

ISSN 2518-7678



ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ТЕЛЕКОМУНІКАЦІЙ

Є ЧЛЕНОМ МІЖНАРОДНОГО СОЮЗУ
ЕЛЕКТРОЗВ'ЯЗКУ



ДЕРЖАВНЕ ПІДПРИЄМСТВО
«УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ЗВ'ЯЗКУ»

Науковий журнал

НАУКОВІ ЗАПИСКИ УКРАЇНСЬКОГО НАУКОВО-ДОСЛІДНОГО ІНСТИТУТУ ЗВ'ЯЗКУ

1(45) • 2017

Виходить щоквартально

Засновано в м. Київ у 2007 р.

Журнал індексується в наукометричній базі Google Scholar.

Реферативна інформація видання представлена у загальнодержавній реферативній базі даних «Україніка наукова» та публікується у відповідних тематичних серіях УРЖ «Джерело».

Київ

Державний університет телекомунікацій

2017

Наукові записки УНДІЗ

Науковий журнал

Свідоцтво про державну реєстрацію – КВ №22001-11901ПР від 23.03.2016 р.

Наукове фахове видання України –

Наказ Міністерства освіти і науки України від 11.07.2016 №820.

ГОЛОВНИЙ РЕДАКТОР

Беркман Любов Наумівна, д.т.н., проф.

ЗАСТУПНИКИ ГОЛОВНОГО РЕДАКТОРА

Жураковський Богдан Юрійович, д.т.н., проф.

Мороз Сергій Миколайович, директор УНДІЗ

ВІДПОВІДАЛЬНИЙ СЕКРЕТАР

Макаренко Анатолій Олександрович, к.т.н., доцент

ЧЛЕНИ РЕДАКЦІЙНОЇ КОЛЕГІЇ

Блауништейн Натан Олександрович, д.т.н., проф.

Весоловський Кишиштоф, д.т.н., проф.

Вишнівський Віктор Вікторович, д.т.н., проф.

Віноградов Микола Анатолійович, д.т.н., проф.

Гребенніков Валерій Олександрович, к.т.н., с.н.с.

Дружинін Володимир Анатолійович, д.т.н., проф.

Зайка Віктор Федорович, д.т.н., доцент

Каток Віктор Борисович, к.т.н., проф.

Кільчицький Євген Васильович, к.т.н.

Климаш Михайло Миколайович, д.т.н., проф.

Кузнецов Олександр Петрович, д.т.н., проф.

Лемешко Олександр Віталійович, д.т.н., проф.

Лунтовський Андрій Олегович, д.т.н., проф.

Попов Валентин Іванович, д.ф.-м.н., проф.

Поповський Володимир Володимирович, д.т.н., проф.

Рибка Сергій Володимирович, к.т.н.

Савченко Юлій Григорович, д.т.н., проф.

Сайко Володимир Григорович, д.т.н., проф.

Семенко Анатолій Іларіонович, д.т.н., проф.

Сундучков Костянтин Станіславович, д.т.н., проф.

Тарасенко Володимир Петрович, д.т.н., проф.

Трембовецький Максим Петрович, д.т.н., с.н.с.

*Рекомендовано до друку Вченою радою Державного університету телекомунікацій
(протокол №16 від 13.02.2017 р.)*

Редакція може не поділяти думок авторів.

Відповідальність за зміст наданих матеріалів несуть автори.

Адреса редакції: ДУТ. Вул. Солом'янська, 7, м. Київ, 03110

Тел. +38 044 249 29 10; +38 097 509 00 33

Ел. пошта: makarenkoa@ukr.net **Сайт:** <http://www.journals.dut.edu.ua>

© Державний університет телекомунікацій, 2016

© Український науково-дослідний інститут зв'язку, 2007

© «Наукові записки Українського науково-дослідного інституту зв'язку», 2007

З М І С Т

Гороховський Є.П. Метод вирішення завдання багатокритеріальної оптимізації систем управління різнорідними телекомунікаційними мережами	5
Сайко В.Г., Лисенко Д.О., Грищенко Л. М., Дакова Л.В., Кравченко В.І. Алгоритм адаптації радіосистеми до середньостатистичних змін параметрів радіоканалу терагерцового діапазону	12
Бондаренко В.Є., Блєднов О.В. Суб'єктивно-ймовірнісна модель синтезу живучих комп'ютерних мереж	19
Захарченко М.В., Корчинський В.В., Домрачева К.О., Шокотько А.А. Використання таймерної сигнальної конструкції при імпульсно-кодовій модуляції мовного сигналу	26
Гринкевич Г.О., Макаренко А.О., Жебка В.В., Куклов В.М., Підручний А.І. Аналіз працездатності програмно-конфігурованих мереж	32
Недашківський О.Л. Сценарії організації зв'язку з використанням технології BPL в Metro Ethernet мережах доступу	40
Бондаренко Т.Г., Зенів І.О. Ніжник Р.С. Результати дослідження твердотілого хвильового гіроскопу з металевим резонатором	49
Федорова Н.В. Алгоритм управління мультисервісної макромережею	59
Ільїн О.О. Розробка моделі конкурентоспроможного випускника методом анкетування потенційного роботодавця	65
Попов А.А. Алгоритм розрізнення детермінованих ортогональних сигналів, побудований на основі операцій L-групи	72
Шефер О.В. Підвищення завадостійкості радіотехнічних систем шляхом адаптивного преналагодування та інверсного кореляційного підходу до виявлення корисного сигналу	82
Буценко Ю.П., Савченко Ю.Г. Оцінювання рівня «випадковості» послідовності псевдовипадкових бінарних чисел	89
Грінченко О.О., Грінченко С.А. Концептуальні основи моделювання екосистем програмного забезпечення	94
Данік О.В. Спосіб контролю рівня надійності суднових комплексів при нестабільних умовах спостережень	104
Захаріудакіс Лефтеріос Метод швидкої автентифікації віддалених користувачів на основі концепції “нульових знань”	109
Мусорін О.О., Трофименко І.В., Шапран Ю.Є. Особливості аналітичного забезпечення експлуатації суден у сучасних умовах	117

C O N T E N T S

Gorohovskyy E.P. The method of solving the problem of multi-objective optimization of control system of telecommunications networks	5
Saiko V.H., Lysenko D.O., Hryshchenko L.M., Dakova L.V., Kravchenko V.I. Radio system adaptation algorithm to average changes of parameters of the terahertz radio channel	12
Bondarenko V.E., Blednov A.V. The subjective-probabilistic model of synthesis of surviving computer networks	19
Zaharchenko N.V., Korchinskiy V.V., Domracheva K.O., Shokotko A.A. Using of the timer signal constructions for pulse-code modulation of the voice signals	26
Grynkevych G.O., Makarenko A.O., Zhebka V.V., Kuklov V.M., Pidruchniy A.I. Analysis serviceability program-configured networks	32
Nedashkivskyy O.L. Scenarios of use BPL technology in the Metro Ethernet access networks	40
Bondarenko T.G., Zeniv I.O., Nizhnyk R.S. Research results of solid-state wave gyroscope with metallic resonator	49
Fedorova N.V. Algorithm of management of multi-service macro network	59
Ilin O.O. The development of a competitive graduate model by the method of questioning a potential employer	65
Popov A.A. Deterministic orthogonal signals classification algorithm built on the basis of L-group operations	72
Shefer O. V. The increase of radio technical noise immunity systems by adaptive premaligant and inversive correlation approach to the detection of the beneficial signal	82
Butsenko Y.P., Savchenko Y.G. Evaluation of “random” pseudorandom binary sequence of numbers	89
Grinenko O.O., Grinenko S.A. Conceptual foundations of methods of software ecosystem modeling	94
Danik O.V. A method for controlling the level of reliability marine complex in unstable conditions of observation	104
Zacharioudakis Eleftherios Method for high speed remote user authentication based on zero-knowledge conception	109
Musorin O.O., Trofimenko I.V., Shapran Y.E. Features of analytical providing of ships expatriation in operation conditions	117

УДК 621.391.3

Гороховський Є.П., здобувач

МЕТОД ВИРІШЕННЯ ЗАВДАННЯ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ СИСТЕМ УПРАВЛІННЯ РІЗНОРІДНИМИ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Gorohovskyy E.P. The method of solving the problem of multi-objective optimization of control system of telecommunications networks. In the article the solution of multi-objective optimization of management systems for telecommunications networks to ensure optimal performance of quality control that most affect the efficiency of the network. The described solution of vector optimization based on analysis of Pareto. The problem of optimal synthesis is the choice of control variables X , which are permitted area and provide optimal value characteristics $CS Q(X)$. Identified priorities vector synthesis, provides guidance on the selection range of quality, its quantity. It is shown that the main objective in the design of control systems and reduce their costs is to minimize the number of managing information. The problem minimax method of finding the minimum number of managing information in a linear programming problem. Private shown the determination criteria using linear programming methods.

Keywords: system management, optimization, vector optimization controlled objects minimization objective function.

Гороховський Є.П. Метод вирішення завдання багатокритеріальної оптимізації систем управління різномірними телекомунікаційними мережами. У статті пропонується рішення задачі багатокритеріальної оптимізації систем управління телекомунікаційними мережами для забезпечення оптимальних показників якості управління, що найбільш впливають на ефективність функціонування мережі. Описані рішення задачі векторної оптимізації на основі аналізу множин Парето. Визначені першочергові завдання векторного синтезу, даються рекомендації щодо вибору спектру показників якості, їх кількості. Показано, що основним завданням при проектуванні систем управління та зменшення їх вартості є мінімізація кількості управляючої інформації. Приведені визначення приватних критеріїв за допомогою методів лінійного програмування.

Ключові слова: система управління, оптимізація, векторна оптимізація, контрольовані об'єкти, мінімізація, цільова функція.

Гороховский Е.П. Метод решения задачи многокритериальной оптимизации систем управления разнородными телекоммуникационными сетями. В статье предлагается решение задачи многокритериальной оптимизации систем управления телекоммуникационными сетями для обеспечения оптимальных показателей качества управления, наиболее влияющих на эффективность функционирования сети. Описаны решения задачи векторной оптимизации на основе анализа множества Парето. Определены первоочередные задачи векторного синтеза, даются рекомендации по выбору спектра показателей качества, их количества. Показано, что основной задачей при проектировании систем управления и уменьшение их стоимости является минимизация количества управляющей информации. Приведенные определения частных критериев с помощью методов линейного программирования.

Ключевые слова: система управления, оптимизация, векторная оптимизация, контролируемые объекты, минимизация, целевая функция.

Вступ

У сучасній науково-технічній літературі розглянуті методи багатокритеріальної оптимізації систем управління (СУ) телекомунікаційними мережами [1 - 9]. Описано особливості СУ як складної системи. Визначено основні критерії (показники) якості які найбільш впливають на ефективність управління мережами. Розроблено методи об'єднання суперечливих критеріїв і визначення узагальненого критерію. Рішення задачі оптимального синтезу полягає у виборі керуючих змінних X , які належать допустимій області та забезпечують оптимальне значення характеристик СУ $Q(X)$.

Виклад основного матеріалу дослідження

Як відомо, характеристика, яка показує відносну перевагу одного варіанта в порівнянні з іншим, називається критерієм оптимальності (цільовою функцією, критерієм ефективності, функцією корисності і т. п.).

Екстремальне значення критерію оптимальності $Q(X)$ (кількісне значення) може бути отримано в залежності від конкретного завдання максимуму або мінімуму цієї функції.

Оптимізація систем управління, як правило, ведеться за кількома критеріями. Має місце задача векторної оптимізації

$$l(q) \rightarrow \min_{q \in Q}.$$

Компоненти l_i векторного критерію I називаються приватними критеріями (показниками). Результати мінімізації приватних критеріїв в загальному випадку не збігаються. На рис. 1 ілюструється завдання мінімізації двох приватних критеріїв $l_1(q)$, $l_2(q)$ які залежать від одного параметра. Оскільки оптимальні значення параметрів не збігаються, тобто $q_1^* \neq q_2^*$, то виникає питання, що слід вважати рішенням завдання векторної оптимізації.

За визначенням, рішенням завдання векторної оптимізації є множина значень параметрів, де зміна будь-якого параметра з метою поліпшення одного з приватних критеріїв обов'язково погіршує хоча б один інший. Таку множину непокрощуючих рішень називають множиною Парето.

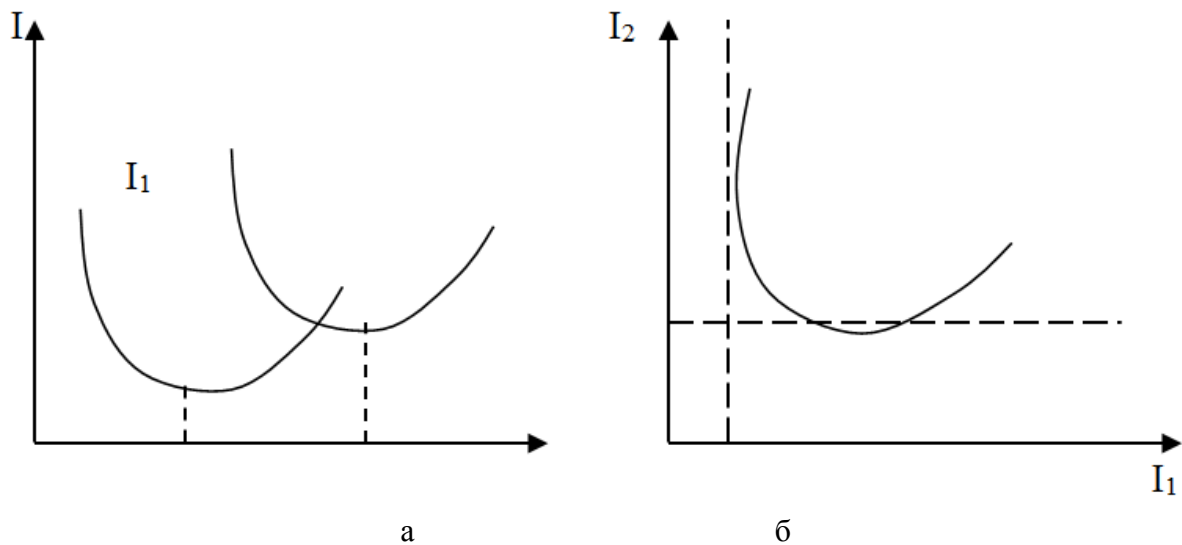


Рис. 1. Ілюстрація завдання векторної оптимізації

На рис. 1, а області Парето на осі параметра q відповідає відрізок між значеннями q_1^* і q_2^* приватних оптимумів. Тут зміна q з метою зменшення одного показника призводить до збільшення іншого показника. Інша ілюстрація області Парето приведена на рис. 1, б, де по осях відкладені значення приватних показників $l_1(q)$ і $l_2(q)$.

Для кожного критерію $Q_1(X)$, $Q_2(X)$, ..., $Q_s(X)$ необхідно знайти вектор, $\bar{X} = (x_1, x_2, \dots, x_n)$ який забезпечує мінімальне (максимальне) значення критерію оптимальності:

$$Q_i(x_1, x_2, \dots, x_n) \geq 0, i = \overline{1, m};$$

$$x_j^- \leq x_j \leq x_j^+, j = \overline{1, n}.$$

Таким чином, рішення задачі оптимізації може бути зведено до вирішення умови оптимізації - тобто визначення оптимального значення X^* і знаходження мінімального (максимального) значення критерію оптимальності.

Для СУ доцільно за допомогою методу експертних оцінок визначити наступні приватні критерії:

$Q_1(X)$ - функція, що характеризує кількість керуючої інформації при забезпеченні необхідного спектра послуг;

$Q_2(X)$ - функція, що характеризує затримку керуючої інформації при певній кількості контрольованих об'єктів і швидкодії центрів комутації пакетів СУ;

$Q_3(X)$ - функція, що характеризує достовірність інформації, що передається;

$Q_4(X)$ - функція, що характеризує надійність структури при заданих обмеженнях;

$Q_5(X)$ - функція, що характеризує вартість СУ з урахуванням всіх перерахованих властивостей.

Відзначимо, що екстремальне значення критерію оптимальності $Q(X)$ (кількісне значення) характеризує одне з найважливіших властивостей СУ.

Взагалі при векторному синтезі першочерговим завданням є вибір як спектра показників якості, так і їх кількості. Якщо при виборі критеріїв нехтувати хоча б один показник, який значно впливає на якість СУ, то природно ми не отримаємо ефективне рішення. А якщо їх буде занадто багато, то це призведе не до поліпшення, а до погіршення результатів синтезу.

Реалізуючи векторний синтез, будемо вважати оптимальною систему управління, яка забезпечує виконання умов:

$$K_p = \min f_p(\kappa_1, \dots, \kappa_i, \dots, \kappa_m), \quad (1)$$

$$\kappa_i \leq \overline{\kappa_{im}}, i = \overline{1, m},$$

де κ_{im} - значення показника якості максимально допустиме з точки зору вимог замовника; m - множина, якій належать допустимі параметри системи S .

Мінімаксний критерій представимо в наступному вигляді:

$$K_p = \min f_p(\kappa_1, \kappa_2, \kappa_3, \kappa_4). \quad (2)$$

Тоді цільова функція при переході до нормованих критеріїв має вигляд

$$f_p = [C_1 \kappa_1; C_2 \kappa_2; C_3 \kappa_3; C_4 f(\kappa_3)] = \min \left[C_1 \frac{\kappa_1}{\kappa_{1m}}; C_2 \frac{\kappa_2}{\kappa_{2m}}; C_3 \frac{\kappa_3}{\kappa_{3m}}; C_4 f\left(\frac{\kappa_3}{\kappa_{3m}}\right) \right], \quad (3)$$

де $\kappa_4 = f(\kappa_3)$.

Для вирішення таких завдань мінімаксним методом необхідно розглянути допустимі варіанти зміни критеріїв від мінімально можливих до максимально допустимих значень і, відповідно, вибрати варіант, що забезпечує мінімум цільової функції.

Найбільш прийнятний метод - це метод ітерації.

Таким чином, необхідно визначити як максимально допустимі значення критеріїв, так і мінімальні. Якщо перші, як зазначалося вище, визначаються замовником, то другі за допомогою відомих методів лінійного програмування.

У загальному вигляді задача оптимізації за одним показником якості може бути представлена:

$$\left. \begin{aligned} \kappa_1 &= F_1(x_1, \dots, x_n) = \min \\ \kappa_2 &= F_2(x_1, \dots, x_n) \leq \kappa_{2M} \\ &\text{-----} \\ \kappa_m &= F_m(x_1, \dots, x_n) \leq \kappa_{mM} \end{aligned} \right\} \quad (4)$$

(у виконанні всіх інших умов і обмежень, накладених на систему). В цьому випадку цільові функції $F_2 = (x_1, \dots, x_n), \dots, F_m(x_1, \dots, x_n)$ грають роль функцій обмежень $F_j = (x_1, \dots, x_n)$.

Таким чином, для кожного окремого критерію, що входить в формулу (3), необхідно знайти рішення вираження (3).

Розглянемо, наприклад, рішення задачі (4) для таких критеріїв, як мінімум керуючої інформації.

Припустимо, при організації СУ доцільно закріпити контрольовані об'єкти (КО) за даними медіатора, або SMS (операційною системою).

Різниця об'єктів полягає в тому, що в процесі управління інформаційні потоки, що виникають в результаті взаємодії КО і операційної системи, можуть бути залежні або незалежні між собою.

Характер інформаційних потоків залежить від призначення КО і можливих несправностей, які виявляються СУ в процесі функціонування. Деякі несправності діють на генерацію інформаційних потоків таким чином, що вони залежні, тобто зміни одного параметра тягне несправність іншого.

Природно, якщо інформаційні потоки, які генеруються компонентами КО і SMS (або медіатором) залежні, то кількість керуючої інформації значно зменшується. Це відбувається за рахунок того, що сумарна кількість інформації для залежних повідомлень завжди менше, ніж для незалежних.

Основним завданням при проектуванні СУ є, як відомо, мінімізація кількості керуючої інформації, що значно зменшує вартість СУ.

Це завдання можна вирішити методом лінійного програмування. Для цього необхідно розподілити навантаження на SMS і медіатори таким чином, щоб мінімізувати інформаційні потоки, що виникають між ними за рахунок певного розподілу КО і SMS.

Розглянемо задачу знаходження мінімуму кількості керуючої інформації у вигляді задачі лінійного програмування. Припустимо, що кількість видів КО дорівнює L . Відповідно, результат розрахунку кількості керуючої інформації розподілиться на два види I_1 і I_1' (I_1 - це сумарна кількість керуючої інформації, яка відповідає незалежним інформаційним потокам, а I_1' - залежним).

Кількість інформації, що управляє, необхідної для даної ділянки мережі, представлено в табл. 1.

Математично це завдання представимо у вигляді нерівностей

$$\left. \begin{aligned} I_1 x_1 &\leq L_1 \quad (KO_1); \\ I_1' x_2 &\leq L_1' \quad (KO_1'); \\ I_2 x_1 &\leq L_2 \quad (KO_2); \\ I_2' x_2 &\leq L_2' \quad (KO_2'); \\ I_3 x_1 &\leq L_3 \quad (KO_3); \\ I_3' x_2 &\leq L_3' \quad (KO_3'); \\ I_4 x_1 &\leq L_4 \quad (KO_4); \\ I_4' x_2 &\leq L_4' \quad (KO_4'). \end{aligned} \right\} \quad (5)$$

При умові (5) загальна кількість керуючої інформації складе

$$F = Ix_1 + I'x_2. \quad (6)$$

Необхідно серед невід'ємних розв'язків системи (S) вибрати таке, при якому форма F приймає найменше значення.

Уявімо з точки зору лінійного програмування рішення задачі знаходження мінімуму затримки керуючої інформації. Це питання для СУ є актуальним, так як транспортна мережа, яка використовується СУ це мережа з комутацією пакетів X.25.

Таблиця 1

Види КО	Параметри КО	Середнє квадратичне відхилення параметрів КО від норми		Кількість управляючої інформації	
		До включення СУ	Необхідне	Для незалежних потоків	Для залежних потоків
S ₁	П ₁₁	σ_{11}	σ_{11}'	I ₁₁	I ₁₁ '
	П ₁₂	σ_{12}	σ_{12}'	I ₁₂	I ₁₂ '
	П ₁₃	σ_{13}	σ_{13}'	I ₁₃	I ₁₃ '
	П ₁₄	σ_{14}	σ_{14}'	I ₁₄	I ₁₄ '
S ₂	П ₂₁	σ_{21}	σ_{21}'	I ₂₁	I ₂₁ '
	П ₂₂	σ_{22}	σ_{22}'	I ₂₂	I ₂₂ '
	П ₂₃	σ_{23}	σ_{23}'	I ₂₃	I ₂₃ '
	П ₂₄	σ_{24}	σ_{24}'	I ₂₂	I ₂₂ '
S ₃	П ₃₁	σ_{31}	σ_{31}'	I ₃₁	I ₃₁ '
	П ₃₂	σ_{32}	σ_{32}'	I ₃₂	I ₃₂ '
	П ₃₃	σ_{33}	σ_{33}'	I ₃₃	I ₃₃ '
	П ₃₄	σ_{34}	σ_{34}'	I ₃₄	I ₃₄ '
S ₄	П ₄₁	σ_{41}	σ_{41}'	I ₄₁	I ₄₁ '
	П ₄₂	σ_{42}	σ_{42}'	I ₄₂	I ₄₂ '
	П ₄₃	σ_{43}	σ_{43}'	I ₄₃	I ₄₃ '
	П ₄₄	σ_{44}	σ_{44}'	I ₄₄	I ₄₄ '
	П ₄₅	σ_{45}	σ_{45}'	I ₄₅	I ₄₅ '
Сумарна кількість управляючої інформації				I	I'

Основні дані, необхідні для складання цільової функції, представлені в табл. 2, де UC_{ij} - кількість вузлів мережі з комутацією пакетів однієї продуктивності П1, а П2 - іншої. Припустимо, що П1 вище П2, тоді і затримка T_{ij} нижче, ніж T'_{ij} .

Таблиця 2

Види вузлів	Кількість центрів комутації пакетів для даного вузла		Затримка переданої інформації	
	Продуктив. П1	Продуктив. П2	T	T'
S_1	YC_{ij}	YC_{ij}'	T_{11}	T_{11}'
	YC_{12}	YC_{12}'	T_{12}	T_{12}'
	YC_{13}	YC_{13}'	T_{13}	T_{13}'
	YC_{14}	YC_{14}'	T_{14}	T_{14}'
S_2	YC_{21}	YC_{21}'	T_{21}	T_{21}'
	YC_{22}	YC_{22}'	T_{22}	T_{22}'
	YC_{23}	YC_{23}'	T_{23}	T_{23}'
	YC_{24}	YC_{24}'	T_{24}	T_{24}'
S_3	YC_{31}	YC_{31}'	T_{31}	T_{31}'
	YC_{32}	YC_{32}'	T_{32}	T_{32}'
	YC_{33}	YC_{33}'	T_{33}	T_{33}'
	YC_{34}	YC_{34}'	T_{34}	T_{34}'
S_4	YC_{41}	YC_{41}'	T_{41}	T_{41}'
	YC_{42}	YC_{42}'	T_{42}	T_{42}'
	YC_{43}	YC_{43}'	T_{43}	T_{43}'
	YC_{44}	YC_{44}'	T_{44}	T_{44}'
Сумарна затримка			T	T'

Необхідно розподілити вузли комбінації таким чином, щоб сумарна затримка передачі керуючої інформації між КО і SMS була мінімальною.

Математично завдання знаходження мінімуму затримки керуючої інформації представимо у вигляді:

$$\left. \begin{aligned} T_1 x_1 &\leq L_1(S_1); \\ T_1' x_2 &\leq L_2'(S_1'); \\ T_2 x_1 &\leq L_2(S_2); \\ T_2' x_2 &\leq L_2'(S_2'); \\ T_3 x_1 &\leq L_3(S_3); \\ T_3' x_2 &\leq L_3'(S_3'); \\ T_4 x_1 &\leq L_4(S_4); \\ T_4' x_2 &\leq L_4'(S_4'). \end{aligned} \right\} \quad (7)$$

При цих умовах загальне значення затримки переданої інформації складе

$$F = T x_1 + T' x_2 \quad (8)$$

Необхідно серед невід'ємних розв'язків системи (7) вибрати таке, при якому F приймає найменше значення [7, 8].

Висновки

У статті пропонується рішення задачі багатокритеріальної оптимізації систем управління телекомунікаційними мережами для забезпечення оптимальних показників якості управління, що найбільш впливають на ефективність функціонування мережі. Описані рішення задачі векторної оптимізації на основі аналізу множин Парето. Визначені першочергові завдання векторного синтезу, даються рекомендації щодо вибору спектру показників якості, їх кількості. Показано, що основним завданням при проектуванні систем управління та зменшення їх вартості є мінімізація кількості управляючої інформації. Приведені визначення приватних критеріїв за допомогою методів лінійного програмування.

Список використаної літератури

1. Стеклов В.К., Беркман Л.Н. Проективання телекомунікаційних мереж. – К.: Техніка, 2002. – 792 с.
2. Стеклов В.К., Беркман Л.Н., Лев Ю.О., Мніщенко С.І. Постановка задачі оцінки обсягу управляючої інформації у системі управління інтелектуальною мережею // Одеса: Інформатика и связь. – 1996. – №1. – С. 75-87.
3. Стеклов В.К., Беркман Л.Н. Системный метод оптимального проектирования интеллектуальной сети // Зв'язок. – 1998. – №4. – С. 28-32.
4. Стеклов В.К., Карпенко Н.Ф., Беркман Л.Н. Многокритериальная оптимизация систем управления телекоммуникационными сетями // Зв'язок. – 1999. – №6. – С. 26-28.
5. Стеклов В.К., Беркман Л.Н. Оценка объёма управляющей информации в информационных сетях // Электросвязь. – 2000. – № 6. – С. 34-37.
6. Стеклов В.К., Беркман Л.Н., Иванов А.И. Метод определения задержки управляющей информации в системах управления телекоммуникационными сетями // Зв'язок. – 2001. – №1. – С. 49-51.
7. Стеклов В.К., Стародуб Н.М. Беркман Л.Н. Выбор обобщённого критерия оптимальности систем управления информационными сетями // Зв'язок.-2000.-№5. – С. 48-50.
8. Стеклов В.К., Стародуб Н.М. Беркман Л.Н., Объединение векторных критериев оптимальности систем управления телекоммуникационными сетями // Матеріали доповідей учасників Ювілейної міжнародної науково-практичної конференції. – К.: тов. “Знання України”. – 2000. – С. 90-92.
9. Имаев Д.Х., Краснопрошина А.А., Яковлев В.Б. Теория автоматического управления. ч.1.: Учебник для вузов – К.: Вища школа, 1992 – 248 с.

Автори статті

Гороховський Євген Петрович - здобувач, старший викладач кафедри телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна.

Authors of the article

Gorohovskyy Evgen Petrovych - applicant, senior lecturer of Department of Telecommunication systems, State university of telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 02.02.2017 р.

Рецензент: д.т.н., проф. Л.Н. Беркман

УДК 621.396.662.072.078

Сайко В.Г., д.т.н., Лисенко Д.О., аспірант; Грищенко Л. М., аспірант;
Дакова Л.В., аспірант; Кравченко В.І., аспірант

АЛГОРИТМ АДАПТАЦІЇ РАДІОСИСТЕМИ ДО СЕРЕДНЬОСТАТИСТИЧНИХ ЗМІН ПАРАМЕТРІВ РАДІОКАНАЛУ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ

Saiko V.H., Lysenko D.O., Hryshchenko L.M., Dakova L.V., Kravchenko V.I. **Radio system adaptation algorithm to average changes of parameters of the terahertz radio channel.** This paper presents ways to reduce the likelihood of erroneous data reception in the terahertz fading radio channels. But this approach to determine the low-loss transmission windows, from our point of view, is not rational. It can be explained by the fact that at the fixed limit threshold level the utilization factor of radio channel will be variable and therefore efficiency of low-loss transmission windows will also be variable. Therefore it was proposed a new adaptive model with variable threshold level. It can be explained by the fact that at the fixed limit threshold level the utilization factor of radio channel will be variable and therefore efficiency of low-loss transmission windows will also be variable. Therefore it was proposed a new adaptive model with variable threshold level. It allows at change of signal to noise ratio to maintain a constant given utilization factor of radio channel and therefore transmission speed. On the basis of the developed and probable model, in this article the mechanism of adaptation of mobile system functioning mode to the average changes of the parameters of terahertz wireless links, which allows to provide an optimal selection of frequency bands or low-loss transmission windows.

Keywords: low-loss transmission windows, radio channel, terahertz band, propagation medium of radio waves, adaptive analyzer

Сайко В.Г., Лисенко Д.О., Грищенко Л.М., Дакова Л.В., Кравченко В.І. **Алгоритм адаптації радіосистеми до середньостатистичних змін параметрів радіоканалу терагерцового діапазону.** В статті на основі ймовірної моделі [1] запропоновано спосіб зниження ймовірності помилкового приймання даних в радіоканалах терагерцового діапазону, який дозволить забезпечити оптимальний вибір частотних діапазонів або вікон прозорості. В залежності від вимог необхідних додатків можна зробити раціональний вибір параметрів радіосистем, які відповідатимуть критеріям пропускної здатності і дальності зв'язку цих додатків.

Ключові слова: вікна прозорості, радіоканал, терагерцовий діапазон, середовище розповсюдження радіохвиль, адаптивні аналізатори

Сайко В.Г., Лисенко Д.А., Грищенко Л.Н., Дакова Л.В., Кравченко В.И. **Алгоритм адаптации радиосистемы к среднестатистическим изменениям параметров радиоканала терагерцового диапазона.** В статье на основе предполагаемой модели [1] предложен способ снижения вероятности ложного приема данных в радиоканалах терагерцового диапазона, который позволит обеспечить оптимальный выбор частотных диапазонов или окон прозрачности. В зависимости от требований необходимых приложений можно сделать рациональный выбор параметров радиосистем, отвечающих критериям пропускной способности и дальности связи данных приложений.

Ключевые слова: окна прозрачности, радиоканал, терагерцовый диапазон, среда распространения радиоволн, адаптивные анализаторы

Вступ

Постановка задачі. Основними вимогами, що пред'являються до мобільних систем радіозв'язку нового покоління, є висока швидкість і надійність передачі даних великій кількості користувачів в складних умовах поширення сигналів. Для практичної реалізації цих вимог розробники здебільшого приділяють велику увагу найбільш перспективним шляхам побудови мереж мобільного зв'язку четвертого і п'ятого поколінь (4G і 5G) використанню телекомунікаційних систем цифрового радіозв'язку терагерцового діапазону та переходу на малі стільники (мікростільники, пікосоти і фемтосоти), які являють собою базові станції з обмеженим діапазоном дії і встановлюються для розширення зони покриття базових станцій макрорівня. На сьогоднішній день дослідження для таких мобільних систем сфокусовано переважно на збільшенні пропускної здатності каналу зв'язку при використанні

надширококустових сигналів, що займають весь терагерцовий діапазон [2]. Однак, варто зазначити, що в багатьох перспективних додатках для мереж 5-го покоління дальність зв'язку відіграє більш значиму роль, ніж швидкість передачі даних. Таким чином, розробка методики збільшення радіусу дії окремого вузла зв'язку терагерцового діапазону є досить важливою науковою задачею.

Мета роботи полягає в зниженні ймовірності помилкового приймання даних в радіоканалах терагерцового діапазону із замираннями завдяки застосуванню алгоритму адаптації режиму роботи систем до середньостатистичних змін параметрів радіолінії систем мобільного зв'язку в залежності від рівня порога при фіксованих значеннях потужності передавача і середньої величини відношення сигнал/шум.

Для подальшого дослідження можливостей використання радіохвиль ТГц діапазону в радіотехнічних системах (РТС), насамперед виконаємо аналіз результатів досліджень [3-5] молекулярного поглинання в атмосфері і гідрометеорах досліджуваних радіохвиль.

1. Особливості приймання і передачі сигналів в терагерцовому діапазоні

З [3-5] відомо, що при функціонуванні радіотехнічних систем (РТС) в атмосфері енергія електромагнітних коливань під час поширення послаблюється експоненціально за законом Бугера. Тому для визначення реальної дальності дії РТС необхідно отримати дані щодо коефіцієнту сумарного поглинання і ослаблення, а також його розподілу в просторі і в часі. У зв'язку з цим доцільно проаналізувати особливості поширення терагерцових радіохвиль в атмосфері, в дощах, туманах і пилодимових завадах.

Згідно з [3,4] повний коефіцієнт поглинання і ослаблення можна подати у вигляді суми виду:

$$\gamma_{\text{ноз.}} = \gamma_{H_2O} + \gamma_{O_2} + \gamma_D + \gamma_T + \gamma_O + \gamma_{MS} + \gamma_S \quad (1)$$

де γ_{H_2O} - коефіцієнт поглинання у водяній парі; γ_{O_2} - коефіцієнт поглинання в кисні; γ_D - коефіцієнт ослаблення в дощі; γ_T - коефіцієнт ослаблення в тумані; γ_O - коефіцієнт ослаблення в хмарах; γ_{MS} - коефіцієнт поглинання в мокрому снігу; γ_S - коефіцієнт поглинання в сухому снігу.

При цьому необхідно зазначити, що одна з основних проблем в мікрохвильовому діапазоні пов'язана з розходженням електромагнітних хвиль при видаленні від випромінювача через дифракції. З теорії антен відомо, що потужності і передавальної і приймальної антен пов'язані між собою:

$$P_1 = P_2 \left(\frac{\lambda}{4\pi d} \right)^2 G_2 G_1 F_2(\theta_2, \varphi_2) F_1(\theta_1, \varphi_1) \tau \xi \quad (2)$$

де G - направленість; F - функція розподілу нормованої інтенсивності поля; d - відстань між антенами; τ - коефіцієнт передачі потужності; ξ - поляризаційний коефіцієнт передачі; θ та φ - сферичні координати.

Зі зростанням відстані від передавальної антени через кутове розходження поперечний переріз пучка електромагнітних променів збільшується пропорційно квадрату відстані і квадрату кута розходження. Тому на великій відстані від джерела електромагнітна енергія розтікається вздовж дедалі зростаючої площі, і на одиницю площі припадає частка загальної електромагнітної енергії, яка дедалі зменшується.

Для випадку ідеального узгодження приймальної та передавальної антен рівняння (2) можна замінити іншим виразом:

$$P_1 = P_2 \frac{S_1 S_2}{d^2 \lambda^2} F_2(\theta_2, \varphi_2) F_1(\theta_1, \varphi_1) \tau \xi \quad (3)$$

где S_1 и S_2 - ефективна площа передавальної та приймальної антен.

Зі співвідношення (3) видно, потужність, що приймається, тим більше, чим вище λ , отже, в терагерцовому діапазоні ефективність передачі електромагнітного випромінювання

зростає в порівнянні з мікрохвильовим. В [6] з використанням (3) було проведено оціночні розрахунки для двох комунікаційних систем з робочими частотами 60 і 400 ГГц. Незважаючи на те, що терагерцеві джерела поступаються за потужністю мікрохвильовим, при передачі сигналу на відстань до 2 км цей недолік було скомпенсовано більш високою направленістю.

Проведений аналіз досліджень питань поширення радіохвиль в терагерцевому діапазоні [1,3-7] дозволив сформулювати наступні висновки.

1. Особливостями поширення радіохвиль в атмосфері, в тому числі і в гідрометеорах (дощ, туман, сніг) є наявність в ТГц діапазоні цілої низки ділянок спектра (1,3 мм; 0,98 мм і 0,88 мм). Ослаблення для зазначених довжин хвиль становить: 2 дБ/км, 7 дБ/км і 13 дБ/км відповідно, що дозволяє використовувати ці ділянки спектра в радіотехнічних системах.

2. Ослаблення в туманах в ТГц діапазоні хвиль при водності $0,1 \text{ г/м}^3$, в порівнянні з дощами, невелике і не перевищує 2 дБ/км.

3. Ослаблення поширення ТГц хвиль в снігу не піддається суворій теоретичній оцінці. Однак відомо, що воно приблизно є вдвічі меншим, ніж в дощах з інтенсивністю менше 5 мм/год.

Найбільш придатними для освоєння під мобільні телекомунікаційні системи є вікна прозорості, які можна визначити за певним рівнем загасання. Згідно з [7], таким граничним рівнем може бути 100 дБ/км. Тоді маємо п'ять вікон прозорості і пропускну здатність у смугах вікон терагерцового діапазону може досягати сотень Гбіт/с. Причому, чим менша відстань радіотраси, тим меншого впливу зовнішніх факторів і тим більшої пропускну здатності можна досягати.

Але цей підхід для визначення вікон прозорості, з нашої точки зору, не є раціональним. Це зумовлено тим, що за фіксованого граничного рівня порога коефіцієнт використання радіоканалу буде змінним і, відповідно, ефективність використання вікна прозорості також буде змінною. Тому в [1] було запропоновано нову адаптивну модель зі змінним рівнем порогу. Вона дозволяє при зміні відношення сигнал/шум підтримувати постійний заданий коефіцієнт використання радіоканалу і, відповідно, швидкість передачі даних.

На основі ймовірної моделі [1], в даній статті запропоновано механізм адаптації режиму роботи системи до середньостатистичних змін параметрів радіолінії терагерцового діапазону, який дозволяє забезпечити оптимальний вибір частотних діапазонів або вікон прозорості. Сутність методики полягає у визначенні оптимальних значень параметрів засобів радіозв'язку нового покоління для забезпечення надійного зв'язку каналу зв'язку терагерцового діапазону між приймачем і передавачем під час функціонування в умовах низьких відношень сигнал-шум у вікнах прозорості та забезпечення необхідної якості приймання.

2. Сутність механізму адаптації режиму роботи системи до середньостатистичних змін параметрів радіоканалу в терагерцевому діапазоні

Критерій оцінки ступеня впливу дисперсійних властивостей середовища розповсюдження радіохвиль на стійкість каналу. В умовах замирань сигналу контроль поточного стану радіоприймання (якість каналу) доцільно оцінювати через відношення середньої тривалості інтервалів $\bar{t}_p$ стійкої роботи каналу до середньої тривалості інтервалів $\bar{t}_z$ замирань сигналу. Очевидно, що величина $w = \bar{t}_p / \bar{t}_z$ характеризує відносну стаціонарність каналу за якістю в умовах випадкових змін характеристик радіотрас. При цьому, як показують експериментальні дослідження трас мобільного радіозв'язку [8-10], параметр σ_A змінюється в межах $\sigma_A \approx (0.2...5)m_A$. Оскільки на середньо пересічній місцевості траси радіозв'язку протяжністю близько 2...5 км в переважній кількості випадків є закритими або напівзакритими, то для оцінки якості каналу справедливо обмежитися значеннями $\sigma_A \approx (1...5)m_A$. На рис. 1 наведено графічні залежності параметра, σ_A від

середнього співвідношення сигнал-шум, отримані шляхом аналітичного моделювання процесів поширення радіохвиль в середовищі, при різних значення параметра σ_A огинаючої сигналу. Прямолінійний характер графіків дозволяє із загальних статистичних позицій оцінювати очікувану на найближчий час якість каналу шляхом прогнозування.

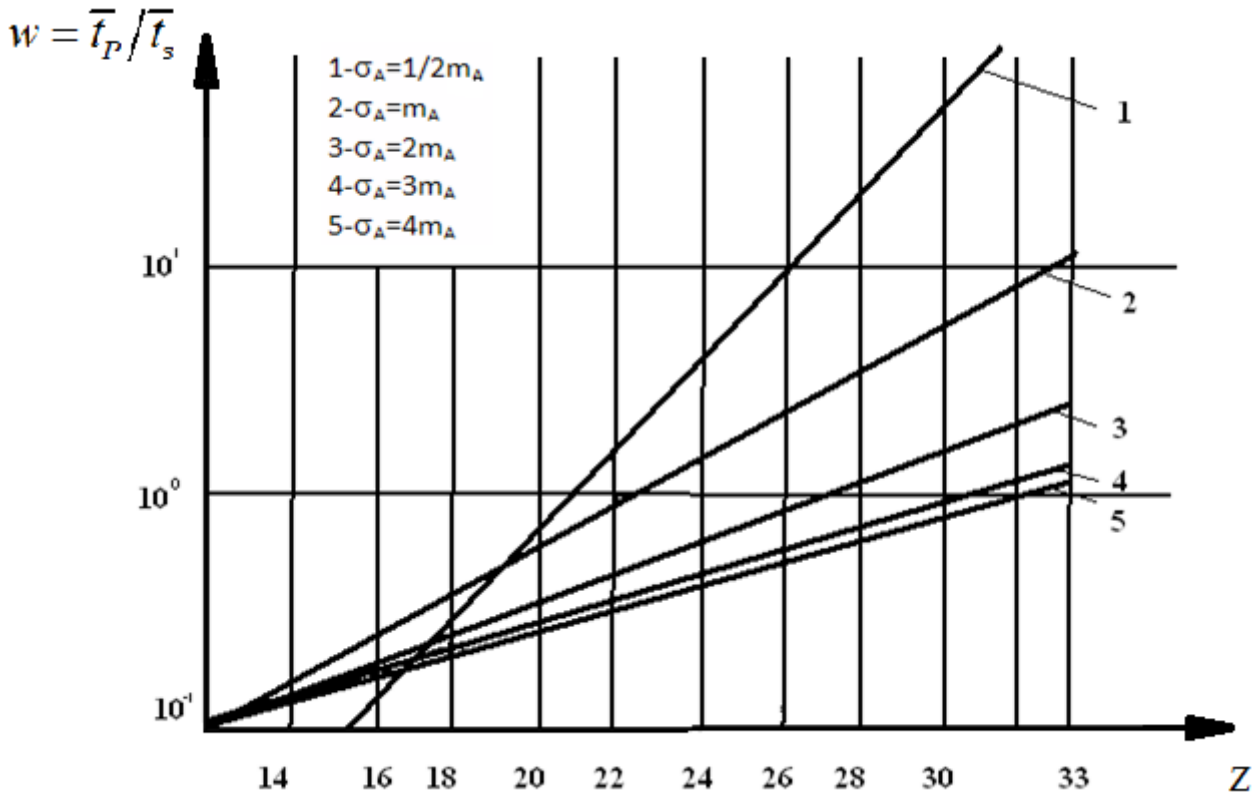


Рис. 1. Графічні залежності параметра w від середнього співвідношення сигнал-шум Z

З рис. 1 видно, що на відкритих трасах зв'язку [8] ($\sigma_A \approx 0,2 - 0,5 m_A$) збільшення енергетики радіоліній зумовлює істотне поліпшення якості каналу. Так, при збільшенні співвідношень сигнал-шум $\bar{Z}$ з 25 дБ до 36 дБ параметр w збільшується в сотні разів. Чим більше параметр σ_A , тим більше ослаблення сигналу в місці приймання за рахунок дифракції хвиль на великомасштабних компонентах траси зв'язку, ефекту затінення і багаторазового відбиття радіохвиль в процесі їх розповсюдження. Зменшення нахилу графіків при цьому вказує на можливість досягнення дедалі меншого відчутного виграшу в якості каналу шляхом збільшення співвідношення сигнал-шум.

Таким чином, критерієм оцінки ступеня впливу дисперсійних властивостей середовища розповсюдження на стійкість каналу може слугувати параметр $\theta = \operatorname{tg} \alpha$, α - кут нахилу графіків. Через характеристики каналу параметр θ виражається наступним чином (див. рис. 1):

$$\theta = \frac{\lg w_2 - \lg w_1}{\bar{Z}_2 - \bar{Z}_1}; w_i = \frac{\bar{t}_{pi}}{\bar{t}_{si}}; \bar{Z}_i = \frac{m_{Ai}}{U_{3+u}}; i=1, 2. \quad (4)$$

Звідки

$$\bar{Z}_2 = (\lg w_2 - \lg w_1 + \theta \bar{Z}_1) / \theta. \quad (5)$$

Для практичної реалізації алгоритму адаптації режиму роботи системи до середньостатистичних змін параметрів радіоканалу в терагерцовому діапазоні необхідно

розглянути також особливості побудови сучасних вимірювачів характеристик параметрів викидів випадкових процесів.

3. Особливості побудови адаптивних аналізаторів розподілу інтервалів перебування випадкового процесу всередині і поза заданими межами

Розглянемо стаціонарний випадковий процес $X(t)$, що перетинає в випадкові моменти часу фіксовані рівні x_1 і $x_2 \gg x_1$. Нехай $\lambda_1(x_1)$ – інтенсивність викидів процесу під (над) рівнем, відповідно $\lambda_1(x_2)$ – інтенсивність викидів над рівнем x_2 . Сумарне середнє число $\bar{N}$ інтервалів перебування процесу всередині заданих меж x_1 і x_2 за час T може бути знайдено через сумарну інтенсивність викидів:

$$\bar{N} = [\lambda_1(x_1) + \lambda_1(x_2)] \cdot T$$

Середній час $\bar{T}_{\text{преб.}}$ перебування всередині кордонів за час аналізу T :

$$\bar{T}_{\text{преб.}} = P(x_2 \geq x \geq x_1) \cdot T$$

де $P(x_2 \geq x \geq x_1) = \int_{x_1}^{x_2} W(x) dx$ – ймовірність попадання миттєвих значень процесу $X(t)$ між рівнями аналізу, $W(x)$ – щільність розподілу миттєвих значень.

Відповідно, середній час перебування процесу поза межами:

$$\bar{T}_{\text{непр.}} = T - \bar{T}_{\text{преб.}} = [1 - P(x_2 \geq x \geq x_1)]T$$

Звідси можна знайти середні тривалості інтервалів перебування процесу всередині і поза заданими межами:

$$\bar{\tau}_{\text{преб.}} = \frac{\bar{T}_{\text{преб.}}}{\bar{N}} = \frac{P(x_2 \geq x \geq x_1)}{\lambda_1(x_1) + \lambda_1(x_2)} \quad (9)$$

$$\bar{\tau}_{\text{непр.}} = \frac{\bar{T}_{\text{непр.}}}{\bar{N}} = \frac{1 - P(x_2 \geq x \geq x_1)}{\lambda_1(x_1) + \lambda_1(x_2)} \quad (10)$$

Як видно з (9) і (10), $\bar{\tau}_{\text{преб.}}$ та $\bar{\tau}_{\text{непр.}}$ залежать від розподілу миттєвих значень процесу, висоти відносних рівнів аналізу $\frac{x_1}{\sigma}$ і $\frac{x_2}{\sigma}$, ширини зони аналізу $\frac{x_2 - x_1}{\sigma}$, інтенсивності викидів над заданими рівнями, тобто ширини енергетичного спектра процесу. У загальному випадку, $\bar{\tau}_{\text{преб.}}$ та $\bar{\tau}_{\text{непр.}}$ можуть різко відрізнятися один від одного, тому вид щільності розподілу $W_{\text{преб.}}(\tau, x_1, x_2)$ та $W_{\text{непр.}}(\tau, x_1, x_2)$ очікується різним. Внаслідок цього і ширина диференціального коридору при експериментальному вимірі обох щільностей не може вибиратися однаковою. За аналогією з [11,12], оптимальна ширина диференціального коридору $(\Delta\tau)_{\text{opt}}$ після адаптації аналізатора повинна встановлюватися пропорційно середньому значенню вимірюваного інтервалу. А саме, необхідно задати:

$$(\Delta\tau)_{\text{преб.}} = k\bar{\tau}_{\text{преб.}}$$

$$(\Delta\tau)_{\text{непр.}} = k\bar{\tau}_{\text{непр.}}$$

Таким чином, за час адаптації аналізатора до випадкового процесу на його вході доцільно одночасно за двома паралельними каналами оцінити середні інтервали перебування процесу всередині і поза заданими межами і виробити оптимальні диференціальні коридори. Потім в процесі вимірювання функцій розподілу накопичити одночасно за двома каналами інформацію про інтервали перебування і не перебування, після чого одночасно закінчити вимірювання в момент накопичення певної кількості інтервалів перебування всередині заданих меж. По суті, даний адаптивний аналізатор складається з двох незалежних аналізаторів тривалості викидів, за аналогією з [11,12]. Деяким спрощенням є наявність

загальних блоків для обох каналів, таких як генератор, що задає лічильні імпульси, формувачі часу адаптації та вимірювань і низку інших.

4. Основні етапи алгоритму адаптації режиму роботи системи до середньостатистичних змін параметрів радіоканалу

1. Виконання вимірювань параметрів сигнал-шум Z_o для кожного активного в даний момент часу радіоканалу.

2. Виконання вимірювань параметрів квазіперіодів t_p та t_z зміни енергетичного стану середовища.

3. Визначення розрахункового значення параметра m_A сигналу в частотній області за оцінюванням залежності величини W від відношення сигнал-шум за різних можливих значеннях m_A (рис.1) як елементу заданої множини розрахункових значень параметра m_A сигналу, найбільш близького до знайденого m_A сигналу в частотній області;

4. Визначення розрахункового оптимального порогового значення k_{opt} і діапазону змінювання порога $k_{min} \dots k_{max}$ із залежності $U(\geq m, n) = f(k)$ [1], де $k = A / A_o$; A, A_o -- відповідний поточний (що приймається) і середній рівень сигналу.

5. Виконання вимірювань величини пакетної помилки для усіх можливих значень порогового рівня в діапазоні $k_{min} \dots k_{max}$ багаточастотної системи радіозв'язку;

6. Для кожного з виконаних вимірювань порівняння виміряної величини пакетної помилки з пороговою величиною, необхідною для забезпечення необхідної якості радіоканалу;

7. Виключення з подальшого аналізу тих вимірювань, для яких виміряна величина пакетної помилки менше порогової величини, необхідної для забезпечення необхідної якості радіоканалу;

- для кожного з виконаних вимірювань, крім виключених з аналізу:

8. Визначення результуючої ймовірності правильного приймання пакета багаточастотної системи радіозв'язку для кожного можливого значення порогової величини, крім виключених з розгляду, усереднюючи знайдену ймовірність правильного приймання пакета багаточастотної системи радіозв'язку за всіма виконаними вимірюваннями, крім виключених з аналізу;

9. Визначення оптимального значення порогової величини як порогової величини, за якої значення результуючої ймовірності правильного приймання пакета багаточастотної системи радіозв'язку є максимальним.

Висновки

Відмінною рисою зазначеної методики є поєднання аналітичних і імітаційних методів зі статистичними методами аналізу середовища реалізації радіоканалу в терагерцевому діапазоні, яке набуває особливого значення при побудові перспективних радіосистем для мереж 4-го і 5-го покоління в зазначеному діапазоні.

Таким чином, за допомогою розробленої методики можна визначити оптимальні смуги пропускання каналу (вікна прозорості) для практичної реалізації і, відповідно, в залежності від вимог використовуваних додатків можна зробити раціональний вибір параметрів, які відповідають критеріям пропускну здатності і дальності зв'язку цих додатків.

Список використаної літератури

1. Сайко В.Г. Метод визначення оптимальних параметрів вікон прозорості в терагерцевому діапазоні // Сайко В.Г., Грищенко Л.М., Дакова Л.В., Лисенко Д.О., Кравченко В.І.// Телекомунікаційні та інформаційні технології. –2017.-- № 1.

2. Самоорганизующиеся радиосети с сверхширокополосными сигналами: Монография / [Ильченко М.Е., Бунин С.Г., Войтер А.П., Романюк В.А.] – К.: НПП Издательство „Наукова думка” НАН Украины. – 2013. – с.444.
3. Быстров Р. П. Дальность действия миллиметровых радиолокационных станций в дождях / Р. П. Быстров, А. В. Соколов, Р. Н. Чеканов // Радиотехника. – М., 2005. – № 1. – С. 19–23.
4. Быстров Р.П., Соколов А.В. Распространение короткой части миллиметровых и субмиллиметровых волн: возможные области их применения. // Радиотехника, - № 5, - 2006. - С. 11-18.
5. Малышенко Ю.И. Оценка воздействия дождей на параметры радиолокационных станций микроволнового диапазона с учетом метеостатистических сведений о продолжительности выпадения дождей / Ю. И. Малышенко, Ю. В. Левадный // ИРЭ НАН Украины. – Радиофизика и электроника. – 2012. – т. 3(17), № 1. – с. 36-40.
6. Mann C.M. Towards terahertz communications systems, terahertz sources and systems / Ed by R. Miles et al. Amsterdam: Kluwer Academic. 2001.
7. Link budget considerations for THz Fixed Wireless links/ M. Grigat // IEEE Trans. on Terahertz science and technology. – 2012. – vol. 2, № 2. – p.567-572.
8. Связь с подвижными объектами в диапазоне СВЧ / Под ред. У.К. Джейкса: пер. с англ./ Под ред. М.С. Ярлыкова, М.В. Чернякова. – М.: Связь. – 1979. – 304 с.
9. Пономарев Г.А. Распространение УКВ в городе./ Пономарев Г.А., Куликов А.Н., Тельпуховский Е.Д. // Томск.: МП РАСКО.-- 1991.- 223с.
10. Сайко В.Г. Системи цифрового бездротового радіозв'язку нового покоління: монографія. – К.: ПП «Золоті ворота», 2011. – 300 с.
11. Фомин Я.А. Теория выбросов случайных процессов. – М.: Связь, 1980. – 216 с.
12. Тихонов В.И. Выбросы траекторий случайных процессов / Тихонов В.И. Хименко В.И. – М: Наука, 1987. - 305 с.

Автори статті

- Сайко Володимир Григорович** - доктор технічних наук, професор, завідувач кафедри радіотехнологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 044 249 25 04. E-mail: vgsaiko@gmail.com
- Лисенко Дмитро Олександрович** - аспірант кафедри радіотехнологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 067 959 02 38. E-mail: lysenko@ucrf.gov.ua
- Грищенко Людмила Миколаївна** - науковий співробітник кафедри радіотехнологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 093 672 65 40. E-mail: mila_1956@mail.ru
- Дакова Лариса Валеріївна** - аспірант кафедри радіотехнологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 099 905 31 23. E-mail: l_dakova@gmail.com.
- Кравченко Владислав Ігорович** - аспірант кафедри радіотехнологій, Державний університет телекомунікацій, м. Київ. Тел. +38 063 801 81 16. E-mail: vladislav_kravchenko@mail.ua

Authors of the article

- Sayko Volodymyr Hryhorovych** - doctor of sciences (technical), professor, head of Department of Radio technologies, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 044 249 25 04. E-mail: vgsaiko@gmail.com.
- Lysenko Dmytro Oleksandrovych** - post-graduate student of Department of Radio technologies, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 067 959 02 38. E-mail: lysenko@ucrf.gov.ua
- Hryshchenko Liudmyla Mykolaivna** - research assistant of Department of Radio technologies, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 093 672 65 40. E-mail: mila_1956@mail.ru
- Dakova Larysa Valeriivna** - postgraduate student of Department of Radio technologies, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 093 672 65 40. E-mail: l_dakova@gmail.com
- Kravchenko Vladyslav Ihorovych** - postgraduate student of Department of Radio technologies, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 063 801 81 16. E-mail: vladislav_kravchenko@mail.ua

Дата надходження в редакцію: 01.02.2017 р.

Рецензент: д.т.н., проф. М.М. Климаш

Бондаренко В.Є., д.т.н.; Бледнов О.В., студент

СУБ'ЄКТИВНО-ЙМОВІРНІСНА МОДЕЛЬ СИНТЕЗУ ЖИВУЧИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Bondarenko V.E., Blednov A.V. The subjective-probabilistic model of synthesis of surviving computer networks.

The computer network constantly feels the destructive influences of the environment where it works. Therefore, the actual problem is the development of survivable networks, resisted such influences.

The destructive influences on the network are, as a rule, is random. However, the evaluation of such random events, based on the classical probability theory, is difficult. Because such events are not systematic and do not have the mass character. But the mass character of an event is necessary for estimate its probability as the classical probability theory says.

This paper proposes a new model for synthesis survivable hierarchical computer networks. The model is formulated as the problem of nonlinear Boolean programming. The model uses subjective probabilities of survivability of the network's devices connection. The network is formed by the criterion of maximum survivability.

Keywords: survivability, subjective probability, modeling, computer networks, nonlinear Boolean programming.

Бондаренко В.Є., Бледнов О.В. Суб'єктивно-ймовірнісна модель синтезу живучих комп'ютерних мереж.

Комп'ютерна мережа весь час зазнає деструктивних впливів середовища, в якому вона функціонує. Тому, актуально стоїть проблема розробки живучих комп'ютерних мереж, які протидіють таким впливам, зберігаючи свою працездатність.

Деструктивні впливи на мережу носять, як правило, випадковий характер, але оцінка таких випадкових подій, на основі класичної теорії ймовірностей зустрічає серйозні труднощі, оскільки такі події є не систематичними і не носять масового характеру, що необхідно для оцінки частоти подій, яка визначає її класичну ймовірність.

В роботі пропонується нова модель синтезу живучої ієрархічної комп'ютерної мережі. Розроблена модель вкладається в рамки задачі нелінійного булевого програмування. Модель використовує суб'єктивні ймовірності працездатності підключення різних пристроїв мережі в умовах деструктивних впливів. Мережа формується за критерієм максимальної живучості (суб'єктивної ймовірності функціонування мережі при деструктивних впливах).

Ключові слова: живучість, суб'єктивна ймовірність, моделювання, комп'ютерні мережі, нелінійне булеве програмування.

Бондаренко В.Е., Бледнов А.В. Субъективно-вероятностная модель синтеза живучих компьютерных сетей.

Компьютерная сеть постоянно испытывает деструктивные воздействия среды, в которой она функционирует. Поэтому, актуально стоит проблема разработки живучих компьютерных сетей, противодействующих таким воздействиям, сохраняя свою работоспособность.

Деструктивные воздействия на сеть носят, как правило, случайный характер, но оценка таких случайных событий, на основе классической теории вероятностей встречает серьезные трудности, поскольку такие события являются не систематическими и не носят массовый характер, что необходимо для оценки частоты события, определяющей его классическую вероятность.

В работе предлагается новая модель синтеза живучей иерархической компьютерной сети. Разработанная модель укладывается в рамки задачи нелинейного булевого программирования. Модель использует субъективные вероятности работоспособности подключения различных устройств сети в условиях деструктивных воздействий. Сеть формируется по критерию максимальной живучести (субъективной вероятности функционирования сети при деструктивных воздействиях).

Ключевые слова: живучесть, субъективная вероятность, моделирование, компьютерные сети, нелинейное булево программирование.

Вступ

Комп'ютерна мережа весь час зазнає деструктивних впливів соціально-фізичного середовища, в якому вона функціонує. Тому актуально стоїть проблема розробки живучих комп'ютерних мереж [1], які здатні протидіяти таким впливам, зберігаючи свою працездатність.

© Бондаренко В.Є., Бледнов О.В., 2017

Деструктивні впливи на мережу носять, як правило випадковий характер, але для оцінки випадкових подій такого типу, використання класичної теорії ймовірностей зустрічає серйозні труднощі, оскільки такі дії є не систематичними і не носять масового характеру, що необхідно для оцінки частоти події, яка дає оцінку класичної ймовірності події.

Тому, в роботі запропонований новий підхід для оцінки стану мережі в залежності від випадкових ознак, які не носять масового характеру, але пов'язані з станами мережі і визначаються на основі знань групи експертів. Таку оцінку будемо називати суб'єктивною ймовірністю. На основі суб'єктивної ймовірності ознак, проводиться оцінка підключень обладнання мережі з точки зору живучості.

Входячи з оцінки підключень обладнання мережі, пропонується модель синтезу живучої комп'ютерної мережі, яка вкладається у рамки нелінійного булевого програмування.

Модель синтезу структури ієрархічної комп'ютерної мережі

Задачу синтезу структури ієрархічної комп'ютерної мережі за критерієм підвищеної живучості можна сформулювати так: знайти такі невідомі X_{ij} , які дають максимум функції живучості V мережі, де X_{ij} - невідомі елементи матриці підключень,

$$X_{ij} = \begin{cases} 1 & \text{— якщо } j \text{ — ий пристрій мережі підключений до } i \text{ — ого,} \\ 0 & \text{— якщо } j \text{ — ий пристрій мережі не підключений до } i \text{ — ого.} \end{cases}$$

$$V = \prod_{i=1}^n \prod_{j=1}^n c_{ij} X_{ij} \rightarrow \max, \quad (1)$$

де c_{ij} — корисність (суб'єктивна ймовірність живучості підключення j -го пристрою до i -го), n — кількість елементів мережі.

Якщо необхідно синтезувати мережу з заданим рівнем живучості a , то функція живучості матиме вигляд

$$V = \left(\prod_{i=1}^n \prod_{j=1}^n c_{ij} X_{ij} - a \right)^2 \rightarrow \min.$$

Якщо експерт або група експертів оцінюють ймовірність настання тієї або іншої випадкової події на основі досвіду, наявної інформації і інтуїції, а не частоти появи події, то така ймовірність називається суб'єктивною ймовірністю [2]. Суб'єктивна ймовірність має використовуватися коли випадкові події не носять масового характеру, що відбуваються в однакових умовах. До класу таких подій відносяться і деструктивні впливи на телекомунікаційні (комп'ютерні) мережі.

В роботі розглядається підхід до побудови суб'єктивної ймовірності того, що підключення j -го пристрою до i -го, яке базується на суб'єктивних оцінках зв'язку цього підключення і випадковими деструктивними ознаками, що спостерігаються в процесі функціонування мережі, буде мати необхідний рівень живучості.

Нехай є набір n станів $D_1, D_2, \dots, D_n$ підключення j -го пристрою до i -го. Наприклад, підключення повністю працездатне, повністю непрацездатне. Нехай є набір m ознак $k_1, k_2, \dots, k_m$, які супроводжують стани підключення. Наприклад, розрив кабелю, ураження комутатора.

Оскільки важко проводити числові статистичні експерименти з діючою складною системою, то для аналізу будемо використовувати суб'єктивні ймовірності. Такі ймовірності обчислюються на основі думки експертів.

Оцінка експертів формується у матрицю виду:

	D_1	D_2	$\dots$	D_n
D_1	1			
D_2		1		
$\dots$			1	
D_n				1

У клітці матриці заносяться оцінки експертів a_{ij} , які означають у скільки разів частіше стан D_i , яким помічений рядок матриці зустрічається частіше ніж стан D_j , яким помічений стовпець матриці. З такого визначення видно, що головна діагональ матриці має одиничні значення.

Таким чином, якщо $D_i = p D_j$, тобто стан D_i мережі зустрічається в p раз частіше стану D_j , то звідси маємо $D_j = 1/p D_i$.

Тобто, якщо оцінка $a_{ij} = p$, то $a_{ji} = 1/p$, а $a_{ii} = 1$.

Аналогічно матриці станів, експерти будують для кожного стану D_i системи матрицю ознак, де кожний рядок і стовпець матриці помічено ознаками $k_1, k_2, \dots, k_m$:

D_i	k_1	k_2	$\dots$	k_m
k_1	1			
k_2		1		
$\dots$			1	
k_m				1

Для матриці ознак, як і для матриці станів системи, мають місце співвідношення: $b_{ij} = p$, то $b_{ji} = 1/p$, а $b_{ii} = 1$.

У клітці матриці заносяться оцінки експертів b_{ij} , які означають у скільки разів частіше ознака k_i , якою помічений рядок матриці зустрічається у стані D_i частіше ніж ознака k_j , якою помічений стовпець матриці.

Для визначення суб'єктивної ймовірності, як станів, так і ознак у кожному стані, необхідно визначити власний вектор матриць і нормувавши його на одиницю, отримаємо суб'єктивну ймовірність.

Власний вектор $\{c_r\}_{r=1}^n$ приблизно можна обчислити за таким співвідношенням:

$$c_r = (a_{r1} \times a_{r2} \times \dots \times a_{rn})^{1/n},$$

де a_{ij} – елементи матриці станів, n – кількість станів системи.

Суб'єктивні ймовірності $P(D_i)$ для станів D_i обчислюються за формулою нормування

$$P(D_i) = \frac{c_i}{\sum_{i=1}^n c_i},$$

Умовні суб'єктивні ймовірності $P(k_i / D_j)$ присутності ознаки k_i , коли має місце стан D_j , обчислюються аналогічно обчисленням суб'єктивної ймовірності $P(D_i)$ для станів D_i .

Використовуючи формулу Баєса обчислимо суб'єктивні ймовірності станів складної системи, коли має місце множина ознак B .

$$P(D_i / B) = \frac{P(D_i)P(B / D_i)}{\sum_{j=1}^n P(D_j)P(B / D_j)},$$

де $B \subset k$ – підмножина множини ознак $k = \{k_1, k_2, \dots, k_m\}$.

Якщо деяка i -та ознака з множини B відсутня у стані системи D_j , то це означає, що її ймовірність $1 - P(k_i / D_j)$, де $P(k_i / D_j)$ – ймовірність присутності ознаки k_i коли має місце стан D_j .

Ймовірність $P(B / D_j)$, якщо всі ознаки з множини B присутні коли система знаходиться в стані D_j задається виразом

$$P(B / D_j) = P(k_1 / D_j) P(k_2 / D_j) \dots P(k_m / D_j).$$

Якщо деяка t -та ознака з множини B відсутня для стану D_j системи, то

$$P(B / D_j) = P(k_1 / D_j) P(k_2 / D_j) (1 - P(k_t / D_j)) \dots P(k_m / D_j).$$

Розглянемо простий приклад. Нехай експерти сформували матрицю станів деякої комп'ютерної мережі у такому вигляді:

	D ₁	D ₂	D ₃
D ₁	1	1/6	1/9
D ₂	6	1	1/9
D ₃	9	9	1

Тоді суб'єктивні ймовірності станів D_j розраховуються так.

$$c_1 = (a_{11} \times a_{12} \times a_{13})^{1/3} = (1 \times 1/6 \times 1/9)^{1/3} = 0,265;$$

$$c_2 = (a_{21} \times a_{22} \times a_{23})^{1/3} = (6 \times 1 \times 1/9)^{1/3} = 0,874;$$

$$c_3 = (a_{31} \times a_{32} \times a_{33})^{1/3} = (9 \times 9 \times 1)^{1/3} = 4,327.$$

$$c_1 + c_2 + c_3 = 0,265 + 0,874 + 4,327 = 5,46.$$

$$P(D_1) = c_1 / 5,46 = 0,05;$$

$$P(D_2) = c_2 / 5,46 = 0,15;$$

$$P(D_3) = c_3 / 5,46 = 0,8.$$

Нехай матриці ознак для кожного стану експерти задали у такому вигляді.

D ₁	k ₁	k ₂
k ₁	1	1/2
k ₂	2	1

D ₂	k ₁	k ₂
k ₁	1	1/1,5
k ₂	1,5	1

D ₃	k ₁	k ₂
k ₁	1	8
k ₂	1/8	1

Виконуючи розрахунки, аналогічні до розрахунків суб'єктивної ймовірності станів, отримаємо.

$$P(k_1 / D_1) = 0,33; P(k_2 / D_1) = 0,66; P(k_1 / D_2) = 0,4; P(k_2 / D_2) = 0,6;$$

$$P(k_1 / D_3) = 0,89; P(k_2 / D_3) = 0,11.$$

Визначимо ймовірність стану системи D_1 , якщо обидва показники k_1 і k_2 мають місце. $B = \{ k_1, k_2 \}$.

$$P(D_1 / B) = \frac{P(D_1) \cdot P(k_1 / D_1) \cdot P(k_2 / D_1)}{P(D_1) \cdot P(k_1 / D_1) \cdot P(k_2 / D_1) + P(D_2) \cdot P(k_1 / D_2) \cdot P(k_2 / D_2) + P(D_3) \cdot P(k_1 / D_3) \cdot P(k_2 / D_3)}.$$

$$P(D_1 / B) = 0,05 \times 0,33 \times 0,66 / (0,05 \times 0,33 \times 0,66 + 0,15 \times 0,4 \times 0,6 + 0,8 \times 0,89 \times 0,11) = 0,087;$$

Нехай $B_i \subset k = \{ k_1, k_2, \dots, k_m \}$ – підмножина множини ознак деструктивних впливів, де $i=1,2,\dots,s$, тоді обчислимо множину $\{ P(D_1/B_1), P(D_1/B_2), \dots, P(D_1/B_s) \}$. Ця множина являє собою множину ймовірностей знаходження підключення j -го пристрою до i -го у працездатному стані (D_1) при виконанні деструктивних впливів, що задаються підмножинами $B_1, B_2, \dots, B_s$ множини ознак деструктивних впливів k .

Звідси, корисність c_{ij} (суб'єктивна ймовірність) знаходження підключення j -го пристрою до i -го у працездатному стані (D_1) при будь-яких деструктивних впливах з множини $B_1, B_2, \dots, B_s$ задається виразом.

$$c_{ij} = P(D_1/B_1) + P(D_1/B_2) + \dots + P(D_1/B_s) \quad (2)$$

Множину ознак деструктивних впливів k , її підмножини $B_1, B_2, \dots, B_s$, а також стан (D_1) підключення j -го пристрою до i -го, для якого обчислюється суб'єктивна ймовірність c_{ij} визначається експертами.

При цьому, окрім функції живучості (1), повинні виконуватися наступні обмеження, які випливають з властивостей ієрархічних структур телекомунікаційних (комп'ютерних) мереж:

1. До одного елементу вищого рівня не може підключатися більше P елементів нижчого рівня.

$$\sum_{j=1}^n X_{ij} \leq P, \quad i=1,2,\dots,n, \quad (3)$$

де P – максимальна кількість пристроїв підключених до пристрою вищого рівня ієрархії, X_{ij} – невідомі елементи матриці підключень.

2. Кожний елемент структури мережі має бути підключений не більше ніж одному вищестоящому елементу (один елемент може бути головним і нікому не підпорядковуватися):

$$\sum_{i=1}^n X_{ij} \leq 1, \quad j=1,2,\dots,n, \quad (4)$$

де X_{ij} – невідомі елементи матриці підключень.

Це обмеження означає, що у кожному стовпці матриці підпорядкувань має бути не більше ніж одна одиниця. Може бути один стовпець з елементом найвищого рівня ієрархії, який нікому не підпорядковується. У такому стовпці стоять лише нулі, тому сума елементів такого стовпця буде дорівнювати 0. Однак, може трапитися випадок, коли умова (4) виконується $\left(\sum_{i=1}^n X_{ij}=0\right)$, але елемент у цьому випадку є ізольованим (він ні до чого не підключений і до нього пристрої не підключені), що не припускається у структурі мережі. Для недопущення такого випадку використовується умова (5).

3. Кожний елемент структури мережі має хоча б один зв'язок підпорядкування, тобто він не може бути ізольованим, автономним, без підключення.

$$\sum_{i=1}^n X_{ij} + \sum_{k=1}^n X_{jk} \geq 1, \quad j=1,2,\dots,n, \quad (5)$$

де X_{jk} – невідомі елементи матриці підключень, що визначають значення підпорядкування k -го елемента (k -го стовпчика таблиці підпорядкувань) j -му елементу (j -му рядку таблиці підпорядкувань).

Тобто, кожен елемент має бути хоча б комусь підпорядкований, або йому має бути підпорядкований хоча б якийсь елемент. Говорячи мовою таблиці підпорядкувань, це означає, що сума елементів стовпця і рядка з тим самим номером має бути не менша за одиницю.

4. Всього зв'язків підпорядкування має бути на одиницю менше ніж кількість всіх елементів структури мережі, тому що кожен елемент, за винятком одного (головного), має бути комусь підпорядкований.

$$\sum_{i=1}^n \sum_{j=1}^n X_{ij} = n - 1. \quad (6)$$

Оскільки у кожному з $(n-1)$ стовпців матриці має бути по одній одиниці, а у одному стовпці, якому відповідає головний елемент, жодної, то сума усіх елементів матриці підключень має дорівнювати $n-1$.

5. У системі не повинно бути циклічних зв'язків підключення, коли вищестоящий елемент підпорядковується нижчестоящому елементу, який йому підпорядкований безпосередньо, або через низку елементів проміжних рівнів.

Ця умова задається виразом (7), одержаним з аналізу графів структур ієрархічних мереж.

Для того, щоб n -вершинний граф G з матрицею суміжності $A = A(G)$ не мав контурів, необхідно і досить, щоб матриця $B = A^2 + A^3 + \dots + A^n$ мала нульові діагональні елементи. Тобто

$$B = \sum_{k=2}^n |X_{ij}|^k, \quad \sum_{i=1}^n b_{ii} = 0, \quad (7)$$

де $|X_{ij}|$ – матриця підключень, X_{ij} – невідомі елементи матриці підключень, b_{ii} – елементи головної діагоналі матриці B , n – кількість елементів у структурі.

Реалізація моделі виконувалась статистичним методом з детермінованим навчанням [3].

На основі створених теоретичних положень, розроблена на мові Visual Basic в середовищі системи Excel, програмна система для синтезу живучих ієрархічних комп'ютерних мереж. Загальний вигляд системи представлений на рис. 1.

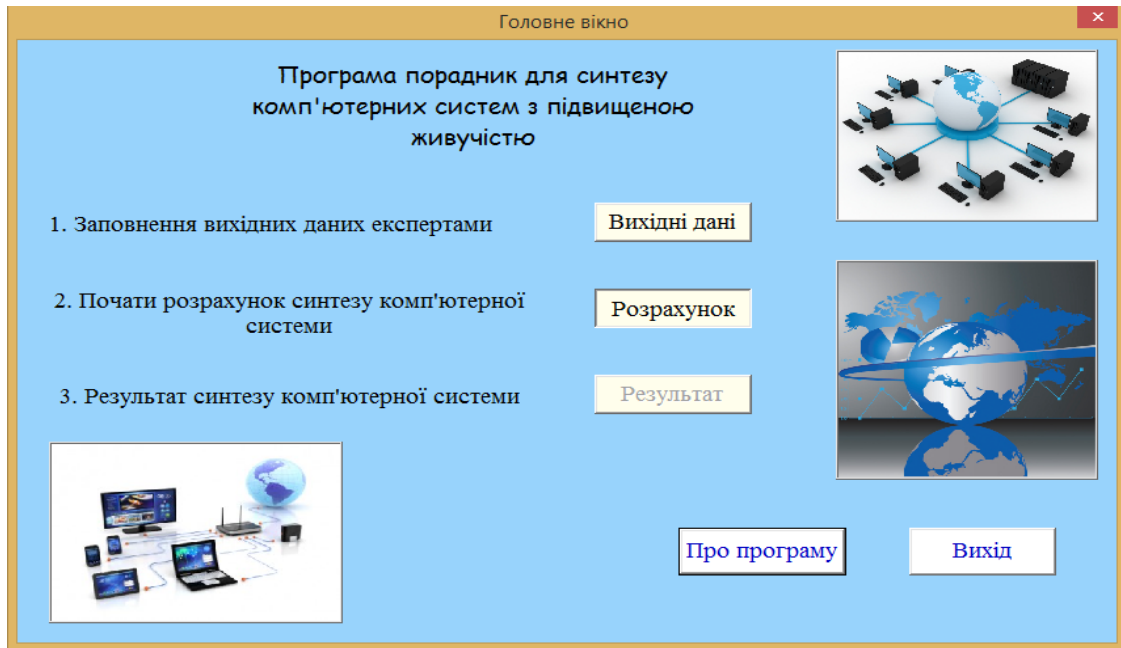


Рис. 1. Загальний вигляд системи для синтезу живучих ієрархічних комп'ютерних мереж

На рис.2 наведена залежність кількості операцій, необхідних для синтезу живучої комп'ютерної мережі у порівнянні з повним перебором варіантів. Як видно з рис.2. при кількості елементів мережі більшій за 35 кількість операцій в процесі повного перебору для пошуку найкращого варіанту структури мережі різко зростає. Кількість операцій в процесі пошуку найкращого варіанту структури мережі запропонованим методом практично не залежить від максимальної кількості пристроїв підключених до пристрою вищого рівня ієрархії мережі (параметр P в обмеженні (3) моделі).

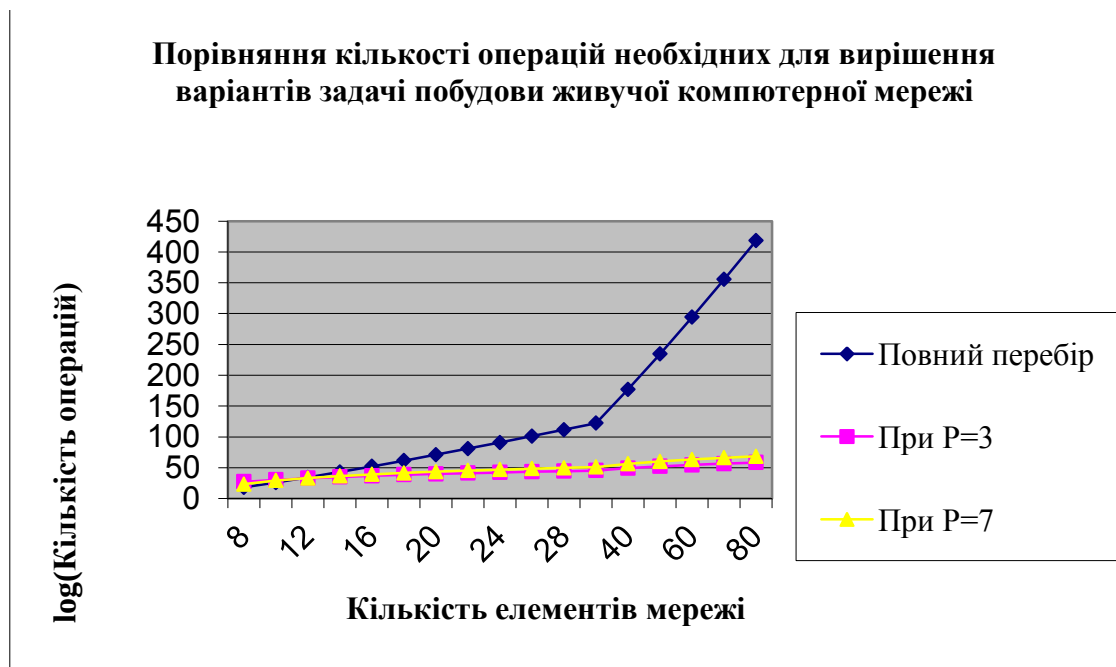


Рис. 2. Кількість операцій необхідних для вирішення варіантів задачі побудови живучої комп'ютерної мережі

Висновки

1. В роботі запропонована модель синтезу живучої ієрархічної комп'ютерної мережі як задача нелінійного булевого програмування, цільова функція якої являє собою суб'єктивну ймовірність (живучість) синтезованої мережі.

2. Запропонований підхід оцінки суб'єктивної ймовірності працездатності підключення пристроїв мережі в умовах різноманітних комбінацій деструктивних впливів на таке підключення.

3. На основі створених теоретичних положень, розроблена на мові Visual Basic в середовищі системи Excel, програмна система для синтезу живучих ієрархічних комп'ютерних мереж.

Список використаної літератури

1. Бондаренко В.Є. Система-порадник для побудови топології живучої комп'ютерної мережі. Наукові записки українського науково-дослідного інституту зв'язку. № 5(33), 2014. с. 65-72.

2. Бондаренко В.Є. Елементи суб'єктивної теорії ймовірностей для оцінки можливості шкідливих впливів і деструктивних дій в комп'ютерних мережах. Наукові записки українського науково-дослідного інституту зв'язку. № 4(32), 2014. с. 17-21.

3. Бондаренко В.Е. Статистический метод поиска экстремума с детерминированным обучением. "Гибридные вычислительные машины и комплексы", 1989, в. 12., с.40 - 45.

Автор статті

Бондаренко Віктор Євгенович - доктор технічних наук, доцент, професор кафедри комп'ютерних систем та мереж, Державний університет телекомунікацій, Київ, Україна. Тел. +38 099 520 62 19. E-mail: victorbondarenko@ukr.net

Бледнов Олексій Васильович - студент, Державний університет телекомунікацій, Київ, Україна. Тел.: +38 095 896 98 93. E-mail: alexeyblednov@mail.ru

Author of the article

Bondarenko Viktor Evgenevych - doctor of sciences (technic), associate professor, professor of Department of Computer Systems and Networks, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 099 520 62 19. E-mail: victorbondarenko@ukr.net

Blyednov Oleksiy Vasylovych - student, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 095 896 98 93. E-mail: alexeyblednov@mail.ru

Дата надходження в редакцію: 10.01.2017 р.

Рецензент: д.т.н., проф. К.С. Козелкова

УДК 621.396

Захарченко Н.В., д.т.н.; Корчинский В.В., д.т.н.;
Домрачева Е.А., аспирант; Шокотко А.А., аспирант

ИСПОЛЬЗОВАНИЕ ТАЙМЕРНЫХ СИГНАЛЬНЫХ КОНСТРУКЦИЙ ДЛЯ ИМПУЛЬСНО-КОДОВОЙ МОДУЛЯЦИИ РЕЧЕВОГО СИГНАЛА

Zaharchenko N.V., Korchinskiy V.V., Domracheva K.O., Shokotko A.A. Using of the timer signal constructions for pulse-code modulation of the voice signals.

The work represents the possibility of improving telecommunication systems characteristics by using timer-signal constructions. It's shown that the use of timer-signal constructions makes possible to achieve 2 fold decreasing of required radio-channel bandwidth in comparison with PCM method. The authors propose the telecommunication system scheme and shows transmission levels of digital voice signals in the multi-channel system based on timer-signal constructions, that allows to transmit standard information flows with 2-fold reduction of radio-channel bandwidth, which is important for satellites systems.

Keywords: voice signal, noise immunity, timer-signal constructions, Nyquist pulse, PCM.

Захарченко М.В., Корчинський В.В., Домрачева К.О., Шокотко А.А. Використання таймерної сигнальної конструкції при імпульсно-кодовій модуляції мовного сигналу.

У роботі показана можливість зменшення смуги пропускання каналу при передачі цифрового мовного сигналу в 2 рази і поліпшення його завадозахищеності в порівнянні з методом ІКМ шляхом застосування таймерних сигнальних конструкцій.

Ключові слова: мовний сигнал, завадозахищеність, таймерна сигнальна конструкція, найквістовий імпульс, імпульсно-кодова модуляція.

Захарченко Н.В., Корчинский В.В., Домрачева Е.А., Шокотко А.А. Использование таймерных сигнальных конструкций для импульсно-кодовой модуляции речевого сигнала.

В работе показана возможность уменьшения полосы пропускания канала при передаче цифрового речевого сигнала в 2 раза и улучшения его помехозащищенности по сравнению с методом ИКМ путем применения таймерной сигнальной конструкции.

Ключевые слова: речевой сигнал, помехозащищённость, таймерная сигнальная конструкция, найквистовый импульс, импульсно-кодовая модуляция.

Введение

В настоящее время особый интерес представляют методы передачи, которые повышают эффективность использования канальных ресурсов сети и обеспечивают защиту информации от несанкционированного доступа на канальном и физическом уровнях модели OSI. В [1] показано, что решение указанных задач возможно за счет усложнения структуры сигнальных кодовых конструкций путем применения таймерных сигнальных конструкций (ТСК), которые были предложены в 80-е годы прошлого века для повышения скорости передачи информации в бинарном канале[1]. На их основе был создан новый принцип контроля верности кодовых комбинаций без проверочных символов. В [2] показано, что ТСК обладают также свойствами скрытности, что снижает эффективную работу средств по перехвату и распознаванию смыслового содержания сообщений.

В опубликованных работах по таймерным сигналам недостаточно освещены вопросы практического применения их в реальных системах связи. Данное исследование актуально, так как направлено на повышение как показателей помехозащищенности системы (помехоустойчивости и скрытности), так и на уменьшение полосы пропускания реального канала при заданной скорости передачи. Целью данной работы является повышение эффективности системы передачи сигнала в аппаратуре ИКМ-30 на основе применения ТСК.

© Захарченко М.В., Корчинський В.В., Домрачева К.О., Шокотко А.А., 2017

1. Создание цифрового речевого сигнала с использованием таймерной сигнальной конструкции

ТСК позволяют создавать большое количество реализаций при передаче импульсных сигналов, длительность которых не меньше найквистового интервала[1,2]

$$\tau_c \geq \frac{1}{\Delta f}, \quad (1)$$

где Δf – полоса пропускания канала, обеспечивающая минимальные межсимвольные искажения данного сигнала.

Информация в таких сигнальных конструкциях содержится в длительности нескольких отдельных временных отрезков и их взаимном положении.

В ТСК осуществляется увеличение числа реализаций сигнальных конструкций на интервале

$$T_c = m\tau, \quad (2)$$

где m – число найквистовых интервалов τ . Это возможно за счет введения модуляции информационных параметров сигнала в точках, не кратных τ , а кратных некоторому элементу

$$\Delta = \frac{\tau}{s}, (s \in 1, 2...), \quad (3)$$

где s – число элементов Δ на интервале τ .

При этом с целью исключения межсимвольных искажений расстояние между значащими моментами модуляции - ЗММ (длительность импульсов в ТСК) выбирается

$$\tau_c \geq \tau. \quad (4)$$

На рис. 1. представлено несколько реализаций ТСК для бинарного канала из $m = 4$ элементов длительностью τ . На интервале кодового слова T_c можно сформировать несколько отрезков τ_c с определёнными длительностями и положениями в пределах кодового слова. Например, для ТСК-1 длительности первого, второго и третьего импульсов соответственно будут: $\tau_{c1} = 4\Delta$, $\tau_{c2} = 5\Delta$ и $\tau_{c3} = 7\Delta$. Для ТСК-2: $\tau_{c1} = 4\Delta$, $\tau_{c2} = 4\Delta$ и $\tau_{c3} = 8\Delta$. Для ТСК-3: $\tau_{c1} = 6\Delta$, $\tau_{c2} = 5\Delta$ и $\tau_{c3} = 5\Delta$. Информация о передаваемом символе заложена в длительностях отрезков τ_c и количестве ЗММ.

Конкретные реализации ТСК создаются путем поочередного добавления к первому импульсу длительностью τ единичного элемента Δ при постоянной длительности второго импульса, размещенного в конце интервала T_k . Затем, такая же операция производится и над вторым импульсом при сохранении длительности первого импульса. При одновременном изменении длительности первого и второго импульсов необходимо обеспечить минимальный временной интервал между ними величиной τ .

Таким образом, в канал передаются отрезки сигнала длительностью

$$\tau_c = \tau + k\Delta, [k = 0, 1, 2, ..., s \cdot (m - 2)]. \quad (5)$$

В ТСК энергетическое расстояние между сигнальными конструкциями определяется величиной $\Delta < \tau$, поэтому, число их реализаций L на интервале T_c значительно больше по сравнению с разрядно-цифровым кодом [1] и в общем виде определяется как

$$L = \sum_{i=1}^m C_{ms-i(s-1)}^i, \quad (6)$$

где i – число ЗММ.

Таким образом, основная задача при синтезе ТСК состоит в том, чтобы при заданных параметрах m , s и i сформировать необходимое множество реализаций.

Важным достоинством применения ТСК является повышенная структурная скрытность передачи информации по сравнению с позиционными кодами, которая зависит от числа реализаций L и определяется формулой Шеннона [3]

$$S_{тск} = \log_2 L. \quad (7)$$

Из этой формулы следует, что чем больше количество реализаций L , тем сложнее методом перебора распознать структуру сигнала.

Причем, так как системы с ТСК свободны от шумов квантования, их помехозащищенность будет выше, чем в системах с импульсно-кодовой манипуляцией (ИКМ).

Создание цифрового речевого сигнала на основе ТСК возможно при соответствующем выборе параметров таймерного кодирования, которые должны быть согласованы с временными параметрами каналаообразования ИКМ. Рассмотрим параметры преобразования сигнала, которые производятся в аппаратуре ИКМ-30 [4]:

- 1) частота дискретизации речевого сигнала со спектром 0,3-3,4 кГц

$$f_g = 8 \text{ кГц};$$

- 2) длительность цикла импульсного сигнала $T_{ц} = 125 \text{ мкс}$;

- 3) количество каналов $N_z = 32$ (30 информационных каналов);

- 4) интервал передачи сигнала в одном канале $T_z = 3,9 (\approx 4) \text{ мкс}$;

- 5) количество разрядов двоичного сигнала при квантовании сигнала в одном канале $n=8$;

- 6) длительность одного кванта $t_k = 0,4906 (\approx 0,5) \text{ мкс}$;

- 7) количество уровней квантового сигнала $z = 2^n = 256$;

- 8) частота следования канальных интервалов $F_k = 256 \text{ кГц}$;

- 9) частота следования символов в цикле передачи

$$f_c = f_g \cdot n \cdot N_k = 2048 \text{ кГц} (\approx 2 \text{ МГц});$$

- 10) необходимая полоса пропускания радиоканала $\Delta f = 2,038 (\approx 2) \text{ МГц}$ при найквистовой длительности импульса $t_k = 0,49 (\approx 0,5) \text{ мкс}$.

В работе [4] определено, что для качественного воспроизведения речи, преобразованной в импульсные сигналы, достаточно реализовать $L=256$ уровней квантования амплитуд.

Рассмотрим алгоритм построения ТСК для импульсного речевого сигнала, который обеспечивает $L=276$ уровней [1]. Увеличение числа уровней позволяет повысить качество передачи речевого сигнала по сравнению с ИКМ-30. Данное количество реализаций можно получить для ТСК, имеющей согласно табл. 3.4 [1] количество ЗММ $i=2$ при величине параметра $m=4$

$$m = \frac{T_c}{\tau} \quad (8)$$

и количестве единичных элементов $s=11$

$$s = \frac{\tau}{\Delta}, \quad (9)$$

где Δ – длительность единичного элемента, которая определяется величиной среднеквадратического значения помехи в канале δ

$$\Delta = (2 - 4)\delta. \quad (10)$$

Реализацию ТСК в данном случае целесообразно произвести на интервале $T_c = 4\tau$ [5]. На рис.2 приведена структура ТСК, обеспечивающая $L=276$ реализаций для преобразования аналогового речевого сигнала в импульсный цифровой с параметрами

$$T_k = 4\text{мкс}, \tau=1\text{мкс}, s=11, \Delta=0,09\text{мкс}.$$

После увеличения длительности первого и второго импульсов путем поочерёдного добавления отрезка Δ их максимальная длительность будет составлять 2τ .

При построении системы целесообразно осуществлять квантование по нелинейному закону как в ИКМ-30 [4].

Практическое число реализаций ТСК при заданном количестве ЗММ для данного случая удобно определить по формуле [1]

$$L = C_{ms-i(s-1)}^i = C_u^i = \frac{u!}{i!(u-i)!}, \quad (11)$$

где $u = ms - i(s-1)$.

После подстановки параметров в формулу (11) получим

$$L = C_{4*11-2*10}^2 = C_{24}^2 = \frac{24!}{2!*22!} = 23*12 = 276.$$

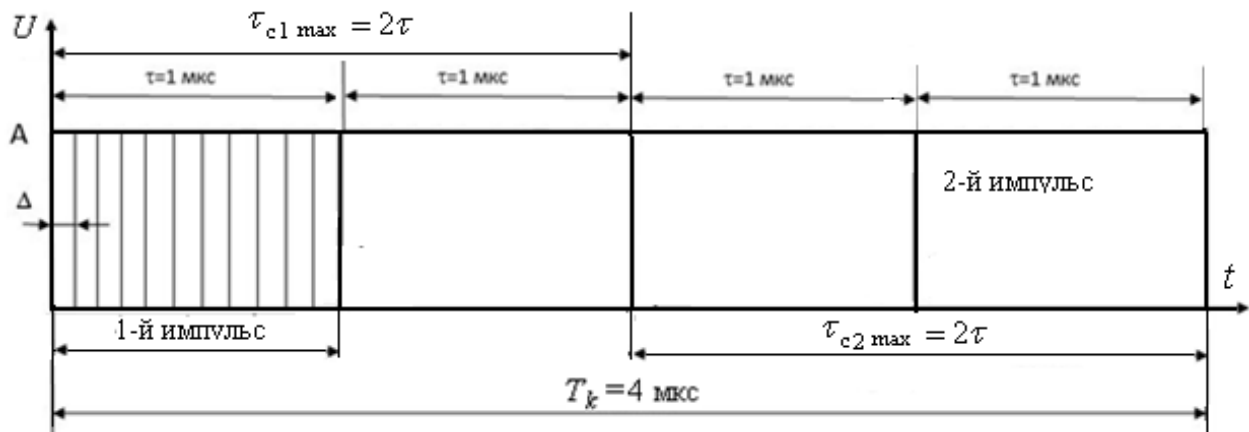


Рис 2. Структура ТСК для цифрового речевого сигнала

Блок-схема приемо-передающей системы для цифрового речевого сигнала с применением ТСК приведена на рис. 3.

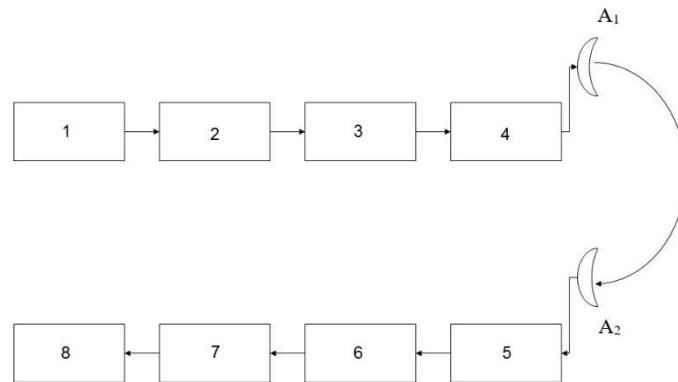


Рис. 3. Блок-схема приемо-передающей системы для цифрового речевого сигнала с применением ТСК: 1 – формирователь сигнала с ТСК (кодер); 2 – модулятор; 3, 6 – преобразователи частоты; 4 – выходной усилитель; A_1 , A_2 – антенны передатчика и приемника; 5 – малошумный усилитель; 7 – демодулятор; 8 – декодер ТСК

Формирование и обработка ТСК производится с помощью программно-аппаратных средств – кодера и декодера ТСК.

Таким образом, применение ТСК позволяет создать новую приемо-передающую систему связи для цифрового речевого сигнала, имеющего при сохранении параметров 1-4 классической системы следующие новые параметры:

- длительность найквистового импульса $\tau = 1$ мкс;
- количество реализаций (уровней сигнала) $L = 276$;
- частота следования символов в цикле $f_c = 1$ МГц.

Следовательно, использование ТСК при передаче речевого цифрового сигнала позволяет использовать в 2 раза меньшую полосу пропускания радиоканала по сравнению с классическим методом, используемым ИКМ–30.

Цифровые потоки для стандартных цифровых каналов с применением ТСК по аналогии с классической ИКМ 30 можно обозначить Е1 ТСК, Е2 ТСК, Е3 ТСК, Е4 ТСК (табл.1). Такие потоки позволяют уменьшить в 2 раза необходимую полосу пропускания радиоканала по сравнению с использованием ИКМ, что особенно важно при передаче сигнала в спутниковой системе.

В табл. 1 скорость передачи сигнала при использовании ТСК определена с учетом служебной информации, как в ИКМ 30.

Таблица 1. Скорость передачи цифровой информации в системах с ИКМ и ТСК

№ п/п	Количество стандартных каналов	Скорость передачи при классической ИКМ, Мбит/с	Скорость передачи при использовании ТСК, Мбит/с
1	30	Е1 2,048	Е1 ТСК 1
2	120	Е2 8,448	Е2 ТСК 4,125
3	480	Е3 34,368	Е3 ТСК 16,78
4	1920	Е4 139,264	Е4 ТСК 67, 99

Выводы

Применение таймерных сигнальных конструкций для создания цифрового речевого сигнала позволяет уменьшить полосу пропускания радиоканала в 2 раза по сравнению с применением классического метода ИКМ. Это особенно важно при передаче стандартных потоков в спутниковых системах.

Список использованной литературы

1. Захарченко М.В. Системы передавання даних. – Т. 1: Завадостійке кодування: підручник [для студентів вищих технічних навчальних закладів] / М.В. Захарченко. – Одеса: Фенікс. 2009. – 448с.
2. Скляр Б. Цифровая связь: Теоретические основы и практическое применение. – М.: Издат. дом «Вильямс», 2003. – 1104 с.
3. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012). – Lviv: Publishing House of Lviv Polytechnic, 2012. – С. 317.
4. Иванов Ю.П. Аппаратура ИКМ.30. / Под. ред. Ю.П. Иванова. – М.: Радио и связь. 1983. – 185с.
5. Захарченко Н.В., Семенко А.И., Корчинский В.В., Домрачева Е.А. Использование таймерных сигнальных конструкций для мониторинга сигналов аналогового датчика// Зв'язок. – 2016. - №6.- С.40-43.

Автори статті

Захарченко Микола Васильович - доктор технічних наук, професор, Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна. Тел. +38 068 292 27 65. E-mail: albrona@mail.ru

Корчинський Володимир Вікторович - доктор технічних наук, професор, Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна. Тел. +38 095 208 27 10. E-mail: vladkorchin@ukr.net

Домрачева Катерина Олексіївна - аспірант, асистент кафедри Телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна. Тел. +38 063 579 50 80. E-mail: katyscha@ukr.net

Шокотько Андрій Андрійович - аспірант кафедри Телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна. Тел. +38 093 567 20 19. E-mail: postbox78@ya.ru

Authors of the article

Zakharchenko Mikola Vasilovich - doctor of technical sciences, professor, Odessa National Academy of Telecommunications named after A.S. Popova, Odessa, Ukraine. Tel. +38 068 292 27 65. E-mail: albrona@mail.ru

Korchinsky Volodymyr Vitovich - doctor of technical sciences, professor, Odessa National Academy of Telecommunications Popova, Odessa, Ukraine. Tel. +38 095 208 27 10. E-mail: vladkorchin@ukr.net

Domracheva Katerina Oleksiivna - post-graduate student, assistant of department of Telecommunication systems and networks, State university of telecommunications, Kyiv, Ukraine. Tel. +38 063 579 50 80. E-mail: katyscha@ukr.net.

Shokotko Andriy Andriyovich - post-graduate student, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 093 567 20 19. E-mail: postbox78@ya.ru

Дата надходження в редакцію: 25.01.2017 р.

Рецензент: д.т.н., проф. А.І. Семенко

УДК 621.391

Гринкевич Г.О., к.т.н.; Макаренко А.О., к.т.н.; Жебка В.В., к.т.н.;
Куклов В.М., аспірант; Підручний А.І., аспірант

АНАЛІЗ ПРАЦЕЗДАТНОСТІ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ

Grynevykh G.O., Makarenko A.O., Zhebka V.V., Kuklov V.M., Pidruchniy A.I. Analysis serviceability program-configured networks.

The paper presents the concept of Software-Defined-Networking, and the history of programmable networks and associated review of the latest standards. One of them, the OpenFlow protocol, played an important role in promoting the concept of SDN, significantly influenced research and industry. Consider in more detail the basic principles of OpenFlow. Proposed expansion OpenFlow specification for deployment of decentralized monitoring network, including packet generation and processing on network devices. Technology can restore protection OpenFlow network within 50 ms. For this purpose any action from the network controller is not required, because the switch can immediately respond to setbacks. The technique of restoration controller must interact with network devices that takes longer and makes the method less convenient for large networks with many made components.

Keywords: information network, software-configured network, information security, Linux, Ethernet, OpenFlow.

Гринкевич Г.О., Макаренко А.О., Жебка В.В., Куклов В.М., Підручний А.І. Аналіз працездатності програмно-конфігурованих мереж.

У статті представлено концепцію Software-Defined-Networking, а також історію програмованих мереж і огляд пов'язаних з ними новітніх стандартів. Один з них, протокол OpenFlow, відіграв важливу роль у просуванні концепції SDN, значно вплинув на наукові дослідження і промисловість. Розглянуто більш детально основні принципи OpenFlow.

Ключові слова: інформаційні мережі, програмно-конфігуровані мережі, інформаційна безпека, Linux, Ethernet, OpenFlow.

Гринкевич А.А., Макаренко А.А., Жебка В.В., Куклов В.М., Пидручный А.И. Анализ работоспособности программно-конфигурируемых сетей.

В статье представлена концепция Software-Defined-Networking, а также история программируемых сетей и обзор связанных с ними новых стандартов. Один из них, протокол OpenFlow, сыграл важную роль в продвижении концепции SDN, значительно повлиял на научные исследования и промышленность.

Ключевые слова: информационные сети, программно-конфигурируемые сети, информационная безопасность, Linux, Ethernet, OpenFlow.

Вступ

Постановка задачі. В літературі і в промисловості, концепція програмованих мереж або Software-Defined-Networking (SDN) все ще використовується розробниками, які мають власні ідеї стосовно її оновлення. Фонд Open Network [1] – організація для користувачів з метою сприяння розвитку SDN, описує його як “Фізичне розділення управління мережами в площині від переадресації і до площини управління, що управляє декількома пристроями”.

Термін “програмованість” відноситься до гнучкості в площині управління, яка безпосередньо опрацьовується в програмному забезпеченні і включає в себе канал керування для обміну даними з мережевих пристроїв. Інтерфейс (API) дозволяє додаткам взаємодіяти з площиною управління для отримання доступу і зміни мережевих послуг. Наслідком цього виступає новий принцип конструкції, що підвищує гнучкість в управлінні мережею. За аналогією, цю еволюцію порівнюють з переходом від телефонів з обмеженою гнучкістю до смартфонів з операційною системою і більш широким функціоналом. Концепція традиційних комп’ютерних мереж ґрунтувалась на надмережевих пристроях, які містять як дані, так і площини управління. Для вирішення від парадигми SDN, назовемо їх непрограмованими мережами.

Передумови. Парадигма програмованих мереж попередньої розробки, активно використовувалася в середині 1990-х років. Зусилля дослідників, зосереджені навколо програмованих мереж, були розділені на два напрями. [2]. Перша школа, так звана активна мережа (AN), складалась з великої групи проектів і була заснована DARPA. Вона характеризується гнучким і динамічним підходом в напрямку провадження послуг в мережі. Наприклад, один пакет може бути використаний як для зміни мережевих послуг, так і для забезпечення максимуму гнучкості у конфігурації мережі.

На противагу йому, OpenSignalling (OpenSig) запропонували ідею створення стандартизованих інтерфейсів для зв'язку з мережевими пристроями, що була реалізована за допомогою IEEE P1520 [3]. Маршрутизатор і комутатори мають відкритий доступ використання інтерфейсів програмування (API), щоб надати можливість розробляти додаткове програмне забезпечення для нього. Незважаючи на дослідження в співтоваристві OpenSig, центрування навколо програмованих мереж, промисловість не адаптувалася до ідеї програмованих мереж зі стандартизованим API. Це призвело до патентованих протоколів із закритою складовою пристрою, що характеризує сучасні мережі.

1. Архітектури і інтерфейси

Різноманіття архітектур промисловості і наукових співтовариств розвивалися паралельно з моменту створення SDN.

Галузі в основному засновані на власному розумінні SDN, хоча деякі з них були стандартизовані або, принаймні, обговорюються в робочих групах Internet Engineering Task Force (IETF2).

Для того, щоб прискорити інновації в вендора нейтральним чином і визначити стандарти для SDN, Фонд Linux встановив (ODL) 3 лабораторних проекта OpenDaylight. Ця відкрита структура в даний час підтримується 29-ма провідними членами промисловості, такими як, Cisco, IBM, Juniper і NEC. Проект заснований на існуючих інтерфейсах і протоколах (наприклад, OpenFlow і NETCONF [4]), в даний час може розглядатися як найбільш перспективний крок на шляху розвитку SDN. Нижче вказані підходи, що виникли навколо SDN.

У той час як в OpenFlow більшість функціональних можливостей управління є централізованими, Tesseract розміщує інтелект в комутаторі.

Платформа маршрутизації управління (RCP). Робота RCP [5] виконується за допомогою AT&TLabs для того, щоб подолати обмеження вибору шляху до Інтернету. Кожен RCP присвоюється автономній системі (AS) з протоколом Inter-AS та інформацією про маршрутизацію між ними. В межах RCP, BorderGatewayProtocol (BGP) використовується в якості протоколу управління для обміну даними з маршрутизаторами. Вони містять площину даних на основі таблиць IP-експедиторських, які забезпечують лише невелику частину списку полів в OpenFlow.

Tesseract. Конструкція Tesseract [6] заснована на архітектурі 4D, що приймає рішення про поширення, виявлення і дані площини, як вказано на рис. 1 (а). Комутатори вмикають виявлення тегу задля знаходження хостів, комутаторів та для передачі пакетів, ґрунтуючись на площині даних. Тессеракт дозволяє здійснювати прямий контроль комп'ютерної мережі шляхом відділення логіки прийняття рішень (наприклад, маршрут обчислення) з нижчих протоколів. Цей підхід може також використовуватися для розгортання централізованої політики управління в мережі. У порівнянні з архітектурою OpenFlow, показаної на рис. 1 (б), мережеві пристрої містять тільки потік таблиць і спрощені вимоги до обчислювальної техніки.

Експедиція і управління елементом розподілу (Forces). Мета робочої групи (RFC 5810 [5]) полягає в розробці протоколу для Software-DrivenNetworking. Це вказує на деяку схожість з протоколом OpenFlow, окрім того, що площина даних – структурована. У той час як OpenFlow заснований на потоці таблиць, Forces використовує LFBs (логічні функціональні блоки), щоб встановити канали передачі даних і створення пакета потоків.

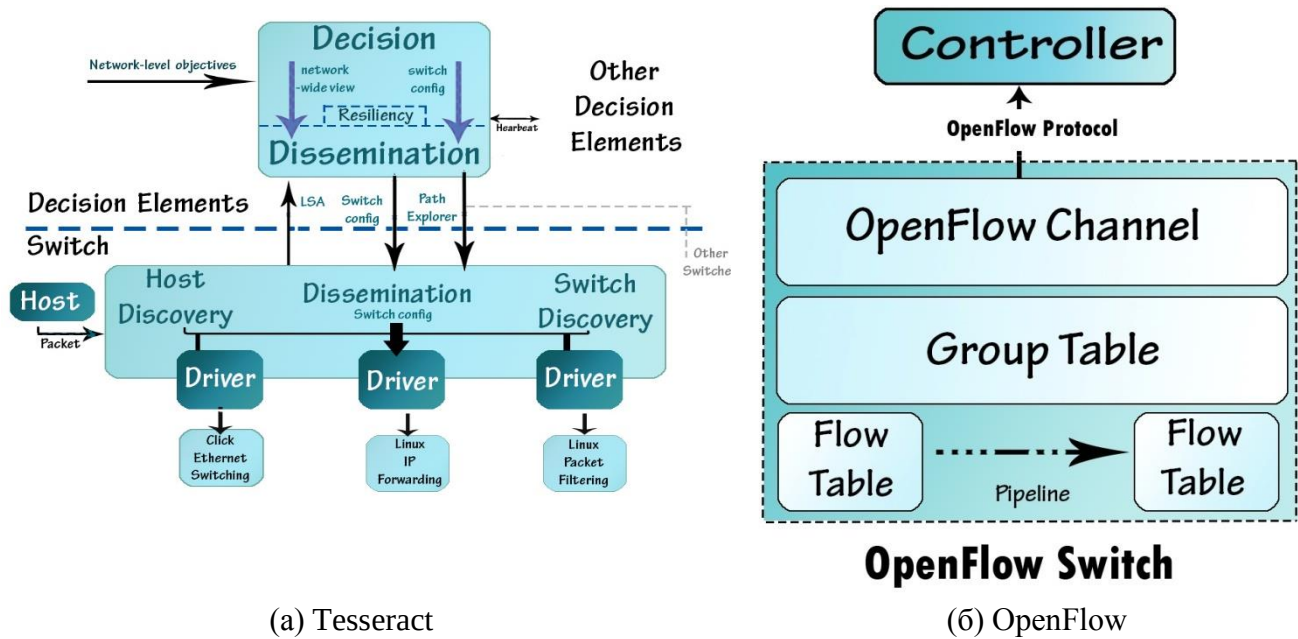


Рис. 1. Архітектура Tesseract і OpenFlow

ONF і OpenFlow. Поява SDN в значній мірі сприяла розвитку OpenFlow [1], відкритого протоколу, який використовується для обміну даними між централізованим мережним контролером і мережевими пристроями. Вона була ініційованою Мартіном Касадо в Етан [2], SANE [3] і CleanSlate проекту в Стенфордському університеті (табл. 1). В 2008 році OpenFlow був успішно розгорнутий в їх мережі з використанням обладнання комутаторів, що містили тільки площину даних, управління з котрого перемістилось на мережевий контролер (рис. 2). Специфіки OpenFlow визначені і розроблені ONF.

Таблиця 1. Архітектури і інтерфейси для SDN

Архітектура	Інтерфейси	Централізація	Стандартизація	Підтримка промисловості
RCP	BGP, Inter-AS	середня	-	-
Тессеракт	множинний	середня	-	-
-	ForCES	висока	RFC 5810	-
ODL	множинний	середня	-	Всі основні постачальники
ONF	OpenFlow	висока	-	Всі основні постачальники
PCE	pCEP	низький	RFC 4655	-
-	I2RS	низький	IETF Проект	Всі основні постачальники
ONE	onePK	низький	патентований	Cisco

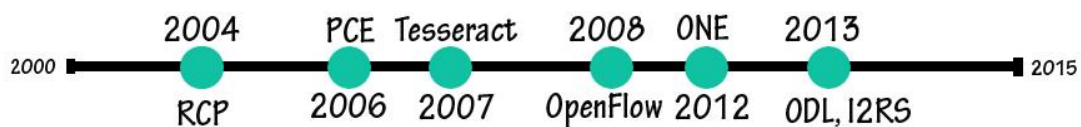


Рис. 2. Хронологія історичного розвитку SDN

Елемент шляху обчислення (PCE) PCE є програмним компонентом, який використовується для розрахунку шляху через ярлик багатопроTOCOLЬНОЇ комутації по мітках

(MPLS) мережі. Такий підхід призводить до виникнення мережевих пристроїв, в котрих видаляється з площини управління тільки компонент розрахунку управління. У той час як PCE надає менше функціональних можливостей і гнучкості ніж OpenFlow, її розгортання в глобальних мережах (WAN) менше, ніж для операторів, так як тільки крайові маршрутизатори повинні бути модифіковані [7]. PCE був стандартизований IETF, наприклад, в RFC 4655 [8].

Інтерфейс до системи маршрутизації (I2RS) I2RS являє собою робочу групу в IETF, яка має підтримку з боку ряду постачальників. Вона зберігає дані і керуючі компоненти в мережевих пристроях. На противагу пропонує інтерфейс, який дозволяє налаштувати зв'язок з площинами управління, які можуть бути розташовані за межами локальної мережі. Це дозволяє взаємодіяти з протоколами маршрутизації від зовнішнього програмного забезпечення керованого екземпляру.

Open Network Environment (ONE). Управління SDN вимагає декількох API-інтерфейсів, наприклад, одного каналу доступу до мережевих пристроїв в той час як другий буде керувати обміном даних між мережевими службами і зовнішніми додатками. ONE компанії Cisco [9] це архітектура інтерфейсу One Platform Kit (OnePK), що були об'єднані в єдине рішення. Це дозволяє розгортання мережевих додатків не тільки на виділеному контролері мережі, як запропоновано в OpenFlow, а й на самих мережевих пристроях. Також це виключає використання товарного обладнання, але дозволяє більш гнучке розбиття функціональності між даними і площинами управління.

Крім вказаних архітектур загальний дизайн SDN все ще розвивається. Наприклад, Fabric (тканинний) [10] підхід поєднує в собі мережі програмованості з MPLS з метою підвищення SDN. Пакети, які входять або виходять з мережі, обробляються за допомогою вхідного/вихідного граничного комутатора, який управляється контролером. Він може надавати мережеві послуги, такі як безпека, фільтрація і ізоляції. Завдання пересилання пакетів по мережі здійснюється через "мережеві ділянки". Такий поділ дозволяє їм і самому перемикачу еволюціонувати окремо, без впливу один на одного.

Термін, який тісно пов'язаний з SDN – є віртуалізацією мережі. Вона пропонує стиккування обладнання в програмному забезпеченні, щоб забезпечити певні завдання, наприклад, для визначення кількості віртуальних комутаторів. Вони можуть бути реалізовані, наприклад, з відкритим vSwitch, який заснований на використанні відкритого програмного забезпечення і широко використовується в операційних сценаріях. Поняття віртуалізація мережі також можуть бути використані в якості основи для розробки рішень SDN.

OpenFlow на основі SDN. Ця стаття фокусується на OpenFlow – основі парадигми SDN, так як більшість поточних досліджень і програмного забезпечення з відкритим вихідним кодом зосереджена саме навколо нього. В результаті, він є все найбільш розгорнутим у виробничому середовищі. Наприклад, Google використовує концепцію OpenFlow на основі SDN для їх внутрішньої магістральної мережі під назвою G-Scale [8], яка є великою міжнародною мережею. Досвід компанії був дуже багатообіцяючим, що дозволило швидко розгорнути багатьох функцій і спрощенню управління мережею. У промисловості більшість виробників мережевого устаткування забезпечують мережеві пристрої з підтримкою OpenFlow, такі як Cisco, HewlettPackard [11] і NEC. Архітектура SDN з OpenFlow показана на рис. 3 і складається з трьох рівнів.

Інфраструктура рівня. Цей рівень використовується для пересилки пакетів на основі OpenFlow – підтримуваних мережевих пристроїв. Спеціалізоване обладнання, включаючи пам'ять для зберігання потоку інформації, дозволяє швидку обробку пакетів. Типові мережеві пристрої, які належать до цього шару, – це комутатори і маршрутизатори. Комутатор зазвичай працює на рівні ISO7 лінії зв'язку (L2), в той час як маршрутизатор може також обробляти мережевий рівень (L3) інформації, що дозволяє пересилку пакетів за межі локальних мереж (LAN).

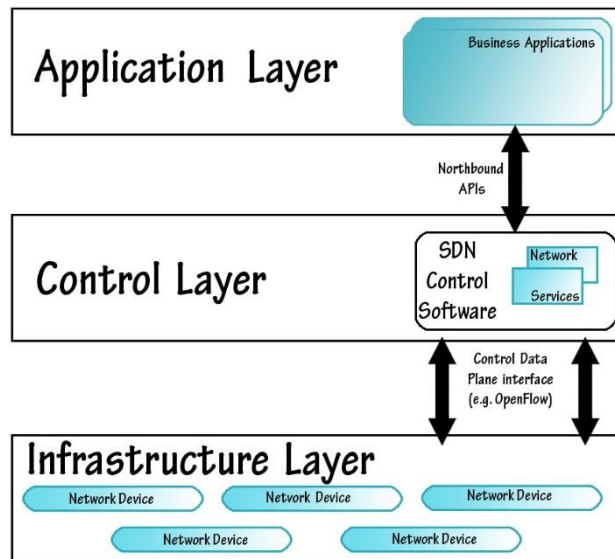


Рис. 3. Конструкція тривірневої програмно-визначеної архітектури

Контроль рівня. Мережевий контролер, який часто використовують в якості операційної системи, включає в себе площину управління і має централізоване подання. Це може бути використано для виконання рішень переадресації, що засновані на врахуванні стану всіх підключених мережевих пристроїв. Контролер здійснює зв'язок з мережевими пристроями через інтерфейс OpenFlow в південному напрямку. Другий тип API, інтерфейс в північному напрямку, використовується для обміну даними між сервісами і бізнес-додатками. Типові приклади мережевих послуг включають в себе маршрутизацію, комутації пакетів (L2) і MPLS. Крім того, кілька контролерів можуть бути розгорнуті з різних причин, наприклад, щоб уникнути єдиної точки відмови або для окремих завдань.

Натхнені першим відкритим вихідним мережевим контролером, NOX [12], написаної в C++, науково-дослідні інститути і компанії розробили мережеві контролери для широкого кола цілей, з відкритим вихідним кодом спільноти: типові контролери POX [13] (Python), Beacon (Java) і Floodlight (Java). Останній підтримується компанією BigSwitchNetworks, який вважається комерційним.

Прикладний рівень. Даний рівень дозволяє використовувати бізнес-додатки для зміни і надання мережевих послуг клієнтам. Це – вимога визначення API для того, щоб дозволити стороннім розробникам створювати і продавати мережеві додатки до оператора мережі.

Frenetic [14] є мовою програмування мережі, що використовується для визначення політики вищого рівня. Це забезпечує підвищення абстракції втратити зв'язку із мережею для того, щоб приховати обробку пакетів низького рівня від програміста. Проект нещодавно був запропонований Python на основі мови під назвою Pyretic [15]. Це забезпечує створення абстрактної моделі пакету, логічну політику високого рівня і мережевих об'єктів.

Протокол OpenFlow. Інтерес до SDN значно зріс після розробки протоколу OpenFlow, що сьогодні використовується під управлінням ONF [5]. У той час як основна функціональність була повністю реалізована у версії 1.0, більш пізні розробки включають в себе підтримку IPv6 і MPLS.

Мережеві потоки. Протокол OpenFlow заснований на концепції мережевих потоків для моніторингу та управління TRAFFI C всієї мережі. Це поліпшило масштабованість за рахунок збільшення швидкості мережі і в даний час підтримуються потоки з підтримкою пристроїв від всіх основних виробників. Є кілька визначень терміна потоку в літературі. IPFlow робоча група в рамках IETF [16] описує IP потік таким способом: “Потік, що визначається як сукупність IP-пакетів, котрий проходять через точку спостереження в мережі

протягом певного інтервалу часу. Всі пакети, що належать до конкретного потоку, мають ряд загальних властивостей”.

Наприклад, зв’язок між двома об’єктами призводить до двох притоків, як показано рис. 5. Типові властивості одного потоку включають в себе джерело і IP-адреси призначення, порту джерела і одержувача, а також тип протоколу (TCP, UDP, ICMP, і т.д.).



Рис. 4. Flow на основі зв’язку між двома учасниками

Таблиця витрат. Для пересилання пакетів, заснованих на концепції притоків, кожен комутатор OpenFlow має містити одну або кілька поточкових таблиць, використовуваних для зберігання попереднього потоку записів/правила. Наприклад, адреса управління доступом до середовища передачі (MAC) може бути використана для ідентифікації вузлів в комутованій мережі. Кожен запис потоку містить наступні компоненти:

Зіставлення полів | пріоритет | Лічильники | інструкції | таймаут | файл Cookie

Для всіх вхідних пакетів, які надходять на розмикач, потік таблиці перегляду виконується шляхом зіставлення заголовка пакета проти Match Fields всіх потоків записів. Кожен OpenFlow на основі комутатора підтримує відповідність полів, зазначених на рис. 6, які можуть бути або містять Спеці значення.

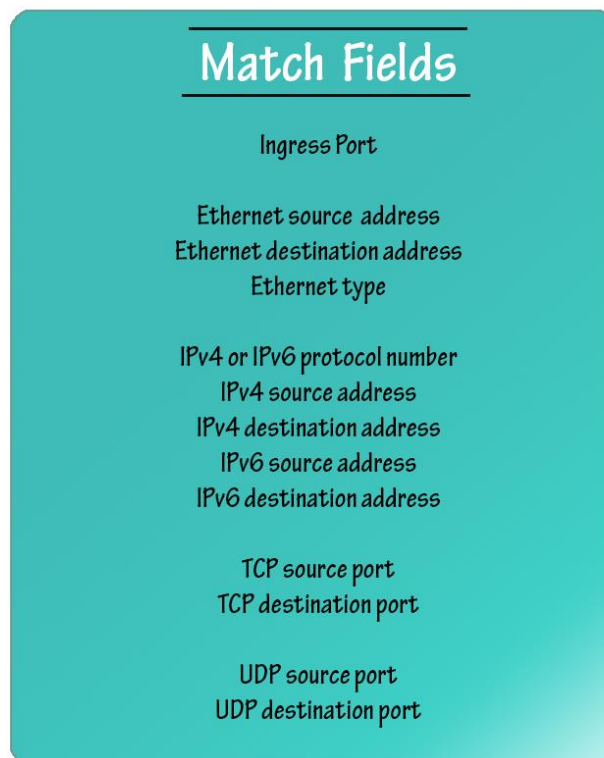


Рис. 5. Match Fields всіх потоків записів

Висновки

В даний час дослідження в області OpenFlow на основі SDN вже допомогли вирішити деякі питання до стадії оперативного розгортання самого проекту. Як вище зазначено, управління несправностями концентрується в основному на виявленні та виправленні переривання зв'язку, які можуть пошкодити не тільки дані, а й зв'язок з контролером. Для того, щоб запропонувати нові схеми виявлення несправностей для SDN, відповідні методи моніторингу для цієї архітектури повинні бути вивчені. Існує декілька підходів до вимірювання та моніторингу мережі, котрі ґрунтуються на вставці додаткових шарів між пристроями і контролером мережі. Це дозволяє забезпечити перевірку керуючих повідомлень OpenFlow. Наприклад, щоб ідентифікувати трафік перевантаження. Так як додатковий шар відрізняється від оригінальної архітектури OpenFlow і вимагає додаткових апаратних засобів, аналізу потоку записів на мережі контролера. Це може бути досягнуто шляхом розгортання алгоритмів моніторингу, що працюють на основі мережевого контролера. Аналізи потоку можуть бути використані для виявлення характеристик трафіку і побудови повної картини мережі шляхом включення вхідних сигналів від всіх мережевих пристроїв.

Для налагодження програмного забезпечення необхідно забезпечити контроль за пакетами в мережі, хоч формально перевірка може бути використана для визначення правильності потоку. Це необхідно для того, щоб генерувати докладні мережеві знімки, а також інспектувати параметри функції при певних умовах мережі. З точки зору безпеки, потенціал OpenFlow реалізований на нових схемах безпеки не були добре вивченим. Аналізуючи пакети в повідомленні Packet на контролері мережі вони можуть бути використані для ідентифікації і визначення проникнення зв'язку, перш ніж потік налаштується. У той час як для безпеки мережі були досліджені нові вектори атак, централізований контролер мережі і канал управління залишаються частково незахищеними.

Список використаної літератури

1. McKeown N. "OpenFlow: enabling innovation in campus networks," / N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner // SIGCOMM Comput. Commun. Rev, vol. 38, no. 2. -Mar. 2008- pp. 69–74.
2. Дуравкин Е.В. Архитектура SDN. Анализ основных проблем на пути развития [Електронний ресурс] / Е.В. Дуравкин, Е.Б. Ткачева, Иссам Саад// Системи обробки інформації . – 2015. – випуск 3 (128) - Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwiM_Mee87DSAhXBvBoKHbr3AhcQFghTMAc&url=http%3A%2F%2Fwww.hups.mil.gov.ua%2Fperiodic-app%2Farticle%2F12126%2Fsoi_2015_3_21.pdf&usg=AFQjCNH6PaaG9b2Jn1SzKgoF2Rh3VlQYG
3. Смелянский Р. Программно-конфигурируемые сети [Электронный ресурс]/ Р. Смелянский // Открытые системы. – 2012. – № 9. – Режим доступа к статье: www.osp.ru/os/2012/09/13039421/
4. О. Р. Лапони́на Способы трансформации сетей к SDN-Архитектуре [Електронний ресурс] / О. Р. Лапони́на, В.А.Сухомлин // – Режим доступу: <http://injoit.org/index.php/j1/article/viewFile/191/143>
5. Open Networking Foundation, "SDN Definition," [Електронний ресурс] // Open Networking Foundation. - 2013. – Режим доступу: <https://www.opennetworking.org/index.php?option=comcontent&view=article&id=686&Itemid=272&lang=en>
6. Wall D.W. "Messages as active agents," / D.W.Wall // in Proceedings of the 9th ACM SIGPLAN SIGACT Symposium on Principles of Programming Languages (POPL'82).- New York, NY, USA: ACM. – 1982. - pp. 34–39.
7. Красотин А. А. Программно-конфигурируемые сети как этап эволюции сетевых технологий / А. А. Красотин, И. В.Алексеев // Моделирование и анализ информационных систем. – 2013. – Т. 20. – №. 4. – С. 110-124.
8. Фещенко О. А. Анализ задач, возложенных на программно-конфигурируемые сети // Системи обробки інформації. – 2013. – Випуск 9 (116). – С. 181-183.

9. Роговой В. П. ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ НА БАЗЕ ТЕХНОЛОГИИ SDN // Роговой В. П. // Праці УДК 621.3 . – 2013. – №3 . – С. 16-19 .
10. Smith J. “Active networking: one view of the past, present, and future,” Systems, Man, and Cybernetics, Part C: Applications and Reviews. / J. Smith and S. Nettles. // IEEE Transactions on. - Feb. 2004. - vol. 34, no. 1. - pp. 4–18.
11. Tennenhouse D. “A survey of active network research,”/ D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, and G. Minden. // IEEE Communications Magazine. - Jan. 1997. - vol. 35, no. 1. - pp. 80–86.
12. Biswas J. “The IEEE P1520 standards initiative for programmable network interfaces,”. / J. Biswas, A. A. Lazar, J. F. Huard, K. Lim, S. Mahjoub, L. F. Pau, M. Suzuki, S. Torstensson, W. Wang, and S. Weinstein. // Comm. Mag. - Oct. 1998. - vol. 36, no. 10. - pp. 64–70.
13. Stadler R. Active Technologies for Network and Service Management. / R. Stadler and B. Stiller. // 10th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM'99), ser. Lecture Notes in Computer Science. - Oct. 1999. - vol. 1700. Springer .
14. Brunner M. “Management in telecom environments that are based on active networks,” . / M. Brunner and R. Stadler. // J. High Speed Netw. - Dec. 2000. - vol. 9, no. 3,4. - pp. 213–230.
15. Enns R. NETCONF Configuration Protocol (IETF RFC 6241). / R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman. - June 2011.
16. Feamster N. “The case for separating routing from routers,”. / N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, and J. van der Merwe. // in Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA'04). - New York, NY, USA: ACM. – 2004. - pp. 5–12.

Автори статті

Гринкевич Ганна Олександрівна – к.т.н., доцент кафедри телекомунікаційних систем, Державний університет телекомунікацій, Київ, Україна. Тел. +38 067 440 52 75. E-mail: ggrynkevych@i.ua

Макаренко Анатолій Олександрович – кандидат технічних наук, доцент, доцент кафедри Інформаційно-комунікаційних технологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 097 509 00 33. E-mail: makarenkoa@ukr.net

Жебка Вікторія Вікторівна - к.т.н., доцент кафедри інженерії програмного забезпечення, Державний університет телекомунікацій, Київ, Україна. Тел. +38 098 728 46 13. E-mail: viktorija_zhebka@ukr.net

Куклов Валентин Михайлович – аспірант, асистент кафедри телекомунікаційних систем та мереж, Державний університет телекомунікацій, Київ, Україна. Тел. +38 066 297 14 53. E-mail – vm.kuklov@gmail.com

Підручний Артем Ігорович – аспірант, асистент кафедри Комп'ютерних наук і інформаційних технологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 093 335 95 42. E-mail: mrtom0311@gmail.com

Authors of the article

Grynkevych Ganna Oleksandrivna – candidate of science (technic), assistant professor, assistant professor of Department of Telecommunication systems, State university of telecommunications, Kyiv, Ukraine. Tel. +38 093 996 26 02. E-mail: ggrynkevych@i.ua.

Makarenko Anatoliy Oleksandrovych – candidate of Science (technic), associate professor, associate professor of Department of Information and communications technology, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 097 509 00 33. E-mail: makarenkoa@ukr.net

Zhebka Viktoria Viktorivna - candidate of science (technic), assistant professor of Department of Application Programming, State university of telecommunications, Kyiv, Ukraine. Tel. +38 098 728 46 13. E-mail: viktorija_zhebka@ukr.net

Kuklov Valentyn Mykhaylovych - postgraduate student, teaching assistant of Department of Telecommunication systems and networks, State university of telecommunications, Kyiv, Ukraine. Tel. +38 066 297 14 53. E-mail: vm.kuklov@gmail.com

Pidruchniy Artem Igorovych - postgraduate student, teaching assistant of Department of Computer Science and information technolog, State university of telecommunications, Kyiv, Ukraine. Tel. +38 093 335 95 42. E-mail: mrtom0311@gmail.com

Дата надходження в редакцію: 08.02.2017 р.

Рецензент: д.т.н., проф. В.Ф. Заїка

УДК 621.391

Недашковский А.Л., к.т.н.

СЦЕНАРИИ ОРГАНИЗАЦИИ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ BPL В METRO ETHERNET СЕТЯХ ДОСТУПА

Nedashkivsky O.L. Scenarios of use BPL technology in the Metro Ethernet access networks.

The classification of telecommunications networks and equipment that support PLC technology are shown. The organization of communication scenarios using BPL technology in Metro Ethernet access networks are analyzed and proposed. The boundaries of the economic feasibility of the use of different scenarios are evaluate and define. It showed a positive effect from synergy of operators of communication efforts and utility distribution companies.

Obtained results show that the most economical is the scenario 3 «Replacing the dwelling distribution network». However, even in this case, the cost of a «standard service» a little above then standard solutions based on cables of fifth category.

When compared with non-standard connections should take into account the total cost of ownership including the expenses for the organization of interfloor low voltage risers or telephone conduit, the cost of which is high and not always possible. In such situations, BPL becomes economically viable solution, and sometimes only one possible solution.

The parallel deployment of BPL access networks and NPL-AMR networks provides a more cost-effective solution from a synergy of efforts of telecommunications operators and the utility companies.

Keywords: Metro Ethernet, NPL, BPL, access network, dwelling distribution networks, Internet AMR

Недашківський О.Л. Сценарії організації зв'язку з використанням технології BPL в Metro Ethernet мережах доступу.

Наведено класифікацію телекомунікаційних мереж і класів обладнання, яке підтримує технологію PLC. Проаналізовано та запропоновано сценарії організації зв'язку з використанням технології BPL в Metro Ethernet мережах доступу. Оцінені і визначені межі економічної доцільності застосування різних сценаріїв. Показаний позитивний ефект від синергії зусиль операторів зв'язку і енергорозподіляючих компаній.

Ключові слова: Metro Ethernet, NPL, BPL, мережі доступу, будинкові розподільчі мережі, Інтернет, АСКОЕ.

Недашковский А.Л. Сценарии организации связи с использованием технологии BPL в Metro Ethernet сетях доступа.

Приведена классификация телекоммуникационных сетей и классов оборудования поддерживающих технологию PLC. Проанализированы и предложены сценарии организации связи с использованием технологии BPL в Metro Ethernet сетях доступа. Оценены и определены границы экономической целесообразности применения различных сценариев. Показан положительный эффект от синергии усилий операторов связи и энергораспределяющих компаний.

Ключевые слова: Metro Ethernet, NPL, BPL, сети доступа, домовые распределительные сети, Интернет, АСКУЭ.

Вступление

В общем случае PLC (Power Line Communications - передача информации по силовым линиям) это технология, позволяющая рассматривать силовые сети как альтернативную среду передачи данных [1, 2].

Потенциальные преимущества технологии PLC можно сформулировать следующим образом:

- не требуется дорогостоящих работ, связанных с прокладкой телекоммуникационных кабелей;
- не требуется радиочастотный ресурс;
- обеспечивается быстрое развертывание сети и возможность её поэтапного наращивания по мере необходимости;
- возможно предоставление всего спектра мультимедийных и телекоммуникационных услуг (Интернет, телефония, цифровое телевидение и др.);

© Недашківський О.Л., 2017

- идеально подходит для предоставления «энергетических услуг» и услуг по управлению «интеллектуальным домом» (автоматическое снятие показаний различных счетчиков, дистанционный мониторинг, сигнализация, биллинг и др.);

- возможность комплексного предоставления энергетических и телекоммуникационных услуг одним поставщиком, то есть является настоящей альтернативой существующим технологиям «последней мили», особенно для сельской местности.

При этом целесообразно обозначить, что перспективы технологии PLC во многом зависят от:

- теории и практики построения PLC сетей;

- динамики снижения цен на оборудование;

- наличия государственных программ по развертыванию систем широкополосного абонентского доступа на основе различных технологий, включая PLC;

- активности крупных региональных энергетических компаний по проектам, которые фокусировались бы на внедрении телекоммуникационных технологий двойного назначения, в т.ч. предназначенных для предоставления современных телекоммуникационных услуг населению самостоятельно или через аффилированные структуры;

- масштаба развертывания коммерческих проектов по предоставлению услуг широкополосного доступа на базе альтернативных технологий (xDSL, сетей КТВ, ВОЛС и др.);

- конкурентоспособности решений на основе PLC и их адаптированности к отечественным электрическим сетям;

- роста платежеспособного спроса населения на услуги широкополосного доступа в целом;

- накопления положительного опыта строительства коммерческих сетей PLC за рубежом.

Целью данной статьи является проведение классификации типов технологии PLC; разработка сценариев применения PLC для построения сетей доступа согласно концепции Metro Ethernet; оценка технической и экономической целесообразности применения различных сценариев.

1. Классификация PLC технологий

Семейство технологий PLC можно классифицировать (рис. 1) по таким критериям как:

- максимальная скорость передачи данных;
- возможность поддержки многоуровневой архитектуры.

Тогда, согласно первого критерия, можно выделить:

- низкоскоростные технологии PLC с максимальной скоростью до 2 Мбит/с, которые будем называть NPL (Narrowband over PowerLine);

- высокоскоростные технологии PLC с максимальной скоростью более 2 Мбит/с, которые будем называть BPL (Broadband over PowerLine).

NPL как правило применяется для организации служебной связи, телеконтроля, телеуправления, телеметрии, АСКУЭ (автоматизированных систем комплексного учета электроэнергии).

BPL используется для построения локальных сетей (LAN- Local Area Network), сетей доступа (Accesses Network), а также интеллектуальных систем АСКУЭ, которые чаще называют системами AMR (Automatic Meter Reading).

Согласно второго критерия, среди технологий BPL можно и исключительно важно выделить две подгруппы:

- технологии индивидуального использования – SOHO BPL (SOHO – Small office / Home Office - «малый офис / домашний офис») [3, 4];

- технологии операторского класса – Carrier Class BPL [5].

Очевидно, что для построения Metro Ethernet сетей доступа приемлемы только высокоскоростные технологии PLC, т.е. BPL. Основные характеристики которых:

- использование существующих электрических сетей;
- скорость передачи данных выше 200 Мбит/с;

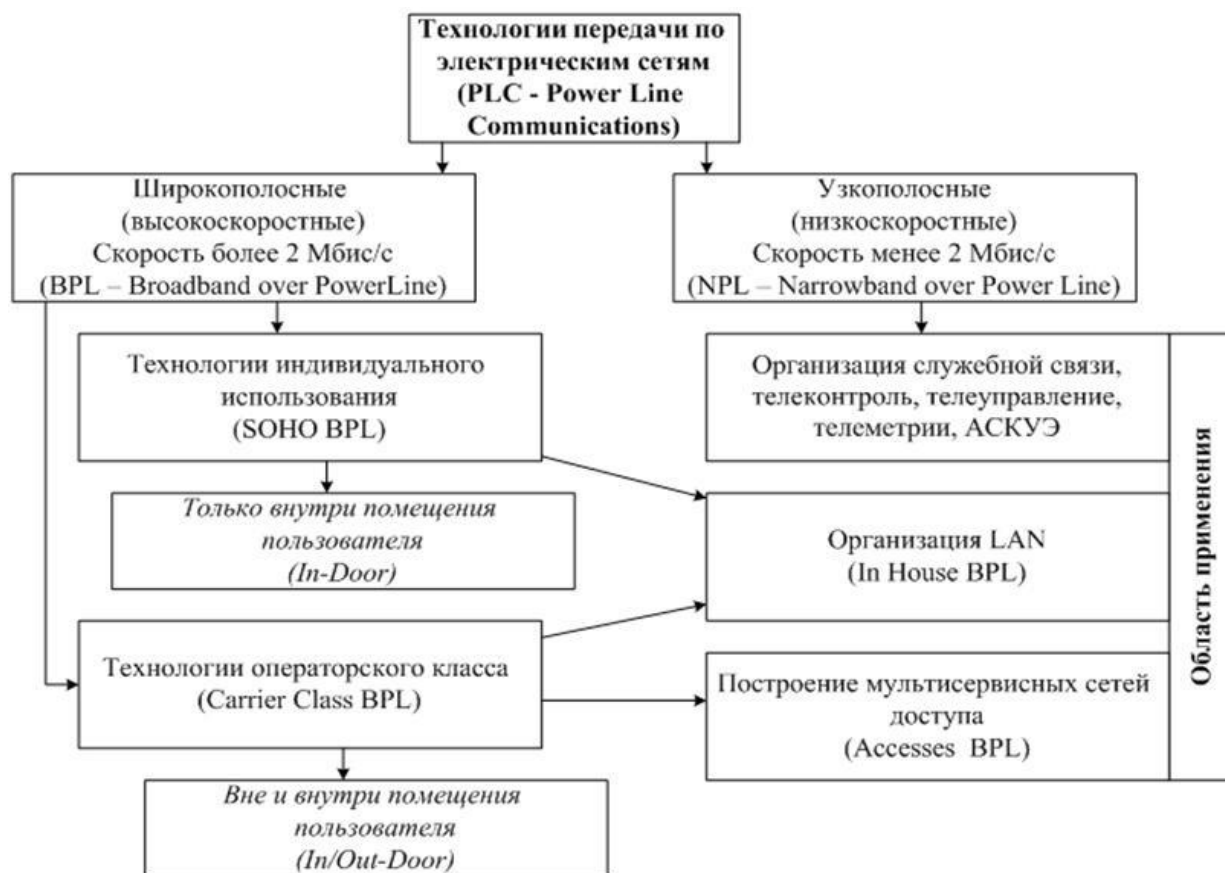


Рис. 1. Классификация телекоммуникационных технологий на базе электросетей

- полная поддержка протоколов IP и технологии Ethernet;
- дальность передачи данных до 200 м. без использования регенераторов, а при использовании и больше;
- оконечные абонентские устройства (далее CPE - Customer Premises Equipment для общего термина или BPL-CPE, если речь идет о BPL совместимом CPE) предоставляют все необходимые интерфейсы, а именно:

- базовые:

- Ethernet, BPL;
- дополнительные: WiFi, VoIP;
- BPL-CPE предоставляют все необходимые телекоммуникационные функциональные возможности, а именно:
- базовые: Ethernet Bridge (Ethernet-мост);
- дополнительные: Switch (Ethernet-мост), Router (IP маршрутизатор), WiFi AP (WiFi точка доступа), VoIP Gateway (шлюз IP-телефонии).

Результаты сравнения основных характеристик различных BPL технологий представлены в таблице 1.

2. Сценарии организации связи

На рисунке 2 приведена схема сценария 1 применения SOHO BPL. Данный сценарий можно назвать «Замена квартирной разводки» или «Виртуальный патчкорд». Сценарий предусматривает прокладку обычной витой пары категории 5 от точки присутствия (как правило Ethernet коммутатор доступа) оператора универсальной мультисервисной сети (УМСС) до помещения клиента. В помещении клиента устанавливается два BPL-адаптера

(на рис. 2 обозначены как «Home Plug PLC адаптер»). Один для связи Ethernet сети провайдера с BPL сетью клиента, а второй для подключения BPL сети клиента к абонентским Ethernet устройствам.

Таблица 1. Сравнительная характеристика SOHO BPL и Carrier Class BPL

SOHO BPL	Carrier Class BPL (Access BPL)
Ключевые особенности: - сегмент: SOHO; - покрытие: In-Door (внутри помещения пользователя); - тип сети: одноранговая; - количество устройств: до 16; - элементы BPL-сети: BPL-адаптеры (BPL-модемы); - локальное управление; - технология виртуальных локальных сетей (VLAN - Virtual Local Area Network): не поддерживается.	Ключевые особенности: - сегмент: Accesses Network; - покрытие: In/Out-Door (вне и внутри помещения пользователя); - тип сети: многогранговая; - количество устройств: до 64; - элементы BPL -сети: BPL-модемы (BPL -CPE), BPL-HeadEnd (центральный контроллер BPL сети), BPL-Repeater (BPL регенераторы); - централизованное управление; - полная поддержка VLAN; - возможность применения для построения АСКУЭ (AMR)
Классическое применение: - «Точка-точка» (режим моста), т.е. как «виртуальный патч-корд»; - «Домашняя ЛВС» (режим концентратора (хаба)), т.е. как «виртуальный Ethernet концентратор».	Классическое применение: - «Точка-многоточка» (т.е. построение сетей доступа).



Рис. 2. Сценарий 1 применения SOHO BPL: «Замена квартирной разводки»

Отличительные особенности такого сценарии:

- возможность предоставления только одного класса услуг доступа (One Play);
- невозможность поддержки параметров качества обслуживания (QoS);
- обеспечение свободы перемещения оборудования пользователя в пределах его помещения;
- дальность передачи Ethernet пакетов может быть больше 100 м.

При этом существуют такие ограничения:

- требуется «изоляция» PLC-сегментов (от квартиры к квартире: по необходимости);
- максимум 16 «Home Plug» PLC адаптеров в одном сегменте.

На рисунке 3 приведена схема такого же сценария но с применением Access BPL. Отличие состоит в том, что в помещении клиента устанавливается минимум один BPL-HeadEnd (на рис. 3 обозначены как «OPERA PLC Head End») и необходимое количество BPL-CPE (на рис.3 обозначены как «OPERA PLC CPE», «OPERA PLC/WiFi CPE», «OPERA

PLC/VoIP CPE») требуемой функциональности. BPL-HeadEnd связывает Ethernet сеть провайдера с BPL сетью клиента, а BPL-CPE для подключения BPL сети клиента к абонентским Ethernet устройствам.

Отличительные особенности такого сценарии:

- возможность предоставления всех классов услуг доступа (One Play, Double Play, Triple Play);
- поддержка параметров качества обслуживания (QoS);
- обеспечение свободы перемещения оборудования пользователя в пределах его помещения;
- дальность передачи Ethernet пакетов может быть больше 100 м.

При этом существуют такие ограничения:

- требуется «изолирование» PLC-сегментов (от квартиры к квартире: по необходимости);
- максимум 64 BPL-CPE на один BPL-HeadEnd.



Рис. 3. Сценарий 2 применения Access BPL: «Замена квартирной разводки»

Рассмотрим следующий сценарий - «Замена ДРС» (домовая распределительная сеть). В нем предусматривается соединение оборудования точки присутствия оператора, в которой устанавливается BPL-HeadEnd, с BPL-CPE различных клиентов (рис. 4) посредством кабельных силовых стояков, т.е. для организации «последнего шага». При этом в помещении пользователя BPL-CPE выполняет роль шлюза между BPL сетью и абонентской LAN. Реализация такого сценария осуществима только на базе Carrier Class BPL.

Отличительные особенности такого сценарии:

- возможность предоставления всех классов услуг доступа (One Play, Double Play, Triple Play);
- позволяет оператору сэкономить на строительстве домовых распределительных сетей;
- отличное решение в случае серьезных сложностей прокладки абонентских линий по существующим межэтажным слаботочным стоякам;
- дальность передачи Ethernet пакетов может быть больше 100 м.

При этом существуют такие ограничения:

- скорость PLC-кластера делится на все CPE;
- BPL сегмент должен поддерживать прозрачную передачу маркировки VLAN;
- максимум 64 BPL-CPE на один BPL-HeadEnd.

Сценарий 4 «PLC сеть доступа» (рис.5) предусматривает использование технологии PLC для построения сетей доступа, т.е. организации «последней мили». Реализация осуществима только на базе CarrierClassBPL и востребована, в основном, при низкой плотности клиентов. Сценарий предусматривает установку точки присутствия оператора либо в трансформаторной подстанции, которая обслуживает группу зданий либо в каждом здании, как в сценарии 3 «Замена ДРС». Кроме того в нем предусматривается отсутствие абонентской Ethernet-LAN, которая заменяется полностью на BPL-LAN. Соединение

оборудования точки присутствия оператора, в которой устанавливается BPL-HeadEnd или их группа, с BPL-CPE различных клиентов (рис. 5) в различных зданиях осуществляется посредством электрических питающих кабелей и кабелей силовых стояков, т.е. для организации «последней мили». При этом в помещении пользователя BPL-CPE выполняет не роль шлюза между BPL сетью и абонентской LAN, а роль BPL-Ethernet адаптера. Реализация такого сценария осуществима только на базе Carrier Class BPL.

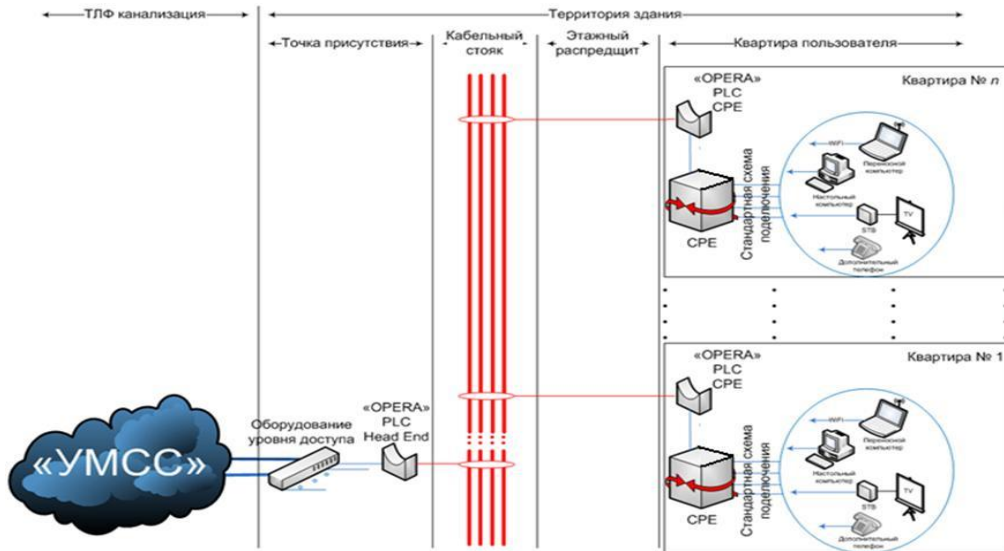


Рис. 4. Сценарий 3 применения Access BPL: «Замена ДРС»

Отличительные особенности такого сценарии:

- возможность предоставления всех классов услуг доступа (One Play, Double Play, Triple Play);
- позволяет оператору сэкономить на строительстве домовых распределительных сетей;
- позволяет оператору сэкономить на строительстве или аренде телефонной канализации;
- отличное решение в случае серьезных сложностей прокладки абонентских линий по существующим межэтажным слаботочным стоякам и каналам телефонной канализации;

При этом существуют такие ограничения:

- скорость PLC-кластера делится на все CPE;
- BPL сегмент должен поддерживать прозрачную передачу маркировки VLAN;
- максимум 64 BPL-CPE на один BPL-HeadEnd.

3. Сценарии применения BPL для задач АСКУЭ (AMR)

Типовое решение для задач АСКУЭ на базе PLC должно предусматривать построение BPL-сети доступа и замену всех электрических счетчиков на цифровые с встроенным PLC-адаптерами, что на сегодняшний день в Украине высокой актуальности проблемы внедрения энергоэффективных технологий в масштабах всей страны.

Общий анализ предложений и тестовых полигонов по созданию АСКУЭ показывает, что главной проблемой является транспортирование к вычислительным центрам энергокомпаний готовых данных о потреблении электроэнергии, тепла и т.д. непосредственно со счетчиков или с групповых контроллеров. На рис. 6 приведена обобщенная схема наиболее распространенных систем АСКУЭ.

Исходя из и изложенного, акцент в применении BPL для предоставления услуг под задачи АСКУЭ следует делать на способах транспортировки учетных данных. При этом следует исходить из следующих исходных данных:

- интерфейсы счетчиков: RS-232 или RS-485;
- интерфейсы контроллеров: Ethernet, RS-232 или RS-485;

- интерфейсы ЦОД: Ethernet;
- контроллер может обслуживать одно или группу зданий.

Тогда задача может быть сведена к следующему: требуется обеспечить транспорт для системы сбора данных.

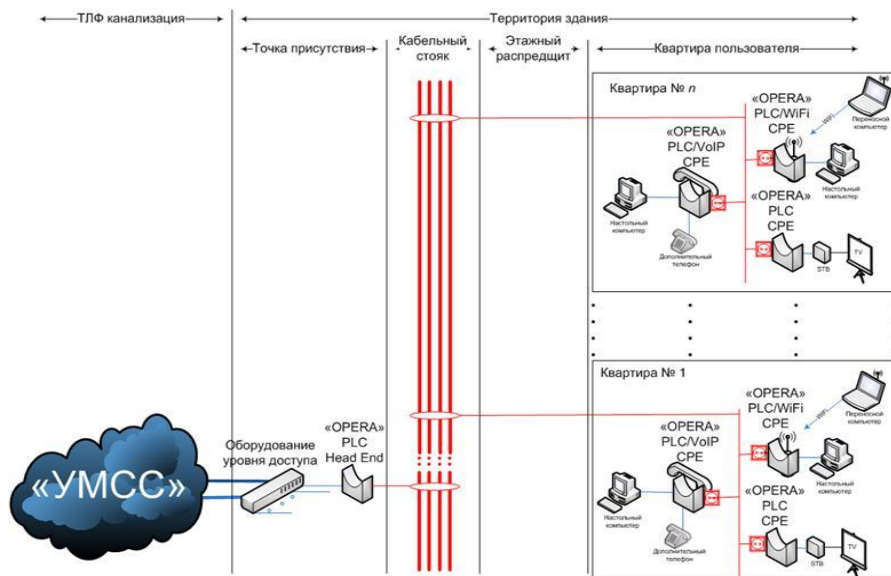


Рис. 5. Сценарий 4 применения Access BPL: «PLC сеть доступа»

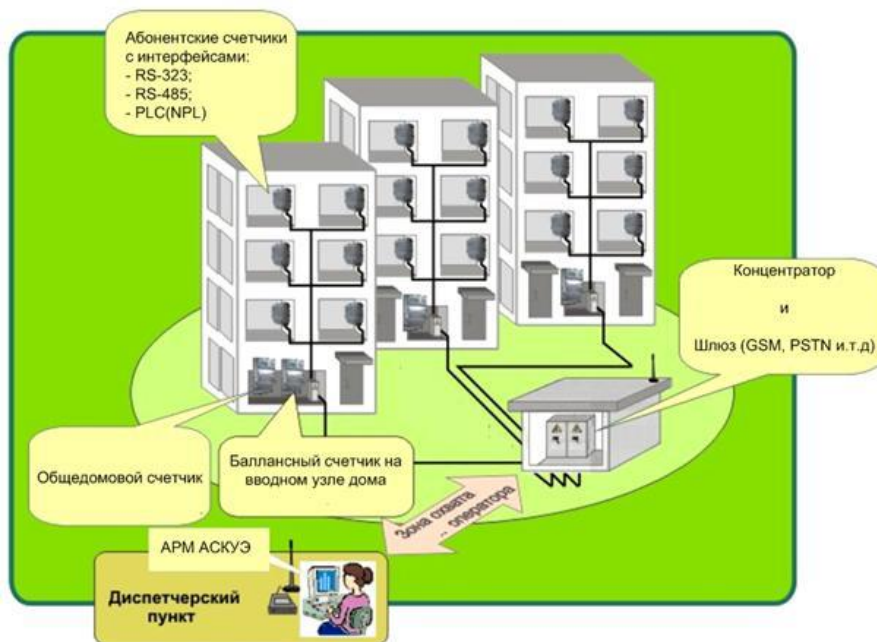


Рис. 6. Обобщенная схема наиболее распространенных систем АСКУЭ

Сценарий 1 предусматривает следующую схему организации связи (рис. 7). Счетчик подключается к конвертеру, который преобразует интерфейс счетчика в Ethernet. Выход конвертера подключается к CPE клиента (либо BPL-CPE). Далее CPE клиента (либо BPL-CPE) соединяется с базовой Metro Ethernet сетью, которая транспортирует данные до ЦОД (центра обработки данных) энергокомпании.

При этом:

- счетчики клиентов подключаются в сеть Metro Ethernet используя конвертеры RS-to-Ethernet через свободный порт абонентского CPE. Счетчики не клиентов подключаются в сеть Metro Ethernet используя конвертеры RS-to-Ethernet через свободный порт оборудования

уровня доступа;

- ЦОД энергокомпании подключается в сеть Metro Ethernet любым стандартным способом;
- все счетчики и ЦОД объединены в одну VLAN и вопросы безопасности обеспечиваются на стороне энергокомпании и производителями счетчиков/конверторов.

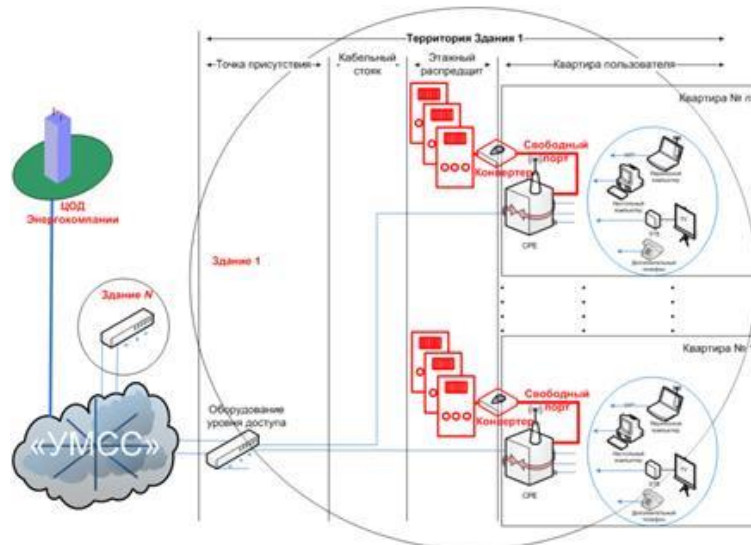


Рис. 7. Сценарий 1 АСКУЭ: Счетчик $\diamond$ Конвертор $\diamond$ CPE (BPL-CPE) $\diamond$ Сеть Metro Ethernet $\diamond$ ЦОД

Сценарий 2 предусматривает следующую схему организации связи (рис.8). Контроллер счетчиков (как правило персональный компьютер) подключается к коммутатору доступа напрямую либо с использованием BPL-CPE, а базовая Metro Ethernet сеть транспортирует данные до ЦОД.

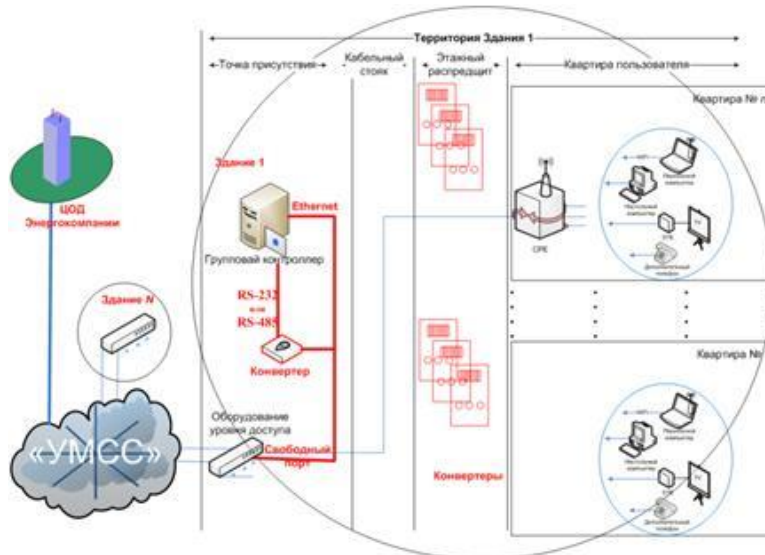


Рис. 8. Сценарий 2 АСКУЭ: Контроллер $\diamond$ Сеть Metro Ethernet $\diamond$ ЦОД

При этом:

- групповые контроллеры систем АСКУЭ подключаются в сеть Metro Ethernet используя либо конверторы RS-to-Ethernet, либо напрямую через свободный порт оборудования уровня доступа⁴
- ЦОД энергокомпании подключается в сеть Metro Ethernet любым стандартным способом;

- все контроллеры объединены в одну VLAN и вопросы безопасности обеспечиваются на стороне энергокомпании и производителями счетчиков/конверторов.

В случае необходимости подключения счетчиков или групповых контроллеров, которые находятся на трансформаторных подстанциях 10/0,4кВ, логика подключения не меняется. В таких случаях должна использоваться только сеть на пазе BPL.

Выводы

1. Расчеты показывают, что наиболее экономичным является сценарий 3 «Замена ДРС». Однако даже в этом случае, стоимость одного «стандартного сервис включения» немного выше стандартного решения с прокладкой кабелей пятой категории.

2. При сравнении стандартных подключений с нестандартными следует учитывать полные затраты владения в том числе затраты на организацию межэтажных слаботочных стояков и телефонной канализации, стоимость которых высока и не всегда возможна. В таких ситуациях BPL становится экономически обоснованным решением, а иногда и единственным.

3. Параллельное развертывание BPL сетей доступа и NPL-AMR сетей [7] позволяет получить еще более экономически выгодное решение от синергии усилий операторов телекоммуникаций и энергораспределяющих компаний.

Список использованной литературы

1. Недашківський О.Л. Аналіз нормативно-правової бази, що визначає системні вимоги до побудови мереж на основі технології PLC // Системи управління, навігації та зв'язку.- 2014, випуск 1(29) –С. 115-119.

2. Недашківський О.Л., Дослідження місця мереж на основі PLC в структурі існуючих і перспективних хребтів для «останньої милі» // Наукові записки Українського науково-дослідного інституту зв'язку.-2014.-№2(30). –С. 61-66.

3. ITU-T Recommendation G.9960 [Електронний ресурс] // - Режим доступа: <http://www.itu.int/rec/T-REC-G.9960/en> (08.11.2016 р.).

4. HomePlugAlliance _ Home.htm [Електронний ресурс] // - Режим доступа: <http://www.homeplug.org/> (08.11.2016 р.).

5. IEEE 1901-2010 [Електронний ресурс] // - Режим доступа: <http://standards.ieee.org/findstds/standard/1901-2010.html> (08.11.2016р.).

6. MEF 33: Ethernet Access Services Definition [Електронний ресурс] // - Режимдоступу: https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_4.pdf (08.11.2016 р.).

7. Недашківський О.Л. Особливості використання технології BPL в якості технології мереж доступу // 6-а Міжнародна науково-практична конференція «Інфокомунікації – сучасність і майбутнє», ОНАС, Одеса 27-28 жовтня 2016 г.

Автори статті

Недашківський Олексій Леонідович – кандидат технічних наук, доцент, доцент кафедри Інформаційно-комунікаційних технологій, Державний університет телекомунікацій, Київ, Україна. Тел. +380 67 506 20 00. E-mail: al_1@ua.fm.

Authors of the article

Nedashkivskyy Oleksiy Leonidovych - candidate of science (technic), assistant professor, assistant professor of Information and communication technologies chair, State university of telecommunications, Kyiv, Ukraine. Tel. +380 67 506 20 00. E-mail: al_1@ua.fm.

Дата надходження в редакцію: 12.01.2017 р.

Рецензент: д.т.н., проф. А.І. Семенко

Bondarenko T.G.; Zeniv I.O.; Nizhnyk R.S.

RESULTS OF RESEARCH THE SOLID-STATE WAVE GYROSCOPE WITH METALLIC RESONATOR

Bondarenko T. G., Zeniv I.O., Nizhnyk R.S. Research results of solid-state wave gyroscope with metallic resonator.

In proposed article we present the results of an experimental research of solid-state wave gyroscope with a metal resonator. The developed block diagram of the equipment is described, which includes a low noise buffer amplifier of the capacitive sensor, a band-pass filters, a microcontroller for the formation of control signals of the equipment, a high-voltage drive pulse amplifier and a high-frequency pulse power supply. The oscillograms of the measured gyro sensor signals are shown during the rotation of the resonator and in its stationary state. The principle of formation of high-voltage excitation pulses resonator described. The phase and amplitude of signals carry information about the gyroscope angular rate and about the direction of rotation. The results prove the propriety of calculations to optimize the parameters of electronic circuits and that the proposed principle of signal processing can be used to build solid-state gyroscopes with metal resonators.

Keywords: solid state wave gyroscope, metallic resonator, rotation of resonator, oscillograms of the gyro sensor.

Бондаренко Т.Г., Зенів І.О. Ніжний Р.С. Результати дослідження твердотільного хвильового гіроскопу з металевим резонатором.

У статті, що пропонується, наведені результати експериментального дослідження твердотільного хвильового гіроскопу з металевим резонатором. Описано розроблену структурну схему устаткування, яка містить малошумливий буферний підсилювач ємнісного датчика, смугові фільтри, мікроконтролер для формування керуючих сигналів апаратури, високовольтний підсилювач імпульсів розкачування, високочастотний імпульсний блок живлення. Описано принцип формування високовольтних сигналів розкачування резонатора. Наведені осцилограми сигналів датчика гіроскопу, що виміряні під час його обертання та у непорушному стані. Фаза та амплітуда сигналів несуть інформацію про кутову швидкість обертання гіроскопу та про напрям повороту. Отримані результати доводять вірність розрахунків з оптимізації параметрів електронної схеми та те, що запропонований принцип обробки сигналів може бути використаний для побудови твердотільних гіроскопів з металевим резонатором.

Ключові слова: твердотільний хвильовий гіроскоп, металевий резонатор, обертання гіроскопу, осцилограми сигналів датчика гіроскопу.

Бондаренко Т.Г., Зенів И.О. Ніжний Р.С. Результаты исследования твердотельного волнового гироскопа с металлическим резонатором.

В предлагаемой статье приводятся результаты экспериментального исследования твердотельного волнового гироскопа с металлическим резонатором. Описана разработанная структурная схема аппаратуры, включающая малошумящий буферный усилитель емкостного датчика, полосовые фильтры, микроконтроллер для формирования управляющих сигналов аппаратуры, высоковольтный усилитель импульсов раскачки и высокочастотный импульсный блок питания. Описан принцип формирования высоковольтных сигналов раскачки резонатора. Приведены осциллограммы измеренных сигналов датчика гироскопа во время вращения резонатора и в его неподвижном состоянии. Фаза и амплитуда сигналов несут информацию про угловую скорость вращения гироскопа и про направление поворота. Полученные результаты подтверждают правильность расчетов по оптимизации параметров электронной схемы и то, что предлагаемый принцип обработки сигналов может быть использован для построения твердотельных гироскопов с металлическим резонатором.

Ключевые слова: твердотельный волновой гироскоп, металлический резонатор, вращение гироскопа, осциллограммы сигналов датчика гироскопа.

Introduction

Many of the well-known works [1-4] describe the design and features of the operation of a solid-state wave gyroscope. However, gyroscopes with dielectric (quartz or sapphire) resonators were usually considered there. A theoretical calculation of the sensitivity of the circuit for measuring the quality factor of a solid-state wave gyroscope was carried out. The article presents

the results of an investigation of a gyroscope with a metal resonator, which, as is well known, has a much lower Q-value.

The main material research

1. Overall block diagram

For the measurement of small mechanical vibration of resonator is proposed to use signal processing method with the capacitive sensor, as in the famous condenser microphone. The capacitor is charged through to high voltage. If you change the distance between the plates of the capacitor, it caused changes and the voltage across it. This voltage signal is to be amplified. Thus, the signal voltage will modulate the voltage on the capacitor.

The entire electronic circuit was assembled on four boards:

- 1) pre-amplifier with high input impedance and low noise, the board should be placed directly close to resonator,
- 2) main board, on which located: the amplifier - bandpass filter and amplifier of high-voltage excitation pulses,
- 3) power supply unit board,
- 4) microcontroller board.

Overall block diagram is shown in Figure 1.

Readout principle is the same: high DC voltage of +104V is applied to the common electrode of the gyroscope. Readout signals electrodes of two channels - main and quadrature, are charged to this high voltage. When vibrations resonator varies the distance between the common electrode and the partial electrodes of capacitors, then respectively, changes the voltage on the partial plates.

The preamplifier board receives the main and quadrature channels signals from resonator. Also to the preamplifier board come the signals: excitation impulses; ban impulse to key circuit performing disconnection of the amplifier inputs in moments of action the excitation pulse.

In main amplifier is performed frequency filtering and gain the main channel signal. The current objective of quadrature channel signal analysis is not put, so this channel is switched off. At the input of the main amplifier board also coming pulses generated by the microcontroller, from which the excitation pulses are generated in the high voltage amplifier.

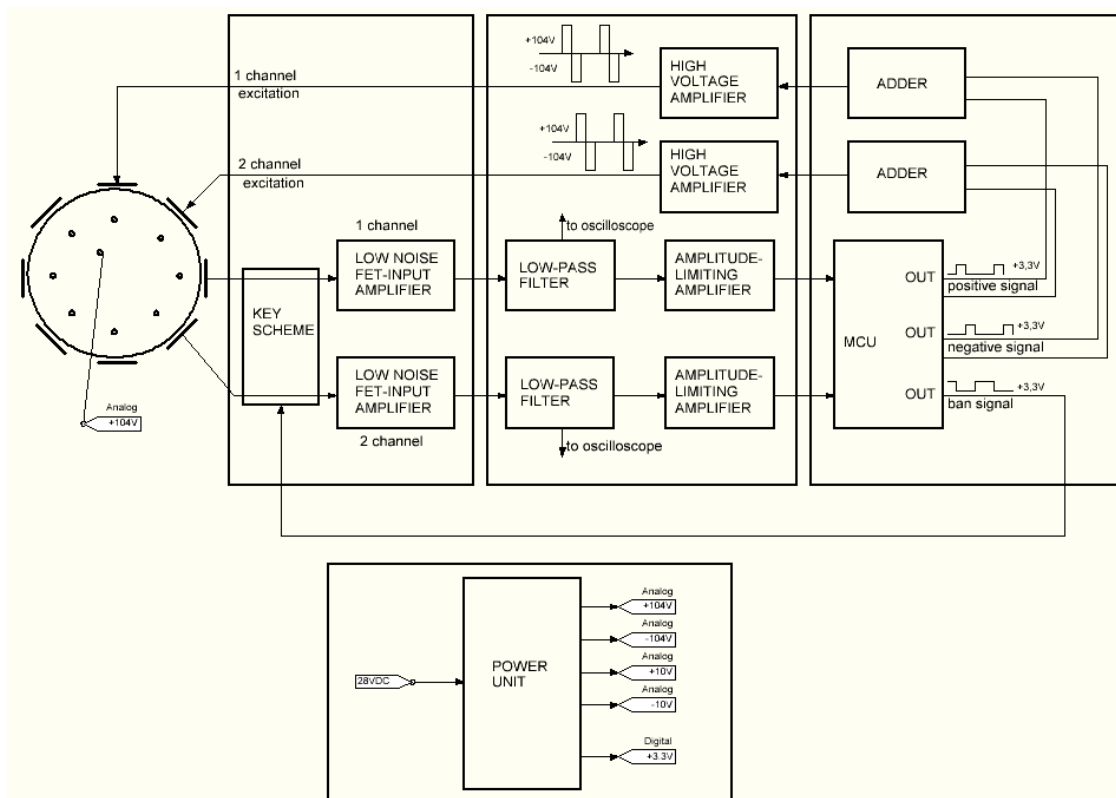


Fig. 1. Block diagram of the entire electronic circuit

Microcontroller card receives synchronization signal from an external master oscillator. In moments determined by the synchronization pulse, the microcontroller generates: pulses for creating the excitation pulses; pulse for suppression input voltage for the preamplifier.

The power unit produces stabilized voltage for all circuit boards.

In carrying out the experimental measurements the very strong capacitive coupling between the electrodes of the resonator has been found, in the case of a metal resonator. Measurements showed that the parasitic capacitance connections between pairs of electrodes arranged perpendicularly was, on various occasions, from 23 to 32 pF. This is a large capacity, which leads to the emergence of a strong interference signal to the readout electrodes during the excitation pulses (Figure 2).

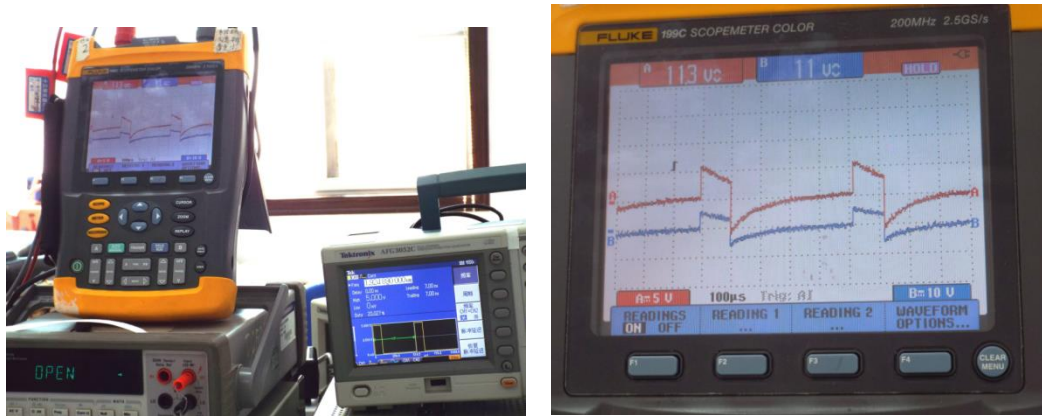


Fig. 2. Measured signals directly on the readout electrodes (without amplification and filtering)

On the screen red and blue color shows the signals taken from the electrodes of the main and quadrature channels (Left unit) at the time of the excitation pulse (right unit). As can be seen from the oscillograms, the interference pulse amplitude reaches 11V.

It is important to compare the displayed values of interference with useful signal value, which can be present on the electrodes of the reading [5,6] in the condenser sensor.

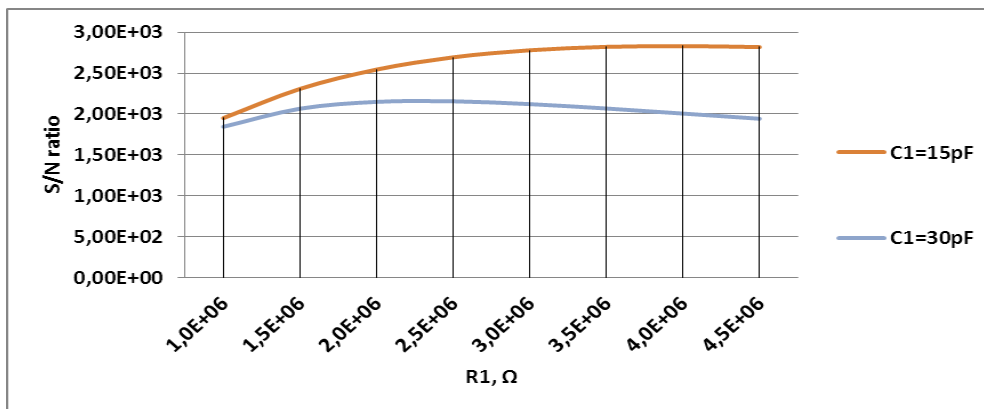


Fig. 3. S/N ratio depending from the value of resistor R1 in the input circuit (C1 - parasitic capacitance)

Calculations show that at the following initial data:

- the frequency of resonator 1935 Hz;
- the capacity of the two opposing readout electrodes 6 pF;
- the modulation index $m=0,001$;
- DC voltage bias $U=100$ V;
- the bandwidth of filter 800 Hz (large enough);
- the spectral density of the amplifier noise 14 nV/ $\sqrt{\text{Hz}}$ (not the best value);

g) value of resistor $R1=3\text{ M}\Omega$ in the input circuit,

so the useful signal amplitude on the readout electrode will be 17,4 mV while the parasitic capacitance $C1=15\text{ pF}$; and will be 13,3 mV with $C1=30\text{ pF}$.

We can see that these values are about 1000 times less than the amplitude of interfering signals which are observed. It is clear that without the use of a special method it will be difficult to select the desired signal on the background of such interference.

In this connection it has been tasked to select the useful signal from the high-power interference and realize resonator's electrostatic excitation to a level at which it will be possible observation of useful signal.

1.1. The preamplifier board

Considering the small amplitude of the signal and the extremely low value of capacitance of the partial capacitors for signal amplification is necessary to use amplifiers with high input impedance and low input capacitance. During action the excitation signal the input of the amplifier is connected to the "ground" with the help of a key scheme. The principle of operation is shown in Figure 4.

In operating mode, the resistance between the chip's pins S1 and D1 is large, leakage current not exceeding 0,01 nA, and input capacitance is 4 pF.

When the ban signal arrived to input IN1, the resistance between the S1 and D1 becomes small, about 40Ω .

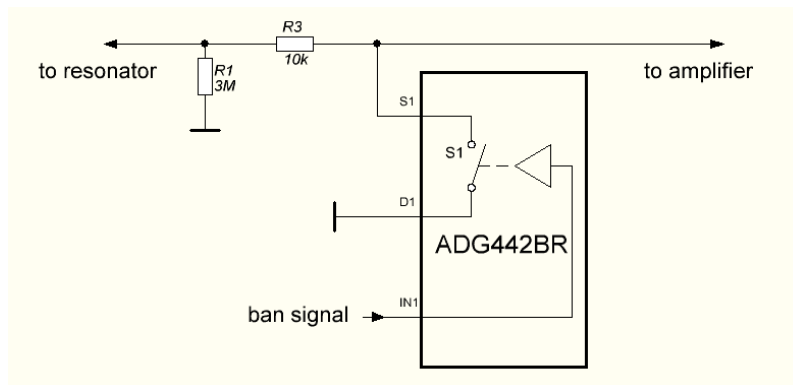


Fig. 4. The principle of the ban of the input signal

The board of the input amplifier also has circuit elements for supply DC +104V to the common electrode resonator (capacitors and inductance of the low pass filter). They are used to filter the DC voltage in order to reduce interference on the common electrode.

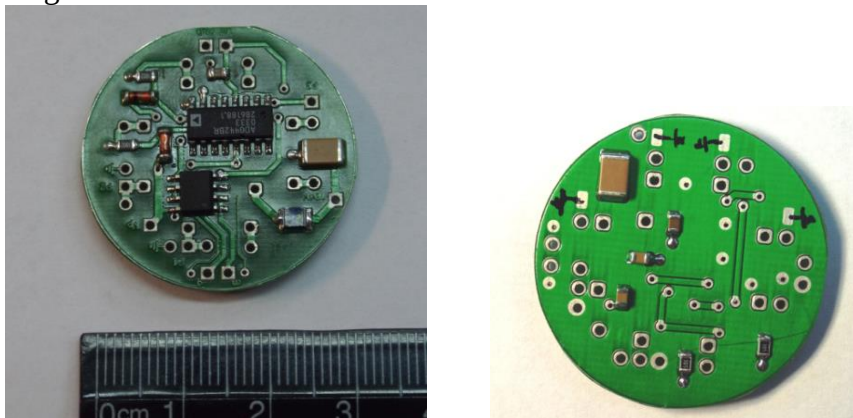


Fig. 5. Photo of preamplifier board

1.2. The main circuit board

Since this board is supposed to be used together with other resonators having a different frequency, the two-stage low-pass filter with cutoff frequency 3500 Hz is applied (Figure 6,7).

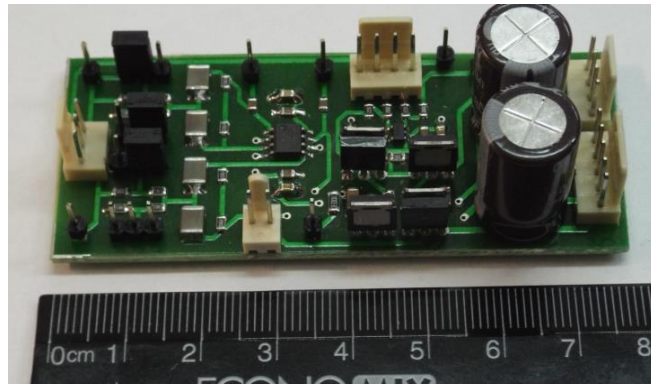


Fig. 6. Photo of main board

8). The schematic diagram of a high-voltage amplifier of drive pulses can be of interest (Figure

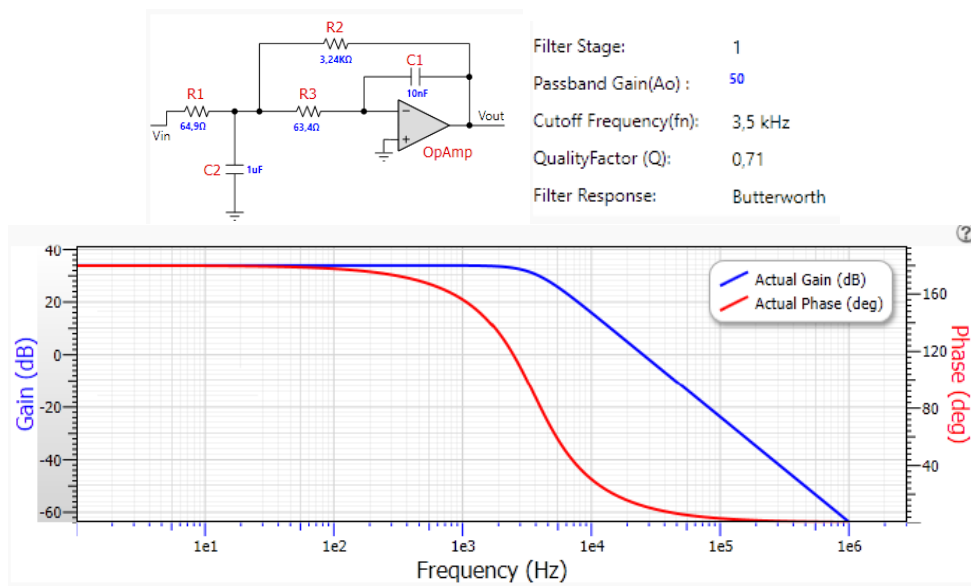


Fig. 7. The results of calculation of the low-pass filter

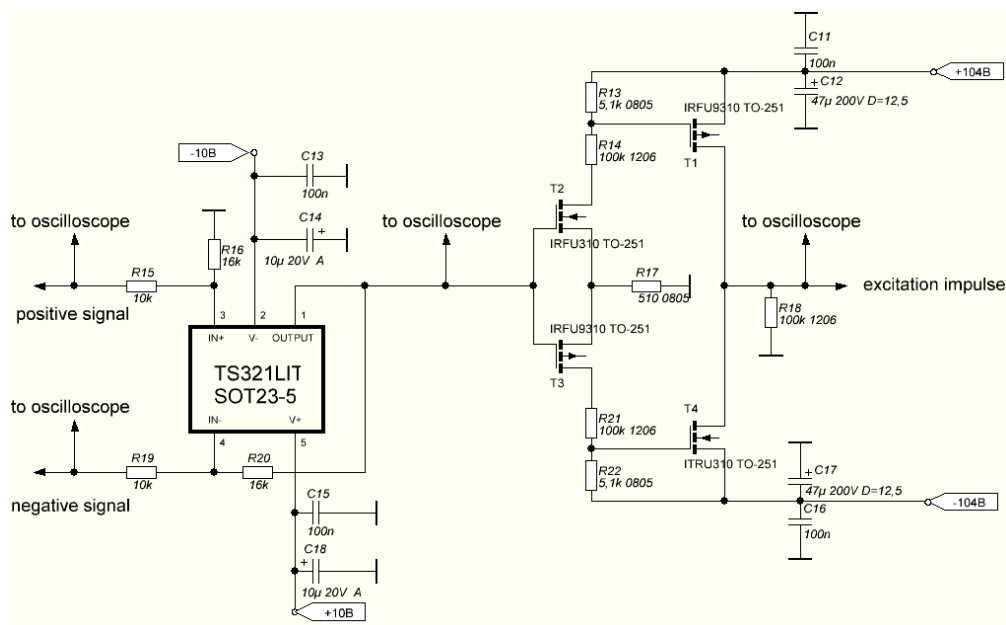


Fig. 8. Circuit diagram of a high-voltage drive pulse amplifier

1.3. The power supply board

Constant voltage + 28V is supplied to the input of the power supply unit (Figure 8). This unit generates the following constant stabilized voltage:

- a) constant voltage +104V for the high voltage amplifier of excitation pulse, and for supplying the bias voltage to the common electrode of the resonator,
- b) constant voltage -104V for the high voltage amplifier of excitation pulse,
- c) constant voltages $\pm 10V$ for chips.

The power supply unit is high frequency switching, running at 43 kHz, uses a chip SELF-OSCILLATING HALF-BRIDGE DRIVER IC IRS21531D, has no singularities.

Converter from +10V voltage to +3.3V for the microcontroller placed on the microcontroller board.

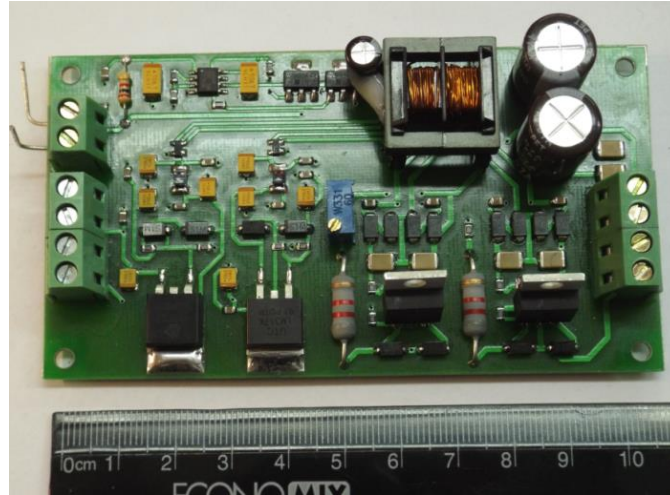


Fig. 8. Photo of power supply board

1.4. Features of microcontroller

In this scheme, the microcontroller (Figure 9) is designed to generate pulses that control the operation of the buffer and the high-voltage amplifiers.

Therefore pulses from the external master clock are used with a repetition rate from 1935 Hz to 2751 Hz, which are applied to the microcontroller input for synchronization of all circuit elements.

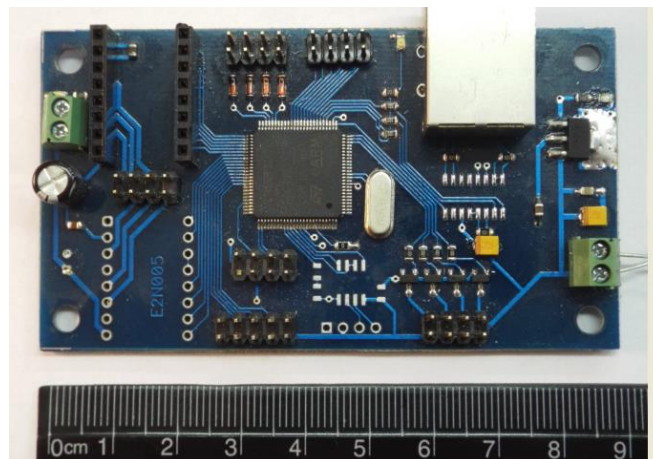


Fig. 9. Photo of microcontroller PCB

Diagram of signals that generates the microcontroller is shown in Figure 10.

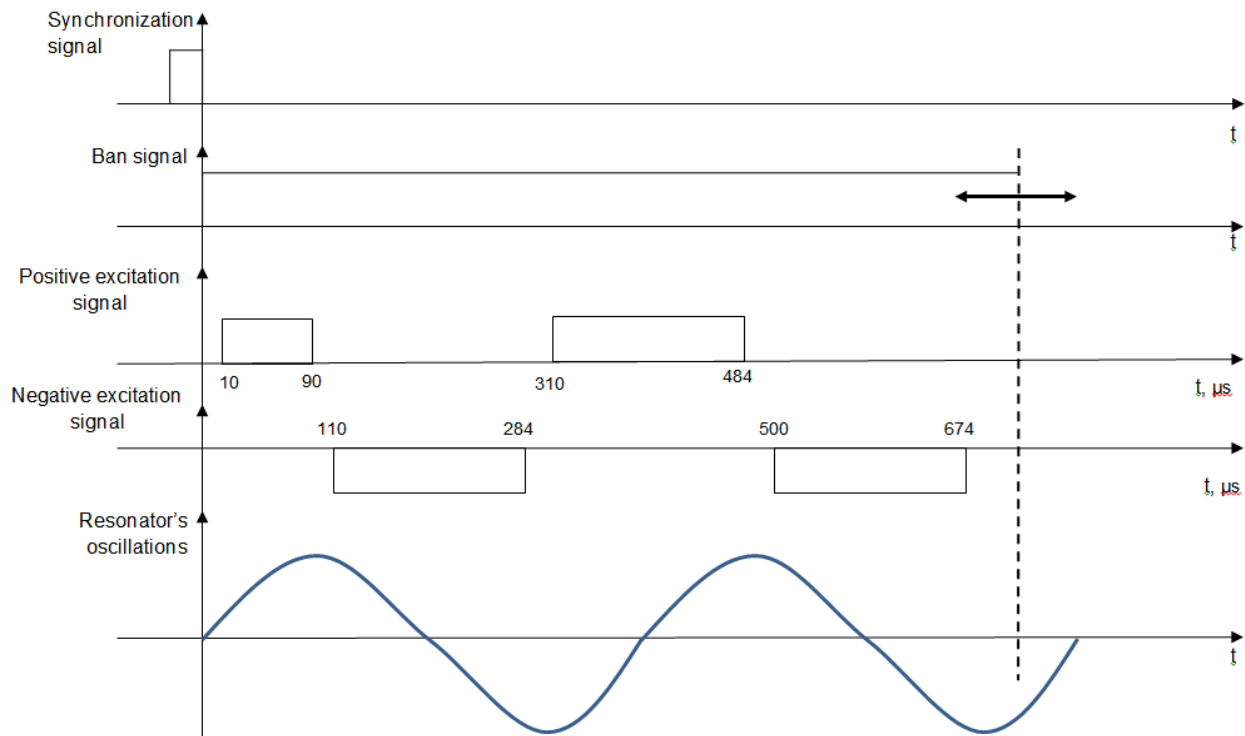


Fig. 10. The signals at the input and output of the microcontroller

In the first quarter of resonator oscillation, when the distance between the plates of the main channel reading capacitor (read-out) decreases, to the orthogonally positioned swinging electrode must be fed a high potential «Excitation signal N4» from high-voltage amplifier.

This will lead to the absence of attraction between the excitation electrode and the resonator, whose potential is large. Voltage on all other electrodes (including on the read-out signal pickoff electrodes) will be zero, and they will be attracted by resonator. Therefore, the resonator will move away from the excitation electrode and approach to read-out electrode.

In the second quarter of resonator oscillation, when the distance near the read-out electrode begins to increase, the output voltage «Excitation signal N5» of the high-voltage amplifier will be negative, so the resonator will be acts force of attraction. Consequently, the resonator will be attracted to excitation electrode and keep away from the read-out electrode.

Excitation pulses are not generated during the signal read-out.

2. Results of measurements and oscillograms

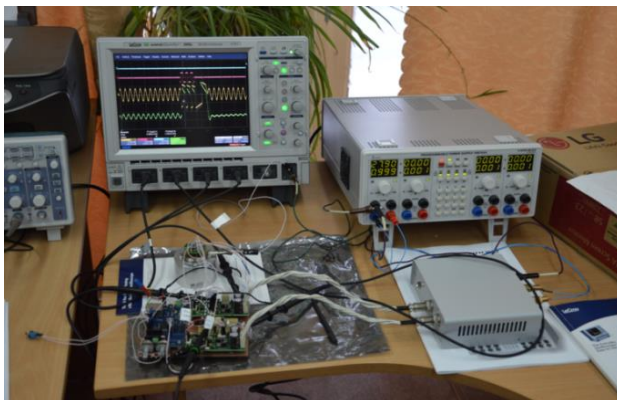


Fig.11. Hardware in experiment

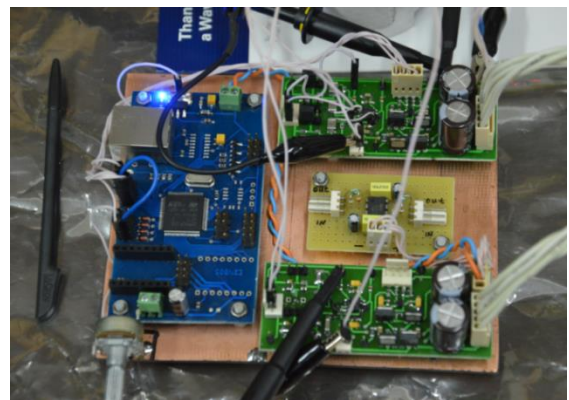


Fig.12. Main board & MCU

2.1. Observation of swinging of the main channel



- ▶ Blue – excitation pulses
- ▶ Yellow – main channel output
- ▶ Green – quadrature channel output

Fig. 13. Observation of swinging of the main channel only. There are oscillations in the quadrature channel appear too. We observe the transfer of energy from the main channel to the quadrature channel

2.2. Observation of swinging of the main and quadrature channels



- ▶ Blue – excitation pulses in main channel
- ▶ Red - excitation pulses in quadrature channel
- ▶ Yellow – main channel output
- ▶ Green – quadrature channel output

Fig.15. The oscillations in the main channel are excited. The oscillations in the quadrature channel are suppressed by the suppression pulses (red)



- ▶ Blue – excitation pulses in main channel
- ▶ Red - excitation pulses in quadrature channel
- ▶ Yellow – main channel output
- ▶ Green – quadrature channel output

Fig. 16. Adjustment of the suppression in the quadrature channel by changing the duration and phase of the first suppression pulse

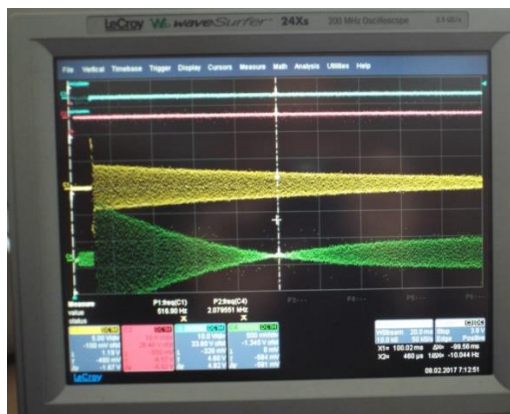


Fig. 17. The oscillogram after setting the suppression in the quadrature channel at time moment 0.1 seconds



Fig. 18. The oscillogram after setting the suppression in the quadrature channel in the neighborhood of the time moment is 0.1 seconds. We observe almost complete suppression of the signal in the quadrature channel. The resonator is stationary

2.3. Observation of the gyroscope rotation

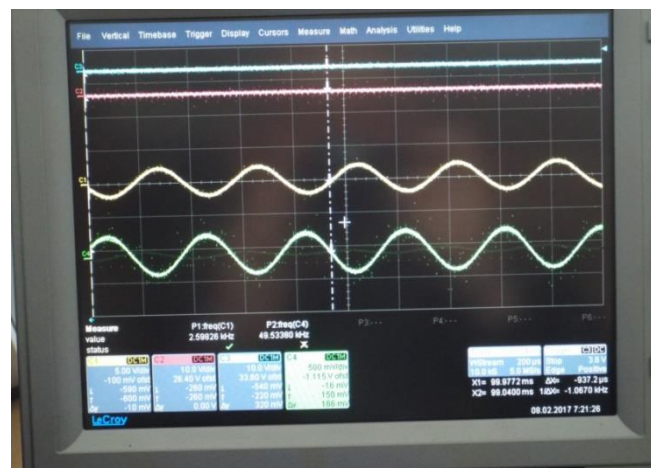


Fig. 19. Rotate the gyroscope clockwise. Rotation speed 10 degrees per second



Fig.20. Rotate the gyroscope counter clockwise. Rotation speed 10 degrees per second. The change in the phase of the oscillations in quadrature channel carries information about the direction of rotation

Conclusions

It has been experimentally verified that it is possible to observe and measure the signals in the quadrature channel when the solid-state gyroscope rotates. The amplitude and phase of the signal carries information about the angular velocity and direction of rotation.

Further research can be carried out in the direction of automatic calibration of the measuring system using a microcontroller. Calibration consists in compensation of oscillations in a quadrature channel at a certain time.

A program for automatic processing of measurement results should also be developed.

References

1. Sarapuloff S.A. 15 Years of Solid-State Gyrodynamics Development in the USSR and Ukraine: Results and Perspectives of Applied Theory //Proc. of the National Technical Meeting of US Institute of Navigation (ION) (Santa Monica, Calif., USA. January 14-16, 1997). — P.151-164.7. http://www.ti.com/ww/ru/prod_amps.html.
2. Sarapuloff S.A., Huinam Rhee, Bondarenko T.G. Simulations & Experiments of Low-Frequency Spectrum of Hemispherical Resonator Gyroscopes (HRG), February 23-25, 2016. Laguna Beach, CA, USA, The 3rd International Symposium on Inertial Sensors & Systems ("ISS-2016"), <http://2017.ieee-inertial.org/>.
3. D.D. Lynch, A. Matthews, G.T. Varty. Transfer of Sensor Technology from Oil-Drilling to Space Applications. 5th Saint Petersburg International Conference on Integrated Navigation Systems, 1998.
4. Kenji Numata, Guiseppe Bertolotto Bianc, Naoko Ohishi, Atsushi Sekiya, Shigemi Otsuka, Keita Kawabe, Masaki Ando, Kimio Tsubono. Measurement of the intrinsic mechanical loss of low-loss samples using a nodal support. - Dep. of Physics, Univ. of Tokyo, Japan. Physics Letters A 276 (2000) 37-46. www.elsevier.nl/locate/pla.
5. Бондаренко Т. Г., Долинская О.Г. Расчет силы, действующей на диэлектрический резонатор твердотельного гироскопа при электростатической раскачке// Системи управління, навігації та зв'язку. – вип. 4(28).- Полтава: Полтавський Національний технічний університет ім. Ю. Кондратюка, 2013. –с.39-42.
6. Бондаренко Т.Г., Зенів І.О. Расчет чувствительности схемы для измерения амплитуды колебаний кварцевого резонатора твердотельного волнового гироскопа // Телекомунікаційні та інформаційні технології. – Київ, 2015. – №2. – с. 61-66.

Автор статті

Бондаренко Тарас Григорович - кандидат технічних наук, доцент кафедри Телекомунікаційних Технологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 050 351 58 67. E-mail: phoenix94@list.ru

Зенів Ірина Онуфріївна - кандидат технічних наук, доцент кафедри Телекомунікаційних Технологій, Державний університет телекомунікацій, Київ, Україна. Тел. +38 050 200 55 05. E-mail: zenechka@ukr.net

Ніжнік Руслан Сергійович - інженер, начальник відділу НПО «Енергія 2000», НПО «Енергія 2000», Київ, Україна. Тел. +38 095 425 95 09. E-mail: blessed_ua@ukr.net

Author of the article

Bondarenko Taras Grigorovich - candidate of sciences (technic), associate professor of Telecommunication Technologies, University of Telecommunications, Kyiv, Ukraine. Tel. +38 050 351 58 67. E-mail: phoenix94@list.ru

Zeniv Iryna Onufriyivna - candidate of sciences (technic), associate professor of Telecommunication Technologies, University of Telecommunications, Kyiv, Ukraine. Tel. +38 050 200 55 05 E-mail: zenechka@ukr.net

Nizhnyk Ruslan Sergeyeovich - engineer, head of the NGO "Energy 2000", Kyiv, Ukraine. NGO "Energy 2000". Тел. +38 095 425 95 09. E-mail: blessed_ua@ukr.net

Дата надходження в редакцію: 18.01.2017 р.

Рецензент: д.т.н., проф. В.А. Дружинін

УДК 621.373-187.4; 621.39.072.9

Федорова Н. В., к.т.н.

АЛГОРИТМ УПРАВЛЕНИЯ МУЛЬТИСЕРВИСНОЙ МАКРОСЕТЬЮ**Fedorova N.V. Algorithm of management of multi-service macro network.**

With development of mobile networks and their adaptation to new types of devices and services to them new and most various demands are made. In this regard, approach "one technology for all" can hardly be effective for support of the growing number of various needs from business, society and certain users. The transparent integration of the existing and new technologies will promote improvement of quality of the user experience and appearance of a number of new services. The active development and functioning of the technologies connecting society in uniform space promotes and carries to creation of a multiservice macronetwork of the operator.

The main difference of networks of the next generation from traditional networks that all information circulating on a network is broken into two components: the signaling information providing switching of subscribers and rendering of services; and directly the user data containing the payload capacity intended to the subscriber (a voice, video, data).

In case of integration into the existing network of the operator, important criterion is the model of control of this network - the multilayer system of control appears.

In multilayer system of control the level at which there is a controller of a multiservice macronetwork exercising direct manipulation of segments of access 2G, 3G, 4G, 5G is offered.

Keywords: multiservice macronetwork, control of a multiservice macronetwork, four-level management system, programmable logic controller, controller of a multiservice macronetwork.

Федорова Н.В. Алгоритм управління мультисервісної макромережею.

Розглянуто перспективи створення мультисервісної макромережі на базі технологій 2G, 3G, 4G і 5G. Визначено актуальні питання й задачі з управління мультисервісною макромережею. Запропонована чотирьохрівнева система управління мультисервісною макромережею. В якості контролера мультисервісної макромережі запропоновано логічний контролер, що програмується. Наведено алгоритм роботи контролера мультисервісної макромережі.

Ключові слова: мультисервісна макромережа, управління мультисервісною макромережею, чотирьохрівнева система управління, логічний контролер, що програмується, контролер мультисервісної макромережі.

Федорова Н.В. Алгоритм управления мультисервисной макросетью.

Рассмотрены перспективы создания мультисервисной макросети на базе технологий 2G, 3G, 4G и 5G. Обозначены актуальные вопросы и задачи по управлению мультисервисной макросетью. Предложена четырехуровневая система управления мультисервисной макросетью. В качестве контроллера мультисервисной макросети предложен программируемый логический контроллер. Показан алгоритм работы контроллера мультисервисной макросети.

Ключевые слова: мультисервисная макросеть, управление мультисервисной макросетью, четырехуровневая система управления, программируемый логический контроллер, контроллер мультисервисной макросети.

Введение

С развитием мобильных сетей и их адаптацией к новым типам устройств и услуг – от интеллектуальных электросчетчиков, автомобилей и подключенных бытовых приборов до промышленных объектов – к ним выдвигаются новые и самые разнообразные требования. В этой связи, подход «одна технология для всех» вряд ли может быть эффективным для обеспечения растущего числа разнообразных потребностей со стороны бизнеса, общества и отдельных пользователей. Технологии продолжают свое развитие в направлении к более высокой производительности и всё большему числу возможностей. В дополнение к существующим технологиям радиодоступа, появятся также новые технологии, которые позволят решать те задачи, которые решить с помощью 2G/3G/4G невозможно [1].

Постановка задачи. Прозрачная интеграция существующих и новых технологий будет способствовать повышению качества пользовательского опыта и появлению целого ряда новых услуг. Активное развитие и функционирование технологий, соединяющих общество в

едином пространстве, способствует и ведет к созданию мультисервисной макросети оператора.

Проблема перехода от традиционных сетей с коммутацией каналов к сетям с коммутацией пакетов является одной из наиболее актуальных для операторов связи. Перспективные разработки в области IP-коммуникаций связаны с созданием комплексных решений, позволяющих при развитии сетей следующего поколения сохранять существующие подключения и обеспечить бесперебойную работу в любой сети доступа: на инфраструктуре медных пар, по оптическим каналам, на беспроводной (WiMAX, WiFi) и проводной (ETTH, PLC и т. д.) сети.

Согласно концепции «неразрушающего» перехода, подобные решения должны позволять точно переводить отдельные сегменты на новые технологии без кардинальной смены всей структуры сети [2-4].

Основное отличие сетей следующего поколения от традиционных сетей в том, что вся информация, циркулирующая в сети, разбита на две составляющие: сигнальная информация, обеспечивающая коммутацию абонентов и предоставление услуг; и непосредственно пользовательские данные, содержащие полезную нагрузку, предназначенную абоненту (голос, видео, данные). Пути прохождения сигнальных сообщений и пользовательской нагрузки могут не совпадать. На рис. 1 показана общая архитектура мультисервисной макросети [2-4].

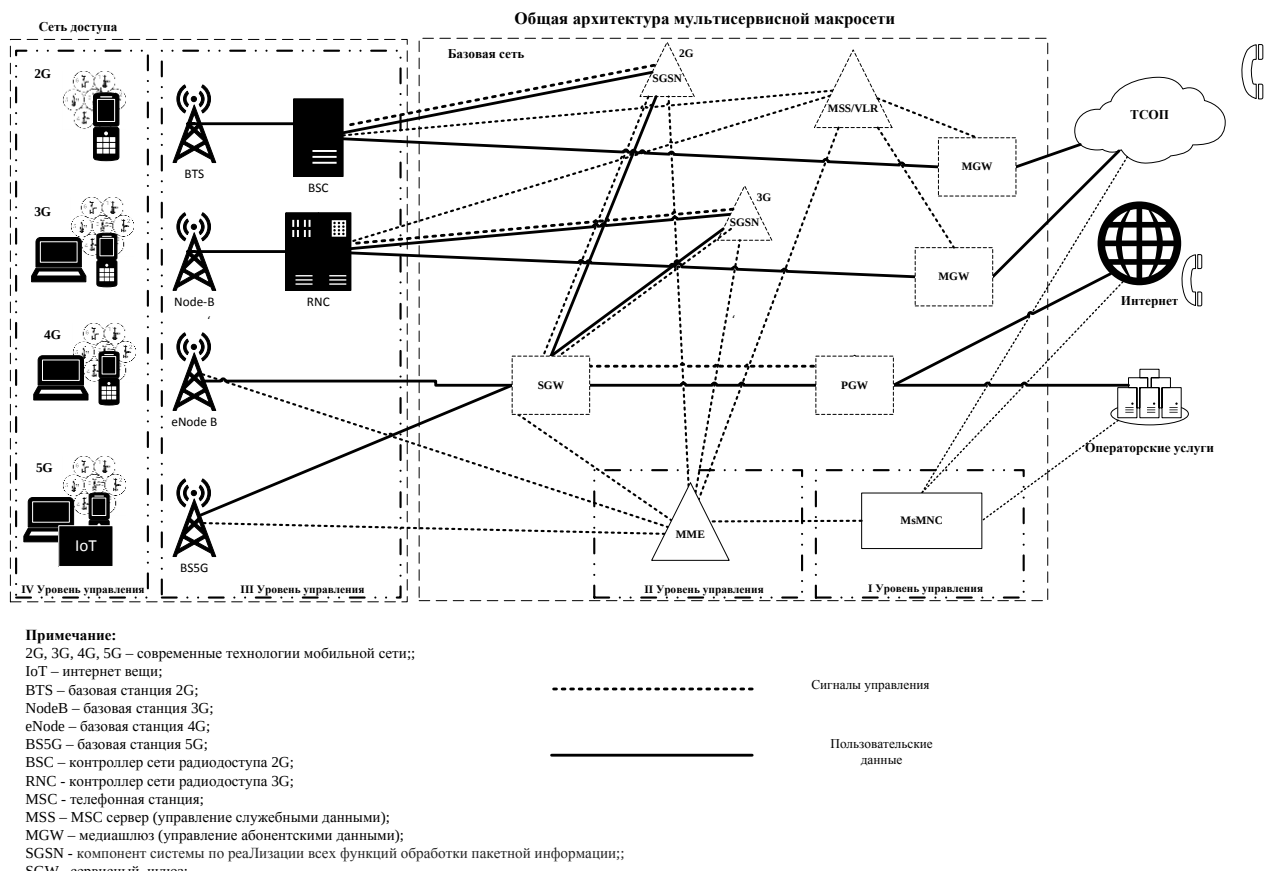


Рис. 1. Общая структура мультисервисной макросети

При интеграции в существующую сеть оператора, важным критерием является модель управления данной сетью - появляется многоуровневая система управления [3].

Основная часть.

Для мультисервисной макросети, показанной на рис. 1, такая модель системы управления приобретает четыре уровня управления (рис. 2).

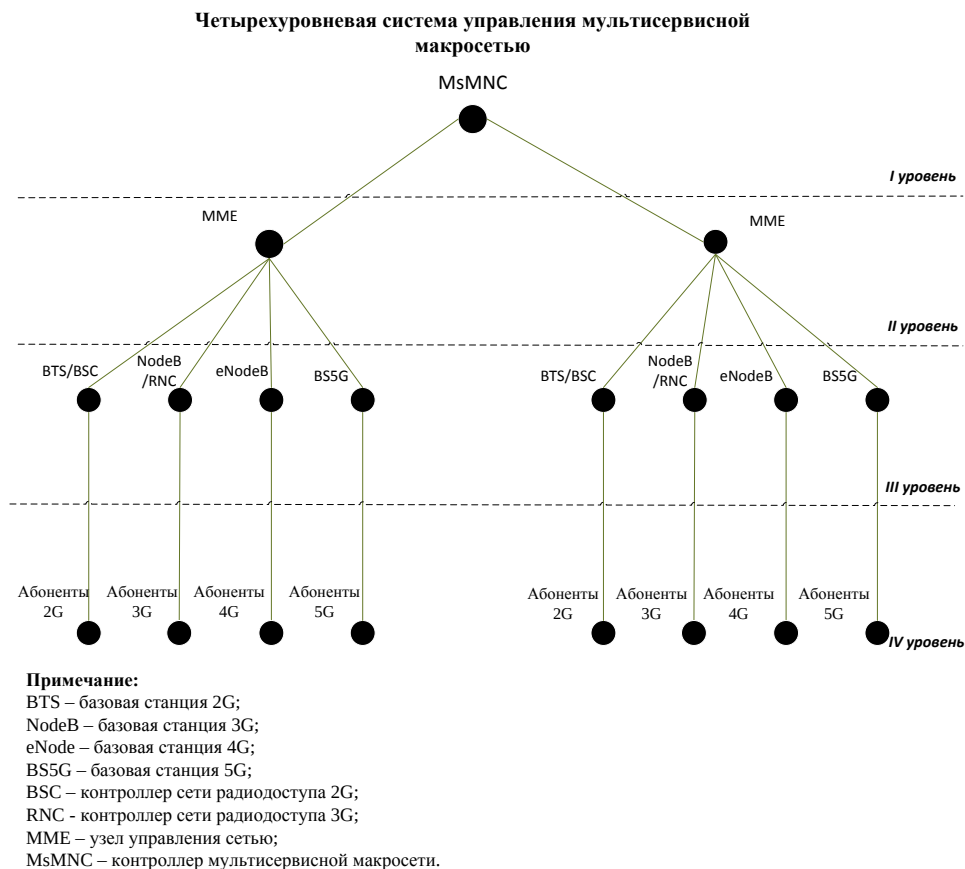


Рис. 2. Четырехуровневая система управления мультисервисной макросетью

Каждый уровень данной системы выполняет набор определенных функций. Уровни II – IV уже известны и предназначены для выполнения ряда функций [3, 4].

Например, на уровне IV находятся абонентские терминалы сегментов доступа 2G, 3G, 4G, 5G, которые могут осуществлять управление своим мобильным ресурсом.

На III уровне размещены базовые станции совместно с контроллерами базовых станций. Одной из основных функций уровня III является управление радиочастотным ресурсом.

На уровне II находятся узлы управления мобильностью (MME - Mobility Management Entity), которые являются контролирующими модулями и отвечают за процедуры обеспечения мобильности. MME предоставляет плоскость функций контроля для обеспечения мобильности между технологиями 4G и 2G/3G в мультисервисной макросети [4].

С появлением на рынке телекоммуникаций технологии 5G [4] для повышения точности и быстродействия мультисервисной макросети возникнет необходимость рационального подхода к управлению данной сети в целом. Поэтому на рис. 1 и 2 предложен еще один уровень – *уровень I*. На данном уровне находится *контроллер мультисервисной макросети* (MsMNC – *Multiservice Macro-Network Controller*), который и осуществляет непосредственное управления сегментами доступа 2G, 3G, 4G, 5G.

Контроллером в системах автоматизации называют устройство, выполняющее управление физическими процессами по записанному в него алгоритму, с использованием информации, получаемой от датчиков и выводимой в исполнительные устройства. А основной целью MsMNC является оценка входного трафика и направление его по конкретному пути прохождения через мультисервисную макросеть согласно изначально заданной таблице приоритетов MsMNC. Для мультисервисной макросети предполагается использовать программируемый логический контроллер (ПЛК), типовая архитектура которого показана на рис. 3.

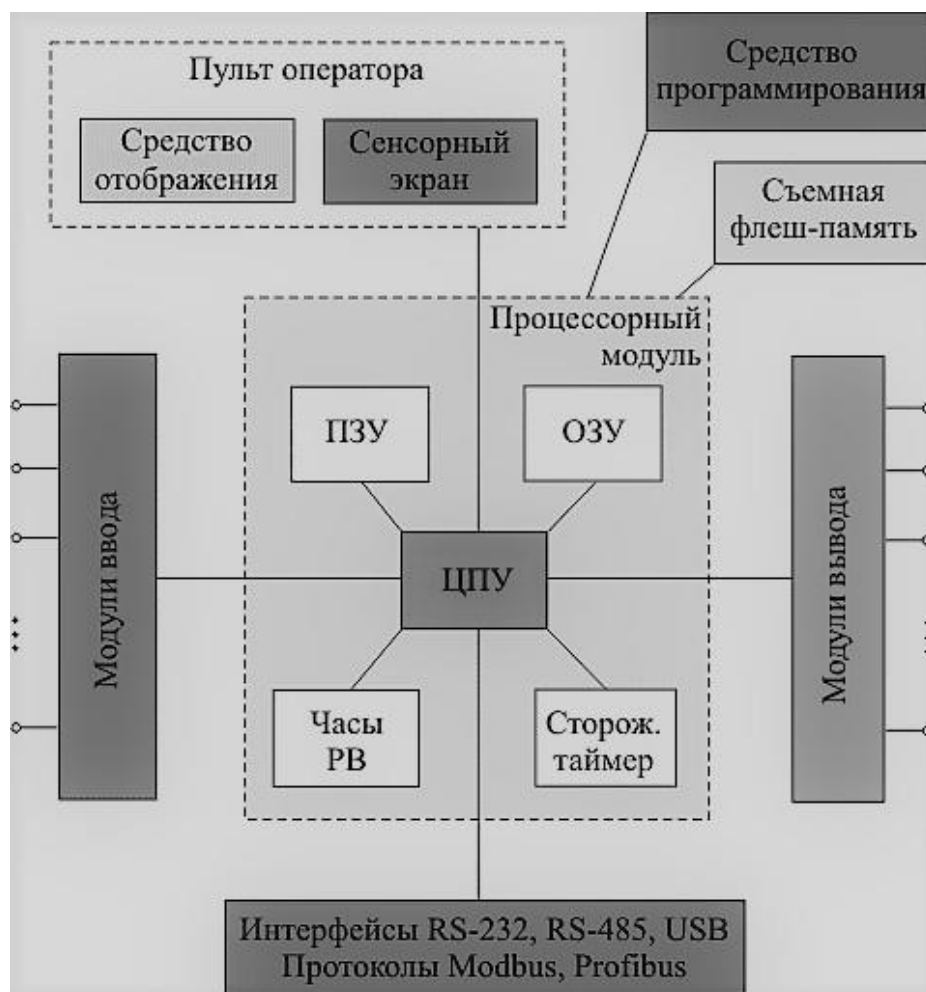


Рис. 3. Типовая архитектура ПЛК

Типовой состав ПЛК включает центральный процессор, память, сетевые интерфейсы и устройства ввода-вывода. Также эта конфигурация дополняется устройством для программирования и пультом оператора, устройствами индикации, иногда - принтером, клавиатурой, мышью или трекболом.

В таблицу 1 сведены данные о возможных сервисах согласно поколений мобильных технологий. Таблица 2 является таблицей приоритетов для контроллера MsMNC.

Таблица 1

Поколение	2G	3G	4G	5G
Сервисы	цифровая телефония и передача сообщений; мобильность и роуминг; поддержка передачи данных	широкополосная передача данных и передача речи по протоколу IP; мобильность и роуминг; сервисная концепция	большая ёмкость, IP-ориентированная сеть, поддержка мультимедиа, скорости до сотен мегабит в секунду	“умный” город “умный” дом
Сеть	сеть с коммутацией каналов	сеть с коммутацией каналов и пакетной коммутацией	сеть пакетной коммутации	сеть пакетной коммутации

Таблиця 2

Поколение	2G	3G	4G	5G
Приоритеты	1	2	3	4
Доступная скорость передачи для абонента	9,6-14,4 кбит/с	до 3,6 Мбит/с	100 Мбит/с – 1 Гбит/с	до 10 Гбит/с
Доступность базовой станции	BTS	NodeB	eNodeB	BS5G
Вход контроллера MsMNC	1	2	3	4

Алгоритм работы MsMNC показан на рис. 4.

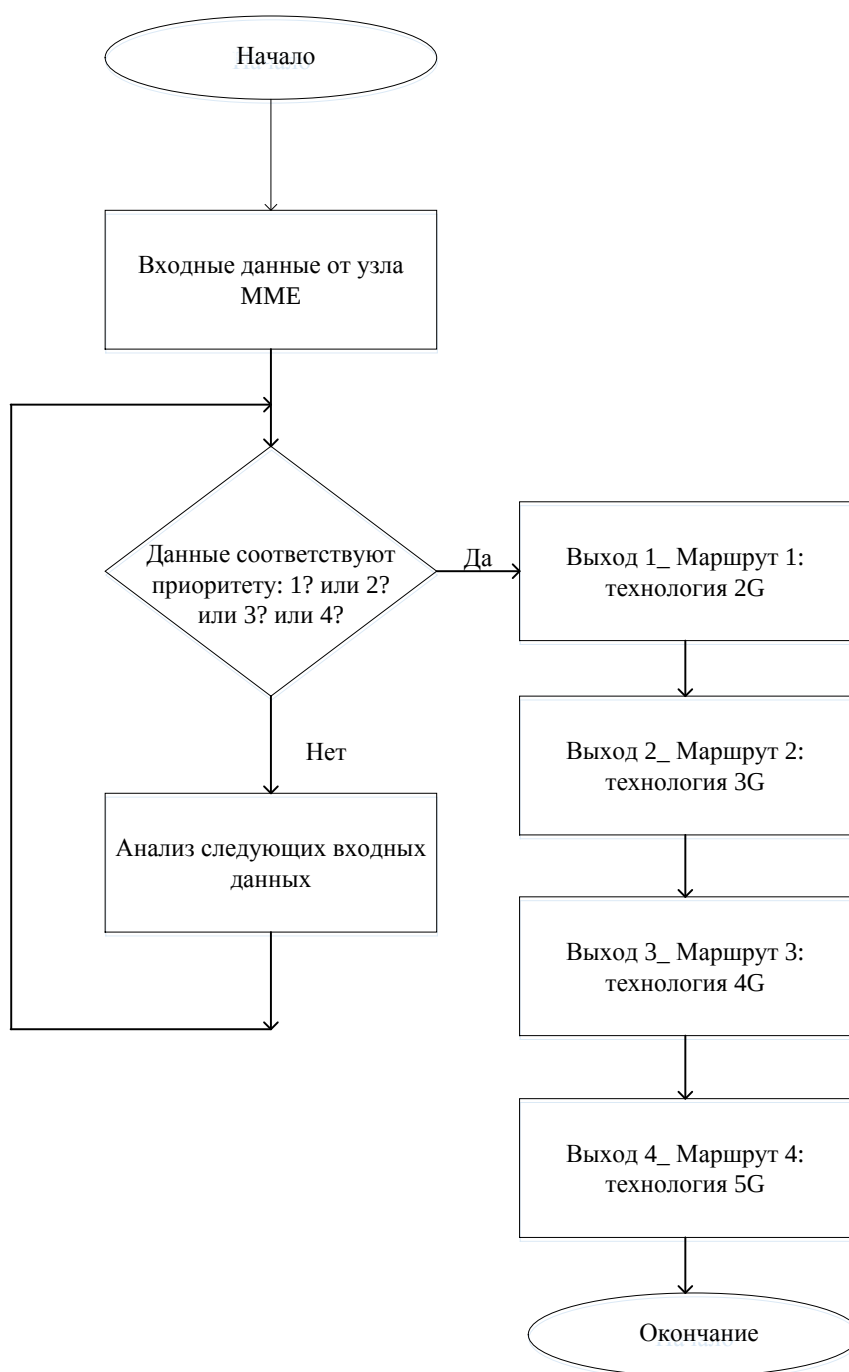


Рис. 4. Алгоритм работы контроллера MsMNC

Контроллер MsMNC получает на свои входы информацию от узла ММЕ - данные об абонентах (какие сервисы им доступны, на каких скоростях, разрешен ли роуминг и пр.). Эти данные носят технический характер и предназначены только для работы сети. Согласно таблице приоритетов (табл.2) контроллер MsMNC делает выбор в пользу того или иного приоритета, при этом оценивая информацию по доступной скорости абоненту и типу доступной базовой станции, и указывает узлу ММЕ маршрут прохождения услуги по мультисервисной макросети.

Выводы

1. При интеграции технологий в одну мультисервисную макросеть оператора, важным критерием является модель управления сетью - появляется многоуровневая система управления.
2. Многоуровневая система управления является разновидностью адаптивной системы, изменяющейся структуры в зависимости от накопленного опыта, а также представляет собой робастную систему управления.
3. Контроллер мультисервисной макросети MsMNC как элемент управления многоуровневой системы управления осуществляет непосредственное управления сегментами доступа 2G, 3G, 4G, 5G.
4. Многоуровневая системы управления обеспечивает требуемые запасы устойчивости при варьируемых показателях быстродействия и точности.

Список использованной литературы

1. Богапов Герман Прыжки через G: 3G – 4G – 5G / [Электронный ресурс]: Герман Богапов // Газета “Зеркало недели. Украина”. - 2016. № 15.
2. Чижиков Дмитрий Мультисервисные сети следующего поколения: потребности рынка, принципы, мониторинг / [Электронный ресурс]: Дмитрий Чижиков // [http: www.iksmedia.ru](http://www.iksmedia.ru).
3. Тихвинский В. О. Сети мобильной связи LTE: технология и архитектура / В. О. Тихвинский, С. В. Терентьев, А. Б. Юрчук. – Москва: Эко-Трендз, 2010. – 139 с.
4. Громаков Ю.А. Сотовые системы подвижной радиосвязи. Технологии электронных коммуникаций / Ю.А. Громаков. - Москва: Эко-Трендз, 1994. - Том 48.

Автори статті

Федорова Наталія Володимирівна – кандидат технічних наук, доцент, Державний університет телекомунікацій, Київ, Україна. Тел. +38 067 224 09 65. E-mail: natasha_f@ukr.net

Authors of the article

Fedorova Nataliya Volodymyrivna – candidate of Science (technic), associate professor, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 067 224 09 65. E-mail: natasha_f@ukr.net

Дата надходження в редакцію: 01.02.2017 р.

Рецензент: д.т.н., проф. В.А. Дружинін

РОЗРОБКА МОДЕЛІ КОНКУРЕНТОСПРОМОЖНОГО ВИПУСКНИКА МЕТОДОМ АНКЕТУВАННЯ ПОТЕНЦІЙНОГО РОБОТОДАВЦЯ

Ilin O.O. The development of a competitive graduate model by the method of questioning a potential employer.

The work defines and justifies the indicators of competency assessment of a competitive graduate student taking into account the requirements of a potential employer. The study shows that competitive young professionals are characterized by both specialized knowledge and personal qualities that are valued in the country's labor market. To determine the degree of student's compliance with these qualities, it is suggested to take into account the requirements of employers for young professionals. The model of a competitive graduate is proposed to be built in several stages. The first stage is devoted to the construction of a database of employers. At the second stage, it was suggested to use the method of questioning employers, which would fully consider the personal qualities of the future employee individually for each employer. At the third stage, based on the cognitive map of the performance indicators, a model of a competitive graduate individually oriented to a specific enterprise is synthesized.

Keywords: model, competence, competitive, graduate, method, employer

Ільїн О.О. Розробка моделі конкурентоспроможного випускника методом анкетування потенційного роботодавця.

В роботі визначено та обґрунтовано показники оцінювання компетенцій конкурентоспроможного випускника з урахуванням вимог потенційного роботодавця. Запропоновано метод анкетування потенційних роботодавців, який би всебічно враховував особисті якості майбутнього працівника індивідуально для кожного роботодавця. На основі когнітивної карти представлення показників розроблено модель конкурентоспроможного випускника індивідуально орієнтованого на конкретне підприємство.

Ключові слова: модель, компетенції, конкурентоспроможний, випускник, метод, роботодавець

Ильин О.А. Разработка модели конкурентоспособного выпускника методом анкетирования потенциального работодателя.

В работе определены и обоснованы показатели оценивания компетенций конкурентоспособного выпускника с учетом требований потенциального работодателя. Предложен метод анкетирования работодателей, который бы всесторонне учитывал личностные качества будущего работника индивидуально для каждого работодателя. На основе когнитивной карты представлений показателей разработана модель конкурентоспособного выпускника индивидуально ориентированного на конкретное предприятие.

Ключевые слова: модель, компетенция, конкурентоспособный, выпускник, метод, работодатель

Вступ та постановка проблеми

Сучасний етап розвитку суспільства ставить нові вимоги до вищих навчальних закладів щодо підготовки конкурентоздатних фахівців. Суть конкурентоздатності полягає не тільки у тому, що випускник є носієм сучасних знань, умінь та навичок (компетенцій), але й ще йому мають бути притаманні певні соціально-психологічні якості [1]. До вимог сучасних роботодавців входять такі параметри, як досвід застосування професійних та інших компетенцій – особистих в т.ч. Цим вимогам складно відповідати в першу чергу молодим спеціалістам, випускникам ВНЗ, які ще не встигли отримати цей досвід, або він мінімальний.

Таким чином, актуальною є задача побудови моделі випускника ВНЗ та визначення технологій, інформаційних в тому числі, для цілеспрямованого розвитку системи необхідних професійних та особистих компетенцій у рамках компетентісно-орієнтованого підходу до навчання у сучасних ВНЗ.

Аналіз досліджень та публікацій

Серед даних чисельних досліджень, присвячених конкурентоздатності випускників системи вищої освіти, наприклад [1 - 3] присутні такі точки зору. В [2] відмічається, що

конкурентоздатними на ринку труда випускників вищих навчальних закладів (ВНЗ) роблять або спеціалізовані знання, що мають високий ринковий попит, або особисті якості, які цінуються у ринковій економіці більше понад знань, отриманих у ВНЗ. Спеціалізовані знання визначаються як спеціальністю, що є найбільш затребуваною на ринку в даний час, так і якістю підготовки в її межах. Що стосується особливих особистих якостей, їх розбивають на дві групи: так звані «ринкові компетенції» та "корпоративні компетенції" [2]. До «ринкові компетенції» відносять такі характеристики працівників (за даними опитування роботодавців, [2]):

- активна життєва позиція;
- серйозність мотивації до професії;
- схильність до саморозвитку;
- працелюбність та бажання працювати;
- вміння комунікувати;
- здатність отримувати результат;
- здоров'я;

А до корпоративних компетенцій відносять наступні характеристики:

- системність мислення;
- професіоналізм;
- прийнятність нового;
- командність;
- стресостійкість;
- вміння відповідати корпоративним нормам;
- результативність;
- сумлінне ставлення до роботи.

Для формування та розвитку цих компетенцій важливі три періоди [2]:

- до вступу у ВНЗ (етап обрання перспективної спеціальності);
- під час навчання у ВНЗ, де формуються професійні та особисті компетенції через додаткові види активності, не передбачені базовою програмою підготовки: додаткові курси, суспільна робота, трудовий досвід тощо;
- після ВНЗ.

У [1] також відзначається, що під час прийому на роботу особистим компетенціям віддається перевага у більшості випадків (75%), ніж якості освіти (63%). В той же час традиційні підходи до навчання в ВНЗ спрямовані саме на підвищення якості освіти.

Окрім того, внаслідок відкриття ринків праці Європи для працевлаштування випускників Українських ВНЗ, на наш погляд, слід враховувати європейський досвід. Для галузі інформаційно-комунікаційних технологій (ІКТ) існує міжнародний досвід опису професійних компетенцій спеціалістів галузі, викладений у робочих документах Європейської рамки компетенцій 2.0 [4]. У ньому професійні компетенції групуються у відповідності до трьох категорій:

- знання (сукупність «знаю що»);
- навички (здатність вирішувати конкретні технічні та управлінські задачі);
- відношення (здатність до аналізу/синтезу, гнучкість, прагматизм тощо).

Нажаль, проблемними питаннями залишаються наступні: яким чином враховувати особливості вимог конкретного роботодавця та яким чином інтегрувати їх у навчальний процес. Оскільки, саме конкретні вимоги до випускника з боку потенційного роботодавця в кінцевому рахунку стануть вирішальними при влаштуванні випускника на роботу. Для вирішення цих проблемних питань пропонується скласти модель випускника, до складу якої повинні увійти окрім професійних компетенцій, і компетенції особистого характеру, ранжированих за ступенем важливості для потенційних роботодавців.

Мета роботи – запропонувати метод анкетування вимог потенційних роботодавців для укладання когнітивної карти конкурентоспроможного випускника ВНЗ.

Основна частина роботи

Для вирішення поставленої задачі доцільно використовувати метод анкетування. Метою його застосування є впорядкування професійних, ринкових та особистих компетенцій випускників ВНЗ за ступенем важливості при отриманні роботи на підприємствах сфери ІКТ. Метод анкетування дозволяє врахувати конкретні особливості підприємств при ранжируванні компетенцій випускника відносно посад, на які вони можуть бути зараховані. Це дозволить, з одного боку, оптимально підбирати випускників для кожного потенційного роботодавця, з іншого – впливати на корегування навчального процесу ВНЗ в умовах змін на ринку праці.

Технологія побудова моделі конкурентоспроможного випускника відповідно до посади та конкретного підприємства передбачає наступні етапи.

1. Вибір й укладання бази даних потенційних роботодавців.

2. Укладання форми та змісту анкети опитування.

3. Побудова когнітивної карти вимог роботодавця до конкурентоспроможного випускника.

4. Вибір методу обробки даних та побудова моделі конкурентоспроможного випускника відповідно до посади та конкретного підприємства.

Перший етап передбачає інформаційний пошук підприємств сфери ІКТ, що діють на території України та потенційно можуть виступати в ролі роботодавців. Такі підприємства заносяться до бази даних потенційних роботодавців. База даних потенційного роботодавця представлена на рис.1.

Наявність бази даних потенційних роботодавців у ВНЗ, з одного боку, дає більш широкі можливості щодо допомоги випускникам у подальшому влаштуванні на роботу, з іншого – можливість студентам проходження практики (стажування) під час навчання.

Назва підприємства	Форма власності	Посада 1	Кількість місць	Когнітивна карта випускника
		...	...	...
		Посада N	Кількість місць	Когнітивна карта випускника

Рис. 1. Структурно-логічна схема бази даних потенційного роботодавця

Це також надає можливості певним чином корегувати набуттям практичних навичок у студентів, наприклад, шляхом виконання курсових робіт, які мають безпосередню практичну значимість для роботодавця. Крім того, визначення підприємств державної форми власності та кількості посад, на які можуть бути влаштовані випускники надає керівнику ВНЗ вагомого аргументу перед відповідними державними установами щодо корегування бюджетних місць для студентів.

Другий етап передбачає розробку форми та змісту анкети опитування. Оскільки результати опитування є складовою єдиної бази даних потенційних роботодавців, то зрозуміло, форма анкети має бути уніфікованою. З іншого боку роботодавцю необхідно надати можливість додавання своїх (на його погляд) важливих характеристик. З цією метою пропонується об'єднати компетенції випускника в узагальнюючі групи, що з психологічної точки зору дозволить роботодавцю сконцентрувати увагу на найбільш вагомим (на його погляд) характеристиках працівника.

З цією метою пропонується сформувати такі узагальнені групи, які характеризують професійні компетенції та особисті якості випускника:

- теоретична підготовка (f_1);
- практичні навички (f_2);
- загальноосвітня підготовка (f_3);
- особисті якості випускника (з урахуванням ринкових і корпоративних вимог) (f_4);
- стан здоров'я (f_5).

Форма анкети представлена в табл. 1.

Таблиця 1. Приклад анкети ранжирування професійних компетенцій та особистих якостей випускника i -м роботодавцем

Код гр.	Найменування групи якостей	Первинні посади в установах відповідного профілю					
		Сфера телекомунікаційних послуг		Сфера програмування (інформаційних послуг в т.ч.)		Сфера безпеки інформаційних та комунікаційних систем	
f_1	теоретична підготовка	9	актуально	9	актуально	10	актуально
f_2	практичні навички	5	рекомендовано	7	рекомендовано	8	актуально
f_3	загальноосвітня підготовка	3	рекомендовано	6	рекомендовано	6	рекомендовано
f_4	особисті якості	3	не актуально	5	рекомендовано	3	рекомендовано
f_5	стан здоров'я	8	актуально	4	рекомендовано	4	рекомендовано

Спочатку кожному роботодавцю із бази даних (див. рис. 1) пропонується впорядкувати групи за ступенем їх важливості з точки зору працевлаштування випускника. Для цього кожній групі встановлюються у відповідність ранги, тобто чисельні значення з інтервалу [1,10], які інтерпретуються через лінгвістичні концепти. Так, інтервал значень [1,3] відповідає концепту «не актуально», інтервал значень [4,7] – «рекомендовано», інтервал значень [8,10] – «актуально». Відповідно до кожної посади потенційний роботодавець надає цифрове значення з інтервалу [1,10] для кожної групи. Відповідний лінгвістичний концепт виставляється представником ВНЗ (особою, яка відповідає за збір й обробку даних). Якщо для всіх посад в якійсь групі є значення «не актуально», то в подальшому дана група позицій роботодавцю не пропонується.

Далі в кожній групі формуються якісні характеристики, що відповідають даній групі показників. При цьому, якщо роботодавець вважає, що запропоновані показники не повні, він додає до анкети ті показники, що є важливими на його думку. Так, наприклад, в першу групу (теоретична підготовка) роботодавець може додавати, наприклад, ті мови програмування, які не зазначені в анкеті, оскільки не вивчаються в даному ВНЗ тощо. До групи «практичні навички», наприклад, можуть включатися з боку роботодавця такі показники, як участь у корпоративних проектах тощо. Кожному показнику в групі потенційний роботодавець також надає цифрове значення з інтервалу [1,10]. Всі цифрові значення інтерпретуються через лінгвістичні концепти: «не актуально» (інтервал значень [1,3]), «рекомендовано» (інтервал значень [4,7]), «актуально» (інтервал значень [8,10]). Для кожної групи відповідно до первинних посад, визначених роботодавцем, складається окрема анкета. Форма анкети є уніфікованою. В ній перераховуються якісні показники, які визначені освітньо-професійною програмою підготовки та навчальними планами ВНЗ (для груп $f_1 - f_3$). Так, до групи f_1 входить перелік фахових навчальних дисциплін, що викладаються у ВНЗ, та які відповідають компетенціям професійним та професійним за спеціалізацією. Крім того, анкета має додаткові пусті рядки, куди роботодавець може за бажанням включити додаткові вимоги щодо теоретичної підготовки випускника, наприклад, знання певної мови

програмування, яка не передбачена навчальним планом ВНЗ. Це дає змогу в моделі управління навчальним процесом налагодити зворотній зв'язок із роботодавцем та враховувати його потреби, наприклад, шляхом введення факультативного курсу. Таке гнучке управління навчальним процесом надає змогу підвищити конкурентоздатність випускника на ринку праці. До групи f_2 входять види діяльності студентів, що характеризують суто практичну складову навчання: дані про виконані курсові та дипломні роботи і проекти, в яких вирішуються конкретні практичні задачі, дані про проходження практики, стажування, участь у реальних проектах та результати наукової діяльності тощо. До групи f_3 входять дані про загальноосвітній рівень випускника: рівень володіння діловою українською мовою, рівень володіння англійською мовою тощо. Група f_4 включає перелік особистих якостей випускника. Приклад анкети щодо особистих якостей випускника представлено в табл. 2.

Таблиця 2. Приклад анкети ранжирування особистих якостей (група f_4) випускника i -м роботодавцем

№	Особисті якості випускника (показники з групи f_4)	Посада					
		Сфера телекомунікаційних послуг		Сфера програмування (інформаційних послуг в т.ч.)		Сфера безпеки інформаційних та комунікаційних систем	
1	активна життєва позиція	10	актуально	3	не актуально	10	актуально
2	серйозність мотивації до професії	1	не актуально	9	актуально	9	актуально
3	схильність до саморозвитку	3	не актуально	9	актуально	10	актуально
4	працелюбність та бажання працювати	3	не актуально	10	актуально	9	актуально
5	вміння комунікувати	7	рекомендовано	8	актуально	8	актуально
6	здатність отримувати результат	3	не актуально	10	актуально	7	рекомендовано
7	системність мислення	2	не актуально	5	рекомендовано	5	рекомендовано
8	прийнятність нового	2	не актуально	4	рекомендовано	7	рекомендовано
9	командність	3	не актуально	5	рекомендовано	5	рекомендовано
10	стресостійкість	6	рекомендовано	4	рекомендовано	9	актуально
11	вміння відповідати корпоративним нормам	1	не актуально	7	рекомендовано	2	не актуально
12	сумлінне ставлення до роботи	1	не актуально	10	актуально	5	рекомендовано

Анкета групи f_5 (стан здоров'я випускника) призначена для виявлення роботодавців, які можуть брати на роботу випускників з обмеженими можливостями.

На третьому етапі укладається когнітивна карта конкурентоспроможного випускника відповідно до кожної початкової посади з точки зору конкретного роботодавця. Власне

когнітивна карта конкурентоспроможного випускника являє собою результати анкетування потенційних роботодавців. Когнітивна карта має уніфіковану форму представлення як відносно посади, так і відносно потенційного роботодавця. До когнітивної карти входять лише ті позиції, які є актуальними або рекомендованими роботодавцем для певної посади. Приклад когнітивної карти конкурентоспроможного випускника визначеного i -м роботодавцем для посади у сфері телекомунікаційних послуг представлена в табл. 3.

Таблиця 3. Приклад когнітивної карти конкурентоспроможного випускника визначеного i -м роботодавцем для посади у сфері телекомунікаційних послуг

Роботодавець: ТОВ "АНТ-МЕД"			
Посада: інженер телекомунікаційних послуг			
Код гр.	№	Найменування	Значення
f_1	1	Теорія алгоритмів	рекомендовано
	25	Управління ІТ-проектами	рекомендовано
	37	Управління проектами в галузі телекомунікацій	актуально
f_2	1	Виробнича практика у компанії телекомунікаційного напрямку	актуально
f_3	1	знання ділової української мови	рекомендовано
f_4	1	активна життєва позиція	актуально
	5	вміння комунікувати	рекомендовано
	10	стресостійкість	рекомендовано
f_5	1	практично здоровий	актуально

Когнітивні карти є складовою бази даних роботодавців (див. рис.1).

На четвертому етапі за когнітивною картою випускника (фактично наданою роботодавцем) будується модель, яка є придатною для подальшої автоматичної обробки. Фактично модель конкурентоспроможного випускника для конкретного роботодавця визначається формулою:

$$H_i^j = \{f_{kl}^q\},$$

де H_i^j – конкретний роботодавець із бази даних (див.рис.1), нижній індекс i – порядковий номер роботодавця в базі даних, верхній індекс j – порядковий номер посади, на яку може претендувати випускник у i роботодавця; f_{kl}^q – множина вимог з боку роботодавця щодо професійних компетенцій та особистих якостей випускника і береться з когнітивної карти (див. табл. 3), нижній індекс: k – порядковий номер групи якостей (в нашому випадку $k \in \{1, 2, 3, 4, 5\}$), l – порядковий номер показника у відповідній групі, верхній індекс q – лінгвістичне значення відповідного показника: актуально (чисельне значення 1), рекомендовано (чисельне значення 2).

Так модель конкурентоспроможного випускника на первинну посаду у оператора телекомунікаційних послуг для i -го роботодавця буде мати наступний вигляд (вихідні дані представлені в табл. 3):

$$H_i^1 = \{f_{11}^2, f_{125}^2, f_{37}^1, f_{21}^1, f_{31}^2, f_{41}^1, f_{45}^2, f_{410}^2, f_{51}^1\}$$

Обробка даних моделі відбувається наступним чином. Модель роботодавця накладається на модель випускника, остання безпосередньо укладається у ВНЗ. Модель випускника також формується на базі когнітивної карти випускника, яка містить результати оцінювання його професійних компетенцій та особистих якостей на інтервалі $[1,10]$, які також приводяться до лінгвістичних концептів: «низький рівень» (інтервал значень $[1,3]$), «середній рівень»

(інтервал значень $[4,7]$), «високий рівень» (інтервал значень $[8,10]$). На відміну від моделі роботодавця, яка містить лише показники, які є або актуальними або рекомендованими з боку роботодавця, модель випускника містить всі показники. Крім того, в неї для f_{kl}^q верхній індекс може приймати значення: 1, яке відповідає інтервалу $[8,10]$, 2 – інтервалу $[4,7]$, 3 – інтервалу $[1,3]$. Для **автоматичного підбору випускників** для кожного роботодавця задається операція перетинання множин моделі роботодавця і моделей випускників. На операцію перетинання множин накладається умова: значення 1 верхнього індексу q у відповідного елемента моделі випускника вважається таким, що перетинається із значенням 2 моделі роботодавця. На фізичному рівні це відповідає тому, що випускник має кращі показники, ніж вимагає роботодавець. Якщо результат перетинання множин є не пуста множина, то це означає, що даний випускник підходить роботодавцю.

Висновки

Запропонований метод анкетування дозволяє мати, з одного боку, повну картину конкурентоздатності випускників на ринку праці в Україні, з іншого – враховувати особливості кожного окремого підприємства. Наявність і ведення бази даних потенційних роботодавців в технологічному плані дозволяє щільно працювати з потенційними роботодавцями і управляти як професійними компетенціями студента, так і його особистими якостями (шляхом мотивування) під час всього навчання. А це, в свою чергу, в умовах жорсткої конкуренції є додатковим вагомим фактором при першому працевлаштуванні.

Побудована модель компетенцій конкурентоспроможного випускника базується на об'єднанні двох множин компетенцій – професійних компетенцій, які побудовані із врахуванням Європейської рамки ІКТ компетенцій, та особистих компетенцій, ранжированих по ступеню важливості потенційними роботодавцями.

Список використаної літератури

1. Н.П. Кириллов, Е.Г. Леонтьев Конкурентоспособность выпускников вузов: проблем и решения // Вестник ТГПУ. - 2014. - №6(147). - С.9-13.
2. А.А. Малышева, И.В. Невраева Компетенции молодых выпускников вузов глазами работодателей // Известия ТПУ. - 2006. - т.309. - №8. - С.225-229
3. Дідківська О.Г. Конкурентоспроможність випускників ВНЗ у контексті компетентісного підходу // Науковий вісник Херсонського державного університету. - 2014.- №7(4).-С.150-154
4. Соглашение рабочей группы CEN. Европейская рамка ИКТ - компетенций 2.0. Часть 1. [Електронний ресурс] // Режим доступа: http://www.ecompetences.eu/site/objects/download/6197_rus_CWA162341Part12010.pdf
5. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. - 2-е изд. - М.: Статистика. - 1980. - 263 с.

Автори статті

Ільїн Олег Олександрович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук та інформаційних технологій, Державний університет телекомунікацій, Київ, Україна. Тел.: +38 067 901 03 03. E-mail: oleg.ilin.ua@gmail.com

Authors of the article

Ilin Oleg Oleksandrovych - candidate of Science (technic), associate professor, associate professor of Department of Computer Science and information technology, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 067 9010303. E-mail: oleg.ilin.ua@gmail.com

Дата надходження в редакцію: 10.02.2016 р.

Рецензент: д.т.н., проф. В.В. Вишнівський

УДК 621.391

Попов А.А., к.т.н.

АЛГОРИТМ РАЗЛИЧЕНИЯ ДЕТЕРМИНИРОВАННЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ, ПОСТРОЕННЫЙ НА ОСНОВЕ ОПЕРАЦИЙ L -ГРУППЫ

Popov A.A. Deterministic orthogonal signals classification algorithm built on the basis of L -group operations.

Deterministic signals classification problem is formulated within signal space with L -group properties. Deterministic signals classification algorithm is considered that is based on the method of linear space mapping into the signal space with L -group properties which is realized by signal phase inverting in frequency domain. Main relationships determining the aforementioned method of mapping are established. We show block diagrams of the devices realizing, on the one hand, method of linear space mapping into the signal space with L -group properties, and on the other hand, deterministic orthogonal signals classification in signal space with L -group properties. Realization of considered method is illustrated with oscillograms of the signals in the output of main elements of processing unit block diagram. It is shown that deterministic orthogonal signals classification unit based on this method, being quasioptimal, provides signal-to-noise ratio gain as against optimal demodulator of signals upon wide class of distributions which describe behaviour of interference (noise) of pulse type.

Keywords: signal classification, deterministic signal, orthogonal signals, L -group, signal estimator, probability of error of signal classification

Попов А.А. Алгоритм розрізнення детермінованих ортогональних сигналів, побудований на основі операцій L -групи.

Формулюється задача розрізнення детермінованих сигналів в просторі з властивостями L -групи. Розглядається алгоритм розрізнення детермінованих сигналів, побудований на методі відображення лінійного простору в простір сигналів з властивостями L -групи, який реалізується шляхом інвертування фази сигналу в частотній області. Показується, що пристрій розрізнення детермінованих ортогональних сигналів, побудоване на даному методі, будучи квазіоптимальний, забезпечує вииграш у відношенні сигнал-шум у порівнянні з оптимальним демодулятором сигналів на широкому класі розподілів, які описують поведінку шумів (перешкод) імпульсного типу.

Ключові слова: розрізнення сигналів, детермінований сигнал, ортогональні сигнали, L -група, оцінка сигналу, ймовірність помилки розрізнення сигналів

Попов А.А. Алгоритм различения детерминированных ортогональных сигналов, построенный на основе операций L -группы.

Формулируется задача различения детерминированных сигналов в пространстве со свойствами L -группы. Рассматривается алгоритм различения детерминированных сигналов, построенный на методе отображения линейного пространства в пространство сигналов со свойствами L -группы, который реализуется путем инвертирования фазы сигнала в частотной области. Показывается, что устройство различения детерминированных ортогональных сигналов, построенное на данном методе, являясь квазиоптимальным, обеспечивает выигрыш в отношении сигнал-шум по сравнению с оптимальным демодулятором сигналов на широком классе распределений, которые описывают поведение шумов (помех) импульсного типа.

Ключевые слова: различение сигналов, детерминированный сигнал, ортогональные сигналы, L -группа, оценка сигнала, вероятность ошибки различения сигналов

Введение

Современная теория обработки сигналов активно исследует вопросы повышения эффективности решения задач обработки сигналов в условиях априорной неопределенности [1-4]. Все это в полной мере относится к задачам различения сигналов [3-6]. Пусть модель взаимодействия сигнала $s_i(t)$ из множества сигналов $S = \{s_i(t)\}$, $i = 1, \dots, m$ и помехи (шума) $n(t)$ в пространстве сигналов со свойствами L -группы $\Gamma(+, \vee, \wedge)$ описывается операцией сложения «+» L -группы [7]:

$$x(t) = s_i(t) + n(t), \quad t \in T_s, \quad (1)$$

где $T_s = [t_0, t_0 + T]$ – область определения сигнала $s_i(t)$; t_0 – время прихода сигнала $s_i(t)$; T – длительность сигнала $s_i(t)$; $m \in \mathbf{N}$, $\mathbf{N}$ – множество натуральных чисел.

Задача различения сигналов на фоне помех состоит в том, чтобы, используя некоторый критерий, вынести решение о том, какой сигнал из множества сигналов $S = \{s_i(t)\}$, $i = 1, \dots, m$ содержит наблюдаемый процесс $x(t)$ [3-6]. Задача различения детерминированных ортогональных сигналов из множества сигналов $S = \{s_i(t)\}$, $i = 1, \dots, m$ в пространствах со свойствами L -группы в рамках аддитивной модели взаимодействия полезных сигналов и помехи (шума) (1) будет рассматриваться, во-первых, с учетом наличия готового решения, полученного в [8; §7.5] для модели взаимодействия $x(t) = s_i(t) \odot n(t)$ [8, (7.5.1)] (где $\odot$ – операция решетки L -группы), а во-вторых, с использованием метода отображения линейного пространства сигналов в пространство сигналов со свойствами L -группы.

Метод отображения линейного пространства сигналов в пространство сигналов со свойствами L -группы [9, 10], реализуемый путем инвертирования фазы сигнала в частотной области, основан на использовании оценки $\overline{n(t) - s_i(t)}$ разности $n^*(t) - s_i(t)$ реализации $n^*(t)$ помехи (шума) $n(t)$ и сигнала $s_i(t)$, которая определяется следующими взаимосвязанными соотношениями:

$$\overline{n(t) - s_i(t)} = \mathbf{F}^{-1}[X''(f)]; \quad (2)$$

$$\overline{s_i(t) + n(t)} = \mathbf{F}^{-1}[X'(f)]; \quad (3)$$

$$X'(f) = \begin{cases} X^*(f), & h(f) = 0; \\ X^*(f)h(f), & h(f) \neq 0, \end{cases} \quad (4a)$$

$$X''(f) = \begin{cases} X^*(f), & h(f) = 0; \\ -X^*(f)h(f), & h(f) \neq 0, \end{cases} \quad (4б)$$

$$X^*(f) = \mathbf{F}(x^*(t)); \quad (4в)$$

$$h(f) = \frac{|S(f)|}{\max(S(f))} \left[\frac{|S(f)|}{\max(S(f))} - S_\varepsilon \right]; \quad (4г)$$

$$S(f) = \mathbf{F}[s(t)] = \sum_{l=1}^L S_{0,l}(f); \quad (4д)$$

$$S_\varepsilon = |S_{0,l}(f_{2,l})| = |S_{0,l}(f_{1,l})|; \quad (4е)$$

$$\int_{f_{1,l}}^{f_{2,l}} (S_{0,l}(f))^2 df / \int_{-\infty}^{\infty} (S_{0,l}(f))^2 df = 1 - \varepsilon, \quad (4ж)$$

где $x^*(t)$ – реализация суммы (1) полезного сигнала $s_i(t)$ и помехи (шума) $n(t)$: $x^*(t) = s_i(t) + n^*(t)$; $X^*(f)$, $S(f)$ – отображения $\mathbf{F}$ реализаций суммы $x^*(t)$ (1) и полезного сигнала $s_i(t)$ в частотной области, выполняемые на основе известных преобразований (например, преобразования Фурье, косинус преобразования, преобразования Хартли и т.д.); $S_{0,l}(f)$ – парциальный спектр l -го дискрета фазоманипулированного сигнала; $\mathbf{F}$ – отображение сигнала из временной области в частотную; $\mathbf{F}^{-1}$ – отображение, обратное $\mathbf{F}$: $\mathbf{F} \cdot \mathbf{F}^{-1} = \mathbf{F}^{-1} \cdot \mathbf{F} = 1$; $X'(f)$ – модифицированное отображение $X^*(f)$ реализации суммы $x^*(t)$ (1) в частотной области; $X''(f)$ – отображение оценки $\overline{n(t) - s_i(t)}$ разности $n^*(t) - s_i(t)$ реализации $n^*(t)$ помехи (шума) $n(t)$ и сигнала $s_i(t)$ в частотной области; $h(f)$ – функция окна в частотной области, на котором осуществляется инвертирование фазы

сигнала; $l(*)$ – единичная ступенчатая функция Хевисайда; S_ε – некоторый пороговый уровень, устанавливающий ширину функции окна $h(f)$ в частотной области, определяемый верхней $f_{2,l}$ и нижней $f_{1,l}$ граничной частотой l -го дискрета фазоманипулированного сигнала в соответствии с соотношениями (4е,ж); ε – сколь угодно малое положительное число, которое устанавливает процентное соотношение энергии l -го дискрета полезного сигнала, которое сосредоточено в полосе $[f_{1,l}, f_{2,l}]$.

Целью статьи является анализ эффективности алгоритма различения детерминированных сигналов, построенном на методе отображения линейного пространства в пространство сигналов со свойствами L -группы, который реализуется путем инвертирования фазы сигнала в частотной области, в условиях негауссовости широкого класса распределений помех (шумов).

Изложение основного материала исследования

Основные идеи соотношений (2), (3), (4а)...(4ж) поясняются на рис. 1а,б,в. На рис. 1а показан фрагмент спектра $S(f)$ фазоманипулированного сигнала $s_i(t)$, состоящий из парциальных спектров $S_{0,l}(f)$ дискретов сигнала. Здесь и далее в качестве отображения $\mathcal{F}$ сигнала из временной области в частотную используется короткое дискретное косинус преобразование [11], которое осуществляется на интервале длительности дискрета полезного сигнала $s_i(t)$. На рис. 1б показан фрагмент функции окна в частотной области $h(f)$ (4г), на котором осуществляется инвертирование фазы сигнала. Функция $h(f)$, определяемая соотношением (4г), состоит из отдельных окон, каждое с областью определения на интервале частот $[f_{1,l}, f_{2,l}]$, выбираемый в соответствии с уравнениями (4е), (4ж), таким образом, что каждому l -му дискрету полезного сигнала соответствует свое отдельное окно. На рис. 1в показаны модифицированное отображение $X'(f)$ (4а) реализации суммы $x^*(t)$ (1) в частотной области и отображение $X''(f)$ (4б) оценки $\overline{n(t) - s_i(t)}$ разности $n^*(t) - s_i(t)$ реализации $n^*(t)$ помехи (шума) $n(t)$ и сигнала $s_i(t)$ в частотной области. Показанные реализации $X'(f)$, $X''(f)$ соответствуют случаю аддитивного взаимодействия полезного сигнала $s_i(t)$ с нормальным шумом $n(t)$ при отношении сигнал-шум, равном 1000.

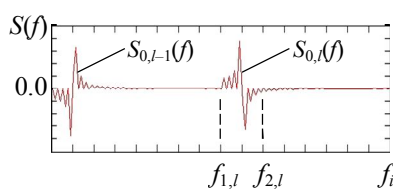


Рис. 1а

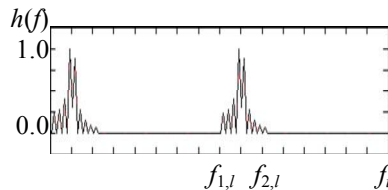


Рис. 1б

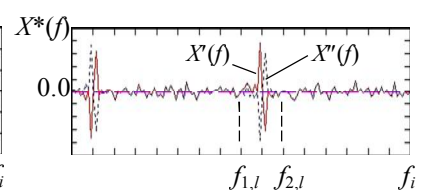


Рис. 1в

Здесь следует заметить, что для детерминированных фазоманипулированных ортогональных сигналов из множества $S = \{s_i(t)\}$, $i = 1, \dots, m$, функция окна $h(f)$, определяемая соотношением (2в), является одинаковой.

Имея оценку $\overline{n(t) - s_i(t)}$ (2), пространство сигналов со свойствами L -группы $\mathcal{L}(+, \vee, \wedge)$ может быть реализовано путем преобразования сигналов линейного пространства таким образом, что оценки $\hat{x}_\vee(t)$, $\hat{x}_\wedge(t)$ результатов взаимодействия $x_\vee(t)$, $x_\wedge(t)$ сигнала $s_i(t)$ и помехи $n(t)$ в пространстве сигналов со свойствами L -группы $\mathcal{L}(+, \vee, \wedge)$ с операциями верхней и нижней граней формируются в соответствии с соотношениями, аналогичными [7; §XIII.3;(14)], [7; §XIII.4;(22)]:

$$\hat{x}_\vee(t) = \{\overline{[s_i(t) + n(t)]} + |\overline{n(t) - s_i(t)}|\} / 2; \quad (5a) \quad \hat{x}_\wedge(t) = \{\overline{[s_i(t) + n(t)]} - |\overline{n(t) - s_i(t)}|\} / 2. \quad (5b)$$

Демодулятор детерминированных ортогональных сигналов, реализующий метод отображения линейного пространства сигналов в пространство сигналов со свойствами L -группы путем инвертирования фазы сигнала в частотной области содержит устройство отображения пространства сигналов и, собственно, устройство различения сигналов (см. рис. 2).

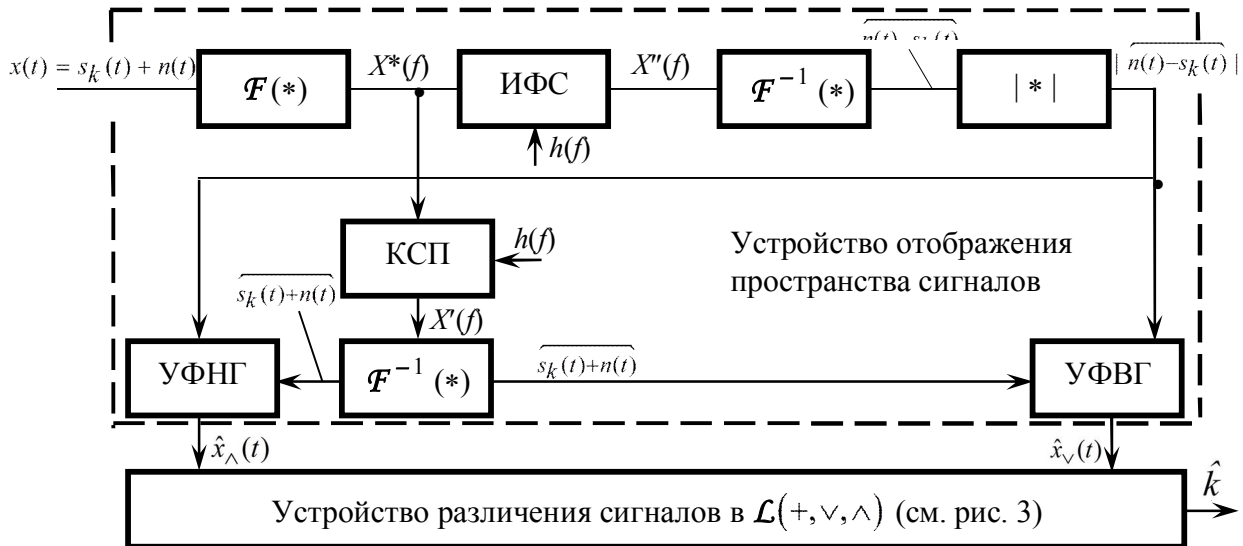


Рис. 2.

Устройство отображения пространства сигналов содержит: устройство отображения реализации $x^*(t)$ суммы (1) принимаемого полезного сигнала $s_k(t)$ и помехи (шума) $n(t)$ в частотную область $X^*(f)$ – блок $\mathbf{F}^*$; инвертор фазы сигнала (ИФС), осуществляющий поворот фазы спектра $X^*(f)$ на π на функции окна $h(f)$ (4г) в частотной области и обеспечивающий получение отображения $X''(f)$ (4б) оценки $\overline{n(t) - s_k(t)}$ разности $n^*(t) - s_k(t)$ реализации $n^*(t)$ помехи (шума) $n(t)$ и сигнала $s_k(t)$ в частотной области; устройство формирования оценки $\overline{n(t) - s_k(t)}$ разности $n^*(t) - s_k(t)$ реализаций $n^*(t)$ помехи (шума) $n(t)$ и сигнала $s_k(t)$ путем отображения спектра $X''(f)$ во временную область – блок $\mathbf{F}^{-1}$; устройство вычисления модуля – блок $|*|$; корректор спектральной плотности мощности помехи (шума) (КСПП), который формирует модифицированное отображение $X'(f)$ (4а) реализации $x^*(t)$ суммы (1) в частотной области; устройство формирования скорректированной суммы $\overline{s_k(t) + n(t)}$ – блок $\mathbf{F}^{-1}$; устройство формирования оценки $\hat{x}_\wedge(t)$ (5б) нижней грани (УФНГ) $x_\wedge(t) = s_k(t) \wedge n(t)$; устройство формирования оценки $\hat{x}_\vee(t)$ (5а) верхней грани (УФВГ) $x_\vee(t) = s_k(t) \vee n(t)$.

Вся последующая обработка осуществляется устройством различения детерминированных ортогональных сигналов, структурная схема которого показана на рис. 3 в соответствии с общим алгоритмом [8,(7.5.6)] и его отдельными этапами, которые определяются следующими соотношениями (в предположении приема сигнала $s_k(t)$):

$$\arg \max_{i \in I; s_i(t) \in S} |z_i(t)|_{x(t)=s_k(t)+n(t)} = \hat{k}; \quad (6)$$

$$z_i(t) = \int_{t \in T_s} y_i(t) s_i(t) dt; \quad (7)$$

$$y_i(t) = y_{i,+}(t) + y_{i,-}(t); \quad (8)$$

$$y_{i,+}(t) = y_{i,\wedge}(t) \vee 0; \quad (8a) \quad y_{i,-}(t) = y_{i,\vee}(t) \wedge 0; \quad (8б)$$

$$y_{i,\wedge}(t) = \hat{x}_{\vee}(t) \wedge s_i(t); \quad (9a) \quad y_{i,\vee}(t) = \hat{x}_{\wedge}(t) \vee s_i(t). \quad (9б)$$

Смысл соотношения (6) состоит в принятии решения о приеме сигнала $s_k(t)$ из множества сигналов $S = \{s_i(t)\}$, $i = 1, \dots, m$ на основе выбора того номера канала $\hat{k}$, который соответствует максимальному значению корреляционного интеграла $z_i(t)$ (7). При этом оценка $y_i(t)$ (8) принимаемого сигнала $s_k(t)$ в i -ом канале обработки формируется как сумма положительной $y_{i,+}(t)$ (8a) и отрицательной $y_{i,-}(t)$ (8б) частей оценок $y_{i,\wedge}(t)$ (9a), $y_{i,\vee}(t)$ (9б) принимаемого сигнала $s_k(t)$ соответственно. Оценки $y_{i,\wedge}(t)$ (9a), $y_{i,\vee}(t)$ (9б) формируются в соответствии с правилом [8,(7.5.4)].

Структурная схема устройства различения детерминированных сигналов в пространстве сигналов со свойствами L -группы включает решающее устройство (РУ) и m параллельных каналов обработки, каждый из которых содержит устройство формирования оценки $y_i(t)$ сигнала $s_i(t)$, устройство вычисления корреляционного интеграла $z_i(t)$ и устройство стробирования (УС) (см. рис. 3).

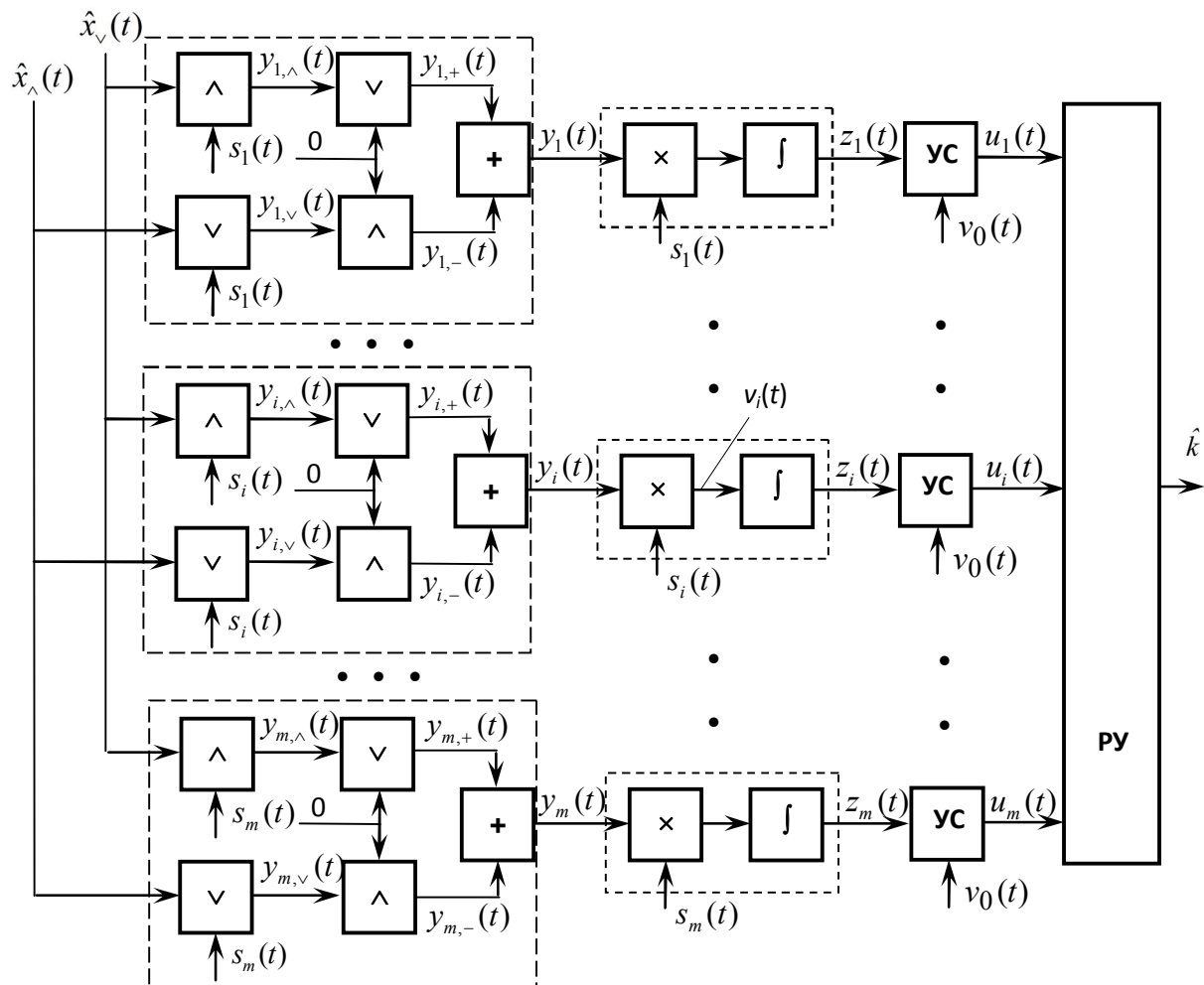


Рис. 3.

Устройство формирования оценки $y_i(t)$ сигнала $s_i(t)$ содержит канал формирования положительной $y_{i,+}(t)$ (8а) части оценки $y_{i,\wedge}(t)$ (9а) принимаемого сигнала $s_i(t)$ и канал формирования отрицательной $y_{i,-}(t)$ (8б) части оценки $y_{i,\vee}(t)$ (9б) принимаемого сигнала $s_i(t)$, объединенных сумматором. Канал формирования положительной части оценки содержит последовательно соединенные блоки вычисления нижней и верхней граней соответственно. Канал формирования отрицательной части оценки содержит последовательно соединенные блоки вычисления верхней и нижней граней соответственно.

Устройство вычисления корреляционного интеграла состоит из перемножителя и интегратора.

Рассмотрим особенности работы устройства различения детерминированных ортогональных фазоманипулированных сигналов при реализации метода отображения линейного пространства сигналов в пространство сигналов со свойствами L -группы путем инвертирования фазы сигнала в частотной области, который основывается на уравнениях (2), (3), (4а)...(4ж), (5а,б). Особенности функционирования устройства различения сигналов, показанного на рис.2.3.3, будут приведены на примере результатов статистического моделирования процесса различения детерминированных ортогональных фазоманипулированных сигналов в соответствии с алгоритмом, который определяется соотношениями (6), (7), (8), (8а,б), (9а,б).

Все приведенные ниже рисунки соответствуют следующим условиям моделирования: принимаемые полезные сигналы из множества сигналов $S = \{s_i(t)\}$, $i = 1, \dots, m$ – детерминированные ортогональные фазоманипулированные с одинаковой энергией длительностью T , $T=512$ отсчетов, каждый сигнал содержит восемь дискретов; помеха $n(t)$ – гауссовский шум с независимыми отсчетами; отношение сигнал-помеха E/N_0 составляло величину $E/N_0=2$, где E – энергия сигнала $s_i(t)$, N_0 – спектральная плотность мощности помехи.

На рис. 4а, 4б показаны реализации $\hat{x}_{\vee}^*(t)$, $\hat{x}_{\wedge}^*(t)$ оценок $\hat{x}_{\vee}(t)$, $\hat{x}_{\wedge}(t)$ верхней $x_{\vee}(t) = s_k(t) \vee n(t)$ и нижней $x_{\wedge}(t) = s_k(t) \wedge n(t)$ граней сигнала $s_k(t)$ и помехи $n(t)$, сформированные в соответствии с соотношениями (5а,б) на основе оценки $\overline{n(t) - s_k(t)}$ разности $n^*(t) - s_k(t)$ реализации $n^*(t)$ помехи (шума) $n(t)$ и сигнала $s_k(t)$. Напомним, что оценки $\hat{x}_{\vee}(t)$, $\hat{x}_{\wedge}(t)$ результатов взаимодействий $x_{\vee}(t), x_{\wedge}(t)$ сигнала $s_k(t)$ и помехи $n(t)$ в пространстве сигналов со свойствами L -группы $\mathcal{L}(+, \vee, \wedge)$ с операциями верхней и нижней граней $\vee, \wedge$ являются входными сигналами для устройства различения сигналов, показанного на рис. 3.

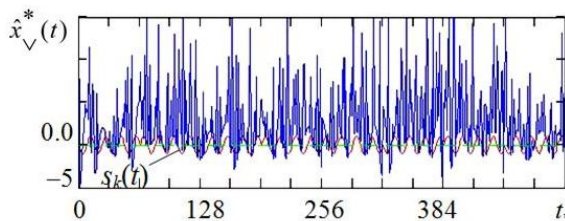


Рис. 4а

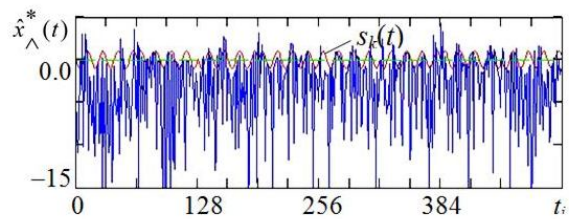


Рис. 4б

На рис. 5а, 5б показаны реализации $y_{k,\wedge}^*(t)$, $y_{k,\vee}^*(t)$ (сплошной линией) процессов $y_{k,\wedge}(t)$, $y_{k,\vee}(t)$ на выходе блоков вычисления нижней и верхней граней соответственно

устройства формирования оценки $y_k(t)$ сигнала $s_k(t)$ в k -ом канале обработки при условии, что осуществляется прием сигнала $s_k(t)$. Принимаемый сигнал $s_k(t)$ показан пунктиром.

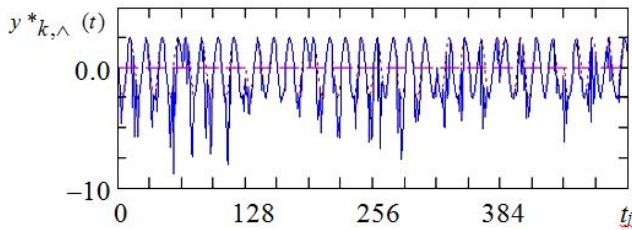


Рис. 5а

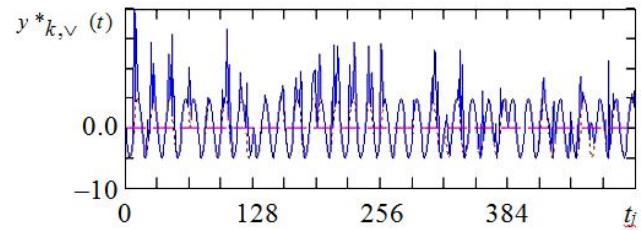


Рис. 5б

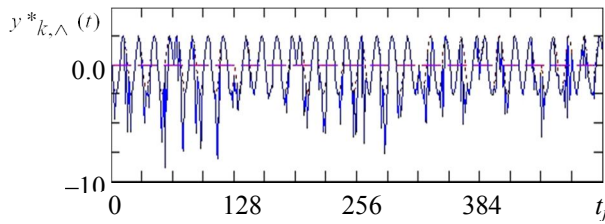


Рис. 5а

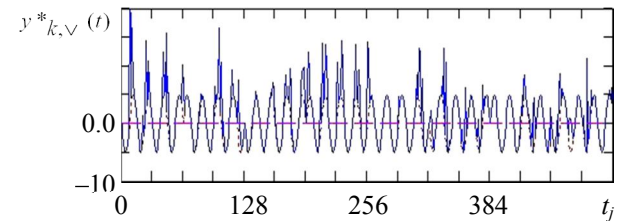


Рис. 5б

На рис. 6а, 6б показаны реализации $y_{i,∧}^*(t)$, $y_{i,∨}^*(t)$ (сплошной линией) процессов $y_{i,∧}(t)$, $y_{i,∨}(t)$ на выходе блоков вычисления нижней и верхней граней соответственно устройства формирования оценки $y_i(t)$ сигнала $s_i(t)$ в i -ом канале обработки при условии, что осуществляется прием сигнала $s_k(t)$. Принимаемый сигнал $s_k(t)$ показан пунктиром.

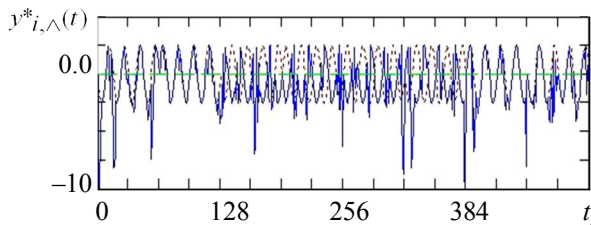


Рис. 6а

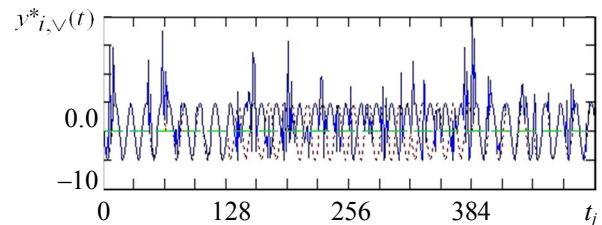


Рис. 6б

Заметим одну важную особенность, видную на рис.6а,б. Опорные сигналы $s_k(t)$ и $s_i(t)$ k -ого и i -ого каналов соответственно, являющиеся ортогональными, характеризуются синфазными первыми двумя дискретами (интервал $[0, 128]$), противоположными по фазе 3-м, 4-м, 5-м, 6-м дискретами (интервал $[128, 384]$), а также синфазными последними двумя дискретами (интервал $[384, 512]$). При условии синфазности дискрет опорного сигнала в канале обработки с дискретами принимаемого сигнала $s_k(t)$ (в данном случае на интервалах $[0, 128]$ и $[384, 512]$) предварительные оценки сигнала $y_{i,∧}(t)$, $y_{i,∨}(t)$ весьма коррелированы с принимаемым сигналом $s_k(t)$. В случае нахождения дискрет опорного сигнала в канале обработки с дискретами принимаемого сигнала $s_k(t)$ в противофазе (в данном случае на интервале $[128, 384]$), предварительные оценки сигнала $y_{i,∧}(t)$, $y_{i,∨}(t)$ слабо коррелированы с принимаемым сигналом $s_k(t)$. Напомним, что сигналы, показанные на рис.5а,б; 6а,б соответствуют условию, когда отношение сигнал-шум (сигнал-помеха) составляет 2 (по мощности). Как видно из рисунков, отрицательные части процессов $y_{k,∧}(t)$, $y_{i,∧}(t)$ и

положительные части процессов $y_{k,\vee}(t)$, $y_{i,\vee}(t)$ характеризуется наличием помеховых выбросов, которые впоследствии будут удалены на следующем этапе обработки.

На рис. 7а, б показаны реализации $y_k^*(t)$, $y_i^*(t)$ процессов $y_k(t)$, $y_i(t)$ на выходе сумматора в k -ом и i -ом каналах обработки соответственно (см. рис. 3) при условии, что осуществляется прием сигнала $s_k(t)$. Опорные сигналы $s_k(t)$, $s_i(t)$ в k -ом и i -ом каналах

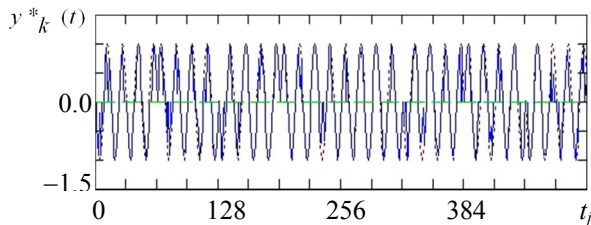


Рис. 7а

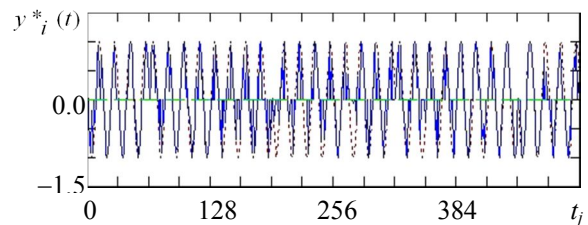


Рис. 7б

обработки соответственно показаны пунктиром.

Подчеркнем важную особенность, имеющую место на рис. 7а,б. В целом, оценка $y_k(t)$ в k -ом канале обработки достаточно хорошо согласуется с принимаемым сигналом $s_k(t)$ (рис. 7а). При условии синфазности дискрет опорного сигнала $s_i(t)$ в i -ом канале обработки с дискретами принимаемого сигнала $s_k(t)$ (в данном случае на интервалах $[0,128]$ и $[384,512]$) оценка сигнала $y_i(t)$ в i -ом канале обработки весьма коррелирована с принимаемым сигналом $s_k(t)$ и опорным сигналом $s_i(t)$ данного канала. В случае нахождения дискрет опорного сигнала $s_i(t)$ в i -ом канале обработки в противофазе с дискретами принимаемого сигнала $s_k(t)$ (в данном случае на интервале $[128,384]$), оценка сигнала $y_i(t)$ в i -ом канале обработки также является коррелированной с опорным сигналом $s_i(t)$ канала, однако менее коррелирована, чем в случае синфазности дискрет, что создает основу для различения сигналов $y_k(t)$ и $y_i(t)$ по энергетическому параметру, что собственно, и предусмотрено последующим этапом обработки.

На рис. 8а показаны графики зависимости полной вероятности ошибки различения ортогональных сигналов $P_e(q_b^2)$ от приведенного отношения сигнал-шум $q_b^2 = E_b / N_0$, $E_b = E / \log_2 m$, $q^2 = q_b^2 \log_2 m$, рассчитанные по известному соотношению (см., например

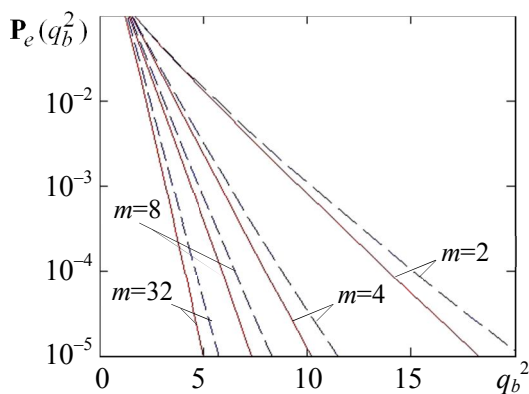


Рис. 8а

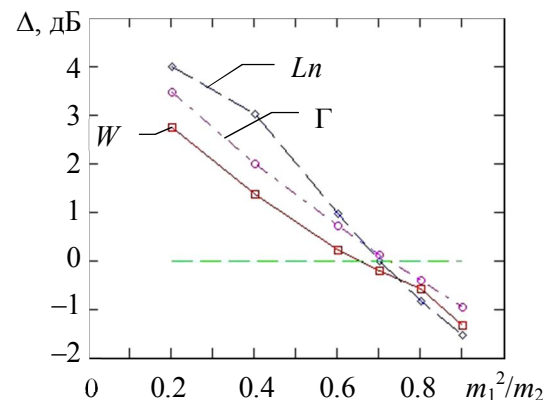


Рис. 8б

[5,(2.4.43)] (сплошной линией) для оптимального демодулятора, показанного, например, на рис. 2.206 [5], а также рассчитанной по соотношению, полученному для демодулятора,

схема которого приведена на рис. 2 (штриховой линией), для сигналов из множества $S = \{s_i(t)\}$, $i = 1, \dots, m$, $m = 2, 4, 8, 32$. Также, как и в предыдущем случае, помехоустойчивость демодулятора, который решает задачу различения ортогональных сигналов в пространстве сигналов со свойствами L -группы, характеризуется небольшим проигрышем (не более 1 дБ при $m \geq 8$, $P_e(q_b^2) = 10^{-5}$) в необходимом отношении сигнал-шум по сравнению с теоретически возможным результатом.

Напомним, что зависимости, приведенные на рис. 8а, получены в предположении нормальности распределения помехи (шума).

На рис. 8б показаны результаты статистического моделирования зависимости величины выигрыша (проигрыша) $\Delta = 10 \lg(q_{LS}^2 / q_L^2)$, получаемого при различении ортогональных сигналов $m = 2$ демодулятором, который осуществляет обработку в пространстве сигналов со свойствами L -группы (см. рис. 2) относительно оптимального различителя детерминированных сигналов, осуществляющего обработку в линейном пространстве сигналов, схема которого показана на рис. 2.20б [5], от соотношения m_1^2 / m_2 квадрата математического ожидания m_1 ко второму моменту m_2 огибающих помехи (шума) $n(t)$ с распределениями на трех классах, где q_{LS}^2, q_L^2 – величины отношения сигнал-шум для оптимального различителя детерминированных сигналов и демодулятора, показанного на рис. 2, соответственно, при которых обеспечивается полная вероятность ошибки $P_e(q^2) = 10^{-3}$. Огибающие помехи (шума) $n(t)$ на каждом из указанных трех классов распределения характеризуются соотношениями: $m_1^2 / m_2 = 0.2; 0.4; 0.6; 0.7; 0.8; 0.9$. Распределения помехи (шума) $n(t)$ на трех классах обозначены следующим образом: Вейбулла (W) — сплошная кривая, помеченная квадратами $\square-\square-\square$; логнормальное (Ln) — штриховая линия, обозначенная ромбами $\diamond-\diamond-\diamond$; Гамма (Γ) — штрих-пунктирная линия, помеченная кружочками $\circ-\circ-\circ$.

Как следует из результатов статистического моделирования, показанных на рис. 8б, при огибающей помехи (шума) $n(t)$ с соотношением $m_1^2 / m_2 = 0.9$, демодулятор пространства сигналов со свойствами L -группы проигрывает оптимальному различителю около 1.0...1.6 дБ на трех видах распределения. При огибающих помехи (шума) $n(t)$ с соотношением $m_1^2 / m_2 = 0.8$ демодулятор пространства сигналов со свойствами L -группы проигрывает оптимальному различителю около 0.3...0.9 дБ. При огибающей помехи (шума) $n(t)$ с соотношением $m_1^2 / m_2 = 0.7$ на всех трех видах распределения величина выигрыша (проигрыша) при обработке не превышает 0.2 дБ. При огибающей помехи (шума) $n(t)$ с соотношением $m_1^2 / m_2 = 0.6$ демодулятор пространства сигналов со свойствами L -группы обеспечивает выигрыш при обработке до 1.0 дБ. Та же картина, но с еще большим выигрышем, наблюдается при огибающей помехи (шума) $n(t)$ с соотношениями $m_1^2 / m_2 = 0.4; 0.2$: здесь демодулятор пространства сигналов со свойствами L -группы обеспечивает выигрыш 1.3...3.0 дБ и 2.8...4.0 дБ соответственно.

Выводы

1) Исследуемый различитель ортогональных сигналов, построенный на алгоритме обработки (6), (7), (8), (8а,б), (9а,б), незначительно уступает оптимальному демодулятору в качестве различения при обработке сигналов на фоне гауссовских помех (шумов).

2) Различитель сигналов, построенный на алгоритме обработки (6), (7), (8), (8а,б), (9а,б), обеспечивает выигрыш в отношении сигнал-шум по сравнению с оптимальным демодулятором сигналов на широком классе распределений, которые описывают поведение

шумов (помех) импульсного типа, для которых характерно соотношение m_1^2/m_2 первых двух моментов огибающей помехи (шума) на интервале $0 < m_1^2/m_2 < 0.7$, причем получаемый выигрыш может быть тем значительнее, чем меньше m_1^2/m_2 . 3) Предложенные алгоритмы целесообразно реализовывать в форме цифровой обработки сигналов.

Список использованной литературы

1. Репин В.Г. Статистический синтез при априорной неопределенности и адаптации информационных систем / В.Г. Репин, Г.П. Тартаковский – М.: Сов. радио, 1977. – 432 с.
2. Kassam S.A., Poor H.V. Robust techniques for signal processing: A Survey / S.A. Kassam, H.V. Poor // Proceedings of IEEE. – 1985. – Vol. 73, №3. – pp. 433–481.
3. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Радио и связь, 1989. – 656 с.
4. Богданович В.А. Теория устойчивого обнаружения, различения и оценивания сигналов / В.А. Богданович, А.Н. Вострецов. – М.: Физматлит, 2004. – 320 с.
5. Тихонов В.И. Оптимальный прием сигналов / В.И. Тихонов. – М.: Радио и связь, 1983. – 320 с.
6. Трифонов А.П. Совместное различение сигналов и оценивание их параметров на фоне помех / А.П. Трифонов, Ю.С. Шинаков. – М.: Радио и связь, 1986. – 264 с.
7. Биркгоф Г. Теория решеток / Г. Биркгоф. – М.: Наука, 1984. – 568 с.
8. Попов А.А. Основы обработки сигналов в метрических пространствах со свойствами решетки. Часть 1. Математические основы теории информации в приложении к обработке сигналов / А.А. Попов. – К.: ЦНИИ ВВТ, 2013. – 416 с.
9. Патент 95158 Україна, Н 04 В 15/00. Пристрій перетворення простору сигналів / Попов А.О. Заявник і патентовласник Попов А.О.; заявл. 04.07.2014; опубл. 10.12.2014 // Бюл. № 23.
10. Патент 98995 Україна, Н 04 В 15/00. Спосіб перетворення простору сигналів / Попов А.О. Заявник і патентовласник Попов А.О.; заявл. 17.12.2014; опубл. 12.05.2015 // Бюл. № 9.
11. Rao K.R., Yip P. Discrete Cosine Transform: Algorithms, Advantages, Applications / K.R. Rao, P. Yip. Boston, MA: Academic Press, 1990. – 428 p.

Автори статті

Попов Андрій Олексійович - кандидат технічних наук, доцент, провідний науковий співробітник, Центральний науково-дослідний інститут озброєння та військової техніки, Київ, Україна. Тел. +38 066 299 29 80. E-mail: andoff@rambler.ru

Authors of the article

Popov Andriy Oleksiyovych - candidate of science (technic), assistant professor, leading research scientist, Central Research Institute of Armament and Defence Technologies, Kyiv, Ukraine. Tel. +38 066 299 29 80. E-mail: andoff@rambler.ru

Дата надходження в редакцію: 04.02.2017 р.

Рецензент: д.т.н., доцент В.Ф. Заїка

УДК 621.391.82

Шефер О.В., к.т.н.

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ РАДІОТЕХНІЧНИХ СИСТЕМ ШЛЯХОМ АДАПТИВНОГО ПЕРЕНАЛАГОДЖЕННЯ ТА ІНВЕРСНОГО КОРЕЛЯЦІЙНОГО ПІДХОДУ ДО ВИЯВЛЕННЯ КОРИСНОГО СИГНАЛУ

Shefer O.V. The increase of radio technical noise immunity systems by adaptive premalignant and inversive correlation approach to the detection of the beneficial signal.

In article the ways of radio engineering noise stability systems increase which have an expanded scope are offered, in comparison with the known methods.

The main purpose is the increase of noise immunity and the reduction in degree of electromagnetic waves radio distortion. To achieve this purpose it is possible reduce the electromagnetic compatibility distortion degree in the telemetry range, in case of external interference signals impact. Using of the offered adaptive synchronous change-over approach in combination with determination of the useful signal hidden by noise parameters differs in the increased profitability.

The relative noise stability of radio engineering functioning control systems of SC is as a result provided. Essential increase in the relation of signal / noise can be reached by decrease in level of a hindrance and increase in size of transfer coefficient. The used vernier inverse - correlation method showed the acceptable results for identification of a noisy beneficial signal.

Keywords: noise immunity, radio technical system, adaptive tuning, inversive correlation, beneficial signal.

Шефер О.В. Підвищення завадостійкості радіотехнічних систем шляхом адаптивного переналагодження та інверсного кореляційного підходу до виявлення корисного сигналу.

У статті запропоновано шляхи підвищення завадостійкості радіотехнічних систем, котрі мають розширену область застосування. Використання розробленого підходу адаптивного синхронного переналагодження у поєднанні із визначенням параметрів прихованого шумами корисного сигналу, відрізняється підвищеною економічністю.

Забезпечується відносна завадостійкість функціонування радіотехнічних систем управління КА. Використаний ноніусний інверсно-кореляційний метод показав прийнятні результати для виявлення зашумленого корисного сигналу.

Ключові слова: завадостійкість, радіотехнічна система, адаптивне переналагодження, інверсна кореляція, корисний сигнал

Шефер А.В. Повышение помехоустойчивости радиотехнических систем путем адаптивной перенастройки и инверсного корреляционного подхода к выявлению полезных сигналов.

В статье предложены пути повышения помехоустойчивости радиотехнических систем, которые имеют расширенную область применения. Использование разработанного подхода адаптивной синхронной перенастройки в сочетании с определением параметров скрытого шумами полезного сигнала, отличается повышенной экономичностью.

В результате обеспечивается относительная помехоустойчивость функционирования радиотехнических систем управления КА. Использованный нониусный инверсно-корреляционный метод показал приемлемые результаты для выявления зашумленного полезного сигнала.

Ключевые слова: помехоустойчивость, радиотехническая система, адаптивная перенастройка, инверсная корреляция, полезный сигнал.

Вступ

Велика кількість керованих об'єктів потребує саме якісного зв'язку. Проблеми зі зв'язком виникають внаслідок природної, або штучно створеної зашумленості корисного сигналу, в наслідок електромагнітної несумісності радіотехнічних системи (РТС). Це можуть бути багатокоштовні і небезпечні, у випадку руйнування, космічні апарати та об'єкти військово-промислового комплексу.

Постановка задачі. Залишається актуальною задача розробки універсальних методів виявлення і ідентифікації параметрів корисних сигналів за шумовими сигналам. Розв'язання цієї проблеми дозволить запобігти аварій, із відповідними негативними наслідками. Щоб забезпечити своєчасність виявлення та ідентифікації, необхідно мати метод, котрий дозволить виявити корисний сигнал із їх суміші з випадковим процесом за умови значних співвідношень шум – періодичний сигнал.

Аналіз літературних джерел. Основним напрямом підвищення завадостійкості приймально-передавального тракту космічного апарату (КА) є підтримка відношення сигнал / шум не нижче встановленого значення [1]. Існуючі методи розв'язання даного завдання засновані на виборі необхідної потужності (РТС), або пов'язані із використанням схем автоматичного регулювання чутливості (підсилення) радіосигналу, або побудовані на базі логарифмічних підсилювачів [2, 3].

Використання методів першого типу погіршує умови електромагнітної сумісності РТС, застосування ж методів другого і третього типів призводить до зниження дальності дії телеметрії, у випадку впливу зовнішніх сигналів завад, як зазначено у [4].

Мета та задачі дослідження. Метою роботи є підвищення завадостійкості та зменшення ступеня спотворення електромагнітних коливань радіодіапазону РТС.

Для досягнення мети необхідно максимально усунути зазначені недоліки існуючих методів підвищення завадостійкості. Пропонується використовувати адаптивне синхронне переналагодження потужності випромінювання РТС та динамічного діапазону, з урахуванням енергетичних параметрів вхідних впливів, а також використання кореляційного підходу до виявлення корисного сигналу із суміші шум - сигнал.

Адаптивне синхронне переналагодження параметрів випромінювання РТС. Представимо вихідні електромагнітні коливання радіодіапазону РТС $y(t)$, згідно із [4, 5] у вигляді:

$$y(t) = y_l(t) + y_{nl}(t) + n(t), \quad (1)$$

де $y_l(t)$, $y_{nl}(t)$ – відповідно лінійна і нелінійна складові вихідного сигналу;
 $n(t)$ – внутрішні шуми РТС.

Тоді відношення сигнал/шум на вході РТС із урахуванням компонент нелінійних спотворень радіосигналу, згідно із [5] може бути описано виразом:

$$\sigma = \frac{x(t)}{n_0(t) + \mu(t)} \cdot \gamma, \quad (2)$$

де $x(t)$, $\mu(t)$ – рівень корисного сигналу і сигналу завад на вході РТС, відповідно;

$n_0(t)$ – рівень зашумленості РТС; γ – коефіцієнт погіршення відношення сигнал/шум внаслідок нелінійності характеристик тракту приймання - передачі. Цей коефіцієнт лежить у межах $0 \leq \gamma \leq 1$, причому для лінійного режиму РТС $\gamma = 1$.

Суттєве підвищення відношення сигнал/шум, у відповідності із (2), може бути досягнуто шляхом зниження рівня перешкоди $\mu(t)$ і підвищення величини коефіцієнта γ (до одиниці). Це відбувається за рахунок штучного введення режиму роботи РТС у лінійну область, за допомогою зменшення коефіцієнта передачі та одночасним підвищенням рівня корисного сигналу $x(t)$, за рахунок відповідного збільшення потужності випромінювання РТС [6], рис. 1.

Даний метод можна реалізувати шляхом забезпечена формуванням на виході РТС спеціального сигналу θ , котрий співпадає з нелінійною складовою вихідного сигналу $y_{nl}(t)$, згідно з (1).

Виділений сигнал θ слугує керуючим впливом для переналагодження коефіцієнта передачі та потужності випромінювання РТС. Шляхом адаптивного узгодження рівня

корисного сигналу на вході РТС, за допомогою зміни коефіцієнта підсилення каскадів приймача, можна розширити його лінійний динамічний діапазон і усунути його перевантаження сигналами завад значного рівня, під час протікання перехідних процесів T_s .

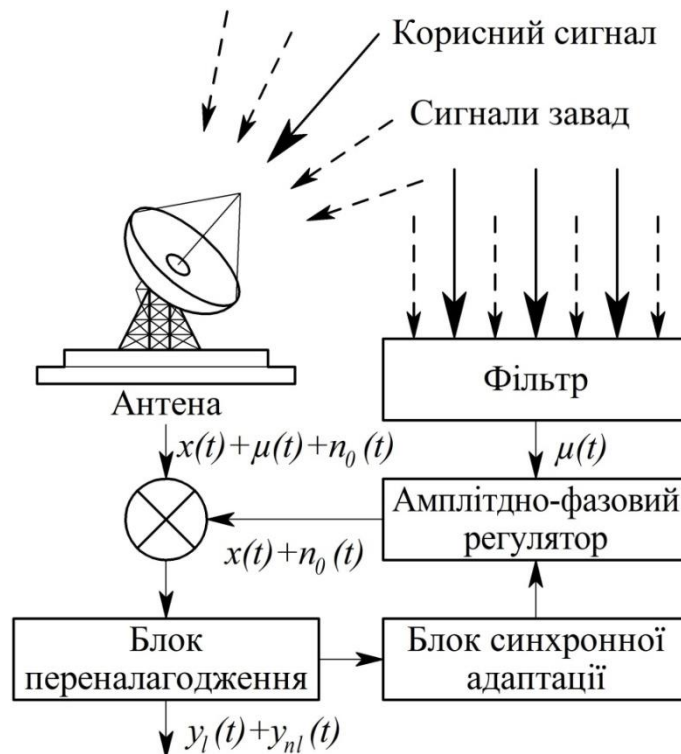


Рис. 1. Адаптивне переналагодження із фільтрацією корисного сигналу

Використання кореляційного підходу до виявлення корисного сигналу із суміші шум – сигнал. Виділити корисний сигнал можна використавши кореляційний алгоритм, оскільки він має більш високі експлуатаційні характеристики та точність, у порівнянні з іншими типами фільтрів [7, 9, 10].

Суміш періодичного сигналу і випадкової перешкоди розкладається в ряд Фур'є:

$$\left. \begin{aligned} b_i &= \frac{2}{n} \sum_{t=1}^k y(t) \cdot \sin i\omega_0 h t \\ c_i &= \frac{2}{n} \sum_{t=1}^k y(t) \cdot \cos i\omega_0 h t \end{aligned} \right\} \quad (3)$$

де h – крок у часі, $i = \overline{1, m}$; ω_0 – базова частота, береться менше інтервалу корелювання періодограми $\left(\omega_0 \approx \frac{1}{4} \frac{2\pi}{nh} \right)$. Обчислюється амплітуда A_i i -х гармонік ряду $A_i = (b_i^2 + c_i^2)^{\frac{1}{2}}$.

Якщо деяке A_j із A_i ($i = \overline{1, m}$) більше заданого порогового значення A_n , то вважається, що в $y(t)$ існує на частоті $j\omega_0$ періодичність. Поріг, як функція частоти ω задається таким чином, щоб за відсутності періодичності виконувалась умова

$$P(A_j > A_n(j\omega_0)) = P_{\text{пп}}, \quad (4)$$

де $P_{\text{пп}}$ – ймовірність помилкового прийняття рішення про наявність періодичності.

Тоді ефективність частотного порогового методу буде визначатися ймовірністю виявлення P_b корисного сигналу амплітуди A_c за умови заданої ймовірності $P_{\text{пп}}$ помилкового

рішення. Визначимо ймовірність P_b виявлення корисного сигналу. За відсутності періодичності, коефіцієнти b_i і c_i в (3) є випадковими некорельованими величинами з нульовим математичним очікуванням і дисперсією σ_{ab}^2 . Двовірна щільність розподілення a і b має вигляд:

$$f(a, b) = \exp\left(-\frac{a^2 + b^2}{2\sigma_{ab}^2}\right), \quad (5)$$

тобто вона являє собою ймовірність виходу вектора (a, b) за межі кола з радіусом A_n із центром на початку координат. Тоді

$$P_{nm} = \exp\left(-\frac{A_n^2}{2\sigma_{ab}^2}\right), \quad (6)$$

тобто одиниця мінус ймовірність попадання в еліпс розсіювання. З (6) знаходимо значення порогу A_n :

$$A_n = \sigma_{ab} \sqrt{-2 \ln P_{nm}}. \quad (7)$$

На площині (a, b) визначимо підобласті виявлення і невиявлення корисного сигналу з амплітудою A_c і нульовою фазою.

Для кожної частоти $i\omega_0$ амплітуди сигналу $y(t)$ і шуму $\mu(t)$ векторно складаються: $\vec{A}_c + \vec{\mu}$. Межею області виявлення буде лінія

$$A_n = |\vec{A}_c + \vec{\mu}|, \quad (8)$$

тобто коло радіуса A_n . Центр кола розташовано на відстані A_c від початку координат. Коло невиявлення з центром у точці $(0, -A_c)$ наведено на рис.2.

Тоді ймовірність невиявлення дорівнює двократному інтегралу від $f(a, b)$ в цьому колі, а ймовірність виявлення – одиниці мінус ймовірність невиявлення:

$$P_e = 1 - \int_{-(A_c + A_n)}^{-A_c + A_n} \int_{-\sqrt{A_n^2 - (a + A_c)^2}}^{\sqrt{A_n^2 - (a + A_c)^2}} f(a, b) da db. \quad (9)$$

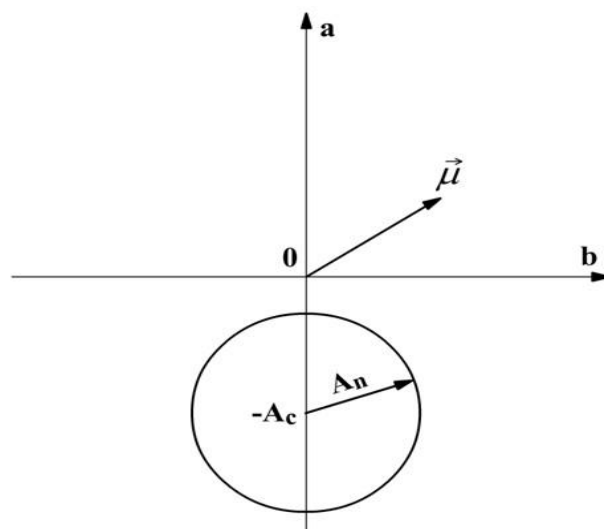


Рис. 2. Підобласті виявлення і невиявлення корисного сигналу

Для визначення σ_{ab} була набрана статистика. Для реалізацій шуму $\mu(t)$ знайдемо значення коефіцієнтів (3) і усереднено із 40 реалізацій шуму при $k=1450$ і $h=1/160$ с:

$$\bar{A}_i = \frac{1}{40} \sum_{k=1}^{40} A_{ik} \quad (10)$$

Для розрахунку P_e обчислювались σ_{ab} , поріг A_n , інтеграл (9) і далі P_e сигналу $x(t) = A_c \cdot \sin(b\pi h k)$ для різних значень P_{np} і A_c . Результати обчислень наведено в табл. 1.

Таблиця 1

Залежність відсотку виявлення сигналу з амплітудою A_c від порогового значення A_n і ймовірності P_n помилки

A_n	P_n	A_c	% виявлення корисного сигналу
1,36	0,01	1,2	43
1,36	0,01	1,5	68
1,36	0,01	2,0	94
1,67	0,001	1,2	19
1,67	0,001	1,5	40
1,67	0,001	2,0	81
1,67	0,001	2,5	97
1,67	0,001	3,0	99,9

Спектри виявлення корисного сигналу із суміші шуму та прихованої періодичності представлено на рис. 3 – 6.

У відповідності до табл.1 маємо відчутний виграш інверсного ноніусного кореляційного підходу до виявлення корисного сигналу.

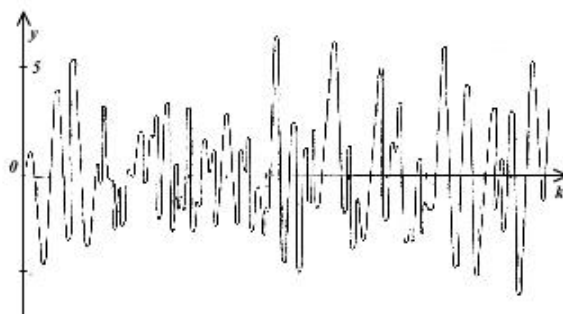


Рис. 3. Зашумлений корисний сигнал

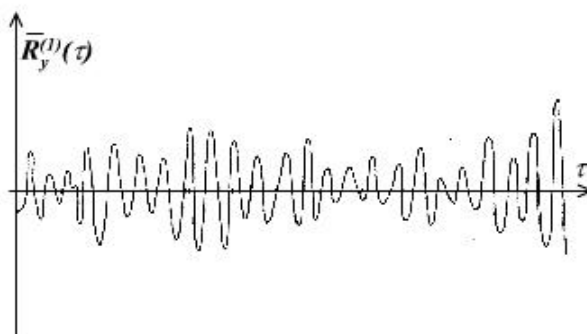


Рис. 4. Перша інверсна кореляція від суміші шуму та корисного сигналу

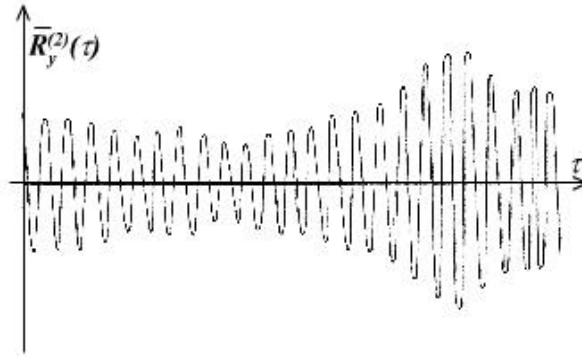


Рис. 5. Друга інверсна кореляція від суміші шуму та корисного сигналу

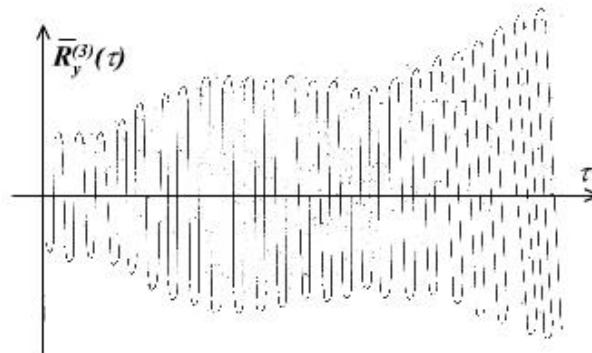


Рис. 6. Третя інверсна кореляція від суміші шуму та корисного сигналу

Даний кореляційний фільтр самоналаштовується до миттєвого значення нелінійної складової вихідного сигналу РТС $\lim_{\gamma \rightarrow \infty} Z(t + \tau) = y_{nl}(t) \cong Z(t + T_p)$, де T_p – період часу, котрий потрібен для автоналаштування фільтра, зараз досяжні значення T_p близько одиниць мікросекунд і менше, що дозволяє порівняно просто виконати задану умову $T_p \ll T_s$.

Застосування такого самоналаштування дозволить усунути багато суттєвих недоліків і обмежень детермінованих фільтрів із апріорно-визначеними параметрами [8].

Висновки

У результаті проведених досліджень, запропоновано шляхи підвищення завадостійкості РТС, котрі мають розширену область застосування, в порівнянні з відомими методами. Використання даного підходу адаптивного синхронного переналагодження у поєднанні із визначенням параметрів прихованої шумами періодичності, відрізняється підвищеною економічністю, так як за інших рівних умов не потрібно "грубих" регулювань коефіцієнта передачі. Також забезпечується відносна завадостійкість функціонування РТС при малопотужних випромінюваннях, що особливо важливо для РТС управління КА. Запропонований ноніусний інверсно-кореляційний метод може бути з успіхом використано, як альтернативу відомому кореляційному [9] у випадку, коли треба виявити зашумлений корисний сигнал.

Список використаної літератури

1. Кантор Л. Я./ Расцвет и кризис спутниковой связи / Л. Я. Кантор // Электросвязь, 2007. – №7. – С. 19-23.
2. Зюко А. Г. Помехоустойчивость и эффективность систем передачи информации/ А. Г. Зюко, А. И. Фалько, И. П. Панфилов, Л. В. Банкет, П. В. Иващенко. – М: Радио и связь, 1985 – 272 с.

3. Куприянов А.И. Радиоэлектронная борьба / А.И. Куприянов. – М.: Вузовская книга, 2013. – 360 с.
4. Козелков С. В. Пути повышения помехоустойчивости радиотехнических систем на основе адаптивной синхронной перестройки приемопередающего тракта / Д.П. Пашков, С.А. Тыщук // Системи обробки інформації. – 2002. – №6(22). – С. 216-219.
5. Егоров Е.И. Использование радиочастотного спектра и радиопомехи / Е.И. Егоров, Н. И. Калашников, А.С. Михайлов. – М.: Радио и связь, 1986. – 304 с.
6. Егоров И.П. Система пространственной режекции помех на основе когерентного весового суммирования / И. П. Егоров, П. В. Русаков, В. В. Павлов, Д. Д. Ганзий // Радиотехника. – М., 2007. – № 11. – С 3–5.
7. Уайт Д. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи. В 3-х вып. Вып. 3. Измерение электромагнитных помех и измерительная аппаратура: Сокр. пер. с англ./Под.ред. А. Д. Князева. – М.: Сов. радио, 1979. – 464 с.
8. Максимов М. В. Защита от радиопомех / М. В. Максимов, М. П. Бобнев, Б. Х. Кривицкий. – М.: Сов. радио, 1976. – 496 с.
9. Волгин В.В., Каримов Р.Н. Оценка корреляционных функций в промышленных системах управления. М.: Энергия, 1978. – 79 с
10. Кулій В.М., Сільвестров А.М., Шефер О.В. Ноніусно-кореляційний метод контролю вібрацій механічних систем // Адаптивні системи автоматичного управління. – 2002 №5(25) С. 93 – 99.

Автор статті

Шефер Олександр Віталійович – кандидат технічних наук, доцент кафедри автоматизації та електропривода, Полтавський національний технічний університет імені Юрія Кондратюка. Тел.: +38 050 183 83 03. E-mail: avs075@ukr.net

Author of the article

Shefer Oleksandr Vitaliiovych – candidate of Sciences (technical), Associate Professor of automation and electric drive Department, Poltava National Technical Yuri Kondratyuk University. Tel.: +38 050 183 83 03. E-mail: avs075@ukr.net

Дата надходження в редакцію: 28.01.2017 р.

Рецензент: д.т.н., проф. С.В. Козелков

ОЦІНЮВАННЯ РІВНЯ «ВИПАДКОВІСТІ» ПОСЛІДОВНОСТІ ПСЕВДОВИПАДКОВИХ БІНАРНИХ ЧИСЕЛ

Butsenko Y.P., Savchenko Y.G. Evaluation of “random” pseudorandom binary sequence of numbers.

The problem of numerical estimation of proximity of pseudorandom sequence to really random sequence is investigated. It is well known an actuality of such a problem, then, in practice, a wide range of tests is used. This tests, predominately, have as a mathematical fundament the theory of independent random trials. If we have a simplest case (p equals q). For n greater, then 100, the using of Gaussian approach and, subsequently, appropriate statistical methods is possible and obvious. At this paper the general approach is connected with an 'entropy' notion.

At proposed entropic approach, main instruments -statistical entropies for different length fragments. The level of dependence of this entropies from length of fragments is used for graphic illustration of proximity of investigated sequence to really random. Authors believe ,that the proposed method is the similar to the compression test of NISTs test suite.

Keywords: pseudorandom sequence, generator, entropy, testing

Буценко Ю.П., Савченко Ю.Г. Оцінювання рівня «випадковості» послідовності псевдовипадкових бінарних чисел.

Розглянуто задачу кількісної оцінки рівня наближеності послідовності псевдовипадкових чисел до істинно випадкової послідовності. Як основний інструмент пропонується застосувати обчислення статистичних ентропій для окремих фрагментів послідовності. Графічно залежність значень ентропій від довжини фрагментів наочно ілюструє наближеність досліджуваної послідовності до істинно випадкової. Пропонований підхід близький до тестування на стиснення в наборі тестів NIST.

Ключові слова: псевдовипадкова послідовність, ентропія, генератор, тестування

Буценко Ю.П., Савченко Ю.Г. Оценка уровня «случайности» последовательности псевдослучайных бинарных чисел.

Рассматривается задача количественной оценки степени приближения последовательности псевдослучайных бинарных чисел к истинно случайной последовательности. В качестве основного инструмента предлагается использовать энтропийный подход и вычисление соответствующих значений энтропии для фрагментов последовательности различной длины. Полученная в результате зависимость энтропии на фрагмент от длины фрагмента в графическом виде иллюстрирует степень приближения тестируемой последовательности к истинно случайной. Проведено сравнение энтропийного подхода с использованием популярных тестов NIST. Показано, что наиболее близким к энтропийному подходу из тестов NIST является тест на сжатие последовательности.

Предлагаемый подход может быть использован для тестирования генераторов последовательностей псевдослучайных чисел.

Ключевые слова: псевдослучайная последовательность, энтропия, генератор, тестирование

Вступ

Актуальність оцінки якості послідовності псевдовипадкових бінарних чисел (ПВБЧ) визначається перед усім використанням таких послідовностей як ключів при шифруванні та паролів доступу до інформаційних ресурсів і послуг. Сьогодні, коли для захисту інформаційного обміну використовуються виключно стандартні шифри (AES, DES, RSA та небагато інших), алгоритми шифрування для яких загальновідомі, саме можливість «підібрати ключі» стає вирішальним фактором безпеки. Мова йде про нейтралізацію хакерських атак та інших спроб несанкціонованого доступу до конференційної інформації. В той же час саме поняття якості зазначених об'єктів є дискусійним і не має сьогодні формального визначення. На неформальному рівні випадковість деякої послідовності чисел (не обов'язково бінарних) визначається можливістю (неможливістю) передбачити, яке число буде наступним у послідовності на основі знання попередніх чисел. Це питання трохи в інших термінах може бути поставлене так: чи є якась закономірність у розташуванні чисел у заданій послідовності? Для справжньої випадкової (істинно випадкової) послідовності такої закономірності не повинно існувати за визначенням.

Виклад основного матеріалу дослідження

При розв'язанні задачі оцінювання рівня «випадковості» послідовності ПВБЧ слід розрізняти два принципово різні випадки.

1. Отримання оцінки умовної якості *однієї* послідовності – дати оцінку (бажано чисельну) рівня наближеності заданої послідовності до істинно випадкової.

2. Оцінювання деякої скінченної множини послідовностей, отриманих від генератора (програмного або апаратного) послідовностей ПВБЧ. Необхідно оцінити усереднену якість генерованих послідовностей, тобто, по суті, якість генератора як джерела, наприклад, ключів для шифрування.

Перший випадок вже за самою постановкою задачі є досить проблематичним з точки зору коректності. Справа в тому, що будь-яка *одна* послідовність чисел сама по собі є випадковою, якщо не відома множина, з якої вона вибрана. Тобто випадковість (якість) однієї послідовності можливо оцінити лише на основі її внутрішніх властивостей. І тут виникає питання: яких саме властивостей? Найбільш відомим тестом з точки зору внутрішніх властивостей є, мабуть, перевірка на визначення значення наступного в послідовності біта на основі всіх попередніх значень. Якщо визначити це значення з ймовірністю, відмінною від $\frac{1}{2}$, неможливо, то така послідовність є випадковою. Це строго доведено ще у 1983 році Андре Йо [1]. Але, на жаль, до цього часу не запропоновано конструктивної процедури проведення такої перевірки.

В узагальненому вигляді оцінювання рівня випадковості заданої послідовності є задачею виявлення внутрішніх закономірностей, притаманних їй, зокрема кореляційних зв'язків між значеннями окремих бітів або груп бітів у послідовності. Такі закономірності повинні, як слід очікувати, обов'язково проявити себе вже на статистичному рівні, тобто у вигляді нерівномірності появи окремих груп бітів у послідовності.

Для прикладу розглянемо числову послідовність натурального ряду $1, 2, \dots, N$. Зрозуміло, що вона не є випадковою, а кореляційний зв'язок між елементами послідовності можна побачити на статистичному рівні, якщо розглядати відносні частоти появи *сусідніх пар* чисел у послідовності. Аналогічно для послідовності

$$1, 1, 2, 4, 8, 16, 32, \dots$$

легко виявити закономірність: кожен наступний елемент є сумою всіх попередніх елементів. У загальному випадку закономірності, притаманні конкретній послідовності, можуть бути досить складними та проявляються лише на статистичному рівні.

Уявімо, що проведено такий статистичний експеримент: досліджувана послідовність записується у деякий регістр і шляхом послідовних зсувів та лічильників фіксуються кількості бітових фрагментів різної довжини. Як результат отримаємо умовний частотний спектр досліджуваної послідовності у вигляді

$$f_0, f_1, f_{00}, f_{01}, f_{10}, f_{11}, f_{000}, f_{001}, \dots, f_{111}, \dots, f_{11\dots10}, f_{11\dots11},$$

де індекс при символі f відповідає тому фрагменту послідовності, який з'явиться в умовному «вікні» при зсувах регістру. Отримані значення f є відображенням частот (або ймовірностей), з якими відповідні фрагменти з'являються в послідовності. Тоді можна обчислити статистичні ентропії повідомлень за умови, що вони начебто передаються як одно- двох-... k -бітові слова

$$\begin{aligned} H_1 &= -\left(\frac{f_0}{N} \log_2 \frac{f_0}{N} + \frac{f_1}{N} \log_2 \frac{f_1}{N} \right), \\ H_2 &= -\frac{1}{2} \left(\frac{f_{00}}{N} \log_2 \frac{f_{00}}{N} + \frac{f_{01}}{N} \log_2 \frac{f_{01}}{N} + \frac{f_{10}}{N} \log_2 \frac{f_{10}}{N} + \frac{f_{11}}{N} \log_2 \frac{f_{11}}{N} \right), \\ &\dots\dots\dots \\ H_k &= -\frac{1}{k} \sum_{00\dots0}^{11\dots1} \frac{f_{ij\dots g}}{N} \log_2 \frac{f_{ij\dots g}}{N}, \end{aligned}$$

де k – довжина відповідного фрагменту.

У більшості реальних випадків, зокрема для генераторів послідовностей, що використовують реєстри зсуву із зворотними зв'язками по модулю 2 функція $H_k = \varphi(k, N)$ є спадаючою та має такий характерний вигляд (рис. 1).

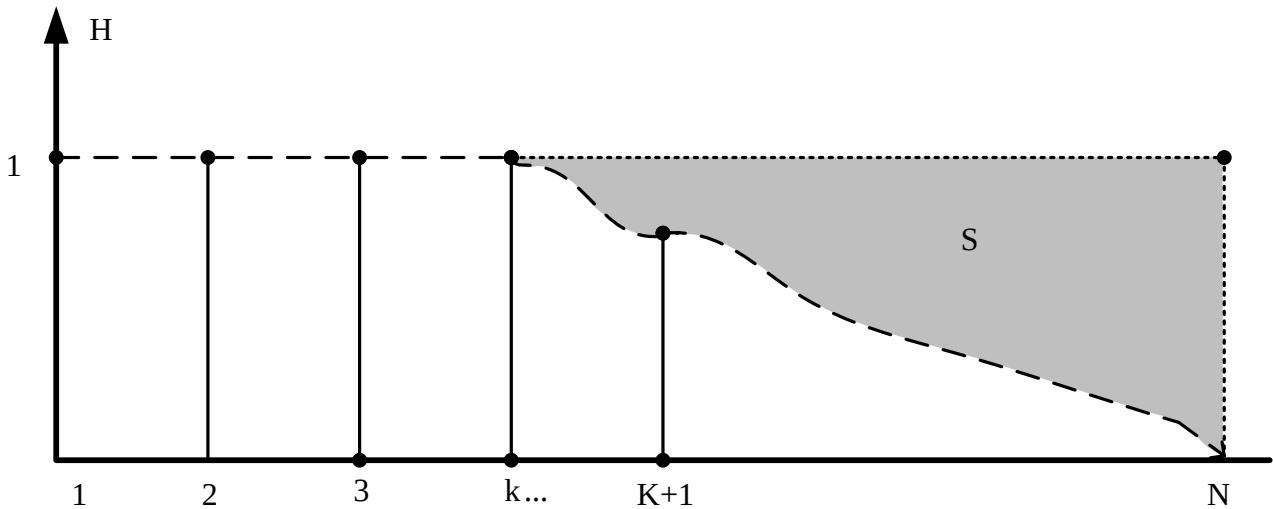


Рис. 1

Цей вигляд можна пояснити таким чином.

Генератори, побудовані на базі реєстрів із зворотними зв'язками, використовують для утворення цих зв'язків коефіцієнти примітивних поліномів у полі GF2, що гарантує разом із іншими умовами генерацію послідовностей максимальної довжини, а це, в свою чергу, забезпечує появу в реєстрі *всіх* можливих комбінацій розрядності k та всіх можливих їх фрагментів. Тому відповідні статистичні ентропії мають максимальне значення для всіх значень k , які менше за довжину реєстру. Далі, після цієї точки відбувається природне зменшення ентропії за рахунок зменшення комбінаторного різноманіття можливих фрагментів (не всі фрагменти довжини, більшої за k може містити генерована послідовність). Мінімальне значення ентропії, очевидно, відповідає випадку, коли $k = N$.

У другому випадку, коли необхідно обчислити деяку усереднену оцінку рівня випадковості сукупності послідовностей, можна спочатку обчислити таку оцінку для кожної з послідовностей, а потім знайти їх середнє арифметичне, вважаючи, що вибираються вони випадковим чином з рівними ймовірностями. Можна очікувати, що загальний вигляд залежності ентропії від довжини фрагментів залишиться приблизно таким самим, як і для однієї послідовності.

Зазначимо, що в усіх відношеннях аналогічно генератору випадкових 0 та 1 є реалізація найпростішої схеми випробувань Бернуллі ($p = q = 1/2$). Така схема давно та, можна сказати, вичерпно досліджена. Основними при цьому є формула Бернуллі (для імовірності кількості «успіхів» у n випробуваннях), локальна та інтегральна формули Муавра-Лапласа як асимптотичні варіанти попередньої. Зазначимо, що на практиці рекомендується використовувати останні дві формули, починаючи з $n = 100$ (у нашому випадку це довжина послідовності ПВБЧ), причому при збільшенні n точність формул зростає. До того ж саме при $p = q = 1/2$ точність максимальна. Закладену у формулах можливість апроксимувати центровану та нормовану певним чином кількість 0 (або, що теж саме, 1) у послідовності за допомогою випадкової величини, розподіленої за стандартним нормальним законом використовують такі тести NIST [2], як частотний побітовий, частотний блочний, тест на однакові біти, що йдуть підряд, на найдовшу послідовність одиниць. Як і слід було очікувати, їх рекомендується використовувати при $n \geq 100$. Більш витонченим, можна сказати, є ранговий тест, що ґрунтується на роботах І.М. Коваленка [3]. По суті, він еквівалентний дослідженню, чи не є група m послідовних символів із n лінійною комбінацією попередніх аналогічних фрагментів довжини m

Близьким до рангового є спектральний тест, що виявляє повторюваність фрагментів у послідовності. Тести на повторюваність шаблонів (різновиди – шаблони перетинаються або не перетинаються) виявляють можливість отримання блоків шляхом внутрішніх перестановок. До цих тестів, у свою чергу, близьким є тест на лінійну складність, який має на меті виявлення факту застосування для генерації послідовностей вже згаданих регістрів зсуву із зворотними зв'язками по модулю 2.

Значно ширшим за можливою сферою застосування є універсальний тест Мауера, що полягає у з'ясуванні можливості безвтратного стиснення послідовності. Тести кумулятивних сум та на довільні відхилення фактично ведуть до вивчення поведінки випадкових блукань по одновимірній цілочисельній решітці та спираються на відповідні граничні теореми. З точки зору пропонованого підходу особливу увагу до себе звертають тести на підпослідовності та наближену ентропію.

У загальному та практичному плані найбільш привабливим серед відомих тестів можна вважати тести на стиснення. Чим в більшій мірі може бути стиснена тестована послідовність, тим гірші її показники «випадковості». Їх аналогами з формальних тестів є тести ентропії, які

спираються на той факт, що функція $E(x_1, \dots, x_k) = -\frac{1}{k} \sum_{i=1}^k x_i \log_2 x_i$ має за наявності рівняння зв'язку $x_1 + x_2 + \dots + x_n = 1$ єдиний максимум, рівний 1. Якщо $x_1, x_2, \dots, x_n$ – частоти деякого повного набору можливих бінарних комбінацій у послідовності (зазвичай $n = 2^k$), то розглядаються всі можливі бінарні фрагменти, то $H_k = 1$ при $x_1 = x_2 = \dots = x_k = \frac{1}{2^k}$ (ідеальний

випадок). В той же час ці частоти при $N \gg 1$ внаслідок існуючих граничних теорем дуже близькі до своїх теоретичних значень для майже всіх реалізацій випадкової послідовності та менші 1 для генерованих псевдовипадкових послідовностей при однакових значеннях N .

Спираючись на припущення, зроблене А.М. Колмогоровим ще в 1965 р. у класичній роботі [4], можна обережно стверджувати, що складність опису процедури генерації (формування) послідовності ПВБЧ є показником наближеності її до істинно випадкової. Можна, мабуть, сказати, що за простим алгоритмом генерації не можна сформулювати «якісну» послідовність ПВБЧ. Тому виникає незвична та парадоксальна ситуація: чим складніший алгоритм генерації, тим краще! Правда, зразу ж виникає проблема: а чим вимірювати складність? Із цієї точки зору популярні алгоритми генерації, що базуються на використанні регістрів зсуву, є занадто простими і тому майже не захищені від так званих алгебраїчних атак [5]. При використанні більш складних моделей цього недоліку можна у багатьох випадках уникнути, наприклад, застосовуючи моделі цифрових автоматів із пам'яттю [6].

Насправді, якщо замислитись, що таке випадкова послідовність чисел? Мабуть, така, яку ми не зможемо передбачити, тобто **будь-яка**. А чи можливо **будь-яку** послідовність якось описати іншим способом, ніж переліком її елементів у послідовності? Хто може стверджувати, що здатен запропонувати такий спосіб? Якщо існує такий спосіб, в ентропійному вимірі це відповідає можливості стиснення первинного опису. Тобто відносна площа області «сірої зони» S на рисунку (наприклад, у відсотках до загальної площі прямокутника) і є тією кількісною мірою відхилення досліджуваної послідовності від істинно випадкової. Із такої точки зору будь-яка послідовність, сформована за допомогою детермінованої процедури принципово не може бути істинно випадковою. Але важко сподіватись, що такі загальнотеоретичні питання можуть бути вирішені у короткому повідомленні. Тому на завершення зупинимось на практичних аспектах задачі.

Оцінювання рівня випадковості однієї окремо взятої послідовності з практичної точки зору позбавлено, на наш погляд, сенсу, оскільки не відомо, як можна реально використати результат такого оцінювання. Інша справа, коли мова йде про результати, отримані для деякої сукупності послідовностей, сформованих реальним генератором (програмним чи апаратним). У цьому випадку кількісна оцінка може стати базою для порівняння різних алгоритмів генерації та відбору кращого з них. Окрім того, конкретний вигляд залежності $H_k = \varphi(k, N)$ надає корисну інформацію для криптоаналізу. Зокрема, значення k , при якому починається спадання залежності, у більшості випадків однозначно співпадає з довжиною

реєстру зсуву при реєстровій реалізації генератора або кількості елементів пам'яті при використанні для цього автоматних моделей.

Висновок

На завершення слід зауважити, що реалізація пропонованого, а також параметричного [7] підходів при реальних значеннях довжини ключів ($N = 64 \dots 256$) може бути пов'язана із обмеженнями витрат на час реалізації статистичного експерименту із досліджуваною послідовністю. Тому для частини залежності $H_k = \varphi(k, N)$ доведеться скористатися її, наприклад, лінійною апроксимацією. Але найбільш важливим у запропонованому підході, на нашу думку, є можливість отримання саме кількісної оцінки рівня випадковості послідовностей ПВБЧ та порівняння різних алгоритмів генерації.

Список використаної літератури

1. Danny Dolev, Andrew Chi-Chih Yao On the security of public key protocols / Danny Dolev, Andrew Chi-Chih Yao // - IEEE Trans. Information Theory. - 1983. - №29. - P. 198-207.
2. Потий А., Орлова С. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / А. Потий, С. Орлова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. - 2001. - №2. - С. 206-214
3. Коваленко И.Г. Теория вероятностей и ее применение / И.Г. Коваленко // М.: Физматлит, 1972. - 435 с.
4. Колмогоров А.Н. Три подхода к определению понятия «количество» информации / А.Н. Колмогоров // Проблемы передачи информации. - 1965. - Т.1. - С. 3-11
5. Пометун С.О. Алгебраїчні атаки на потокові шифратори як узагальнення кореляційних атак / С.О. Пометун // Системні дослідження та інформаційні технології. - 2008. - №2. - С. 29-40
6. Буценко Ю.П., Савченко Ю.Г. Автоматні моделі генераторів псевдовипадкових бінарних чисел / Ю.П. Буценко, Ю.Г. Савченко // Сучасний захист інформації. - 2016. - №1. - С. 32-37
7. Буценко Ю.П., Савченко Ю.Г. Тестування бінарних послідовностей: параметричний підхід / Ю.П. Буценко, Ю.Г. Савченко // П'ятнадцята міжнародна наукова конференція імені академіка Михайла Кравчука, Матеріали конференції, ч. 3 – Теорія ймовірностей та математична статистика. - 2013. - С. 30-32

Автори статті

Буценко Юрій Павлович - кандидат фізико-математичних наук, доцент, доцент кафедри математичного аналізу та теорії ймовірностей, Національний технічний університет України «КПІ» ім. І. Сікорського, Київ, Україна. Тел. +38 050 207 34 42. E-mail: armchairdoc@yandex.ua

Савченко Юлій Григорович - доктор технічних наук, професор, професор кафедри звукотехніки та реєстрації інформації, Національний технічний університет України «КПІ» ім. І. Сікорського, Київ, Україна. Тел. +38 095 838 97 69. E-mail: ssaavvaa@ukr.net

Authors of the article

Butsenko Yuriy Pavlovich – Candidate of Sciences (physics and mathematics), associate professor, associate professor of Department probability theory and mathematical analysis, National Technical University of Ukraine “Igor Sikorsky KPI”, Kyiv, Ukraine. Tel. +38 050 207 34 42. E-mail: armchairdoc@yandex.ua

Savchenko Yulij Grigorievich – Doctor of Sciences(technical), professor, professor of Department Audio Engineering and Information Registration, National Technical University of Ukraine “Igor Sikorsky KPI”, Kyiv, Ukraine. Tel. +38 095 276 92 70. E-mail: ssaavvaa@ukr.net

Дата надходження в редакцію: 30.01.2017 р.

Рецензент: д.т.н., проф. А.І. Семенко

УДК 004.413 (045)

Грінченко О.О.; Грінченко С.А.

КОНЦЕПТУАЛЬНІ ОСНОВИ МЕТОДІВ МОДЕЛЮВАННЯ ЕКОСИСТЕМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Grinenko O.O., Grinenko S.A. Conceptual foundations of methods of software ecosystem modeling.

The study of software ecosystems consists of the analysis and construction of representations. This paper proposes to consider conceptual methods of software ecosystems modeling according to information interactions between its components. There were made analysis of several scientific papers, which deal with models and modeling of software ecosystems, i.e. i*, UML, Petri nets. The purpose of the article is to develop a conceptual basis of modeling techniques of software ecosystems. There were described the main components of software ecosystems, their relationships and methods for their modeling. It was paid great attention to Model Driven Architecture (MDA), which are used for software ecosystem modeling. MDA provides a common environment for software development that promotes interaction between groups of developers in the process of data analysis and validation of systems; engineers can find and fix errors on the early stages of designing of a system, when time and financial implications of changes in the system are minimized; MDA promotes the reuse of models to improve the system and derived systems with advanced features. Another important problem, which is considered in the article is an assessment of the software, its environment and components.

Грінченко О.О., Грінченко С.А. Концептуальні основи моделювання екосистем програмного забезпечення. Дослідження екосистем програмного забезпечення складається з аналізу і побудови уявлень про них. У даній статті пропонується розглянути концептуальні методи моделювання екосистем програмного забезпечення відповідно до інформаційної взаємодії між їх компонентами. Також у роботі описуються основні компоненти екосистем програмного забезпечення, зв'язки між ними і методи їх моделювання. Було приділено велику увагу модельно-орієнтованому підходу (Model Driven Architecture – MDA), який використовується для моделювання екосистем програмного забезпечення.

Гриненко А.А., Гриненко С.А. Концептуальные основы моделирования экосистем программного обеспечения. Исследование экосистем программного обеспечения состоит из анализа и построения представлений о них. В данной статье предлагается рассмотреть концептуальные методы моделирования экосистем программного обеспечения в соответствии с информационным взаимодействием между их компонентами. Также в работе описываются основные компоненты экосистем программного обеспечения, связи между ними и методы их моделирования. Было уделено большое внимание модельно-ориентированного подхода (Model Driven Architecture - MDA), который используется для моделирования экосистем программного обеспечения.

Вступ

На сьогодні стан програмного забезпечення (ПЗ) можна охарактеризувати глобальним поширенням, надвеликим обсягом, складними взаємодіями, інтеграцією в повсякденне життя людей, а також появою нових видів взаємодій при управлінні.

Така ситуація штовхає вчених та розробників на нові шляхи дослідження програмного забезпечення. Однією з нових тенденцій є розгляд систем програмного забезпечення з позиції біологічних екосистем. Такий підхід отримав назву екосистема програмного забезпечення (ЕПЗ). Як показав досвід таких брендів як Microsoft, Google, Apple побудова ЕПЗ є ефективним шляхом розвитку ПЗ.

Тому питання побудови моделей ЕПЗ є актуальним. Швидкий розвиток інформаційних технологій спонукає до систематизації ПЗ, яке можна регулювати на всіх стадіях його життєвого циклу. Правильно організована робота розробників, замовників, та користувачів програмного забезпечення – запорука успіху для компаній ІТ індустрії.

Одним з основних факторів ефективності ЕПЗ є інформаційна взаємодія між компонентами системи. Чим швидше і достовірніше надається інформація в процесі управління ПЗ тим більш злагоджено буде функціонувати екосистема.

Аналіз публікацій

Дослідження та побудова моделей ЕПЗ на даний час є актуальним питанням.

Поняття та визначення «екосистема програмного забезпечення» та супутні терміни активно використовуються виробниками і дослідниками ПЗ. Огляд web-сайтів провідних виробників ПЗ показує, що більшість з них застосовують поняття «екосистема ПЗ» [1, 2], позначаючи цим системи, що включають розробника, його ПЗ та партнерів. Наукові дослідження, що використовують поняття екосистем, на сьогоднішній день представлені кількома працями [2, 3]. У роботі [3] автори описують типові елементи екосистем та їх контекст, а також екосистеми розглядаються як рівень абстракції над проектами, який може бути описаний шляхом аналізу нижніх рівнів. У науковій роботі [4], присвяченій системам ультравеликого масштабу (Ultra-Large-Scale Systems), наголошується, що в галузі існує тенденція до використання концепцій екосистем, для позначення соціально-технічних систем ПЗ. В Україні відомі роботи науковців [5–9], які протягом останніх 10 років вивчають та досліджують ЕПЗ. Наприклад, у роботі [5] представлено застосування екологічного підходу до дослідження ПЗ та формуються основні поняття розділу інженерії програмного забезпечення – екології програмного забезпечення.

Основними елементами екосистеми ПЗ є прикладні продукти та послуги, виробники продуктів та послуг, споживачі, зв'язки між ними. Важливим у дослідженні ЕПЗ є створення їх моделей, а також засобів для їх моделювання та дослідження основних задач, пов'язаних з моделюванням ЕПЗ.

Для опису моделей ЕПЗ застосовують наступні засоби моделювання і*, UML, мережі Петрі [8].

І* мова моделювання. Використовується для розуміння та моделювання ЕПЗ [8]. І* дає можливість розробникам отримати потрібну інформацію на ранньому етапі процесу розробки ПЗ.

Мова UML. Мова UML розвивається з 1994 року і є результатом злиття трьох найбільш відомих об'єктно-орієнтованих підходів: методу Буча, OTM, і OOSE. Вона об'єднує велику кількість різних графічних нотацій з метою впорядкування хаотичного набору графічних засобів, які використовуються під час створення ПЗ. Виступає універсальною мовою моделювання [8]. UML модель ЕПЗ можна представити за допомогою діаграми прецедентів. Діаграма прецедентів (Use Case Diagram) є графічним засобом специфікування вимог.

Мережі Петрі. На практиці моделювання систем часто доводиться вирішувати завдання, пов'язані з формалізованим описом і аналізом причинно-наслідкових зв'язків в складних системах, де одночасно паралельно протікає кілька процесів. Мережі Петрі є найпоширенішим в даний час формалізмом, що описує структуру і взаємодію паралельних систем і процесів [8, 10].

Формування мети дослідження

Мета статті полягає в розробці концептуальних основ методів моделювання ЕПЗ.

Основна частина

На сьогодні існує величезна кількість методів моделювання систем [10-17] і вибрати найкращий для опису ЕПЗ є складною задачею. При розробці моделі слід враховувати дві взаємно суперечливих тенденцій: прагнення до повноти опису і прагнення до отримання необхідних результатів максимально простими засобами. Досягнення компромісу ведеться зазвичай шляхом побудови серії моделей, що починаються з гранично простих і висхідних до високої складності (існує відоме правило: починай з простих моделей, а далі ускладнюй). Прості моделі допомагають глибше зрозуміти досліджувану проблему. Ускладнені моделі

використовуються для аналізу впливу різних чинників на результати моделювання. Такий аналіз дозволяє виключати деякі чинники з розгляду.

Виходячи з вищевикладеного можна запропонувати наступний метод моделювання ЕПЗ. Реалізація цього методу полягає у використанні модельно-орієнтованого підходу (MDA).

Одним із головних намірів MDA є відділення логіки предметної області від конкретної технології реалізації, дозволяючи цим двом частинам змінюватись незалежно одна від одної.

Наприклад, компанія Nissan Motor Co., LTD, використовуючи MDA для проектування системи зменшення вихлопу, сертифікованої за California Air Resources Board (CARB) згідно з стандартом Partial Zero Emission Vehicle (PZEV), скоротила час розробки на 50%, зменшила число датчиків і одержала премію від управління з охорони навколишнього середовища (США).

Компанія ABB також застосувала MDA для проектування розробки і перевірки ПЗ системи управління силових електронних блоків управління АС 800РЕС для силових перетворювачів. В результаті час і вартість розробки скоротилась, процес розробки став більш ефективним, якість генерованого коду помітно підвищилася.

Отже, дамо загальні визначення основним поняттям MDA. Слід, спочатку, зазначити що серед спільноти, яка вивчає модельно-орієнтований підхід, в силу різних причин, не існує однозначного тлумачення основних термінів: моделі, мета-моделі й інших. Усе ж таки зупинимось на більш компромісних варіантах.

Означення 1. Модель – це спрощення існуючої системи, побудоване у відповідності до певної мети. В рамках даної статті будемо розглядати модель ЕПЗ.

Означення 2. Мета-модель – це модель мови моделювання.

Модель до мета-моделі знаходяться у відношенні відповідності, оскільки модель написана на мові, яку мета-модель визначає. Позначимо це відношення через $\mathcal{X}$. Мета-модель за означенням є моделлю, отже, вона написана на мові своєї мета-моделі – так званої мета-мета-моделі. Ланцюжок відношень модель-мета-модель теоретично може бути як завгодно довгим.

Щоб краще зрозуміти призначення різних стандартів в MDA, потрібно розглянути поняття **рівнів моделювання**.

OMG використовує чотириохрівневу архітектуру, яка часто називається, характеризуючи її вміст, архітектурою 3+1. Рівні в цій архітектурі позначаються таким чином: M0, M1, M2, і M3 (див. рис. 1).

В архітектурі 3+1 бачимо троє відношень відповідності ($\mathcal{X}$): M1-M2, M2-M3, M3-M3 та одне відношення відображення (μ): M0-M1.

Наявність трьох рівнів моделювання, кожен з яких знаходиться у відповідності з вищим рівнем (крім M3), дає змогу проводити трансформації моделей на усіх 3-х рівнях.

Розглянемо кожен рівень моделювання більш детально.

M0. ЕПЗ.

Найнижчим рівнем є M0 – рівень досліджуваної нами системи. Модель відображає (μ) цю систему на рівні M1. Модель рівня M1 відповідає ($\mathcal{X}$) своїй мета-моделі, яка знаходиться на рівні M2. А мета-модель, у свою чергу, відповідає мета-мета-моделі на рівні M3. Завершується цей ланцюжок відношень рівнем мета-мета-моделі встановленням відношення відповідності на себе.

Для створення моделі рівня M1, з рівня M0 необхідно надати інформацію про компоненти за зв'язки ЕПЗ. ЕПЗ може бути представлена як сукупність компонентів: навколишнє середовище, людина та ПЗ. У якості зв'язків можна розглядати інформаційну взаємодію між компонентами, яка розділена на чотири категорії: дія, управління, реакція та плив.

Концептуально модель інформаційної взаємодії ЕПЗ буде мати наступний вигляд (рис.2.):

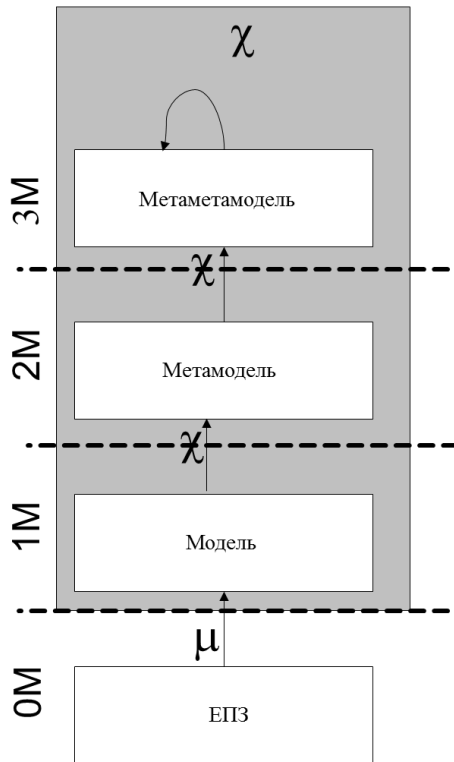


Рис. 1. Архітектура 3+1

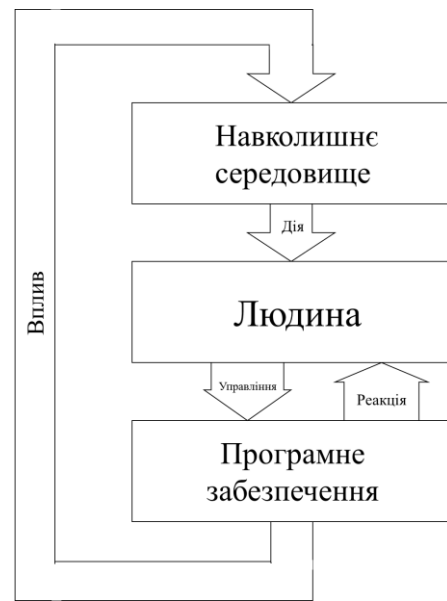


Рис. 2. Концептуальна модель інформаційної взаємодії ЕПЗ

Така модель дає уявлення про взаємодіючі компоненти екосистеми та категорії зав'язків, але не показано їх сутності. Не зрозуміло, яким чином навколишнє середовище діє на людину і як ця дія спонукає до управління ПЗ. Такої інформації недостатньо для побудови адекватної моделі ЕПЗ.

Тому, для створення моделі ЕПЗ рівня 1М спочатку необхідно вирішити задачу формалізації інформаційної дії в ЕПЗ. Основою вирішення цієї задачі буде теорія несилової взаємодії. Оскільки вона в числовій формі досить точно дозволяє ідентифікувати необхідні зміни у відношенні до категорій навколишнього середовища у суб'єктів системи (компонент – людина). Для цього необхідно стандартизувати бачення різноманітних компонентів навколишнього середовища і особливо їх взаємозв'язок з баченням представників зацікавлених сторін та менеджерів того результату, який заданий цілями ЕПЗ. Інструменти інформаційної дії на людину включатимуть в себе способи отримання необхідної інформації. Вирішення цієї задачі дозволить досягти мети – ефективно управляти ПЗ.

Управління інформацією повинне бути таким, щоб діяти на суб'єкти ЕПЗ таким чином, щоб вони оптимально реагували на готовність ПЗ і його частин на відхилення в плані управління ПЗ, на ситуацію в навколишньому середовищі та в середовищі самої екосистеми.

Для управління ПЗ важливим є не тільки факт відхилення його стану від планових змін, але й сама величина відхилення. Будемо розглядати два ключові відхилення, які впливають найбільше на рішення в управлінні ПЗ. Це відхилення у навколишньому середовищі та відхилення в стані ПЗ. Задамо функції, що визначають:

1. Дію на суб'єктів екосистеми ПЗ, яка обумовлена відхиленням

$$\eta(V_e(t), V_e^*(t), G_e(t), G_e^*(t), S, t), \text{ де}$$

- | | |
|------------|---|
| $V_e(t)$ | – план управління ПЗ; |
| $V_e^*(t)$ | – фактичне управління ПЗ; |
| $G_e(t)$ | – плановий стан ПЗ в момент часу t ; |
| $G_e^*(t)$ | – фактичний стан ПЗ в момент часу t . |

$\eta(V_e(t), V_e^*(t), G_e(t), G_e^*(t), S, t)$ – інформаційна дія на суб'єкти ЕПЗ, що визначається часом, зацікавленою стороною, величиною відхилення в навколишньому середовищі та в стані ПЗ в момент часу t ; t – момент часу; S – зацікавлена сторона.

2. Реакція зацікавленої сторони, яка є результатом відхилення

$$d(\eta(V_e(t), V_e^*(t), G_e(t), G_e^*(t), S, t), t_0),$$

де $d(\eta(V_e(t), V_e^*(t), G_e(t), G_e^*(t), S, t), t_0)$ – можливі реакції зацікавленої сторони S , що визначаються інформаційним впливом $\eta(V_e(t), V_e^*(t), G_e(t), G_e^*(t), S, t)$ в момент часу t_0 ; t_0 – момент часу, коли формується реакція зацікавленої сторони.

Визначення оптимальної інформаційної дії, яка повинна формуватися під час взаємодії компонентів ПЗ – людина було б зробити не складно, якщо це відносилось лише до одного фактору взаємодії. Для 4-х наведених впливів (навколишнє середовище, стан, зацікавлена сторона і час), в яких, скажімо, виділяється до 20 різноманітних значень (насправді їх набагато більше) буде отримано $20^4=160000$ варіантів. Що неможливо описати в будь якій системі. Тому необхідне застосування спеціальних методів по визначенню найбільш інформативних впливів (дій) на суб'єкти ЕПЗ. І по окремим діям на них визначати оптимальну реакцію в тій чи іншій ситуації. Для цього спочатку сформуємо математичну модель декомпозиції інформаційних дій на суб'єктів екосистеми ПЗ.

Означення 3. Інформаційна дія на суб'єкти екосистеми – цілеорієнтоване надання суб'єктам ЕПЗ інформації про зміни в навколишньому середовищі.

Означення 4. Суб'єкти ЕПЗ – зацікавлені сторони управління ПЗ, особи, що приймають рішення, виконавці робіт та контрагенти.

Означення 5. Інформаційні впливи – екологічні звіти, технічне завдання на розробку ПЗ, відклики користувачів, звіти про роботу ПЗ, інше.

Для того, щоб визначити найбільш вагому дію на зацікавлених сторін, залежну від наведених чотирьох чинників, розглянемо суперпозицію функцій:

$$\eta(V_e(t), V_e^*(t), G_e(t), G_e^*(t), S, t) = f(\eta^1(V_e(t), V_e^*(t)), \eta^2(G_e(t), G_e^*(t)), \eta^3(S), \eta^4(t)),$$

де $\eta^1(V_e(t), V_e^*(t))$ – інформаційна дія на суб'єктів, що визначається величиною відхилення в навколишньому середовищі;

$\eta^2(G_e(t), G_e^*(t))$ – інформаційна дія на суб'єктів екосистеми ПЗ, що визначається величиною відхилення в стані програмного забезпечення;

$\eta^3(S)$ – інформаційна дія суб'єкту екосистеми ПЗ S ;

$\eta^4(t)$ – інформаційна дія часу t .

Запропонована в теорії несилової взаємодії модель дає можливість отримати по спостереженню за проявами окремих об'єктів, чи по окремим експертним оцінкам, їх спільну дію на рішення по управлінню ПЗ. Нехай методами експертної оцінки, чи з застосуванням статистичних методів отримані суб'єктивні імовірності, чи оцінки вибору (в межах $[0,1]$) тих чи інших впливів на зацікавлених сторін в залежності:

1. Від відхилення в навколишньому середовищі:

$$p_{ej}^1 = f_1(\eta^1(V_e(t), V_e^*(t)) = F_j), \quad (1)$$

де $p_{ej}^1 = f_1(\eta^1(V_e(t), V_e^*(t)) = F_j)$ – оцінка того, що при заданих плановому і фактичному показниках в навколишньому середовищі необхідна інформаційна дія F_j ; F_j – інформаційна дія на зацікавлених сторін (інформація про необхідність покращення, аналізу чи пристосування до навколишнього середовища за допомогою ПЗ або ліквідація шкідливих наслідків використання ПЗ).

2. Від стану компонента ЕПЗ:

$$p_{ej}^2 = f_2(\eta^2(G_e(t), G_e^*(t)) = F_j), \quad (2)$$

де $p_{ej}^2 = f_2(\eta^2(G_e(t), G_e^*(t)) = F_j)$ – оцінка того, що при заданих плановому і фактичному показниках зміни стану ПЗ необхідна інформаційна дія F_j .

3. Від зацікавленої сторони:

$$p_{ej}^3 = f_3(\eta^3(S) = F_j), \quad (3)$$

де $p_{ej}^3 = f_3(\eta^3(S) = F_j)$ – оцінка того, що зацікавлена сторона екосистеми ПЗS буде вимагати інформаційну дію F_j .

4. Від того, на якій стадії знаходиться ПЗ:

$$p_{ej}^4 = f_4(\eta^4(t_e) = F_j), \quad (4)$$

де $p_{ej}^4 = f_4(\eta^4(t_e) = F_j)$ – імовірність того, що на фазі життєвого циклу ПЗ t_e буде інформаційна дія F_j ; t_e – фаза ПЗ.

По суті цими функціями задана випадкова поведінка системи інформування зацікавлених сторін S , відносно ПЗ, де з ймовірностями, які відповідають оцінкам $p_{ej}^k(X)$, $k = \overline{1,4}$ реалізується вибір виду дії (впливу) на зацікавлені сторони F_j .

М1. Модель

Після отримання декомпозиції інформаційної дії в ЕПЗ можна перейти до побудови моделі.

По принципу чорної скриньки у якості вхідної інформації будемо мати компоненти ЕПЗ та інформаційні взаємозв'язки між ними, а вихідною інформацією є модель ЕПЗ (рис.3).



Рис. 3. Чорна скринька MDA

Побудова моделі ведеться певною мовою моделювання. Запропонованою мовою моделювання від OMG є Unified Modeling Language (UML), яка є мовою загального призначення. Але є можливість розширення під свою предметну область.

Візуальне моделювання в UML можна представити як деякий процес покрокового спуску від найбільш загальної і абстрактної концептуальної моделі вихідної системи до логічної, а потім, і до фізичної моделі відповідної програмної системи. Для досягнення цих цілей спочатку будується модель у формі так званої діаграми варіантів використання (use case diagram), що описує функціональне призначення системи або, іншими словами, те, що система буде робити в процесі свого функціонування. Діаграма варіантів використання є вихідним концептуальним поданням або концептуальною моделлю системи в процесі її проектування й розробки.

Суть даної діаграми полягає в наступному: проектована система представляється у вигляді множини сутностей та акторів, що взаємодіють із системою за допомогою так званих варіантів використання. При цьому актором (actor), або діючою особою, називають будь-яку сутність, що взаємодіє із системою ззовні. Це може бути людина, технічний пристрій, програма або будь-яка інша система, що може бути джерелом впливу на систему, що

моделюється, так, як визначить сам розробник. У свою чергу, варіанти використання (use case) слугують для опису сервісів, які система надає акторові.

Наведена вище діаграма варіантів використання, у свою чергу, може бути деталізована далі з метою більш глибокого уточнення поставлених до системи вимог і конкретизації деталей її наступної реалізації.

Побудуємо модель ЕПЗ з використанням інформаційних впливів на її елементи. Як було описано вище ЕПЗ складається з трьох сутностей Людина – ПЗ – Зовнішнє середовище.

М2. Мета-модель

Існує дві причини чому побудова мета-моделей важлива для модельно-орієнтованого підходу. По-перше, потрібний механізм для визначення недвозначних (формалізованих) мов моделювання. У модельно-орієнтованому підході такий механізм здійснюється через побудову мета-моделей (метамодельювання) [6].

По-друге, ключові для модельно-орієнтованого підходу механізми трансформації моделей використовують мета-моделі. Інструменти, що реалізують механізми перетворень, уміщують опис, як модель на вхідній мові може бути перетворено в моделі на вихідній мові. Ці правила використовують мета-моделі початкових і цільових мов для визначення перетворення.

Побудова мета-моделі здійснюється на основі аналізу атрибутів, функцій, структури та інших властивостей моделі. У залежності від виду моделей, можна виділити два підходи до створення мета-моделей:

- алгебраїчний (або безпосередній), що здійснюється на підставі аналізу моделей, як частини дійсності;
- логічний(або опосередкований), що здійснюється на підставі аналізу інформаційних потоків в моделі.

У першому випадку входом методу для побудови метамоделі є атрибути, структура, правила, операції та інші елементи моделі, що надані у формі фізичних величин, випадкових процесів, математичних функцій, фізичних законів та тому подібне. У другому випадку метамоделі будуються на основі моделі знань (зокрема, семантичної мережі, продукційної, фреймової, логічної моделі тощо)[13].

Зазначимо, що можливим є існування змішаних випадків, коли входом методу для побудови метамоделі є водночас як алгебраїчні так і логічні моделі.

У даній роботі розглядається метод розробки метамоделей на основі логічних моделей, що має важливе окреме значення у рамках сучасних ІТ.

Сутність підходу полягає у зануренні логічної моделі у деяку систему, що містить інформаційні зв'язки між об'єктами, та розглядається як метамоделі.

Таким чином, логічна модель розглядається як метамоделі(М2).

М3. Мета-мета-модель

Рівень мета-мета-моделі утворює початкову основу для усіх мета-модельних представлень. Головне призначення цього рівня полягає в тому, щоб визначити мову для специфікації метамоделі. Мета-мета-модель визначає модель мови UML на самому високому рівні абстракції і являється найбільш компактним її описом. З іншого боку, мета-мета-модель може включати декілька мета-моделей, чим досягається потенціальна гнучкість включення додаткових понять. Прикладами понять цього рівня служать мета клас, метаатрибут.

Слід зазначити, що семантика мета-мета-моделі не входить в опис мови UML. З одного боку, це робить мову UML простішою для вивчення, оскільки не потрібно знання теорії формальних мов і формальної логіки. З іншого боку, наявність мета-мета-моделі надає мові UML статус науковості, який потрібний йому для того, щоб бути непротирічною формальною мовою. Якщо ці особливості можуть представлятися мало цікавими для багатьох програмістів, то розробники інструментальних засобів ніяк не можуть їх ігнорувати.

В рамках даної статті ми використали мову моделювання MOF (Meta Object Facility). MOF – стандарт OMG, який визначає мову, яка слугує для визначення мов моделювання. MOF знаходиться на найвищому рівні (М3) моделі чотирьох рівневої архітектури OMG. MOF є мета-мета-моделлю для всіх мета-моделей. MOF використовується не лише для побудови мов моделювання, але й для побудови інструментів для побудови мов моделювання. Тому MOF забезпечений додатковою функціональністю. MOF, також

використовується для визначення потокового, або файлового формату обміну для моделей рівня M1. Кожна мова моделювання визначена у відповідності з мета-моделлю описаної в MOF. MOF визначає стандартний шлях проводити обмін для мов моделювання. Цей формат обміну базується на XML, і має назву XMI (XML Metadata Interchange). Оскільки MOF є мета-моделлю для себе, XMI може використовуватися також для генерації стандартного формату обміну для мета-моделей.

Розглянемо на прикладі використання методу MDA для приладобудівного підприємства.

Для побудови моделі рівня M1 зобразимо відношення замовника та користувача ПЗ. Вони взаємодіють через PRP-system. Користувач отримує необхідну інформацію з PRP-system, а замовник під впливом навколишнього середовища ініціює її розробку (рис. 4.).

Як видно на рис.5. з'явився суб'єкт Розробник, який виконує розробку PRP-system, а Кінцевий користувач в свою чергу надає вимоги до розроблюваної системи, Замовник виконує задачу управління розробкою.

Модель M3 ще більш деталізує і розкриває сутності взаємовідношень ЕПЗ та процеси розробки PRP-system.

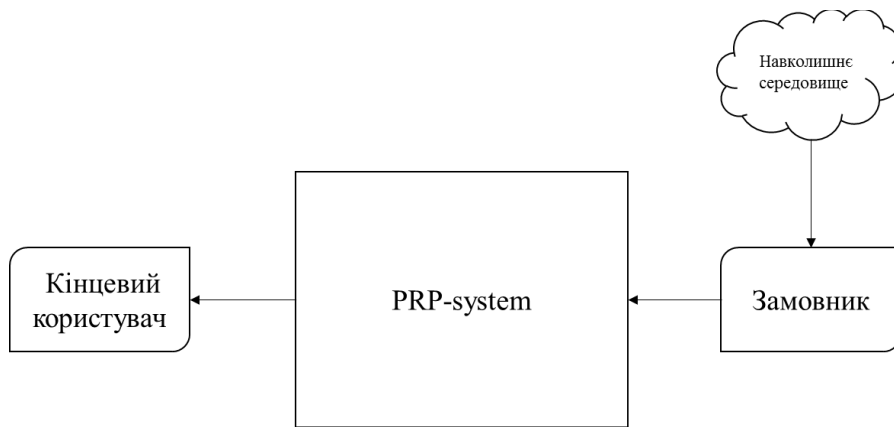


Рис. 4. Модель M1 ЕПЗ

Далі продовжуємо деталізувати відношення між компонентами системи. Додаються нові суб'єкти та сутності системи (рис. 5).

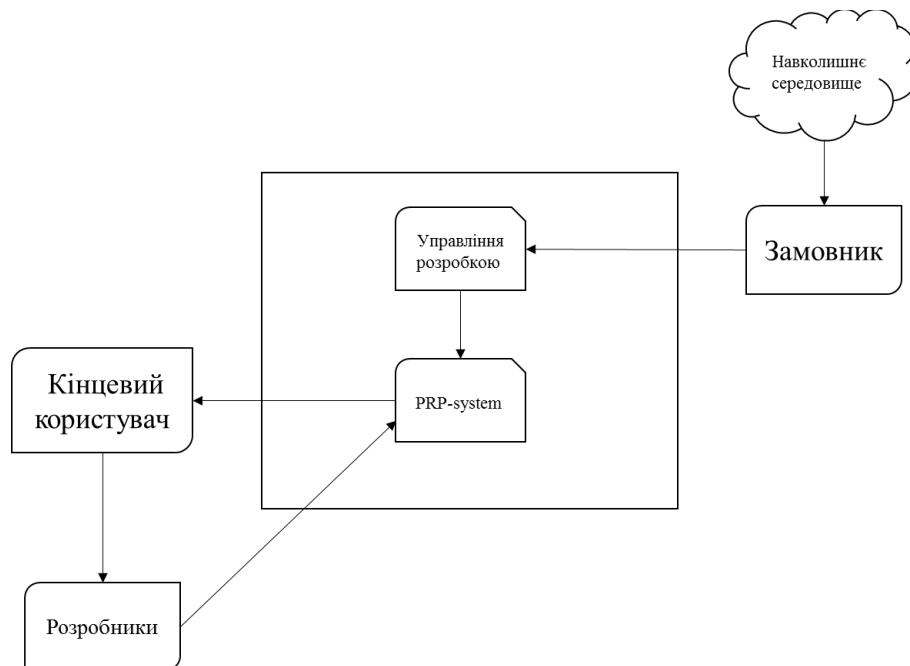


Рис. 5. Модель M2 ЕПЗ

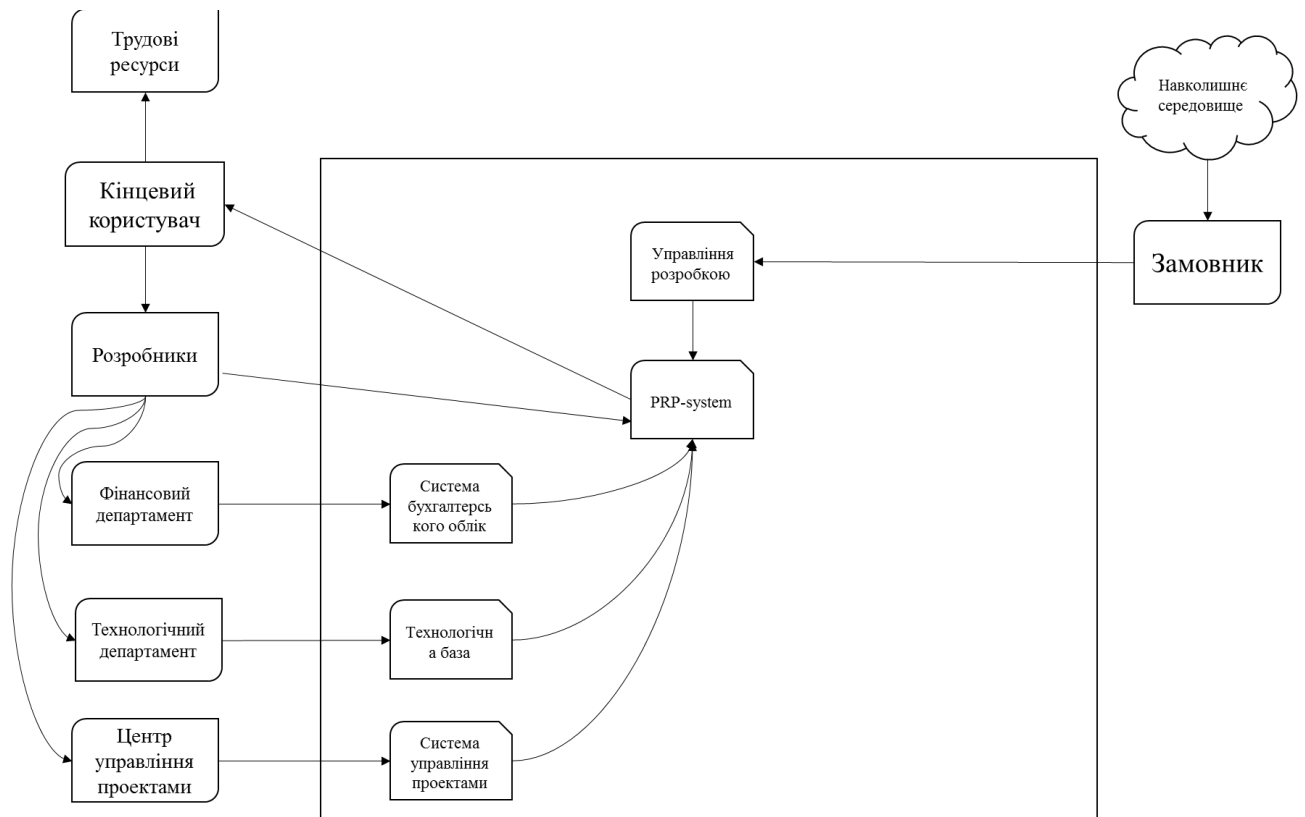


Рис. 6. Модель М3 ЕПЗ

Висновки

В статті запропоновано використання модельно-орієнтованого підходу MDA до моделювання ЕПЗ.

Такий підхід має ряд переваг: MDA надає загальне середовище для розробки ПЗ, що сприяє взаємодії груп розробників в процесі аналізу даних та перевірки системи; інженери можуть знайти та виправити помилки на ранніх стадіях проектування системи, коли час та фінансові наслідки зміни системи зводяться до мінімуму; MDA сприяє повторному використанню моделі для покращення системи та створення похідних систем з розширеними можливостями.

Ще однією з найважливіших задач в моделюванні ЕПЗ є задача оцінки стану ПЗ, його оточення та навколишнього середовища. Ця задача невідривна від процесів управління інформацією, яка в свою чергу використовується для прийняття раціональних рішень на всіх стадіях функціонування ЕПЗ. І MDA може забезпечити створення ЕПЗ на основі даних про інформаційну взаємодію між компонентами системи.

Отже, можна зробити висновки, що використання модельно-орієнтованого підходу найкраще підходить для моделювання ЕПЗ. Моделювання ЕПЗ потребує подальших досліджень. Для побудови адекватної моделі ЕПЗ необхідно спрогнозувати вплив ПЗ на навколишнє середовище і навпаки, а також розробити математичний апарат для моделювання ЕПЗ.

Список використаної літератури

1. Jansen, S. Understanding Software Ecosystems: A Strategic Modeling Approach [Text] / S. Jansen, J. Bosch // Proceedings of the Workshop on Software Ecosystems. – 2011. – P. 65 – 76.
2. Duinkerken, W. Transaction Cost Economics in Software Ecosystems [Text] / W. Duinkerken // Some empirical evidence. – 20 April 2009. – P. 22 – 37.
3. Dyba, T. Empirical studies on agile software development: A systematic review [Text] / T. Dyba, T. Dingsoyr // Information and Software Technology. – 2008. – Vol. 50, № 9 – 10. – P. 833 – 859. doi:10.1016/j.infsof.2008.01.006

4. Messershmitt, D. Ultra-Large-Scale Systems [Text] / D. Messershmitt, C. Szyperski // Understanding an Indispensable Technology and Industry. — London: MIT press, 2003. — 233 p.
5. Сидоров Н. А. Экология программного обеспечения [Текст] / Н. А. Сидоров // Инженерия программного обеспечения. – 2010. – № 1. – С. 53 – 61.
6. Хоменко В. А. Экосистемы программного обеспечения [Текст] / В. А. Хоменко // Вісник Національного технічного університету «ХПІ». – 2011. – № 23. – С. 114 – 118.
7. Луцький, М. Підтримка придатності та супроводження експлуатації програмного забезпечення авіаційної техніки [Текст] / М. Луцький, М. Сидоров, Ю. Рябокінь // Проблеми програмування. — 2010. — № 23. — С. 229–239.
8. Sidorov N. A. Software Ecosystems Modeling [Text] / N. A. Sidorov, O. O. Grinenko // Инженерия программного обеспечения. – 2013. – № 2(14). – Р. 38 – 48.
9. Грінченко О. О. Экосистема программного обеспечения как система систем [Текст] / О. О. Грінченко // Наукоємні технології. – 2014. – № 3 (23). – С. 280 – 283.
10. Томашевський В. М. Моделирование систем [Текст]: підручник / В. М. Томашевський. – Київ, 2005. – 349 с.
11. Boucharas, V. Formalizing software ecosystem modeling [Text] / V. Boucharas, S. Jansen, S. Brinkkemper // Proceedings of the 1st international workshop on Open component ecosystems. – 2004. – P. 41–50. doi:10.1145/1595800.1595807
12. Jansen, S. A sense of community: A research agenda on software ecosystems [Text] / S. Jansen, A. Finkelstein, S. Brinkkemper // 31th International Conference on Software Engineering, New and Emerging Research Track. – 2009. – P. 187 – 190. doi:10.1109/icse-companion.2009.5070978
13. Самарский А.А., Михайлов А.П. Математическое моделирование: Идеи. Методы. Примеры. – М.: Наука, 1997. – 320 с.
14. Аристов А.О. Теория квазиклеточных сетей: научная монография. – М: МИСиС, 2014. – 188 с.
15. Емельянов А.А., Власов Е.А., Дума Р.В. Имитационное моделирование экономических процессов: Учеб. пособие / Под ред. А.А. Емельянова. М.: Финансы и статистика, 2002. – 368 с.
16. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. – СПб.: БХВ-Петербург, 2005. – 400 с.
17. Кобелев Н.Б. Основы имитационного моделирования сложных экономических систем: Учеб. пособие. – М.: Дело, 2003. – 336 с.

Автори статті

Грінченко Олена Олександрівна – старший викладач кафедри інженерії програмного забезпечення, Навчально-науковий інститут комп'ютерних інформаційних технологій, Національний авіаційний університет, Київ, Україна. Тел. +380979125920. E-mail: Elena.Grinenko@livenau.net.

Грінченко Сергій Анатолійович – асистент кафедри інженерії програмного забезпечення, Навчально-науковий інститут комп'ютерних інформаційних технологій, Національний авіаційний університет, Київ, Україна. Тел. +380979710776. E-mail: SergGrinenko@gmail.com.

Authors of the article

Grinenko Olena Oleksandrivna – Senior Lecturer of Software Engineering Department, Scientific Research Institute of Computer Information Technologies, National Aviation University, Kyiv, Ukraine. Tel.: +380979125920. E-mail: Elena.Grinenko@livenau.net.

Grinenko Sergiy Anatoliyovich – assistant of Software Engineering Department, Scientific Research Institute of Computer Information Technologies, National Aviation University, Kyiv, Ukraine. Tel.: +380979125920. E-mail: SergGrinenko@gmail.com.

Дата надходження в редакцію: 11.01.2017 р.

Рецензент: д.т.н., проф. В.В. Вишнівський

УДК 519.873

Данік О.В.

СПОСІБ КОНТРОЛЮ РІВНЯ НАДІЙНОСТІ СУДНОВИХ КОМПЛЕКСІВ ПРИ НЕСТАБІЛЬНИХ УМОВАХ СПОСТЕРЕЖЕНЬ

Danik O.V. A method for controlling the level of reliability marine complex in unstable conditions of observation.

This article is provided for solving the problem of the reliability of statistical control units of automatic control of ship power plants according to chosen probabilistic model of the flow of failures in the form of composite Poisson distribution, taking into account the conditions of instability observations, and in accordance with the chosen method of statistical control, which procedures based on the use of testing statistical hypotheses. Use of statistical control technique to improve the reliability of possible statistical reliability control units.

Also, the article provides an analysis of the possible causes reduction in reliability, if necessary with the assistance of forces and facilities repair business. The analysis developed and carried out measures to improve or maintain the level of reliability (target performance reviews and audits, extraordinary performance of routine maintenance, carrying out improvements, etc.).

Keywords: statistical control, reliability, marine equipment

Данік О.В. Спосіб контролю рівня надійності суднових комплексів при нестабільних умовах спостережень.

У статті наведено вирішення задачі статистичного контролю рівня надійності суднових комплексів. Обґрунтовано імовірнісна модель потоку відмов у вигляді складового розподілу Пуассона, що враховує нестабільність умов спостережень. Імовірнісна модель у відповідності з обраним способом статистичного контролю, базується на використанні процедур перевірки статистичних гіпотез. Використання результатів статистичного контролю надійності дозволило удосконалити методику статистичного контролю надійності суднових комплексів.

Ключові слова: статистичний контроль, рівень надійності, суднове обладнання

Даник А.В. Способ контроля уровня надежности судовых комплексов при нестабильных условиях наблюдений.

В статье показано решение задачи статистического контроля уровня надежности судовых комплексов. Обоснован выбор вероятностной модели потока отказов в виде составного распределения Пуассона, которая учитывает нестабильность условий наблюдений. Вероятностная модель, в соответствии с выбранным способом статистического контроля, базируется на использовании процедур проверки статистических гипотез. Использование результатов статистического контроля надежности позволило усовершенствовать методику статистического контроля надежности судовых комплексов.

Ключевые слова: статистический контроль, уровень надежности, судовое оборудование

Вступ

У відповідності до обраного способу статистичного контролю рівня надійності, моделі потоку відмов сукупності однотипних агрегатів систем автоматичного управління суднових комплексів, статистичні гіпотези H_0 та H_1 формуються наступним чином:

- гіпотеза H_0 , яка полягає у тому, що при даному значенні фактичної кількості відмов n_{ϕ} агрегатів суднових комплексів j -го типу за i -й період експлуатації параметр n_{H_0} закону розподілу величини кількості відмов n дорівнює статистичній оцінці деякої заданої (очікуваної) кількості відмов $\hat{n}_3 > 0$ для даного контрольного періоду;
- гіпотеза H_1 , яка полягає у тому, що при даному значенні фактичної кількості відмов n_{ϕ} агрегатів j -го типу за i -й період експлуатації параметр n_{H_1} закону розподілу величини кількості відмов n перевищує $\hat{n}_3$ ($n_{H_1} > \hat{n}_3$, у загальному випадку $n_{H_1} \neq \hat{n}_3$) [1-5].

Виклад основного матеріалу дослідження

Статистика критерію правдоподібності Неймана – Пірсона для складового розподілу Пуассона має вигляд

$$W(n_\phi, \hat{n}_3, n_{H_1}) = \frac{P_{n_{(H_1)_i}} \{n \leq n_\phi\}}{P_{\hat{n}_{3_i}} \{n \leq n_\phi\}} =$$

$$= \frac{\sum_{n=0}^{n_\phi} \frac{n_{(H_1)_i}^n}{n!} \cdot e^{-n_{(H_1)_i}} \cdot \frac{1}{\sigma \sqrt{2\pi}} \sum_{n_{H_1}=0}^{n_{(H_1)_i}} n_{H_1} \cdot e^{-\frac{(n_{(H_1)_i} - \hat{n}_{3_0})^2}{2\sigma^2}}}{\sum_{n=0}^{n_\phi} \frac{\hat{n}_{3_i}^n}{n!} \cdot e^{-\hat{n}_{3_i}} \cdot \frac{1}{\sigma \sqrt{2\pi}} \sum_{\hat{n}_3=0}^{\hat{n}_{3_i}} \hat{n}_3 \cdot e^{-\frac{(\hat{n}_{3_i} - \hat{n}_{3_0})^2}{2\sigma^2}}}, \quad (1)$$

де $n_{(H_1)_i}$ - значення параметру закону розподілу величини кількості відмов n для i -го періоду експлуатації, яке відповідає гіпотезі H_1 . Для визначення величини $\hat{n}_{3_i}$, яка є функцією статистичної оцінки заданого (очікуваного) значення параметра потоку відмов $\hat{z}_{3_i}$ однотипних виробів, слід використовувати значення $\hat{z}_{3_i}$, отримані за результатами прогнозування, якщо часовий ряд значень статистичної оцінки фактичного значення параметра потоку відмов $\hat{z}_\phi$ є нестационарним. За умови стаціонарності часового ряду $\hat{z}_\phi$ величину $\hat{z}_{3_i}$ можна визначати як середнє значення за результатами спостережень протягом попередніх періодів експлуатації [2-6].

Умовами прийняття гіпотез H_1 або H_0 є виконання відповідних нерівностей:

$$W(n_\phi, \hat{n}_3, n_{H_1}) = \frac{P_{n_{(H_1)_i}} \{n \leq n_\phi\}}{P_{\hat{n}_{3_i}} \{n \leq n_\phi\}} \geq A, \quad (2)$$

$$W(n_\phi, \hat{n}_3, n_{H_1}) = \frac{P_{n_{(H_1)_i}} \{n \leq n_\phi\}}{P_{\hat{n}_{3_i}} \{n \leq n_\phi\}} \leq B, \quad (3)$$

$$\text{де } A \geq \frac{1-\beta}{\alpha}, \quad B \leq \frac{\beta}{1-\alpha}.$$

Для прийняття рішення за результатами перевірки гіпотез необхідно визначити критичну область значень статистики критерію (1). Критична область значень статистики критерію визначається величинами α і β . У загальному випадку величини α і β , що визначають відповідно рівень значимості та функцію потужності критерію, можуть бути задані довільно. Але, максимальна вірогідність прийняття або відхилення однієї з конкуруючих гіпотез відповідає мінімальним значенням α і β . Оскільки функція (1) залежить від отриманих статистичних даних n_ϕ , параметру n_{H_1} та умов спостережень $\hat{n}_{3_i}$ (обсягу вибірки, сумарного наробітку виробів t_Σ за контрольний період), то і мінімальні значення α і β будуть визначатися областю можливих значень функції (1) при даних умовах спостережень і отриманих статистичних даних. В цьому випадку задача зводиться до пошуку екстремумів статистики критерію Неймана - Пірсона для конкретних умов спостережень [5-7]:

$$\hat{n}_3 \in \Omega_{\hat{n}_3}, n_\phi \in \Omega_{n_\phi}, n_{H_1} \in \Omega_{n_{H_1}},$$

$$W(\hat{n}_3, n_\phi, n_{H_1}) \rightarrow \max_{n_{H_1}}, \quad W(\hat{n}_3, n_\phi, n_{H_1}) \rightarrow \min_{n_{H_1}}, \quad (4)$$

та визначення відповідних величин $\alpha_{min} = f(W_{max}, W_{min})$, $\beta_{min} = f(W_{max}, W_{min})$.

Для статистичних даних про відмови та несправності блоку логіки системи контролю у період експлуатації з 2010 року по 2016 рік були розраховані значення статистики критерію Неймана-Пірсона у залежності від величин n_ϕ , n_{H_1} при різних умовах спостережень $\hat{n}_{3_i}$ (рис. 1, 2).

З графіків видно, що кожній парі значень n_ϕ , $\hat{n}_{3_i}$ відповідає максимальне значення критерію, яке визначається параметром n_{H_1} . Це максимальне значення визначає верхню межу для величини $A \geq \frac{1-\beta}{\alpha}$. Аналіз виразу (1) свідчить, що мінімальне значення критерію досягається при $n_{H_1} \rightarrow \infty$. Але, як видно з графіків, при $n_{H_1} > 6$ зменшення функції (1) значно уповільнюється і функція (1) приймає значення у межах 0,1...0,4 при $n_{H_1}=7$ для різних n_ϕ .

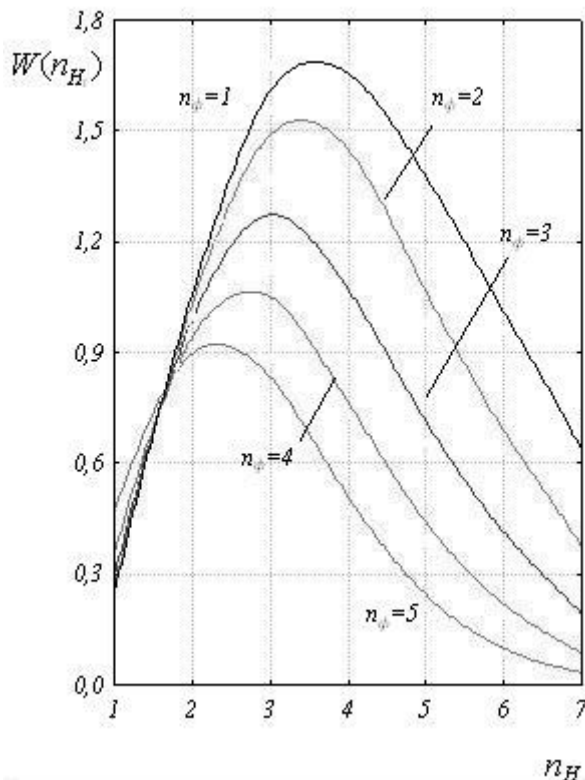


Рис. 1. Залежність величини статистики $W(n_{H_1})$ від параметру n_{H_1} при $\hat{n}_{3_i} = 2$

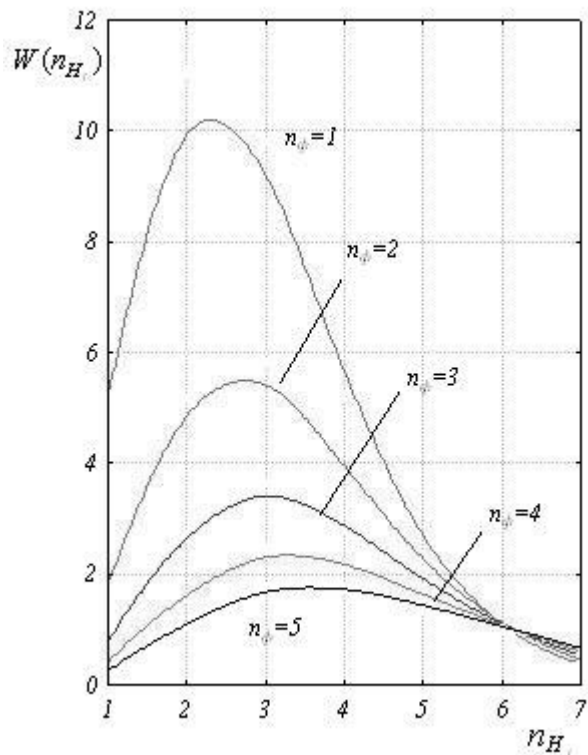


Рис. 2. Залежність величини статистики $W(n_{H_1})$ від параметру n_{H_1} при $\hat{n}_{3_i} = 6$

Тому, доцільно в якості мінімального значення статистики критерію (W_{min}) прийняти значення, що відповідає $n_{H_1}=7$. Це мінімальне значення критерію визначає нижню межу для

величини $B \leq \frac{\beta}{1-\alpha}$. Таким чином, для кожної пари значень n_ϕ , $\hat{n}_{3_i}$ можна знайти два значення параметру $(n_{H_1})_1$, $(n_{H_1})_2$, що визначають максимальне (W_{max}) і мінімальне (W_{min}) значення статистики критерію Неймана-Пірсона і, відповідно, верхню та нижню межі для величин A і B [5-8]. Тоді, з використанням отриманих значень A і B можна вирішити систему нерівностей відносно α і β :

$$\begin{cases} A \geq \frac{1-\beta}{\alpha}, \\ B \leq \frac{\beta}{1-\alpha}. \end{cases} \quad (5)$$

Результати вирішення системи (5) можна представити у графічному вигляді (рис. 3, 4). З графіків видно, що кожній парі значень A, B відповідають значення α_{min} і β_{min} . При $A=\text{const}$ і $B \downarrow \rightarrow \alpha_{min} \uparrow$, але $\beta_{min} \downarrow$. І навпаки, при $B=\text{const}$ і $A \uparrow \rightarrow \alpha_{min} \downarrow$, але $\beta_{min} \uparrow$.

Результати вирішення системи нерівностей (5) відносно α і β при відповідних значеннях $n_\phi, \hat{n}_3, n_{H_1}$ дозволили побудувати графіки залежностей $\alpha_{min}(\hat{n}_3), \beta_{min}(\hat{n}_3)$, що відповідають отриманим значенням параметру n_{H_1} для різних значень n_ϕ (рис. 3, 4).

Значення параметру n_{H_1} , що підлягають порівнянню з $\hat{n}_3$ при перевірці гіпотез H_0 та H_1 при різних значеннях n_ϕ , наведені у таблиці 1.

Таблиця 1. Значення параметру n_{H_1} для порівняння з $\hat{n}_3$ при перевірці гіпотез H_0 та H_1 при різних значеннях n_ϕ

$n_\phi = 1$		$n_\phi = 2$		$n_\phi = 3$		$n_\phi = 4$		$n_\phi = 5$	
$\hat{n}_3$	n_{H_1}	$\hat{n}_3$	n_{H_1}	$\hat{n}_3$	n_{H_1}	$\hat{n}_3$	n_{H_1}	$\hat{n}_3$	n_{H_1}
1,0	2,0	1,0	3,0	1,0	3,0	1,0	3,0	1,0	3,0
2,0	3,0	2,0	3,0	2,0	3,0	2,0	3,0	2,0	3,0
3,0	2,0	3,0	2,0	3,0	4,0	3,0	4,0	3,0	4,0
4,0	2,0	4,0	3,0	4,0	3,0	4,0	3,0	4,0	3,0
5,0	2,0	5,0	3,0	5,0	3,0	5,0	3,0	5,0	3,0
6,0	2,0	6,0	3,0	6,0	3,0	6,0	3,0	6,0	3,0

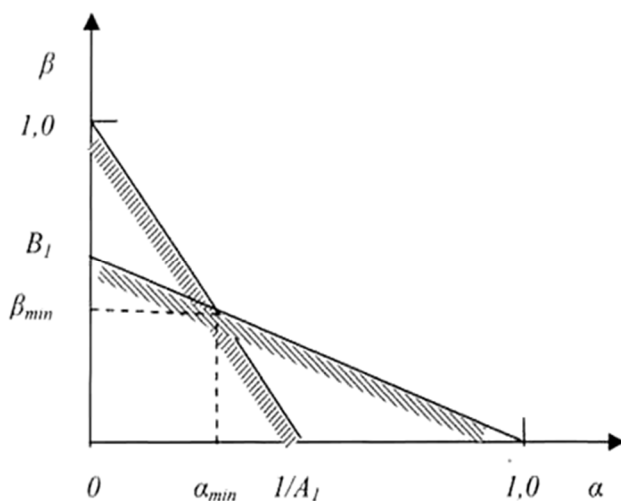


Рис. 3. Результати вирішення системи (5) при A_1, B_1 .

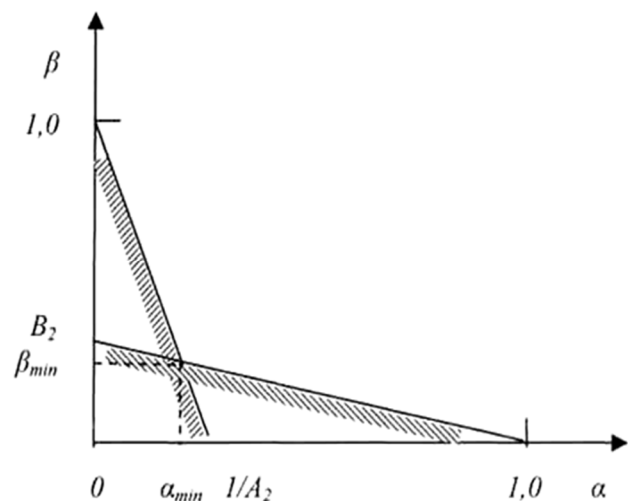


Рис. 4. Результати вирішення системи (5) при $A_1 < A_2, B_1 > B_2$.

Висновки

При виконанні умови $n_{H_1} > \hat{n}_{3(i+1)j}$ необхідно перевірити можливість прийняття гіпотези H_1 , а саме:

- порівняти мінімальні значення ймовірностей помилок першого роду (α_{min}) та другого роду (β_{min}) для $n_{\Phi(i+1)j} = 3$, та $\hat{n}_{3(i+1)j} = 3$;
- якщо $\alpha_{min} > \beta_{min}$, це свідчить на користь гіпотези H_1 . Для нашого прикладу $\alpha_{min} \approx 0,99$, $\beta_{min} \approx 0,01$. Це означає, що з достатньо високою ймовірністю може бути прийнята гіпотеза H_1 ;
- при конкретному значенні n_{Φ} за контрольний період експлуатації фактичний рівень надійності, що характеризується параметром n_{H_1} , нижче заданого, що відповідає умові $n_{H_1} > \hat{n}_{3(i+1)j}$.

У цьому випадку необхідно провести аналіз можливих причин зниження рівня надійності, при необхідності з залученням сил та засобів ремонтного підприємства. За результатами аналізу розробляються та проводяться заходи з підвищення або підтримання рівня надійності (виконання цільових оглядів та перевірок, позачергове виконання регламентних робіт, проведення доробок тощо).

Якщо $\alpha_{min} < \beta_{min}$, це свідчить на користь гіпотези H_0 : при конкретному значенні n_{Φ} за контрольний період експлуатації фактичний рівень надійності, що характеризується параметром n_{H_1} , дорівнює заданому, що відповідає умові $n_{H_1} = \hat{n}_{3(i+1)j}$.

Прийняття гіпотези H_0 є підставою для продовження експлуатації суднових комплексів даного типу.

Список використаної літератури

1. Рабочая книга по прогнозированию / [Араб-Оглы Э.А., Бестужев-Лада И.В., Гаврилов Н.Ф. и др.]; под ред. И.В. Бестужева-Лады. – М.: Мысль, 1982. – 430 с.
2. Хеннан Э. Многомерные временные ряды / Э. Дж. Хеннан; пер. с англ. А.С. Холево. – М.: “Мир”, 1974. – 576 с.
3. Андерсон Т. Статистический анализ временных рядов / Т. Андерсон; пер. с англ. И.Г. Журбенко и В.П. Носко. – М.: “Мир”, 1976. – 756 с.
4. Гаскаров Д.В. Прогнозирование технического состояния и надежности радиоэлектронной аппаратуры / Гаскаров Д.В., Голинкевич Т.А., Мозгалевский А.В. // Советское радио, 1974. – 224 с.
5. Навігаційне забезпечення управління рухом суден (навчальний посібник) / [Богом'я В.І., Давидов В.С., Доронін В.В., Пашков Д.П., Тихонов І.В.]. – Вид.1-е. – К.: ДВВП «Компас», 2012 – 336 с.
6. Гудков Д.Н. Системы динамического позиционирования судов как эргатический инструмент повышения безопасности мореплавания / Д.Н. Гудков, И.В. Тихонов // Системы обработки інформації. – 2013. – Вип. 8 (115). – С. 32–36.
7. Тюрин Ю.П., Макаров А.А. Анализ данных на компьютере / Ю.П. Тюрин, А.А. Макаров. – М.: “Инфра-М”, 2003. – 544 с.
8. Боровиков В. STATISTICA. Искусство анализа данных на компьютере: для профессионалов / Боровиков В. – СПб.: Питер, 2003. – 688 с.

Автори статті

Данік Олексій Володимирович – старший викладач, Київська державна академія водного транспорту, Київ, Україна. Тел. +38 050 398 47 96. E-mail: bog2603@mail.ru

Authors of the article

Danik Oleksij Volodymyrovych – senior lecturer, Kyiv State Academy of Water Transport, Kyiv, Ukraine. Tel.: +38 050 398 47 96. E-mail: bog2603@mail.ru

Дата надходження в редакцію: 05.02.2017 р.

Рецензент: д.т.н., проф. В.І. Богом'я

Захариудакис Лефтериос, аспирант

МЕТОД БЫСТРОЙ АУТЕНТИФИКАЦИИ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ КОНЦЕПЦИИ “НУЛЕВЫХ ЗНАНИЙ”

Zacharioudakis Eleftherios. Method for high speed remote user authentication based on zero-knowledge conception.

The method for high speed remote abonent authentication has been proposed. Proposed method realized the progressive zero-knowledge conception of cryptographically strong authentication. From mathematical point of view developed method is based on Boolean irreversible transformation in contradistinction to known method which realized zero-knowledge conception utilized the function transformation based on modular arithmetic. The Boolean irreversible transformation in proposed method are implemented by using of standard irreversible hash transformation. Such solution provides a high degree of security against to attacks.

The procedures for remote user registration and authentication cycle were developed in detail. The evaluation of the effectiveness of the proposed method compared to the existing systems of realizing progressive zero-knowledge conception remote abonent authentication of the multi-user system was made. It has been shown that utilization of proposed authentication technology allowed to increase the identification rate by 2-3 orders.

Key words: remote abonent authentication, interactive authentication, strong authentication methods, zero-knowledge authentication conception, hash algorithms.

Захаріудакіс Лефтеріос. Метод швидкої автентифікації віддалених користувачів на основі концепції “нульових знань”.

Запропоновано метод прискореної автентифікації віддалених абонентів багатокористувацьких систем на основі криптографічно строгої концепції “нульових знань”. На відміну від відомих методів реалізації вказаної концепції, що мають за основу модулярну арифметику, запропоноване рішення базується на використанні незворотних булевих перетворень, що реалізовані за допомогою стандартизованих хеш-перетворень. Це забезпечує високий рівень стійкості до атак, а також значне спрощення обчислювальних процедур. Проведена теоретична та експериментальна оцінка ефективності довела, що запропонований метод забезпечує підвищення швидкості автентифікації на 2-3 порядки в порівнянні з відомими методами.

Ключові слова: автентифікація віддалених користувачів, інтерактивна автентифікація, строга автентифікація, концепція автентифікації “нульових знань”, хеш-алгоритми.

Захариудакис Лефтериос. Метод быстрой аутентификации удаленных пользователей на основе концепции “нулевых знаний”.

Метод быстрой аутентификации удаленных пользователей на основе концепции “нулевых знаний”. Предложен метод ускоренной аутентификации удаленных абонентов многопользовательских систем на основе криптографически строгой концепции “нулевых знаний”. В отличии от известных методов реализации указанной концепции, которые основываются на модулярной арифметике, предложенное решение базируется на использовании необратимых булевых преобразований, которые реализованы с помощью стандартизованных хеш-преобразований. Это обеспечивает высокий уровень устойчивости к атакам, а также значительное упрощение вычислительных процедур. Проведенная теоретическая и экспериментальная оценка эффективности показала, что предложенный метод обеспечивает ускорение аутентификации на 2-3 порядка по сравнению с известными методами.

Ключевые слова: аутентификация удаленных пользователей, интерактивная аутентификация, концепция аутентификации “нулевых знаний”, хеш-алгоритмы.

Вступление

Постановка задачи. Появление компьютерных сетей означает формирование информационного пространства как нового явления, которое перевело жизнь человечества в новое качественное состояние. Разрешив наметившуюся к концу прошлого века проблему “информационного бума”, сетевые технологии открыли принципиально новые возможности доступа к данным. Явление глобальной информационной интеграции стало в значительной мере определять прогресс человечества во всех сферах его деятельности.

Оборотной стороной информационной интеграции является настоятельная необходимость в контроле за ее распространением. Значительная часть представляющих практический интерес информационных продуктов является результатом трудоемких исследований и разработок, то есть представляет собой товарный продукт, распространение которого требует возмещения затрат на его создание. Ограничения на использование другого широкого класса информационных ресурсов обусловлены их конфиденциальным характером. Вместе с тем, доступ к этим информационным ресурсам в рамках информационной интеграции должен быть обеспечен легализованным пользователям. Соответственно, возникает задача аутентификации пользователей.

В современных условиях задача аутентификации имеет тенденцию к усложнению, что обусловлено динамичным ростом количества пользователей и расширением технических возможностей для реализации несанкционированного доступа к информационным ресурсам. Это требует адекватного совершенствования методов и средств аутентификации удаленных пользователей, как в плане снижения риска незаконного доступа к информации, так и в плане повышения скорости аутентификации.

С этих позиций повышение эффективности аутентификации удаленных пользователей интегрированных систем представляется актуальной и практически важной для современного этапа развития компьютерных технологий.

Анализ литературных источников. Основным требованием к системам аутентификации удаленных пользователей интегрированных систем обработки информации является обеспечение практической невозможности:

- доступа к ресурсам системы несанкционированным пользователям.
- имитации системой обращения к ней абонента;
- имитации предоставления пользователю ресурсов заинтересованной стороной.

Исходя из анализа методов незаконного получения злоумышленниками доступа к ресурсам многопользовательских систем можно сформулировать следующие требования к системам аутентификации удаленных пользователей:

- при передаче идентификационной информации от пользователя к системе и обратно она должна изменяться от сеанса к сеансу с тем, чтобы не позволить реализовать несанкционированный доступ путем перехвата и повторного использования такой информации злоумышленником;

- аутентификация пользователей должна выполняться, исходя из наличия у них идентифицирующей информации, которая не должна передаваться по линиям связи и которая должна однозначно определять объем информационных ресурсов, доступных пользователю;

- в системе не должно храниться информация, позволяющая реконструировать в полном объеме идентификационную информацию пользователя с тем, чтобы система не могла имитировать обращения к ней со стороны пользователя или незаконное проникновение в систему (с использованием вирусов) не открывало возможностей получения доступа к ресурсам системы под видом и за счет пользователя;

- система аутентификации удаленных абонентов, являясь системой массового обслуживания, должна обеспечивать высокую скорость реализации процесса идентификации пользователей.

В литературе [1] методы идентификации, удовлетворяющие первым трем из приведенных требований называют “строгими”, в противовес остальным, которые называются “слабыми”. К классу “строгих” процедур относятся, большей частью, методы аутентификации, в основе которых лежит концепция “нулевых знаний”. Суть этой концепции состоит в том, что:

- пользователь единолично обладает математической процедурой генерации “правильных” паролей, которые меняются при каждом обращении к системе;

- система обладает математической процедурой, которая позволяет проверить правильность пароля пользователя, но не сама не может сгенерировать “правильный” пароль.

К классу “слабых” процедур аутентификации относится, например, процедура аутентификации пользователей, используемая в операционной системе UNIX [1]. Эта процедура предусматривает сохранение в системе только хеш-образов паролей пользователей, что, при использовании необратимых хеш-преобразований, исключает возможность воспроизведение пароля системой; однако сами пароли не меняются, что позволяет достаточно просто их перехватить.

Наиболее известным из протоколов аутентификации, реализующих прогрессивную концепцию “нулевых знаний” является метод FFSIS (Feige Fiat Shamir Identification Scheme) [2]. FESIS представляет собой относительно простую и вместе с тем достаточно эффективную схему аутентификации абонентов многопользовательских систем, на основе которой создано ряд имеющих практическое значение модификаций. Базовой вычислительной операцией метода является модулярное возведение в квадрат чисел, разрядностью 2048-4096. В плане практического использования основным недостатком FFSIS считается:

- необходимость в большом числе обменов данными между пользователем и системой, что заметно нагружает линии передач и замедляет процесс аутентификации;
- большая вычислительная сложность операции модулярного возведения в квадрат, выполняемой над числами, разрядность которых значительно превышает разрядность процессора.

Другие схемы идентификации, реализующие концепцию “нулевых знаний” с использованием модулярной арифметики, предложенные в [3] требуют существенно меньшего объема пересылок, но предусмотренные ими процедуры имеют большую вычислительную сложность, поскольку вместо операции возведения в квадрат, в них используются операции модулярного экспоненцирования.

В работе [4] предложена система, реализующая идентификацию удаленных пользователей на основе концепции “нулевых знаний” с использованием многозначных необратимых булевых функциональных преобразований. Эта схема позволяет ускорить процесс аутентификации пользователей за 2-3 порядка по сравнению с методами, основанными на модулярной арифметике больших чисел. Однако, рассматриваемая система имеет следующие недостатки:

- процедура генерации неоднозначных необратимых преобразований достаточно сложная и ее реализации требует значительных вычислительных ресурсов;
- хранение таблиц нелинейных булевых преобразований от большого числа переменных требует для каждого из многих тысяч пользователей системы требует больших объемов памяти;
- устойчивость системы к различным видам взломам не достаточно изучена и доказана. В частности, остается открытым вопрос об устойчивости предложенных булевых преобразований к методам дифференциального анализа.

Нерешенные вопросы. Проведенный анализ литературных источников позволяет сделать следующие выводы: расширение использования распределенных систем хранения и обработки данных а также “облачных технологий” требует повышения эффективности аутентификации удаленных пользователей как в плане обеспечения высокого уровня защищенности удаленных ресурсов от незаконного доступа, так и в плане повышения скорости выполнения соответствующих процедур. Наиболее высокий уровень защиты обеспечивают протоколы аутентификации, в основе которых лежит теоретическая концепция “нулевых знаний”. Существующие методы аутентификации, реализующие эту прогрессивную концепцию не обеспечивают высокой скорости выполнения процедуры аутентификации в силу того, что используют мультипликативные операции модулярной арифметики, имеющие высокую вычислительную сложность.

Цель и задачи исследования. Целью исследований является повышение эффективности аутентификации удаленных пользователей за счет сокращения времени выполнения

соответствующих вычислительных процедур при сохранении высокого уровня защищенности.

Для достижения поставленной цели в работе решаются такие задачи:

- разработка метода аутентификации удаленных пользователей, реализующего теоретическую концепцию нулевых знаний на основе использования стандартизированных криптографических примитивов;
- теоретическое и экспериментальное исследование эффективности разработанного метода как в плане достигаемого уровня защищенности так и в плане скорости реализации вычислительных процедур, связанных с реализацией аутентификации.

1. Метод ускоренной аутентификации

Поставленная цель – радикальное ускорение вычислительной реализации аутентификации, основанной на концепции “нулевых знаний” может быть достигнута за счет применения в качестве базового криптографического преобразования необратимых булевых функций вместо модулярного экспоненцирования. Теоретически считается принятым [1], что в основе любого криптографического механизма лежит математическое необратимое преобразование, то есть преобразование, для которого определено аналитически прямое преобразование, но из которого аналитическим путем принципиально не может быть получено обратное преобразование. На практике криптографической защиты данных в качестве необратимых математических преобразований чаще всего модулярное экспоненцирование (алгоритмы RSA, DSA), операции на эллиптических кривых (алгоритмы ECC) или нелинейные булевы преобразования, которые являются базовыми для построения всех алгоритмов симметричного шифрования (алгоритмы AES и Rijndael в частности), а также все хеш-алгоритмы (SHA-1 и Ripemd-160). Известно, что основным достоинством использования в качестве необратимых преобразований нелинейных булевых функций по сравнению с операциями модулярного экспоненцирования является высокая скорость вычислительной реализации. Так, применительно к задачам шифрования принято считать, что при примерно равном уровне защищенности, алгоритмы симметричного шифрования типа Rijndael обеспечивают на 3 порядка большую скорость по сравнению с алгоритмом шифрования с открытым ключом - Rijndael [5].

Таким образом, использование криптографических механизмов, в основе которых лежат булевы преобразования, для реализации прогрессивной концепции “нулевых знаний” применительно к аутентификации пользователей потенциально позволяет существенно уменьшить время аутентификации.

Для практической реализации указанной возможности предлагается метод аутентификации удаленных пользователей, который реализует концепцию “нулевых знаний” с использованием стандартизированных криптографических примитивов – хеш-алгоритмов. Хеш-алгоритм осуществляет необратимое преобразование сообщения произвольной длины в код хеш-сигнатуры фиксированной длины. Основное свойство хеш-алгоритмов состоит в их необратимости, то есть в том, что нахождение двух разных сообщений с одинаковой хеш-сигнатурой представляется практически невозможным. Хеш-алгоритмы, прошедшие тщательное и всестороннее тестирование, дополненное опытом практического использования получают статус стандарта, необратимость которого гарантируется соответствующими государственными органами. Наиболее известными стандартизированными хеш-алгоритмами являются SHA-1, MD-5 и Ripemd-160 [1].

Предлагаемый метод включает в себя процедуры регистрации пользователя и непосредственно аутентификации.

Процедура регистрации пользователя состоит из следующей последовательности действий:

- 1) Пользователем определяется число n предполагаемых циклов обращения к системе, выбирает иницилирующую символьную строку S , случайным образом формируется маскирующая строка Z .

2) Пользователем вычисляется код $p_n = H(S||n)$, где $||$ - операция конкатенации, H -хеш-преобразование, регламентируемое одним из стандартизированных хеш-алгоритмов.

3) Рекуррентно осуществляется вычисление n кодов сеансовых паролей $p_{n-1}, p_{n-2}, \dots, p_1, p_0$ в соответствии со следующей формулой:

$$\forall j \in \{0, 1, \dots, n-1\} : p_j = H(p_{j+1} || j). \quad (1)$$

4) Коды сеансовых паролей $p_{n-1}, p_{n-2}, \dots, p_1, p_0$ сохраняются в закрытой от постороннего вмешательства памяти пользователя.

5) Пользователем генерируется случайным образом ключ Θ симметричного блочного шифра.

6) Системой сообщается пользователю общедоступный закрывающий системный ключ K_3 . Этот ключ используется системой на этапе регистрации пользователей как составная часть несимметричного шифра типа RSA. Открывающий ключ K_0 этого шифра содержится системой в секрете.

7) С использованием закрывающего ключа K_3 системы, пользователем шифруются код p_0 , сгенерированный ключ Θ и маскирующая строка Z : $C_1 = \text{НСШ}(p_0, K_3)$, $C_2 = \text{НСШ}(\Theta, K_3)$, $C_3 = \text{НСШ}(Z, K_3)$, где через аббревиатуру $\text{НСШ}(x, y)$ обозначено несимметричное шифрование (например с использованием алгоритма RSA) сообщения x ключом y . Полученные коды C_1 , C_2 и C_3 пересылаются системе.

8) Система с использованием секретного открывающего ключа K_0 производит расшифровку полученных кодов: $p_0 = \text{НСДШ}(C_1, K_0)$ и $\Theta = \text{НСДШ}(C_2, K_0)$, $Z = \text{НСДШ}(C_3, K_0)$ где аббревиатурой $\text{НСДШ}(x, y)$ обозначено несимметричное дешифрование закодированной посылки x ключом y . Восстановленные коды p_0 , Z и Θ сохраняются системой в защищенной памяти вместе с номером η последнего сеанса ($\eta=0$). Значение p_0 сохраняется в виде переменной λ : $\lambda = p_0$.

Выполнение j -го цикла аутентификации, $j \in \{1, 2, \dots, n\}$ сводится к следующей последовательности действий:

1) Пользователем выбирается из защищенной памяти код j -того сеансового пароля p_j . С использованием ключа Θ шифруется конкатенация p_j сеансового пароля и номера j сеанса обращения пользователя к системе: $U_j = \text{СШ}(p_j || j, \Theta)$, где аббревиатурой $\text{СШ}(x, y)$ обозначено симметричное шифрование сообщения x ключом y .

2) Зашифрованный сеансовый пароль U_j посылается пользователем системе.

3) Системой с использованием ключа Θ производится дешифрование сеансового пароля U_j , восстанавливая пересланные ей пользователем значения p_j и j : $p_j || j = \text{СДШ}(U_j, \Theta)$, где аббревиатурой $\text{СДШ}(x, y)$ обозначено симметричное дешифрование закодированной посылки x ключом y .

4) Системой производится контроль синхронизации сеансов аутентификации путем сравнения кодов j и η . Если $j = \eta + 1$, то сеансы пользователя и системы синхронизированы и выполняется переход на п.5. Если $j > \eta + 1$, то нарушение синхронизации состоит в том, что система не восприняла предыдущие сеансы аутентификации со стороны пользователя. В этом случае система посылает соответствующее сообщение пользователю, зашифрованное ключом Θ . Получение такого сообщения означает что имела место имитации системы заинтересованной стороной. Для восстановления синхронизации пользователь выполняет $j - \eta - 1$ пустых циклов аутентификации начиная с $(\eta + 1)$ -го цикла. Если $j < \eta + 1$, то нарушение синхронизации означает, что к системе были обращения заинтересованной стороны от имени пользователя или что система сама делала попытки имитации обращения к ней со стороны пользователя, имея ввиду определенный коммерческий интерес. В этом случае система посылает соответствующее сообщение пользователю, зашифрованное ключом Θ . Для восстановления синхронизации система устанавливает значение $\eta = j - 1$ и актуализирует соответствующее значение $\lambda = p_{\eta-1}$.

5) Системой выполняется хеш-преобразование $r = H(p_j \parallel j)$ и полученный результат сравнивается с хранящимся в системе значением λ . Если $r = \lambda$, то идентификация пользователя произведена успешно и ему предоставляются соответствующие права доступа к ресурсам системы. При этом, системой сохраняется в переменной λ значение p_j , а в переменной η значение j : $\lambda = p_j$ и $\eta = j$.

6) Системой выполняется хеш-преобразование $r_j = H(p_j \parallel Z)$ и полученный код пересылается пользователю.

7) Пользователь, по получении от системы кода r_j производит хеш-преобразование $d = H(p_j \parallel Z)$. Если $d = r_j$, то считается подтвержденным, что пользователь действительно работает с системой.

2. Анализ эффективности

2.1 Анализ криптостойкости. Важнейшим фактором эффективности предложенного метода аутентификации удаленных пользователей, реализующего криптографически строгую концепцию “нулевых знаний” является оценка уровня защищенности от попыток получить несанкционированный доступ к ресурсам системы.

Повторное использование передаваемого по каналу зашифрованного сеансового пароля U_j на j -том сеансе полностью исключается тем, что сам сеансовый пароль меняется в каждом сеансе.

Если сторона, осуществляющая нарушение защиты имеет доступ к информации, передаваемой по открытому каналу, то при отслеживании h сеансов в ее распоряжении могут оказаться h кодов: $U_1, U_2, \dots, U_h$ и h хеш-сигнатур $r_1, r_2, \dots, r_h$. Каждый из кодов $U_1, U_2, \dots, U_h$ представляет собой шифротекст соответствующего из сеансовых паролей $p_1, p_2, \dots, p_h$, зашифрованных неизвестным ключом Θ . Единственным рациональным вариантом действий злоумышленника является перебор всех возможных ключей Θ , дешифрация наблюдаемых кодов с получением кодов $\zeta_1, \zeta_2, \dots, \zeta_h$. Если $\zeta_1 = H(\zeta_2 \parallel 2)$, $\zeta_2 = H(\zeta_3 \parallel 3)$, ..., $\zeta_{h-1} = H(\zeta_h \parallel h)$, то ключ Θ подобран правильно. Подбор ключа симметричного алгоритма шифрования представляет собой ресурсоемкую задачу, поскольку объем перебора составляет 2^l , где l – разрядность ключа. При типовом для настоящего времени значении $l = 256$ объем перебора 2^{256} требует предельно больших ресурсов. Но даже восстановив перебором код ключа Θ , злоумышленник не имеет возможности сгенерировать корректный сеансовый пароль в силу того, что, согласно (1), последний перехваченный им сеансовый пароль является результатом необратимого преобразования над следующим сеансовым паролем. Это означает, что для восстановления текущего пароля злоумышленнику придется каждый раз выполнять процедуру нахождения кода, хеш-сигнатура которой совпадает с последним использованным паролем. При использовании стандартизированных хеш-алгоритмов эта процедура считается практически невыполнимой. Таким образом, предложенный метод обеспечивает фактически двойную защиту сеансового пароля пользователя от стороннего злоумышленника.

Со стороны самой системы практически исключается возможность имитации обращения к ней пользователя, поскольку каждый следующий сеансовый пароль известен только пользователю. Система знает только предыдущий сеансовый пароль и для получения следующего ей необходимо выполнить обратное хеш-преобразование, что при использовании стандартизированных хеш-алгоритмов считается практически невыполнимым. По той же причине информации, хранящейся в системе недостаточно для получения следующего сеансового пароля пользователя. Поэтому проникновение к информации, хранящейся в системе с использованием вирусных атак или недобросовестного персонала не позволит получить данные, достаточные для обращения к системе от лица пользователя. Это обеспечивает надежную защиту от несанкционированного доступа с правами и за счет пользователя используя информацию самой системы.

Важным достоинством предложенного метода является его ориентация на использование стандартизированных, тщательно оттестированных и хорошо проверенных практикой криптографических механизмов – стандартизированных шифроблоков и хеш-алгоритмов.

2.2. Оценка производительности реализации функций аутентификации.

Основным преимуществом предложенного метода реализации концепции криптографически строгой аутентификации “нулевых знаний” является повышение скорости выполнения вычислительных процедур.

Предложенный метод в вычислительном плане требует выполнения одной процедуры шифрования и двух операций вычисления хеш-сигнатуры. Если считать, что для шифрования используется современный алгоритм Rijndael с размером блока данных 256, то время выполнения процедуры шифрования можно оценить следующим образом. Алгоритм выполняет 14 циклов. В каждом цикле выполняется: 256 операций замены (время выполнения $256 \cdot t_L$, где t_L – время выполнения процессором логической операции), 24 операций сдвига, 24 операций логического сложения. Таким образом, общее число логических команд и операций замены, необходимых для выполнения 14-ти циклов алгоритма Rijndael составляет 4256, время их выполнения примерно равно $4256 \cdot t_L$. Учитывая, что логические операции в современных процессорах выполняются за один такт [6], можно, в оценочном плане, говорить о том, что алгоритм Rijndael может быть реализован за 4256 тактов.

Хеш-алгоритм SHA-1 состоит из 80-ти циклов, причем на первых 20-ти циклах выполняется 10 логических операций, на вторых и последних 20 циклах – 9 логических операций, а на третьей двадцатке циклов – 11 логических операций. Таким образом, суммарное количество логических операций равно 780. Учитывая, что логическая операция выполняется за один такт, можно считать, что хеш-алгоритм SHA-1 требует для своей реализации 780 тактов работы процессора. Общее число тактов работы процессора, требующееся для реализации предложенного метода аутентификации в оценочном плане определяется как $4256 + 2 \cdot 780 \approx 5800$.

Методом FFSIS процедура аутентификации предусматривает 20 циклов обмена данными между пользователем и системой. На каждом из циклов системой выполняется модулярное возведение в квадрат q -разрядных чисел (в большинстве современных протоколов $q=2048$). Практически q -разрядное число разбивается на k секций, длина которых равна разрядности процессора. При $q=2048$ и разрядности процессора 32 число секций равно 64, $k=64$. Модулярное возведение в квадрат состоит из k^2 процессорных умножений и операций суммирования. Среднее количество операций суммирования равно $1.5 \cdot k^2$. Операция редукции (нахождение остатка) включает в себя, в среднем, q операций вычитания q -разрядных чисел, каждая из которых состоит из k операций процессорного вычитания. Таким образом, время выполнения модулярного возведения в квадрат определяется как $k^2 \cdot (t_m + 1.5 \cdot t_a) + q \cdot k \cdot t_a$, где t_m – время процессорного умножения, t_a – время выполнения процессорной операции сложения или вычитания. Для типичных для практики значений $q=2048$, $k=64$, с учетом того, что операция умножения на современных процессорах выполняется за 10 тактов, а сложения – за 2 такта [6], суммарное число тактов, требующееся для одного модулярного возведения в квадрат может быть оценено как $434 \cdot 10^3$.

Сопоставление числа тактов работы процессора, требующееся для проведения аутентификации предложенным методом (5800) и наиболее быстродействующего аналога – FFSIS показывает, что время реализации предложенной процедуры примерно в 75 раз меньше. На практике метод FFSIS требует примерно 20 выполнений модулярного возведения в квадрат, поэтому расчетное ускорение процесса аутентификации близко к $75 \cdot 20 = 1500$.

Проведенные экспериментальные исследования показали, что время выполнения операции шифрования и двух хеш-преобразований реально в 50-60 раз меньше времени выполнения модулярного возведения в квадрат. Экспериментальная оценка выигрыша во времени полной процедуры аутентификации затруднена тем, что в методе FFSIS выполняется 20 циклов обмена данными по сети между системой и пользователем. Это время, как показали эксперименты, сильно зависит от сетевого трафика. Однако, в целом, можно говорить о том, что предложенный метод обеспечивает ускорение процесса аутентификации удаленных абонентов примерно на 3 порядка.

Вывод

В результате проведенных исследований был предложен метод быстрой аутентификации удаленных абонентов многопользовательских систем, реализующий криптографически строгую концепцию “нулевых знаний”. Особенностью предложенного метода является ориентация на стандартизированные, хорошо и всесторонне испытанные криптографические примитивы – стандартизированные шифроблоки и хеш-преобразования. Это позволяет ускорить процедуру аутентификации, упростить ее реализацию и обеспечивает высокую надежность защиты от попыток несанкционированного доступа в ресурсы системы.

Теоретически и экспериментально доказано, что предложенный метод, за счет использования необратимых булевых преобразований, позволяет на три порядка ускорить вычислительную реализацию аутентификации по сравнению с известными методами реализации строгой аутентификации, в основе которых лежит использование необратимых преобразований теории чисел.

Достижимое ускорение процедуры аутентификации позволяет увеличить число абонентов многопользовательских систем удаленного доступа к ресурсам, а также повысить уровень защищенности от попыток перехвата третьей стороной процесса обмена данными между системой и пользователем. Разработанный метод ориентирован на использование в облачных технологиях удаленного предоставления информации или вычислительных ресурсов пользователям.

Список использованной литературы

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. / B. Schneier - Ed. John Wiley, 1996 - 758 p.
2. Feige U. Zero knowledge proofs of identity / U. Feige., A. Fiat., A. Shamir // Journal of Cryptology.- V.1, №.2.- 1988, - P. 77-94.
3. Soonhwa S. User authentication using mobile phones for mobile payment / S. Soonhwa, Y. Cheong, K. Eunbae, R. Jaechol // Proceedings of the 2015 International Conference on Information Networking (ICOIN) – 2015 - P. 51-56.
4. Markovskyy O. Fast subscriber identification based on the zero knowledge principle for multimedia content distribution/ O. Markovskyy, N. Bardis, N. Doukas // International Journal of Multimedia Intelligence and Security - V.1,- 2010. - P. 78-82.
5. Зенин О.С. Стандарт криптографической защиты AES./ О.С. Зенин О.С., М.А. Иванов - М.: Из-во Кудиц-Образ.-2002.- 174 с.
6. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы / Б. Брэй пер с англ.- 4 вид.- СПб.: Изд-во “БХВ-Петербург”, 2005.- 1328 с.

Автор статті

Захаріудакіс Лефтеріс – аспірант кафедри обчислювальної техніки, Національний технічний університет України «КПІ» ім. І. Сікорського, Київ, Україна. Тел. +38 097 799 24 62. E-mail: 5b4agl@gmail.com

Author of the article

Zahariudakis Lefteris – post-graduate student of Department Computer systems, National Technical University of Ukraine “Igor Sikorsky KPI”, Kyiv, Ukraine. Tel. +38 097 799 24 62. E-mail: 5b4agl@gmail.com

Дата надходження в редакцію: 05.02.2017 р.

Рецензент: д.т.н., проф. М.А. Віноградов

ОСОБЛИВОСТІ АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЕКСПЛУАТАЦІЇ СУДЕН У СУЧАСНИХ УМОВАХ

Musorin O.O., Trofimenko I.V., Shapran Y.E. Features of analytical providing of ships expatiation in operation conditions.

The goal of this article is to determine the priorities of scientific and technical nature, the solution of which creates conditions for improving the operation of ships and restore the basic parameters that characterize the operation of ship equipment reliability.

In article resulted values of data processing reliability during operation is usually compared with the corresponding values compared to the previous periods. This approach allows a qualitative assessment of reliability relative to prior periods of operation. However, is not considered the impact on the statistical evaluation of the intensity of use.

Statistical data failures and faults received in the unstable conditions of observation, which significantly affects the accuracy and reliability assessment. One of the partial objectives of the study is to improve methods of statistical control units ship equipment reliability with the influence the intensity of exploitation and unstable conditions of observation.

Keywords: exploitation, diagnostic, control of parameters, ship equipment

Мусорін О.О., Трофименко І.В., Шапран Ю.Є. Особливості аналітичного забезпечення експлуатації суден у сучасних умовах.

Ціллю даної статті є визначення пріоритетних задач науково-технічного характеру, вирішення яких створює умови до удосконалення процесу експлуатації суден та наведення основних показників, які характеризують надійність експлуатації суднового обладнання.

У статті значення показників надійності за період експлуатації, які отримані у результаті обробки інформації порівнюються з відповідними значеннями показників за попередні періоди. Такий підхід дозволяє здійснити якісну оцінку рівня надійності по відношенню до попередніх періодів експлуатації. При цьому, не враховується вплив на статистичну оцінку показника інтенсивності експлуатації.

Статистичні дані про відмови та несправності отримуються при нестабільних умовах спостережень, що значно впливає на точність та достовірність оцінки. Одним з часткових завдань дослідження є удосконалення методики статистичного контролю надійності агрегатів суднового обладнання з урахуванням впливу інтенсивності експлуатації та нестабільних умов спостережень.

Ключові слова: експлуатація, діагностика, контроль параметрів, суднове обладнання

Мусорин О.О., Трофименко И.В., Шапран Ю.Е. Особенности аналитического обеспечения эксплуатации судов в современных условиях.

Целью данной статьи является определение приоритетных задач научно-технического характера, решение которых создает условия для совершенствования процесса эксплуатации судов и наведения основных показателей, характеризующих надежность эксплуатации судового оборудования.

В статье, значения показателей надежности за период эксплуатации, полученные в результате обработки информации сравниваются с соответствующими значениями показателей за предыдущие периоды. Такой подход позволяет осуществить качественную оценку уровня надежности по отношению к предыдущим периодам эксплуатации. При этом, учитывается влияние на статистическую оценку показателя интенсивности эксплуатации.

Статистические данные об отказах и неисправностях получаемые при нестабильных условиях наблюдений, значительно влияет на точность и достоверность оценки. Одним из частных задач исследования является совершенствование методики статистического контроля надежности агрегатов судового оборудования с учетом влияния интенсивности эксплуатации и изменяющимся условиям наблюдений.

Ключевые слова: эксплуатация, диагностика, контроль параметров, судовое оборудование

Вступ

Серед важливих задач у напрямку удосконалення експлуатації за технічним станом є удосконалення системи збору, обробки та аналізу інформації про технічний стан та надійність суден.

Своєчасне виявлення моментів виникнення деградаційних процесів, що визначають терміни переходу у граничний стан та є індивідуальними для кожного типу виробів, є основною метою контролю рівня надійності техніки на даному етапі її експлуатації.

Аналіз останніх досліджень і публікацій.

На практиці у процесі експлуатації техніки для оцінки безвідмовності використовуються, як правило, показники інтенсивності відмов, параметру потоку відмов, середній наробіток до відмови, середній наробіток на відмову.

У науково-технічній літературі [1, 2, 8-15] загальноприйнятим вважається підхід до оцінювання показників надійності технічних виробів (інтенсивності відмов, параметру потоку відмов) як функції наробітку при різних законах розподілу часу між відмовами. Методи статистичного оцінювання показників при різних планах випробувань (спостережень) на надійність закріплені у державних стандартах України [3, 6]. Але, як відмічається у [4, 5, 7], реальні умови експлуатації техніки не відповідають жодному плану, встановленому стандартом.

Деякі автори відмічають, що фізичне зношування технічних виробів виникає як під час їх використання за призначенням – зношування 1-го роду, так й під час простоїв (зберігання) – зношування 2-го роду [7, 10, 13].

Проведений аналіз літератури свідчить про відсутність чітко обґрунтованих рекомендацій щодо урахування впливу на величину статистичної оцінки показника надійності виробу календарного терміну його експлуатації поряд з наробітком.

Формулювання цілей статті.

Таким чином, ціллю даної статті є визначення пріоритетних задач науково-технічного характеру, вирішення яких створює умови до удосконалення процесу експлуатації суден та наведення основних показників, які характеризують надійність експлуатації суднового обладнання.

Виклад матеріалів дослідження.

Для оцінки надійності технічних виробів використовуються встановлені стандартами показники. Так для опису *безвідмовності* використовуються такі показники: ймовірність безвідмовної роботи – $P(t)$; інтенсивність відмов – $\lambda(t)$; параметр потоку відмов – $z(t)$; середній наробіток до відмови – T_1 ; середній наробіток на відмову – T_0 .

Для опису *довговічності* використовуються: середній ресурс – T_n ; експлуатаційний ресурс – T_e ; гамавідсотковий строк служби – $T_{\gamma\%}$. Для опису *ремонтпридатності* використовуються такі показники: імовірність відновлення – P_v ; інтенсивність відновлення – $\mu(t)$; середня тривалість відновлення – T_v .

Одиничні показники надійності (наприклад, ремонтпридатність) характеризують тільки одну із властивостей технічного об'єкту, в той час як комплексні показники характеризують декілька властивостей, і в подальшому будуть використовуватися у якості основних для оцінки ефективності таких складних об'єктів, як судно та його функціональних систем. До цих показників відносяться коефіцієнт готовності – K_r , коефіцієнт оперативної готовності – $K_{ог}$ та коефіцієнт технічного використання – $K_{тв}$ [1–4].

Коефіцієнт готовності $K_r(t)$ прийнято визначати як імовірність того, що об'єкт буде в працездатному стані в будь-який момент часу, крім запланованих періодів, впродовж яких застосування об'єкта за призначенням не передбачається [2].

Залежність $K_r(t)$ від часу часто називають нестационарним коефіцієнтом готовності (функцією готовності). Отримати вираз для нестационарного коефіцієнта готовності в аналітичному вигляді досить складно і в загальному випадку він має вигляд [2-6]

$$K_r(t) = P(t) + \int_0^t P(t-\tau) \cdot \omega_b(\tau) \cdot d\tau,$$

де $\omega_b(\tau)$ – параметр потоку відновлень.

Поряд з цим, для будь-яких законів розподілу наробітку між відмовами та часу відновлення можна довести, що стаціонарний коефіцієнт готовності має вигляд

$$K_r = \frac{M(T_0)}{M(T_0) + M(T_b)},$$

де $M(T_0)$ – математичне очікування часу знаходження ЛА у справному стані; $M(T_b)$ – математичне очікування часу відновлення ЛА.

Поряд з $K_r(t)$ ДСТУ вводять коефіцієнт оперативної готовності $K_r(t, t+\tau)$ як імовірність того, що об'єкт буде знаходитися у працездатному стані в довільний проміжок часу, крім запланованих періодів, впродовж яких застосування об'єкта за призначенням не передбачається, та починаючи з цього моменту буде працювати безвідмовно упродовж заданого інтервалу часу τ

$$K_r(t, t+\tau) = P(t+\tau) + \int_0^t P(t+\tau-x) \cdot \omega_b(x) dx.$$

Для дослідження впливу впроваджених методів та режимів технічного обслуговування і ремонту на ефективність процесу технічної експлуатації застосовують ще один комплексний показник надійності – коефіцієнт технічного використання $K_{тв}$, який дорівнює відношенню математичного очікування (МО) часу перебування об'єкта у працездатному стані за деякий період експлуатації $M(T_0)$ до суми МО часу перебування об'єкта в працездатному стані та сумарного часу простоїв на всіх видах профілактичних та ремонтних робіт

$$K_{тв} = \frac{M(T_0)}{M(T_0) + M(T_{пр})},$$

де $M(T_{пр})$ – сума математичних очікувань часу простою об'єкта на періодичних, регламентних, сезонних роботах, під час проведення доробок, ремонтів, усунення несправностей тощо.

Для оцінки рівня надійності (безвідмовності) відновлюваних об'єктів використовують характеристики потоку відмов: параметру потоку відмов $\hat{z}$ або наробітку на відмову $\hat{T}_0$

$$\hat{z} = \frac{n}{t_{\Sigma}}, \quad \hat{T}_0 = \frac{t_{\Sigma}}{n},$$

де n – сумарна кількість відмов і пошкоджень, що були виявлені в польоті та на землі за досліджуваний період часу експлуатації τ сукупності однотипних виробів; t_{Σ} – сумарне напрацювання у польоті сукупності однотипних виробів за той же період часу τ .

Припустимо, що на виріб впливають два незалежних потоки відмов. Перший потік відмов пов'язаний з наробітком, другий – з календарним часом його експлуатації. Обидва потоки є простішими з відповідними інтенсивностями z_1 та z_2 . При цьому виріб являє собою об'єкт зі змінним режимом експлуатації.

З урахуванням наведених припущень в деякій літературі можна знайти наступне граничне співвідношення [2-9]

$$z_1 + \frac{z_2}{K_l} = z = \frac{1}{T_0},$$

звідки отримуємо

$$\frac{K_I}{z_1 \cdot K_I + z_2} = T_0, \quad (1)$$

Коефіцієнт $0 \leq K_I < 1$ характеризує інтенсивність льотної експлуатації виробу за час T_e і визначається за виразом

$$K_I = \frac{T_e - T_{TO} - T_{відн} - T_{прост}}{T_e} \approx \frac{t}{T_e} \quad (2)$$

де T_e – календарний час експлуатації виробу за період (рік, півріччя), год., T_{TO} – середній час ТО виробу за той же період, год., $T_{відн}$ – середній час відновлення виробу за період, год., $T_{прост}$ – середній час простою виробів за період без застосування за призначенням, год., t – середній наробіток виробу за період, год.

За своїм змістом K_I схожий на коефіцієнт планованого застосування $K_{ПЗ}$, але останній враховує наробіток, що планується, та не враховує час простою без застосування за призначенням.

За допомогою виразу (1) та (2) можна виконати якісну та кількісну оцінку впливу інтенсивності експлуатації виробу K_I на показник його надійності (безвідмовності) T_0 .

Якісно з (1) видно, що при збільшенні інтенсивності експлуатації сукупності виробів K_I збільшується чисельник та добуток в сумі знаменника ($z \cdot K_I$), але у зв'язку з тим, що $z_1 < 1$, чисельник зростає швидше, тому оцінка T_0 теж збільшується

$$K_I \uparrow \Rightarrow \frac{K_I \uparrow \uparrow}{(z_1 \cdot K_I) \uparrow + z_2} \Rightarrow T_0 \uparrow$$

Навпаки, при зменшенні інтенсивності експлуатації сукупності виробів $K_I \downarrow$ оцінка середнього наробітку на відмову та пошкодження T_0 теж зменшується

$$K_I \downarrow \Rightarrow \frac{K_I \downarrow \downarrow}{(z_1 \cdot K_I) \downarrow + z_2} \Rightarrow T_0 \downarrow$$

Таким чином, статистичний показник надійності змінюється в залежності від інтенсивності експлуатації, хоча реальний рівень надійності при цьому залишається незмінним.

Розглянемо граничні випадки. Очевидно, що при достатньо високій інтенсивності відбувається швидке вичерпання ресурсу виробу за наробітком, відсутні тривалі простої без застосування за призначенням, тому інтенсивність потоку відмов, пов'язаних з старінням матеріалів $z_2 \rightarrow 0$. В цьому випадку, як видно з виразу (1), маємо

$$T_0 = \frac{1}{z_1},$$

тобто міжперіодична оцінка дозволяє достатньо точно оцінити реальний рівень надійності та не залежить від зміни інтенсивності застосування.

Інша справа, якщо інтенсивність експлуатації мала [5-9]. В цьому випадку мають місце довготривалі простої без застосування за призначенням, відбувається інтенсивне старіння матеріалів конструкції на етапі, коли досягається вичерпання ресурсу за календарними термінами служби при істотному залишку ресурсу за наробітком. В граничному випадку, коли спостерігаються високі значення z_2 при $z_1 \rightarrow 0$, вираз (1) приймає вигляд

$$T_0 = \frac{K_I}{z_2}, \quad (3)$$

що свідчить про прямопропорційну залежність оцінки показника (3) від інтенсивності експлуатації.

Висновки

Отримані у результаті обробки інформації значення показників надійності за період експлуатації, як правило, порівнюються з відповідними значеннями показників за попередні періоди. Такий підхід дозволяє здійснити якісну оцінку рівня надійності по відношенню до

попередніх періодів експлуатації. При цьому, як зазначено вище, не враховується вплив на статистичну оцінку показника інтенсивності експлуатації.

Статистичні дані про відмови та несправності отримуються при нестабільних умовах спостережень, що значно впливає на точність та достовірність оцінки. Одним з часткових завдань дослідження є удосконалення методики статистичного контролю надійності агрегатів судового обладнання з урахуванням впливу інтенсивності експлуатації та нестабільних умов спостережень.

Список використаної літератури

1. Мясников Ю.Н. Надежность и техническая диагностика судовых энергомеханических систем / Мясников Ю.Н. – СПб: Издательство Федерального государственного унитарного предприятия “Центральный научно-исследовательский институт имени академика А.Н.Крылова”, 2008. – 183 с.
2. Система технического обслуживания и ремонта техники: ГОСТ 18322:78. – [Действующий с 1979-01-07]. – М.: Государственный комитет СССР по стандартам, 1978. – 14 с.
3. Барлоу Р. Статистическая теория надежности и испытания на безотказность / Р. Барлоу, Ф. Прошан; пер. с англ. И. А. Ушакова. – М.: Наука, 1985. – 328 с.
4. Smith A. M. RCM: gateway to world class maintenance / Anthony M. Smith., Glenn R. Hincheliffe – Elsevier Inc., Burlington, USA, 2004. – 340 p.
5. Надійність техніки. Експериментальне оцінювання та контроль надійності. Основні положення: ДСТУ 2864 : 94. – [Чинний від 1996-01-01]. – К.: Держстандарт України, 1995. – 30 с.
6. Надійність техніки. Терміни та визначення: ДСТУ 2860 : 94. – [Чинний від 1996-01-01]. – К.: Держстандарт України, 1995. – 79 с.
7. Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги: ДСТУ 2862:94. – [Чинний від 1994-12-08]. – К.: Держстандарт України, 1994. – 38 с.
8. Райншке К. Оценка надежности систем с использованием графов / Райншке К., Ушаков И.А.; [под ред. И.А.Ушакова]. - М.: Радио и связь, 1988. - 208 с.
9. Большие технические системы: проектирование и управление / [Л.М. Артюшин, Ю.К. Зиатдинов, И.А. Попов, А.В. Харченко.]. – Харьков: Факт, 1997. – 400 с.

Автори статті

Мусорін О.О. - аспірант, Київська державна академія водного транспорт імені гетьмана Петра Конашевича-Сагайдачного, Україна. Тел. +38 050 398 47 96. E-mail: bog2603@ukr.net

Трофименко І.В. - аспірант, Київська державна академія водного транспорт імені гетьмана Петра Конашевича-Сагайдачного, Україна. Тел. +38 050 398 47 96. E-mail: bog2603@ukr.net

Шапран Ю.Є. - аспірант, Київська державна академія водного транспорт імені гетьмана Петра Конашевича-Сагайдачного, Україна. Тел. +38 050 398 47 96. E-mail: bog2603@ukr.net

Authors of the article

Musorin O.O. – post-graduate student, The Kyiv State Maritime Academy named after hetman Petro Konashevich-Sahaydachnyi Kyiv, Ukraine. Tel. +38 050 398 47 96. E-mail: bog2603@ukr.net

Trofimenko I.V. – post-graduate student, The Kyiv State Maritime Academy named after hetman Petro Konashevich-Sahaydachnyi Kyiv, Ukraine. Tel. +38 050 398 47 96. E-mail: bog2603@ukr.net

Shapran Y.E. – post-graduate student, The Kyiv State Maritime Academy named after hetman Petro Konashevich-Sahaydachnyi Kyiv, Ukraine. Tel. +38 050 398 47 96. E-mail: bog2603@ukr.net

Дата надходження в редакцію: 19.01.2017 р.

Рецензент: д.т.н., проф. В.І. Богомья