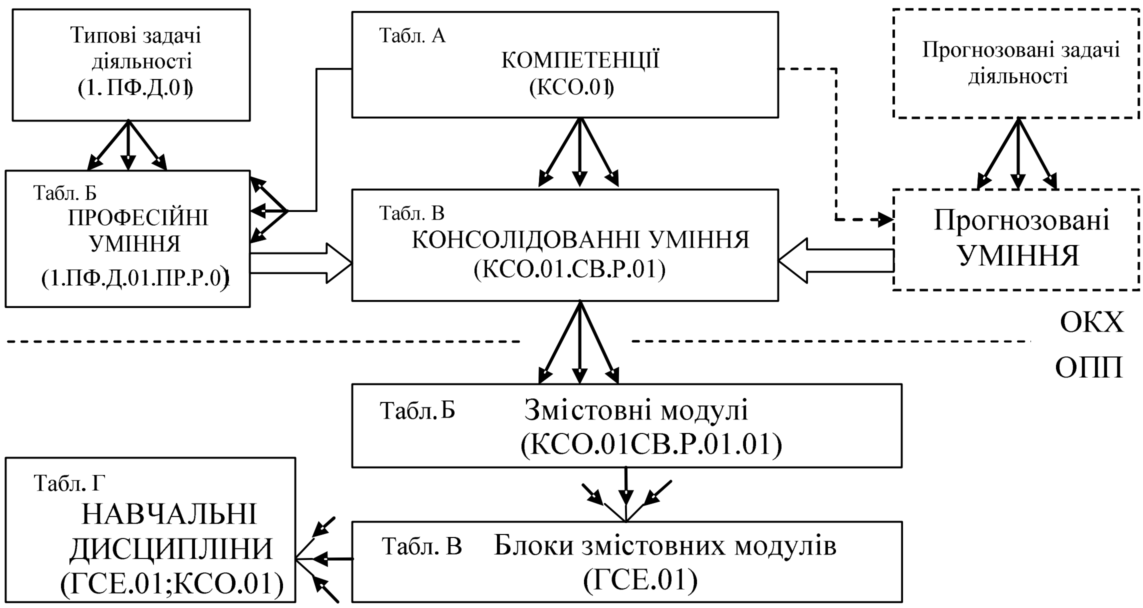


Рис. 2. Процедура формування ГСВОУ 8.17010301-13 магістра за спеціальністю управління інформаційною безпекою

Третя група процедур формування переліків представлена ГСВОУ 8.18010015-07 магістра за спеціальністю специфічних категорій «Консолідована інформація». Ця група така ж, як і перша за винятком того, що: відсутня таблиця компетенції; замість компетенції застосовуються «здатності».

Різноманіття способів кодувань та процедур породжуються першою колізією, яка полягає в тому, що один і той же узагальнений об'єкт – «уміння» кодується двома способами за двома різними форматами а) і б). А існуючі методики, наприклад [5], не містять вказівок, як формувати єдиний перелік умінь. Щоб розібратись у причинах такої колізії розглянемо керівні нормативні документи з цих питань. На рис. 3 [11], який запозичено із [11], показані спрямованість та послідовність розробки нормативного та методичного забезпечення підготовки фахівців. Видно, що зв'язок між ОКХ і ОПП реалізується через єдиний блок «Система умінь». Ясно, що у цьому блоці кодування має бути єдиним. Але яким? З рис. 3 робимо висновок, що система умінь формується на базі блоку виробничих функцій і узагальнених задач діяльності. У цьому блоці кодування може бути виконане по способу з форматом а). Але цей код не обов'язково передавати до блоку системи умінь. В останньому кодування слід виконувати по способу з форматом б).

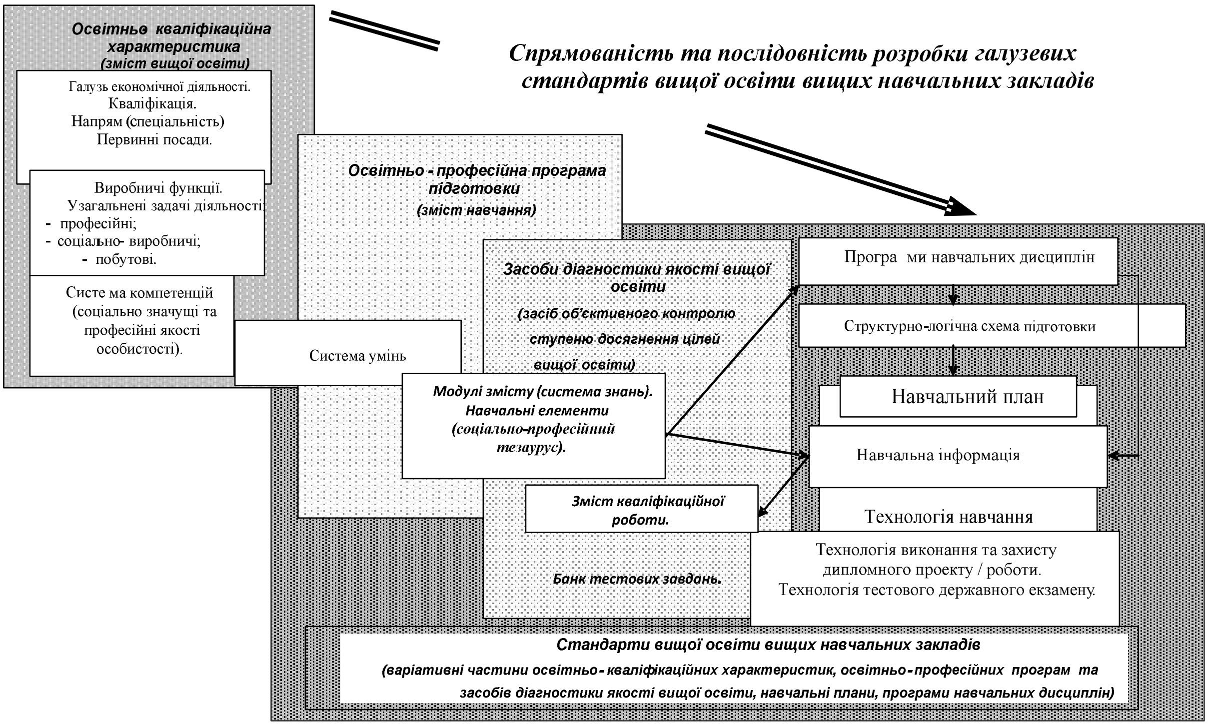


Рис. 3. Спрямованість та послідовність розробки нормативного та методичного забезпечення підготовки фахівців

Із загального розгляду рис. 3 робимо висновок, що у послідовності розробки нормативного та методичного забезпечення підготовки фахівців не передбачені явно внутрішні та зовнішні зворотні зв'язки та сучасний підхід у вигляді циклічної послідовності: збір інформації – аналіз – рішення – дія і далі за циклом. Точніше, методикою передбачені зовнішні зворотні зв'язки з виробничими галузями. Але механізми реалізації цих зв'язків не акцентуються. Усунення вказаних недоліків можливе при застосуванні моделі навчальної та наукової діяльності.

Модель навчальної й наукової діяльності як постачальника компетенції на ринок праці

Галузеві стандарти повинні постійно розвиватись і оновлюватись, не відстаючи від прискорювання технологій. У процедурах формування галузевих стандартів та стандартів вищої освіти вищих навчальних закладів повинні бути внутрішні й зовнішні зворотні зв'язки та модель суб'єкта, який ці зв'язки актуалізує. Ми покажемо далі, що в компетентнісному підході відповідні механізми та модель вже закладені. Завдання полягає у тому, щоб ці механізми представити у явному вигляді та внести корективи у відповідні процедури.

Дійсно у [5] показано наступне. Уміння, представлені у табл. Б і В відповідних додатків до ОКХ. Опис умінь суто професійної сфери подано у таблиці Додатка Б. «Тобто, якщо таблиця Додатка Б є формалізованим описом (моделлю) професійної діяльності фахівця, то таблиця Додатка В – формалізованим описом (моделлю) особистості, готової до вирішення складних проблем та завдань сьогодення та прогнозованого майбутнього на певному рівні, якого вимагає вища освіта [5, розділ 5 методики розроблення ОКХ]». Але у сфері умінь є і третя сторона, сторона, що формує ці уміння. Формування умінь забезпечується виконанням вимог стандарту ОПП. Стандарт ОПП є споживачем продукції стандарту ОКХ. Тому в стандарті ОКХ має бути модель споживача. І цей споживач представляє собою одну із виробничих галузей – галузь виробництва (віртуального), яке поставляє компетенції на ринок праці (точніше – формує уміння у носіїв компетенції). Модель навчальної та наукової діяльності (ННД) вже існує. Формалізований її опис можна ввести в ОКХ такими способами:

1. Сформувати опис ННД на базі таблиці Додатка Б, як це зроблено у першій групі процедур формування стандарту. Цей спосіб неприйнятний внаслідок складної кодифікації у таблиці Додатка Б. Крім того, перелік умінь виявляється занадто детальним.
2. Сформувати консолідований опис із включенням опису ННД на базі таблиці Додатка В, як це зроблено у другій групі процедур формування стандарту.
3. Створити додаткову таблицю у новому Додатку Г, де навести перелік умінь з урахуванням всіх трьох моделей – моделі професії, моделі професіонала та моделі системи, яка формує професіонала.

Найбільш прийнятним є спосіб 2. Для реалізації цього способу можна внести доповнення до процедур формування стандартів так, як це показано на рис. 2 пунктиром.

Пояснимо детальніше функції моделі ННД. Неформальний опис функцій моделі надано у розділі 6 методики розроблення ОКХ, де, зокрема, сказано: «У разі встановлення структури праці слід також враховувати результати прогнозу професійних і соціально важливих задач діяльності, які в майбутньому буде виконувати випускник вищого навчального закладу (ВНЗ) у своїй практичній діяльності на рівні компетенції, що вимагається. Опис діяльності випускника ВНЗ на первинній посаді повинен віддзеркалювати середньостроковий прогноз змін цієї діяльності [5, с. 40]». Далі цитуємо цю методику у вільному переказі, звертаючи увагу на особливостях моделі.

Прогнозування діяльності фахівців здійснюється шляхом визначення структури проблем прогресу, які вони повинні вирішувати в майбутній діяльності. Зміст проблем визначають, виходячи з результатів наукових досліджень і практики виробництва.

Проблематика діяльності наукових установ, наукової та науково-методичної діяльності самого вузу, дослідження розвитку технологій допомагає визначити зміст майбутніх професійних завдань як у науковій, так і у виробничій сферах діяльності. Те, що сьогодні представляє наукову чи технологічну проблему, завтра може стати однією з конкретних задач діяльності.

Розроблена класифікація, яка може стати структурою формалізованого опису в ОКХ моделі навчальної й наукової діяльності. Так визначено вектор ознак у таксономії виробничих функцій: дослідницька, проектувальна, організаційна, управлінська, технологічна, контрольна, прогностична, технічна.

Визначені функції формування переліків прогнозованих задач діяльності та відповідних прогнозованих умінь у блоках, які додані до процедури формування стандартів на рис. 2. «На основі аналізу структури професійної діяльності фахівця, переліку предметів його професійної праці й сукупності виробничих функцій, що виконує фахівець на основних, посадах або виконання яких прогнозується в майбутньому, необхідно встановити перелік типових задач, які йому потрібно вміти вирішувати, та вид задачі діяльності, до якого кожна з них віднесена. Перелік задач професійної діяльності подається до таблиці Додатка Б до ОКХ. [5]». Консолідований перелік у системі умінь може формуватись за допомогою таблиці Додатка В до ОКХ.

Оцінка якості системи класифікації за допомогою оцінки внутрішньої кореляції ознак

«Класифікація являється інтелектуальною діяльністю високого рівня, необхідною нам для розуміння природи. Класифікація – це упорядкування об'єктів за їх схожістю [1, с.]». Об'єкту приписується вектор дескрипторів. Кількісно оцінити схожість можна таким способом. Експерт робить загальну оцінку схожості об'єктів і виражає числом від 0 до 1 або за допомогою нерівностей між парами або трійками об'єктів. Отримані результати оцінок усереднюються по деякому достатньому числу експериментів. Другий спосіб кількісної оцінки схожості полягає у спробі знайти основу для суджень щодо схожості. «Це досягається звичайно за допомогою детального опису властивостей, на основі яких, як уважають, можна виразити схожість. Цей підхід привів до деталізації та дробленню дескрипторів об'єктів, які необхідно класифікувати. Кожному об'єкту приписуються довгі списки дескрипторів [1]».

У нашому випадку, умінням приписується ієрархія векторів дескрипторів. Уміння, як ОТО, представлені у просторі, вимірами якого є ознаки. Цей ознаковий простір формально є n-мірним. Наприклад, умінню «використовуючи посібники, довідники, словники, документи написати наукову статтю (доповідь) на одній з іноземних мов», якому надано код 1.ПФ.Д.04.ПР.О.02, приписані ознаки: ПФ – професійної типової задачі діяльності, Д – діагностичного класу діяльності, ПР – предметно-розумового виду уміння, О – рівня сформованості уміння. Числа приписують уміння до номеру, відповідно, номеру виробничої функції, номеру типової задачі діяльності та номеру самого уміння.

Між ознаками ОТО можуть бути кореляції. Якщо кореляції між ознаками ОТО значні, то за звичаєм, простір ознак може бути перетворено у простір меншої розмірності з невеликою втратою інформації. Тому дослідження внутрішньої кореляції класифікації має сенс з точки зору пошуку можливостей вдосконалення класифікації.

Дослідимо кореляції між лівою та правою частиною ознак у класифікації умінь виконувати типові задачі діяльності у трьох стандартах, які розглядаються у даній роботі. Результати дослідження наведені у табл. 1. Якщо кореляції між показниками ознак малі, то формально якість класифікації висока. Навпаки, якщо є суттєві кореляції, то – якість низька.

Із аналізу табл. 1 слідує, що частості появи пар ознак розподіляються по певному кластеру більш-менш рівномірно. Кореляції між ознаками у парі майже всюди малі. Зважаючи на малий об'єм вибірки, точність оцінки невисока. Але можна стверджувати, що в цілому, формально, якість класифікації висока. Є лише один виняток значної кореляції, майже функціональна залежність у рядку 10 табл. 1. Якщо з'явилась комбінація ознак ПФ.С, то майже завжди її буде супроводжувати комбінація ознак ПП.О. Але розгляд табл. 1 виявляє ряд принципових моментів, які вказують на можливість вдосконалення класифікації в ГСВОУ.

1. Викликає здивування, що кластери кодів умінь у ГСВОУ, які розроблені у різних науково-методичних комісіях, зовсім не пересікаються. На рівні погрішності є

незначний виняток у рядку 4 табл. 1. Цьому нема раціонального пояснення. Такої несхожості стандартів одного й того ж освітньо-кваліфікаційного рівня не може бути. Автори схиляються до думки, що справа тут у суб'єктивності оцінок. Можна припустити, що при формуванні стандартів не застосовувалась одна з важливих процедур експертних оцінок, коли після проведення раунду незалежних оцінок, експертам пред'являються результати оцінок і пропонують скоригувати свої оцінки. І так доти, поки якість експертних оцінок не досягне прийнятного рівня.

Таблиця 1.

Оцінка кореляції (частотності появи) пари ознак лівої та правої частини у класифікації коду уміння виконувати типові задачі діяльності

№ з\п	Пари ознак класифікації умінь виконувати типові задачі	Кількість (частотність) появи пари ознак у		
		ГСВОУ 8.17010301 «Управління інформаційною безпекою»	ГСВОУ 8.05100304 «Прилади і системи екологічного моніторингу»	ГСВОУ 8.18010015 «Консолідована інформація»
1	2	3	4	5
1	ПФ.Д – ПР.Р	3	–	–
2	ПФ.Д – ПП.Р	2	–	–
3	ПФ.Д – ЗП.Р	3	–	–
4	ПФ.Д – ПР.О	1	20	–
5	ПФ.Д – ПП.О	–	8	–
6	ПФ.Е – ПП.Р	1	–	–
7	ПФ.Е – ПР.Р	2	–	–
8	ПФ.Е – ЗП.Р	2	–	–
9	ПФ.Е – ЗР.Р	2	–	–
10	ПФ.С – ПП.О	6	–	–
11	ПФ.С – ПП.Р	1	–	–
12	СВ.Д – ЗП.Р	6	–	–
13	СВ.Д – ЗР.Р	2	–	–
14	СВ.Е – ЗР.Р	8	–	–
15	СВ.Д – ПР.О	–	5	–
16	СВ.Д – ПП.О	–	4	–
17	СВ.Д – ПР.Р	–	7	–
18	СВ.Д – ПР.О	–	7	–
19	СВ.Д – ЗР.О	–	–	2
20	ПФ.Е – ЗР.О	–	–	6
21	ПФ.Д – ЗР.О	–	–	7
	Всього (вибірка)	39	51	15

Проте, може бути доцільним заохочувати вузи до впровадження академічних свобод.

2. Спостерігається суб'єктивність та різноманіття у застосуванні шкали класів задач діяльності. Частість застосування показників цієї ознаки виглядає так:

ГСВОУ 8.17010301: Е – 16 разів, Д – 17 разів, С – 7 разів;
ГСВОУ 8.05100304: Е – 0 разів, Д – 51 раз, С – 0 разів;
ГСВОУ 8.18010015: Е – 6 разів, Д – 9 разів, С – 0 разів.

Одні вузи застосовують шкалу рівномірно, другі приписують умінням магістр лише діагностичний (Д) клас, інші не використовують стереотипний (С) клас задач діяльності.

Позиція авторів полягає у тому, що клас задач діяльності повністю корелює із освітньо-кваліфікаційним рівнем (є функціональний зв'язок) і приписується всім умінням магістра. Це може бути евристичний (Е) клас, а для специфічних галузей – діагностичний (Д).

Якщо одне і теж значення ознаки зустрічається в усіх без винятку кодуваннях умінь, то цю ознаку треба винести у префікс коду і позначати його на титульному аркуші стандарту для економії місця. Інакше кажучи, треба винести цю ознаку поза стандарт на рівень, з яким він корелює. Тоді узгодження кодування типів задач діяльності з кодуванням компетенції при консолідації переліку умінь стане простішим.

3. Розглянемо, не як пропозицію, а скоріше як роздуми щодо проблеми рівнів сформованості уміння. Тут також спостерігається нерівномірність і хаотичність у застосуванні шкали рівнів сформованості уміння. Частість застосування виглядає так:

ГСВОУ 8.17010301: Н – 0 разів, Р – 32 рази, О – 7 разів;

ГСВОУ 8.05100304: Н – 0 разів, Р – 7 разів, О – 44 рази;

ГСВОУ 8.18010015: Н – 0 разів, Р – 0 разів, О – 15 разів.

Рівень Н не застосовується зовсім. Використання рівня Р та О нагадує попередній випадок. Можна стверджувати, що рівень сформованості уміння корелює з класом задач діяльності. Тому, якщо цю ознаку залишати у системі класифікації то вони, частково, дублюють одна одну. Автори не можуть оцінити наскільки ознака «рівень сформованості уміння» важлива для класифікації типів задач діяльності. А в сфері вищої освіти ознака рівня сформованості уміння може бути зайвою після запровадження змагальності у навчальному процесі та рейтингової системи оцінки успішності навчання. Для діагностики якості вищої освіти можна застосовувати рейтингову систему оцінки.

Різні підходи до застосування шкал та приписування показників ознакам класифікації можна пояснити як наслідок застосування різних процедур формування ГСВОУ. Нагадаємо, що у процедурах першого та третього типів (див. рис. 1) на основі переліку умінь, сформованих в ОКХ, формуються відповідні їм змістовні модулі. У процедурі другого типу (див. рис. 2) – формуються відповідні їм блоки змістовних модулів. Тобто, у процедурі другого типу формулюються уміння більш узагальнені і менш деталізованими. Деталізація змістовних модулів виконується у сформованих навчальних дисциплінах. Більш раціональною здається процедура другого типу, що пояснюється наступним.

В сучасній науці, і слідом за нею в освіті відбувається перехід від дроблення напрямів і спеціальних дисциплін, до розвитку міждисциплінарних наук. Прикладом можуть бути інформатика та кібернетика, управління інформаційною безпекою, синергетика, консолідована інформація тощо.

Для обґрунтування означених позицій авторів розглянемо табл. 2, де показані співвідношення класу задач діяльності та освітньо-кваліфікаційного рівня у індустріальному суспільстві та прогноз цього співвідношення для постіндустріального суспільства.

Таблиця 2.

Прогноз динаміки типів задач діяльності та освітньо-кваліфікаційних рівнів

Класи задач діяльності	Освітньо-кваліфікаційні рівні в	
	індустріальному суспільстві	постіндустріальному суспільстві
С – стереотипна	Робочий, молодший спеціаліст	Робот
Д – діагностична	Спеціаліст	Креативний спеціаліст
Е – евристична	Магістр	Магістр

Є функціональний зв'язок між класами задач діяльності та відповідними освітньо-кваліфікаційними рівнями. Існує тенденція до передачі стереотипної діяльності роботам навіть на побутовому рівні. Змінюється розподіл працюючих за видами виробництва. Доля працівників, зайнятих у сільському господарстві, впаде до 2 – 4 %. Доля зайнятих у матеріальному виробництві зменшиться до 10 – 15 %. Основна маса працюючих зосередиться у сфері обслуговування, інформаційній сфері, віртуального (інформаційного) виробництва, у сфері культури тощо. Відповідно зміниться структура та задачі освітянської сфери. На всіх рівнях значно збільшиться потреба у такій складовій компетенції як креативність.

Поняття креативності остаточно ще не сформовано. Креативність – це творчі здібності людини, які можуть проявлятись у мисленні, почуттях, спілкуванні, окремих видах діяльності, характеризувати особистість у цілому та/або її окремі сторони, продукти діяльності, процеси створення. Креативність визначається не стільки критичним відношенням до нового з точки зору наявного досвіду, скільки сприйнятливістю до нових ідей. П. Торенс визначив креативність як процес появи чутливості до проблем, до дефіциту або дисгармонії наявних знань, визначення цих проблем, пошук їх вирішення, висунення гіпотез, перевірок, намірів, зміни та перевіряння гіпотез, і нарешті, формулювання та повідомлення результату рішення.

Стирається різниця між освітньою діяльністю і віртуальною виробничою діяльністю. Вони стають подібними один одному. Обидві галузі виробляють інформацію і знання. Стає можливою природна конвергенція цих галузей. Універсальна освітянська галузь має поставляти на ринок праці компетентність, креативність та самоосвітність. Втім, проблеми класифікації умінь та компетенції в постіндустріальному суспільстві ще тільки назрівають. Цей напрямок може стати тематикою подальших досліджень. Повертаючись до проблеми консолідації класифікації, можна стверджувати наступне.

Внаслідок суб'єктивного характеру створення та застосування класифікації фахових умінь існуюча класифікація являється занадто детальною і складною. Це робить її незручною для формування ГСВОУ, відволікаючи увагу від змістовної частини стандарту. Існуюча класифікація умінь закріплює деякі застарілі принципи і положення. Це приводить до колізій і утруднює досягнення мети класифікації. Існуюча класифікація відповідає потребам індустріального суспільства. Це ставить задачу еволюції системи класифікації та розробки її не принципах мобільності та циклічності, універсальності та модульності, конвергентності та самоорганізації. Це трудні задачі нового, але недалекого майбутнього.

Дослідження міжкластерної кореляції компетенції та виробничих функцій

Діяльність навчання, не кажучи вже про наукову діяльність, значно складніша у порівнянні з виробничою діяльністю. Виробничою діяльністю ціле направлено займається група (іноді багато численна) фахівців даної галузі виробництва, більш-менш незалежна від інших груп. Діяльністю навчання теж займається певна група фахівців галузі віртуального навчального виробництва. Продукцією цього виробництва є компетенція, яка постачається на ринок праці. Ринок праці потребує носіїв цієї компетенції – людей і роботів.

Але в діяльності навчання (і самонавчання), свідомо чи несвідомо, приймають участь багато інших груп: сім'я, трудові колективи, неформальні угрупування, соціальні мережі, книги, засоби масової інформації, телебачення, Інтернет, по суті все суспільство і навіть навколишнє середовище. Мають значення традиції, менталітет, моральний клімат, і ще багато чого, можливо ще не до кінця вивченого. Не дивно, що для класифікації виробничої та навчальної діяльності застосовуються різні шкали. Для класифікації виробничої діяльності застосовується шкала видів типових задач діяльності: ПФ, СВ, СП. Для класифікації навчальної (і, можливо, наукової) діяльності застосовується шкала ознак компетенції: КСО, КЗП, КІ, КЗП, КСП. Шкали різні як по кількості ознак, так і за змістом. І тут, при формуванні ГСВОУ, виникає ще одна (друга) колізія: різні шкали застосовуються до одного й того ж суб’єкта – професіонала, (моделі) особистості, готової до вирішення складних проблем та завдань сьогодення. Для консолідації переліку умінь, ці шкали треба якось узгодити. Тоді необхідно дослідити степінь їх схожості і оцінити схожість кількісно. Виникає задача оцінки міжкластерної кореляції.

Ми маємо тут третю колізію – термінологічну. Ознака ПФ – професійний є частиною більш широкої ознаки СВ – соціально-виробнича. За словником іншомовних слів поняття «соціальний» означає: суспільний, громадський, той, що стосується суспільного ладу. Професійна сфера є частиною соціально-виробничої сфери. Тому будемо розуміти СВ як загальну соціально-виробничу сферу, а ПФ – як спеціальну соціально-виробничу сферу.

Послідовність процедур класифікації така, що об’єкти, які належать до класифікації – ОТО – представлені у просторі, вимірами якого є ознаки. У нашому випадку цей ознаковий простір являється двомірним.

Схожість між ОТО, які описуються словесними позначеннями оцінюються коефіцієнтами асоціативності. Вони представляють собою відношення спостерігаємої співпадаємості значень ознак для пари ОТО до можливого числа співпадань або до можливого числа означень схожості. «Загальний вид коефіцієнта асоціативності – це коефіцієнт схожості» [1, формула на с.11]

$$S_{jk} = \sum_{i=1}^{n} w_{ijk} s_{ijk} \Big/ \sum_{i=1}^{n} w_{ijk}\ , \qquad (1)$$

де $0 \le s_{ijk} \le 1$ – схожість між станами ознаку i для ОТО j та k; w_{ijk} – вага, що приписується цій ознаці; n – число ознак.

Середній коефіцієнт асоціативності по всьому кластеру

$$S_{\text{C}} = \sum_{j=1}^{m} \sum_{k=1}^{l} S_{jk} \Big/ (ml), \qquad (2)$$

де n та l – число ознак по відповідним осям простору ознак.

Таблиця 3.

Оцінки схожості показників видів типових задач діяльності та компетенції

Види типових задач діяльності	Компетенції				
	КСО	КЗН	КІ	КЗП	КСП
ПФ	0	0.5	0.33	0.33	0.33
СВ	0.5	0.4	0.33	0.33	0.33
СП	0.5	0.1	0.2	0	0

Побудуємо матрицю за формулою (1), показану у табл. 3, і яка має розмірності по осі видів типових задач діяльності та осі компетенції. Вагу, що приписується кожній з ознак будемо вважати однаковою. Тоді у знаменнику формули (1) маємо $\sum = 1$. В комірках матриці показані оцінки експертів – авторів даної роботи – схожості ознак умінь професіонала з позицій виробництва і з позицій навчання. Оцінки подані в шкалі від 0 до 1. Якщо певна ознака схожа на декілька ознак по другій осі, то оцінка поділяється між останніми. Наприклад, ознака КСО – соціально-особистісної компетенції схожа на ознаки СВ – соціально-виробничих задач та СП – соціально-побутових задач діяльності. Тоді кожній з останніх приписуємо оцінку 0.5.

Середній коефіцієнт асоціативності по всьому кластеру, обчислений за формулою (2), складає величину $S_c = 0.28$. Середній коефіцієнт асоціативності можна підвищити за рахунок вдосконалення системи класифікації. Більш ефективною може бути розробка політетичної класифікації умінь, заснованої на статистичному підході [1, с. 9]. «За такої класифікації ОТО агреговані відносно багатьох вимірювань простору ознак. Різні ОТО будуть відхилятись від кластера вздовж різних ознакових осей, але можуть бути розподіленими по всій області деяких значень». Тоді класи об’єктів можна визначати не за всіма ознаками, а по найбільшому числу спільних значень ознак, так що ні одна з ознак самостійно не визначає належність до даного класу. Такого типу класифікації близькі до багатьох природних класифікацій.

Висновки

Сформовані в даній статті принципи консолідації класифікації фахових умінь та модель наукової та навчальної діяльності придатні для формування галузевих стандартів вищої освіти, принаймні, у технічних, економічних і природничих галузях вищої освіти. Консолідована класифікація простіша, враховує сучасні тенденції техніки і науки до конвергенції, міждисциплінарності, що дозволить підвищити якість освітніх стандартів. Вони дозволяють чітко визначити напрямки подальших досліджень щодо побудови консолідованої класифікації та кодифікації фахових умінь та компетенції, а також розробки ефективної процедури формування галузевих стандартів вищої освіти. Темою подальших досліджень може стати розробка політетичної класифікації фахових умінь.

Список літератури

1. Классификация и кластер [Текст] / ред. Дж. Вэн. Райзен, перевод с англ. П.П. Кольцова под ред. Ю.И. Журавлева. – М.: Издательство МИР, 1980. – 391 с.
2. Яремчук, Ю.Є. Підхід до формування ієрархічних класифікацій методів захисту телекомунікаційних мереж від негативного впливу / Ю.Є. Яремчук, А.А. Шиян // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2014. – № 4. – С. 226–230.
3. Матвієнко, О.В. Консолідована інформація : навч. посібник / О.В. Матвієнко, М.Н. Цивін. – К.: «Центр учбової літератури», 2014. – 134 с.
4. Професійна педагогічна освіта: компетентнісний підхід: монографія / за ред. О.А. Дубасенюк. – Житомир: Вид-во ЖДУ ім. І. Франка, 2011. – 412 с.
5. Гуло, В.Л. Методичні рекомендації з розроблення складових галузевих стандартів вищої освіти (компетентнісний підхід) / В.Л. Гуло та ін. – К.: Вид. ІІТЗО, 2013. – 92 с.
6. ГСВОУ 8.17010301-13. Галузевий стандарт вищої освіти України. Освітньо-кваліфікаційна характеристика магістра за спеціальністю управління інформаційною безпекою. – 41 с.
7. ГСВОУ 8.05100304-13. Галузевий стандарт вищої освіти України. Освітньо-кваліфікаційна характеристика магістра за спеціальністю прилади і системи екологічного моніторингу. – 38 с.
8. ГСВОУ 8.18010015-07. Галузевий стандарт вищої освіти України. Освітньо-кваліфікаційна характеристика магістра за спеціальністю специфічних категорій «Консолідована інформація». – 20 с.
9. Управление риском [Электронный ресурс] / под ред. Г.Г. Малинецкого. – М.: РАН, 2000. – 249 с. – Режим доступа: http://risk.keldysh.ru/risk/risk.htm.
10. Малинецкий, Г.Г Процессы глобализации и компьютерное моделирование [Электронный ресурс] / Г.Г. Малинецкий, С.А. Махов, С.А. Посашков // Раздел сайта С.П. Курдюмова «Глобализация: синергетический подход». – 6 с. – Режим доступа: http://spkurdyumov.ru/globalization/processy-globalizacii-i-kompyuternoe-modelirovanie/.
11. Болюбаш, Я.Я. Комплекс нормативних документів для розроблення складових системи галузевих стандартів вищої освіти / Я.Я. Болюбаш та ін. // Інститут інноваційних технологій і змісту освіти. – К.: ІІТЗМО, 2008. – 64 с.

КОНСОЛИДАЦИЯ КЛАССИФИКАЦИИ В МОДЕЛЯХ КОМПЕТЕНЦИИ И УМЕНИЙ В ОТРАСЛЕВЫХ СТАНДАРТАХ ВИЩЕГО ОБРАЗОВАНИЯ

А.А. Кобозева[1], В.Г. Кононович[1], И.В. Кононович[2], О.В. Николаенко[1]

[1] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net
[2] Одесская национальная академия пищевых технологий
ул. Канатная, 112, г. Одеса, 65039, Украина; e-mail: kononovich@mail.ru

Рассматривается проблема классификации и кодификации умений специалистов в связи с обнаруженными коллизиями в практике формирования стандартов высшего образования в технических и экономических отраслях в условиях применения компетентностного подхода. Найдены коллизии, причини которых состоят в том, что: а) отсутствует методика формирования единого перечня умений специалиста с умений решать типовые задачи деятельности и умений, которые обеспечивают формирование компетенции; б) отсутствуют модели обратных связей и модель поставщика компетенции на рынок труда. Использованы методы шкалирования, информационной аналитики и корреляционный кластер-анализ. Предложен вариант модели деятельности обучения. Сформированы принципы консолидации классификации умений, которая применима, по крайней мере, в технических, экономических и природных отраслях высшего образования. Консолидированная классификация проще, учитывает современные тенденции техники и науки к конвергенции, междисциплинарности, что позволит повысить качество образовательных стандартов.

Ключевые слова: классификация, кластеры, отраслевые стандарты, консолидация информации, компетенции, умения, задачи деятельности, классы задач деятельности, корреляция, коды (шифры) умений.

IN HIGHER EDUCATION INDUSTRY STANDARDS: THE ECONOMIST'S POINT OF VIEW

A.A. Kobozeva[1], V.G. Kononovich[1], I.V. Kononovich[2], O.V. Nikolayenko[1]

[1]Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: vl_kononovich@ukr.net
[2]Odessa National Academy of Food Technologies,
112 Kanatna St., Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

The paper discusses the problem of classification and codification of professional skills in the context of the conflicts found in the practice of the development of higher education standards for technical and economical branches using a competency-based approach. We found the conflicts caused by the following: (a) no methodology exists to form a uniform list of professional skills from the skills of solving typical professional tasks and those ensuring the formation of competency; (b) neither the feedback model nor the model of the competency supplier to the labor market exists. Scaling, data analysis and correlation cluster analysis methods were used. An education activity model was proposed. We proposed the principles to develop a consolidated classification of professional skills which would be suitable in technical, economical and natural science branches of higher education. A consolidated classification is rather simple, and takes account of the current science and technology trends to convergence and integrated approach, thus making it possible to improve education standards.

Keywords: classification, clusters, branch standards, data consolidation, competency, professional skills, professional activity tasks, classes of professional activity tasks, correlation, skill codes.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, PP. 57-64

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ, ОБЕСПЕЧИВАЮЩИЙ ПРОВЕРКУ ЦЕЛОСТНОСТИ И АУТЕНТИЧНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

А.А. Кобозева, М.А. Козина

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

В работе предлагается усовершенствование ранее разработанного авторами стеганографического метода, решающего одновременно актуальную на сегодня триединую задачу стеганографии: скрытой передачи данных, проверки их аутентичности и целостности. В качестве контейнера используется цифровое цветное изображение, а в качестве дополнительной информации выступает произвольным образом сформированная бинарная последовательность. Усовершенствование стеганографического метода включает в себя: уменьшение объема необходимо передаваемой информации по защищенному каналу связи для организации аутентификации данных; обеспечение возможности декодирования переданной информации без наличия контейнера. Приведены результаты вычислительных экспериментов, подтверждающие высокую эффективность предложенного метода.

Ключевые слова: стеганографический метод, скрытый канал связи, целостность, аутентичность, дискретное преобразование Фурье, цифровое изображение.

Введение

Стеганография – наука, которая изучает и обеспечивает сокрытие информации в произвольном носителе-контейнере (например, фото, видео и др.), таким образом, чтобы никто, кроме отправителя и получателя, не подозревал о существовании передаваемой информации [1,2]. Не ограничивая общности рассуждений, далее как контейнер используется цифровое изображение (ЦИ).

Стеганография помогает решать вопросы, связанные с защитой авторских прав, проверкой подлинности, целостности различных информационных контентов.

Существующие стеганографические методы могут осуществлять погружение скрываемой, или дополнительной информации (ДИ), как в пространственной, так и в частотной областях изображения. Традиционно считается [1], что стеганопреобразование, реализуемое в частотной области изображения, более устойчиво к различным видам возмущений (под устойчивостью стеганографического алгоритма, согласно [3], понимается нечувствительность к возмущающим воздействиям сформированного им стеганосообщения (СС) (СС – результат внедрения ДИ в контейнер)).

К современным стеганографическим методам предъявляется ряд требований, одновременное удовлетворение которых является нетривиальной, нерешенной до конца, а потому актуальной на сегодняшний день задачей. Так при организации скрытого канала связи внутри канала общего пользования необходимо обеспечение не только надежности восприятия СС [3], устойчивости стеганоалгоритма к атакам против встроенного сообщения и стеганоанализу, но и возможности проверки целостности передаваемой информации/контейнера, аутентификации информационных контентов.

Необходимо заметить, что последнее требование, которое чаще всего в настоящий момент обеспечивается путем использования цифровой подписи, имеет свои особенности при обеспечении его для мультимедийной информации: сообщение, содержащее цифровую подпись, должно храниться или передаваться абсолютно точно «бит в бит», но данные, которые хранятся в цифровом формате, могут незначительно искажаться как на этапе хранения (например, при сжатии), так и при передаче по каналу связи, не теряя своей аутентичности. Кроме того, значительным недостатком цифровой подписи является то, что ее можно легко удалить и прикрепить новую, отвечающую другому владельцу/автору информации [3]. Все это оставляет на сегодняшний день актуальной задачу организации аутентификации информации саму по себе.

Попытки одновременного решения нескольких задач стеганографии, в частности, организации скрытого канала связи с проверкой аутентичности ЦИ-контейнера уже предпринимались [4-6], однако предлагаемые решения нельзя назвать удовлетворительными. Так стеганографический метод, предложенный в [4], не гарантирует надежность восприятия формируемого СС, что ставит под сомнение принципиальную возможность его использования при организации стеганографического канала связи. Усовершенствование обсуждаемого метода было предложено в [5], однако и здесь вопрос обеспечения надежности восприятия СС не нашел окончательного решения. Не лишен значительных недостатков и метод, разработанный в [6].

В [7] Козиной М.А. был предложен стеганографический метод, обеспечивающий скрытую передачу произвольной бинарной последовательности с одновременной проверкой целостности ДИ, соблюдение надежности восприятия стеганосообщения, устойчивость к возмущающим воздействиям в канале связи, который послужил основой для разработки в [8-9] уникального, как можно судить из открытой печати, метода, обеспечивающего решение триединой задачи стеганографии (ТЗ):

1. Организации скрытого канала связи (с соблюдением надежности восприятия и нечувствительности формируемого СС к возмущающим воздействиям);
2. Проверку целостности ДИ;
3. Проверку аутентичности передаваемой информации.

Цель статьи и постановка заданий

При всей своей уникальности, стеганометод, предложенный в [8,9], не лишен недостатков:

1. Необходимость наличия контейнера для организации декодирования ДИ;
2. Большой объем информации, необходимо передаваемой по защищенному каналу связи.

В связи с этим *целью* данной работы является усовершенствование предложенного в [8,9] стеганографического метода путем уменьшения объема информации, которую необходимо передавать по защищенному каналу связи для организации аутентификации данных; обеспечения возможности декодирования передаваемой информации без наличия контейнера.

Задачи, которые необходимо решить для достижения цели:

1. Выбор информации, которая будет передаваться по защищенному каналу связи для обеспечения возможности декодирования скрываемой информации без наличия контейнера;
2. Выбор способа формирования секретного ключа стеганометода ;
3. Выбор устойчивого к возмущающим воздействиям способа внедрения ключа для организации аутентификации ДИ, обеспечивающего надежность восприятия СС.

Основная часть

В работе в качестве контейнера выступает цифровое цветное изображение произвольного формата, для хранения которого используется схема RGB. Пусть B — $M \times N$ -матрица — одна из цветовых составляющих ЦИ-контейнера.

Рассмотрим основные шаги предлагаемого усовершенствованного стеганографического метода, обозначаемого далее SM_3, и принципиальные его отличия от разработанного в [8,9].

Кодирование. Опираясь на существующие принципы аутентификации передаваемой информации, описанные в [1], разобьем множество имеющихся изображений-контейнеров произвольно на подмножества. Каждому *i*-му подмножеству поставим в соответствие уникальную числовую метку num_i, выбираемую из диапазона [a; b], и уникальный бинарный ключ кодирования K_j − $q \times p$ -матрицу, участвующий в предварительном кодировании дополнительной информации, $j = 1,2,...,2^{q \cdot p}$, которые в совокупности образуют так называемую стеганографическую пару (num_i, K_j), далее обозначаемую *SP*. В общем случае количество сформированных ключей кодирования K_j должно быть не меньше количества меток num_i, чтобы каждое подмножество контейнеров получило свой уникальный ключ кодирования. Соответствие между метками подмножеств контейнеров и ключами кодирования (или их однозначно определяемыми номерами, или однозначно определяемыми метками) устанавливается произвольным образом. Множество полученных стеганографических пар, обозначаемое далее *MSP*, определяет секретный ключ стеганоалгоритма, передается по защищенному каналу связи, в отличие от [8,9] имеет реальные размеры.

Основные шаги при определении ЦИ-контейнера и соответствующих ему параметров в SM_3:

1. Выбрать случайным образом из *MSP* стеганографическую пару *SP* (num_i, K_j).
2. Выбрать подмножество контейнеров, которое отвечает метке num_i.
3. Из полученного на предыдущем шаге подмножества выбрать произвольным образом ЦИ-контейнер для дальнейшего погружения ДИ, с использованием соответствующей *SP* (num_i, K_j).

Опишем основные моменты стеганопреобразования, обеспечивающего надежность восприятия СС, которые были предложены в [7] и используются в SM_3.

Матрица B разбивается стандартным образом на непересекающиеся блоки размером 2×2, которые далее обозначаются $F_{nm}^{(B)}$, $n = \overline{1, \left[\frac{N}{2}\right]}$, $m = \overline{1, \left[\frac{M}{2}\right]}$. Для каждого блока строится дискретное преобразование Фурье (ДПФ). В [10] была обоснована целесообразность выбора упомянутого размера блока, который обеспечивает получение вещественных частотных коэффициентов, а также предложен способ получения целых частотных коэффициентов ДПФ, что явилось основой для организации проверки нарушения целостности ДИ на этапе декодирования.

Дополнительная информация представляет из себя случайным образом сформированную бинарную последовательность $p_1, p_2, ..., p_t$, $p_j \in \{0,1\}$, $j = \overline{1,t}$. С помощью ключа кодирования K_m, для которого $q = p = R$, происходит ее побитовое кодирование:

$$p_j \otimes K_m = \begin{pmatrix} p_j \otimes K_{1,1}^{(m)} & p_j \otimes K_{1,2}^{(m)} & \dots & p_j \otimes K_{1,R}^{(m)} \\ p_j \otimes K_{2,1}^{(m)} & p_j \otimes K_{2,2}^{(m)} & \dots & p_j \otimes K_{2,R}^{(m)} \\ \dots & \dots & \dots & \dots \\ p_j \otimes K_{R,1}^{(m)} & p_j \otimes K_{R,2}^{(m)} & \dots & p_j \otimes K_{R,R}^{(m)} \end{pmatrix} = \begin{pmatrix} P_{1,1}^{j(K)} & P_{1,2}^{j(K)} & \dots & P_{1,R}^{j(K)} \\ P_{2,1}^{j(K)} & P_{2,2}^{j(K)} & \dots & P_{2,R}^{j(K)} \\ \dots & \dots & \dots & \dots \\ P_{R,1}^{j(K)} & P_{R,2}^{j(K)} & \dots & P_{R,R}^{j(K)} \end{pmatrix} = P^{j(K)},$$

где p_j - очередной бит ДИ, $\otimes$ - логическая операция «исключающее ИЛИ»; $K_{k,l}^{(m)}$, $k,l=\overline{1,R}$ - элементы матрицы K_m; $P^{j(K)}$ - $R\times R-$матрица с элементами $P_{k,l}^{j(K)}, k,l=\overline{1,R}$, которая отвечает 1 биту p_j ДИ после кодирования.

После этого каждый очередной элемент $P_{k,l}^{j(K)}$ сформированной бинарной матрицы $P^{j(K)}$ внедряется в очередной используемый для стеганопреобразования блок $F_{nm}^{(B)}$. Результат – блок $FF_{nm}^{(B)}$ с элементами:

$$FF_{nm}^{(B)}(u,v)=bitset\left(F_{nm}^{(B)}(u,v), pos, P_{k,l}^{j(K)}\right),\ u,v=\overline{0,1}, \tag{1}$$

где $bitset$ - операция, которая реализована в пакете Matlab (2009), работает следующим образом: значение $P_{k,l}^{j(K)}$ устанавливается в указанной позиции pos от правого конца двоичного представления элемента $F_{nm}^{(B)}(u,v)$, где $pos\in\{2,3,4\}$ [7]. Таким образом, погружение 1 бита ДИ происходит в блок матрицы B размером $2R\times 2R$, что с учетом желаемого обеспечения достаточной скрытой пропускной способности, накладывает ограничения сверху на размер R матрицы ключа кодирования.

Внедрение ДИ происходит не во все $2R\times 2R-$блоки матрицы B. Предлагается оставлять P (P – нечетное число) блоков $Bl_k, k=\overline{1,P}$, размером 8×8, расположение которых в пределах B может являться частью секретного ключа стеганоалгоритма, реализующего SM_3, для погружения метки контейнера num_i. Выбор размера блока связан с предлагаемым способом погружения num_i, описанным ниже, и никак не связан с размером матриц, участвующих при кодировании и погружении ДИ.

В каждый из выбранных P блоков погружается num_i при помощи устойчивого к атакам против встроенного сообщения стеганографического алгоритма, основой для которого послужил стеганоалгоритм, описанный в [11]: для каждого $Bl_k, k=\overline{1,P}$, строится сингулярное разложение

$$Bl_k = U\Sigma V^T, \tag{2}$$

где U,V - ортогональные $8\times 8-$матрицы, столбцы которых – левые и правые сингулярные векторы матрицы Bl_k соответственно, $\Sigma = diag(\sigma_1,..,\sigma_8)$, $\sigma_1 \ge \sigma_2 \ge ....\sigma_8 \ge 0$ - сингулярные числа. Погружение num_i происходит в сингулярные числа Bl_k в соответствии с формулой:

$$\sigma_1 = [\sigma_1 - \sigma_2/K]\cdot K + num_i + \sigma_2,\quad K = \max_i(num_i)+10,\quad K\in N,$$

где N — множество натуральных чисел.

Для обеспечения устойчивости предложенного стеганоалгоритма предлагается использовать числовые метки num_i с шагом 10 (если взять метки с меньшим шагом обеспечить устойчивость к возмущающим воздействиям будет крайне затруднительно). В практической части работы предлагается формировать метку подмножеств контейнеров из диапазона [0,50].

После внедрения ДИ в частотной области ЦИ-контейнера происходит возвращение в пространственную при помощи обратного дискретного преобразования Фурье (ОДПФ) для дальнейшей передачи изображения по каналу связи. ОДПФ будет происходить без округлений с учетом специфики формирования коэффициентов Фурье для блоков 2×2 благодаря предложенной организации погружения ДИ [7-9].

Декодирование. На этапе декодирования происходит выделение той составляющей $\overline{\overline{B}}$ цветного ЦИ-СС, в которую происходило погружение ДИ. В общем случае $B \neq \overline{\overline{B}}$.

Декодирование ДИ начинается с выделения метки подмножества контейнеров из $\overline{\overline{B}}$, которую обозначим далее $\overline{num_i}$, из P возможно измененных, а потому обозначаемых далее $\overline{Bl_k}$, $k=\overline{1,P}$, блоков, задействованных для пересылки num_i. В ходе этого для каждого блока $\overline{Bl_k}$ строится сингулярное разложение вида (2), в результате которого вычисляются его сингулярные числа $\overline{\sigma_1}^{(k)} \geq \overline{\sigma_2}^{(k)} \geq ....\overline{\sigma_8}^{(k)} \geq 0,\ k=\overline{1,P}$. Для извлечения метки $\overline{num_i}^{(k)}$ из блока $\overline{Bl_k}$, $k=\overline{1,P}$, необходимо проделать следующие шаги:

1. Вычислить значение $M = \left\lfloor \left(\overline{\sigma_1}^{(k)} - \overline{\sigma_2}^{(k)}\right) / K \right\rfloor$;
2. Из всех значений меток num_i, задействованных при формировании *MSP*, выбрать ближайшее к M. Положить $\overline{num_i}^{(k)} = M$.

В общем случае $\overline{num_i}^{(k)} \neq num_i$. В качестве $\overline{num_i}$ выбирается тот номер, который повторяется большее количество раз среди $\overline{num_i}^{(k)}$, $k=\overline{1,P}$.

Выделение ДИ будет происходить из частотных коэффициентов преобразования Фурье для непересекающихся блоков 2×2, полученных при помощи стандартного разбиения матрицы $\overline{\overline{B}}$. Из матрицы блока частотных коэффициентов ДПФ $\overline{F_{nm}}^{(\overline{\overline{B}})}(u,v),\ u,v=\overline{0,1}$ происходит выделение 1 элемента (возможно) возмущенной матрицы $\overline{P}^{j(K)}$. Для установления аутентичности/неаутентичности переданной ДИ проводится сравнение $\overline{P}^{j(K)}$ с ключом кодирования $\widetilde{K}_j$ или его инверсией, которые получаются по возможно возмущенному выделенному номеру $\overline{num_i}$ из множества стеганографических пар *MSP*, имеющихся у получателя. При таком сравнении ведется подсчет количества K1 совпадений матрицы $\overline{P}^{j(K)}$ с ключом кодирования $\widetilde{K}_j$ или его инверсией. С учетом полученного в [9] порогового значения A=87% для K1, проверка аутентичности ДИ в SM_3 проводится следующим образом:

если $K1 > 87\%$
то аутентичность дополнительной информации не нарушена
иначе аутентичность дополнительной информации нарушена.

В случае, когда аутентичность ДИ не нарушена, в SM_3 проводится двухэтапная проверка ее целостности аналогично тому, как это предложено в [8]. Для этого на первом этапе из бинарного представления каждого частотного коэффициента каждого блока $\overline{F_{nm}}^{(\overline{\overline{B}})}$, использованного при стеганопреобразовании, происходит выделение значения, которое стоит в использованной при погружении позиции pos (см. формулу

(1)). Если из различных элементов текущего блока $\overline{F}_{nm}{}^{(\overline{\overline{B}})}$ выделяются неодинаковые значения, то целостность ДИ нарушена. Второй этап осуществляет проверку принадлежности всех частотных коэффициентов множеству целых чисел:

если для $\overline{\overline{B}}$ существует блок $\overline{F}_{nm}{}^{(\overline{\overline{B}})}$, для которого среди его элементов $\overline{F}_{nm}{}^{(B)}(i,j),\ i,j=\overline{0,1},$ существует $\overline{F}_{nm}{}^{(B)}(i,j)\notin \mathrm{Z}$, где Z -множество целых чисел

то целостность передаваемой информации нарушена;

иначе целостность передаваемой информации не нарушена.

Декодирование очередного возможно возмущенного бита $\overline{p}_j$ ДИ из очередного блока СС осуществляется следующим образом:

если матрица $\overline{P}^{j(K)}$, удовлетворяет: $\overline{P}^{j(K)}=K_j$,

то $\overline{p}_j=0$.

если матрица $\overline{P}^{j(K)}$, удовлетворяет: $\overline{P}^{j(K)}=\overline{K_j}$,

то $\overline{p}_j=1$,

иначе пусть t_0 - количества совпадений между значениями соответствующих элементов матриц $\overline{P}^{j(K)}$ и K_j , а t_1 - количества совпадений между значениями соответствующих элементов матриц $\overline{P}^{j(K)}$ и $\overline{K}_j$.

если $t_0>t_1$,

то $\overline{p}_j=0$,

иначе $\overline{p}_j=1$.

Таким образом, преимуществом предлагаемого стеганографического метода является не только уменьшенный объем информации, который необходимо передавать по защищенному каналу связи, по сравнению с [8-9], но и то, что он является «слепым», не требующим исходного контейнера на этапе декодирования ДИ.

Результаты

Для апробации предложенного метода SM_3 предлагается реализующий его алгоритм, для которой используются следующие значения параметров:

1. Количество подмножеств контейнеров – *Kol*=5;
2. Количество блоков для погружения метки подмножества контейнеров — *P=5*;
3. Метки подмножеств контейнеров выбирались из множества $\{10,20,30,40,50\}$. Необходимо отметить, что при увеличении/уменьшении шага между значениями меток повышается/понижается устойчивость к возмущениям стеганоалгоритма, использованного для погружения метки контейнера. Предлагаемое множество используемых значений обеспечивает компромисс между устойчивостью упомянутого стеганоалгоритма и вероятностью обеспечения надежности восприятия формируемого СС;
4. Размер ключа кодирования $-\ R=4$.

Погружение метки подмножества контейнеров происходило в пять блоков контейнера размером 8×8, для которых все значения яркости пикселей находились в диапазоне [50;200], что обеспечивало невыход яркости пикселей СС за границы [0;255].

Непосредственное значение *P=5* выбиралось экспериментальным путем. Благодаря устойчивости стеганоалгоритма, использованного для погружения метки,

$P=5$ обеспечивает декодирование num_i даже при наложении возмущений на СС, которые приводят к нарушению его надежности восприятия (что нельзя утверждать для $P<5$). Таким образом, увеличение P, приводящее к уменьшению скрытой пропускной способности организуемого стеганографического канала связи, является нецелесообразным.

Для проверки эффективности реализующего стеганометод SM_3 алгоритма при указанных значениях параметров в среде Matlab был проведен вычислительный эксперимент, в котором задействовалось 300 ЦИ-контейнеров. В результате эксперимента ошибки первого и второго рода выявлены не были.

Выводы

В работе предлагается усовершенствование уникального стеганографического метода, решающего одновременно актуальную на сегодня триединую задачу стеганографии, включающую в себя одновременную организацию передачу конфиденциальных данных, проверку их аутентичности и целостности.

Предложенная модификация имеет ряд преимуществ по сравнению с методом, разработанным в [8-9]: уменьшенный объем информации, необходимо передаваемой по защищенному каналу связи; SM_3 является «слепым» стеганометодом.

Результаты вычислительных экспериментов подтверждают высокую эффективность усовершенствованного метода SM_3.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2009. – 272 с.
2. Конахович, Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
3. Кобозєва, А. А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К.: Вид. ДУІКТ, 2010. – 316 с.
4. Глумов, Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – т.35, №2. – С.262-267.
5. Кобозева, А. А. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера / А.А. Кобозева, А.Д. Шовкун // Науковий вісник Міжнародного гуманітарного університету. – 2012. – №4. – С. 21-28.
6. Ghoshal, N. A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT) / N. Ghoshal, J.K. Mandal // Malaysian Journal of Computer Science. – 2008/ – Vol. 21, No. 1. – PP. 24-32.
7. Козина, М. А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации / М.А. Козина // Сучасна спеціальна техніка. – 2014. – №4(39). – С. 98-106.
8. Кобозева, А.А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А.А. Кобозева, М.А. Козина. // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. – №3 (26). – С. 93-106.
9. Козіна, М.О. Метод перевірки автентичності інформації, що передається стеганографічний каналом зв'язку / М.О. Козіна. // Вісник Вінницького політехнічного інституту. – 2015. – №1. – С. 99-104.
10. Kozina, M.O. Discrete Fourier transform as a basis for steganography method / M.O. Kozina // Праці Одеського політехнічного університету. – 2014. – Вип.2(44). – С.118-126.
11. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – No2(8). – С. 99–106.

МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ, ЯКИЙ ЗАБЕЗПЕЧУЄ ПЕРЕВІРКУ ІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ

А.А. Кобозєва, М.О. Козіна

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

У роботі пропонується вдосконалення раніше розробленого автором стеганографічного методу, який вирішує одночасно актуальну на сьогодні триєдину задачу стеганографії: прихованої передачі даних, перевірки їх автентичності та цілісності. В якості контейнера використовується цифрове кольорове зображення, а в якості додаткової інформації виступає довільним чином сформована бінарна послідовність. Удосконалення стеганографічного методу включає в себе: зменшення обсягу необхідно переданої інформації по захищеному каналу зв'язку для організації автентифікації даних; забезпечення можливості декодування переданої інформації без наявності контейнера. Наведено результати обчислювальних експериментів, що підтверджують високу ефективність запропонованого методу.
Ключові слова: стеганографічний метод, прихований канал зв'язку, цілісність, автентичність, дискретне перетворення Фур'є, цифрове зображення.

HIDDEN DATA TRANSMISSION METHOD THAT PROVIDES VERIFY THE INTEGRITY AND AUTHENTICITY OF TRANSMITTED INFORMATION

A.Kobozeva, M. Kozina

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

In this work it is proposed the previously developed steganographic method, which solves both actual today triune task steganography: to hide data, verify their authenticity and integrity. As a container used digital color image, as an additional information acts randomly generated binary sequence. Improving steganographic method includes: reduction of transmitted information necessary to secure a communication channel for the organization authentication data; to be able to decode the transmitted information without container. The results of computational experiments confirming the high efficiency of the proposed method.
Keywords: steganography method, hidden communication channel, integrity, authenticity, discrete Fourier transform, a digital image.

УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 65-70

СТВОРЕННЯ ВДОСКОНАЛЕНОГО ПЛАГІНА ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ІНТЕРНЕТ–МАГАЗИНУ НА ПЛАТФОРМІ WORD PRESS

М.О. Мельник, А.Р. Агаджанян, Я.Г. Маховська

Одеський національний політехнічний університет
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: ritochek@ya.ru

В роботі шляхом дослідження різних платформ для створення інтернет – магазинів, була вибрана найпоширеніша, аналіз якої проводився за наступними факторами: популярність, розмір співтовариства користувачів і розробників, зручність адміністрування, технічна підтримка. Був проведений аналіз недоліків існуючих засобів для організації захисту інформації даних обраної платформи. Розроблений скомпільований програмний модуль для захисту даних в інтернет - магазинах, створених на обраній платформі.

Ключові слова: інтернет – магазин, скомпільований програмний модуль, плагін, Word Press, концепція безпеки в електронних магазинах, система управління вмістом (CMS).

Вступ

Поширення з великою швидкістю інтернет–магазинів (електронних магазинів) в наш час є невід`ємною частиною суспільства. Одною із складових електронної комерції є технічні рішення, тобто системи управління сайтом. Їх можна розділити на системи управління вмістом (CMS) і програми для просування, ведення, моніторингу та аналізу статистики [1]. Ринок технічних рішень для електронної комерції досить різноманітний, тому в роботі ми спробували сконцентруватися на основних функціональних можливостях існуючих платформ, які необхідні на сьогоднішній день для ефективного ведення процесів, пов'язаних з технічною стороною захисту інформації.

Не втрачають своєї актуальності проблеми безпеки електронних магазинів. Кожен рік відкриваються тисячі таких магазинів, але 85% існують менше року [1]. Така статистика пов`язана не тільки зі складним економічним становищем, а й з питаннями безпеки інформації: низьким рівнем стандартної розробки, відсутністю єдиної концепції безпеки, використанням декількох акаунтів для одного користувача та ін.

Необхідно звернути увагу на те, що при зміні стандартних налаштувань JavaScript додаткові розширення можуть не працювати. Такі проблеми можуть виникнути, якщо підключити JS-скрипт у файлі шаблону, а потім використовувати плагін, якому потрібен цей же скрипт. Таким чином порушується логіка підключення, і плагін не буде функціонувати. Найчастіше таке відбувається з JavaScript-бібліотеками, наприклад, з підключенням jQuery.

Не слід забувати, що у більшості випадків розробники плагінів не мають доступу до файлів шаблону, створеному на платформі WP. Разом з тим розробники повинні гарантувати можливість підключення необхідних скриптів, тому для них одним з кращих варіантом буде використання функція wp_enqueue_script. Ця функція підключає JS-файл, якщо він не був підключений раніше, її можна викликати кілька разів для одного і того ж скрипта і при цьому скрипт буде вставлений тільки один раз.

Мета статті та постановка досліджень

Метою роботи є аналіз рівня інформаційної безпеки сучасних CMS для електронного магазину, аналіз існуючих засобів захисту та організація захисту даних в електронному магазині, виявлення недоліків та запропонування шляху вдосконалення захисту.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Провести аналіз платформ, які найбільш використовуються для створення інтернет-магазинів; вибрати найпоширенішу за наступними факторами: популярність, зручність адміністрування, технічна підтримка;
2. Провести аналіз існуючих засобів для організації захисту інформації даних обраної для створення інтернет-магазинів платформи;
3. Розробити програмний модуль для захисту даних в інтернет-магазинах, створених на обраній платформі.

Основна частина

Аналіз платформ, які найчастіше використовуються для створення інтернет-магазинів, показав, що найпоширинішею є платформа WordPress. Подальші дослідження в роботі будуть пов'язані з WordPress у зв'язку з її популярністю, зручністю адміністрування, великим співтовариством користувачів і розробників. Крім того, одною з вагомих переваг є її легка адаптація до пошукових алгоритмах, що є важливим для подальшого просування електронного магазину [2].

Для рішення означених в роботі задач важливим є наступне твердження [3]:

Твердження 1. Своєчасно поновлювані версії CMS знижують ризик появи проблем з захистом інформації в середньому в два рази.

Аналіз існуючих програмних модулів (плагінів) для захисту зображень і текстового контенту показав, що до недоліків тут можна віднести наступне [4]:

1. Розширений функціонал пропонується у більшості плагінів тільки в платних версіях;
2. Більшість плагінів несумісні з новою версією WP.

Було прийнято рішення по створенню власного плагіна з назвою WP-Copy-Protection-System, який буде повністю безкоштовним і включатиме в себе максимальну кількість функцій для захисту інформації сайту. Плагін можна встановити двома способами: використовуючи адміністративну панель магазину, за допомогою FTP-клієнта (завантажуємо плагін у папку 0:/www/ваш_сайт/wp-content/plugins/ (рис. 1)).

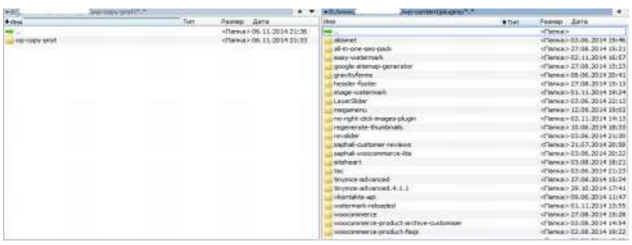


Рис. 1. Початок завантаження плагіна

Після завантаження плагін необхідно активувати (рис. 2). Наступним кроком є його налаштування. Для цього в меню адміністратора знаходяться панелі «Налаштування» і вибирається плагін WP-Copy-Protection-System.

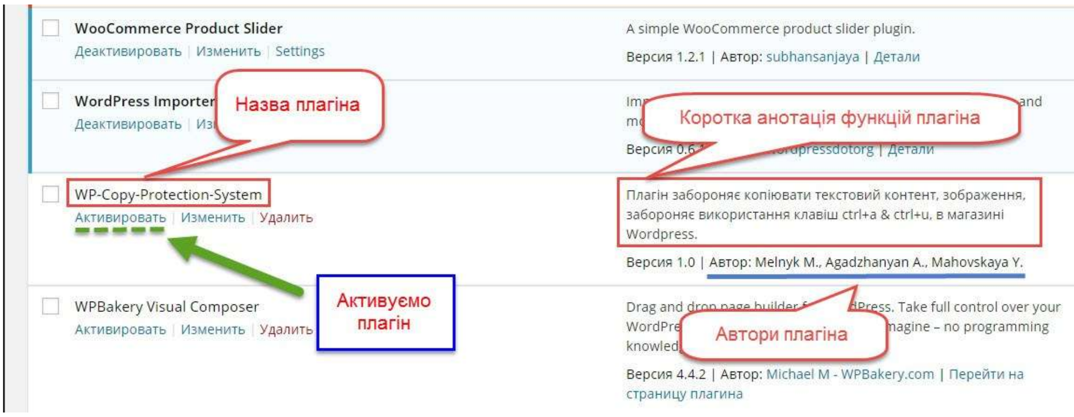
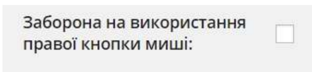
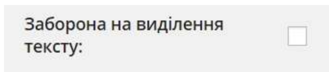


Рис. 2. Активізація плагіна

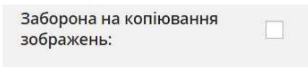
Переходимо безпосередньо до налаштувань самого плагіна. Використання правої кнопки миші для копіювання текста дуже розповсюджене. Наступна опція забороняє використовувати праву кнопку миші в інтернет-магазині, на сайті. Використовуючи дану опцію, можна зменшити кількість вкраденої інформації з інтернет-магазину шляхом простого виділення і копіювання через праву кнопку миші (рис. 3, а).



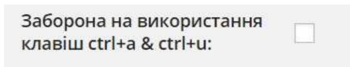
а



б



в



г

Рис. 3. Опції, що використовуються для захисту інформації: а – заборона налаштування правої кнопки миші; б – заборона виділення тексту; в – заборона копіювання фото (малюнків); г – заборона використання клавіш ctrl+a & ctrl+u

Опції «Заборона виділення тексту» (рис. 3, б) дуже важлива для захисту інтернет-магазину від копіювання контенту. Адже для того, щоб магазин постійно збільшував кількість відвідувачів, які в тій чи іншій кількості перетворюються на покупців, необхідно нарощувати саме текстовий контент з унікальністю 97-100%, правильно його оформляти, розробити семантичне ядро і розставити в тексті ключеві слова, за допомогою яких робот пошукової системи проаналізує сторінки магазину і занесе їх в базу. Як показує практика, чим унікальніший і цікавіший текст, що містить ключові слова, тим вищий рейтинг у магазина. Саме тому дуже важливо захищати свій контент від копіювання.

Кожен інтернет-магазин намагається продавати товар, використовуючи власні фото. Дуже часто для отримання якісних фото запрошують професійного фотографа, якій правильно виставляє освітлення, кути огляду того чи іншого товару, робить багато знімків, для того, щоб їх потім відсортувати і поставити як зображення товару в інтернет-магазині. І тому дуже важливо, щоб отримані такою важкою працею фото, залишились тільки у власника магазина на сайті, а не стали кращими зображеннями конкурентів. Тому рекомендується захищати зображення від копіювання за допомогою опції «Заборона копіювання зображень» (рис. 3, в).

Заборона використання клавіш ctrl+a & ctrl+u – ще одна потрібна опція (рис. 3, г): заборона виділення за допомогою клавіш ctrl+a всього змісту сторінки; невикористання комбінації ctrl+u дає можливість заборонити перегляд коду сторінки, тобто не дає можливості переглянути, на якій CMS працює інтернет-магазин, які скрипти в його роботі використовуються, які плагіни, як прописані метатеги і т.і. Використання блокування перегляду коду сторінки створює додатковий захист для інтернет-магазину.

Опція «Додавання адреси першоджерела до скопійованого тексту» (якщо функція заборони виділення тексту вимкнена) важлива для захисту текстового контенту. Під час використання даної функції до скопійованого тексту автоматично додається посилання на першоджерело. Таким чином, скопіювавши матеріал і розмістивши цей матеріал на сторонньому магазині (сайті), ми отримаємо зворотнє посилання на свій магазин, що буде добре для пошукової оптимізації. Звісно, уважно перечитавши текст, посилання можна знайти і видалити, але, як показує практика, близько 40% користувачів не видаляє таких посилань. Тому і цей метод захисту контенту може бути корисним. Слід зауважити, що для активування даної функції необхідно, щоб функція «Заборона виділення тексту» була деактивована (рис. 4).

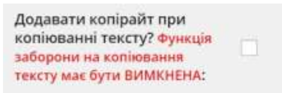


Рис. 4. Додавання адреси першоджерела до скопійованого тексту

Наступна опція розміщення повідомлення про заборону копіювання контенту носить інформаційний характер. Її активація дозволяє проінформувати відвідувачів інтернет-магазину, що використовується плагін, який захищає текстовий контент і зображення. В налаштуваннях може вказуватися будь-який текст. Дана опція підтримується html (рис. 5).

Рис. 5. Налаштування повідомлення про заборону копіювання контенту

Приклад використання даної функції в роботі інтернет-магазину представлений на (рис. 6).

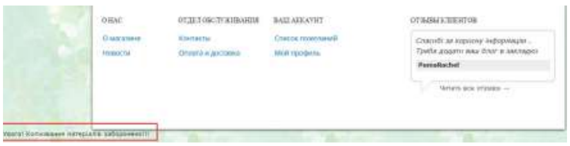


Рис. 6. Приклад роботи налаштування повідомлення про заборону копіювання контенту

Після завершення налаштувань натискається кнопка «Зберегти» (рис.7).

Рис. 7. Правильне завершення налаштувань плагіна

Після вірного налаштування, плагін використовує усі заявлені функціональні можливості.

Висновки

В результаті роботи було зроблено наступне:

1. Проведений аналіз платформ, які найчастіше використовуються для створення інтернет-магазинів. Вибрана найпоширеніша платформа за наступними факторами: популярність, зручність адміністрування, технічна підтримка;
2. Проведений аналіз існуючих засобів для організації захисту інформації даних обраної платформи для створення інтернет-магазинів. Зроблений аналіз недоліків існуючих засобів.
3. Розроблений плагін для захисту даних в інтернет-магазинах, створених на обраній платформі.

Розроблений пагін має переваги: він включає всі функції розроблених раніше розширень, але, на відміну від них, плагін синхронізований до нової версії WP.

Розроблений плагін був протестований на двох інтернет-магазинах. Робота плагіна відповідає заявленим потребам захисту інформації в інтернет-магазині. Всі заявлені функції підключені та працюють. Передумовою для роботи плагіну має бути включений JavaScript в браузерах користувачів. При відключеному JavaScript сайт не повинен працювати взагалі:

```
<noscript>
  <style>
body{display:none;}
  </style>
</noscript>.
```

Наступним кроком авторів є розробка загальної концепції безпеки, ліквідація існуючих слабких місць (наприклад, таких, як вхід в адміністративну панель). Крім того, ще раз звернемо увагу на те, що при зміні стандартних налаштувань JavaScript додаткові розширення можуть не працювати. Найчастіше таке відбувається з JavaScript-бібліотеками, наприклад, з підключенням jQuery. Актуальність підключення бібліотек до обновлених версій WP є безумовною. Розв`язання цього питання буде обов`язково розглянуто в наступних роботах авторів.

Список літератури

1. Орлов, Л.В. Как создать электронный магазин в Интернет / Л.В. Орлов. – М: Бук пресс, 2006. – 384 с.
2. Мельник, М.А. Цикл поисковой оптимизации как основа поисковой оптимизации электронных магазинов / М.А. Мельник, А.С. Ганенко // Інфокомунікації – сучасність та майбутнє: матеріали четвертої міжнародної наук.-пр. конф., м. Одеса 30-31 жовт. – 2014. – Ч.4. – С 116-117.
3. Алексунин, В Электронная Коммерция и маркетинг в Интернете / В. Алексунин, В. Родигин. – М: Дашков и Ко, 2009. – 216 с.
4. WorldPress.org [Електроний ресурс]. Режим доступу: http://wordpress.org

СОЗДАНИЕ УСОВЕРШЕНСТВОВАННОГО ПЛАГИНА ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ ИНТЕРНЕТ – МАГАЗИНА НА ПЛАТФОРМЕ WORD PRESS

Мельник М.О., Агаджанян А.Р., Маховская Я.Г.

Одесский национальный политехнический университет
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: ritochek@ya.ru

В работе путем анализа наиболее популярных платформ для создания интернет - магазинов, была выбрана самая распространённая. Анализ наиболее распространённой платформы, проводился путём рассмотрения следующих факторов, таких как популярность платформы, размер сообщества пользователей и разработчиков, удобство администрирования, техническая поддержка. Был проведен анализ существующих средств для организации защиты информации данных, рассматриваемой платформы. Проведен анализ недостатков предлагаемых средств. Разработан скомпилированный программный модуль для защиты данных в интернет - магазинах, созданных на выбранной платформе.

Ключевые слова: интернет - магазин, скомпилированный программный модуль, плагин, Word Press, концепция безопасности в электронных магазинах, система управления содержимым (CMS).

DEVELOPMENT MORE COMPLETE PLUGIN FOR INFORMATION PROTECTION FOR THE ONLINE SHOPS BASED ON THE PLATFORM WORD PRESS

Melnyk M., Agadzhanyan A., Mahovska Y.

Odessa National Polytechnic University
1 Shevchenko Str., Odessa, 65044, Ukraine; e-mail: ritochek@ya.ru

In this paper, by analyzing the most popular platforms for develop online - shops, was selected the most common. The analyze of the most common platforms, conducted by considering the following factors, such as the popularity of the platform, the size of the community of users and developers, ease of administration, technical support. By analyzing the shortcomings were found existing tools to protect information. Develop more complete plugin for information protection for the online shops based on the platform WordPress (WP).

Keywords: online shop, plugin, WordPress, the concept of security in e-shops, content management system (CMS).

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp.71-76

USING CIRCULAR BLOCKS FOR DETECTION OF FORGED REGIONS IN DIGITAL IMAGES

E. Lebedeva

Odessa National Polytechnic University
1 Shevchenko Str., Odessa, 65044, Ukraine; e-mail: whiteswanhl@yahoo.com

In this work, the use of circular blocks for the detection and location of cloned regions was investigated to improve the detection accuracy. The procedure to develop circular and sector blocks in a digital image was presented. The modified method developed for the detection and location of cloned regions allows locating a cloned region with the use of circular blocks in a more accurate way.

Keywords: digital image forgery, forgery detection, cloning, circular block

Introduction

Widespread use of modern digital cameras and digital image (DI) processing software (such as Adobe Photoshop and GIMP) has lead to the emergence of image forgery hardly detectable to the human eye. Since the tools of these graphic editors are rather easy to use, the number of image forgeries has been increasing day by day. Digital images are of primary importance in cyberspace and are used in the printed media, medicine, science, forensic proceedings, etc. It is essential not only to detect forged regions, but to determine their borders as accurately as possible. Therefore, solving the problem of accurate detection of forged regions in digital images is an *urgent* issue.

Statement of the problem and purpose of the study

In this paper, we discuss cloning, one of the commonest methods used for digital image forgery. In cloning, parts of the DI are changed with parts of the same image.

Implementation of this approach with graphics editors such as Adobe Photoshop and GIMP generally involves the use of specific tools (*Rectangular Marquee Tool*, *Lasso Tool*, *Eraser Tool*, etc.). The tools mentioned make it possible to create a cloned region of an irregular shape.

In [1, 2], a method has been developed to detect and locate cloned regions using standard blocks. For the purpose of methodology, a standard block means a square-shape block of any size. Investigations performed with that method revealed that the 8 x 8 block has the most favorable size among standard blocks. However, the results of the experiments have shown that the use of standard blocks does not allow for proper accuracy in the size and location (shape) of the detected forged regions.

To detect cloned regions more accurately, one should use the blocks of non-standard shape.

The *Purpose* of the study was to investigate the potential for the use of circular blocks in DI, and to develop a modification of the method for the detection and location of cloned regions using circular blocks in order to improve the detection accuracy.

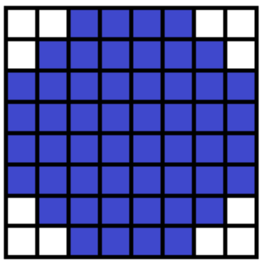
The detection accuracy was assessed by the percentage ratio of the area of detected cloned region to the actual area of cloned region. The actual area of cloned region was determined as the difference between the original image and the forged image. The area was measured in pixels.

To accomplish the purpose of the work, the following problems were to be solved:

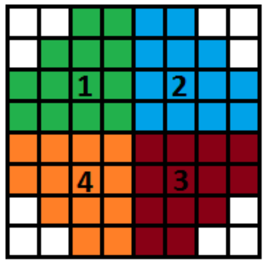
1. To elaborate the procedure of obtaining circular blocks;
2. To modify the method for the detection and location of cloned regions in order to use circular blocks;
3. To use computational experiments to conclude whether it is expedient to use circular blocks.

Procedure of obtaining circular blocks

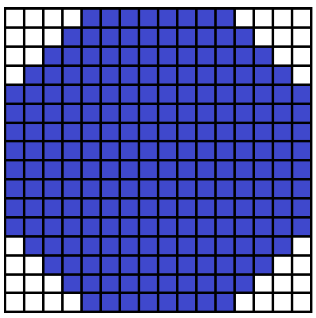
Let us address the development of a circular block based on a square-shaped block (Fig.1)



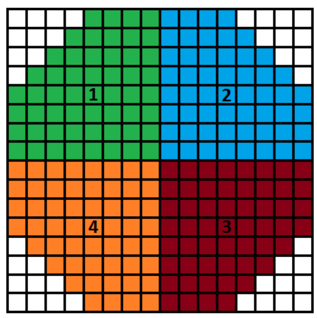
a



b



c



d

Figure 1. Decomposition of a square-shaped block into: a – round 8x8 block; b – sectors of a round 8x8 block; c – round 16x16 block; d – sectors of a round 16x16 block

The brightness matrix S of a square-shaped DI block will be used as a basic one. The brightness matrix L of a circular block is formed from the brightness values of marked pixels (Fig. 1 a, c) of matrix S, whereas the values of non-marked pixels are zeroed. Aside from a circular block, one can obtain sector-shaped blocks (Fig. 1 b, d). In this case, we will get four sector matrices L_1, L_2, L_3, L_4 to be filled in a similar way, i.e., e.g., matrix L_1 will contain the values of pixels of matrix S located in zone 1 (Fig. 1 b, d), whereas the values of other pixels are zeroed.

Method for the detection and location of cloned regions using circular blocks

Let us modify the basic method in order to use circular blocks for the detection and location of cloned regions.

Briefly, the procedure of the method for the detection and location of cloned regions in a DI using circular blocks is as follows.

1. Divide the brightness matrix Y of a DI into $p \times p$ overlapping blocks $C = \{c_1, c_2, \ldots, c_s\}$, $\bigcup_{i=1}^{s} c_i = Y$, (here each block c_i is obtained by a single-pixel right shift, left shift, down-shift or up-shift of block c_{i-1}).

2. For a block pair considered, c_i, c_j, $i = 1, \ldots, s$, $j = i+1, \ldots, s$ obtain circular subdivision blocks $c_i^{'}$ and $c_j^{'}$, respectively. For each subdivision:

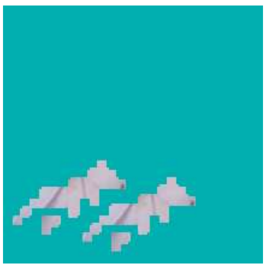
3. Calculate the correlation coefficient $\delta = Correlation(c_i', c_j')$.

4. Analyze the value of correlation coefficient δ to determine pairs of blocks $c_i^{'}$ and $c_j^{'}$ suspected for belonging to cloned regions and to a clone prototype.

Fig. 2 shows a sample of application of the modification method developed for the detection and location of cloned regions.

a

b



c

d

Figure 2. Results of the application of the modification method for the detection and location of cloned regions using the blocks of circular shape: a – original image, b – forged image, c – result of the detection using 8x8 square-shape blocks, d – result of the detection using 8x8 circular-shape blocks

To improve the accuracy of detection of clone borders, let us use not only circular blocks, but also sector-shaped blocks (Fig. 1 b, d) within the process. In this case, briefly, the procedure of the method for the detection and location of cloned regions in a DI using circular blocks is as follows.

1. Divide the brightness matrix Y of a DI into $p \times p$ overlapping blocks $C = \{c_1, c_2, \dots, c_s\}$, $\bigcup_{i=1}^{s} c_i = Y$, (here each block c_i is obtained by a single-pixel right shift, left shift, down-shift or up-shift of block c_{i-1}).

2. For a block pair considered, c_i, c_j, $i = 1, \dots, s$, $j = i+1, \dots, s$ obtain circular subdivision blocks $c_i^{'}$ and $c_j^{'}$, respectively. For each subdivision:

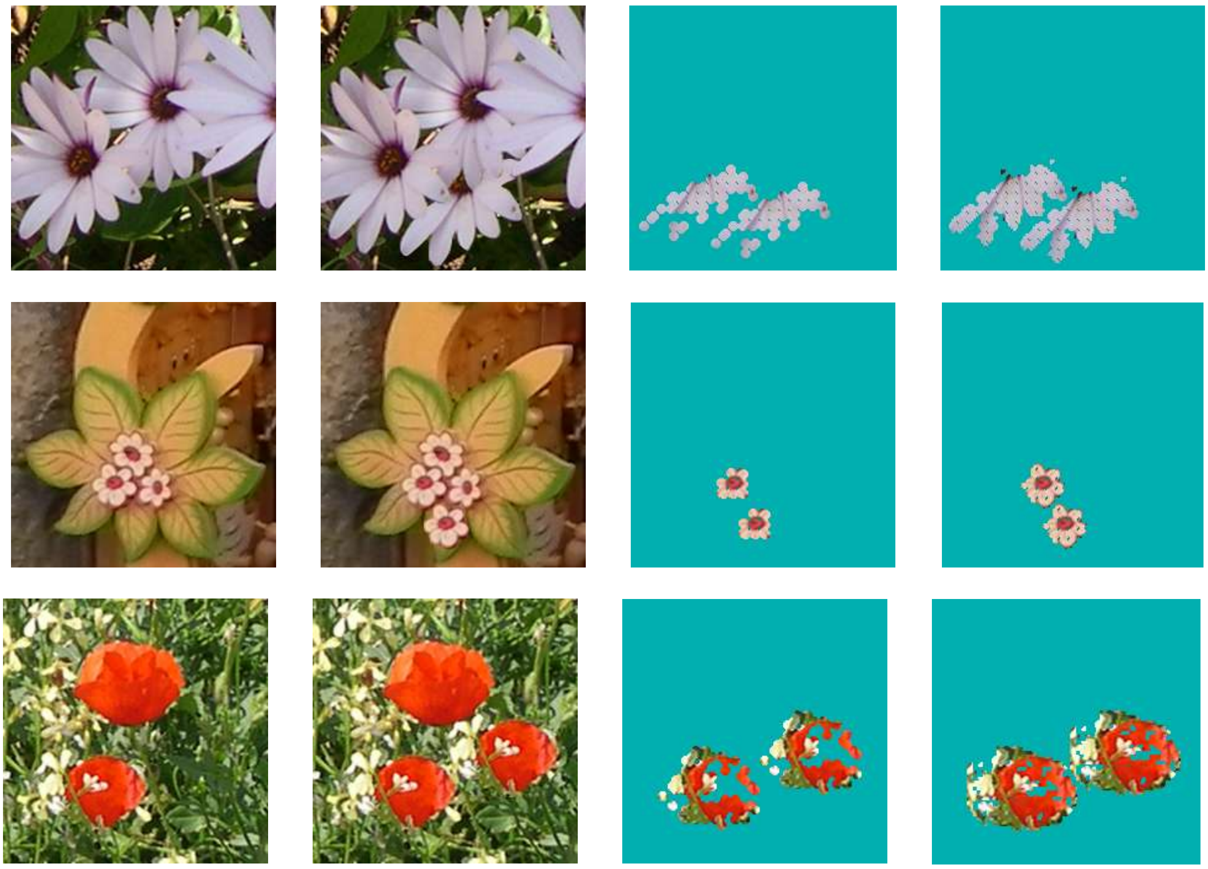
2.1. Calculate the correlation coefficient $\delta' = Correlation(c_i', c_j')$

2.2 Analyze the value of correlation coefficient δ' to determine pairs of blocks $c_i^{'}$ and $c_j^{'}$ suspected for belonging to cloned regions and to a clone prototype. If the suspected blocks are not found, obtain sector-shaped blocks c_i^k and c_j^k, $k = 1, \dots, 4$. For each subdivision:

2.2.1 Calculate the correlation coefficient $\delta^k = Correlation(c_i^k, c_j^k)$

2.2.2 Analyze the value of correlation coefficient δ^k to determine pairs of blocks c_i^k and c_j^k suspected for belonging to cloned regions and to a clone prototype.

Fig. 3 shows a sample of application of the modification method developed for the detection and location of cloned regions using circular and sector-shaped blocks.



a **b** **c** **d**

Figure 3. Results of the application of the modification method for the detection and location of cloned regions using circular and sector-shaped blocks: a – original image, b – forged image, c – result of the detection using circular-shaped blocks, d – result of the detection using circular and sector-shaped blocks

The use of circular and sector-shaped blocks for the detection and location of cloned regions allowed increasing the detectable area of cloned region, as compared to the use of circular blocks only. E.g., regarding the images presented at Fig.3, the ratio of area of detected cloned region to actual area of cloned region increased 1.34, 1.57, and 1.47 times, as compared to the use of circular blocks only.

Hereinafter, by "using circular blocks" we mean "using circular and sector-shaped blocks".

A computational experiment was performed to analyze the efficiency of the method developed for the detection and location of cloned regions using circular blocks based on the accuracy of detection of cloned regions. Within the experiment, the size of a cloned region was arbitrarily selected depending on the specific image, and irrespective of the size of subdivision blocks used in experiments. The cloned region boundary was subjected to blurring to get the improved visual embedding into the image. After application of cloning technology, the forged digital image obtained was saved using lossless format. The results of the experiments are presented in Tables 1 and 2.

Table 1.

Accuracy of the detection of a cloned region with blurred boundaries using the square-shaped and circular blocks

Types of subdivision	Percentage ratios of area of detected cloned region to actual area of cloned region		
	Max	Min	Average
Blocks of square shape	69.17	32.13	47.51
Blocks of circular shape	74.69	49.66	63.42

Table 2.

Evaluation of the accuracy of the cloned region detection with the method developed by means of a relative mean error of the area of detected cloned regions

Types of subdivision	Relative mean error of the area value (%)
Blocks of square shape	52.49
Blocks of circular shape	36.58

Conclusions

A procedure was developed to obtain circular blocks based on a square-shaped block of the DI matrix. A method for the detection and location of cloned regions was modified in order to use circular blocks. A computational experiment was performed to analyze the efficiency of the method developed for the detection and location of cloned regions using circular blocks based on the accuracy of detection of cloned regions. The experiment showed that the ratio of area of detected cloned region to actual area of cloned region increases more than 1.3 times, and relative mean error of the area value decreases 1.44 times, as compared to the use of square-shaped blocks. The results obtained prove that it is expedient to use circular blocks for the detection and location of cloned regions.

References

1. Лебедева, Е.Ю. Исследование метрик используемых при обнаружении клонированных участков изображений в задачах выявления фальсификации / Е.Ю. Лебедева, Ю.Ф. Лебедев // Вісник національного технічного університету «ХПІ». – 2011. – №35. – С.25–31.
2. Лебедева, Е.Ю. Обнаружение клонированных участков изображений в задачах выявления фальсификации / Е.Ю. Лебедева // Труды XII международной научно-практической конференции «Современные информационные и электронные технологии». – 2011. – С. 175.

ВИКОРИСТАННЯ КРУГЛИХ БЛОКІВ ДЛЯ ВИЯВЛЕННЯ ОБЛАСТІ ФАЛЬСИФІКАЦІЇ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

О. Ю. Лебедєва

Одеський національний політехнічний університет
пр. Шевченко, 1, Одеса, 65044, Україна; e-mail: whiteswanhl@yahoo.com

У статті досліджується використання круглих блоків при виявленні та локалізації областей клонування для підвищення точності виявлення клонованих областей. Наводиться методика побудови круглих і секторних блоків у цифрових зображеннях. Розроблена модифікація методу виявлення та локалізації областей клонування, що дозволяє більш точно локалізувати клоновану область з використанням круглих блоків.

Ключові слова: фальсифікація зображень, виявлення фальсифікації, клонування, круглий блок.

ИСПОЛЬЗОВАНИЕ КРУГЛЫХ БЛОКОВ ДЛЯ ВЫЯВЛЕНИЯ ОБЛАСТИ ФАЛЬСИФИКАЦИИ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

Е. Ю. Лебедева

Одесский национальный политехнический университет
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: whiteswanhl@yahoo.com

В статье исследуется использование круглых блоков при обнаружении и локализации областей клонирования для повышения точности обнаружения клонированных областей. Приводится методика построения круглых и секторных блоков в цифровых изображениях. Разработана модификация метода обнаружения и локализации областей клонирования, что позволяет более точно локализовать клонированную область с использованием круглых блоков

Ключевые слова: фальсификация изображений, обнаружения фальсификации, клонирование, круглый блок.

УДК 519.81

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 77-83

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ПРИ ФОРМУВАННІ ПРОГРАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: МОДЕЛІ ЗАГРОЗ І РИЗИКІВ

С.В. Зибін, В.О. Хорошко

Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03680, Україна; e-mail: professor_va@ukr.net

Пропонується підхід до підтримки прийняття рішень для формування комплексних, цільових програм інформаційної безпеки держави при наявності загроз і ризиків, який базується на введенні моделей загроз і ризиків в ієрархію цілей програм (задач) і її цільової оцінки. Модель ризику має фактор ризику, який являється випадковим процесом і має спеціальну ціль. Загроза моделюється спеціальною програмою, яка вводиться в ієрархію цілей.

Ключові слова: підтримка прийняття рішень, моделі загроз і ризиків, інформаційна безпека, ієрархія цілей, цільова оцінка.

Вступ

Комплексна програма забезпечення інформаційної безпеки держави (ПІБД) являє собою сукупність заходів, які об'єднані єдністю глобальної мети й загальними ресурсами [1, 2]. Основні завдання розробки складних ПІБД – відбір програм, що входять в комплексну програму, й розподіл між ними ресурсів. При цьому ПІБД, як правило, може плануватися на великі проміжки часу, тому необхідно оцінювати ефективність програм на заданому інтервалі часу.

При розробці ПІБД слід враховувати можливість виникнення загроз і ризиків, аналізувати їхній вплив і на цій основі передбачати заходи щодо протидії їм або усунення їх. При формуванні ПІБД із урахуванням загроз і ризиків необхідно розв'язувати наступні задачі:

1. Визначення кількісних характеристик впливу загроз і ризиків на ефективність ПІБД;
2. Визначення кількісних показників ефективності програм при наявності загроз і ризиків;
3. Розподіл ресурсів між засобами протидії загрозам і ризикам та програмами, що мають спрямованість на підвищення інформаційної безпеки держави.

Відомі методи розв'язання першої задачі передбачають ідентифікацію ризиків (якісний аналіз), а також оцінювання ймовірностей і розмірів можливого збитку (кількісний аналіз) [3, 4]. Однак при цьому задача оцінки ефективності програм з врахуванням ризиків не вирішується й залишається на розсуд експерта – особи, що приймає рішення (ОПР). Більше того, визначення збитку в абсолютному вимірюванні часто неможливо для складних ПІБД.

Ціль роботи

У роботі пропонуються методи рішення задач ПІБД. Робота складається із двох частин. У першій частині викладається сутність запропонованого підходу й моделі загроз і ризиків, а в другій – методи обчислення кількісних показників відносної ефективності програм ІБД в умовах загроз і ризиків, напрямків виконання ПІБД із урахуванням загроз і ризиків; відносної ефективності заданої множини: загроз і ризиків, засобів протидії загрозам і ризикам.

Основна частина

Метод рішення задачі оцінки відносної ефективності програм при наявності загроз і ризиків природно розробляти на основі методів рішення даної задачі без обліку цих факторів. Найбільше розповсюдження сьогодні одержали мультикритеріальні методи оцінки програм [5]. Галузь їх застосування обмежується двома умовами, яким повинна задовольняти конкретна задача.

Перша умова – наявність множини критеріїв, по кожному з яких можна оцінити окрему альтернативу.

Друга умова – здатність ОПР оцінити тим або іншим способом кожну альтернативу за окремим критерієм.

Перша умова в більшості випадків формування складних ПІБД не виконується через істотну різницю природи програм, що входять у них. Виконання другої умови являється досить проблематичною, коли вибір найбільш оптимального варіанта з декількох або ранжирування такої кількості варіантів вимагає обліку їх оцінок по декільком десяткам взаємозалежних критеріїв. Така ситуація має місце при прийнятті рішень по формуванню складних ПІБД.

Тому методи підтримки прийнять рішень при формуванні ПІБД в умовах загроз і ризиків можна розробляти шляхом модифікації методів цільового оцінювання варіантів [1, 2, 5]. При підтримці рішень по розробці ПІБД відносна ефективність програм повинна оцінюватися як функція часу, задана на інтервалі планування [3]. Тому можливість обліку фактору часу при оцінці програм ІБД принципова для розв'язання задач підтримки рішень такого роду.

Основна ідея запропонованого підходу до аналізу впливу загроз і ризиків при виконанні ПІБД полягає в тому, що події, які спричиняють загрози або ризики, розглядаються як складова частина ПІБД, тобто програми впливу зовнішнього середовища. Тому такі програми-моделі загроз або ризиків включаються в ієрархію цілей ПІБД [6], встановлюються їхні зв'язки з іншими програмами й цілями ПІБД. Таким чином, кожна із програм-моделей загроз або ризиків має хоча б одну ціль або програму, на досягнення якої (ступінь виконання якої) вона безпосередньо впливає. Виходячи із [6], визначимо такі цілі (програми) безпосередніми надцілями програми-моделі загрози або ризику. При цьому вплив загрози й/або ризику, як і інших програм ПІБД, оцінюється ступенем впливу на досягнення головної цілі програми. Ефективність програми ІБД оцінюється за умови наявності загроз і ризиків з врахуванням їх ймовірнісних характеристик. Такий підхід дає можливість розподілити ресурси на відбивання загроз і ризиків нарівні з розподілом ресурсів на програми, що складають сутність ПІБД.

Для реалізації запропонованого підходу необхідно вирішити ряд часткових задач. Перша пов'язана з розробкою математичних моделей загроз і ризиків, що дозволяють включати події, які спричиняють загрозу й/або ризик, в ієрархію цілей ПІБД. Сутність другої задачі полягає в розробці методу кількісного оцінювання впливу загрози й/або ризику. Наступна задача – пошук способу оцінки відносної ефективності програми ІБД при наявності загроз і ризиків.

Аналіз, який визначає загрози дозволяє виявити деякі властивості, що характеризують це поняття. По-перше, слід зазначити, що загроза – це наслідок події, що полягає у виникненні ситуації, яка впливає на виконання ПІБД. Однак загроза являється результатом діяльності певних груп людей на відміну від ризику, який в основному являється наслідком випадкової події. По-друге, інтенсивність впливу загрози на виконання задач ПІБД – це випадкова величина, що змінюється із часом.

Загальним для понять "загроза" і "ризик" є вплив зовнішнього середовища на виконання ПІБД і те, що вони являються наслідком її впливу на виконання ПІБД.

На підставі проведених досліджень сформулюємо визначення.

Визначення 1. Загроза є стан середовища, що впливає на ефективність задач ПІБД, у якому виконується комплексна цільова програма.

Крім того, можна зробити висновок про існування засобів нейтралізації загрози, які впливають на рівень її небезпеки.

Із цього випливає можливість побудови моделі загрози, яка являє собою деяку задачу ПІБД, причому існує хоча б одна задача або ціль, рівень досягнення якої залежить від рівня виконання задачі-моделі загрози (ЗМЗ). Крім того, ЗМЗ може мати в якості підзадач інші задачі, що впливають на її ефективність, тобто заходи нейтралізації загрози.

Таким чином, модель загрози має всі властивості задачі ПІБД із деякими особливостями.

Визначимо у відповідність загрозі r_i деяке число $0 \le M_i \le 1$, яке називається ступенем реалізації загрози, причому $M_i = 0$, при повній відсутності впливу загрози й $M_i = 1$ при максимально можливій її прояві. Крім того, будемо характеризувати загрозу r_i ймовірністю p_t її реалізації в момент часу *t*. Цю величину повинні визначити експерти за допомогою групових методів експертного оцінювання [2, 8].

Визначення 2. Частковий коефіцієнт впливу α_{ij} (ЧКВ) загрози r_i на досягнення її безпосередньої надцілі λ_j (ступінь виконання задачі P_j) є приріст ступеня досягнення надцілі λ_j ступінь виконання задачі P_j), отриманий внаслідок повної реалізації загрози r_i.

У роботі далі, якщо це не викликає різночитань, будемо використовувати термін "надціль" для позначення як цілі, на ступінь досягнення якої безпосередньо впливає задача-модель загрози, так і задачі, на ступінь виконання якої впливає ця загроза.

Для більш адекватного опису задач підтримки рішень щодо комплексного цільового планування з урахуванням загроз і ризиків доцільно враховувати зміни в часі їх впливів. Виходячи із цього будемо говорити про миттєві значення в момент часу *t* коефіцієнта впливу $\alpha_{ink}(t)$ загрози r_i на досягнення її безпосередньої надцілі λ_n, який визначається з виразу

$$\alpha_{ih}(t) = \begin{cases} 0, \ \textit{якщо}\ t < \tau_{ih}; \\ \beta(\alpha_{ih}, t), \textit{інакше}, \end{cases} \tag{1}$$

де α_{ih} – стаціонарне значення коефіцієнта впливу (СЗКВ) загрози r_i на безпосередню надціль λ_h;

τ_{ih} – експертна оцінка затримки впливу загрози r_i на надціль λ_h;

λ – поліноміальна функція, яка описує зміну коефіцієнта впливу в часі.

Так як достовірна інформація щодо точності експертних оцінок коефіцієнтів полінома $\beta(\alpha_{ih}, t)$ відсутня, визначимо в (1) $\beta(\alpha_{ih}, t) = \alpha_{ih}$, тобто будемо враховувати тільки затримку впливу загрози на її безпосередню надціль. Цю величину визначають експерти.

Стаціонарні значення коефіцієнтів впливу $\alpha_{ih} \in A_h, i = (1, n_h)$, безпосередніх підцілей надцілі α_h, серед яких можуть бути загрози, що задовольняють умові $\sum_{i=1}^{nh} |\alpha_{ih}| = 1$.

У загальному випадку загроза r_i є безпосередня підціль декількох надцілей $\lambda_1, \lambda_2, ..., \lambda_h, ..., \lambda_z$, причому будь-яка надціль λ_h має деяку множину $\{\Lambda_h = \Lambda_{hk}\}$ альтернативних підмножин сумісних безпосередніх підцілей, $\Lambda_{hk} \cap \Lambda_{hl} \neq \phi, k \neq l$. Тому можливий випадок, коли $\lambda_i \in \Lambda_{hk}, \lambda_i \in \Lambda_{hl}, k \neq l$,і одна й та сама загроза r_i буде мати різні стаціонарні значення $\alpha_{ihk}, \alpha_{ihl}$ коефіцієнта впливу на одну й ту саму безпосередню надціль λ, які обчислені для різних альтернативних підмножин $\Lambda_{hk}, \Lambda_{hl}$.

Якщо досягнення підцілі λ_i сприяє досягненню її безпосередньої надцілі λ_h, тоді її СЗКВ $\alpha_{ihk} > 0$, інакше $\alpha_{ihk} < 0$. Із вмісту поняття загроз випливає, що часткові коефіцієнти впливу задач, які являються моделями відповідних загроз, від'ємні. Зауважимо, що до початку процесу визначення СЗКВ підцілей ієрархія повинна бути перетворена таким чином, щоб СЗКВ всіх підцілей були доданими. Це досягається заміною підцілей, які негативно впливають на відповідні надцілі, підцілями, які являються їх логічними інверсіями.

Тепер визначимо характеристики загроз. Першою характеристикою, яка визначає тип загрози, є спосіб вираження умов і наслідків її реалізації. Якщо умови реалізації загрози можна виразити результатом виміру деякої однієї, конкретної величини-ресурсу, то така загроза називається кількісною по входу, інакше – якісною.

Оскільки вплив ЗМЗ на досягнення їх безпосередніх надцілей негативний, то для найгіршого випадку ступінь їх виконання при відсутності компенсуючих впливів приймається рівним 1. При цьому ресурс визначається як кількісне вираження умов компенсації загрози, яка приводить до того, що ступінь виконання ЗМЗ буде дорівнювати нулю. Так, ресурс задачі, який являється моделлю загрози "атаки на інформаційні ресурси держави" являє собою суму окремих атак на різні елементи цих ресурсів.

Якщо значення ресурсу кількісної по входу загрози відомо, то така загроза є кількісною по входу визначеною. Значення ресурсу такої загрози однозначно визначається експертами при побудові ієрархії цілей. Якщо ж значення її ресурсу напевно невідомо, то така загроза являється кількісною по входу невизначеною. Для таких загроз визначаються погоджені узагальнені експертні оцінки величини ресурсу [1, 8].

Тому що ЗМЗ завжди являється безпосередньою підціллю якої-небудь цілі або задачі, вона характеризується результатом його виконання. Якщо результат повного виконання загрози можна виразити ефектом, тобто результатом виміру деякої однієї величини, то загроза є кількісною по виходу, а якщо ні, то – якісною по виходу.

Зрозуміло, що при визначенні ступеня досягнення надцілі повинні враховуватися ефекти від досягнення тільки множини її сумісних цілей. Тому що загроза діє незалежно від виконавців ПІБД, слід вважати її сумісної з кожною з підцілей. Тому ЗМЗ входить у кожну підмножину сумісних підцілей тієї надцілі, на досягнення якої безпосередньо впливає загроза. Отже, можна сформулювати наступне визначення.

Визначення 3. Безпосередні підцілі λ_i і λ_j, у тому числі й загрози деякої надцілі λ_S, називаються сумісними, якщо досягнення однієї не виключає можливості або доцільності досягнення іншої, і несумісними в протилежному випадку.

На підставі проведених досліджень приступимо до створення узагальненої моделі загрози. При цьому миттєве значення $M_h(t)$ ступеню реалізації загрози r_h у момент часу *t* визначається в такий спосіб:

$$M_h(t)=\begin{cases}0,\ якщо \sup_k \sum_i \alpha_{ihk}(t)\,M_i(t)<\Pi_h;\\ \Pi_h,\ якщо\ \sup_k \sum_i \alpha_{ihk}(t)\,M_i(t)=\Pi_h;\\ f(\sup_k \sum_i \alpha_{ihk}(t)\,M_i(t)),\ якщо\ \Pi_h<\sup_k \sum_i \alpha_{ihk}(t)\,M_i(t)<1-\sum_q \left|\alpha_{qhk}^{(-)}(t)\right|;\\ 1,\ якщо\ (1-\sum_q \left|\alpha_{qhk}^{(-)}(t)\right|)\le \sup_k \sum_i \alpha_{ihk}(t)\,M_i(t)\le 1;\end{cases} \quad (2)$$

де Π_h – поріг загрози r_h;
$f(\sup_k \sum_i \alpha_{ihk}(t)\,M_i(t))$ – функція ступеня реалізації загрози r_k;
k – номер підмножини Λ_{hk} сумісних безпосередніх підцілей загрози r_k;
i – номер підцілі $\lambda_i \in \Lambda_{hk}$;
$\alpha_{ihk}(t)$ – миттєве значення в момент часу t часткового коефіцієнта впливу підцілі $\lambda_i \in \Lambda_{hk}$ на досягнення загрози r_k, обчислене за умови, що підціль λ_i розглядається як елемент підмножини Λ_{hk} сумісних, безпосередніх підцілей загрози r_k;
$M_i(t)$ – миттєве значення ступеня досягнення підцілі λ_i у момент часу t;
$\alpha_{qhk}^{(-)}(t)$ – миттєве значення в момент часу t часткового коефіцієнта впливу підцілі $\lambda_q \in \Lambda_{hk}$, що негативно впливає на загрозу r_k.

Важливі окремі випадки загроз – це загрози квазілінійна й порогова.

Ступінь M_j виконання квазілінійні ЗМЗ r_j визначається виразом

$$M_j=\begin{cases}\sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh},\ якщо \sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh},\le 1;\\ 1,\qquad якщо \sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh},>1,\end{cases}$$

де h – номер підмножини Λ_{jk} сумісних, безпосередніх підцілей ЗМЗ загрози r_j;
s – номер підцілі $\lambda_{sjh} \in \Lambda_{jh}$;
α_{sjh} – частковий коефіцієнт впливу підцілі $\lambda_{sjh} \in \Lambda_{jh}$ на досягнення загрози r_j.

Вираз для обчислення M_j ступеня досягнення порогової загрози r_j має наступний вигляд

$$M_j=\begin{cases}1, \sup\limits_h \sum\limits_S \alpha_{sjh} M_{sjh}\ge \left|1-\sum\limits_{j\in J\bar{i}} \alpha_j\right|;\\ 0, в\ іншому\ випадку;\end{cases}$$

де $J_{\bar{i}}$ – множина номерів підцілей загрози r_j с негативним впливом.

Тепер приступимо до розробки моделі ризику. Поняття ризику характеризується невизначеністю, пов'язаною з можливістю виникнення в ході реалізації задачі ПІБД несприятливих ситуацій і наслідків [3, 4]. Інакше кажучи, під ризиком слід розуміти наслідок випадкової події, викликаної зовнішніми відносно ПІБД факторами, яка полягає у виникненні ситуації, що впливає на виконання програми ІБД.

Оскільки ризик є наслідок випадкової події, яка чи то відбудеться, чи то ні, тому, залежно від того, чи являється розробник ПІБД оптимістом або песимістом, сутність події, яка викликає ризик, можна сформулювати в одному випадку так, що його виникнення викличе негативний вплив на виконання програми, або так, що воно буде мати позитивний вплив.

Залежно від природи подій, які викликають ризик, розрізняють: техніко-технологічні, політичні, економічні, воєнні, фінансові, екологічні ризики учасників задачі, ризики обставин непереборної сили (форс-мажор) і специфічні ризики [4, 9]. При цьому одна й та сама подія може викликати ризики, які мають зовсім різні наслідки для виконання ПІБД. При цьому ризики необхідно оцінювати, виходячи із системного підходу, з урахуванням мети ПІБД і її структури.

Запровадимо визначення деяких понять.

Визначення 4. Фактором ризику ψ для ПІБД *P* називається процес ξ_ψ такий, що $\exists\, p_i \in P \lfloor V(p_i)\,\xi_\psi(t) \neq V(p_i)\neg\xi_\psi(t) \rfloor$, де $V(p_i)\,\xi_\psi(t) \neq V(p_i)\neg\xi_\psi(t)$ – відносна ефективність задачі (програми) $p_i \in P$ з урахуванням фактору ризику $\xi_\psi(t)$ і без його урахування, відповідно.

Визначення 5. Індикатором ризику ψ називається фіктивна ціль λ_ψ, єдиної підціллю якої є фактор ризику ψ.

Зазначимо, що фактор ризику є підціль для таких індикаторів ризику як λ_{ψ_1} і λ_{ψ_2}. Підцілі λ_{ψ_1} і λ_{ψ_2} – індикатори ризику, повністю описуються функціями ступеня досягнення цілі. У загальному випадку миттєве значення $M_h(t)$ ступеня досягнення безпосередньої надцілі λ_h у момент часу *t* визначається виразом (2).

При завданні функції досягнення цілі-індикатора ризику необхідно враховувати наступні особливості:

1. Оскільки пороги цілей задовольняють умові [10] $0 \le \prod_h \le 1$, тому значення випадкового процесу $\xi_\psi(t)$, що задає фактор ризику ψ, повинне також задовольняти умові $0 \le \xi_\psi(t) \le 1$;

2. Якщо $\lfloor \partial M(\lambda_{\psi_1}) / \partial\xi_\psi(t) \rfloor < 0$, у якості фактору ризику для цілі λ_{ψ_i}, що являється індикатором цього ризику, необхідно вибирати $\lfloor 1 - \xi_\psi(t) \rfloor$ замість $\xi_\psi(t)$.

Висновки

Пропонується підхід до підтримки прийняття рішень при формуванні комплексних програм забезпечення інформаційної безпеки держави з врахуванням загроз і ризиків. Під загрозою розуміється стан середовища, що впливає на ефективність задач ПІБД, у якому виконується комплексна цільова програма. Ризик визначений як наслідок випадкової події, викликаної впливом зовнішніх відносно ПІБД факторів, що полягає у виникненні ситуації, яка впливає на виконання ПІБД. Запропоновані моделі загроз і ризику.

Список літератури

1. Тоценко, В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / В.Г. Тоценко. – К: Наукова думка, 2002. – 382 с.
2. Орловский, С.А. Проблемы принятия решений при нечёткой исходной информации / В.Г. Орловский – М: Наука, 1981. – 208 с.
3. Згуровский, М.З. Информационный подход к анализу и управлению проектными рисками / М.З. Згуровский, Н.И. Коваленко, К. Кондрак, Э. Кондрак // Проблемы управления и информатики. – 2000. – № 4. – С. 148–156.
4. Грачёва, М.В. Анализ проектных рисков. Учебное пособие для вузов / М.В. Грачёва. – М.: ЗАО «Финстатинформ», 1999. – 216 с.
5. Кини, Р.Л. Принятие решений при многих критериях: предпочтения и замещения / Под ред. И.Ф. Шахнова. – М.: Радио и связь, 1981. – 560 с.

6. Руа, Б. Проблемы и методы принятия решений в задачах со многими целевыми функциями / Б. Руа // Вопросы анализа и процедуры принятия решений // под ред. И.Ф. Шахнова. – М.: Мир, 1976. – С. 20–58.
7. Катренко, А. В. Теорія прийняття рішень: підручник з грифом МОН / А.В. Катренко, В.В. Пасічник, В.П. Пасько. – К.: Видавнича група BHV, 2009. – 448 с.
8. Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь, 1993. – 278 с.
9. Макаров, И.М. Теория выбора и принятия решений / И.М. Макаров, Т.М. Виноградская, А.А. Рубчинский, В.Б. Соколов. – М: Наука, 1982. – 328 с.
10. Зибін, С.В. Оцінка якості функціонування комплексних систем технічного захисту й систем підтримки ухвалення рішення в їхньому складі / В.О. Хорошко, С.В. Зибін // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Вип. 2 (24). – С. 7–15.

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПРИ ФОРМИРОВАНИИ ПРОГРАММ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА: МОДЕЛИ УГРОЗ И РИСКОВ.

С.В. Зыбин, В.А. Хорошко

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03680, Украина; e-mail: professor_va@ukr.net

Предлагается подход к поддержке принятия решений для формирования комплексных целевых программ информационной безопасности государства при наличии угроз и рисков, который базируется на введении моделей угроз и рисков в иерархии целей программ (задач) и целевой оценки её. Модель риска имеет фактор риска, который является случайным процессом и имеет специальную цель. Угроза моделируется специальной программой, которая вводится в иерархию целей.

Ключевые слова: поддержка принятия решений, модели угроз и рисков, информационная безопасность, иерархия целей, целевая оценка.

DECISION-MAKING SUPPORT IN THE DEVELOPMENT OF NATIONAL INFORMATION SECURITY PROGRAMS. PART 1: DANGER-AND-RISK MODELS

S.V. Zybin, V.O. Khoroshko

National aviation university
1, Kosmonavta Komarova Avenue, Kyiv, 03680, Ukraine; e-mail:professor_va@ukr.net

The paper presents an approach to decision-making support in the development of comprehensive special-purpose national information security programs in the presence of dangers and risks. The approach relies on the introduction of danger-and-risk models into the hierarchy of program/task targets and on the target-based assessment of the support. The risk model has a random risk factor and a special target. The danger is simulated by a special program which is introduced into the target hierarchy.

Keywords: decision-making support, danger-and-risk models, information security, target-based assessment.

УДК 519.852:004.424.27.021

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 84-91

МОДИФИКАЦИИ МЕТОДА ВЕТВЕЙ И ГРАНИЦ ДЛЯ РЕШЕНИЯ ЗАДАЧ ЦЕЛОЧИСЛЕННОГО ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ И ИХ ЭФФЕКТИВНОСТЬ

Б.И. Юхименко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: pm1987pm@gmail.com

В работе дан краткий обзор разработок по комбинаторным методам решения задач целочисленной линейной оптимизации. Приведены основные составляющие метода ветвей и границ, которые можно рассматривать по-разному и получать новые модификации этого метода. Даны некоторые оценки эффективности работы модификационных составляющих.

Ключевые слова: оценка, последовательное построение, конкретизация, частичное решение, функции предпочтения.

Введение

Оптимизация. Принятие оптимальных решений. Эти фразы всё чаще используются в разговорах современных людей. Действительно, любое разумное решение можно назвать оптимальным. Оно определяется путём сравнения с другими возможными решениями. С математических позиций «оптимальное решение» требует значительно больше. Математик может назвать решение оптимальным только тогда, когда оно удовлетворяется признаку оптимальности.

Многовариантность и наличие критерия предопределяет теорию оптимизации. Нахождение оптимального варианта согласно выбранному критерию создает основу методов оптимизации. Метод оптимизации во многом зависит от форм математического описания, как множества вариантов, так и самого критерия оптимизации. В связи с этим хорошо известна условная и безусловная, дискретная и непрерывная оптимизация.

Наибольшего внимания среди математиков вызывает условная дискретная оптимизация. Такая популярность предопределяется простотой математического описания задач оптимизации, а также их реализации в вычислительном смысле. Теоретически возможный полный перебор вариантов заменяется частичным, и чем меньше вариантов пересматривается, тем алгоритм считается более эффективным. При разработке, в основном, используется комбинаторный подход. Это дает возможность вводить новые элементы при разработке или модификации алгоритмов. Не сложно перерабатывается программное обеспечение и сами IT-технологии, что упрощает реализацию практических задач, относящихся к задачам дискретной оптимизации.

Основная часть

Первые разработки по алгоритмизации, разработке методов и методик решения задач дискретной оптимизации были направлены на использование имеющегося математического аппарата для решения задач непрерывной оптимизации. К примеру, идея Данцига [1], предопределяющая возможность использовать симплекс метод для решения задач линейной дискретной оптимизации, дала начало целому направлению решения задач целочисленного линейного программирования. Идею Данцига реализовал Гомори [2]. Ему удалось решить все проблемы, связанные с алгоритмизацией и возможностями практического использования этой идеи. В настоящее время методы отсекающих плоскостей широко известны в сфере дискретной оптимизации.

Другое направление в дискретной оптимизации имеет свое начало с появлением работы Лэнд и Дойг [3]. Метод, предложенный австрийскими математиками, так же основан на симплекс методе, но уже в другом ракурсе. Решение определённой задачи линейного программирования используется, в основном, для получения оценки подмножества вариантов. Значение целевой функции при оптимальном варианте подмножества ограничивает сверху (снизу) значения целевой функции других его вариантов. В принципе, метод Лэнд и Дойг имеет комбинаторный характер. При помощи дополнительных ограничений формируется подмножество вариантов. Введен признак оптимальности с использованием оценок подмножеств. Данное направление в дискретной оптимизации стало именоваться методом ветвей и границ.

Широкого использования метод Лэнд и Дойг не получил. Следующим толчком в дискретной линейной оптимизации было появление работы Литла, Мурти и др. Им предложен метод ветвей и границ для решения задачи о коммивояжере [4]. Это была та идея, которая породила множество алгоритмов современной дискретной вычислительной математики. Тогда ещё интуитивное суждение о разбиении множества вариантов решения на подмножества, не что иное, как идея последовательного построения решения [5].

Что касается оценивания подмножеств, это идея сужения – расширения множества вариантов [6]. Другими словами, приведение задачи к легко разрешаемой задаче, с целью использования существующего программного обеспечения для её решения.

Метод ветвей и границ состоит из трёх основных процедур:

1. Разбиение множества вариантов на подмножества;
2. Оценивание подмножества вариантов;
3. Проверка на оптимальность полученного варианта.

Разбиение множества вариантов на подмножества – это разделение вариантов по определённому признаку. Скажем, в алгоритмах метода Лэнд и Дойг множество вариантов делится на два подмножества. В одном подмножестве некоторая переменная должна быть не меньше определённого целого значения, а во втором меньше. Практически, это исключение из рассмотрения нецелочисленных значений рассматриваемой переменной в единичном интервале. К примеру, если в результате решения компонента x_k^* получила нецелочисленное значение, то формируется ограничения типа

$$x_k \ge \left[x_k^*\right] + 1\,, \tag{1}$$

$$x_k \le \left[x_k^*\right], \tag{2}$$

где $\left[x_k^*\right]$ – целая часть x_k^*.

Объединение ограничений (1) и (2) поочередно с ограничениями исходной линейной задачи, формируются два подмножества вариантов с определёнными требованиями к компоненте x_k.

Совсем другой подход ветвления был предложен Литлом и его коллегами. Параметром разбиения множества вариантов объезда городов является пара городов

(k,l). Пара либо включается в вариант объезда либо нет. Таким образом, имеется два подмножества вариантов. Одно подмножество содержит переезд из k в l, другое – этот переезд запрещен. Математически, если вариант решения задачи о коммивояжере представляется матрицей инцидентности, то строка k либо инцидентна столбцу l, либо нет.

Оценивание подмножества вариантов – это определение границы сверху (снизу – для задач минимизации) значения целевой функции вариантов оцениваемого подмножества. Оценка предопределяет приоритетность подмножеств. Для дальнейшего разбиения выбирается самое приоритетное подмножество. Его обычно называют перспективным подмножеством вариантов.

Существуют различные способы получения оценок подмножеств вариантов. Однако, чем точнее, т.е. чем ближе значение оценки к экстремальному значению целевой функции вариантов подмножества, тем лучшим считается способ оценивания. Через оценки подмножеств выражается признак оптимальности метода ветвей и границ. Что, в свою очередь, влияет на скорость сходимости алгоритма.

Простейшим и самым точным способом оценивания является решение соответствующей задачи линейного программирования для получения оценок множества целочисленных вариантов. Этот способ был выявлен при создании метода Лэнд и Дойг. В самом деле, это не что иное, как расширение множества вариантов и приведение задачи целочисленного линейного программирования к задаче линейного программирования. Решение такой задачи не составляет трудностей в алгоритмическом смысле, но является не эффективным в вычислительном смысле, поскольку решать линейных задач приходится достаточно много.

Что касается признака оптимальности, то формально он состоит из двух частей. Первая часть – проверяется наличие перспективного подмножества вариантов, то есть подмножества, в котором может находиться лучше вариант, чем проверяемый на оптимальность. Если таких подмножеств не существует, то рассматривается вторая часть признака. Поскольку в подмножестве вариантов может находиться вариант лучше проверяемого, то значение целевой функции проверяемого варианта сравнивается с оценкой подмножества. Требуется совпадение по величине этих значений. Этот момент и предопределяет скорость сходимости алгоритма, зависящего от точности оценки.

Перебираемое количество вариантов в методе вервей и границ в некоторой степени зависит и от выбранной вершины дерева решений в случае, если полученный очередной вариант окажется не оптимальным. Обычно выбирается вершина с наилучшей (максимальной или минимальной) оценкой. Этот прием понимается, как само собой известный, используется, можно сказать, по умолчанию. Однако, максимальные по значению оценки имеют подмножества, в которых количество вариантов побольше. Это в дереве решений находится в верхних ярусах и до получения варианта необходимо пройти длинный путь, что уменьшает эффективность работы алгоритма. Возможны другие подходы, в том числе и рандимизированный по отношению к оценкам подмножеств. В работе [7] были предложены функции предпочтения, используемые при выборе вершины. Это ещё один элемент, позволяющий модифицировать алгоритмы метода ветвей и границ с целью увеличения их скорости сходимости.

Приведем несколько подходов реализации метода ветвей и границ и доведения до алгоритмов.

Достаточно давно [7] был предложен способ оценивания множества вариантов решения задачи линейного программирования с булевыми переменными, используя идею расширения – сужения множества вариантов. Сама идея была предложена профессором Шкубой В.В. [6]. Её использование значительно упрощает процедуру получения оценок, хотя далеко не всегда даёт желаемую точность оценивания. Однако часто неточность компенсируется вычислительной простотой процедуры определения значения оценки.

Идея состоит в том, что множество вариантов, задаваемых системой ограничений, расширяется путем отбрасывания некоторых требований к искомым величинам. Задача переносится в другой класс задач линейной оптимизации, решение которой не составляет трудностей.

Пусть имеется задача целочисленного линейного программирования (ЦЛП) в постановке

$$Z = \max \sum_{j=1}^{n} c_j x_j , \tag{3}$$

при ограничениях

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i ,\ i = \overline{1,m}; \tag{4}$$

$$x_j \ge 0,\ j = \overline{1,n}; \tag{5}$$

$$x_j \in \{0, N\}, \tag{6}$$

где N – множество натуральных чисел.

Отбрасывая требования целочисленности (6), получаем задачу линейного программирования (ЛП). Значение целевой функции при оптимальном решении задачи ЛП даст оценку множества вариантов, описываемых ограничениями (4)-(5)-(6), причем достаточно точную.

Если требование (6) заменить на требование

$$x_j \in \{0,1\}, \tag{7}$$

то имеем задачу ЦЛП с булевыми переменными. Соответствующая задача ЛП будет иметь удвоенную размерность. Требование (7) распадается на два требования, а именно

$$x_j \le 1;$$

$$x_j \text{ –целое.}$$

Матрица условий становится размером (m+n)×n. Решение задачи симплекс методом, причем многократно, при такой размерности затруднительно во времени.

Процедуру решения задачи ЦЛП с булевыми переменными с целью оценки множества вариантов можно привести к решению m одномерных не целочисленных задач о ранце [6].

Данный подход был опубликован [9] и сразу получил позитивную оценку и был использован при определении оптимального размещения геологических установок [10].

В 60-х годах XX столетия в институте кибернетики АН УССР был разработан метод последовательного анализа вариантов, состоящий в последовательном поэтапном конструировании конкурентоспособных вариантов [5].

Последовательное конструирование решения представляет собой пошаговый процесс. На каждом шаге конкретизируется значение одной компоненты вектора решений. Присвоение значения компоненте предопределяет подмножество тех вариантов, которые содержат компоненту с конкретным значением. Таким образом, последовательное построение решения используется как способ разбиения множества вариантов на подмножества.

Сама организация последовательного построения решений – это последовательная «сборка» варианта по одной компоненте с конкретным её значением. Номер компоненты, подлежащей конкретизации на очередном шаге может определяться по-разному. Простейший способ – это следование лексикографическому упорядочению самих компонент. На первом шаге конкретизируется первая компонента, на втором – вторая и т.д. Однако в таком случае необходимо пересмотреть все компоненты, независимо от того, компонента может иметь положительное значение или только нулевое. Любое упорядочение с учётом значений коэффициентов целевой функции, а также влияние конкретизируемой положительным значением компоненты на неувязки в системе ограничений не может не влиять на скорость сходимости алгоритма.

Установление очереди конкретизации переменных имеет начало в методе Балаша [11]. Метод является основным (может и единственным) представителем одностороннего ветвления. Здесь отсутствует понятие оценки подмножеств. Вводится понятие множества так называемых «хороших векторов». Смысл состоит в том, что на основе уже имеющегося частичного решения выбираются остальные компоненты вектора решений, которые могут принимать значение «единица». Вариант решения считается определенным, если не имеется компонент, конкретизируемых единичным значением. Признак оптимальности в данном методе тоже обособленный. Заключается он в том, что больше единичных значений нельзя поставить ни в одном продолжении ни одного частичного решения. Такой признак считается «слабым» и может привести к полному перебору, чтобы убедиться в отсутствии лучшего варианта. Довольно часто [12] проверка на оптимальность занимает больше времени, чем получение самого оптимального решения. Однако эту идею установки приоритетности переменных удалось перенести в алгоритмы с двухсторонним ветвлением, где признак оптимальности более «жесткий».

Случай определения номера конкретизируемой компоненты, навеянный идеями алгоритма Балаша, был предложен автором [13], и дал очень хорошие результаты в смысле скорости сходимости [14]. Сущность этого подхода состоит в том, что предпочтение отдается компоненте, которая дает относительно больший «вклад» в значение целевой функции и, тем самым, меньше всего «исчерпает» компоненты вектора ограничений.

С целью уменьшения количества пересматриваемых компонент создается множество называемых «хороших» компонент, т.е. тех, которые могут принимать положительное значение.

Каждая переменная, которая в силу ограничений может принимать положительное значение, оценивается. По величине оценки устанавливается приоритетность (перспективность) каждой переменной. Другими словами, устанавливается очередь их конкретизации, т.е. включение переменных в вариант решения с положительным значением. Величина оценки приоритетности зависит от двух моментов. Во-первых, какой «вклад» в значении целевой функции принесет конкретизируемая переменная. Это определяется как относительная величина по сравнению с минимальным значением коэффициента целевой функции. Во-вторых, насколько в сумме изменится значение компонент вектора ограничений, если переменная будет подлежать конкретизации. Произведение этих двух величин даст оценку переменной. Более подробно смотрите [13].

Что касается стратегии выбора вершины для дальнейшего ветвления, то включение эвристик в детерминированную часть алгоритмов метода ветвей и границ также дает свой результат. Структура метода позволяет осуществить выборку любой вершины дерева решений. Исход – получение лучшего решения зависит от того «начала», которое было выбрано. Какой вершине отдать предпочтение предопределяет функция предпочтения.

В детерминированном случае выбор ветви может осуществляться согласно величине оценки ветви. Довольно часто оценки ветвей либо одинаковые, либо близки между собой. Однозначный выбор одной из них не всегда оправдан. По этому, схемы решения дополняются идеями Монте-Карло таким образом, что выбор ветви осуществляется с частотой, пропорциональной значению оценки, либо с одинаковой частотой.

Предположим, что вершины пронумерованы от 1 до N. Сопоставим в соответствие каждой вершине величину p_q такую, что $\sum_{q=1}^{N} p_q = 1$, и некоторый интервал $[r,s]$, где $r_q = S_{q-1}; s_q = r_q + p_q u r_0 = 0$.

Длина интервала p_q может быть различной. Рассматриваются три случая:

1. Все вершины имеют одинаковую вероятность при выборе: $p_q = 1/N$;
2. Величина вероятности пропорционально зависит от величины оценки ветви: $p_q = \xi_q \Big/ \sum_{q=1}^{N} \sigma_q$;
3. Величина вероятности пропорционально зависит от k «наилучших» оценок вершин $p_q = \xi_q \Big/ \sum_{q \in R_q} \sigma_q$, где R_q номера k вершин с наибольшими значениями оценок.

Алгоритмически реализация функций предпочтения осуществляется через генерацию равномерно-распределенных случайных чисел из интервала $[0,1]$. Функции предпочтения могут использоваться в работе детерминированных алгоритмов метода ветвей и границ. Тогда их эффективность оценивается числом итераций при получении оптимального решения. Если алгоритм предназначен для получения достаточно «хорошего решения», то их эффективность оценивается рядом показателей, основанных на статистике. В первую очередь необходимо определить степень близости к оптимальному плану, из планов, получаемых этой функцией предпочтения. Кроме того, математическое ожидание отклонения полученных планов от оптимального тоже является оценкой эффективности функции предпочтения. При более серьезной оценке функции предпочтения следует рассмотреть динамику изменения отклонений от оптимального плана, что можно использовать при прогнозировании появления улучшенного плана.

Выводы

Были приведены различные модификации метода ветвей и границ для решения задач целочисленного линейного программирования. Модифицировались все основные составляющие самого метода. Упрощалась процедура получения оценок множества вариантов. Решение соответствующей линейной задачи заменялось решением ряда нецелочисленных одномерных задач о ранце. При таком упрощении процедуры оценивания «ослаблялась» точность получения оценок, но значительно упрощалась вычислительная сложность. Потеря точности компенсировалась простотой вычислительной процедуры и ускорила получение оптимального решения.

Приведенная процедура разбиения множества вариантов на подмножества имеет две модификации. На основе последовательного построения решения была предложена компоновка решения согласно лексикографическому упорядочению компонент варианта решения и выборочным способом конкретизации переменных. Оба способа являются дополнением классического метода ветвей и границ. Кроме того, второй способ (выборочный) значительно ускорил сходимость алгоритмов, построенных на этой идее.

В практическое использование метода ветвей и границ введены элементы Монте-Карловских процессов. Функции предпочтения со случайным выбором ветви для продолжения компоновки решения, можно сказать, новый элемент по сравнению и детерминированным выбором по наибольшей оценке ветви. Небольшой эксперимент даёт надежду на ускорение сходимости алгоритмов с использованием функции предпочтения.

Все рассмотренные моменты модифицирования метода ветвей и границ между собой независимы, так как усовершенствуются разные элементы метода. Следуя этому, можно создать не один алгоритм метода и выбрать самый удачный.

Список литературы

1. Dantzig, G.B. Discrete –variable extremum problems / G.B. Dantzig // Operat. Res. – 1957. – Vol. 5, №2. – PP. 266–277.
2. Gomory, R.E. Outline of an algorithm for integer solution to linear programs / R.E. Gomory // Bull. Amer. Math. Soc. – 1958. – Vol. 64, №5. – PP. 275–276.
3. Land, A.H. An automatic of solving discreate programming problems / A.H. Land, A.G. Doig // Econometrica. – 1960. – Vol. 28, №3. – PP. 497–520.
4. Little, I.D.C. An algorithm for the traveling salesman problems / I.D.C. Little, K.G. Murty, D.W. Sweeney, C. Karel // Operat Res. – 1963. – Vol. 11, №6. – PP. 972-980.
5. Михалевич, В.С. Последовательные алгоритмы оптимизации и их применение, I, II / В.С. Михалевич // Кибернетика. – 1965. – №1. – С. 45–55; №2. – С. 85–89.
6. Шкурба, В.В. Конструктивные подходы к решению задач дискретной оптимизации / В.В. Шкурба // В кн. «IVсимпозиум по экстремальным задачам» тезисы докладов, Каунас, 1969. – С. 15–17.
7. Лиепоните-Юхименко, Б.И. Об эффективности функций предпочтения целочисленнорго линейного программирования / Б.И. Лиепоните-Юхименко // Lietuvos matematikos rinkinys. – 1983. – XXIII, №1. – С. 134–140.
8. Шкуба, В.В. Схема ветвей и границ в задачах целочисленного линейного программирования с булевыми переменными / Шкуба В.В., Юхименко Б.И. // Труды Одесского политехнического института. – 1989. – Вып. 2. – С. 176–215.
9. Юхименко, Б.И. О блочном подходе решения задач целочисленного линейного программирования методом ветвей и границ / Б.И. Юхименко // В сб.: Теоретические и методологические основы создания АСУ. – Межвуз. Научн. сб.: М., 1974. – С. 188–191.
10. Венгерова, И.В. Применение целочисленного программирования к оптимальному планированию геологических мероприятий / И.В. Венгерова, А.В. Тарасенко // Экономико-математические методы. – 1974. – Т. 10, № 5. – С. 1018–1020.
11. Balas, E. An additive algorithm for solving linear programs with zero-one variables / E. Balas // Operat Res. – 1965. – Vol. 13, №4. – PP. 517–546.
12. Корбут, А.А. Дискретное программирование / А.А. Корбут, Ю.Ю. Финкельштейн. – М.: Наука, 1969. – 370 с.
13. Юхименко, Б.И. Ускоренный алгоритм метода ветвей и границ для решения задач целочисленного линейного программирования / Б.И. Юхименко // Труды Одесского политехнического университета. – 2004. – Вып. 2. – С. 223–226.
14. Юхименко, Б.И. Сравнительная характеристика алгоритмов метода ветвей и границ для решения задач целочисленного линейного программирования / Б.И. Юхименко, Ю.Ю. Козина // Труды Одесского политехнического университета. – 2005. – Вып. 2 (24). – С. 199–204.
15. Юхименко, Б.І. Вибір ефективного алгоритму розв’язання задач цілочисельного лінійного програмування / Б.І. Юхименко // Труди Одеського політехнічного університета. – 2003. – Вип. 2 (20). – С. 172–176.
16. Юхименко, Б.И. Обобщение алгоритмов метода ветвей и границ для решения задач линейного программирования с булевыми переменными / Б.И. Юхименко // Информатика и математические методы в моделировании. – 2012. – Том 2, №2. – С. 173–179.

МОДИФІКАЦІЇ МЕТОДУ ГІЛОК І МЕЖ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ ЦІЛОЧИСЛОВОГО ЛІНІЙНОГО ПРОГРАМУВАННЯ ТА ЇХ ЕФЕКТИВНІСТЬ

Б. В. Юхименко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: pm1987pm@gmail.com

В роботі дано короткий огляд розробок за комбінаторних методів розв'язання задач цілочислової лінійної оптимізації. Наведено основні складові методу гілок і меж, які можна розглядати по-різному і отримувати нові модифікації цього методу. Наведено оцінки ефективності роботи модифікаційних складових.

Ключові слова: оцінка, послідовне побудова, конкретизація, часткове рішення, функції переваги.

BRANCH AND BOUND METHOD MODIFICATIONS FOR THE SOLUTION OF INTEGER LINEAR PROGRAMMING PROBLEMS AND THEIR EFFICACY

B.I. Yukhimenko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: pm1987pm@gmail.com

The combinatorial approaches to the solution of integer linear optimization problems were briefly reviewed. We discussed the main components of a branch and bound method which can be considered differently to obtain new modifications of the method. The efficacy of the operation of modified components was assessed.

Keywords: assessment, sequential sampling, obtaining specific forms, preference functions.

УДК 004: 519.2: 519.6

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 1, pp. 92-97

МОДЕЛЮВАННЯ ГАУСІВСЬКИХ ВИПАДКОВИХ ВЕЛИЧИН ІЗ ВИКОРИСТАННЯМ ПЕРЕТВОРЕННЯ ДЖОНСОНА ІЗ СІМ'Ї S_U

С.Б. Приходько

Національний університет кораблебудування імені адмірала Макарова,
просп. Героїв Сталінграду, 9, Миколаїв, 54025, Україна; e-mail: sergiy.prykhodko@nuos.edu.ua

Робота присвячена удосконаленню метода моделювання гаусівських випадкових величин на основі нормалізуючого перетворення Джонсона із сім'ї S_U, який, на відміну від багатьох існуючих методів, для генерування одного значення гаусівської випадкової величини потребує тільки одне значення випадкової величини з рівномірним розподілом та покращує результати моделювання на границях емпіричного розподілу гаусівської випадкової величини, що моделюється.

Ключові слова: моделювання, випадкова величина, розподіл Гауса, перетворення Джонсона

Вступ

При статистичному моделюванні випадкових процесів часто виникає необхідність у значеннях випадкових величин з розподілом Гауса. Зараз для моделювання таких величин використовують методи, основою яких є перетворення випадкових чисел з рівномірним розподілом у такі, що мають розподіл Гауса [1-6]. Всі ці методи можна поділити на дві групи: методи, що базуються на виключеннях [1-3], та методи, що використовують різноманітні перетворення [3-6]. Методи на основі виключень (або методи відбракування) та частина методів, що базується на нелінійних перетвореннях (наприклад, Бокса-Мюллера), потребують для створення визначеної кількості значень гаусівської випадкової величини (ГВВ) приблизно в 1.25 рази більше значень випадкових чисел з рівномірним розподілом. В цьому разі існує проблема зменшення фактичної кількості значень псевдовипадкових чисел з рівномірним розподілом в межах періоду генератора, яку можна використовувати до їх повторення. Один із шляхів рішення цієї проблеми може бути реалізований завдяки методу на основі зворотної функції [3]. Але його використання для моделювання ГВВ ускладнено тим, що не існує аналітичного виразу зворотної функції для функції розподілу Гауса, а це потребує відповідної її апроксимації. Другий шлях – це застосування методу на основі нормалізуючих перетворень, зокрема перетворення Джонсона [5, 6]. В [5] для моделювання ГВВ запропоновано застосовувати нормалізуюче перетворення Джонсона із сім'ї S_B. Слід зазначити, що перетворення із цієї сім'ї не є бієктивним. А це приводить до поганих результатів на границях або «хвостах» емпіричного розподілу ГВВ, що моделюється. В [6] для покращення результатів моделювання випадкових величин з розподілом Гауса запропоновано застосовувати бієктивне нормалізуюче перетворення, яким є перетворення Джонсона із сім'ї S_U. Його застосування дозволило розширити границі змодельованої ГВВ з 2 до 3 середньо квадратичних відхилень від математичного очікування. Але часто виникає потреба в збільшенні меж моделювання ГВВ. А це потребує подальшого удосконаленні метода моделювання ГВВ на основі нормалізуючого перетворення Джонсона із сім'ї S_U, який для генерування одного значення ГВВ потребує тільки одне значення випадкової величини з рівномірним розподілом.

Мета статті і постановка задач дослідження

Мета роботи полягає в подальшому удосконаленні метода моделювання ГВВ на основі нормалізуючого перетворення Джонсона із сім'ї S_U для покращення результатів моделювання на границях емпіричного розподілу ГВВ, що моделюється, в інтервалі більшому за три середньо квадратичних відхилення від математичного очікування.

Для досягнення поставленої мети потрібно вирішити наступні задачі: розглянути перетворення Джонсона з можливістю удосконалення на його основі метода генерування ГВВ; виконати комп'ютерне моделювання ГВВ за удосконаленим методом на основі перетворення Джонсона із сім'ї S_U.

Викладення основного матеріалу

В загальному випадку перетворення Джонсона має вигляд [4]

$$z = \gamma + \eta h(x, \varphi, \lambda); \eta > 0; -\infty < \gamma < \infty; \lambda > 0; -\infty < \varphi < \infty, \tag{1}$$

де z – нормально розподілена випадкова величина з математичним очікуванням нуль і дисперсією одиниця; x – випадкова величина з розподілом Джонсона; γ, η, λ, φ – параметри перетворення або розподілу Джонсона; h – функція з певної сім'ї:

$$h = \begin{cases} \ln(\tilde{x}), & x > \varphi, & \text{для сім'ї } S_L; \\ \ln[\tilde{x}/(1-\tilde{x})], & \varphi < x < \varphi + \lambda, & \text{для сім'ї } S_B; \\ \mathrm{Arsh}(\tilde{x}), & -\infty \le x \le +\infty, & \text{для сім'ї } S_U. \end{cases}$$

Тут $\tilde{x} = (x - \varphi)/\lambda$; $\mathrm{Arsh}(\tilde{x}) = \ln\left(\tilde{x} + \sqrt{\tilde{x}^2 + 1}\right)$.

Для перетворення (1) функції щільності ймовірності (ФЩЙ) випадкової величини x відповідних сімей S_L, S_B, S_U задаються як

$$f_L(x) = \left(\eta / \left(\sqrt{2\pi}(x-\varphi)\right)\right)\exp\left\{-0.5 \cdot \eta^2 \left[(\gamma - \eta \ln \lambda)/\eta + \ln(x-\varphi)\right]^2\right\};$$

$$f_B(x) = \left(\eta\lambda / \left(\sqrt{2\pi}(x-\varphi)(\lambda + \varphi - x)\right)\right)\exp\left\{-0.5\left[\gamma + \eta \ln\left((x-\varphi)/(\lambda+\varphi-x)\right)\right]^2\right\};$$

$$f_U(x) = \left(\eta \Big/ \sqrt{2\pi\left\{(x-\varphi)^2 + \lambda^2\right\}}\right)\exp\left\{-0.5\left[\gamma + \eta \ln\left(\tilde{x} + \sqrt{\tilde{x}^2+1}\right)\right]^2\right\}. \tag{2}$$

Сім'ї розподілів Джонсона у площині асиметрії у квадраті A^2 та ексцесу ε займають значні області (рис. 1). Якщо комбінація A^2 і ε знаходиться біля лінії S_L, то розподіл апроксимується ФЩЙ сім'ї S_L. Розподіл зі значеннями A^2 і ε, які лежать вище лінії S_L, апроксимуються ФЩЙ сім'ї S_U, а які лежать нижче лінії S_L (до лінії критичної області) – ФЩЙ сім'ї S_B. Якщо комбінація A^2 і ε попадає в критичну область, то вибірковий розподіл не можна апроксимувати розподілом Джонсона. Функції, що апроксимують відповідні лінії на рис. 1, наведені в [7].

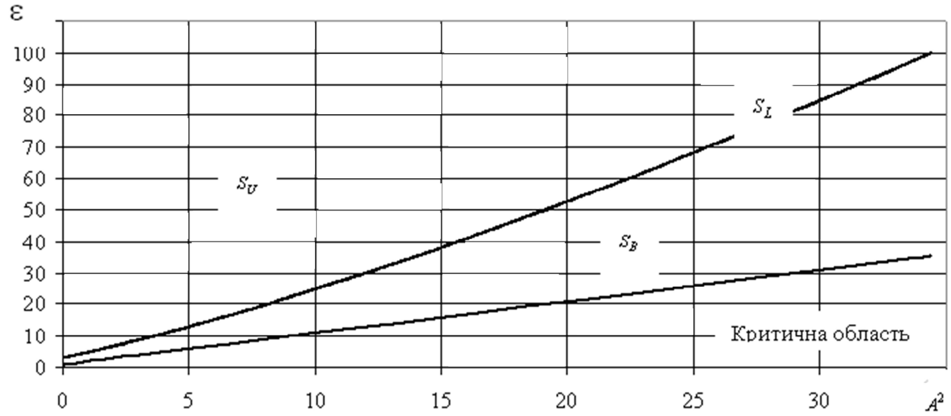


Рис. 1. Комбінації A^2 і ε для розподілів Джонсона

Оцінювання параметрів перетворення Джонсона у разі великої вибірки, коли є можливість побудувати гістограму, можна здійснити за методом найменших квадратів, наприклад, як в роботі [5]. У разі як малої, так і великої вибірок відповідні оцінки параметрів можуть бути визначені за рішенням задачі [5]

$$\hat{\theta} = \arg\min_{\theta} \left\{ A_z^2 + (\varepsilon_z - 3)^2 + \bar{z}^2 + \left(S_z^2 - 1\right)^2 \right\}, \tag{3}$$

де θ – вектор невідомих параметрів, $\theta = \{\gamma, \eta, \lambda, \varphi\}$; $A_z = \dfrac{1}{nS_z^3}\sum_{i=1}^{n}(z_i - \bar{z})^3$; $\varepsilon_z = \dfrac{1}{nS_z^4}\sum_{i=1}^{n}(z_i - \bar{z})^4$; $\bar{z} = \dfrac{1}{n}\sum_{i=1}^{n} z_i$; $S_z^2 = \dfrac{1}{n}\sum_{i=1}^{n}(z_i - \bar{z})^2$; z_i – i-значення величини z у вибірці довжиною n, $i \in [1, n]$, визначаються за перетворенням (1).

В (3) враховане те, що в перетворенні Джонсона (1) z – це нормально розподілена випадкова величина з нульовим математичним очікуванням і одиничною дисперсією.

Оцінки параметрів перетворення Джонсона можуть бути визначені за методом максимальної правдоподібності $\hat{\theta} = \arg\max_{\theta} l(\theta)$, де $l(\theta)$ – логарифмічна функція правдоподібності. Для перетворення Джонсона сім'ї S_U, якому відповідає ФЩЙ (2), логарифмічну функцію правдоподібності можна записати як

$$l(\theta) = n\ln\eta - 0.5\cdot n\ln 2\pi - 0.5\cdot\sum_{i=1}^{n}\ln\left[(x_i - \varphi)^2 + \lambda^2\right] - 0.5\cdot\sum_{i=1}^{n}\left[\gamma + \eta\,\mathrm{Arsh}((x_i - \varphi)/\lambda)\right]^2.$$

Для того, щоб за перетворенням (1) отримати значення ГВВ треба мати значення випадкової величини з розподілом Джонсона, яке потрібно отримувати за значенням випадкової величини з рівномірним розподілом. В [5] було запропоновано значення випадкової величини x з розподілом Джонсона із сім'ї S_B визначати за значення випадкової величини U з рівномірним розподілом за перетворенням

$$x = \sin(\pi U/2),\ U \in [-1, 1]. \tag{4}$$

Використовуючи (4), значення ГВВ з математичним очікуванням нуль і дисперсією одиниця в [5] запропоновано знаходити за перетворенням (1) із сім'ї S_B:

$$z = 0.3522056 \ln[\tilde{x}/(1-\tilde{x})], \tag{5}$$

де $\tilde{x} = (\sin(\pi U/2) + 1.0017416)/2.0034832$.

Але використання (5) для генерування ГВВ дає задовільні результати в межах $m_z \pm 2\sigma_z$. Тут m_z – це математичне очікування випадкової величини z, а σ_z – її середнє квадратичне відхилення. На границях інтервалу $m_z \pm 2.5\sigma_z$ результати генерування стають не задовільними: емпірична абсолютна частота величини z перевищує теоретичну настільки, що з довірчою ймовірністю 0.95 нульова гіпотеза про нормальність закону розподілу повинна бути відкинута. Такий результат можна пояснити тим, що перетворення Джонсона (1) із сім'ї S_B не є бієктивним і множини значень випадкових величин z та x не є ізоморфними.

Виправити таку ситуацію можна за рахунок застосування перетворення Джонсона (1) із сім'ї S_U, яке є бієктивним, а множини значень випадкових величин z та x є ізоморфними [6]. У якості функції, яка дозволяє отримати значення випадкової величини x з розподілом Джонсона (1) із сім'ї S_U за значенням випадкової величини U з рівномірним розподілом, пропонується використати функцію

$$x = tg\left(c_1 U + c_3 U^3\right),\ U \in [-1, 1]. \tag{6}$$

Тут c_1 і c_3 – це певні константи, за допомогою яких можна регулювати розмах значень величини x, а через неї і випадкової величини z.

Значення ГВВ з математичним очікуванням нуль і дисперсією одиниця визначаємо за перетворенням Джонсона (1) із сім'ї S_U:

$$z = \eta\, \mathrm{Arsh}(x/\lambda). \tag{7}$$

За (7) можна виконувати генерування гаусівських випадкових чисел з вибірковим середнім нуль і вибірковою дисперсією одиниця за алгоритмом наведеним в [6]. Для перевірки можливості моделювання ГВВ за перетвореннями (6) і (7) в більшому за $m_z \pm 3\sigma_z$ інтервалі, як і в [6], було виконано моделювання 2000 значень випадкової величини з розподілом Гаусу. З метою порівняння результатів з [6] для обчислення значень величини U використовувався відомий алгоритмічний генератор $U_i = (\omega_i - 32768)/32768$, де ω_i – i-те значення випадкової величини ω з рівномірним розподілом, $\omega \in [0, 65536)$, $\omega_i = (25173\omega_{i-1} + 13849) \bmod 65536$. Так як і в [6], початкове значення ω при генеруванні випадкової величини z дорівнювало 2009.

Результати моделювання випадкової величини з розподілом Гаусу при різних значеннях c_1 і c_3 наведені в табл.1. В табл.1 наведені також параметри перетворення Джонсона (η і λ), границі випадкової величини z, вибіркового середнього $\bar{z}$, вибіркової дисперсії S_z^2, асиметрії A_z, ексцесу ε_z, χ^2. Параметри перетворення Джонсона γ і φ дорівнювали нулю. Оцінювання параметрів перетворення Джонсона здійснювалося за методом максимальної правдоподібності. Критичне значення χ^2 для рівня значимості 0.05 та кількості ступенів вільності 8 дорівнює 15.5, що вказує на те, що гіпотезу про нормальність розподілу для всіх змодельованих вибірок значень z за критерієм Пірсона потрібно прийняти з довірчою ймовірністю 0.95.

Таблиця 1.

Результати моделювання випадкової величини z з розподілом Гаусу при різних значеннях констант c_1 і c_3

c_1	c_3	η	λ	$[z]$	$\bar{z}$	S_z^2	A_z	ε_z	χ^2
1.55	0	0.59831	0.71388	$[-2.90, 2.91]$	-0.013	1.034	0.051	2.82	10.3
1.56	0	0.56617	0.66695	$[-3.14, 3.15]$	-0.013	1.031	0.053	2.93	13.3
0.55	1	0.52215	0.24540	$[-3.07, 3.08]$	-0.013	1.032	0.051	2.78	10.2
0.56	1	0.50913	0.23926	$[-3.29, 3.31]$	-0.013	1.030	0.053	2.86	10.8
0.57	1	0.48779	0.22719	$[-3.90, 4.00]$	-0.013	1.021	0.053	3.05	13.0

Результати в таблиці 1 свідчать про можливість моделювання ГВВ за перетвореннями (6) і (7) в більшому за $m_z \pm 3\sigma_z$ інтервалі. Для значень констант $c_1 = 0.57$ і $c_3 = 1$ цей інтервал складає $[-3.90, 4.00]$, а побудована за результатами моделювання гістограма величини z наведена на рис.2. На рис.2 пунктиром також показана ФЩЙ розподілу Гауса f_z.

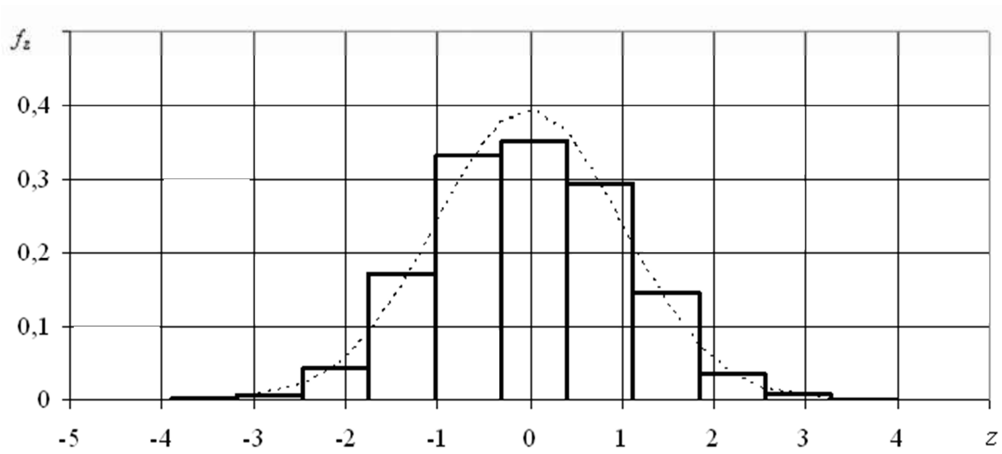


Рис. 2. Емпіричний та теоретичний розподіли випадкової величини z

Перевірка гіпотези про нормальність закону розподілу за критерієм Пірсона (χ^2) показала, що з довірчою ймовірністю 0,95 змодельовані значення випадкової величини z з нульовим математичне сподівання та одиничною дисперсією на інтервалі $[-3.90, 4.00]$ відповідають закону Гауса.

Висновки

Отримав подальший розвиток метод моделювання ГВВ на основі нормалізуючих перетворень за рахунок застосування перетворення Джонсона із сім'ї S_U, який, на відміну від багатьох існуючих методів, для створення одного значення ГВВ потребує тільки одне значення випадкової величини з рівномірним розподілом та покращує результати моделювання на границях емпіричного розподілу ГВВ, що моделюється, в межах інтервалу $m_z \pm 4\sigma_z$.

В подальшому планується для збільшення меж інтервалу моделювання ГВВ застосувати інші функції разом з перетворенням Джонсона із сім'ї S_U.

Список літератури

1. Форсайт, Дж. Машинные методы математических вычислений / Дж. Форсайт, М. Малькольм, К. Моулер. – М.: Мир, 1980. – 279 с.
2. Вероятностные методы в вычислительной технике: Учеб. пособие для вузов по спец. ЭВМ / А.В. Крайников и др.; под ред. А.Н. Лебедева и Е.А.Чернявского. – М.: Высш. шк., 1986. – 312 с.
3. Thomas, D.B. Gaussian Random Number Generators [E-resource] / D.B. Thomas, W. Luk, P.H.W. Leong, J.D. Villasenor // ACM Computing Surveys. – 2007. – Vol. 39. – No. 4. – PP. 1-38. Access mode: http://www.cse.cuhk.edu.hk/~phwl/mt/public/archives/papers/grng_acmcs07.pdf
4. Кендалл, М. Теория распределений: Пер. с англ. / М. Кендалл, А. Стюарт, под ред. А.Н. Колмогорова. – М.: Наука. Гл. ред. физ.-мат. лит., 1966. – 588 с.
5. Приходько, С.Б. Моделювання гаусівських випадкових величин на основі перетворення Джонсона із сім'ї S_B [Текст] / С.Б. Приходько // Інформатика та математичні методи в моделюванні. – 2012. – Т.2, №1. – С.64-69.
6. Приходько, С.Б. Застосування нормалізуючого перетворення Джонсона із сім'ї S_U для моделювання гаусівських випадкових величин [Текст] / С.Б. Приходько // Комп'ютерні науки: освіта, наука, практика: Матеріали Міжнародної науково-технічної конференції. – 2014. – С.149–152.
7. Приходько, С.Б. Аналитическая зависимость для выбора распределения Джонсона семейства S_L [Текст] / С.Б. Приходько, Л.Н. Макарова // Вестник ХНТУ. – 2012. – № 2 (45). – С.101–104.

МОДЕЛИРОВАНИЕ ГАУССОВСКИХ СЛУЧАЙНЫХ ВЕЛИЧИН С ПРИМЕНЕНИЕМ ПРЕОБРАЗОВАНИЯ ДЖОНСОНА ИЗ СЕМЕЙСТВА S_U

С.Б. Приходько

Национальный университет кораблестроения имени адмирала Макарова,
просп.Героев Сталинграда, 9, Николаев, 54025, Украина;
e-mail: sergiy.prykhodko@nuos.edu.ua

Робота посвящена усовершенствованию метода моделирования гауссовских случайных величин на основе нормализирующего преобразования Джонсона из семейства S_U, который, в отличие от многих существующих методов, для генерирования одного значения гауссовской случайной величины требует только одно значение случайной величины с равномерным распределением и улучшает результаты моделирования на границах эмпирического распределения моделируемой гауссовской случайной величины.

Ключевые слова: моделирование, случайная величина, распределение Гаусса, преобразование Джонсона

SIMULATION OF GAUSSIAN RANDOM VARIABLES USING JOHNSON S_U TRANSFORM

S.B. Prykhodko

Adm. Makarov National Shipbuilding University,
9, Geroev Stalingrada Ave., Mykolaiv, 54025, Ukraine; e-mail: sergiy.prykhodko@nuos.edu.ua

The paper presents the modification of simulation for Gaussian random variables using a normalizing Johnson S_U transform. This approach, unlike many others, uses a single random flat value to generate a value of a Gaussian random variable, and improves the simulation results at the boundaries of empiric distribution of the Gaussian random variable simulated.

Keywords: simulation, random value, Gaussian distribution, Johnson transform.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 5, номер 1, 2015. Одеса – 98 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 5, номер 1, 2015. Одесса – 98 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 5, No. 1, 2015. Odesa – 98 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 27.01.2015)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: immm.ukraine@gmail.com