

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 5, № 3

Volume 5, No. 3

Одеса – 2015
Odesa – 2015

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

Виходить 4 рази на рік

Заснований Одеським національним
політехнічним університетом у 2011 році

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

Головний редактор: *Г.О. Оборський*

Заступник головного редактора:

А.А. Кобозєва

Відповідальний редактор:

А.Л. Іванова

Редакційна колегія:

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,
А.Ф. Верлань, Г.М. Востров, В.Б. Дудикевич,
Л.Є. Євтушик, М.Б. Копитчук, С.В. Ленков,
І.І. Маракова, А.Д. Мілка, С.А. Нестеренко,
М.С. Никитченко, С.А. Положаєнко,
О.В. Рибальський, Х.М.М. Рубіо, В.Д. Русов,
І.М. Ткаченко-Горський, А.В. Усов,
В.О. Хорошко, М.Є. Шелест, М.С. Яджак*

Published 4 times a year

Founded by Odessa National Polytechnic
University in 2011

Certificate of State Registration

КВ № 17610 - 6460Р of 04.04.2011

Editor-in-chief: *G.A. Oborsky*

Associate editor:

A.A. Kobozeva

Executive editor:

A.L. Ivanova

Editorial Board:

*T. Banakh, P. Bidyuk, V. Dudykevich,
L. Evtushik, V. Khoroshko, N. Kopytchuk,
S. Lenkov, I. Marakova, A. Milka, S. Nesterenko,
N. Nikitchenko, S. Polozhaenko, J. Rubio,
V. Rusov, O. Rybalsky, M. Shelest,
I. Tkachenko Gorski, A. Usov, N. Vaysfeld,
A. Verlan, G. Vostrov, M. Yadzhak*

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

Оригінал-макет виготовлено редакцією журналу

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

Телефон: +38 048 705 8506

Web: <http://immm.opu.ua>

E-mail: immm.ukraine@gmail.com

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

Tel.: +38 048 705 8506

Web: <http://immm.opu.ua>

E-mail: immm.ukraine@gmail.com

© Одеський національний політехнічний університет, 2015

ЗМІСТ / CONTENTS

РЕКУРЕНТНІ МЕТОДИ СИНТЕЗУ ПОСЛІДОВНОСТЕЙ З ОПТИМАЛЬНИМ ПІК-ФАКТОРОМ СПЕКТРА УОЛША-АДАМАРА М.І. Мазурков, А.В. Соколов	203	RECURRENT SYNTHESIS METHODS OF THE SEQUENCES WITH OPTIMAL PEAK-TO-AVERAGE POWER RATIO VALUE OF WALSH-HADAMARD SPECTRUM Mazurkov M., Sokolov A.
ПЕРЕДОБРОБКА ЦИФРОВОГО ЗОБРАЖЕННЯ ДЛЯ СТИСНЕННЯ О.В. Наріманова, А.Р. Агаджанян, М.С. Кучма	210	PREPROCESSING OF DIGITAL IMAGE FOR COMPRESSION Narimanova O., Agadzhanian A., Kuchma M.
СИНТЕЗ АЛГОРИТМА ОЦЕНИВАНИЯ ЧАСТОТЫ КОМПЛЕКСНОГО МОНОХРОМНОГО СИГНАЛА И. П. Омельчук	218	SYNTHESIS OF THE FREQUENCY ESTIMATION ALGORITHM FOR A SINGLE-TONE COMPLEX SIGNAL Omelchuk I.
РОЗРАХУНОК ОБЛАСТЕЙ СПІВІСНУВАННЯ ФАЗ В СИСТЕМІ $In_xGa_{1-x}Sb_yAs_{1-y}$ А.І. Казаков, Л.Т. Кваташидзе, Г.В. Шаповалов	226	CALCULATION OF THE COEXISTENCE SPACES IN THE SYSTEM $In_xGa_{1-x}Sb_yAs_{1-y}$ Kazakov A., Kvatashidze L., Shapovalov G.
ПРОГНОЗУВАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖАВИ З ВИКОРИСТАННЯМ ПЕРЕТВОРЕННЯ КАРУНЕНА-ЛОЄВА І.Р. Опірський	234	PREDICTION OF UNAUTHORIZED ACCESS TO INFORMATION SYSTEMS OF THE STATE USING KARHUNEN-LOEVE Opirskyy I.
КРИТЕРІЇ ОЦІНКИ ЙМОВІРНОСТІ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ТЕХНІЧНІ КАНАЛИ М.Г. Романюков	240	CRITERIA FOR EVALUATING THE PROBABILITY OF INFORMATION LEAKAGE THROUGH TECHNICAL CHANNELS Romanykov N.
МЕТОДИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ТА МАШИННОЇ ІДЕНТИФІКАЦІЇ НЕСТАЦІОНАРНИХ АНОМАЛЬНИХ ДИФУЗІЙНИХ ПРОЦЕСІВ С.А. Положаєнко, Омар Муаяд Абдуллах	249	METHODS OF MATHEMATICAL DESIGN AND MACHINE AUTHENTICATION OF NON - STATICS ANOMALOUS DIFFUSIVE PROCESSES Polozhaenko S., Omar Muajad Abdullach

НАДІЙНІСТЬ СПЕЦІАЛЬНОГО
ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
ІНТЕГРОВАНІХ ІНФОРМАЦІЙНИХ
СИСТЕМ ОРГАНІВ ВНУТРІШНІХ
СПРАВ УКРАЇНИ

В.А. Кудінов, О.М. Грищак

КЛАСИФІКАЦІЯ МАТЕМАТИЧНИХ
МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ
ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЛЯ
УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

А.Н. Орехов, В.О. Хорошко

УДОСКОНАЛЕННЯ МЕТОДИКИ
ВИЯВЛЕННЯ ЗАКЛАДНИХ
ПРИСТРОЇВ НА АБОНЕНТСЬКИХ
ТЕЛЕФОННИХ ЛІНІЯХ З
УРАХУВАННЯМ МОЖЛИВОСТЕЙ
СУЧАСНИХ ЗАСОБІВ КОНТРОЛЮ

В.В. Хома, В.М. Іванюк

КОНТРОЛЬ ОБЧИСЛЮВАЛЬНИХ
ПРОЦЕСІВ МЕТОДАМИ
ІДЕНТИФІКАЦІЇ ПРИ НАТУРНОМУ
МОДЕЛЮВАННІ

Л. Л. Прокоф'єва, С. П. Савіч,
А. Н. Порпуліт

МОДЕЛЬ ОЦІНКИ ЕФЕКТИВНОСТІ
ЗАХИСТУ ПРОГРАМНОГО КОДУ ВІД
НЕСАНКЦІОНОВАНИХ ЗМІН

А.Є. Кілін, В.Г. Кононович,
І.В. Кононович, В.В. Беззубенко

259 RELIABILITY SPECIAL SOFTWARE
INTEGRATED INFORMATION
SYSTEMS THE DEPARTMENT OF
INTERNAL AFFAIRS OF UKRAINE
Kudinov V., Gryschak O.

268 CLASSIFICATION OF
MATHEMATICAL MODELS OF
SYSTEMS OF PROTECTION OF
INFORMATION SPACE FOR AIR
TRAFFIC CONTROL
Orekhov A., Khoroshko V.

273 IMPROVEMENT OF PROCEDURE FOR
DETECTION OF TELEPHON BUGS
WITH DUE CONSIDERATION OF
MODERN MONITORING DEVICE
CAPABILITIES
Khoma V., Ivanyuk V.

283 CONTROL OF CALCULABLE
PROCESSES BY METHODS OF
AUTHENTICATION AT MODEL
DESIGN
Prokofieva L., Savich S., Porpulit A.

289 MODEL EVALUATION OF THE
EFFECTIVENESS OF PROTECTION
CODE FROM UNAUTHORIZED
CHANGES
Kilin A., Kononovich V., Kononovich I.,
Bezzubenko V.

РЕКУРРЕНТНЫЕ МЕТОДЫ СИНТЕЗА ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ОПТИМАЛЬНЫМ ПИК-ФАКТОРОМ СПЕКТРА УОЛША-АДАМАРА

М.И. Мазурков, А.В. Соколов

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

Предложены три метода синтеза бинарных последовательностей с оптимальным значением пик-фактора спектра Уолша-Адамара, которые могут быть использованы для построения С-кодов, применяемых в технологии CDMA. На основе данных конструкций разработан алгоритм синтеза бесконечных семейств последовательностей, обладающих оптимальным значением пик-фактора спектра Уолша-Адамара.

Ключевые слова: оптимальная кодирующая последовательность, CDMA, С-код, бент-последовательность, пик-фактор.

Введение

Одной из наиболее актуальных технологий множественного доступа является технология MC-CDMA (Multi-Code Code Division Multiple Access), которая является ключевой при построении систем связи четвертого и пятого поколений G4 и G5 [1].

Известно, что в технологии MC-CDMA исходный бинарный вектор данных подвергается ортогональному преобразованию. Входные биты изменяют знак одной из ортогональной функций дискретного времени $h_i(t)$, в качестве которых чаще всего применяются функции Уолша. Таким образом, передаваемый в канал связи сигнал представляет собой коэффициенты преобразования Уолша-Адамара исходного сигнала [2].

Данное обстоятельство приводит к появлению такого недостатка технологии MC-CDMA как высокие значения пик-фактора передаваемого сигнала $S_c(t)$, который определяется как отношение максимальной мощности сигнала $P_{\max}$ к его средней мощности P_{cp}

$$\kappa = \frac{P_{\max}}{P_{cp}} = \frac{1}{N} \max_t \left\{ |S_c(t)|^2 \right\}, \quad (1)$$

где N — длина последовательности $h_i(t)$.

Высокие значения пик-фактора излучаемого сигнала приводят к нерациональному использованию мощности передатчика, искажениям передаваемого сигнала, усложнению применяемого оборудования. Это диктует необходимость поиска методов снижения величины κ [3]. Одним из наиболее распространенных методов снижения пик-фактора является метод, основанный на кодировании исходных сообщений d_i такими кодовыми словами С-кода, которые обладали бы низкими значениями пик-фактора κ (рис. 1) [2].

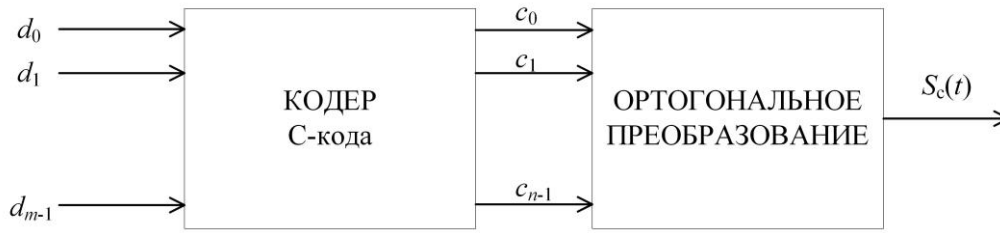


Рис. 1. Схема кодирования информации на основе С-кода

Для построения С-кода наилучшими, с точки зрения минимизации пик-фактора, кодовыми словами являются бент-последовательности [4] — бинарные последовательности $B = [b_0, b_1, \dots, b_i, \dots, b_{N-1}]$, где коэффициенты $b_i \in \{1, -1\}$, четной длины $N = 2^{2m}$, которые обладают равномерным по модулю спектром Уолша-Адамара [5], представимым в матричной форме

$$W_B(\omega) = B \cdot A_N, \quad \omega = \overline{0, N-1}, \quad (2)$$

где A_N — матрица Уолша-Адамара порядка $N = 2^{2m}$.

Существование бент-последовательностей возможно только, если их длина определена четной степенью двойки, т.е. $N = 2, 4, 16, 64, 256, 1024, \dots$, что является существенным ограничением для разрядности используемого в системах связи оборудования.

Целью настоящей статьи является разработка рекуррентных методов построения последовательностей длин нечетной степени двойки ($N = 2^{2m-1} = 8, 32, 128, 512, \dots$), обладающих оптимальным значением пик-фактора $\kappa = 2$.

Определение 1. Оптимальной кодирующей последовательностью (ОКП) назовем такую последовательность, которая обладает значением пик-фактора спектра Уолша-Адамара $\kappa = 2$.

Экспериментальные исследования показывают, что значение пик-фактора $\kappa = 2$ является минимальным значением для длин последовательностей $N = 2^{2m-1}$, $m = 1, 2, 3, \dots$

Установлено, что для построения последовательностей с оптимальным значением пик-фактора $\kappa = 2$ могут быть использованы аналоги алгебраических конструкций, предложенных в работе [6] для синтеза бент-последовательностей.

В настоящей статье обобщен известный метод синтеза бент-последовательностей Майорана-МакФарланда (Метод 1), а также предложены два новых метода (Метод 2, Метод 3) рекуррентного построения ОКП.

Метод 1 (обобщенный метод Майорана-МакФарланда)

Как известно, одним из наиболее эффективных методов построения бент-последовательностей произвольной длины $N = 2^{2m}$ является конструкция Майорана-МакФарланда [5,7], которая основана на конкатенации строк матрицы Адамара A_L порядка $L = \sqrt{N}$, а также всех возможных $L!$ перестановок её строк и 2^L знаковых кодирований. Тогда как, в свою очередь, матрица Адамара A каждого следующего порядка $L = 2^k$ строится в соответствии с известным рекуррентным правилом [1]

$$A_{2^k} = \begin{bmatrix} A_{2^{k-1}} & A_{2^{k-1}} \\ A_{2^{k-1}} & -A_{2^{k-1}} \end{bmatrix}, \quad (3)$$

где $A_1 = 1$.

Например, в соответствии с (3) построим матрицу Адамара A_8 (где для краткости $+1$ обозначены как “+”, а -1 как “-”)

$$A_8 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix}, \quad (4)$$

и, применяя последовательную конкатенацию её строк, получаем бент-последовательность длины $N = 64$, и в соответствии с (2) её спектр Уолша-Адамара

[illegible]

т.е. последовательность (5) действительно удовлетворяет определению бент-последовательности.

В настоящей работе предлагается метод построения последовательностей длин $N = 8, 32, 128, 512 \dots$, основанный на сегментарной конкатенации строк матрицы Уолша-Адамара для построения последовательностей с оптимальным значением пик-фактора $\kappa = 2$.

Рассмотрим, например, матрицу Адамара восьмого порядка A_8 (4). Путем конкатенации её первых четырех строк получаем последовательность Ω длины $N=32$ и коэффициенты её преобразования Уолша-Адамара $W = \Omega A_8$, соответственно

$$\begin{aligned}\Omega &= [+++++--+-+--++--+-+--++]; \\ W &= [8 \ 8 \ 8 \ 8 \ 0 \ 0 \ 0 \ 0 \ 8 \ -8 \ 8 \ -8 \ 0 \ 0 \ 0 \ 0 \ 8 \ 8 \ -8 \ -8 \ 0 \ 0 \ 0 \ 0 \ 8].\end{aligned}\tag{6}$$

Очевидно, что пик-фактор построенной последовательности может быть найден в соответствии с (1) как $\kappa = 8^2/32 = 2$, что, как показывают эмпирические исследования, является наилучшим (оптимальным) значением среди всех последовательностей длины $N = 32$, т.е. последовательность (6) является ОКП.

Установлено, что число ОКП длины 32, может быть существенно увеличено с помощью следующих правил размножения.

Правило 1. Выбор строк матрицы Адамара порядка L для конструирования последовательностей длины N различными $C_L^{L/2}$ способами.

В случае конструирования последовательностей длины $N=32$ с помощью матрицы Адамара порядка $L=8$ получаем количество возможных сочетаний

$$C_8^4 = \frac{8!}{4!(8-4)!} = 70. \quad (7)$$

Правило 2. Конкатенацию выбранных μ строк матрицы Адамара можно провести различными $\mu!$ способами, где $\mu = L/2$, при этом сохраняется оптимальное значение пик-фактора.

Так, например, при конструировании последовательностей длины $N = 32$ с помощью матрицы Адамара порядка $L = 8$ мы производим конкатенацию $\mu = 4$ строк матрицы следующим образом

$$\Omega = \begin{bmatrix} 1 & 2 & 3 & 4 \\ A_{\alpha_1,:} & A_{\alpha_2,:} & A_{\alpha_3,:} & A_{\alpha_4,:} \end{bmatrix}, \quad (8)$$

где « $\cdot$ » — символ горизонтальной конкатенации, « $:$ » — символ выбора всех элементов по столбцам.

Ясно, что в приведенном примере конкатенируемые строки $A_{i,:}$ могут быть переставлены $4! = 24$ различными способами.

Правило 3. Каждый сегмент исходной матрицы Адамара, участвующий в конкатенации, может быть подвергнут знаковому кодированию $2^{L/2}$ различными способами.

Так, при конструировании последовательностей длины $N = 32$, сегменты матрицы могут быть закодированы 16-ю различными способами, т.е.

$$\Omega = [(-1)^{\gamma_1} A_{\alpha_1,:}, (-1)^{\gamma_2} A_{\alpha_2,:}, (-1)^{\gamma_3} A_{\alpha_3,:}, (-1)^{\gamma_4} A_{\alpha_4,:}], \quad (9)$$

где $\gamma_1, \dots, \gamma_4 \in \{0, 1\}$.

Таким образом, на основе Правил 1, 2, 3 может быть построен первый класс ОКП мощности

$$J_1 = C_L^{L/2} \cdot \left(\frac{L}{2}\right)! \cdot 2^{L/2}. \quad (10)$$

Так, при $N = 2^3 = 8$ на основе Метода 1 может быть построено $J = 6 \cdot 2 \cdot 4 = 48$ ОКП. Путем полного перебора, найдено, что всего ОКП длины $N = 8$ существует $J_8 = 112$, десятичные эквиваленты которых приведены в виде следующей алгебраической конструкции

03	05	06	09	0A	0C	11	12	14	17	18	1B	1D	1E	21	22
24	27	28	2B	2D	2E	30	35	36	39	3A	3F	41	42	44	47
48	4B	4D	4E	50	53	56	59	5C	5F	60	63	65	6A	6C	6F
71	72	74	77	78	7B	7D	7E	81	82	84	87	88	8B	8D	8E
90	93	95	9A	9C	9F	A0	A3	A6	A9	AC	AF	B1	B2	B4	B7
B8	BB	BD	BE	C0	C5	C6	C9	CA	CF	D1	D2	D4	D7	D8	DB
DD	DE	E1	E2	E4	E7	E8	EB	ED	EE	F3	F5	F6	F9	FA	FC

Например, $03 = \{11000000\} = \{- - + + + +\}$. Находя преобразование Уолша-Адамара (2) данной последовательности $W = \{4 \ 0 \ -4 \ 0 \ -4 \ 0 \ -4 \ 0\}$, убеждаемся, что она действительно представляет собой ОКП.

Найденные $J_8 = 112$ ОКП могут быть положены в основу конструирования других двух классов оптимальных кодирующих последовательностей.

Метод 2

Проведенные в настоящей работе исследования полного класса из $J_8 = 112$ оптимальных последовательностей длины $N = 8$ позволили классифицировать его с точки зрения весовых структур последовательностей

<i>Вес последовательности</i>	2	4	6
<i>Количество последовательностей</i>	28	56	28

(12)

Каждая последовательность длины 2^{k-2} из данного класса может быть использована для построения оптимальной, с точки зрения пик-фактора, последовательности длины 2^k по следующим правилам (с учетом допустимых знаковых кодирований)

$$ОКП_{2^k} = \begin{bmatrix} r \\ r \\ r \\ \bar{r} \end{bmatrix}, \begin{bmatrix} r \\ r \\ \bar{r} \\ r \end{bmatrix}, \begin{bmatrix} r \\ \bar{r} \\ r \\ r \end{bmatrix}, \begin{bmatrix} \bar{r} \\ r \\ r \\ r \end{bmatrix}, \quad (13)$$

где r — любая ОКП длины 2^{k-2} , k — нечетное.

Например, рассмотрим исходную ОКП длины $N = 8$

$$r = [- - + + + + +], \quad (14)$$

в соответствии с (13) на её основе могут быть построены 4 новые ОКП длины $N = 32$, обладающие значением пик-фактора $\kappa = 2$

$$ОКП = \begin{bmatrix} - - + + + + + - - + + + + + - - + + + + + + - - - - - \\ - - + + + + + - - + + + + + + - - - - - + + + + + \\ - - + + + + + + - - - - - + + + + + - - + + + + + \\ + + - - - - - + + + + + - - + + + + + - - + + + + + \end{bmatrix}, \quad (15)$$

Отметим, что Метод 2 увеличивает мощность множества ОКП в 4 раза на каждой итерации увеличения длины.

Метод 3

Построение ОКП большей длины 2^k также возможно производить на основе 2-х различных ОКП меньшей длины 2^{k-2} с помощью следующей конструкции (и её возможного знакового кодирования)

$$ОКП_{2^k} = \begin{bmatrix} s \\ s \\ q \\ \bar{q} \end{bmatrix}, \begin{bmatrix} s \\ \bar{s} \\ q \\ q \end{bmatrix}, \quad (16)$$

где s и q — любые различные ОКП длины 2^{k-2} , k — нечетное.

При генерации ОКП длины $N = 32$ при помощи множества ОКП длины $N = 8$ выбор исходной последовательности s может быть произведен 112 различными способами, тогда как последовательность r возможно выбрать лишь 111 различными способами так, чтобы они были разными. В общем случае, мощность множества ОКП

на каждой последующей итерации Метода 3 с учетом всех правил размножения с помощью знакового кодирования и перестановок сегментов определяется как

$$J_{2^k} = 2 \cdot J_{2^{k-2}} \cdot (J_{2^{k-2}} - 1). \quad (17)$$

Таким образом, учитывая особенности обобщенного в статье Метода 1 (обобщенный метод Майорана-МакФарланада) и разработанных Методов 2, 3, приведем алгоритм синтеза бесконечных семейств ОКП:

Шаг 1. Методом перебора находим полный класс ОКП длины $N=8$ и мощности $J^8=112$.

Шаг 2. С помощью Конструкции 1 конструируем класс ОКП длины $4 \cdot N=32$ и мощности $J_{1,32}=26880$.

Шаг 3. Используя Конструкции 2 и 3 синтезируем классы ОКП длины $4 \cdot N=32$ мощностей $J_{2,32}=4 \cdot 112=448$ и $J_{3,32}=2 \cdot 112 \cdot 111=24864$.

Шаг 4. Помещаем все последовательности в один массив объема $J_{32}=J_{1,32}+J_{2,32}+J_{3,32}=26880+448+24864=52192$. Если заданная длина достигнута — останов, иначе возвращаемся на Шаг 2, используя найденные последовательности как исходные.

С помощью табл. 1 проиллюстрируем увеличение мощности класса ОКП с ростом их длины N при использовании разработанного алгоритма.

Таблица 1.

Увеличение мощности класса ОКП

Длина n	8	32	128	512	2048	8192
Мощность Конструкции 1	48	26880	$1.3284 \cdot 10^{11}$	$8.2420 \cdot 10^{26}$	$2.0711 \cdot 10^{63}$	$5.6061 \cdot 10^{145}$
Мощность Конструкции 2	—	448	101248	$6.1 \cdot 10^{11}$	$3.2969 \cdot 10^{27}$	$8.2844 \cdot 10^{63}$
Мощность Конструкции 3	—	24864	$2.0 \cdot 10^{10}$	$4.6513 \cdot 10^{22}$	$1.3587 \cdot 10^{54}$	$8.5789 \cdot 10^{126}$
Σ	112	52192	$1.525 \cdot 10^{11}$	$8.2422 \cdot 10^{26}$	$2.0711 \cdot 10^{63}$	$5.6061 \cdot 10^{145}$

Анализ данных табл. 1 показывает, что наиболее быстрорастущим рекуррентным классом ОКП, подобно рекуррентному классу бент-функций является модифицированная (обобщенная) конструкция Майорана-МакФарланада.

Выводы

1. Дальнейшее развитие получил метод рекуррентного синтеза бент-последовательностей Майорана-МакФарланада, который был обобщен на случай длин последовательностей $N=2^{2^m-1}=8,32,128,512,\dots$, для синтеза ОКП (Метод 1).

2. Предложены два метода (Метод 2 и Метод 3) рекуррентного увеличения длины ОКП, использующие в качестве исходного материала полные множества ОКП меньшей длины N и позволяющие синтез больших множеств ОКП длины $4N$.

3. Разработан алгоритм рекуррентного построения ОКП, основанный на предложенных методах. Так, используя полное множество ОКП длины $N=8$ и

мощности $J_8 = 112$, может быть построено, например, множество ОКП длины $N = 128$ мощности $J_{128} = 1.525 \cdot 10^{11}$.

Построенные ОКП могут быть рекомендованы к использованию в современных системах передачи информации, основанных на технологии CDMA, в частности, MC-CDMA в качестве кодовых слов C-кода, обладающих оптимальным значением пик-фактора $\kappa = 2$ спектра Уолша-Адамара.

Список литературы

1. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков // Одесса: Наука и Техника. — 2010. — 340 с.
2. Paterson, K. G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory / K.G. Paterson // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. — P. 46–71.
3. Гепко, И.А. Формирование частотно-компактных сигналов с минимальным пик-фактором для систем MC-CDMA с расширением спектра в частотной области / И.А. Гепко // Изв. вузов. Радиоэлектроника. — 2001. — № 11 — 12, [ч. 1]. — С. 15—25.
4. Rothaus, O.S. On “bent” functions / O.S. Rothaus // J. Comb. Theory Ser. A. — USA: Academic Press Inc. — 1976. — №20(3). — P. 300—305.
5. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. — 2009. — Сер. №1(3). — С. 15—37.
6. Мазурков, М.И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов. — Труды Одес. нац. политехн. ун-та. — Одесса, 2013. — №1. — 40 с.
7. Дворников, В.Д. Метод формирования бент-последовательностей / В.Д. Дворников. — Доклады БГУИР, Минск, 2003. — С. 106—109.

РЕКУРЕНТНІ МЕТОДИ СИНТЕЗУ ПОСЛІДОВНОСТЕЙ З ОПТИМАЛЬНИМ ПІК-ФАКТОРОМ СПЕКТРА УОЛША-АДАМАРА

М.І. Мазурков, А.В. Соколов

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

Запропоновано три методи синтезу бінарних послідовностей з оптимальним значенням пік-фактору спектра Уолша-Адамара, які можуть бути використані для побудови C-кодів, що застосовуються в технології CDMA. На основі даних конструкцій розроблений алгоритм синтезу нескінченних сімейств послідовностей, що володіють оптимальними значеннями пік-фактору спектра Уолша-Адамара.

Ключові слова: оптимальна послідовність, яка кодує, CDMA, C-код, бент-послідовність, пік-фактор.

RECURRENT SYNTHESIS METHODS OF THE SEQUENCES WITH OPTIMAL PEAK-TO-AVERAGE POWER RATIO VALUE OF WALSH-HADAMARD SPECTRUM

M.I. Mazurkov, A.V. Sokolov

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

In this paper three methods of synthesis of binary sequences with optimal value of the peak-to-average power ratio of Walsh-Hadamard spectrum which may be used to construct C-codes used in the CDMA technology are proposed. On the basis of these structures an synthesis algorithm of infinite families of sequences having optimal value of peak-to-average power ratio of Walsh-Hadamard spectrum is developed.

Keywords: optimal coding sequence, CDMA, C-code, bent-sequence, PAPR.

PREPROCESSING OF DIGITAL IMAGE FOR COMPRESSION

O.V. Narimanova, A.R. Agadzhanyan, M.S. Kuchma

Odesa National Polytechnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: semejka@ua.fm, maricha705@gmail.com

Work is devoted to development of technique of preprocessing of digital image on the basis of replacement of left and right singular vectors corresponding to the maximum singular number in blocks of matrix by n -optimum vector to improve the quality of digital image compression (DI) while saving it in JPEG. The criteria of DI compression quality in this study are the volume of DI file after saving and the values of quantitative indicators of both whole and local digital image perception reliability. These quantitative indicators are used according to the previously developed by authors technique of quantitative assessment of digital image perception reliability. The results of computational experiments that confirm the effectiveness of proposed technique usage are shown.

Keywords: compression, digital image (DI), JPEG, preprocessing.

Introduction

With the development of computer technology and the extensive use of multimedia content more and more information is held in the form of digital image (DI). They are subject to stringent requirements regarding the volume of compressed data and recovered image quality with regard to computational complexity of the compression algorithms. In connection with this the problem of improvement of digital image compression algorithms is important.

The most widely used format for storing DI is JPEG, which provides high compression with acceptable levels of perception reliability of the compressed image. JPEG lossy compression method perfectly handles images with continuous tones, in which close pixels usually have similar colors. An important advantage of the JPEG method is a large number of configurable options that user can choose at his discretion, in particular, he can adjust the percentage of loss of information, and, hence, the compression ratio in a wide range [1].

In this paper the method of digital image preprocessing to reduce DI file size while JPEG compression is considered.

Images preprocessing usually contributes to the improvement of characteristics of compressed data (in this case — DI matrices), which in turn increases the final degree of compression.

As it is known [2], the singular values and singular vectors obtained by normal singular value decomposition uniquely and comprehensively characterize the DI matrix (matrices), and therefore can be considered as a complete set of DI parameters.

As a preprocessing in this paper it is considered the process of compression of digital images, based on the change of certain singular vectors obtained using the normal singular value decomposition [2] of the image matrix blocks.

Purpose of study and problem formulation

The *aim* of this work is to develop a method for digital images preprocessing to improve the quality of compression while saving DI in JPEG.

To achieve the aim it is necessary to:

1. Suggest the possibility of improving the DI compression quality based on the change of certain parameters of the complete set of DI parameters;
2. Formulate the basic steps of DI preprocessing method;
3. Select the criteria for assessing the quality of DI compression;
4. Carry out the computational experiments to assess the quality of the compression according to the selected criteria;
5. Carry out a comparative analysis of the JPEG compression algorithm with and without proposed DI preprocessing.

Main section

So, as the complete set of DI parameters it is proposed to use the singular values and singular vectors of DI matrix (matrices) obtained using the normal singular value decomposition. However, during the DI analysis or processing singular value decomposition is not accepted to apply to the entire DI matrix (matrices) virtue of its (their) high dimension. So to start the original image is divided into non-overlapping blocks B of size $n \times n$ pixels.

Singular value decomposition is applied to each block of the image.

Let B be $n \times n$ -matrix with elements $b_{ij}, i, j = \overline{1, n}$. It is true singular value decomposition of B :

$$B = U \Sigma V^T, \quad (1)$$

where U, V are the orthogonal matrices of dimension $n \times n$ containing left $u_1, \dots, u_n$ and right $v_1, \dots, v_n$ singular vectors of matrix B accordingly;

$\Sigma = \text{diag}(\sigma_1, \dots, \sigma_n)$ is a diagonal matrix containing singular values $\sigma_i, i = \overline{1, n}$, $\sigma_1 \geq \dots \geq \sigma_n \geq 0$.

Further let's assume that blocks B of DI matrices are non-degenerate and have pairwise distinct singular values $\sigma_i, i = \overline{1, n}$. Then it is possible to build a single normal singular value decomposition (1), in which the left (right) singular vector are lexicographically positive [3].

In [3] on the basis of the Frobenius theorem is shown that the singular vectors u_1, v_1 of DI matrices blocks corresponding to the largest singular values σ_1 are close to the n -optimal vector [4] of corresponding dimension, which is also confirmed by computational experiments.

As it is known, most DI compression algorithms, including JPEG, are based on reducing a variety of the values of certain parameters defining the images which leads to smaller and simpler method of encoding, which in its turn reduces the size of the DI file.

For example, in the process of compression according to JPEG the quantization of discrete cosine transform (DCT) coefficients of DI matrix blocks of 8×8 is used [1, 5]:

$$\overline{u_{ij}} = [u_{ij} / q_{ij}], \quad (2)$$

where $\overline{u_{ij}}$ is a value of DCT coefficient u_{ij} the next DI matrix block 8×8 after quantization, $u_{ij} \in R$, $\overline{u_{ij}} \in Z$, $i, j = \overline{1, 8}$;

q_{ij} is a quantization coefficient corresponding to u_{ij} , $q_{ij} \in Z$,

[•] is an operation of rounding an argument to the nearest integer.

The process of quantization of DI DCT coefficients during JPEG compression is studied in detail in [5]. In the quantization of DCT coefficients (2) as a result of rounding their domain of definition from the set of real numbers goes into the set of integers. Moreover, due to the division of values u_{ij} by quantization coefficient q_{ij} the range of $\overline{u_{ij}}$ compared to u_{ij} reduces the q_{ij} time, which also reduces the number of possible taken values of $\overline{u_{ij}}$.

In connection with all aforesaid in this paper as a DI preprocessing for compression in JPEG it is proposed to replace singular vectors u_1, v_1 by n -optimal vector of the corresponding dimension in each block of DI.

It is assumed that such replacement of vectors u_1, v_1 , at first, does not lead to significant distortion of DI, since the first singular vectors u_1, v_1 are near n -optimal vector [3]. Secondly, it is assumed that reduction the variety of values of the first singular vectors of DI matrix blocks (which corresponds to the general concept of compression algorithms constructing) will improve the quality of compression in JPEG.

In this paper, we propose to use two criteria of DI compression quality:

- size of DI file after saving;
- values of PSNR and PSNR4 in accordance with the previously developed by the authors method of assessment the digital image perception reliability [6].

The main steps of the method of DI preprocessing for compression:

1. Split the DI matrix into blocks B by $n \times n$ pixels;
2. Apply the normal singular value decomposition to each block B ;
3. In each block B replace the left u_1 and the right v_1 vectors corresponding to the maximal singular value σ_1 by n -optimal vector of the corresponding dimension;
4. Change other vectors u_i and v_j , $i, j = \overline{2, n}$ in each block, so that the matrices U, V (1) contained orthonormal singular vectors;
5. Obtain the image matrix;
6. Save DI in JPEG.

For color images represented by multiple matrices the proposed preprocessing can be carried out for one or several matrices.

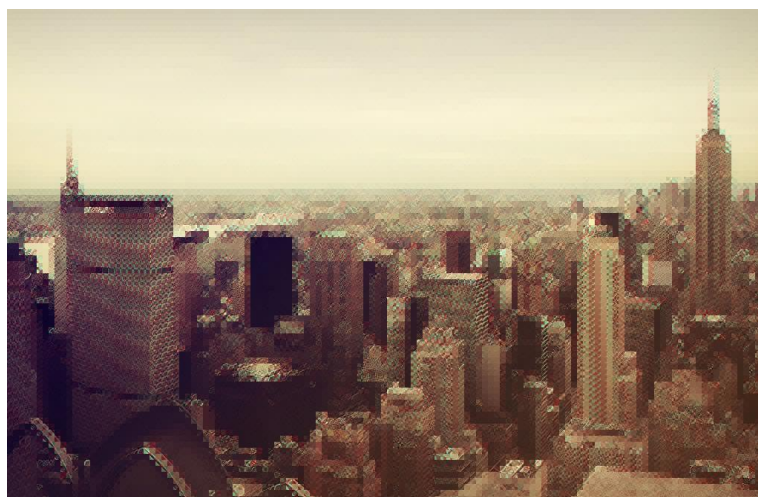
Results of computational experiment

To test the effectiveness of developed method the computational experiment is carried out with the participation of more than 100 DI. During the DI preprocessing in accordance with the developed method by using a variety of block B sizes $n = \{8, 4, 2\}$ are recorded the image file size and values of two parameters: PSNR to evaluate the perception reliability of DI in general and PSNR4 to estimate the local DI visual distortion [6].

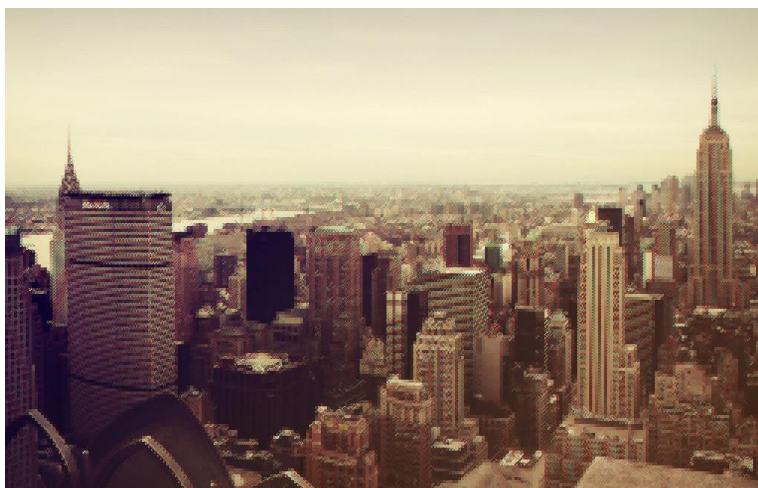
Computational experiment shows that partitioning of the image matrix into blocks of size $n = \{8, 4\}$ during the processing of all three RGB components the DI undergoes significant visual distortions, which can be seen both by values of PSNR, PSNR4 and expert assessment. An example of DI after preprocessing with different block sizes is shown on Figure 1.

An example of DI processing, shown on Fig. 1, except the violations of perception reliability is indicative from the point of the small (compared to the size of the original DI) file size reduction with increasing the size of the blocks $n \times n$. So, there is a significant deterioration of the perception reliability during the changing values from $n = 2$ to $n = 4$ and

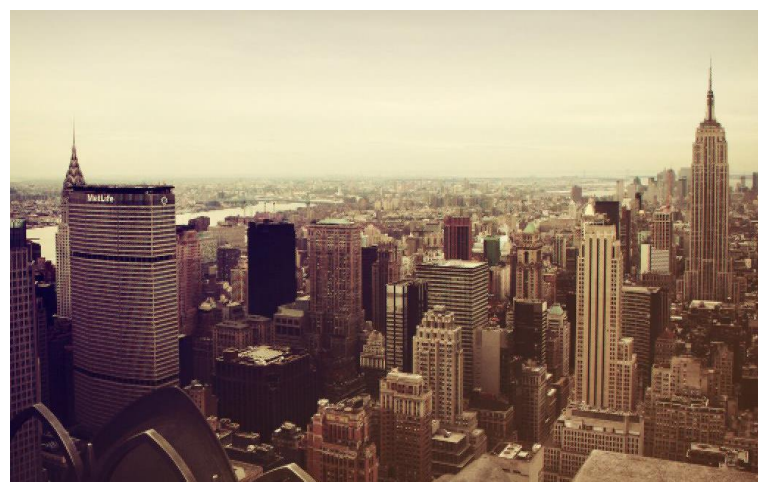
$n = 8$, but significant reduction in file size is not happening. Obviously, the parameter n allows to adjust the compression quality of DI.



a



b



c

Fig. 1. Digital image (file size is 277.350 KB) after preprocessing with blocks of size: a - 8×8 pixels, file size is 91.639 KB; b - 4×4 pixels, file size is 101.850 KB; c - pixels, file size is 107.064 KB

During the computational experiment it is found that to maintain the DI perception reliability during preprocessing only the blue component of the image matrix should be changed with the blocks 2×2 . Examples of DI after such preprocessing are shown on Fig. 2 and 3.



Fig. 2. Digital image: a - without preprocessing, file size is 281.339 KB; b - after preprocessing with blocks of 2×2 pixels, file size is 103.224 KB, PSNR=37.11

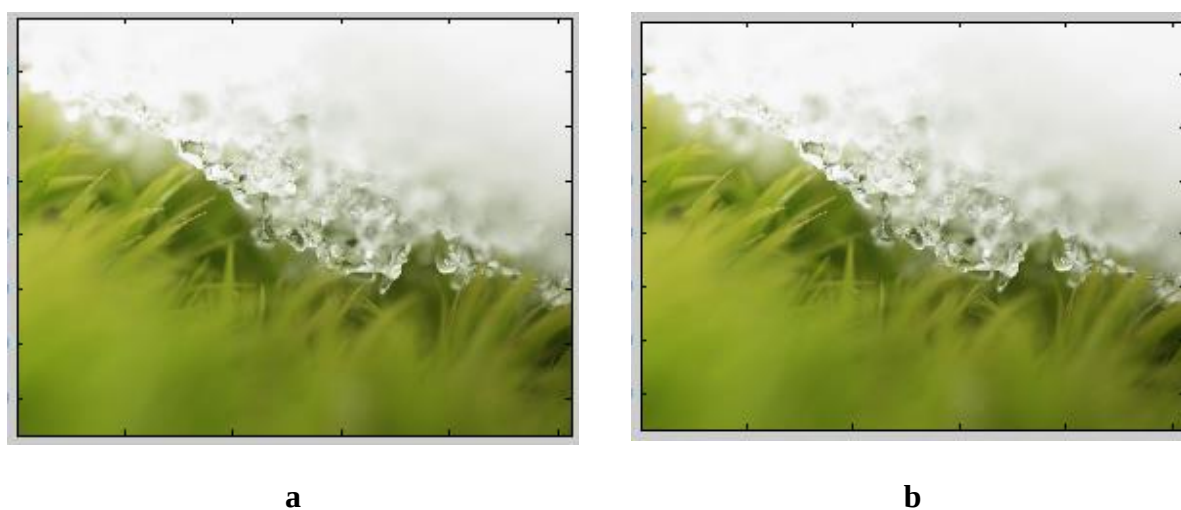


Fig. 3. Digital image: a - without preprocessing, file size is 80.863 KB; b - after preprocessing with blocks of 2×2 pixels, file size is 42.049 KB, PSNR=45.69

The experimental results in processing only the blue component of the image when $n = 2$ for fifteen randomly selected DI are shown in Table 1.

As can be seen from the results shown in Table 1, when values of perception reliability parameters PSNR and PSNR4 are acceptable the DI file size after processing by proposed method reduces on 35 — 50% as compared to DI before processing. At the same time high values of PSNR4 close to the PSNR value indicate a lack of local violations of DI perception reliability, which confirms a high image quality after compression.

Table 1.

Results of DI preprocessing with following saving in JPEG

N	DI file size before preprocessing, KB	DI file size after preprocessing, KB	PSNR value	PSNR4 value
1	767	296	39.6	37.6
2	152	76.5	40.6	38.6
3	281	103	35	33
4	277	114	33	29
5	166	66	38	36.9
6	817	309	41.6	41
7	391	184	30.6	28
8	80	42	44	42
9	429	220	36	33
10	630	224	39	38
11	336	199	39	37
12	845	439	37	34
13	781	294	36	33
14	204	112	45.6	42
15	457	244	34	33

When carrying out the computational experiments after replacing the first singular vectors the images are saved in JPEG format with the default settings. To evaluate the effectiveness of the work of developed method of DI preprocessing for compression the comparative analysis with the JPEG method as the most common modern analogue is conducted.

To be able to carry out such comparative analysis the DI is subjected to such two independent processing:

- saving in JPEG with low quality coefficient (usually with a value of 60%);
- preprocessing in accordance with the developed method with following saving in JPEG with the default settings.

The quality coefficient of 60%, while saving in JPEG leads to visual distortions, comparable to the violation of DI perception reliability during preprocessing in accordance with the developed method. Thus, one of the criteria for comparative assessing the quality of the two compression methods receives similar values, and comparative analysis can be carried out on the second criterion — the size of the DI file. Fig. 4 shows an example of DI, which participated in a comparative analysis.

According to the results of comparative analysis the developed method of DI preprocessing for compression no worse than JPEG compression according to values of selected criteria, however, does not exceed it considerably. At the same time the expert assessment of DI perception reliability after compression revealed some qualitative differences between results of compared methods.

Thus when compressing DI with low values of quality coefficient (JPEG) visual distortions can be seen in blurred contours and the appearance of «squares» in the background parts of image (for example, Fig. 5, *a*). When carrying out the preprocessing with developed method with the following saving in JPEG format with high quality coefficient there are no visible visual disturbances in the images (e.g., Fig. 5, *b*). At the same time the DI file sizes after processing with both compared methods are similar.

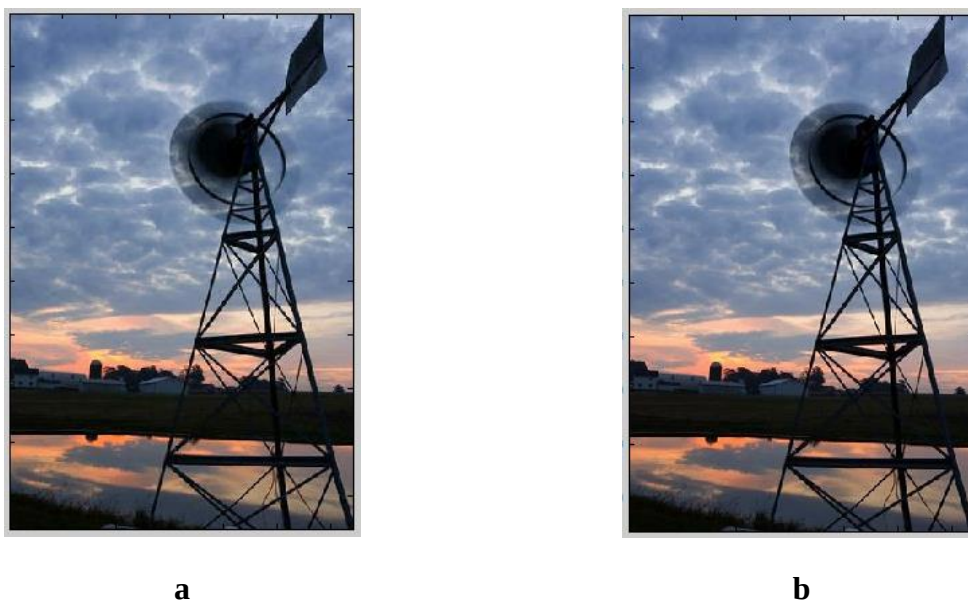


Fig. 4. Digital image: a - after saving in JPEG, PSNR=35.828, file size is 25.497 KB; b - after preprocessing, PSNR=35.824, file size is 24.689 KB

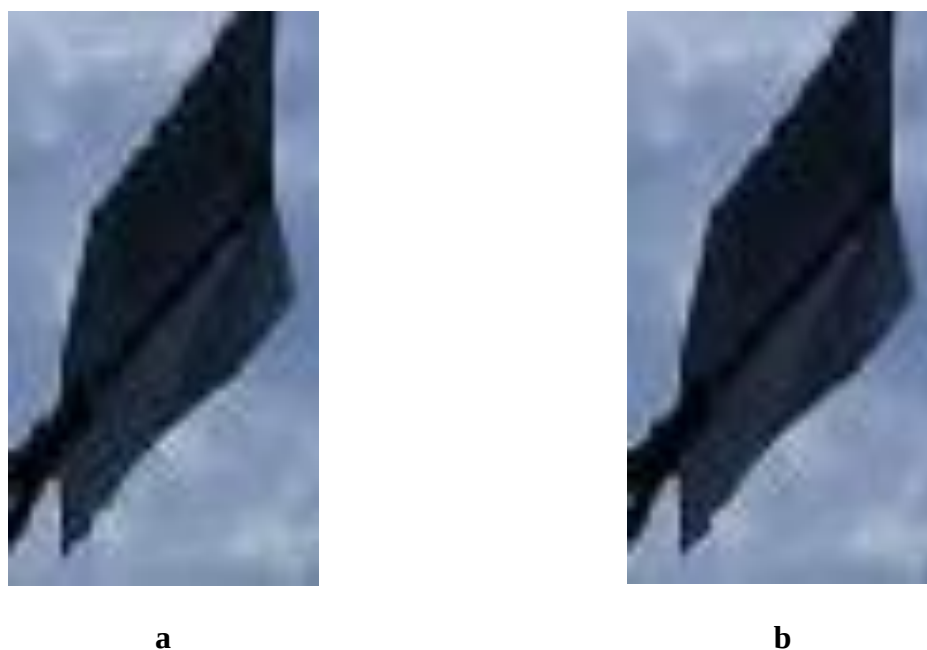


Fig. 5. Fragment of digital image: a - after saving in JPEG; b - after preprocessing and saving in JPEG

Conclusions

It is developed the method of preprocessing the digital image based on the replacement of the left and right singular vectors corresponding to the maximal singular value in blocks of matrices by the n -optimal vector which allows to:

- to achieve a smaller DI file sizes at high values of quality coefficient while saving in JPEG;
- maintain a high level of DI perception reliability, avoiding artifacts typical for JPEG at low values of quality coefficient.

The usage of developed method of digital image preprocessing for compression in JPEG may be recommended in cases where preservation of image contours is essential in decreasing the size of its file.

References

1. Сэломон, Д. Сжатие данных, изображений и звука / Д. Сэломон // М.: Техносфера. — 2004. — 368 с.
2. Кобозева, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. — К.: Вид. ДУИКТ, 2010. — 316 с.
3. Кобозева, А.А. Анализ чувствительности сингулярных векторов матрицы изображения-контейнера как основа стеганоалгоритма, устойчивого к сжатию с потерями / А.А. Кобозева, М.А. Мельник // Захист інформації. — 2013. — №2. — С.49 — 58.
4. Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. — К.: Изд. ГУИКТ, 2009. — 251 с.
5. Нариманова, Е.В. Проверка целостности цифрового сигнала / Е.В. Нариманова. — Донецк: Изд. Цифровая типография, 2011. — 180 с.
6. Нариманова, Е.В. Методика количественной оценки надежности восприятия цифрового изображения / Е.В. Нариманова, Е.А Трифонова, А.Е. Килин, М.С. Кучма // Информатика та математичні методи в моделюванні.— Одеса, ОНПУ.— 2014. — Т.4, №4. — С. 332 — 336.

ПЕРЕДОБРОБКА ЦИФРОВОГО ЗОБРАЖЕННЯ ДЛЯ СТИСНЕННЯ

О.В. Наріманова, А.Р. Агаджанян, М.С. Кучма

Одеський національний політехнічний університет,
пр-т Шевченка, 1, Одеса, 65044, Україна; e-mail: semejka@ua.fm, maricha705@gmail.com

Робота присвячена розробці методу передобробки цифрового зображення на основі заміни лівого і правого сингулярних векторів, що відповідають максимальному сингулярному числу, в блоках матриці на n -оптимальний вектор для підвищення якості стиснення цифрового зображення (ЦЗ) при збереженні в форматі JPEG. Критеріями якості стиснення ЦЗ в даній роботі вважаються об'єм файлу ЦЗ після збереження і значення кількісних показників для оцінки надійності сприйняття ЦЗ в цілому і його локальних візуальних спотворень у відповідності з розробленою авторами раніше методикою кількісної оцінки надійності сприйняття цифрового зображення. Наведені результати обчислювального експерименту, що підтверджують ефективність використання розробленого методу.

Ключові слова: стиснення, цифрове зображення, JPEG, передобробка.

ПРЕДОБРАБОТКА ЦИФРОВОГО ИЗОБРАЖЕНИЯ ДЛЯ СЖАТИЯ

Е.В. Нариманова, А.Р. Агаджанян, М.С. Кучма

Одесский национальный политехнический университет,
пр-т Шевченко, 1, Одесса, 65044, Украина; e-mail: semejka@ua.fm, maricha705@gmail.com

Работа посвящена разработке метода предобработки цифрового изображения на основании замены левого и правого сингулярных векторов, соответствующих максимальному сингулярному числу, в блоках матрицы на n -оптимальный вектор для улучшения качества сжатия цифрового изображения (ЦИ) при сохранении в формате JPEG. Критериями качества сжатия ЦИ в данной работе считаются объем файла ЦИ после сохранения и значения количественных показателей для оценки надежности восприятия ЦИ в целом и его локальных визуальных искажений в соответствии с разработанной авторами ранее методикой количественной оценки надежности восприятия цифрового изображения. Приведены результаты вычислительного эксперимента, подтверждающие эффективность использования разработанного метода.

Ключевые слова: сжатие, цифровое изображение, JPEG, предобработка.

СИНТЕЗ АЛГОРИТМУ ОЦІНКИ ЧАСТОТИ КОМПЛЕКСНОГО МОНОХРОМНОГО СИГНАЛУ

І. П. Омельчук

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

Достатньо поширеними в сучасних інформаційних радіотехнічних системах стають комплексні гармонічні сигнали, зокрема, монохромні (надалі “сигнал”). При прийомі сигналу зазвичай першочергово отримується значення його частоти, від точності якої залежить якість подальшої обробки. Метою роботи є синтез квазіоптимальної оцінки частоти еквідистантно дискретизованого сигналу в явному аналітичному виді при дії гаусівської завади. Основою для цього обрано статистичний метод максимальної правдоподібності із застосуванням моделі вхідного процесу як авторегресії ковзного середнього, що дозволило при синтезі опертися на математично обґрунтовані положення та висновки. Результати роботи частково заповнюють прогалину у створенні оптимальних оцінок частоти сигналів. Доведена незміщеність оцінки. Синтезований алгоритм є достатньо зручним та корисним для практичного використання, оскільки може забезпечити підвищення точності, ефективності та швидкодії радіоприймачів в режимі реального часу.

Ключові слова: комплексний монохромний сигнал, оцінка частоти, максимальна правдоподібність, авторегресія ковзного середнього

Вступ

Найбільш поширеним класом носіїв інформації в радіотехнічних системах є гармонічні сигнали, частоти яких у більшості технічних задач підлягають першочерговому оцінюванню. Це стосується як несучої частоти, так і частот модулюючих сигналів. За відомого значення частоти розрахунки амплітуди та фази сигналу стають достатньо простими.

У сучасних приймачах вихідні процеси після первинної високочастотної фільтрації зазвичай подаються у квадратурному вигляді, що з точки зору подальшої математичної алгоритмізації їхньої обробки відповідає категорії комплексних сигналів. Монохромні є частковим видом комплексних гармонічних сигналів. Вони використовуються у випадках, коли інформація інкапсулюється у послідовності значень частоти одного сигналу, наприклад, у доплерівських радіолокаторах, що вимірюють швидкість цілі або у системах зв'язку з амплітудно-фазовою модуляцією.

Для пристроїв обробки сигналів, поряд з якісною апаратною їх реалізацією, все більшу вагу набувають вимоги покращення алгоритмічного забезпечення. Досягається це шляхом математичного синтезу оптимальних алгоритмів обробки, у тому числі оцінювання параметрів, на підставі статистичних властивостей сигналів та завад.

Аналіз останніх досліджень та публікацій

Необхідно виділити, у першу чергу, напрямок створення алгоритмів оцінювання частоти комплексного монохромного сигналу, що базується на структурному підході з використанням фазових та кореляційних властивостей сигналу [1]. Їхня евристична

різноманітність свідчить про відсутність узагальнюючої статистичної методології, яка б ґрунтовно приводила до оптимальних рішень.

Можливості сучасних цифрових технологій обумовили як найбільш перспективні ті методи оцінювання параметрів гармонічного сигналу, що базуються на обробці кривої миттєвих його значень [2, 3, 4]. Зокрема, в статті [3] синтез оцінки частоти здійснювався на підставі класичного методу максимальної правдоподібності (МП), а в роботі [4] здійснений поглиблений аналіз відомих підходів. Але результати зазначених статей, маючи суттєву методологічну значущість, торкалися лише випадку скалярного сигналу. Відчувається прогалина стосовно оптимальних алгоритмів оцінювання комплексних сигналів.

Мета роботи

У даній роботі поставлена мета отримати математично обґрунтовану квазіоптимальну оцінку (надалі утотожнюємо цей термін з поняттям алгоритм оцінювання) частоти монохромного комплексного сигналу (надалі скорочено “сигнал”) у явному аналітичному вигляді, що забезпечить підвищення ефективності та швидкодії їх обробки в режимі реального часу. Основою для синтезу обрано метод максимальної правдоподібності [5] із застосуванням математичної моделі авторегресії ковзного середнього (АРКС) вхідного процесу [6].

Математична модель вхідного процесу

Сигнал, інформаційним параметром якого вважається тільки частота, розглядається як еквідистантна з інтервалом дискретизації τ послідовність N комплексних значень

$$\dot{s}_n = s_n^{(x)} + j \cdot s_n^{(y)}, \quad \begin{cases} s_n^{(x)} = \rho \cos[\omega(n-1)\tau + \varphi_1] \equiv \rho \cos[\gamma(n-1) + \varphi_1] \\ s_n^{(y)} = \rho \sin[\omega(n-1)\tau + \varphi_1] \equiv \rho \sin[\gamma(n-1) + \varphi_1] \end{cases}, \quad n = \overline{1, N}, \quad (1)$$

з апіорно невідомими, але незмінними на інтервалі спостереження: круговою частотою ω , амплітудою ρ та початковою фазою φ_1 . У правих частинах формул (1) здійснена заміна кругової частоти на різницю фаз γ між суміжними значеннями сигналу згідно тотожності

$$\gamma \equiv \omega\tau. \quad (2)$$

Таке є доречним за відомого τ , оскільки зменшується параметрична розмірність моделі. Причому, згідно з теоремою Котельникова, повинна забезпечуватися вимога $0 < \gamma < \pi$.

Відповідно, питання оцінки кругової частоти $\hat{\omega}$ замінюється на пропорційну оцінку $\hat{\gamma}$, яка у теорії цифрової обробки [7] зазвичай називається нормованою частотою. Надалі будемо використовувати для неї скорочений термін – «частота».

Вважаємо, що вхідний процес $\{\dot{z}_n\}$, який підлягає обробці, подається у вигляді послідовності еквідистантно вимірних пар квадратурних (комплексних) відліків (x_n, y_n)

$$\dot{z}_n \equiv x_n + j \cdot y_n = \dot{s}_n + \dot{\eta}_n, \quad n = \overline{1, N}, \quad (3)$$

що утворюються як адитивна суміш сигналу та стаціонарного некорельованого

центрованого гаусівського шуму (надалі «шум») $\dot{\eta}_n \equiv \eta_n^{(x)} + j \cdot \eta_n^{(y)}$. Комплексні складові шуму є незалежними з однаковою щільністю розподілу імовірностей (ЩРІ) $f(\eta|\sigma)$ та невідомою дисперсією σ^2 .

Модель сигналу у тригонометричній формі (1) відповідає фізичній суті, але значна її нелінійність ускладнює аналітичний синтез оцінки частоти. Для еквідистантних відліків таку можливість надає інша адекватна математична модель сигналу – авторегресійна (АР) [3, 7]:

$$\begin{cases} s_n^{(x)} = \alpha s_{n-1}^{(x)} - s_{n-2}^{(x)} \\ s_n^{(y)} = \alpha s_{n-1}^{(y)} - s_{n-2}^{(y)} \end{cases}, \quad n = \overline{3, N}, \quad (4)$$

де параметр авторегресії α пов'язаний з частотою як

$$\alpha = 2 \cos(\gamma). \quad (5)$$

Вочевидь, авторегресійна модель (4) є інваріантною до початкової фази сигналу, тобто її форма однакова для синусної та косинусної складових. Окрім того в АР-моделі відсутня у явному вигляді амплітуда сигналу; вона залежить лише від перших двох значень у послідовності (4). Таким чином, задача оцінювання зводиться до однопараметричної, а саме, оцінювання параметра авторегресії α .

На підставі визначеної вище сигнально-зададової ситуації математичну модель вхідного процесу можна подати у такому вигляді:

$$\dot{z}_n = \dot{s}_n + \dot{\eta}_n \equiv \alpha \dot{s}_{n-1} - \dot{s}_{n-2} + \dot{\eta}_n, \quad n = \overline{3, N}, \quad (6)$$

де, замінивши згідно з формулою (3) $\dot{s}_{n-1} = \dot{z}_{n-1} - \dot{\eta}_{n-1}$ та $\dot{s}_{n-2} = \dot{z}_{n-2} - \dot{\eta}_{n-2}$, отримаємо

$$\dot{z}_n = (\alpha \dot{z}_{n-1} - \dot{z}_{n-2}) + (\dot{\eta}_n - \alpha \dot{\eta}_{n-1} + \dot{\eta}_{n-2}), \quad n = \overline{3, N}. \quad (7)$$

Це рекурентне рівняння описує модель авторегресії (перші дужки) ковзного середнього (другі дужки) порядку (2, 2) із збуджуючим гаусівським шумом – АРКС-модель. Принциповим моментом отриманої АРКС-моделі є залежність від параметру α як авторегресійної складової, так і ковзного середнього (КС).

Якщо АР-складову розглядати як функцію лінійного прогнозування з використанням деякої оцінки параметра авторегресії $\hat{\alpha}$

$$\hat{z}_n = \hat{\alpha} \hat{z}_{n-1} - \hat{z}_{n-2}, \quad n = \overline{3, N},$$

то для визначення якості оцінки цього параметра доцільно обирати нев'язки $\{\dot{v}_n(\hat{\alpha})\}$, що також є комплексними, між фактично вимірним значенням та спрогнозованим

$$\dot{v}_n(\hat{\alpha}) \equiv \dot{v}_n^{(y)}(\hat{\alpha}) + j \cdot \dot{v}_n^{(x)}(\hat{\alpha}) = \dot{z}_n - \hat{z}_n \equiv \dot{z}_n - \hat{\alpha} \hat{z}_{n-1} + \hat{z}_{n-2}, \quad n = \overline{3, N}. \quad (8)$$

Статистичні властивості АРКС-моделі

З іншого боку, згідно АРКС-моделі (7) та визначенням нев'язки (8), маємо

$$\dot{v}_n(\alpha) = \dot{\eta}_n + \alpha \dot{\eta}_{n-1} - \dot{\eta}_{n-2} \quad (9)$$

(позначення оцінки тильдою для спрощення надалі упускаємо). Тобто стохастичні властивості АРКС-моделі повністю визначаються її КС-процесом. Розглянемо ці властивості більш детально на прикладі уявної складової $\dot{v}_n^{(y)}$ однієї n -ї нев'язки (9), що

однаково й для інших.

Математичне очікування (МО) E суми центрованих гаусівських величин $m_v = E(\nu_n^{(y)}) = 0$. Тоді дисперсію уявної складової визначаємо як

$$\begin{aligned}\sigma_v^2 &= \int_{-\infty}^{\infty} (\eta_n^{(y)} - \alpha \eta_{n-1}^{(y)} + \eta_{n-2}^{(y)})^2 f(\eta | \sigma) d\eta = \\ &= \int_{-\infty}^{\infty} [(\eta_n^{(y)})^2 + \alpha^2 (\eta_{n-1}^{(y)})^2 + (\eta_{n-2}^{(y)})^2] f(\eta | \sigma) d\eta = \sigma^2 (2 + \alpha^2)\end{aligned}\quad (10)$$

При цьому, на підставі некорельованості шуму, використовувалася властивість

$$E(\eta_k^{(y)} \cdot \eta_m^{(y)}) = 0, \quad \forall k \neq m. \quad (11)$$

У загальному випадку коефіцієнти кореляції між величинами $\nu_n^{(y)}(\alpha)$ та $\nu_{n-k}^{(y)}(\alpha)$, що мають затримку у k інтервалів дискретизації, визначаються за формулою

$$r_k^{(y)} = \frac{1}{\sigma_v^2} \int_{-\infty}^{\infty} (\eta_n^{(y)} - \alpha \eta_{n-1}^{(y)} + \eta_{n-2}^{(y)}) (\eta_{n-k}^{(y)} - \alpha \eta_{n-1-k}^{(y)} + \eta_{n-2-k}^{(y)}) f(\eta | \sigma) d\eta.$$

Вочевидь, $r_0^{(y)} = 1$, $r_k^{(y)} = 0$, $\forall k > 2$, а коефіцієнти кореляції з одиничною та подвійною затримкою, з урахуванням властивості (11), визначаються як

$$\begin{aligned}r_2^{(y)} &= -\frac{\alpha}{\sigma_v^2} \int_{-\infty}^{\infty} [(\eta_{n-1}^{(y)})^2 + (\eta_{n-2}^{(y)})^2] f(\eta | \sigma) d\eta = -\frac{2\alpha}{2 + \alpha^2}, \\ r_1^{(y)} &= \frac{1}{\sigma_v^2} \int_{-\infty}^{\infty} (\eta_n^{(y)})^2 f(\eta | \sigma) d\eta = \frac{1}{2 + \alpha^2}.\end{aligned}$$

Тобто кореляційна матриця $R^{(y)}(\alpha)$ має діагональний вигляд, де елементи головної діагоналі – одиниці; елементи діагоналей по обидва боки від головної на відстані одного кроку однакові та становлять $r_1^{(y)}$; елементи діагоналей на відстані двох кроків – $r_2^{(y)}$.

Запишемо сумісну ЩРІ уявних складових усіх нев'язок у такому вигляді [5]:

$$f^{(y)}(\vec{\nu}^{(y)} | \alpha, \sigma) = \frac{1}{(2\pi)^{N/2-1} [\sigma_v(\alpha, \sigma)]^{N-2} [D(\alpha)]^{1/2}} \exp \left[-\frac{1}{D(\alpha)} \sum_{n=3}^N \sum_{i=3}^N \frac{d_{in}^{(y)}(\alpha) \cdot \nu_i^{(y)}(\alpha) \cdot \nu_n^{(y)}(\alpha)}{2[\sigma_v(\alpha, \sigma)]^2} \right], \quad (12)$$

де $\vec{\nu}^{(y)} \equiv \{\nu_n^{(y)}(\alpha)\}$, $D(\alpha) = |R^{(y)}(\alpha)|$ – визначник кореляційної матриці $R^{(y)}(\alpha)$ нев'язок; $d_{in}^{(y)}(\alpha)$ – алгебраїчне доповнення елемента $r_{in}^{(y)}$ визначника $D(\alpha)$.

Оскільки квадратурні канали вважаємо статистично ідентичними, то все залишається аналогічним для дійсної складової нев'язок: $R^{(x)}(\alpha) = R^{(y)}(\alpha)$, $d_{in}^{(x)}(\alpha) = d_{in}^{(y)}(\alpha) \equiv d_{in}(\alpha)$.

З урахуванням некорельованості шуму, запишемо сумісну ЩРІ комплексних нев'язок, яку будемо використовувати як функцію правдоподібності (ФП) для синтезу оцінки частоти:

$$\begin{aligned} f^{(yx)}(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma) &= f^{(x)}(\vec{v}^{(x)} | \alpha, \sigma) \cdot f^{(y)}(\vec{v}^{(y)} | \alpha, \sigma) = \\ &= \frac{1}{(2\pi\sigma_v^2)^{(N-2)} D} \exp[-\Lambda(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma)] \end{aligned} \quad (13)$$

(залежність величин від параметрів упущено), де на підставі ЦПІ (12) визначена статистика

$$\Lambda(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma) = \frac{1}{2D\sigma_v^2} \sum_{i=3}^N \sum_{n=3}^N d_{in} [v_i^{(x)} \cdot v_n^{(x)} + v_i^{(y)} \cdot v_n^{(y)}]. \quad (14)$$

Логарифм ФП (13) запишемо як

$$\ln f^{yx}(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma) = -(N-2) \ln 2\pi - \ln D - 2(N-2) \ln \sigma_v - \Lambda(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma). \quad (15)$$

Синтез алгоритму оцінювання частоти

Використаємо класичний метод максимальної правдоподібності, за яким оптимальні оцінки параметрів α та σ повинні визначатися як розв'язок системи двох рівнянь правдоподібності, що утворюються на підставі отриманого логарифму ФП (15):

$$\begin{cases} \frac{\partial}{\partial \alpha} \ln f^{yx}(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma) = 0 \\ \frac{\partial}{\partial \sigma} \ln f^{yx}(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma) = 0 \end{cases}. \quad (16)$$

Але суттєва нелінійність цих рівнянь не дозволяє знайти розв'язок у явній формі. Для спрощення задачі припустимо незалежність між собою всіх значень послідовності $\{\dot{v}_n\}$; тоді маємо: $d_{in} = 1, \forall i = n$; $d_{in} = 0, \forall i \neq n$, $D = 1$, а статистика (14) набуде наступного виду:

$$\Lambda(\vec{v}^{(x)}, \vec{v}^{(y)} | \alpha, \sigma) \approx \frac{1}{2\sigma_v^2} \Sigma_{x,y}(\alpha), \quad (17)$$

де використане позначення

$$\Sigma_{x,y}(\alpha) = \sum_{i=3}^N \left\{ [v_i^{(x)}(\alpha)]^2 + [v_i^{(y)}(\alpha)]^2 \right\}. \quad (18)$$

За таких умов з першого рівняння (16) отримаємо рівняння правдоподібності

$$-2(N-2) \frac{\sigma'_v}{\sigma_v} + \frac{\sigma'_v}{\sigma_v^3} \Sigma_{x,y} \alpha - \frac{1}{2\sigma_v^2} \Sigma'_{x,y} \alpha = 0. \quad (19)$$

З формули (10) маємо $\sigma_v = \sigma \sqrt{2 + \alpha^2}$, відповідно $\sigma'_v = \frac{\partial \sigma_v}{\partial \alpha} = \frac{\alpha \sigma}{\sqrt{2 + \alpha^2}}$, з

урахуванням чого після зведення (19) до спільного знаменника $-2\sigma^2(2 + \alpha^2)^2$

чисельник набуває вигляду

$$4(N-2)\alpha(2+\alpha^2)\sigma^2 + (2+\alpha^2)\Sigma'_{x,y}(\alpha) - 2\alpha\Sigma_{x,y}(\alpha) = 0. \quad (20)$$

Рівняння правдоподібності (20) є кубічним відносно невідомого параметра α та залежить від потужності шуму σ^2 . Якщо зробити ще одне припущення про незначний рівень шуму та знехтувати у рівнянні (20) першим доданком, то отримаємо квадратне рівняння відносно однієї невідомої змінної α

$$\alpha^2\Sigma'_{x,y}(\alpha) - 2\alpha\Sigma_{x,y}(\alpha) + 2\Sigma'_{x,y}(\alpha) = 0. \quad (21)$$

Враховуючи, що (див. (18))

$$\Sigma'_{x,y}(\alpha) = -2[x_{n-1}(x_n - \alpha x_{n-1} + x_{n-2}) + y_{n-1}(y_n - \alpha y_{n-1} + y_{n-2})],$$

рівняння (21) після тотожних перетворень подамо у наступному вигляді:

$$A\alpha^2 + B\alpha - 2A = 0, \quad (22)$$

коефіцієнти якого визначаються такими формулами:

$$A = \sum_{i=3}^N [(x_n + x_{n-2})x_{n-1} + (y_n + y_{n-2})y_{n-1}], \quad (23)$$

$$B = \sum_{n=3}^N [2x_{n-1}^2 - (x_n + x_{n-2})^2 + 2y_{n-1}^2 - (y_n + y_{n-2})^2].$$

Квадратне рівняння (22) завжди має два дійсні корені:

$$\alpha_{1,2} = (-B \pm \sqrt{B^2 + 8A^2}) / 4A, \quad (24)$$

один з яких дає правильну оцінку параметра $\hat{\alpha}$, за якою далі розраховуються оцінки нормованої та кругової частоти сигналу як

$$\hat{\gamma} = \arccos(\hat{\alpha} / 2), \quad \hat{\omega} = \hat{\gamma} / \tau.$$

Правило вибору вірного кореню з двох (24) обґрунтовується у наступному пункті.

Необхідно зазначити, що отриманий в даній роботі алгоритм оцінювання частоти внаслідок декількох прийнятих у процесі синтезу припущень є квазіоптимальним. Причому, оцінювання дисперсії шуму $\hat{\sigma}$ не вимагається; тобто друге рівняння правдоподібності системи (16) для синтезу оцінки частоти фактично не використовується.

Асимптотичний аналіз помилки оцінки частоти

Для визначення асимптотичної помилки оцінки параметра сигналу $\hat{\alpha}$ замінімо у виразах (23) відліки x_n та y_n відповідними значеннями сигналу $\dot{s}_n$ у тригонометричній формі без шуму. Скориставшись тотожностями: $s_{n+1}^{(y)} + s_{n-1}^{(y)} \equiv 2\rho \sin \phi_n \cos \gamma$,

$s_{n+1}^{(x)} + s_{n-1}^{(x)} \equiv 2\rho \cos \phi_n \cos \gamma$, де ϕ_n – повна фаза n -го значення, та $[s_n^{(x)}]^2 + [s_n^{(y)}]^2 \equiv \rho^2$, після перетворень отримаємо коефіцієнт $B = 2\rho(1 - 2\cos^2 \gamma)$. Подібним чином отримується коефіцієнт $A = 2\rho \cos \gamma$. Підставимо ці коефіцієнти у формулу (24), та скоротивши чисельник та знаменник на 2ρ , маємо:

$$\alpha_{1,2}(\gamma) = \frac{(2\cos^2 \gamma - 1) \pm \sqrt{(2\cos^2 \gamma - 1)^2 + 8\cos^2 \gamma}}{\cos \gamma} = \frac{(2\cos^2 \gamma - 1) \pm (2\cos^2 \gamma + 1)}{\cos \gamma},$$

звідки корені становлять: $\alpha_1(\gamma) = 2\cos \gamma$ та $\alpha_2(\gamma) = 1/\cos \gamma$. Тобто необхідно завжди використовувати корінь з плюсом перед детермінантом.

Для зменшення кількості операцій доцільно перетворити коефіцієнт B (23) до вигляду

$$B = -\left(x_n^2 - x_{n-1}^2 + 2\sum_{n=3}^N x_n x_{n-2} - x_2^2 + x_1^2 + y_n^2 - y_{n-1}^2 + 2\sum_{n=3}^N y_n y_{n-2} - y_2^2 + y_1^2\right),$$

а рівняння (22), використавши додатковий коефіцієнт $G = \frac{-B}{2A}$, подати як

$$\alpha^2 - 2G - 2 = 0.$$

Тоді вірний корінь розраховується за формулою

$$\alpha_1 = G + \text{sign}(A)\sqrt{G^2 + 2},$$

де функція $\text{sign}(A) = \begin{cases} +1 & A \geq 0 \\ -1 & A < 0 \end{cases}$ забезпечує зміну знаку перед детермінантом за від'ємного A .

Висновки

1. Еквідистантну вибірку квадратурної суміші гармонічного сигналу та адитивного некорельованого гаусівського шуму можна подати у вигляді математичної АРКС-моделі.

2. Застосування АРКС-моделі дозволяє за методом МП синтезувати квазіоптимальну оцінку частоти комплексного гармонічного сигналу в явному аналітичному виді.

3. Асимптотична похибка синтезованої АРКС-оцінки частоти дорівнює нулю.

Список літератури

1. Fu, H. Phase-based, time-domain estimation of the frequency and phase of a single sinusoid in AWGN – the role and applications of the additive observation phase noise model / H. Fu, P. Kam // IEEE: Transactions on information theory. – 2013. – Vol.59, № 5. – Pp. 3175–3188.
2. Никитин, А.В. Измерение мгновенной частоты широкополосных сигналов на коротком интервале наблюдения / А.В. Никитин, С.В. Юшанов // Измерительная техника. – 2008. – №2. – С. 50–54.
3. Прокопенко, І.Г. Квазіоптимальна оцінка частоти гармонічного сигналу на обмеженому інтервалі спостереження / І.Г. Прокопенко, І.П. Омельчук // Електроніка та системи управління. – 2009. – № 1 (19). – С. 39–45.

4. Каюков, Н.В. Сравнительный анализ различных методов оценки частоты сигналов / Н.В. Каюков, В.Б. Манелис // Радиоэлектроника. – 2006. – №7. – С. 42–56.
5. Левин, Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Радио и связь, 1989. – 656 с.
6. Бокс, Дж. Анализ временных рядов: прогноз и управление / Дж. Бокс, Г. Дженкинс. – М.: Мир, 1974. – Вып. 1. – 406 с.
7. Марпл-мл, С.Л. Цифровой спектральный анализ и его приложения / С. Л. Марпл-мл. – М.: Мир, 1990. – 584 с.

СИНТЕЗ АЛГОРИТМА ОЦЕНИВАНИЯ ЧАСТОТЫ КОМПЛЕКСНОГО МОНОХРОМНОГО СИГНАЛА

И. П. Омельчук

Национальный авиационный университет
пр. Космонавта Комарова, 1, Киев, 03058, Украина, e-mail: omelip@ukr.net

Достаточно распространёнными в современных информационных радиотехнических системах становятся комплексные гармонические сигналы, в частности, монохромные (далее «сигнал»). При приёме сигнала обычно в первую очередь определяется значение его частоты, от точности которой зависит качество последующей обработки. Целью работы является синтез квазиоптимальной оценки частоты эквидистантно дискретизированного сигнала в явном аналитическом виде при действии гаусовских помех. Основой для этого выбран статистический метод максимальной правдоподобности с использованием модели входного процесса в виде авторегрессии скользящего среднего, что позволило при синтезе опереться на математически обоснованные положения и выводы. Показана несмещённость оценки. Результаты работы частично заполняют пробел в создании оптимальных оценок частоты сигнала. Синтезированный алгоритм является достаточно удобным и полезным для практического применения, поскольку может обеспечить повышение точности, эффективности и быстродействия радиоприёмников в режиме реального времени.

Ключевые слова: комплексный монохромный сигнал, оценка частоты, максимальная правдоподобность, авторегрессия скользящего среднего

SYNTHESIS OF THE FREQUENCY ESTIMATION ALGORITHM FOR A SINGLE-TONE COMPLEX SIGNAL

I. P. Omelchuk

National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, 03058, Ukraine, e-mail: omelip@ukr.net

Complex harmonic signals, particularly single-tone (further called «signal») become spread enough in modern information systems. During the reception of the signal value of its frequency is usually obtained firstly and its accuracy influences on the quality of further processing. The aim of the work is the synthesis of the sub-optimal frequency estimator for the equidistantly sampled signal in explicit analytic form under the action of Gaussian noise. The basis for this is a statistical maximum likelihood method. The autoregressive moving average model of the input process allowed the synthesis rely on mathematically grounded position and conclusions. The results partially fill the gap in creation of optimal signal frequency estimators. The estimator unbiasedness is proven. The synthesized algorithm is quite convenient and useful for practical use because it can provide improvement of the accuracy, efficiency and processing speed of receivers in real time.

Keywords: single-tone signal, complex, autoregressive moving average, frequency, estimation, maximum likelihood.

РАСЧЕТ ОБЛАСТЕЙ СОСУЩЕСТВОВАНИЯ ФАЗ В СИСТЕМЕ $In_xGa_{1-x}Sb_yAs_{1-y}$

А.И. Казаков, Л.Т. Кваташидзе, Г.В. Шаповалов

Одесский национальный политехнический университет
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: anatkaz@mail.ru

В рамках модели регулярного раствора и стандартных термодинамических функций, использованных для описания состояний бинарных соединений и взаимодействия атомов в четырехкомпонентных твердых растворах, были рассчитаны высшие производные свободной энергии гомогенного твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$ со смешением в двух подрешетках с третьей по восьмую производную включительно. Аналитические выражения для производных, численные расчеты и определение нулевых контуров высших производных проводились на основе дифференциального топологического подхода с использованием системы компьютерной математики *Math*. В четырехмерном концентрационном пространстве были рассчитаны сечения фазовой диаграммы твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$, критические пространства и пространства сосуществования фаз для различных температур. Результаты расчетов указывают на возможность формирования областей сосуществования фаз второго порядка в твердых растворах $In_xGa_{1-x}Sb_yAs_{1-y}$, что не противоречит имеющимся экспериментальным данным.

Ключевые слова: дифференциальный топологический подход, твердые растворы, пространства сосуществования фаз, многокомпонентные системы, матричные производные.

Введение

Четырехкомпонентные твердые растворы на основе соединений типа A_3B_5 в настоящее время являются перспективными материалами для изготовления оптоэлектронных приборов на основе эпитаксиальных гетеропереходов, предназначенные для работы в широком спектральном диапазоне. В связи с этим значительный интерес вызывают исследования проблемы самоорганизованного образования упорядоченных структур во многокомпонентных полупроводниковых твердых растворах с неоднородным распределением концентраций компонентов, в которых возникают «квантовые точки», периодические структуры, сверхрешетки, и другие наноструктуры. Привлечение компьютерного моделирования для анализа процессов получения самоорганизовано образующихся упорядоченных наноструктур позволяет рассчитать многомерные фазовые диаграммы, учитывающие возможность существования бифуркационных пространств, критических пространств и пространств сосуществования фаз различных порядков.

Термодинамический подход к описанию фазовых переходов в многокомпонентных системах, позволяющий анализировать особенности потенциальных функций нескольких параметров порядка, позволяет использовать теорию катастроф для самоорганизующихся систем, рассматривая ее как обобщенную форму теории фазовых переходов Гинзбурга-Ландау [1]. Уравнение состояния строится на некотором n -мерном многообразии в соответствующем пространстве. Критерием для определения пространств сосуществования фаз является ситуация, при которой

одно стабільне состояние системи сосушествует с другим стабільным состоянием. Процесс возникновение такого пространства является фазовым переходом первого рода по принципу Максвелла. При этом два или несколько глобальных минимумов потенциальной функции будут иметь одинаковую глубину. Внутри изучаемого фазового пространства при определенных условиях могут возникать бифуркационные подпространства, в которых стабільная фаза может становиться нестабільной. Критическое пространство второго порядка могут возникать в тех областях, где две различные фазы становятся идентичными. Критические пространства порядка 3 и 4 образуются соответственно при наличии трех или четырех идентичных фаз.

В качестве объекта исследования в работе выбран четырехкомпонентный твердый раствор $In_xGa_{1-x}Sb_yAs_{1-y}$. Интерес к этому материалу вызван в связи с тем, что его физические свойства в настоящее время мало исследованы, но при этом привлекают внимание исследователей как перспективный материал для создания оптоэлектронных приборов широкого спектрального диапазона, эффективных светодиодов, быстродействующих фотодиодов, которые могут быть использованы для решения различных научных и практических задач.

Цель работы

Целью работы является расчет на основе дифференциального топологического подхода [1] высших производных потенциальных функций нескольких параметров порядка с третьей по восьмую включительно в рамках термодинамического моделирования в четырехкомпонентном твердом растворе $In_xGa_{1-x}Sb_yAs_{1-y}$. Расчеты проводились в рамках модели регулярного раствора с учетом смещения атомов в двух подрешетках [2].

Изложение основного материала

Анализ четырехкомпонентного твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$ как системы, в которой предполагалось существование многих фаз, был осуществлен на основе обобщения условий существования стабільных фаз [1] на случай концентрационного пространства с размерностью четыре, что позволило проверить возможность возникновения в рассматриваемом твердом растворе критических пространств и пространств сосуществования фаз.

В модели свободная энергия Гиббса исследуемого твердого раствора рассматривалась как смесь четырех гипотетических бинарных соединений:

$$G = G(X_{AC}, X_{BC}, X_{AD}, X_{BD}), \quad (1)$$

где X_{ij} - концентрации бинарных компонентов. В предположении о случайном распределении разнородных атомов по узлам соответствующих подрешеток, выражения для концентраций бинарных компонентов принимают вид [2]:

$$X_{AC} = (1-x)(1-y), X_{AD} = (1-x)y, X_{BC} = x(1-y), X_{BD} = xy, \quad (2)$$

где x и y - концентрационные параметры.

Для проверки возможности возникновения в рассматриваемом твердом растворе критических пространств и пространств сосуществования фаз были получены и исследованы аналитические выражения высших производных потенциальной энергии

системы по параметрам порядка x_i . Высшие производные с третьей по восьмую включительно для свободной энергии Гиббса твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$ по концентрационным параметрам были рассчитаны путем матрично-векторного дифференцирования многомерных систем. Для получения матриц высших производных был использован метод прямых сумм [3, 4].

Расчет высших производных свободной энергии рассматриваемой системы проводился по следующему алгоритму. Из полученных в рамках модели регулярного раствора [5] вторых производных μ_{ij} свободной энергии Гиббса твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$, выражения которых имеют устойчивость к дифференцированию, формировалась матрица A_2 размерностью 4×4 :

$$A_2 = \begin{pmatrix} \mu_{11} & \mu_{12} & \mu_{13} & \mu_{14} \\ \mu_{21} & \mu_{22} & \mu_{23} & \mu_{24} \\ \mu_{31} & \mu_{32} & \mu_{33} & \mu_{34} \\ \mu_{41} & \mu_{42} & \mu_{43} & \mu_{44} \end{pmatrix}, \quad (3)$$

Далее, матрица A_2 дифференцировалась по четырем соответствующим концентрациям X_{ij} . В результате дифференцирования были получены четыре матрицы частных производных третьего порядка размером 4×4 , после чего, с использованием метода прямых сумм формировалась блочно-диагональная матрица полной третьей производной свободной энергии исследуемой системы:

$$A_3 = \begin{pmatrix} \frac{dA_2}{dX_{AC}} & 0 & 0 & 0 \\ 0 & \frac{dA_2}{dX_{AD}} & 0 & 0 \\ 0 & 0 & \frac{dA_2}{dX_{BC}} & 0 \\ 0 & 0 & 0 & \frac{dA_2}{dX_{BD}} \end{pmatrix} \quad (4)$$

Детерминант полученной матрицы A_3 определялся как произведение детерминантов матриц частных производных, находящихся на главных диагоналях:

$$\det A_3 = \det A_{13} \cdot \det A_{23} \cdot \det A_{33} \cdot \det A_{43}, \quad (5)$$

где

$$A_{13} = \frac{dA_2}{dX_{AC}}; A_{23} = \frac{dA_2}{dX_{AD}}; A_{33} = \frac{dA_2}{dX_{BC}}; A_{43} = \frac{dA_2}{dX_{BD}}; \quad (6)$$

Получение производных свободной энергии системы высших порядков с четвертой по восьмую включительно и соответствующих детерминантов $\det A_i$, где i – порядок производной, проводилось с использованием аналогичного алгоритма. Аналитические выражения высших производных были получены с использованием системы компьютерной математики Maxima [6].

После получения аналитических выражений для детерминантов матриц производных свободной энергии рассматриваемой системы были рассчитаны положения нулевых контуров рассматриваемых производных. Для этого значения концентрационных параметров x и y в диапазоне от 0 до 1 с шагом 0.1 подставлялись в выражения для соответствующих детерминантов, после чего проверялось выполнение условия $\det A_i = 0$. Найденные точки отображались на сечении существования твердых растворов диаграммы состояния. Далее определялись области, в которых значения соответствующих детерминантов принимают положительные и отрицательные значения. Положительные значения отмечались светлыми областями, отрицательные – более темными.

Результаты

Путем расчета положений нулевых контуров полученных в работе аналитических выражений для полных производных свободной энергии Гиббса четырехкомпонентного твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$, были численно определены и построены на соответствующем сечении диаграммы состояния исследуемой системы положения областей существования производных и их нулевые контура со второй по восьмую производную включительно для диапазона температур 773-1023K. Термодинамические параметры, использованные в расчетах, приведены в табл. 1.

Таблица 1.

Параметры взаимодействия в твердой фазе для квазибинарных систем

Квазибинарная система	Параметр взаимодействия α_{ij-jk}^5 , Дж/моль, [7]
<i>GaAs - InAs</i>	12570
<i>GaSb - InSb</i>	7961
<i>GaAs – GaSb</i>	18855
<i>InAs - InSb</i>	9427,5

На рис. 1-4, а представлены результаты расчета положений нулевых контуров производных свободной энергии Гиббса в системе $In_xGa_{1-x}Sb_yAs_{1-y}$ по концентрационным параметрам, начиная со второй производной и по восьмую производную включительно для температуры 773 К. Темным цветом показана область отрицательных значений производной и, соответственно, более светлым - область положительных значений. Пунктиром на рис. 1-4 показаны линии, изопериодные подложкам *GaSb* и *InAs*. На диаграммах показаны экспериментальные составы эпитаксиальных слоев $In_xGa_{1-x}Sb_yAs_{1-y}$, выращенных на подложках *GaSb* и *InAs*. В работе [8] монокристаллические слои были выращены на подложке *GaSb*(111) методом жидкофазной эпитаксии. Отмечено удовлетворительное качество слоев для случая положительных значений параметра рассогласования решетки. В работе [9] наблюдалась модуляция состава слоев, выращенных на подложке *GaSb* (100) с периодом около 150 нм и при увеличении значений x и y модуляция приобретала более четко выраженную периодичность. Состав, полученный в работе [10] был выращен на подложке *GaSb*(111). Для экспериментальных точек [11] отмечалось, что соответствующие им составы были получены вблизи области несмешиваемости и не являются стабильными. Эпитаксиальные слои, описанные в [12], были получены с помощью LPE и MOVPE технологий в условиях, близких к термодинамическому

равновесию. На рис. 1-4 так же отмечены точки, в которых наблюдался рост монокристаллических [13] и поликристаллических слоев [14] на подложках из *GaSb* и *InAs*, исходные составы для роста которых находились в области термодинамической неустойчивости.

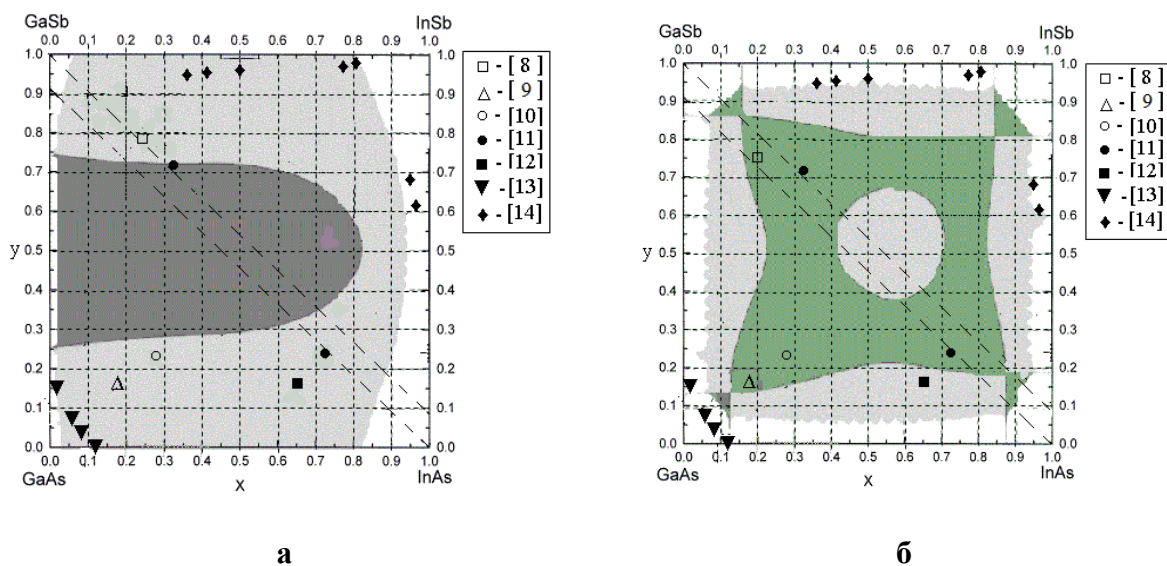


Рис. 1. Результаты численных расчетов: а – второй производной; б – третьей производной свободной энергии в системе $In_xGa_{1-x}Sb_yAs_{1-y}$ на сечении существования твердых растворов диаграммы состояния

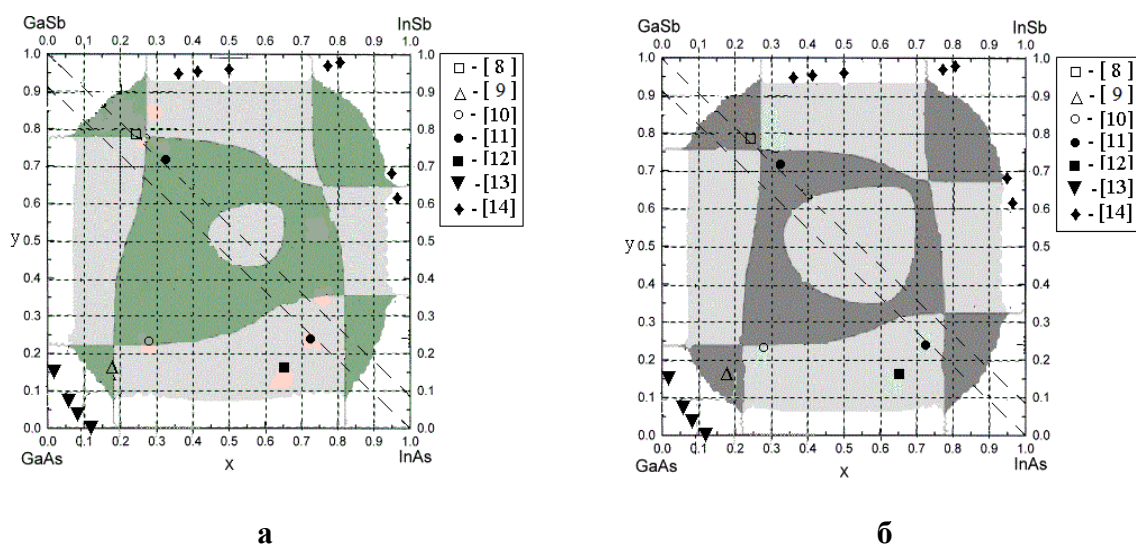


Рис. 2. Результаты численных расчетов: а – четвертой производной; б – пятой производной свободной энергии системы $In_xGa_{1-x}Sb_yAs_{1-y}$ на сечении существования твердых растворов диаграммы состояния

На основе полученных контуров третьей и четвертой производных на сечении существования твердых растворов диаграммы состояния исследуемой системы были построены контура областей сосуществования фаз порядка два. На рис. 4, б представлены результаты моделирования областей на сечении существования твердых растворов диаграммы состояния в системе $In_xGa_{1-x}Sb_yAs_{1-y}$ для температуры 773 К, где возможно сосуществование двух твердых фаз для различных температур. Темным

цветом показаны области выполнения условий формирования пространств сосуществования фаз порядка два, светлым – область существования третьей и четвертой производных. Для построения этих областей были использованы результаты численных расчетов производных со второй по четвертую включительно свободной энергии системы, результаты которых представлены на рис. 1-2. Как видно из рис. 4, б данные по экспериментальному составу [8] попадают в область сосуществования фаз, а точка, соответствующая составу [9], находится в непосредственной близости от рассчитанной области. Большинство экспериментальных составов [10-12] находятся в непосредственной близости от рассчитанной области сосуществования двух фаз. Составы из [13, 14] не попадают в область существования производных в связи с их четко выраженной монокристаллической и поликристаллической структурой.

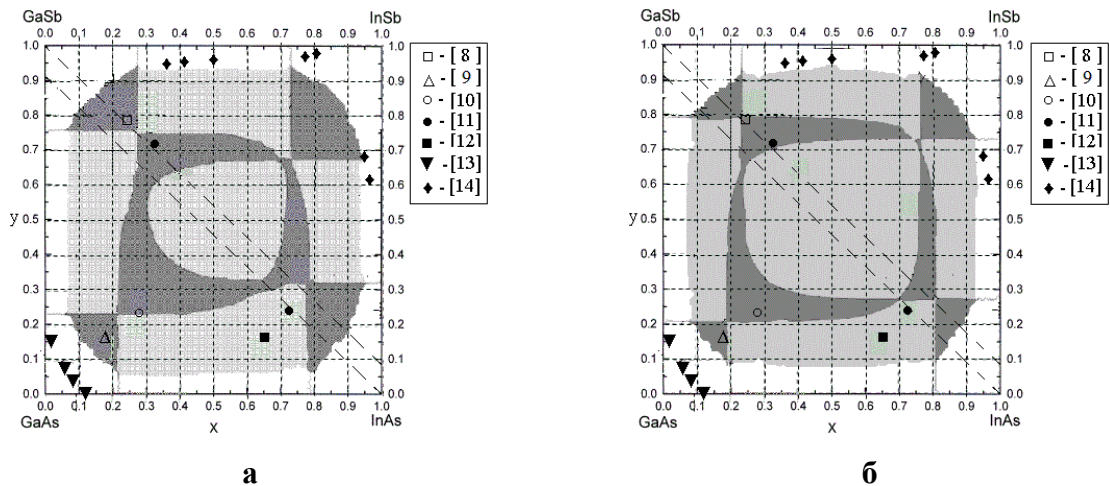


Рис. 3. Результаты численных расчетов: а – шестой производной; б – седьмой производной свободной энергии в системе $In_xGa_{1-x}Sb_yAs_{1-y}$ на сечении существования твердых растворов диаграммы состояния

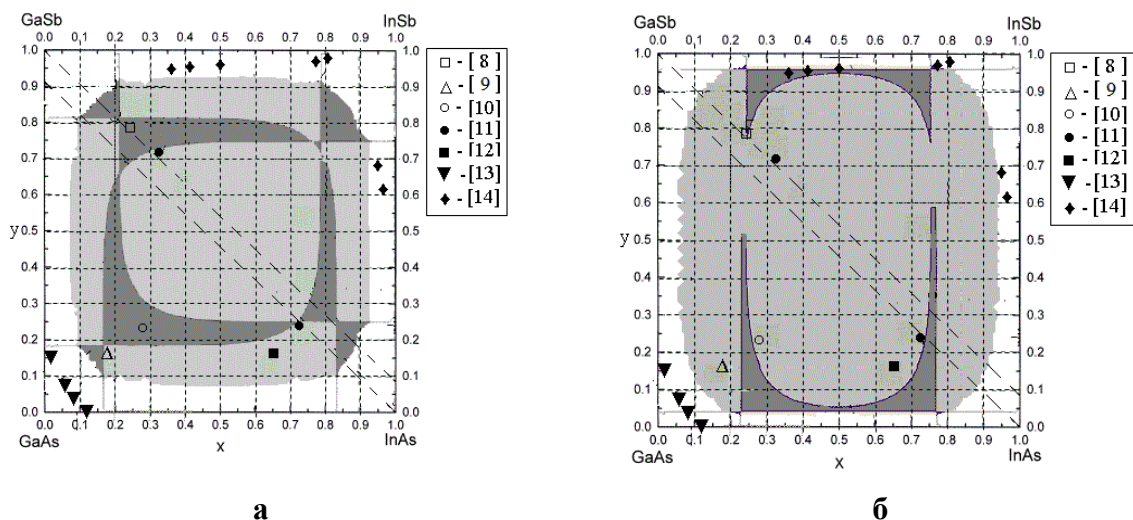


Рис. 4. Результаты численных расчетов: а – восьмой производной свободной энергии в системе $In_xGa_{1-x}Sb_yAs_{1-y}$ на сечении существования твердых растворов диаграммы состояния; б – пространств сосуществования фаз порядка два

Выводы

Полученные в работе результаты моделирования пространств сосуществования фаз порядка два в системе $In_xGa_{1-x}Sb_yAs_{1-y}$ позволяют объяснить имеющиеся экспериментальные данные по спонтанному формированию двухфазных

модулированных структур в эпитаксиальных слоях рассмотренного твердого раствора. Показано, что использованная модель регулярного раствора для свободной энергии Гиббса позволяет проводить достаточно корректную оценку положения пространства сосуществования порядка два на сечении фазовых диаграмм. Исходя из полученных результатов моделирования можно предположить, что предложенная модель может быть использована для прогнозирования пространства возможного образования трехмерных модулированных структур в слоях твердого раствора $In_xGa_{1-x}Sb_yAs_{1-y}$ также для случаев возникновения трех различных фаз для различных составов рассмотренного твердого раствора с помощью построения пространств сосуществования фаз порядка три.

Список литературы

1. Okada, K. Classical calculations on the phase transition I. Phase diagram in four-dimensional space for the system with one order parameter / K. Okada, I. Suzuki // J. Phys. Soc. Jap. – 1982. – Vol. 51, №10. – P. 3250–3257.
2. Onabe, K. Thermodynamics of the type $A_{1-x}B_xC_{1-y}D_y$, III-V quaternary solid solutions / K. Onabe // J. Phys. Chem. Solids. – 1982. – Vol. 43, №11. – P. 1071–1086.
3. Муха, В.С. Анализ многомерных данных: проблемы, состояния, перспективы / В.С. Муха // Доклады БГУИР. – 2004. – №1. – С.38–49.
4. Traat, I. Matrix calculus for multivariate distributions / I. Traat // Уч. зап. Тарт. гос. ун-та. – 1986. – Вып. 733. – С.64–85.
5. Kazakov, A. Computer simulation for stability of quaternary solid solutions / A. Kazakov, I. Kishmar // J. Crystal Growth. – 1991. – Vol. 110. – P. 803–814.
6. Система компьютерной алгебры Maxima: [Электронный ресурс] // Maxima, a Computer Algebra System. Режим доступа: <http://maxima.sourceforge.net> (Дата обращения: 05.11.2013).
7. Казаков, А.И. Расчет фазовых равновесий в многокомпонентных системах / А.И. Казаков, В.А. Мокрицкий, В.Н. Романенко и др. – М.: Металлургия, 1987. – 136 с.
8. Joullie, A. LPE growth of GaInAsSb/GaSb system: The importance of the sign of the lattice mismatch / F. Jia Hua, F. Karouta, H. Mani // J. Crystal Growth. – 1986. – Vol. 75. – P. 309–318.
9. Wang, C.A. Correlation between surface step structure and phase separation in epitaxial GaInAsSb / C.A. Wang // Appl. Phys. Lett. – 2000. – Vol. 76. – P.2077.
10. Vasil'ev, V.I. Properties of GaInAsSb solid solutions obtained from antimony fluxes by liquid-phase epitaxy in the spinodal decay region / A.G. Deryagin, V.I. Kuchinskii, V.M. Smirnov, G.S. Sokolovskii, D.N. Tret'yakov, N.N. Faleev // Tech. Phys. Lett. – 1998. – Vol. 24. – P. 231–232.
11. Cheng, M.J. GaInAsSb metastable alloys grown by organometallic vapor phase epitaxy / G.B. Stringfellow, D.W. Kisker, A.K. Srivastava, J.L. Zyskind // Appl. Phys. Lett. – 1986. – Vol. 48. – P. 419–421.
12. Baranov, A.N. Strained multiple-quantum-well lasers grown on GaSb emitting between 2 and 2.4 μm / Y. Cuminal, N. Bertru, C. Alibert, A. Joullie // Proc. SPIE. – 1997. – Vol. 2. – P. 2–13.
13. Kazakov, A.I. Stability analysis of quaternary $In_xGa_{1-x}Sb_yAs_{1-y}$ alloys / I.N. Kishmar, A.I. Bochkarev, L.V. Dolginov // J. Crystal Growth. – 1992. – Vol. 116. – P.204–212.
14. Dolginov, L. M., A study of phaseequilibria and heterojunction in Ga-In-As-Sb quaternary system / Eliseev P.G., Lapshin A.N., Milvidskii M.G. // Kristall Tech. – 1978. – Vol. 13. – P.631

РОЗРАХУНОК ОБЛАСТЕЙ СПІВІСНУВАННЯ ФАЗ В СИСТЕМІ $In_xGa_{1-x}Sb_yAs_{1-y}$

А.І. Казаков, Л.Т. Кваташидзе, Г.В. Шаповалов

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: anatkaz@mail.ru

В рамках моделі регулярного розчину і стандартних термодинамічних функцій, використаних для опису станів бінарних сполук і взаємодії атомів в чотирьохкомпонентних твердих розчинах, були розраховані вищі похідні вільної енергії гомогенного твердого розчину $In_xGa_{1-x}Sb_yAs_{1-y}$ зі змішанням в двох підґратках з третьої по восьму похідну включно. Аналітичні вирази для похідних, чисельні розрахунки і визначення нульових контурів похідних проводилися на основі диференціального топологічного підходу з використанням системи комп'ютерної математики Maxima. У чотиривимірному концентраційному просторі були розраховані перетини фазової діаграми твердого розчину $In_xGa_{1-x}Sb_yAs_{1-y}$, критичні простори і простори співіснування фаз для різних температур. Результати розрахунків вказують на можливість формування областей співіснування фаз другого порядку в твердих розчинах $In_xGa_{1-x}Sb_yAs_{1-y}$, що ні суперечить існуючим експериментальним даним.

Ключові слова: диференційний топологічний підхід, тверді розчини, простору співіснування фаз, багатоконпонентні системи, матричні похідні

CALCULATION OF THE COEXISTENCE SPACES IN THE SYSTEM $In_xGa_{1-x}Sb_yAs_{1-y}$

A.I. Kazakov, L.T. Kvatashidze, G.V. Shapovalov

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: anatkaz@mail.ru

The higher derivatives of the free energy in $In_xGa_{1-x}Sb_yAs_{1-y}$ solid alloys were calculated with the regular solution model approximation using standard thermodynamic functions of the binaries to describe the interatomic interaction in multi-component alloys. The model of the homogeneous solid solution with mixing in two sublattices was used. Derivatives of the third to eighth order were obtained. The analytical expressions for the derivatives, numerical calculation and determination of the zero contours of higher derivatives on the basis of differential topological approach were obtained using the system of computer mathematics Maxima. The cross sections of the phase diagram of a solid solutions $In_xGa_{1-x}Sb_yAs_{1-y}$, the critical space and space for coexistence of phases in the four-components space for different temperatures were calculated. The results obtained indicate the possibility of the formation of the coexistence spaces of the second order in the $In_xGa_{1-x}Sb_yAs_{1-y}$ alloys. Such results do not contradict the available experimental data.

Keywords: differential topological approach, the solid solution phase coexistence space, multi-component systems, matrix derivatives.

ПРОГНОЗУВАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖАВИ З ВИКОРИСТАННЯМ ПЕРЕТВОРЕННЯ КАРУНЕНА-ЛОЄВА

І.Р. Опірський

Національний університет «Львівська політехніка»,
вул. Ст. Бандери, 12, Львів, 79000, Україна; e-mail: iopirsky@gmail.com

В роботі основною передумовою до рішення задачі прогнозування несанкціонованого доступу (НСД) в інформаційних системах держави є наявність зручного опису випадкового процесу $X(t)$. Пропонується апроксимувати реальний випадковий процес $X(t)$ лінійною функцією часу $X(t) = A + Bt$, де A і B – випадкові коефіцієнти, ймовірні характеристики яких визначаються за допомогою

методу найменших квадратів, виходячи з умови
$$M \left[\int_T (X(t) - (A + Bt))^2 dt \right] = \min ,$$

при чому T – інтервал спостереження випадкового процесу $X(t)$. Проводиться дослідження і опис процесу $X(t)$ для прогнозування НСД з використанням перетворення Карунена-Лоева, приводиться математичне обґрунтування та виведення виразів, що описують математичне визначення векторного випадкового процесу $X(t)$ і дозволяють вирішити задачу прогнозування НСД. Зроблені висновки щодо доцільності використання перетворення Карунена-Лоева для прогнозування НСД в інформаційних системах держави.

Ключові слова: несанкціонований доступ, інформаційні системи держави, перетворення Карунена-Лоева, математичний процес прогнозування.

Вступ

Проблема прогнозування включає в себе ряд численних труднощів, одні з яких власне зв'язані з прогнозуванням, другі характерні для всіх напрямків автоматичного контролю, треті визначають загальні можливості прогнозування і його місце серед інших видів контролю. Прогнозування несанкціонованого доступу (НСД) в інформаційних системах держави, без сумніву, повинно ґрунтуватись на вивченні тенденцій, що спостерігаються в зміні її поточного стану під дією НСД. В теорії автоматичного контролю передбачається, що цей стан може бути представлено сукупністю значень деяких контрольних параметрів. Тоді, очевидно, причиною, що викликає зміни стану інформаційної системи держави, повинні бути зміни значень саме цих параметрів. Таким чином прогнозування НСД в інформаційних системах держави повинно базуватись на прогнозуванні значень складових контрольних параметрів. Це може здійснюватись на базі математичного апарату екстраполяції процесів, що описує закономірності змін в параметрах. В свою чергу використання апарату екстраполяції потребує певної формалізації процесів змін контрольних параметрів, тобто потребує створення певної математичної моделі процесів вимірювання параметрів інформаційної системи держави під впливом НСД.

Прогнозний контроль потребує визначення спеціальних прогнозних параметрів. Важливою проблемою є визначення дійсного місця прогнозуючого контролю серед всіх

форм контролю в підвищенні ефективності використання системи контролю НСД. Рішенням цієї проблеми в чималому степені залежить від самої можливості здійснення прогнозу в тих чи інших конкретних умовах застосування в системах та мережах.

Метою роботи є дослідження і опис процесу $X(t)$ для прогнозування НСД з використанням перетворення Карунена-Лоєва (КЛ), проведення математичного обґрунтування та виведення виразів, що точно описують апостеріорне математичне визначення векторного випадкового процесу $X(t)$ і в рамках зроблених припущень та досліджень дозволяють вирішити задачу прогнозування НСД, а також визначення переваг та недоліків запропонованого перетворення для прогнозування НСД.

Основна частина

В більшій мірі вільно від більшості недоліків представимо процес $X(t)$ для прогнозування НСД ортогональним перетворенням КЛ [1]. При його використанні зберігається ідея представлення процесу $X(t)$ в вигляді сум елементарних випадкових процесів. Однак умова оптимальності перетворення формулюється як вимога мінімуму математичного очікування середнього квадрата помилки на замкнутому інтервалі розкладання $[0, T]$:

$$E = M \left[\int_0^T \left| X(t) - m(t) - \sum_{v=1}^N V_v \varphi_v(t) \right|^2 dt \right] = M \left[\int_0^T \left| \hat{X}(t) - \sum_{v=1}^N V_v \varphi_v(t) \right|^2 dt \right] = \min. \quad (1)$$

В роботі [1] показано, що таке перетворення існує для будь-якого випадкового процесу $X(t)$, що задовольняє умову $M[|X(t)|^2] < \infty$, причому середньоквадратична помилка наближення прямує до нуля рівномірно на $[0, T]$ по мірі росту N .

Таким чином, можна поставити задачу знайти мінімальне число доданків N , при якому забезпечується значення помилок наближення E , що не перевищує заданого рівня E_δ . В роботі [2] показано, що для її рішення може бути використана методика послідовного наближення. Результируюче перетворення, яке було використаним в (1), має вигляд: $X(t) = m(t) + \sum_{v=1}^N V_v \varphi_v(t)$, де N – число доданків, визначених тільки вимогами до точності, а $m(t)$ – математичне очікування процесу. Для його елементів справедливий загальний вираз:

$$v_v = \int_0^T \dot{X}(t) \varphi_v(t) dt, \quad \varphi_v(t) = \frac{1}{D_v} M[\dot{X}(t) V_v], \quad (2)$$

$$\int_0^T K(t, s) \varphi_v(s) ds = D_v \varphi_v(t), \quad E_n = \int_0^T D(t) dt - \sum_{v=1}^N D_v. \quad (3)$$

При цьому коефіцієнти розкладання задовольняють умовам $M[V_v] = 0$, $M[V_v, V_\mu] = 0$, при $v \neq \mu$, а функції $\varphi_v(t)$ образують ортонормовану систему:

$$\int_0^T \varphi_v(t) \varphi_\mu(t) dt = \begin{cases} 1 & \text{при } v = \mu \\ 0 & \text{при } v \neq \mu \end{cases}$$

Перетворення КЛ як засіб опису апіорного процесу $X(t)$ слід порівнювати з його канонічним поданням по трьох основних напрямках: складності алгоритму, що застосовується для його отримання; об'єму пам'яті, необхідної для зберігання апіорної інформації, точності подання процесу обмеженим числом членів ряду. Щоб забезпечити співставлення результатів, уявимо, що вихідний процес $X(t)$ заданий випадковою послідовністю $X(i), i = \overline{1, I}$ в дискретному ряді точок t_i . В цьому випадку алгоритм отримання елементів канонічного розкладання достатньо простий [2].

Вирішення аналогічної задачі для розкладання Корунена-Лоева значно складніше, оскільки координатні функції в даному випадку визначаються інтервальним рівнянням (3). Рішення даного рівняння зводиться до визначення власних значень і власних векторів кореляційної матриці $K(i, j), i, j = \overline{1, I}$ процесу $X(t)$.

Для повного вирішення цієї задачі на ПЕВМ зазвичай використовують метод обертань [3], достатньо трудомісткий в обчислювальному відношенні. Задача полегшується тим, що для її вирішення створені стандартні програми [4]. Можна додатково зменшити об'єм обчислень, так як замість повного вирішення задачі достатньо обмежитись знаходженням декількох найбільших власних значень і відповідних їм векторів, однак і це не змінює суть питання.

Таким чином, можна стверджувати, що з точки зору простоти отримання елементів відповідного представлення розкладання КЛ завжди програє канонічному розкладанню. Це однак не є істотним недоліком при використанні розкладання КЛ в задачах прогнозу, оскільки описана обробка здійснюється попередньо, і для неї можна не використовувати ЕОМ, що володіє великим об'ємом пам'яті і швидкодією.

Порівняння об'ємів пам'яті, необхідних для апіорної інформації про кожне з цих розкладань, повинно проводитись на основі наступних міркувань. При числі членів $N = I$ обидва розкладання точно представляють процес в дискретних точках $t_i, i = \overline{1, I}$. При цьому в пам'яті повинні зберігатися відомості про математичне очікування процесу, про щільності розподілення коефіцієнтів V , про координатні функції.

Скорочення числа членів перетворення не позначається на об'ємі відомостей про математичне очікування і зменшує підлягаючий зберігання об'єм інформації про щільність розподілення коефіцієнтів. Таким чином, необхідно порівнювати лише об'єм пам'яті, необхідний для збереження координатних функцій. Тоді при точному відтворенню процесу кількість комірок пам'яті, необхідних для збереження інформації про координатні функції розкладання КЛ, дорівнює I^2 , а для канонічного розкладання $I(I+1)/2$. Звідси випливає, що при точному представленні процесу перетворення КЛ видається неекономічним. Однак з зниженням вимог до точності кожен відкинутий член перетворення КЛ скорочує необхідний об'єм пам'яті на I комірок, а відкинутий член канонічного представлення на $I - N$ комірок. Таким чином для канонічного представлення процесу зменшення об'єму пам'яті відбувається повільно, а точність його падає швидше. В результаті завжди можна вказати такий рівень вимог та точності, при якому перетворення КЛ виявиться більш економічним від канонічного виразу.

Оскільки форма отримання перетворення нічим не відрізняється від форми канонічного виразу, алгоритм моделювання апіорного процесу також не має істотних особливостей. Разом з тим рішення задач прогнозу з невикористанням перетворення КЛ носить специфічний характер, обумовлений методикою визначення коефіцієнтів V_v . Розглянемо принцип вирішення задач прогнозу в цьому випадку.

Нехай апіорний процес $X(t)$ заданий на інтервалі $[0, T]$ розкладанням КЛ:

$$X(t) = m(t) + \sum_{v=1}^N V_v \varphi_v(t), \quad (4)$$

де $m(t)$ – математичне очікування процесу;

φ_v – не випадкові функції часу;

V_v – випадкові коефіцієнти, некорельовані між собою.

В подальшому можна вважати $m(t) = 0, 0 \leq t \leq T$. Нехай надалі відомий відрізок конкретної реалізації цього процесу $X_\omega(t)$ на проміжку $[0, t_k], t_k < T$. Необхідно передбачити поведінку даної реалізації на $[t_k, T]$.

Оскільки перетворення (4) справедливе для кожної реалізації процесу $X(t)$, в тому числі, для заданого відрізка, майбутнє значення шукається у вигляді [5]:

$$\hat{X}_\omega(t) = \sum_{v=1}^N C_v \varphi_v, \quad t_k \leq t \leq T. \quad (5)$$

Тут $\varphi_v(t)$ – відомі координатні функції КЛ для апріорного випадкового процесу. Таким чином, для вирішення задачі прогнозування НСД в даному випадку достатньо знайти невідомі значення коефіцієнтів C_v , де $v = \overline{1, N}$.

Очевидно, що передбачення буде найкращим, якщо C_v будуть рівні своїм нейтральним значенням, що визначаються формулою (2). Однак, безпосередньому застосуванню цього виразу перешкоджає нестача інформації, оскільки реалізація $X_\omega(t)$ відома лише на частині проміжку розкладання $[0, T]$. Тому може ставитись лише задача знайти найкраще квадратичне наближення коефіцієнтів C_v до їх істинних значень. Однак, як показано в [1], рішення цієї задачі виявляється надто складним і потребує знань моментних функцій вищого порядку випадкового процесу $X(t)$. Тому для обчислення коефіцієнтів C_v зазвичай використовують більш простий, хоч і менш точний метод. Знаходять такі значення C_v , для яких перетворення (4) буде найкращим середньоквадратичним - $X_\omega(t)$ на проміжку $[0, t_k]$, де ця реалізація відома:

$$\int_0^{t_k} [X_\omega(t) - \sum_{v=1}^N C_v \varphi_v(t)]^2 dt = \min. \quad (6)$$

Диференціюючи (6) по $C_v, v = \overline{1, N}$ отримуємо систему лінійних рівнянь:

$$\sum_{v=1}^N C_v \int_0^{t_k} \varphi_v(t) \varphi_\lambda(t) dt = \int_0^{t_k} x(t) \varphi_\lambda(t) dt, \quad \lambda = \overline{1, N}, \quad (7)$$

яка визначає $C_v, v = \overline{1, N}$ однозначно. Як показано в роботі [6], отримані таким чином значення коефіцієнтів C_v є незміщеними оцінками коефіцієнтів V_v вихідного розкладання, що робить використання даної методики раціональним. Після отримання коефіцієнтів C_v подальший хід рішення задачі прогнозування стає тривіальним.

Для рішення задачі прогнозу при реалізації перетворення КЛ необхідно обчислити $k \gg N$ числа відомих значень, оскільки лише при цій умові прийнята методика визначення є ефективною. Однак при виконанні умови отримане значення коефіцієнтів є неточним, що не може не вплинути на ефективність прогнозу [7].

Для ілюстрації цих тверджень на рис.1 наведений приклад прогнозу методом КЛ.

З рис.1 видно, що навіть при значному скороченні числа доданків розкладання ($N=3$) наближення виявляється хорошим. Це підтверджує можливість економії пам'яті за рахунок скорочення об'єму збереженої апріорної інформації про процес.



Рис. 1. Результати прогнозування НСД з використанням перетворення Карунена-Лоєва

Одночасно даний приклад показує, що використання розкладання КЛ доцільно застосовувати в тих випадках, коли наявні жорсткі обмеження на об'єм пам'яті ЕОМ. Якщо ж допускається деяке збільшення об'єму пам'яті чи вимагається рішення задачі повністю прогнозування НСД, то доцільніше використовувати інші методи та перетворення.

Висновки

На основі математичного обґрунтування та виведення виразів, що точно описують апостеріорне математичне визначення векторного випадкового процесу $X(t)$ і в рамках зроблених припущень та досліджень виведено вирази прогнозування НСД в інформаційних системах держави за допомогою перетворення КЛ, що в свою чергу дозволило отримати подальший розвиток вирішенню проблеми прогнозування НСД. Проведений аналіз показав, що використання даного розкладання доцільно застосовувати в тих випадках, коли наявні жорсткі обмеження на об'єм пам'яті ЕОМ, оскільки при значному скороченні числа доданків розкладання ($N=3$) наближення виявляється достатньо хорошим, що підтверджує можливість економії пам'яті за рахунок скорочення об'єму збереженої апріорної інформації про процес.

Список літератури

1. Ивахненко, А.Г. Непрерывность и дискретность: переборные методы моделирования и кластеризации / А.Г. Ивахненко. – Киев: Наукова думка, 1990. – 224 с.
2. Тихонов, В.И. Статистический анализ и синтез радиотехнических устройств и систем / В.И. Тихонов, В.Н. Харисов. – М.: Радио и связь, 1991. – 608 с.
3. Згуровський, М.З. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К: ВНУ, 2007. – 544 с.

4. Борисенков, Е.П. Алгоритмы и программы статистической обработки информации на ЭВМ / Е.П. Борисенков, Н.А. Романов. – Ленинград: Гидрометеоиздат, 1989. – 454 с.
5. Козлова, К.В. Кількісна оцінка захисту радіоелектронних об'єктів / К.В. Козлова, В.О. Хорошко // Захист інформації. – 2007. – №1 – С. 30–32.
6. Тартаковский, А.Г. Последовательные методы в теории информационных систем / А.Г. Тартаковский. – М: Радио и связь, 1991. – 280 с.
7. Lorden, G. Nearly-optimal Sequential Test for Finitely Many Parameters Values / G. Lorden // Ann. Statist. – 1997. – V.5, №1. – P. 1–21.

ПРОГНОЗИРОВАНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВА С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАНИЯ КАРУНЕНА-ЛОЕВА

И.Р. Опирский

Национальный университет «Львовская политехника»,
ул. Бандеры, 12, Львов, 79000, Украина; e-mail: iopirsky@gmail.com

В работе основной предпосылкой к решению задачи прогнозирования несанкционированного доступа (НСД) в информационных системах государства является наличие достаточно удобного описания процесса $X(t)$. При этом предлагается аппроксимировать реальный случайный процесс $X(t)$ линейной функцией времени $X(t) = A + Bt$, где A и B – случайные коэффициенты, вероятностные характеристики которых определяются с помощью метода

наименьших квадратов из условия $M \left[\int_T (X(t) - (A + Bt))^2 dt \right] = \min$, причем T –

интервал наблюдения случайного процесса $X(t)$. Проводится исследование и описание процесса $X(t)$ для прогнозирования НСД с использованием преобразования Карунена-Лоева, приводится математическое обоснование и вывод выражений, описывающих математическое определение векторного случайного процесса $X(t)$ и позволяющих решить задачу прогнозирования НСД. Сделаны выводы о целесообразности использования данного преобразования для прогнозирования НСД в информационных системах государства.

Ключевые слова: несанкционированный доступ, алгоритм экстраполяции, статическая классификация, детерминированные процессы, дисперсия.

PREDICTION OF UNAUTHORIZED ACCESS TO INFORMATION SYSTEMS OF THE STATE USING KARHUNEN-LOEVE

I.R. Opirsky

National University «Lviv Polytechnic»
st. St.Bandery, 12, Lviv, 79000, Ukraine; e-mail: iopirsky@gmail.com

The main prerequisite to solving the problem of forecasting in our work is the presence of convenient enough description of the process $X(t)$. It is proposed to approximate real random process $X(t)$, linear time function $X(t) = A + Bt$, where A and B – random factors likely characteristics are determined by the method of least squares based on the conditions

$M \left[\int_T (X(t) - (A + Bt))^2 dt \right] = \min$ whereby T – interval observing the random process

$X(t)$. Perform the following description may be many representations and transformations. But within this article is to study and description of $X(t)$ to predict UA using Karhunen-Loeve, driven mathematical reasoning and output expressions that describe the mathematical definition of a vector random process $X(t)$ and can solve the problem of forecasting unauthorized access and on the basis of conclusions regarding the usefulness of this transformation for predicting unauthorized access to information systems of the state.

Keywords: unauthorized access, information systems of the state, Karhunen-Loeve, mathematical process of forecasting.

КРИТЕРІЇ ОЦІНКИ ЙМОВІРНОСТІ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ТЕХНІЧНІ КАНАЛИ

М.Г. Романюков

Головне управління міністерства внутрішніх справ України в Одеській області,
вул. Єврейська, 12, Одеса, 65014, Україна; e-mail: kolyanr21@gmail.com

Проведена класифікація сучасних технічних каналів витоку інформації та аналіз їх особливостей з врахуванням сучасних можливих ризиків. Запропонований спосіб кількісного визначення інтегрального показника, що характеризує ступінь безпеки інформації на об'єкті та визначає ймовірність витоку інформації, враховуючи всі фактори, що здійснюють значний вплив на його формування. На основі даного показника проводиться оцінка стану системи захисту інформації. Приведений строго-теоретичний та теоретико-емпіричний підхід для визначення рівня очікуваних втрат при порушенні захисту інформації, що дозволяє, при наявності можливостей, зібрати достатню кількість фактичних даних щодо проявлених загроз та їх наслідків, застосовувати розглянуті в статті моделі для вирішення широкого кола задач по захисту інформації. Обчислюється емпірична величина рівнів затрат, при якій забезпечується мінімізація повної очікуваної вартості захисту інформації.

Ключові слова: технічні канали витоку інформації, модель процесу захисту, ймовірність забезпечення безпеки.

Вступ

Забезпечення інформаційної безпеки є важливим завданням для будь-якої системи захисту, оскільки від збереження конфіденційності, цілісності та доступності інформаційних ресурсів залежать якість і оперативність прийняття технічних рішень, ефективність їх реалізації.

В умовах різних форм власності завдання забезпечення інформаційної безпеки повністю лягає на плечі підприємців, керівників організацій, різних комерційних структур. За підрахунками американських фахівців, втрата 20% інформації веде до розорення організації протягом місяця в 60 випадках зі 100. Інформація є основою для прийняття рішень людиною і від її достовірності, повноти та системної організованості залежить ризик прийняття неефективних і небезпечних рішень [1, 2].

Мета статті

На основі класифікації технічних каналів витоку інформації, запропонувати кількісне визначення інтегрального показника, що характеризує ступінь безпеки інформації на об'єкті та визначає ймовірність витоку інформації, враховуючи всі фактори, що здійснюють значний вплив на його формування. На основі даного показника провести оцінку стану системи захисту інформації. Визначити оптимальний варіант витрат, при яких забезпечується мінімізація повної очікуваної вартості захисту інформації.

Основна частина

Основною класифікаційною ознакою технічних каналів витоку інформації є фізична природа носія інформації. Носії інформації поділяються на польові (фізичні поля), речовинно-польові (потoki частинок), речовинні (матеріали, речовини, структурні елементи та інші макрооб'єкти). На рис. 1 представлена ієрархічна схема фізичних полів, що відносяться до електромагнітної взаємодії.

З використанням фотоелектричних перетворювачів здійснюється перетворення фізичних полів, які випромінюють джерело інформативного сигналу, в інші фізичні поля. Це пов'язано як із взаємодією інформаційних сигналів з об'єктами навколишнього середовища, так із застосуванням технічних засобів. У зв'язку з цим інформативний сигнал може розповсюджуватись одночасно в різних середовищах, може прийматися приймачами, основаними на різноманітних фізичних принципах.

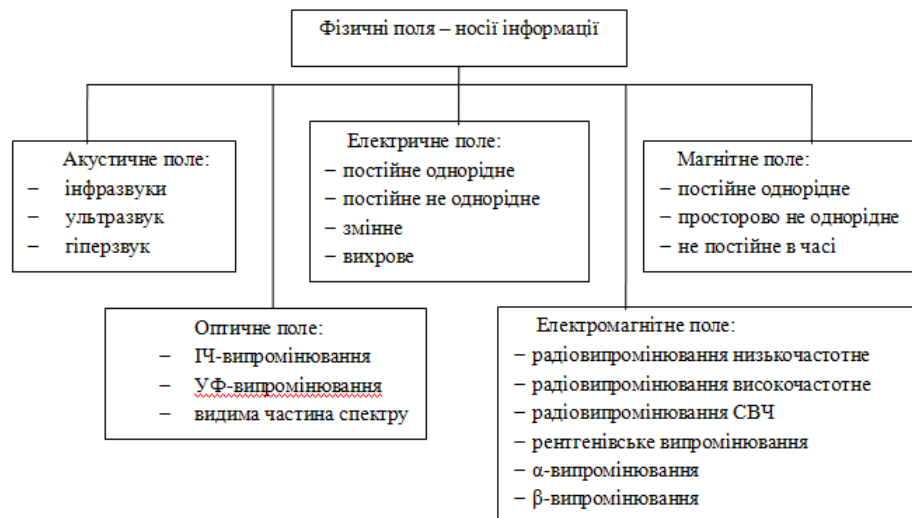


Рис. 1. Схема різновидів фізичних полів – носіїв інформації

В табл. 1 приведений взаємозв'язок між носіями інформаційного сигналу та фізичними середовищами [3].

Таблиця 1.

Взаємозв'язок між носіями інформаційного сигналу та фізичними середовищами

Фізичне середовище Носії інформації	Газоподібна	Рідка	Тверда
Польові			
Акустичне поле	+	+	+
Електричне поле		+	+
Магнітне поле		+	+
Оптичне поле	+	+	+
Електромагнітне поле	+		
Речовинно-польові			
Електрони	+		
Іони	+	+	
α-, β-, γ-випромінювання	+	+	+
Речовинні			
Гази	+	+	+
Рідини	+	+	+
Тверді тіла	+	+	
Структурні елементи	+	+	

Сучасні підходи до аналізу захищеності інформації і побудови систем захисту інформації (СЗІ) базуються на методах аналізу та управління ризиками. Ризик – прогнозована векторна величина збитку, що може виникнути внаслідок ухвалення рішень в умовах невизначеності та реалізації загроз. Він є кількісною мірою безпеки, що дорівнює добутку ймовірності реалізації даної загрози, помноженій на ймовірність величини можливого збитку від неї. Традиційно неповна інформація щодо загроз, втрат (збитків), їх ймовірностей, інтенсивності та рівнів обумовлює доцільність використання моделі "невизначеність – ризик", в основі походження якої – гіпотеза існування вихідної природної невизначеності в результатах виконання певних дій (операцій). Якщо на цю вихідну невизначеність накладається ситуативна багатоваріантність можливих наслідків (рішень) з кількісною оцінкою ймовірності кожного з них, отримуємо типову ситуацію ризику.

За прикладом звернемося до сфери технічних вимірювань. Припустимо, що контролюються значення певної фізичної величини – напруги U , яка в процесі вимірювання має певне незмінне в часі значення u , невідоме досліднику. Для вимірювання застосовується цифровий вольтметр, покази якого містять випадкову похибку. Результат вимірювань – вибірка даних з W послідовно отриманих відліків виміру приладу $\{u_t\}, t=1,2,\dots,W$. Аналіз цієї вибірки приводить до ранжованого ряду варіантів $u_1 \leq u_2 \leq \dots \leq u_n$ з відповідними відносними частотами варіантів

$$W_{ri}, i=1, n, \text{ де } W_{ri} = \frac{W_i}{W}, \text{ де } W_i - \text{частість варіанту } u_{(i)} \text{ у вибірці } \{u_{(i)}\}, \text{ а } W = \sum_{i=1}^n W_i.$$

Вважаючи відносні частоти оцінками ймовірностей $p_{(i)}$ варіантів, отримуємо ймовірнісний розподіл $\{u_{(i)}, p_{(i)}\}, i=1, n$. Маємо типову ризикову ситуацію: у якості невідомого значення u можемо взяти будь-який з варіантів, комбінацію цих варіантів.

Природно припустити, що невідоме значення напруги u лежить в межах замкненого проміжку $[u_1, u_n]$. Зокрема, якщо у якості невідомого значення u приймемо u_1 , ми з ймовірністю p_1 ризикуємо припуститися помилки: $e_1 = u_1 - u$.

Відповідно при виборі варіанту u_2 з ймовірністю p_2 можлива помилка: $e_2 = u_2 - u$, а в загальному випадку для варіанта u_i матимемо з ймовірністю p_i помилку: $e_i = u_i - u, i=1, n$.

Невірний вибір варіанту результату вимірювань спричиняє до певних втрат, збитків, причому, чим більше помилка e , тим суттєвіші втрати. Обсяг цих втрат (збитків) обчислюється за так званою функцією втрат, яка для даної задачі є фактично функцією помилки обраного варіанту результату вимірювань: $L(e_i), i=1, n$. За своєю структурою частіше за все $L(e_i)$ – квадратична функція аргументу: $L(e_i) = (e_i)^2 = (u_i - u)^2 = L(u_i - u)$.

Використовуючи саме цей вид функції втрат, проаналізуємо ризики нашої задачі. Вибір довільного варіанту результату вимірювань u_i супроводжується виникненням ймовірних втрат, величина яких визначається відповідним ризиком: $r_i = p_i(u_i - u)^2$.

Інтегровану оцінку можливих втрат за всіма варіантами вибору дає середній ризик:

$$R = \sum r_i \sum_{i=1}^n p_i(u_i - u)^2, \quad (1)$$

тобто середній ризик – це середні втрати у ситуації ризику (за всіма можливими варіантами і відповідними їм втратами). Кількісні значення $p_i, u_i, i = \overline{1, n}$, у (1) відомі, тому фактично ризик R є функцією одного аргументу – u , кількісна оцінка значення якого є метою оптимальної обробки отриманої вибірки $\{u_i\}$. Очевидно, що найкращою буде та оцінка u , яка мінімізує середні втрати $R(u)$. Застосувавши стандартну процедуру пошуку екстремуму, отримаємо:

$$\frac{d}{du} R(u) = \frac{d}{du} \left\{ \sum_{i=1}^n p_i (u_i - u)^2 \right\} = 2 \sum_{i=1}^n p_i (u_i - u) = 0,$$

звідки

$$u_{opt} = \sum_{i=1}^n p_i u_i = \frac{1}{W} \sum_{i=1}^n u_i = \bar{u},$$

тобто оптимальною оцінкою буде звичайне середнє $\bar{u}$ [1].

Модель процесу захисту в загальному вигляді задається наступними множинами: K – множина показників безпеки інформації; $P^{(C)}$ – множина параметрів зовнішнього середовища; $P^{(3)}$ – множина параметрів впливу зловмисників; $P^{(O)}$ – множина параметрів системи обробки та системи захисту інформації, що підлягає оцінці; $P^{(V)}$ – множина параметрів системи обробки та системи захисту інформації, якими можна управляти; $P^{(0)}$ – множина загальних ресурсів управління; $S^{(V)}$ – множина засобів та ресурсів управління. Тоді для вирішення задачі аналізу, тобто для визначення показників безпеки інформації, можна представити наступний вираз:

$$K = f(P^{(C)}, P^{(3)}, P^{(O)}, P^{(V)}, P^{(0)}, S^{(V)}),$$

де f вказує на існуючу залежність між множиною різномірних параметрів і множиною показників безпеки інформації.

Аналіз даної моделі показує складність моделювання процесу захисту інформації. Одним з найбільш складних з точки зору формалізації є процес моделювання впливу зловмисника у зв'язку із низьким ступенем передбачуваності його характеристик. Для реалізації процесу частіше всього використовують метод вибору найгіршого варіанту.

Загальний підхід до побудови інтегрального показника безпеки інформації на об'єкті Q можна представити у вигляді послідовності наступних кроків:

1. Формується вектор $X = (x_1, \dots, x_n)$ вихідних характеристик об'єкту, де циркулює інформація з обмеженим доступом, кожна з яких необхідна, а всі вони разом достатні для повного і всебічного контролю та оцінювання ступеня захищеності даної конфіденційної інформації.

2. Формується вектор $Q = (q_1, \dots, q_m)$ окремих комплексних показників захищеності, що представляють собою функції $q_i(x), i = \overline{1, m}$ вектора вихідних характеристик $x = x_1, \dots, x_n$ і оцінюючих різних складових захищеності досліджуваного об'єкту із використанням m різних критеріїв.

3. Формується вектор $H = (h_1, \dots, h_k)$ параметрів захищеності, що характеризує кожний окремий показник $q_i(x)$.

4. Обчислюється значення вектора $W = (w_1, \dots, w_m)$, де $w_1, \dots, w_m$ - вагові коефіцієнти, що визначають значимість окремих показників $q_1, \dots, q_m$ для інтегральної оцінки Q та задають ступінь впливу окремих показників $q_1, \dots, q_m$ на цю оцінку.

5. Вибирається вид синтезуючих функцій $Q(q)$, співставних вектору окремих показників $Q = (q_1, \dots, q_m)$, інтегральна оцінка Q (значення Q інтегрального показника $Q(q)$, що характеризує ступінь захищеності інформації досліджуваного об'єкта в цілому):

$$Q = Q(q) = Q(q; w), \quad W = (w_1, \dots, w_m).$$

Оскільки оптимальне вирішення питання про доцільний рівень затрат на захист полягає в тому, що він повинен бути прирівняний до рівня очікуваних втрат при порушенні захищеності, достатньо визначити тільки розмір втрат. Так спеціалістами фірми IBM запропонована наступна емпірична залежність очікуваних втрат від i -ої загрози для інформації:

$$R_i = 10^{(S_i + V_i - 4)},$$

де S_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної i -ої загрози;

V_i – коефіцієнт що характеризує значення можливого збитку під час її виникнення.

Запропоновані значення коефіцієнтів приведені у таблицях 2 та 3 відповідно.

Для обчислення рівня витрат, що забезпечують необхідний рівень захищеності інформації, необхідно насамперед знати, по-перше, повний перелік загроз інформації, по-друге, потенційну небезпеку для інформації кожної із загроз, і, по-третє, розмір витрат, необхідний для нейтралізації кожної із загроз.

Таблиця 2.

Можливі значення коефіцієнтів S_i

Очікувана (можлива) частота появи загрози	Запропоноване значення S_i
Майже ніколи	0
1 раз на 1000 років	1
1 раз на 100 років	2
1 раз на 10 років	3
1 раз на рік	4
1 раз на місяць (приблизно 10 разів на рік)	5
2 рази на тиждень (100 разів на рік)	6
3 рази на день (1000 разів на рік)	7

Таблиця 3.

Можливі значення коефіцієнтів V_i

Значення можливого збитку при виявленні загрози (у.о.)	Запропоноване значення V_i
1	0
10	1
100	2
1000	3
10000	4

Строго теоретичний підхід заснований на тому, що потенційно можливі прояви загроз та рівні потенційно можливих збитків є випадковими подіями, саме тому можуть

бути охарактеризовані законами розподілу та числовими характеристиками. Суть даної моделі на змістовному рівні може бути представлена у наступному вигляді:

1. Введене поняття «середній коефіцієнт можливого вияву загрози» кожного типу, при чому воно розглядається як випадкова змінна з відомим розподілом ймовірностей f . Функція розподілу повинна визначатися на основі обробки статистичних даних, що збираються в процесі реального функціонування системи.

2. Зроблено припущення, що кількість проявів загрози r_t на протязі фіксованого періоду часу (наприклад, одного року) залежить тільки від тривалості періоду спостереження і середнього коефіцієнту прояву, в силу чого для числа прояву загроз справедливим визнано розподіл Пуассона:

$$P(\bar{r} = r / \lambda) = \frac{(\lambda t) e^{-\lambda t}}{r!}.$$

3. По ряду значень числа загроз, отриманих для інтервалів різної тривалості, розподіл середнього коефіцієнта представлено у вигляді гамма-розподілу з параметрами, що характеризують ефективність захисту і визначеними по цілком певним рекурентним залежностям.

4. На основі інтегрування двох названих вище розподілень отримано безумовне розподілення ймовірностей числа прояву загроз за заданий період часу.

Розрахунки для оцінки очікуваних збитків полягають у наступному:

- спочатку розглядається середній збиток від прояву загроз і приймається нормальна функція його розподілу;

- по даним спостереження за проявами загроз і розміром збитків, що мали місце на інтервалах часу різної тривалості, корегуються параметри розподілу середнього збитку;

- виділяючи невизначені параметри із функції розподілу ймовірностей збитку, будується кінцевий розподіл розміру очікуваного збитку.

Теоретико-емпіричний підхід у відомій мірі оснований на синтезі основних положень теоретичного та емпіричного підходів. Суть синтезу полягає в тому, що на основі теоретико-ймовірносних методів будуються моделі, необхідні для визначення та прогнозування показників захищеності, а на основі збору та обробки статистичних даних, отриманих в ході теоретичних досліджень і практичних розробок проблем захисту інформації, формуються вихідні дані, необхідні для практичного використання моделей.

Розглянемо один з методів оцінки безпеки інформації, що відноситься до теоретико-емпіричного підходу. Комплексним показником оцінки безпеки при цьому обрано рівень безпеки інформації, що циркулює на об'єкті та характеризує можливість надання достатньої протидії виникненню каналів несанкціонованого отримання інформації (КНОІ) та причин порушення цілісності інформації (ППЦІ), що визначається як ймовірність забезпечення захисту інформації P_{zi} на об'єкті:

$$P_{zi} = P_{кноі} \cdot P_{ппці},$$

де $P_{кноі}$ – ймовірність захисту інформації від витоку через КНОІ; $P_{ппці}$ – ймовірність забезпечення цілісності інформації.

Забезпечити захист інформації від зазначених видів загроз можна, вирішивши, як вказувалось вище, комплекс задач захисту інформації. Для вирішення даних задач повинні бути обрані типові методи та засоби. Рівень безпеки інформації в кінцевому випадку визначається здатністю застосованих засобів захисту перекрити характерні для об'єкта КНОІ та усунути ППЦІ (рис. 2).

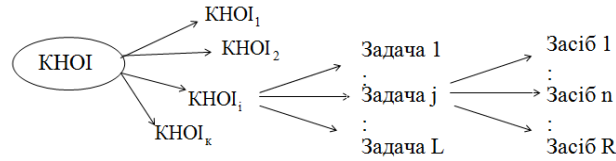


Рис. 2. Схематичне вирішення питання КНОІ об'єкту

Ймовірність захисту інформації на об'єкті від витоку через КНОІ визначається множиною каналів $\bar{K}$, характерних для даного об'єкту.

Виходячи з припущення про незалежність виникнення каналів, значення $P_{кноі}$ можна виразити як:

$$P_{кноі} = \prod_{i=1}^{\bar{K}} P_{кноіi}.$$

Проблему перекриття КНОІ можна вирішити реалізацією різного роду задач із множини L , характерного для i -го КНОІ:

$$P_{кноіi} = 1 - \prod_{j=1}^L (1 - P_3),$$

де P_3 – ймовірність забезпечення безпеки перекриття i -го КНОІ при вирішенні j -ої задачі захисту інформації. Це можливо зробити різними засобами із множини, що є в наявності на об'єкті:

$$P_3 = 1 - \prod_{n=1}^R (1 - P_{cp}),$$

де P_{cp} – ймовірність забезпечення безпеки n -м засобом захисту інформації. З урахуванням ризиків можна сформулювати:

$$P_3 = 1 - \prod_{n=1}^R (1 - P_{cp}) - \frac{\sum_{i=1}^n n_i}{\sum_{i=1}^n (u_i - u)^2}.$$

Аналогічні залежності можна сформулювати і для розрахунку $P_{ппці}$. Розрахунок даних ймовірностей може проводитися по відомим методикам на основі статистичних оцінок коефіцієнтів безпеки, що виражають відношення поточного значення небезпечного сигналу до нормованого значення для відповідного каналу витоку інформації [4].

Емпірична залежність між фінансовими затратами на захист інформації і фінансовими збитками від несанкціонованого доступу до неї має вигляд:

$$C = 10^2 / \bar{R},$$

де C – фінансові затрати на захист інформації (у.о.) та $\bar{R}$ – фінансові збитки від несанкціонованого доступу до інформації (у.о.). Звідси можна сформулювати графічну залежність (рис.3) для C та $\bar{R}$, де $C + \bar{R}$ – повна очікувана вартість захисту інформації (у.о.), $S+V$ – інтегральний коефіцієнт, що враховує частоту появи можливих загроз та викликаних ними збитків:

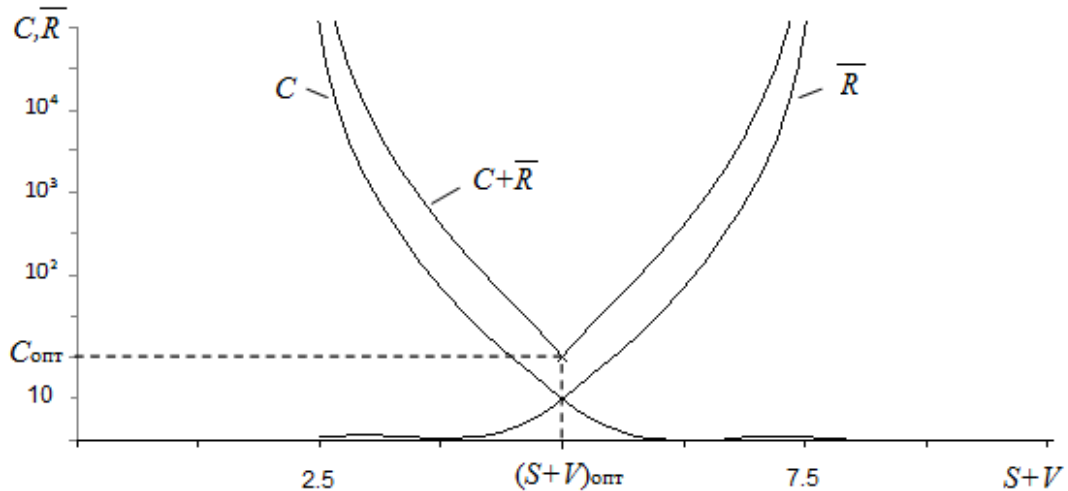


Рис. 3. Вартісні залежності захисту інформації від витоку через технічні канали витоку

Характеризуючи криву фінансових затрат на захист інформації (C), можна сказати, що зі зростанням інтегрального коефіцієнту $S+V$, що враховує частоту появи можливих загроз та викликаних ними збитків, спостерігається зменшення витрат на захист інформації. Для кривої фінансових збитків від несанкціонованого доступу до інформації ($\bar{R}$), є характерним збільшення витрат у випадку несанкціонованого доступу. Оптимальне значення досягається в точці екстремуму $C_{\text{опт}}$, оскільки саме при даному рівні затрат забезпечується мінімізація повної очікуваної вартості захисту інформації.

Висновки

В даній статті проведена класифікація технічних каналів витоку інформації з урахуванням можливих сучасних ризиків та аналіз їх особливостей. Приведена можливість кількісного визначення інтегрального показника, що характеризує ступінь безпеки інформації на об'єкті та визначає ймовірність витоку інформації, враховуючи всі фактори, що здійснюють значний вплив на його формування. На основі даного показника проводиться оцінка стану системи захисту інформації. Приведений строго-теоретичний та теоретико-емпіричний підхід для визначення рівня очікуваних втрат при порушенні захисту інформації. Якщо зібрати достатню кількість фактичних даних про проявлені загрози та їх наслідки, то розглянуті в статті моделі можна використовувати для вирішення широкого кола завдань по захисту інформації. Оптимальним варіантом вирішення поставленої задачі є витрати на захист інформації від витоку через технічні канали витоку фінансових коштів в розмірі $C_{\text{опт}}$, оскільки саме при даному рівні затрат забезпечується мінімізація повної очікуваної вартості захисту інформації.

Список літератури

1. Архипов, О.Є. Концептуалізація моделей ризиків / О.Є. Архипов, С.А. Архіпова // Захист інформації. – 2011. – №4. – С. 5–14.
2. Заячук, Я.І. Аналіз та оцінка ризиків інформаційної безпеки локальної обчислювальної мережі / Я.І. Заячук // Восточно-Европейский журнал передовых технологий. – 2012. – № 4/9(58). – С. 40-43.
3. Соболев, А.Н. Физические основы технических средств обеспечения информационной безопасности / А.Н. Соболев, В.М. Кирилов. – Москва: Гелиос АРВ, 2004. – 215 с.
4. Сёмкин, С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации / С.Н. Сёмкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок. – Москва: Гелиос АРВ, 2005. – 183 с.

КРИТЕРИИ ОЦЕНКИ ВЕРОЯТНОСТИ УТЕЧКИ ИНФОРМАЦИИ ЧЕРЕЗ ТЕХНИЧЕСКИЕ КАНАЛЫ

Н.Г. Романюков

Главное управление министерства внутренних дел Украины в Одесской области,
ул. Еврейская, 12, Одесса, 65014, Украина; e-mail: kolyanr21@gmail.com

Проведена классификация современных технических каналов утечки информации и анализ их особенностей с учетом современных возможных рисков. Предложен способ количественного определения интегрального показателя, характеризующего степень безопасности информации на объекте и определяющего вероятность утечки информации, учитывая все факторы, которые осуществляют значительное влияние на его формирование. На основе данного показателя проводится оценка состояния системы защиты информации. Приведен строго-теоретический и теоретико-эмпирический подход для определения уровня ожидаемых потерь при нарушении защиты информации, что позволяет, при наличии возможностей сбора достаточного количества фактических данных о проявленных угрозах и их последствиях, применять рассмотренные в статье модели для решения широкого круга задач по защите информации. Вычисляется эмпирическая величина уровней затрат, при которой обеспечивается минимизация полной ожидаемой стоимости защиты информации.

Ключевые слова: технические каналы утечки информации, модель процесса защиты, вероятность обеспечения безопасности.

CRITERIA FOR EVALUATING THE PROBABILITY OF INFORMATION LEAKAGE THROUGH TECHNICAL CHANNELS

N.G. Romanykov

General directorate of the ministry of internal affairs of Ukraine in Odessa region,
12 Evrejskaja Str., Odessa, 65014, Ukraine; e-mail: kolyanr21@gmail.com

Classification of modern technical channels of information leakage and the analysis of their characteristics, taking into account today's risks. A method for the quantitative determination of the integral index, which characterizes the degree of safety information on the object and determines the probability of leakage of information taking into account all the factors that exercise a significant influence on its formation. On the basis of this indicator assesses the status of information security systems. We have a strictly theoretical and theoretical-empirical approach to determine the level of expected losses in violation of the protection of information, allowing, where possible, to gather sufficient evidence of the manifestation of threats and their consequences, are considered to apply to become a model for a wide range of applications for protection information. Calculate the empirical value of the cost levels at which minimizes the total expected cost of information protection.

Keywords: technical channels of information leakage protection process model, the probability of safety.

METHODS OF MATHEMATICAL DESIGN AND MACHINE AUTHENTICATION OF NON - STATICS ANOMALOUS DIFFUSIVE PROCESSES

S.A. Polozhaenko, Omar Muajad Abdullach

Odessa national polytechnic university,
1 Shevchenko Ave., Odessa 65044, Ukraine; e-mail: omarukrain@yahoo.com

For a class of the non-statics abnormal diffusive processes which mathematical models are formalized in the form of variation inequalities in private derivatives, the method of mathematical modeling based on optimizing procedure is offered. Thus the problem of realization of mathematical models of non-statics abnormal diffusive processes is reduced to search of a maximum of function of Hamilton defined in space of conditions of studied processes. The method of parametrical identification of mathematical models of non-statics abnormal diffusive processes in case of an induction problem definition of research is also offered. The method is reduced to use of optimizing procedure of a method of a projection of a gradient. Possibility of the solution of a problem of parametrical identification, as for linear, and nonlinear mathematical models of non-statics abnormal diffusive processes is proved.

Keywords: abnormal diffusive process, mathematical model, variation, variation inequality, optimization, principle of a maximum functionality, gradient, parametrical identification.

Introduction

In a number of important applied tasks technological (or naturally natural) processes are characterized by deviations from well-known physical laws. In this regard these processes received in special literature the name anomalous (in particular, abnormal diffusive) [1 — 4]. First of all, the rheological processes connected with mining can be an example of such processes. For the description of abnormal diffusive processes, as the adequate mathematical models (MM) it was offered to use the device of variation inequalities in private derivatives [5 — 8].

As it was shown in work [9], in practical appendices it is most convenient to use the following formalization of abnormal diffusive processes.

Let the function $\psi(t, \bar{z})$, defined on a bounded open set Ω of the space $\mathfrak{R}^n$, $n = 1, 2$, with smooth boundary Γ and the time interval $(0, t_k)$ for $t_k < \infty$, $Q = \Omega \times (0, t_k)$, $\Sigma = \Gamma \times (0, t_k)$ is the solution of the varitional inequality

$$\psi \in K : \left(m(t) \frac{\partial \psi}{\partial t}, v - \psi \right) + (B(t)\psi, v - \psi) + j(v) - j(u) \geq (f, v - \psi) \quad \forall v \in H^1(\Omega), \quad (1)$$

$$\psi(0, \bar{z}) = \psi_0(\bar{z}), \quad (2)$$

where the operator $B(\gamma)$ specifies a linear transformation $B(\gamma): H^1(\Omega) \rightarrow H^1(\Omega)$ and is defined by the bilinear form:

$$(B(t)\psi, v - \psi) = \int_{\Omega} \left(\sum_{i=1}^n \frac{\partial \psi}{\partial z_i} \cdot \frac{\partial (v - \psi)}{\partial z_i} \right) d\bar{z}, \quad (3)$$

f – the driving function of the process, for which the operation $(f, v - \psi)$ coincides with the scalar product in $L^2(\Omega)$, i.e. $(f, v - \psi) = \int_{\Omega} [f(\bar{z}), v - \psi] d\Omega$ or $(f, v - \psi) = \int_{\Gamma} [f(\bar{z}), v - \psi] d\Gamma$ (hereinafter, for simplicity, restrict ourselves to the tasks at the border Γ); $j(\cdot)$ — convex functionals defining the kind of physical process in rheology and which are specified as follows

$$j(\cdot) = \int_{\Gamma} \varphi(\psi, \bar{z}) \cdot \lambda(\psi) d\Gamma, \quad j(\cdot) = \int_{\Omega} \varphi(\psi, \bar{z}) \cdot \lambda(\psi) d\Omega. \quad (4)$$

In the relation (4) accept that $\varphi(\cdot)$ – is a continuous function, $\lambda(\cdot)$ – is continuous differentiable or not having the properties of differentiable functions.

Space of admissible functions $\varphi(\cdot)$ and $\lambda(\cdot)$ are defined as $\Delta \in L^\infty(\bar{Q})$, $\Lambda \in L^\infty(\bar{Q})$ where it is assumed that $\varphi(\cdot), \lambda(\cdot) \in L^\infty(\bar{Q})$, $\bar{Q} = \bar{\Omega} \times (0, t_k)$ and the spaces Δ and Λ are Banach with respect to the norm $\|\varphi(\psi, \bar{z})\|_{\Delta} = \|\varphi(\psi, \bar{z})\|_{L^\infty(\bar{Q})}$.

Method of mathematical modelling of abnormal diffusive processes

The proposed method for solving variational inequalities of the form (1), (2) is based on the proof of the following statements.

To find the optimal solution $\psi(t, \bar{z})$ of the variational inequality (1), (2) there must exist a nonzero continuous function $p(t, \bar{z})$, so that at any time t in the interval $0 \leq t \leq T$ (T — time of physical processes) the Hamiltonian function $\tilde{H}$ in the spatial domain Ω (or on its boundary Γ) would take the maximum value, where

$$\tilde{H} = \langle ((B(t)\tilde{\psi}, \tilde{v} - \tilde{\psi}) + \phi(\tilde{v}) - \phi(\tilde{\psi}) - (\theta(\tilde{\psi}, \tilde{v}), \tilde{v} - \tilde{\psi}) - (f, (\tilde{v} - \tilde{\psi}))), \tilde{p} \rangle.$$

Carry out a preliminary series of reforms to simplify the original formulation of the problem. Introduce the notation

$$\varphi(t, \bar{z}) \cdot \lambda(\psi) = \Phi(\psi), \quad \varphi(t, \bar{z}) \cdot \lambda(v) = \Phi(v),$$

and

$$\phi(\psi) = \int_{\Gamma} \Phi(\psi) d\Gamma, \quad \phi(v) = \int_{\Gamma} \Phi(v) d\Gamma.$$

In addition, introduce an additional unknown function $\theta(\psi, v)$, the structure corresponding to the functionals $j(\cdot)$, such that

$$(\theta(\psi, v), v - \psi) \geq 0 \quad \forall v \in K.$$

Taking into account the executed transformations introduce the relations (1), (2) in the form

$$\begin{aligned} \psi \in K : & \left(m(t) \frac{\partial \psi}{\partial t}, v - \psi \right) + (B(t), v - \psi) + \phi(v) - \phi(\psi) - \\ & - (\theta(\psi, v), v - \psi) = (f, v - \psi) \quad \forall v \in K \end{aligned} \quad (5)$$

$$\psi(0, \bar{z}) = \psi_0(\bar{z}). \quad (6)$$

To solve the problem of finding a state function $\psi(t, \bar{z})$, use an optimization procedure of the Pontryagin maximum principle [10], for which choose the following performance criterion

$$J = \min \int_0^T \int_{\Gamma} |v - \psi| dt d\Gamma \quad (7)$$

The physical meaning of this criterion follows from the next. The trial function $v(t, \bar{z})$ is some approximation of the unknown function $\psi(t, \bar{z})$, reflecting only the essence of physics in the specific process. Therefore, the adequacy of physical processes caused by the action of functions $v(t, \bar{z})$ and $\psi(t, \bar{z})$, is provided up to the accuracy within the difference between these functions. In this case, the integral difference between the trial $v(t, \bar{z})$ and the unknown $\psi(t, \bar{z})$ functions can be regarded as a quantitative measure or a penalty for the deviation of the actual flow of the process from its true value.

Obtain the necessary optimality conditions of the problems (5) (6), (7).

According to [6], introduce a new coordinate

$$\frac{\partial^2 \sigma}{\partial t \partial z} = |v - \psi|^2 \Big|_{z \in \Gamma}. \quad (8)$$

Thus, the original problem will be considered in $(n+1)$ -dimensional space with the equation of dynamics

$$\begin{aligned} \tilde{\psi} \in K : & \left(m(t) \frac{\partial \tilde{\psi}}{\partial t}, \tilde{v} - \tilde{\psi} \right) + (B(t), \tilde{v} - \tilde{\psi}) + \phi(\tilde{v}) - \phi(\tilde{\psi}) - \\ & - (\theta(\tilde{\psi}, \tilde{v}), \tilde{v} - \tilde{\psi}) = (f, \tilde{v} - \tilde{\psi}) \quad \forall \tilde{v} \in K, \end{aligned} \quad (9)$$

where $\tilde{\psi} = (\sigma, \psi_1, \dots, \psi_n)$, $\tilde{v} = (\sigma, v_1, \dots, v_n)$, with the initial conditions $\tilde{\psi}(0, \bar{z}) = [0, \psi_0(\bar{z})]$

Assume that we have found $\psi(t, \bar{z})$. This condition corresponds to the relation

$$\min \int_0^T \int_{\Gamma} |\tilde{v} - \tilde{\psi}|^2 dt d\Gamma \rightarrow J_{\min} = J^*.$$

At $t = \tau$ ($0 \leq \tau \leq T$) perform a needle-shaped variation with the duration ε . As a result of the variation performed the value of the functional J (7) changes

$$\hat{J} = \int_0^T \int_{\Gamma} |\tilde{v} - \tilde{\psi}| dt d\Gamma > J_{\min}.$$

Write down the detailed result of the variation

$$\begin{aligned} \delta \tilde{v} = \tilde{v} - \tilde{\psi} = \varepsilon \{ & [(B(t)\tilde{\psi}, \tilde{v} - \tilde{\psi}) + \phi(\tilde{v}) - \phi(\tilde{\psi}) - (\theta(\tilde{\psi}, \tilde{v}), \tilde{v} - \tilde{\psi}) - (f, (\tilde{v} - \tilde{\psi}))] - (B(t)\tilde{\psi}, \psi) + \\ & + \phi(\tilde{\psi}) - (\theta(\tilde{\psi}), \tilde{\psi}) - (f, \tilde{\psi}) \}_{t=\tau}. \end{aligned} \quad (10)$$

Express $\tilde{v}$ through the variation and optimal function of the state

$$\tilde{v} = \tilde{\psi} + \delta \tilde{v}. \quad (11)$$

Substituting (11) into (9), obtain

$$\begin{aligned} \tilde{\psi} \in K : \left(m(t) \frac{\partial \tilde{\psi}}{\partial t}, (\tilde{\psi} + \delta \tilde{v}) - \tilde{\psi} \right) = & (B(t)\tilde{\psi}, (\tilde{\psi} + \delta \tilde{v}) - \tilde{\psi}) + \phi(\tilde{\psi} + \delta \tilde{v}) - \phi(\tilde{\psi}) - \\ & - (\theta(\tilde{\psi}, (\tilde{\psi} + \delta \tilde{v})), (\tilde{\psi} + \delta \tilde{v}) - \tilde{\psi}) - (f, (\tilde{\psi} + \delta \tilde{v}) - \tilde{\psi}) \quad \forall \tilde{v} \in K. \end{aligned} \quad (12)$$

For further transformations use the coordinate-wise analog (12)

$$\begin{aligned} \tilde{\psi}_i \in K : \left(m(t_i) \frac{\partial \tilde{\psi}_i}{\partial t}, (\tilde{\psi}_i + \delta \tilde{v}_i) - \tilde{\psi}_i \right) = & (B(t)\tilde{\psi}_i, (\tilde{\psi}_i + \delta \tilde{v}_i) - \tilde{\psi}_i) + \phi(\tilde{\psi}_i + \delta \tilde{v}_i) - \phi(\tilde{\psi}_i) - \\ & - (\theta(\tilde{\psi}_i, (\tilde{\psi}_i + \delta \tilde{v}_i)), (\tilde{\psi}_i + \delta \tilde{v}_i) - \tilde{\psi}_i) - (f, (\tilde{\psi}_i + \delta \tilde{v}_i) - \tilde{\psi}_i) \quad \forall \tilde{v}_i \in K \quad i = 0, 1, \dots, n. \end{aligned} \quad (13)$$

$$- (\theta(\tilde{\psi}_i, (\tilde{\psi}_i + \delta \tilde{v}_i)), (\tilde{\psi}_i + \delta \tilde{v}_i) - \tilde{\psi}_i) - (f, (\tilde{\psi}_i + \delta \tilde{v}_i) - \tilde{\psi}_i) \quad \forall \tilde{v}_i \in K \quad i = 0, 1, \dots, n.$$

Expand (13) in Taylor series and restrict the consideration with the quantities of 1-th order of infinitesimally

$$\begin{aligned} m(t) \left(\frac{\partial \tilde{\psi}_i}{\partial t} + \frac{\delta \tilde{v}_i}{\partial t} \right) = & (B(t)\tilde{\psi}_i, \tilde{\psi}_i) + \phi(\tilde{\psi}_i) - (f, \tilde{\psi}_i) + \sum_{i=0}^n \frac{\partial [(B(t)\tilde{\psi}_i, \tilde{\psi}_i)_i + \phi(\tilde{\psi}_i) - (f, \tilde{\psi}_i)]}{\partial \tilde{v}_i} \delta \tilde{v}_i, \\ & i = 0, 1, \dots, n. \end{aligned} \quad (14)$$

From (14) it follows that

$$m(t) \frac{\partial \tilde{v}_i}{\partial t} = \sum_{i=0}^n \frac{\partial [(B(t)\tilde{\psi}_i, \tilde{\psi}_i) + \phi(\tilde{\psi}_i) - (f, \tilde{\psi}_i)]}{\partial \tilde{v}_i} \delta \tilde{v}_i, \quad i = 0, 1, \dots, n. \quad (15)$$

Now turn to $t = T$. Define a variation of the functional at $t = T$

$$\delta J_{t=T} = \hat{J} - J_{\min} > 0 \quad \text{or} \quad -\delta J_{t=T} = -\delta \sigma_{Hb=T} \leq 0.$$

Introduce the variable $\tilde{p}(t, \bar{z})$ so that when $t = T$ this condition is satisfied

$$-\delta J_{t=T} = -\delta \sigma(T) = \langle \delta \tilde{v}, \tilde{p} \rangle_{t=T}. \quad (16)$$

Coordinate wise analog (16) is as follows: $-\delta J_{t=T} = -\delta \sigma(T) = \langle \delta \tilde{v}_i, \tilde{p}_i \rangle_{t=T}, \quad i = 0, 1, \dots, n.$

Since $\delta \sigma(T) > 0$, in order to satisfy this relation there should take place:

$$p^0(T, \bar{z}_i) = -1; p_j(T, \bar{z}) = 0, \text{ where } i = 0, 1, \dots, n; j = 1, \dots, n.$$

Thus, if the optimal solution is not found, then $-\delta J < 0$, and for the optimal solution $-\delta J = 0$ is valid, since the variation of functional must be zero for the optimal solution.

Associate a variable $\tilde{p}(t, \bar{z})$ to the dynamic equation of the process observed through trial function $v(t, \bar{z})$. Find a variable $\tilde{p}(t, \bar{z})$ which satisfies

$$\langle \delta \tilde{v}(t, \bar{z}), \tilde{p}(t, \bar{z}) \rangle = \langle \delta \tilde{v}(T, \bar{z}), \tilde{p}(T, \bar{z}) \rangle_{\tau+\varepsilon \leq t \leq T} = \text{const}.$$

Then we have

$$\frac{\partial}{\partial t} \langle \delta \tilde{v}(t, \bar{z}), \tilde{p}(t, \bar{z}) \rangle = \left\langle \frac{\partial \delta \tilde{v}(t, \bar{z})}{\partial t}, \tilde{p}(t, \bar{z}) \right\rangle + \left\langle \frac{\partial \tilde{p}(t, \bar{z})}{\partial t}, \delta \tilde{v}(t, \bar{z}) \right\rangle_{\tau+\varepsilon \leq t \leq T} = 0. \quad (17)$$

Coordinate wise analog (17) is

$$\sum_{i=0}^n \frac{\partial \delta \tilde{v}_i(t, \bar{z})}{\partial t} \tilde{p}_i(t, \bar{z}) + \sum_{i=0}^n \delta \tilde{v}_i(t, \bar{z}) \frac{\partial \tilde{p}_i(t, \bar{z})}{\partial t} = 0, \quad i = 0, 1, \dots, n. \quad (18)$$

Substitute in (18) the value of the derivative $\frac{\partial \delta \tilde{v}(t, \bar{z})}{\partial t}$ from (15)

$$m(t) \sum_{i=0}^n \tilde{p}_i \times \sum_{i=0}^n \frac{\partial [(B(t) \tilde{\psi}_i, \tilde{\psi}_i) + \phi(\tilde{\psi}_i) - (f, \tilde{\psi}_i)]}{\partial \tilde{v}_i} \delta \tilde{v}_i + \sum_{i=0}^n \delta \tilde{v}_i \frac{\partial \tilde{p}_i}{\partial t} = 0, \quad i = 0, 1, \dots, n. \quad (19)$$

Change the order of summation in (19)

$$m(t) \sum_{i=0}^n \delta \tilde{v}_i + \left[\sum_{i=0}^n \tilde{p}_i \frac{\partial [(B(t) \tilde{\psi}_i, \tilde{\psi}_i) + \phi(\tilde{\psi}_i) - (f, \tilde{\psi}_i)]}{\partial \tilde{v}_i} + \frac{\partial \tilde{p}_i}{\partial t} \right] = 0, \quad i = 0, 1, \dots, n.$$

Finally get

$$\frac{\partial \tilde{p}_i}{\partial t} = - \sum_{i=0}^n \frac{\partial [(B(t) \tilde{\psi}_i, \tilde{\psi}_i) + \phi(\tilde{\psi}_i) - (f, \tilde{\psi}_i)]}{\partial \tilde{v}_i} \tilde{p}_i, \quad i = 0, 1, \dots, n.$$

Note that this equation is the dual of (5), and the variable $\tilde{p}(t, \bar{z})$ is expressed through the function of phase.

Again turn to the variation of functional (7) at $t = T$: $-\delta J_{t=T} = \langle \delta \tilde{v}(t, \bar{z}), \tilde{p}(t, \bar{z}) \rangle_{t=T} = 0$

Replace the variation $\delta \tilde{v}$ with the value of (10), reduce by ε and, since τ can be arbitrary, obtain

$$\begin{aligned} & \langle ((B(t) \tilde{\psi}, \tilde{v} - \tilde{\psi}) + \phi(\tilde{v}) - \phi(\tilde{\psi}) - (\theta(\tilde{\psi}, \tilde{v}), \tilde{v} - \tilde{\psi}) - (f, (\tilde{v} - \tilde{\psi}))), \tilde{p} \rangle_{t=\tau} - \\ & - \langle ((B(t) \tilde{\psi}, \tilde{\psi}) + \phi(\tilde{\psi}) - (f, \tilde{\psi})), \tilde{p} \rangle_{t=T} = 0. \end{aligned} \quad (20)$$

From (20) it follows that the second summand in it corresponds to the optimal solution of the variational inequality (5). In the case when the optimal solution $\psi(t, \bar{z})$ is found, variation of functional J will be zero, i.e. $\delta J = 0$. Given this, the first summand in (20),

defined by the Hamiltonian function

$$\tilde{H} = \langle ((B(t)\tilde{\psi}, \tilde{v} - \tilde{\psi}) + \phi(\tilde{v}) - \phi(\tilde{\psi}) - (\theta(\tilde{\psi}, \tilde{v}), \tilde{v} - \tilde{\psi}) - (f, (\tilde{v} - \tilde{\psi}))), \tilde{p} \rangle, \quad (21)$$

should take the maximum value. Thus, the above statement is proven. Let's show the possibility of determining the maximum value of Hamiltonian function.

Coordinate wise analog (21) is defined by

$$\begin{aligned} \tilde{H} = \langle ((B(t)\tilde{\psi}_i, \tilde{v}_i - \tilde{\psi}_i) + \phi(\tilde{v}_i) - \phi(\tilde{\psi}_i) - (\theta(\tilde{\psi}_i, \tilde{v}_i), \tilde{v}_i - \tilde{\psi}_i) - (f, (\tilde{v}_i - \tilde{\psi}_i))), \tilde{p}_i \rangle, \\ i = 0, 1, \dots, n. \end{aligned} \quad (22)$$

To maximize the value of the function $\tilde{H}$, it's necessary to set all the partial derivatives of this function to zero by a testing variable $v(t, \bar{z})$, that taking into account (22) gives the system of equations

$$\frac{\partial \tilde{H}}{\partial v_i} = 0, \quad i = 0, 1, \dots, n. \quad (23)$$

Coordinate wise analog (22) contains $(n+1)$ of v_i functions, $(n+1)$ of θ_i functions and $(n+1)$ of p_i functions. Since the equations (23) are only $(n+1)$, and the unknown are $(3n+3)$, then the system (23) cannot be solved. To solve (23) define also the partial derivatives

$$\frac{\partial \tilde{H}}{\partial \theta_i} = \tilde{p}_i, \quad i = 0, 1, \dots, n. \quad (24)$$

$$\frac{\partial \tilde{H}}{\partial p_i} = \left[m(t_i) \frac{\partial \tilde{\psi}_i}{\partial \alpha}, \tilde{v}_i - \tilde{\psi}_i \right], \quad i = 0, 1, \dots, n. \quad (25)$$

In this case, the solution of (23) can be obtained.

As a result of the reasoning done, the scheme of the algorithm for solving variational inequality (5) using the maximum principle can be represented as follows:

1. The dynamic equation (9), subject to the additional coordinate σ is written down.
2. An auxiliary function (Hamilton) $\tilde{H}$ in accordance with the expression (22) is compiled.
3. A test function $v(t, \bar{z})$ that delivers maximum $\tilde{H}$ functions in accordance with the expression (23) is determined. For the redefinition of the independent variables θ and p the system (23) is supplemented with equations (24) and (25).
4. The unknown variable $\psi(t, \bar{z})$ is determined by the test variable $v(t, \bar{z})$, which gives the maximum value of function $\tilde{H}$.

Method of parametrical identification of abnormal diffusive processes

At statement of an inductive task - (1) — (4), the method focused on numerical machine realization can be offered parametrical identification of MM of a look. The essence of a method consists in the following.

It agrees [11], to MM (1) — (4) (in increments) it is possible to present in a look

$$-\frac{m\partial(\Delta\psi)}{\partial t}-\int\sum_{\Omega i=1}^n\left[B(t)\frac{\partial^2(\Delta\psi)}{\partial z_i^2}|\Delta v|\right]dz\geq\sum_{j=1}^k\zeta_j(z)f_j,\quad\forall\psi,v\in K, \quad (26)$$

$$\Delta\psi(0,z)=\Delta\psi_0(z), \quad (27)$$

where $\psi=\psi(t,z)$ — sought function; $v=v(t,z)$ — trial function; K — a lot, of that is defined functions $\psi=\psi(t,z)$ and $v=v(t,z)$; f — exciting function; k — number of exciting functions; $\zeta(z)$ — Dirac's function; $m=m(\cdot)$ and $B=B(\cdot)$ — identified parameters.

As criterion of quality of the solution of a problem of identification we will accept functionality of a look

$$J[m(\cdot),B(\cdot)]=\sum_{j=1}^k\left\{\int_{T_j}[\psi'(t,z,m,B)-F_j^\psi(t)]^2dt\right\}, \quad (28)$$

where $\psi'(t,z,m,B)$ — exact values sought functions; $F_j^\psi(t)$ — measured values of the sought function; T — time of measurements.

Let's show that the accepted criterion of quality will be differentiable in any point of spatial area $\bar{z}\in\Omega$ (including and its border Γ), i.e. an increment (28) equal

$$\Delta J=J[(m+h^m),(B+h^B)]-J(m,B)$$

represent able in a look

$$\Delta J=\int_{\Omega}\left\{J'(m,B)h^m\right\}dz+\left\{J'(m,B)h^B\right\}dz+\left\{O(\|h^m\|_{L^2})+O(\|h^B\|_{L^2})\right\}, \quad (29)$$

where $J'(m,B)$ — some function from $L^2(\Omega)$; $O(\|h^m\|_{L^2})$ and $O(\|h^B\|_{L^2})$ — residual members such, that $\lim_{\alpha^m\rightarrow 0}[O(\alpha^m)(\alpha^m)^{-1}]=0$, $\lim_{\alpha^m\rightarrow 0}[O(\alpha^m)(\alpha^m)^{-1}]=0$.

Let's write down formally a functionality increment

$$\begin{aligned} \Delta J &= \sum_{j=1}^k\left\{\int_{\Omega}\left\{\left[\psi(t,z_j,v,B)+\Delta\psi(t,z_j)-F_j^\psi(t)\right]^2-\left[\psi(t,z,m,B)-F_j^\psi(t)\right]^2\right\}dz\right\}= \\ &= \sum_{j=1}^k\left\{\int_{\Omega}\left\{\left[\psi(t,z,m,B)-F_j^\psi(t)\right]^2+\Delta\psi(t,z_j)^2-\left[\psi(t,z_j,v,B)-F_j^\psi(t)\right]^2\right\}dz\right\}= \\ &= \sum_j^k\left\{\int_{\Omega}2\left[\psi(t,z,m,B)-F_j^\psi(t)\right]\Delta\psi(t,z)dz+\int_{\Omega}\Delta\psi^2(t,z)dz\right\}. \end{aligned} \quad (30)$$

Let's transform this expression to a look (29). For this purpose we will enter into consideration of function $p_\psi^*(t,z)\equiv p_\psi^*(t,z,m,B)$ as the solution of the following regional task

$$-\frac{m\partial p_\psi^*}{\partial t}(v-\psi)-\int\sum_{\Omega i=1}^n\left[B(t)\frac{\partial^2 p_\psi^*}{\partial z_i^2}|\Delta v|\right]dz\geq\sum_{j=1}^k\zeta_j(z)f_j,\quad\forall\psi,v\in K, \quad (31)$$

$$p_{\psi}^*|_{t=t_k} = 2[\psi(t_k, z, m, B) - F_j^{\psi}(t)] p_{\psi}^*|_{t=t_k} \quad \forall z \in \Omega. \quad (32)$$

The first integral in the first composed in the right part of equality (30) taking into account (26), (27), (31), (32) it will be transformed so

$$\begin{aligned} I &= 2[\psi(t, z, m, B) - F_j^{\psi}(t)] \Delta \psi(t, z) dz = \int_{\Omega} p_{\psi}^*(t_k, z_j) \Delta \psi(t_k, z_j) dz = \\ &= \int_{\Omega} \left[\int_0^{t_k} \frac{\partial}{\partial t} (p_{\psi}^*, \Delta \psi) dt \right] dz = \int_{\Omega} \left[\int_0^{t_k} \left(\frac{\partial p_{\psi}^*}{\partial t} \Delta \psi + p_{\psi}^* \frac{\partial (\Delta \psi)}{\partial t} \right) dt \right] dz = \\ &= \int_{\Omega} \left[\int_0^{t_k} \left\{ \frac{1}{m(\cdot)} \left[\sum_{i=1}^n \left[B(\cdot) \frac{\partial^2 p_{\psi}^*}{\partial z_i^2} |v| \right] \right] \Delta \psi + p_{\psi}^* \left[\sum_{i=1}^{nk} \left[B(\cdot) \frac{\partial^2 p_{\psi}^*}{\partial z_i^2} |\Delta v| \right] \right] \right\} dt \right] dz. \end{aligned}$$

Integrating the last expression in spatial area, we will receive the following result

$$\begin{aligned} I_{\psi}' &= \int_0^{t_k} \left\{ \frac{1}{m(\cdot)} \left[\sum_{i=1}^n \left[B(\cdot) \frac{\partial^2 p_{\psi}^*}{\partial z_i^2} |v| \right] \right] \Delta \psi + p_{\psi}^* \left[\sum_{i=1}^n \left[B(\cdot) \frac{\partial^2 p_{\psi}^*}{\partial z_i^2} |\Delta v| \right] \right] \right\} dt = \\ &= \int_0^{t_r} \frac{1}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] \Delta \psi dt. \end{aligned}$$

Here, and further, designation $(\cdot)$ determines as the linear (from space), and non-linear (from required function) parameter. The second integrals in composed in the right part (30) the members of the look $\left[O(\|h\|_{L_2}^{\psi}) \right]$, presented in (29) and written down for spatial problem definition define. Let's have in this case: $\Delta J = \int_{\Omega} \frac{1}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] h^{\psi} dz + O(\|h\|_{L_2}^{\psi})$ and, the step h^{ψ} determines cooperative value by steps h^m and h^B . As a result we will receive that the increment of functionality (28) is represented in the form of expression

$$\Delta J = \int_{\Omega} \frac{1}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] h^{\psi} dz + O(\|h\|_{L_2}^{\psi}).$$

Thus, required representation (29) for functionality (28) is received, and the gradient of this functionality looks like

$$J'[m(\cdot), B(\cdot)] \equiv \frac{1}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right], \quad \forall z \in \Omega, t \in [0, t_k]. \quad (33)$$

Further, having a gradient (33) and using procedure of a method of a projection of the gradient [11], defined by ratios

$$Q = \{q(t) : q(t) \in L_2[0, t_k], a \leq q(t) \leq b, \quad \forall t \in [0, t_k]\} \quad \Pr_q[q(t)] = \begin{cases} q(t), & a \leq q(t) \leq b, \\ a, & q(t) < a, \\ b, & q(t) > b. \end{cases}$$

For identified functions $m(\cdot)$ and $B(\cdot)$ also we will receive final ratios on an offered method of parametrical identification

$$m_{u+1}(\cdot) = \begin{cases} m_r - \frac{\alpha_m}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right]; & m_{\min} \leq m_r - \frac{\alpha_m}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] \leq m_{\max}; \\ m_{\min}, & m_r - \frac{\alpha_m}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] < m_{\min}; \\ m_{\max}, & m_r - \frac{\alpha_m}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] > m_{\max}, \end{cases}$$

$$B_{u+1}(\cdot) = \begin{cases} B_r - \frac{\alpha_B}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right], & B_{\min} \leq B_r - \frac{\alpha_B}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] \leq B_{\max}; \\ B_{\min}, & B_r - \frac{\alpha_B}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] < B_{\min}; \\ B_{\max}, & B_r - \frac{\alpha_B}{m(\cdot)} \left[\left(\sum_{i=1}^n B(\cdot) p_{\psi}^* |v| \right) \right] > B_{\max}, \end{cases}$$

where α_m and α_B — method parameters, defined by practical consideration, r — step of the numerical decision.

Conclusion

The conducted numerical researches showed that the offered methods of mathematical model operation and parametrical identification of the abnormal diffusion processes, based on iterative procedures of optimization possess good convergence (the decision is reached no more, than for 8 - 10 iterations) at accuracy of the decision 0.2% are not lower.

References

1. Бернардинер, М.Г. Гидродинамическая теория фильтрации аномальных жидкостей / М.Г. Бернардинер, В.М. Ентов. — М.: Наука, 1975. — 199 с.
2. Положаенко, С.А. Оптимизационный подход к исследованию моделей объектов, представленных в виде вариационных неравенств / С.А. Положаенко // Автоматика, автоматизация, электротехнические комплексы и системы. — 2002. — № 1. — С. 6-12.
3. Положаенко, С.А. Математические модели процессов течения аномальных жидкостей / С.А. Положаенко // Моделювання та інформаційні технології. — 2001. — № 9. — С. 14-21.
4. Ажогин В.В. Автоматизированное проектирование математического обеспечения АСУТП / В.В. Ажогин, М.З. Згуровский. — К.: Высшая школа, 1986. — 336 с.
5. Дюво, Г. Неравенства в механике и физике / Г. Дюво, Ж.Л. Лионс. — М.: Наука, 1980. — 382 с.
6. Киндерлерер, Д. Введение в вариационные неравенства и их приложения / Д. Киндерлерер, Г. Стампахья. — М.: Мир, 1983. — 256 с.

7. Панагиотопулос, П. Неравенства в механике и их приложения / П. Панагиотопулос. – М.: Мир, 1989. – 494 с.
8. Верлань, А.Ф. Математическое моделирование аномальных диффузионных процессов / А.Ф. Верлань, С.А. Положаенко, Н.Г. Сербов. – К.: Наукова думка, 2011. – 416 с.
9. Мацевитый Ю. М. Моделирование нелинейных процессов в распределенных системах / Ю.В. Мацевитый, В.Е. Прокофьев. – К.: Наукова думка, 1985. – 303 с.
10. Понтрягин, Л.С. Математическая теория оптимальных процессов / Л.С. Понтягин, В.Г. Болтянский, Р.В. Гамкрелидзе, Е.Ф. Мищенко. – М.: Наука, 1961. – 352 с.
11. Polozhaenko, S.A. Qualitative analysis of identification problem for water-oil reservoir by parameters of mathematical model setting / S.A. Polozhaenko, Yu.V. Grigorenko, O.B. Babiychuk // Електротехнічні та комп'ютерні системи. – 2013. - № 9. – С. 89-97.

МЕТОДИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ТА МАШИННОЇ ІДЕНТИФІКАЦІЇ НЕСТАЦІОНАРНИХ АНОМАЛЬНИХ ДИФУЗІЙНИХ ПРОЦЕСІВ

С.А. Положаєнко, Омар Муаяд Абдуллах

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

Для класу нестационарных аномальных диффузионных процессов, математичні моделі яких формалізуються у вигляді варіаційних нерівностей у часткових похідних, запропоновано метод математичного моделювання, заснований на оптимізаційній процедурі. При цьому задача реалізації математичних моделей нестационарных аномальных диффузионных процесів зводиться до відшукування максимуму функції Гамільтона, яку визначено у просторі стану досліджуваних процесів. Також запропоновано метод параметричної ідентифікації математичних моделей нестационарных аномальных диффузионных процесів на випадок індукційної постановки задачі дослідження. Метод зводиться до застосування оптимізаційної процедури методу проекції градієнта. Обґрунтовано можливість розв'язання задачі ідентифікації, як для лінійних, так і для нелінійних математичних моделей нестационарных аномальных диффузионных процесів.

Ключові слова: аномальний дифузійний процес, математична модель, варіація, варіаційна нерівність, оптимізація, принцип максимуму, функціонал, градієнт, екстремум, параметрична ідентифікація.

МЕТОДЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ И МАШИННОЙ ИДЕНТИФИКАЦИИ НЕСТАЦИОНАРНЫХ АНОМАЛЬНЫХ ДИФфуЗИОННЫХ ПРОЦЕССОВ

С.А. Положаенко, Омар Муаяд Абдуллах

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

Для класса нестационарных аномальных диффузионных процессов, математические модели которых формализуются в виде вариационных неравенств в частных производных, предложен метод математического моделирования, основанный на оптимизационной процедуре. При этом задача реализации математических моделей нестационарных аномальных диффузионных процессов сводится к отысканию максимума функции Гамильтона, определенной в пространстве состояний исследуемых процессов. Также предложен метод параметрической идентификации математических моделей нестационарных аномальных диффузионных процессов в случае индукционной постановки задачи исследования. Метод сводится к использованию оптимизационной процедуры метода проекции градиента. Обоснована возможность решения задачи параметрической идентификации, как для линейных, так и нелинейных математических моделей нестационарных аномальных диффузионных процессов.

Ключевые слова: аномальный диффузионный процесс, математическая модель, вариация, вариационное неравенство, оптимизация, принцип максимума функционал, градиент, параметрическая идентификация.

НАДІЙНІСТЬ СПЕЦІАЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНТЕГРОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ

В.А. Кудінов, О.М. Грищак

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

Наводиться методика розрахунку комплексної метрики надійності спеціального програмного забезпечення інтегрованих інформаційних систем органів внутрішніх справ України, яка дозволяє диференційовано визначити ступінь надійності певного типу спеціального програмного забезпечення за рахунок врахування відносної важливості одиничних показників.

Ключові слова: інформаційна система, оцінка надійності, спеціальне програмне забезпечення, рівень захищеності

Вступ

Серед основних напрямів державної інформаційної політики в Україні є створення інформаційних систем і мереж, розвиток електронного врядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України [1]. Не залишається осторонь цих завдань і Міністерство внутрішніх справ (МВС) України [2].

Від початку процесу інформатизації органів та підрозділів внутрішніх справ (ОВС) України минуло вже 44 роки. За цей час в них накопичений чималий досвід використання різноманітних інформаційних систем оперативно-розшукового та інформаційно-довідкового призначення [3, 4]. Так, зокрема, на виконання Указу Президента України від 20 жовтня 2005 року № 1497 [5] відповідним наказом МВС України була затверджена Програма створення Інтегрованої інформаційно-пошукової системи (ІПС) ОВС України [6]. Протягом останніх років Департамент інформаційно-аналітичного забезпечення (ДІАЗ) МВС України [7] створив та впровадив в діяльність ОВС України зазначену ІПС [8, 9]. Дана система – сукупність організаційно-розпорядчих, програмно-технічних та інформаційно-телекомунікаційних засобів, що забезпечують формування та ведення довідково-інформаційних, оперативно-розшукових обліків, авторизований доступ до інформаційних ресурсів ІПС [6, 8, 9].

Для ефективного функціонування цієї та інших ІПС ОВС України необхідно забезпечити належну захищеність їх апаратно-програмних та інформаційних ресурсів. Питанням створення методології оцінки рівнів захищеності різноманітних ІПС ОВС України присвячена низка робіт, зокрема [10-13]. Але на теперішній час ще залишається невирішеною актуальна та важлива проблема щодо оцінки надійності спеціального програмного забезпечення (СПЗ) ІПС ОВС України, яка суттєво впливає на загальну оцінку рівня захищеності даних систем. Вирішення зазначеної проблеми є метою даної статті.

Необхідність ретельного дослідження якості саме СПЗ ІПС ОВС України обумовлена тим, що програмне забезпечення несе більше функціональне навантаження при вирішенні завдань управління, ніж технічні засоби. Тому якість СПЗ в значній мірі визначає якість системи в цілому. Якість СПЗ є критично важливим фактором для

забезпечення адекватної та ефективної роботи відповідних ІПС. Сьогодні діяльність суб'єктів правоохоронної сфери прямо залежить від правильної обробки інформації відповідними ІПС. Низька якість програмного забезпечення, що використовується, може привести до серйозних і навіть фатальних негативних наслідків, глобальність яких залежить від специфіки використання СПЗ. Навіть якщо і вдається уникнути надзвичайних подій, використання неякісних програм завдає шкоди ефективності роботи ОВС. Процеси розробки і впровадження складних систем, до яких відноситься зокрема СПЗ ІПС ОВС, повинні знаходитись під твердим управлінським контролем. Станом на сьогодні практично в усіх підрозділах ДІАЗ МВС України, що займаються розробкою СПЗ ІПС, забезпечується контроль найважливіших характеристик, пов'язаних з виробництвом і використанням програмних продуктів, таких як час, фінансові засоби, ресурси та інше. Однак у більшості випадків поза межами сфери контролю знаходиться найбільш важлива характеристика програмних продуктів, заради якої, власне, і здійснюються витрати часу, фінансових засобів і ресурсів – це цільова якість програмного продукту (цільова – означає необхідну і достатню якість, що відбиває реальні потреби користувача). Відсутність можливості установки повного зазначеного контролю викликає зростання кількості необґрунтованих рішень, збільшує проектні ризики, які пов'язані з розробкою і впровадженням ІПС. Значної частини труднощів, що виникають при розробці та впровадженні цього СПЗ, можна уникнути, якщо з самого початку створювати ІПС у відповідності до певної методології. Дана методологія повинна враховувати безперервність процесів розробки та впровадження, статичність цілей розробника, динамічність вимог замовника, необхідність забезпечення високої надійності та точності функціонування, зручності експлуатації та гнучкості системи при зміні нормативних даних та інформаційних масивів.

Основна частина

Для забезпечення необхідного рівня якості програмних продуктів у міжнародній практиці знаходили застосування два підходи: орієнтований на продукт і орієнтований на процес. Обидва підходи вимагають наявності системи управління якістю.

При першому підході акцент робиться на контроль якості шляхом іспиту готового програмного продукту. Цей підхід базується на припущенні, що чим більше виявлено і усунуто помилок у програмному продукті при іспитах, тим вище його якість. Тестування розробленого програмного забезпечення, що проводиться у відриві від інших процесів, може попередити впровадження некондиційного продукту, але не гарантує раціональності використання ресурсів на попередніх етапах розробки СПЗ. Недолік такого підходу полягає в тому, що:

1. Усунення помилок у готовому продукті на етапі іспитів обходиться в десятки разів дорожче, ніж якби ці помилки були відвернені чи усунуті вчасно на ранніх етапах життєвого циклу програмного продукту;
2. Відсутні методи і засоби іспиту програмного продукту, які гарантують повне виявлення у програмних продуктах, що тестуються, помилок і недоліків.

При другому підході акцент робиться на вживання заходів по запобіганню, оперативному виявленню і усуненню помилок у програмному продукті шляхом завчасного визначення відповідальності, планів забезпечення, основних процедур по забезпеченню якості розроблювальних програмних продуктів і проведення відповідних заходів, починаючи із самих ранніх етапів життєвого циклу. Реально працююча “система забезпечення якості” повинна охоплювати всі процеси, що пов'язані зі створенням СПЗ: з моменту першого контакту із замовником і визначення його вимог, аж до вилучення СПЗ із експлуатації.

Цей підхід у даний час можна вважати загально прийнятим. Він покладений в основу Концепції якості програмних продуктів Міжнародних організацій по

стандартизації ISO/IEC і реалізується в численних міжнародних стандартах, проектах стандартів і робочих матеріалах цих організацій. Недоліком цих стандартів є складність оцінки рівня якості процесу розробки СПЗ у відповідності до запропонованої моделі якості, відсутність конкретизації складових процесу забезпечення якості, а також декларативність наведених основних положень. Всі вони пропонують лише узагальнені моделі якості і застосовувати їх в явному вигляді для кожного окремого випадку уявляється проблематичним.

Слід відмітити, що результати досліджень, які наведені в цих стандартах, доводять: чим вище якість процесу розробки, тим вище якість розробленого в цьому процесі СПЗ. Якість на кожній стадії проекту збільшується в основному за рахунок використання проміжного продукту більш високої якості, що був вироблений на попередній стадії життєвого циклу. На основі цього можна зробити наступні висновки:

1. Якість накопичується в програмному продукті кумулятивним чином, причому вклад в цю якість, що був здійснений на ранніх стадіях, більш впливовіший на кінцевий програмний продукт. Це також підтверджується всією практикою програмування – недоліки проектування інформаційних систем та визначення вимог до них не можуть бути компенсовані високою якістю процесу програмного кодування;

2. Тестування і оцінка якості СПЗ повинні відбуватися на всіх стадіях його життєвого циклу.

В рамках цієї статті розглянемо семантичну складову та оцінку надійності СПЗ, як однієї з характеристик якості СПЗ.

Поняття надійності програмного забезпечення, що розглядається у низці робіт [14-17], визначається як властивість об'єкту виконувати задані функції, зберігаючи у часі значення встановлених експлуатаційних показників у межах, які відповідають заданим режимам і умовам використання, технічного обслуговування, ремонтів, зберігання і транспортування. Це визначення сформульовано стосовно технічних засобів і тому без додаткових досліджень властивостей, що визначають надійність, некоректно трактувати його як поняття надійності спеціального програмного забезпечення. Різниця між уявленнями про надійність технічних засобів і СПЗ, в першу чергу, обумовлено різницею в матеріальному уособленні, яке у відповідності з [18] трактується як виріб. Відомо, що технічний об'єкт являє собою сукупність окремих взаємодіючих матеріальних компонент, кожна з яких має параметри, що характеризують його надійність. Отже, зміна надійності окремих компонент визначає зміну надійності об'єкту в цілому. Для технічних засобів вагомим є наявність достатньо визначеної фізичної інтерпретації, яка пояснює причини зменшення або збільшення надійності. В той же час це не є причиною неможливості використання деяких термінів і показників надійності техніки при дослідженні якості СПЗ [19].

В зв'язку з тим, що для спеціального програмного забезпечення причини зміни надійності можуть мати інтерпретацію, що принципово відрізняється відносно технічних засобів, існують достатньо різноманітні підходи як в інтерпретації параметрів, що визначають надійність програмного забезпечення, так і самого поняття при його застосуванні до СПЗ. Наприклад, в роботі [20] достатньо однозначно стверджується, що термін “надійне програмне забезпечення” сприяє помилковому розумінню природи програмного забезпечення. Тому пропонується замість уявлень про надійність використовувати уявлення про “правильне” чи “високоякісне” програмне забезпечення. Уявлення про надійність СПЗ в роботі [20] істотно відрізняється від визначень, що приводились раніше. Під надійністю розуміється показник якості СПЗ, що характеризує властивість програмного продукту проявляти в процесі експлуатації помилки, що залишились (не були виявлені), при певній сукупності вихідних даних.

В ISO/IEC DIS 2382-14:1994 дане таке визначення надійності: «спроможність функціональної одиниці виконувати необхідну функцію...». У цьому документі функціональність є тільки однією з характеристик якості програмного забезпечення.

Тому визначення надійності розширено до «підтримки рівня виконання» замість «...виконання необхідної функції».

Ці визначення переводить надійність із інтегрованої характеристики певного об'єкту в більш вузьку характеристику СПЗ – одиничний показник якості, і базується на висновку, що надійність є функцією помилок, що залишилися у програмному продукті після його вводу до експлуатації. Під час експлуатації помилки виявляються і виправляються. Якщо в процесі виправлення помилок не додається нових помилок або додається менше, ніж виправляється, то під час експлуатації СПЗ його надійність безперервно зростає. Існує ще інша залежність – чим інтенсивніше експлуатується СПЗ, тим інтенсивніше виявляються помилки та швидше зростає надійність.

Іншими авторами надійністю називається ймовірність роботи СПЗ без збоїв на протязі певного періоду часу [21]. Отже:

$$P_{WF} = F(N_F) \quad (1)$$

де P_{WF} – надійність СПЗ;

N_F – кількість помилок, що залишилися у програмному продукті після його вводу до експлуатації.

Оскільки СПЗ представляє собою програмний виріб, то причини існування помилок будуть обумовлюватись, з одного боку, засобами створення, які не можуть бути ідеальним інструментом за своєю надійністю, і, з іншого боку, – передумовами для розробки СПЗ на всіх етапах виготовлення програмного продукту, еквівалентних завданню, що визначає мету виконання роботи [22]. Як відмічено в цій праці, першою передумовою є формування завдання на розробку програмного продукту. Наступні етапи (розробка алгоритмів і текстів, налагодження, перевірка, іспити та дослідна експлуатація СПЗ) розглядаються з точки зору забезпечення максимального надійнісного критерію готового продукту у відповідності з прийнятим підходом. СПЗ відноситься до систем, що не відновлюються, так як в якості причин відмов розглядаються тільки помилки в програмі, що не можуть самоусуватися. Тому за основний критерій надійності приймається тривалість роботи до першої відмови.

Згідно з [23] надійність програмного забезпечення, як комплексний показник його якості, складається з наступних одиничних показників (підхарактеристик надійності): безвідмовність, стійкість до аномалій, відновлюваність, правильність (точність) та реактивність. Оцінка цих властивостей дозволяє скласти достатньо повне уявлення про ступінь надійності СПЗ. Але оскільки одиничні показники надійності СПЗ мають якісний характер, то для оцінки надійності СПЗ необхідно встановити кількісну характеристику його властивостей та розробити методики їх числового оцінювання. Дослідження метричного аналізу якості показують [24], що не існує єдиної метрики, яка б дала універсальний рейтинг якості програмного забезпечення і його надійності, зокрема. Тому специфіка спеціального програмного забезпечення вимагає розробки множини метрик, яка б відображала рівень надійності СПЗ певного типу та отримання інтегральної метрики надійності.

Безвідмовність міжнародними стандартами характеризується частотою відмов через помилки та недосконалість програмного забезпечення. Тому для її оцінки пропонується коефіцієнт безвідмовності K_{SF} , який характеризує напрацювання на відмову (кількість відмов за одиницю часу або середній час між відмовами):

$$K_{SF} = \frac{T}{N_F}, \quad (2)$$

де T – час випробування СПЗ;

N_F – кількість відмов.

Діапазон прийнятних значень цього показника визначається експертним шляхом для кожного типу СПЗ.

Визначення часу напрацювання на відмову $T(\tau)$ можливо також із застосуванням статистичного підходу. Згідно з алгоритмом, наведеним у [25], процес виявлення помилок у програмі може бути охарактеризований функцією $f(t)/R$, де $f(t)$ – кількість виявлених і виправлених помилок за одиницю часу у програмі, що складається з R команд:

$$\frac{f(t)}{R} = \frac{d\varepsilon_n}{dt} \approx \frac{\varepsilon_n(t + \Delta t) - \varepsilon_n(t)}{\Delta t}, \quad (3)$$

де $\varepsilon_n(t) = \frac{1}{R} \int_0^t f(t)dt$ – кількість виявлених і виправлених помилок за час t у розрахунку

на одну команду; τ – час налагодження програми.

Напрацювання на відмову, яка ініційована помилкою у програмі, визначається:

$$T(\tau) = \frac{R}{\varepsilon_0 \delta} e^{-\frac{\tau}{\tau_0}}, \quad (4)$$

де ε_0 та τ_0 – параметри $f(t)$, які визначаються при налагодженні програми; δ – середня кількість команд, що виконуються за одиницю часу (швидкодія машини).

Крім того, аналіз зміни $T(\tau)$ може бути підґрунтям для вибору часу τ налагодження програми, тобто, налагодження закінчується, якщо величина $T(\tau)$ становиться достатньою.

Одним з найважливіших загальних показників надійності є безпомилковість функціонування СПЗ, яку можна охарактеризувати показником безпомилковості K_{WF} . Цей показник може бути розрахований за допомогою коефіцієнта K_F , який відображає кількість помилок на 1000 команд (0.25; 0.5; ... ; 10) [26]:

$$K_{WF} = \frac{K_F N}{1000}, \quad (5)$$

де N – загальна кількість команд.

Питома вага кількості помилок на одну машинну команду, що залишилися у програмі після визначеного терміну налагодження, може бути розрахована за моделлю Шумана [27].

Стійкість до аномалій може бути оцінена за допомогою показника стійкості до аномальних діянь K_{ST} , для визначення якого у роботі [26] пропонується провести серію експериментів, що імітують виникнення таких подій, і зареєструвати відмови у роботі СПЗ:

$$K_{ST} = 1 - \frac{k}{K}, k \in K, K \rightarrow \infty, \quad (6)$$

де K – кількість експериментів, в яких імітувались аномальні діяння; k – кількість експериментів, в яких аномальні діяння викликали відмову.

Відновлюваність СПЗ пропонується оцінювати через середній час поновлення роботи після відмови:

$$\overline{\Delta T_r} = \frac{1}{I_r} \sum_{i=1}^{I_r} \Delta T_{r_i}, \quad (7)$$

де ΔT_{r_i} – час між втратою та поновленням працездатності; I_r – кількість випадків втрати та поновлення працездатності СПЗ, що були проаналізовані.

Адекватність і коректність оцінки правильності (точності) СПЗ можливо забезпечити за допомогою розрахунків середнього значення похибки розрахунку A_x :

$$A_x = \frac{1}{N} \sum_{i=1}^N (|X_{c_i} - X_{p_i}|) \quad (8)$$

та середнього квадратичного відхилення похибки розрахунку S_x :

$$S_x = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (|X_{c_i} - X_{p_i}| - A_x)^2}, \quad (9)$$

де N – кількість обчислень величини X ; X_{c_i} – істинне значення величини X ; X_{p_i} – розрахункове значення величини X .

Реактивність характеризується здатністю своєчасно перетворювати вхідні дані (запити) в необхідний результат. Тому по аналогії з оцінкою відновлюваності пропонується її оцінювати за допомогою розрахунків середнього значення абсолютної реактивності $\overline{\Delta T_{react}}$:

$$\overline{\Delta T_{react}} = \frac{1}{I} \sum_{i=1}^I (T_{e_i} - T_{n_i}), \quad (10)$$

де I – кількість реалізованих запитів на обробку даних; T_{e_i} – час видачі результатів перетворення i -го набору вхідних даних; T_{n_i} – час надходження i -го набору вхідних даних.

Крім того, специфіка СПЗ вимагає проведення його чіткого ранжирування по важливості, відповідно до моделі якості, як набору характеристик і зв'язків між ними, що забезпечує базис для висунення вимог до якості і оцінки якості для гарантування якісного виконання ним завдань за функціональним призначенням.

Для цього в нашому випадку застосуємо методику, що ґрунтується на використанні методу аналізу ієрархій Сааті [28]. Цей метод передбачає декомпозицію задачі (її ієрархічне зображення) на більш прості складові частини і подальшу обробку послідовності суджень експертів попарним порівнянням.

Маємо в наявності R -множину метрик спеціального програмного забезпечення, які характеризують його надійність. Під коефіцієнтом відносної важливості підхарактеристики надійності будемо розуміти пріоритет (перевагу), який вимірюється відносно однієї підхарактеристики над іншою. Коефіцієнти важливості w_n визначаються для кожної підхарактеристики надійності СПЗ, відповідно, таким чином, що: $\sum_{j=1}^n w_j = 1$.

Отже, маємо $R_1, R_2, R_3, \dots, R_5$ – множина з 5 підхарактеристик надійності СПЗ (безвідмовність, стійкість до аномалій, відновлюваність, правильність, реактивність) і $w_{1i}, w_{2i}, w_{3i}, \dots, w_{5i}$ – їх, відповідно, коефіцієнти важливості відносно i -го типу СПЗ.

Тоді надійність спеціального програмного забезпечення i -го типу $R_{СПЗ}^{(i)}$ можна представити у вигляді адитивної згортки:

$$R_{СПЗ}^{(i)} = \sum_{j=1}^5 w_{ji} \hat{R}_j, \quad (11)$$

де $\hat{R}_j$ – j -та підхарактеристика надійності СПЗ, що оцінена кількісно та пронормована;
 w_{ji} – коефіцієнт відносної важливості $\hat{R}_j$ для його i -го типу.

Оскільки множина коефіцієнтів важливості $w_1, w_2, w_3, \dots, w_n$ невідома заздалегідь, то попарні порівняння підхарактеристик надійності СПЗ здійснюються з використанням суб'єктивних оцінок експертів, що чисельно оцінюються за шкалою відносної важливості.

Висновки

1. Використовуючи термін «надійність програмного забезпечення» аналогічно терміну «надійність апаратури», слід пам'ятати, що відмови програмного забезпечення як результат прояву помилок, мають зовсім іншу фізичну природу, ніж відмови техніки. Однак це не є причиною неможливості використання деяких термінів і показників надійності техніки при дослідженні якості СПЗ, наприклад, час напрацювання на відмову.
2. Надійність є комплексним одиничним показником якості СПЗ, який потребує розробки множини метрик для своєї оцінки.
3. Наведені формульні залежності дозволяють обґрунтувати та формалізувати метрики надійності СПЗ ІПС ОВС України і за рахунок цього автоматизувати процес оцінки його надійності.
4. Наведена методика дозволяє отримати інтегральну метрику надійності СПЗ ІПС ОВС України та диференційовано визначити ступінь надійності певного типу СПЗ за рахунок врахування відносної важливості одиничних показників.

Список використаних джерел

1. Про внесення змін до Закону України «Про інформацію»: Закон України від 13 січня 2011 року // Відомості Верховної Ради України. – 2011. – № 32. – ст. 313.
2. Про затвердження Положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 13 серпня 2014 року № 401: [Електронний ресурс]. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/401-2014-%D0%BF>
3. Швець, М. Системна інформатизація правоохоронної діяльності / [М. Швець, С. Антоненко, В. Буржинський та ін.]; за ред. В. Дурдинця, В. Євдокимова, М. Швеця. – К.: НДЦПІ АПРН України, 2006. – 287 с.
4. Черних, С.П. Від арифмометра до високих технологій / С.П. Черних, О.М. Іщенко, І.А. Аршинов. – К.: Преса України, 2012. – 1112 с.
5. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20 жовтня 2005 року № 1497: [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1497/2005>
6. Про затвердження Програми створення Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України: Наказ МВС України від 07 червня 2006 року № 571: [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/z1256-09>
7. Про затвердження Положення про Департамент інформаційно-аналітичного забезпечення МВС України: Наказ МВС України від 29 квітня 2011 року № 174: [Електронний ресурс]. – Режим доступу: https://search.ligazakon.ua/l_doc2.nsf/link1/MVS408.html

8. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: Наказ МВС України від 12 жовтня 2009 року № 436: [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/z1256-09>
9. Про затвердження Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України: Наказ МВС України від 10 березня 2010 року № 75: [Електронний ресурс]. – Режим доступу: https://search.ligazakon.ua/l_doc2.nsf/link1/MVS234.html
10. Кудінов, В. А. Методологія оцінки рівнів захищеності Інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України / В. А. Кудінов, О. Г. Корченко // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: Збірник наук. статей за матеріалами доповідей наук.-практ. конференції, Львів, 14 груд. 2012 р. – Львів: Львівський держ. ун-т внутр. справ, 2012. – С. 7–10.
11. Кудінов, В. А. Оцінка коефіцієнта оперативної готовності організаційних заходів до захисту типового вузла Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України з обробки інформації / В. А. Кудінов // Сучасна спеціальна техніка. – 2013. – № 2. – С. 58–63.
12. Кудінов, В. А. Напрями подальшого розвитку методології оцінки рівнів захищеності Інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України у зв'язку з набуттям чинності нового КПК України / В. А. Кудінов // Сучасна спеціальна техніка. – 2013. – № 1. – С. 126–130.
13. Кудінов, В.А. Проблеми застосування методики експертної оцінки рівнів захищеності Інтегрованої інформаційної системи оперативного інформування МВС України для різноманітних інтегрованих інформаційних систем органів внутрішніх справ України / В. А. Кудінов // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі: Збірник наук. статей за матеріалами доповідей наук.-практ. конференції, Львів, 26 груд. 2014 р. – Львів: Львівський держ. ун-т внутр. справ, 2014. – С. 13-16.
14. Абрамов, С.А. Элементы анализа программ / С.А. Абрамов – М.: Наука, 1986. – 127 с.
15. Головкин, Б.А. Классификация методов обеспечения надежности программ / Б.А. Головкин // Упр. системы и машины. – 1979. – № 5. – С. 3-12.
16. Карповский, Е.Я. Надежность алгоритмов управления / Е.Я. Карповский, В.В. Сагач, А.А. Чернецкий. – К.: Техника, 1983. – 113 с.
17. Майерс, Г. Надежность программного обеспечения / Г. Майерс. – М.: Мир, 1980. – 360 с.
18. Шураков, В.В. Надежность программного обеспечения систем обработки данных / В.В. Шураков. – М.: Финансы и статистика, 1987. – 272 с.
19. Карповский, Е.Я. Надежность программной продукции / Е.Я. Карповский, С.А. Чижов. – К.: Техника, 1990. – 160 с.
20. Кулаков, А.Ф. Оценка качества программ / А.Ф. Кулаков. – К.: Техника, 1984. – 167 с.
21. Musa, J. Software Reliability: Measurement, Prediction, Application / J. Musa, A. Iannino, K. Okumoto. – New York: McGraw-Hill, 1987.
22. Гуляев, В.А. Анализ и исследование методов оценки и увеличения надежности программ / В.А. Гуляев, Ю.М. Коростиль. – К.: 1990. – 44 с.
23. Боэм, Б. Характеристики качества программного обеспечения / [Боэм Б., Браун Дж., Каспар Х. и др.]; пер. с англ. Е.К. Масловского. – М.: Мир, 1981. – 206 с.
24. Воробьева, Н.И. Надежность компьютерных систем / Н.И. Воробьева, В.И. Корнійчук, Е.В. Савчук. – К.: ЧП “Корнійчук”, 2000. – С. 97-98.
25. Молодцова, О.П. Управління якістю програмної продукції: [навч. посіб.] / О.П. Молодцова. – К.: КНЕУ, 2001. – 248 с.
26. Кулаков, А.Ф. Управление качеством программных средств ЭВМ / А.Ф. Кулаков. – К.: Техника, 1989. – 216 с.
27. Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь, 1993. – 320 с.

НАДЕЖНОСТЬ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНТЕГРИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОВД УКРАИНЫ

В.А. Кудинов, О.М. Гришак

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

Приводится методика расчета комплексной метрики надежности специального программного обеспечения интегрированных информационных систем органов внутренних дел Украины, которая позволяет дифференцированно определить степень надежности определенного типа специального программного обеспечения за счет учета относительной важности единичных показателей.

Ключевые слова: информационная система, оценка надежности, специальное программное обеспечение, уровень защищенности

RELIABILITY SPECIAL SOFTWARE INTEGRATED INFORMATION SYSTEMS THE DEPARTMENT OF INTERNAL AFFAIRS OF UKRAINE

V.A. Kudinov, O.M. Gryschak

National Academy of Internal Affairs
1 Solomjanska Squar, 03035, Kyiv, Ukraine; e-mail: kva-navsu@mail.ru

The technique of calculating the reliability of the complex metrics of special software integrated information systems of bodies of internal affairs of Ukraine, which allows to define a differentiated level of reliability of a certain type of special software by accounting for relative importance of individual indicators is presented.

Keywords: information system, reliability evaluation, special software, the level of protection

КЛАССИФИКАЦИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ДЛЯ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

А.Н. Орехов, В.А. Хорошко

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

В работе рассматривается системная классификация моделей информационного пространства систем управления воздушным движением по совокупности трех критериев, которые позволяют проводить моделирование их функционирования. Для выбора методов моделирования оценивается уровень возможности зависимостей между элементами системы.

Ключевые слова: математическая модель, система защиты информации, информационное пространство, система управления воздушным движением.

Введение

Системы управления воздушным движением (СУВД) относятся к категории систем с ограниченным доступом. Это связано с особенностями воздушного транспорта и задачами, которые определяются назначением СУВД. В настоящее время существуют ряд способов воздействия на информационное пространство (ИП) СУВД с целью противодействия их нормальному функционированию. Это приводит к необходимости ограничения доступа к ИП СУВД, а также обеспечения защиты ИП. Успешное решение этой задачи обеспечивает безопасность, регулярность и экономичность полётов, повышение надежности и доступности информационного обеспечения.

Для предотвращения возможности реализации угроз ИП СУВД необходима разработка и использование комплексной системы технической защиты информации (КСТЗИ). Требования к такой системе предусматривают централизованное управление средствами и механизмами защиты на основе политики информационной безопасности и реализующего ее плана технической защиты информации.

Использование методов моделирования в области обеспечения безопасности ИП СУВД привело к разработке большого количества формальных моделей безопасности [1]. Формальные модели используются достаточно широко, потому что только с их помощью можно доказать безопасность системы или объекта, опираясь при этом на объективные и неопровержимые постулаты математической теории. Основная цель создания политики безопасности информационного пространства и описание ее в виде формальной модели - это определение условий, которым должно подчиняться поведение ИП СУВД, выработка критерия безопасности и проведение формального доказательства соответствия его этому критерию.

Целью статьи является разработка системной идентификации моделей ИП СУВД по совокупности критериев для улучшения ее функционирования.

Основная часть

Системная классификация моделей может быть осуществлена по совокупности трех критериев следующего содержания:

1. Способ моделирования, то есть основной прием, который положен в основу построения модели;
2. Характер системы – показатель, который выявляет взаимосвязи между надлежащими определению на модели значениями характеристик системы, которая моделируется, параметрами системы и внешней средой;
3. Масштаб моделирования – показатель, который отображает уровень характеристик, которые определяются на модели.

Согласно первого критерия все модели могут быть разделены на аналитические, подаваемые в виде некоторой совокупности аналитических зависимостей, и статистические, когда моделируемая система представляется в виде некоторого аналога, отображающего для определенных характеристик зависимости реальной системы. Само определение значений этих характеристик осуществляется методом многоразовой имитации реализации зависимостей характеристик от знаковых параметров реальной системы, внешней среды и статистической обработкой полученных при этом результатов.

Сформулированных зависимостей получается очень много, но для выбора методов моделирования наибольшее значение имеет уровень возможностей указанных зависимостей. По этому признаку моделируемые системы разделяются на детерминированные и стохастические.

В соответствии с третьим критерием, модели можно разделить на общие и частные. Общие модели строятся с целью определения значений некоторых обобщенных характеристик моделируемых систем. Частные – с целью определения значений частичных, локальных характеристик [2].

Таким образом, задача заключается в построении модели КСТЗИ ИП СУВД, а также имитации на ней процессов функционирования реальной КСТЗИ ИП СУВД. Методы моделирования являются способами исследования системы с целью построения ее модели. В связи с этим классификация методов моделирования соответствует системной классификации моделей. Исходя из целей моделирования, методы можно разделить на две группы: методы построения моделей или методы описания структуры и процессов функционирования моделируемых систем; методы имитации процессов функционирования систем.

При аналитическом моделировании структура моделируемого ИП СУВД и процессы его функционирования подаются в виде некоторых выражений, которые отображают зависимость определяемых характеристик системы от ее параметров и параметров внешней среды. Имитация процессов функционирования систем является вырожденной, она сводится к расчету по выражениям [1] значений определяемых характеристик для заданных значений параметров системы и внешней среды. Другими словами, в анализируемых моделях структура моделируемых систем и процессы их функционирования подаются в неявном виде.

При статическом моделировании структуры СТЗИ, СУВД и ИП адекватно отображаются в модели. При этом степень адекватности модели реальной системе в процессе имитации определяются целями моделирования, т.е. характеристиками систем, которые могут быть получены в процессе моделирования. Значения характеристик, которые определяются в процессе моделирования, должны соответствовать значениям тех характеристик, которые будут или могут иметь место в процессе функционирования реальных систем.

Построение статистической модели содержится в описании структуры и процессов функционирования ИП СУВД, а имитация процессов функционирования в

проработке тем или иным способом изменений во времени состояний модели системы и принятии на каждом шаге имитации решений, которые обусловлены созданной ситуацией и правилами функционирования реальной системы.

Описание моделируемой системы должно содержать: перечень всех ее значимых элементов; взаимные связи между элементами; характер этих взаимосвязей.

Для описания процессов функционирования стохастических систем необходимы способы отображения случайных факторов. Такие способы содержатся в следующих: метод статистических испытаний или Монте-Карло, теории массового обслуживания, теории вероятных автоматов, неформальной теории систем, нестрогой математики.

В соответствии с классификацией примеры моделей СТЗИ ИП СУВД как детерминированной системы приведены в [1-4], как стохастической системы - в [2,3,5].

Необходимо отметить, что среди моделей систем и процессов защиты информации не встречаются те, которые относятся к статистическим общим для стохастических систем. Это объясняется трудностями, связанными с отсутствием представлений о распределении вероятностей большого числа случайных событий.

Информационная система нуждается в анализе и использовании данных успешно реализованных угроз, накопленных в прошлом. Для реализации простейшего метода, в основе которого лежит библиотека шаблонов атак, необходимо осуществлять аудит работы ИП СУВД и подробно документировать ход атаки. Результатом хода документирования и анализа реализации угрозы является шаблон и дерево атаки. Затем из деревьев выделяются все возможные сценарии реализации угрозы. По мере накопления опыта формируется библиотека шаблонов реализации угроз. Практичность использования дерева атак на ИП СУВД состоит в повторном использовании предварительно разработанных моделей реализации угрозы.

Дерево атаки состоит из узлов [1], которые представляют собой цели или подцели атаки. При этом узел атаки может состоять из:

- набора подцелей атаки, каждая из которых должна быть достигнута для успешного осуществления атаки (И–декомпозиции) (рис.1(а)). Цель G_0 будет достигнута лишь в том случае, если будет достигнута каждая из подцелей $G_1, G_2, \dots, G_n$;
- набора целей атаки, хотя бы одна из которых должна быть достигнута для успешного осуществления атаки (ИЛИ–декомпозиции) (рис.1(б)). Цель G_0 будет достигнута в случае, если будет достигнута хотя бы одна из подцелей $G_1, G_2, \dots, G_n$.

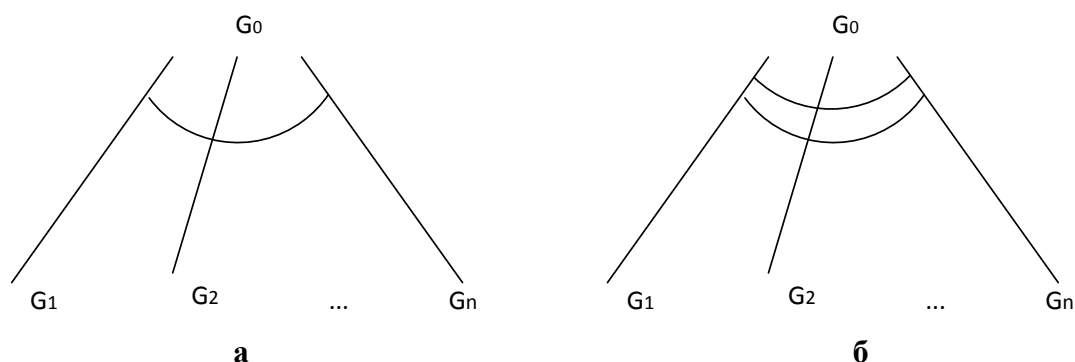


Рис. 1. Структурное представление декомпозиции: а – И–декомпозиции; б – ИЛИ–декомпозиции.

Дерево атаки может состоять из любого набора И– и ИЛИ–декомпозиций. Моделирование атак с помощью деревьев атак позволяет детализировать сценарий до уровня, выбранного разработчиком. Недостатком данного подхода является низкий уровень «эвристики», привязанность к известным типам атак, возможность обнаружения действий нарушителя только по известным сценариям.

Возможно улучшение способа моделирования угроз деревом атак. Для этого необходимо объединить ручное расширение дерева атак и применение библиотек атак [1]. На рис.2. приведена блок-схема процесса использования этого способа.

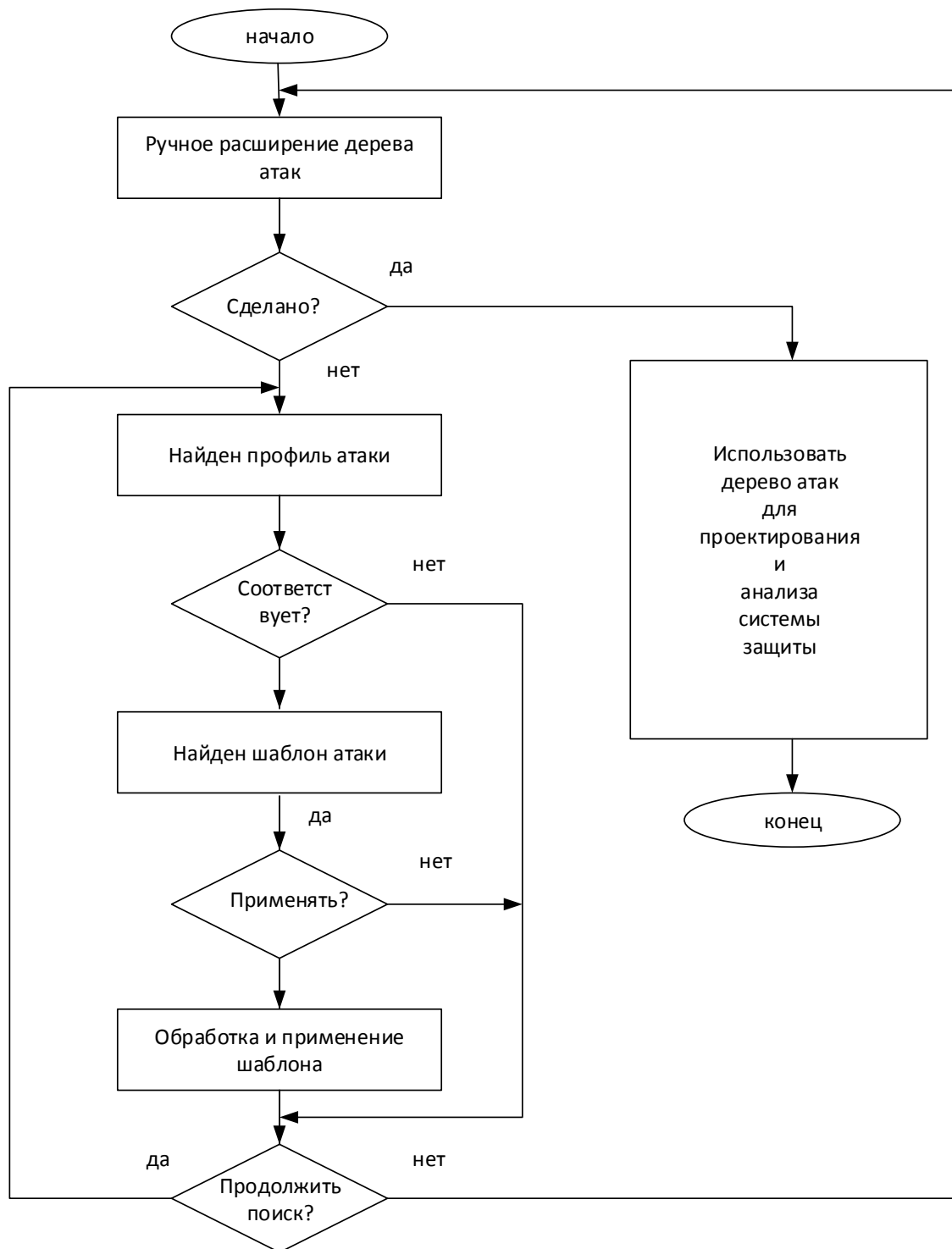


Рис. 2. Блок-схема процесса расширения библиотеки шаблонов атак

Введем понятия шаблона и профиля атаки. Определим шаблон атаки как родственное представление преднамеренной, злонамеренной атаки. Каждый шаблон атаки содержит: общую цель атаки, определяемую шаблоном; список предварительных условий для его использования; шаги для выполнения атаки; список постсостояний системы на случай успешного выполнения атаки. Предварительные условия включают в себя предположения о состояниях системы, при которых возможно реализовать

угрозы. Профили атак содержат: модель общих связей, взаимоотношений; список вариантов; глоссарий определенных терминов и фраз.

Модель связей представляет собой шаблон архитектуры с параметрами, которые могут включать специфичные варианты. Шаблоны атак также определены в терминах вариантов. Как показано на блок-схеме (рис.2) моделирование с помощью метода дерева атак может быть улучшено компромиссным решением – объединением ручного расширения библиотеки атак и использованием приложений для работы с шаблонами. Ручное расширение дерева атак в основном зависит от личного опыта разработчика атак. Использование приложений для работы с шаблонами также зависит от разработчика, но в меньшей степени.

Выводы

Предложена системная классификация моделей ИП СУВД по совокупности трех критериев, которые позволяют проводить моделирование. Для выбора методов моделирования наибольшее значение имеет уровень зависимостей между элементами системы.

Список литературы

1. Богданов, А.М. Моделирование безопасной обработки информации в компьютерных системах / А.М. Богданов, А.В. Корнейко. – К: Наукова думка, 2000. – 160 с.
2. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных. В 2-х томах / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 293 с.
3. Девянин, П.Н. Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Михальский и др. – М.: Радио и связь, 2000. – 192 с.
4. Грушко, А.А. Теоретические основы защиты информации / А.А. Грушко, Е.Е. Тимонина. – М.: Изд-во «Яхтсмен», 1996. – 187 с.
5. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М: Горячая линия - Телеком, 2000. – 452 с.

КЛАСИФІКАЦІЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЛЯ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

А.Н. Орехов, В.О. Хорошко

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

У роботі розглядається системна класифікація моделей інформаційного простору систем управління повітряним рухом за сукупністю трьох критеріїв, які дозволяють проводити моделювання її функціонування, але для вибору методів моделювання необхідно оцінити рівень можливості залежностей між елементами системи.

Ключові слова: математична модель, система захисту інформації, інформаційний простір, система управління повітряним рухом.

CLASSIFICATION OF MATHEMATICAL MODELS OF SYSTEMS OF PROTECTION OF INFORMATION SPACE FOR AIR TRAFFIC CONTROL

A.N. Orekhov, V.A. Khoroshko

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

The paper deals with the classification system model information space systems, air traffic control for a set of three criteria that allow the simulation of its operation, but the choice of modeling methods necessary to assess the level of possible relationships between the elements of the system.

Keywords: mathematical model, the system of information protection, information space, air traffic control system.

УДОСКОНАЛЕННЯ МЕТОДИКИ ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ НА АБОНЕНТСЬКИХ ТЕЛЕФОННИХ ЛІНІЯХ З УРАХУВАННЯМ МОЖЛИВОСТЕЙ СУЧАСНИХ ЗАСОБІВ КОНТРОЛЮ

В.В. Хома, В.М. Іванюк

Національний університет "Львівська політехніка",
вул. С. Бандери, 12, Львів, 79013, Україна; e-mail: Volodymyr.V.Khoma@lpnu.ua

Стаття присвячена питанню структуризації методики проведення робіт з виявлення пристроїв несанкціонованого отримання інформації в абонентських телефонних лініях. Проаналізовано структуру та функціонування сучасних телефонних закладних пристроїв та виділено їх основні демаскувальні ознаки. Проведено також порівняльну характеристику відомих методів, які застосовуються для виявлення несанкціонованих підключень до телефонних ліній, показано шляхи покращення характеристик засобів контролю. У цьому контексті запропоновано використання лінійного адаптера, що реалізує фазовий метод виявлення телефонних закладних пристроїв і володіє підвищеною завадостійкістю. Розроблено та подано у вигляді блок-схеми методику проведення робіт з виявлення несанкціонованих підключень до телефонних ліній, яка враховує можливості сучасних засобів контролю та дає змогу оптимізувати часові витрати.

Ключові слова: абонентська телефонна лінія, телефонний закладний пристрій, демаскувальні ознаки, методи виявлення несанкціонованих підключень, методика проведення пошукових робіт, лінійний адаптер.

Вступ

Телефонний зв'язок, будучи найпоширенішою телекомунікаційною технологією, є вкрай вразливим до несанкціонованого отримання інформації. Зацікавленість зловмисників до абонентської телефонної лінії (АТЛ) зумовлюють такі фактори, як: розгалужена топологія мережі телефонного зв'язку, передача інформації у відкритому вигляді на ділянці від абонентського терміналу до АТС, значна протяжність абонентських ліній, можливість отримання інформації у реальному часі [1,2]. Також слід зазначити придатність АТЛ для віддаленого прослуховування приміщень. За використання спеціальних технічних засобів можна здійснити передачу перехоплених повідомлень по радіоканалу або їх запис на запам'ятовуючі носії. Такі технічні засоби називаються телефонними закладними пристроями (ТЗП), що разом із АТЛ утворюють технічний канал витоку інформації [1,3].

Найуразливішими з точки зору сторонніх підключень є дві ділянки абонентської лінії — від розподільчої шафи до розподільчої коробки та від розподільчої коробки до абонентської розетки, оскільки на цих ділянках повідомлення кожного абонента передаються по визначених та незмінних в часі парах провідників, а сигнали не піддаються ущільненню [1,2]. Таким чином, для забезпечення захищеності телефонного зв'язку важливо своєчасно виявляти підключені до АТЛ закладні пристрої. Постійне удосконалення ТЗП не лише ставить підвищені вимоги до технічних характеристик

засобів контролю сигналів і параметрів АТЛ, але також вимагає перегляду і уточнення методики проведення пошукових робіт.

Метою даної роботи є систематизація відомостей про будову та функціонування сучасних телефонних закладних пристроїв і аналіз їх демаскувальних ознак, порівняльна характеристика методів виявлення телефонних закладок та розроблення методики виявлення несанкціонованих підключень із урахуванням можливостей сучасних засобів контролю сигналів і параметрів АТЛ.

Аналіз демаскувальних ознак телефонних закладних пристроїв

Залежно від природи можна виділити три категорії демаскувальних ознак телефонних закладних пристроїв:

- наявність нештатних предметів упродовж телефонного тракту;
- поява сторонніх сигналів в зоні АТЛ;
- зміна електрофізичних параметрів телефонної лінії.

Сучасні ТЗП використовують найновіші досягнення електроніки і комп'ютерних технологій, тому їх характеристики постійно вдосконалюються, що знижує рівень демаскувальних ознак і ускладнює завдання виявлення несанкціонованих підключень.

Перш ніж проаналізувати демаскувальні ознаки, доцільно коротко описати будову і функціонування ТЗП. Попри велику різноманітність програмно-апаратних і конструктивних рішень у структурі телефонних закладок можна виділити п'ять основних функціональних блоків (рис. 1).

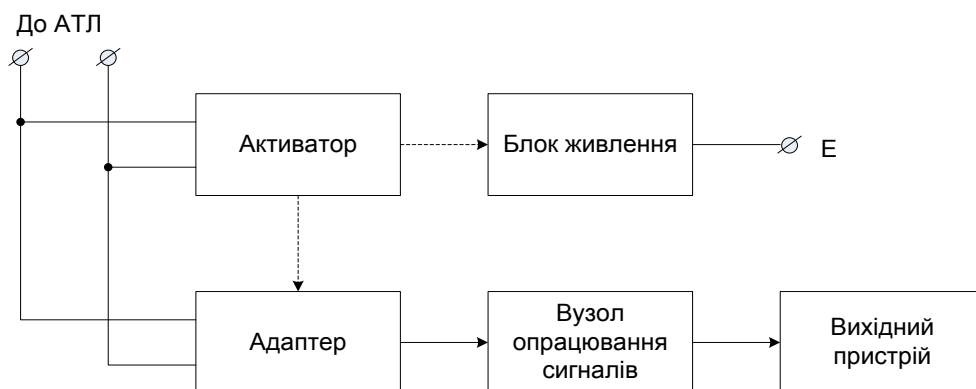


Рис. 1. Узагальнена структура ТЗП

Основою ТЗП є телефонний адаптер, що забезпечує знімання сигналу із АТЛ. Саме адаптер визначає тип підключення: контактне паралельне, контактне послідовне чи безконтактне. Наступним важливим структурним елементом ТЗП є вузол опрацювання сигналу, до функцій якого належить виділення інформативного сигналу та тлі різного роду перешкоджаючих факторів та його підсилення до рівня придатного для подальшого використання.

У телефонних закладках можливі такі способи використання перехоплених сигналів: прослуховування розмови в реальному часі; запис розмовного сигналу; ретрансляція сигналу за межі контрольованої зони. Реалізація вихідного пристрою безпосередньо залежить від способу використання перехоплених сигналів. Для пересилання перехоплених сигналів після відповідного кодування та модуляції може використовуватися і сама АТЛ.

Живлення телефонних закладок може здійснюватися двоюко – безпосередньо від АТЛ або від автономного джерела. У першому варіанті блок живлення реалізується у вигляді спеціального узгоджувального пристрою і забезпечує практично необмежений

термін дії, хоч може бути виявлений за ознакою додаткового навантаження АТЛ. Другий варіант володіє протилежними властивостями.

Для заощадження ресурсу автономних джерел живлення та підвищення рівня маскуванню до складу ТЗП включають спеціальні пристрої-активатори. Їх робота може ґрунтуватися на аналізі стану телефонної лінії (активація телефонної закладки відбувається після піднесення трубки і замикання шлейфу) або на детектуванні розмовного сигналу в АТЛ (так званий акустозапуск).

Демаскувальні ознаки, що віднесені до першої категорії, напряму залежать від габаритних розмірів ТЗП, причому істотний вплив на габарити і вагу закладок має наявність автономного живлення (додається розмір батарейки). Можна стверджувати, що телефонні закладки, виконані у вигляді окремого модуля, візуально легше виявити, ніж закамуфльовані під елементи телефонного апарату, наприклад, конденсатор, телефонний або мікрофонний капсулі, телефонний штекер, розетку тощо.

Демаскувальні ознаки другої категорії насамперед пов'язані із вихідним пристроєм, що виконує ретрансляцію перехоплених повідомлень. Виявити сторонні сигнали у ТЗП, що використовує для передавання технологію розширеного спектра (Spread Spectrum) чи запис перехоплених повідомлень на носій, вкрай складно. Використання активатора також знижує рівень демаскувальних ознак цього типу.

Тип та технічні характеристики адаптера ТЗП визначають рівень демаскувальних ознак третьої категорії. Безконтактні ТЗП неможливо виявити шляхом вимірювання електрофізичних параметрів телефонної лінії, але якість відтворення чи запису не дуже висока через чутливість індуктивного знімача до різних електромагнітних перешкод. Контактні адаптери мають гальванічний контакт із телефонною лінією і тому здатні забезпечити значно вищу якість. Паралельний адаптер підключається до лінії паралельно і відрізняється високим вхідним опором і малою вхідною ємністю, що утрудняє його виявлення. Послідовний адаптер включається в розрив одного із проводів телефонної лінії, має вхідний опір кілька сотень Ом і значну вхідну ємність, що полегшує його виявлення [3].

Основними параметрами телефонних закладних пристроїв є значення вхідної ємності і активного опору. Вхідна ємність забезпечує фільтрацію інформаційного сигналу і захист від постійної складової напруги наявної в лінії. Виникнення додаткового активного опору зумовлене наявністю підсилювача сигналу у вхідній ланці пристрою несанкціонованого отримання інформації з телефонної лінії. Для ТЗП з паралельним підключенням діапазон значень вхідної ємності знаходиться в межах від 20 до 1000 пФ і більше, а вхідний опір може становити від сотень кОм до десятків МОм. Для закладок з послідовним включенням основним параметром є вхідний опір, який може становити від декількох сотень Ом до кОм [3].

Телефонні закладні пристрої з вбудованими джерелами живлення, що гальванічно під'єднані до лінії, мають великий вхідний опір до декількох МОм і низьке значення вхідної ємності. Отже до основних демаскуючих ознак ТЗП відносяться: наявність сторонніх предметів поблизу АТЛ, порушення пломби телефонного апарату, розетки, розподільчого щитка; наявність в АТЛ високочастотного сигналу, промодульованого інформаційним сигналом (зазвичай несуча частота становить від 40 до 600 кГц); наявність радіосигналу промодульованого інформаційним сигналом; наявність струму витоку (від одиниць до декількох десятків мА); відмінність напруги в лінії в порівнянні з іншими лініями підключених до однієї розподільчої коробки; відмінність ємності, індуктивності та активного опору лінії від паспортних значень більше граничнодопустимої величини; відмінність значень повного опору від паспортних значень, при проведенні досліджень в режимах холостого ходу, короткого замикання та узгодженого навантаження.

Порівняльна характеристика методів виявлення телефонних закладних пристроїв

На цей час розроблено чимало методів, які застосовуються для пошуку ТЗП, проте жоден з них не є самодостатнім і ефективним щодо виявлення різних типів несанкціонованих підключень до АТЛ [4,5]. Залежно від стану АТЛ, потреби у підготовчих роботах, скритності виконання пошуку ТЗП методи контролю можна віднести до однієї із п'яти груп: візуальне обстеження АТЛ; контроль сигналів у самій АТЛ та радіо сигналів у зоні навколо неї; пасивний контроль параметрів АТЛ у робочому стані; активний контроль параметрів знеструмленої АТЛ; локалізація місця встановлення ТЗП.

Візуальне обстеження АТЛ є простим, не займає багато часу та не вимагає технічних засобів. Це єдиний метод, який може бути результативним щодо виявлення безконтактних ТЗП із автономним живленням та ретрансляцією сигналу у форматі розширеного спектра. На жаль, цей метод не є ефективним за застосування камуфляжу закладок під штатні технічні засоби, предмети інтер'єру, інших способів приховування.

Методи, які націлені на контроль сигналів, є порівняно простими у реалізації, не вимагають маніпуляцій над АТЛ, хоча для виявлення ТЗП оснащених активатором, додатково потребують підняття слухавки телефонного апарата, запровадження низькочастотного сигналу до лінії чи застосування механізму акустозапуску. Методи контролю сигналів є ефективними щодо радіозакладок та ТЗП, що застосовують ретрансляцію сигналів телефонною лінією, однак телефонні закладки, які використовують запис сигналу не будуть виявлені.

Третя, четверта групи методів пов'язані із контролем за змінами відносно «чистого» стану електрофізичних параметрів АТЛ, насамперед напруги і струму шлейфу, асиметрії опору пар проводів, а також параметрів імпедансу телефонної лінії.

Пасивний контроль параметрів АТЛ не потребує зондувальних сигналів, тому пошукові роботи можуть бути скритими від зовнішнього моніторингу. Реалізація цього методу не вимагає підготовчих робіт, тому АТЛ перебуває у робочому стані. Контролюється напруга і струм в лінії за покладеної та піднятої слухавки. За використання пасивного контролю достовірність результатів не висока, через недостатню стабільність напруги і струму АТЛ.

Арсенал методів виявлення знеструмлених АТЛ значно ширший, а, основне, засоби, які реалізують ці методи, забезпечують потенційно вищу достовірність. Знеструмлення АТЛ, тобто відключення від телефонних станцій, найбільш доцільно здійснювати у розподільчій шафі, оскільки, з одного боку, підключення на абонентській та розподільчій ділянках є найбільш імовірним, а з іншого – протяжна міська ділянка АТЛ зазвичай вносить додаткові завади. Зрозуміло, що дані методи контролю застосовуються лише при виконанні пошукових робіт, а їх спільною особливістю є потреба у використанні зовнішніх джерел зондувальних сигналів у вигляді напруги постійного струму, гармонічних коливань, імпульсних сигналів. Тому такі методи належать до активних, а факт виконання пошукових робіт можна встановити шляхом моніторингу сигналів у самій АТЛ та радіосигналів поблизу неї.

Методи виявлення несанкціонованих підключень на знеструмлених АТЛ базуються на відхиленні параметрів лінії із підключеною телефонною закладкою відносно відповідних параметрів «чистої лінії». Класична модель кабельної лінії зв'язку представляється параметрами – погонними ємністю, індуктивністю, опором та провідністю. З огляду на те, що протяжність АТЛ не перевищує довжини хвилі тонального сигналу, застосовується модель лінії із зосередженими параметрами. Ця модель додатково спрощується для випадків холостого ходу (паралельне сполучення ємності між дротами лінії та провідності ізоляції) і короткого замикання дротів на віддаленому кінці лінії (послідовне з'єднання активного опору та індуктивності).

Характер і ступінь впливу закладки на знеструмлену телефонну лінію значною

мірою залежить від способу підключення [5, 6]. Часто застосовуються такі еквівалентні схеми телефонної лінії: резистивна ланка, що відображає безпосереднє підключення кола живлення телефонної закладки, ємнісно-резистивна ланка для паралельного відбору/передачі інформації та схема живлення закладки через діодний мостик [1,7].

Задля забезпечення прихованості несанкціонованих підключень вхідний імпеданс паралельної телефонної закладки повинен бути якнайбільшим. У цьому сенсі найпридатнішим є спосіб підключення ТЗП через роздільний конденсатор, за якого вплив на АТЛ є мінімальним і проявляється через незначне збільшення ємності лінії.

Залежно від того, які параметри вимірюються, розрізняють такі методи контролю [1,7]: опору шлейфа; асиметрії проводів; первинних параметрів імпедансу (R , C , L); вольт-амперної характеристики; фігур Ліссажу; перехідної чи імпульсної характеристик; амплітудно-частотної та фазочастотної характеристик; нелінійності лінії (нелінійна локація); неоднорідність лінії (імпульсна рефлектометрія).

Пристрої, що реалізують перераховані методи, характеризуються різним ступенем складності, рівнем достовірності результатів контролю. Деякі з них, наприклад, вольт-амперної характеристики, фігур Ліссажу чи перехідної характеристики через обмежену чутливість є сенс застосовувати лише для виявлення ТЗП зі значною нелінійністю.

Покращання параметрів ТЗП та зменшення їх впливу на параметри телефонної лінії значно ускладнює задачу їх виявлення. Засоби контролю, побудовані на основі відомих методів, через обмежену чутливість не виявляють телефонних закладок із високими значеннями імпедансу (понад 200 МОм). Тому актуальним є пошук нових методів виявлення ТЗП та розроблення чіткої методики проведення дослідження АТЛ із їх використанням. Ключовим завданням у цьому напрямку є використання високочутливих засобів інваріантних до впливу зовнішніх дестабілізуючих факторів [6,8]. Прикладом може бути пристрій виявлення несанкціонованих підключень до АТЛ, що використовує мостову схему для виявлення впливу закладки у поєднанні із фазовим методом опрацювання сигналу розбалансу (рис. 2).

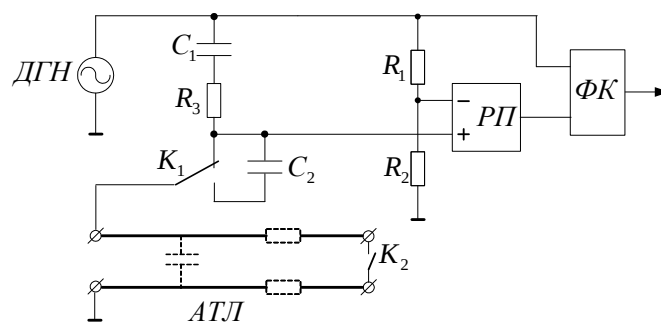


Рис. 2. Пристрій для виявлення несанкціонованого підключення до АТЛ: АТЛ – контрольована телефонна лінія, ДГН – джерело гармонічної напруги, РП – різницевий підсилювач, ФК – фазовий компаратор

Ядром пристрою є лінійний адаптер у вигляді мостової схеми, утвореної резистивним подільником напруги R_1 і R_2 , послідовною RC-ланкою у складі регульованого конденсатора C_1 та резистора R_3 , а також ємністю контрольованої АТЛ. Ємність регульованого конденсатора становлюється рівною відомому значенню чистої лінії, тобто $C_1 = C_{ТЛ}$. Якщо лінія чиста, фазовий зсув між сигналом розбалансу моста (напруга на виході РП) та напругою джерела живлення становить рівно 90° . У разі під'єднання до лінії закладки, фазовий зсув різко змінюється, що фіксується фазовим компаратором [9,10]. Зміна конфігурації мостової схеми за допомогою ключів K_1 і K_2 дає можливість виявляти послідовні закладки. Крім того, підвищити інформативність і достовірність результатів контролю можна шляхом вимірювання частотної залежності

параметрів імпедансу лінії у режимі холостого ходу та короткого замикання, а не лише ємності, індуктивності чи опору на одній фіксованій частоті [6].

Коли встановлено факт несанкціонованого впливу на АТЛ, наступним кроком є локалізація місця підключення телефонної закладки, для чого можуть застосовуватися метод імпульсної рефлектометрії, метод нелінійної локації [1,7].

Методи активного контролю, які використовують зовнішні впливи на АТЛ, можуть бути ефективними щодо виявлення ТЗП оснащених активаторами.

Порядок проведення пошукових робіт на АТЛ

У розробленій методиці проведення пошукових робіт можна виділити 4 етапи:

- підготовчий етап;
- виявлення активних, сторожових та обладнаних акустопуском закладних пристроїв;
- виявлення закладних пристроїв гальванічно під'єднаних до АТЛ;
- завершальний етап (візуальний огляд та паспортизація параметрів лінії).

На рис. 3 наведено блок-схему, яка відображає суть розробленої методики, місце і роль кожного методу контролю у загальному контексті пошукових робіт.

Усі проводові комунікації, зокрема телефонні лінії, що проходять через об'єкт інформаційної діяльності (ОІД), слід перевірити на ділянках від кінцевого обладнання, встановленого у приміщенні, що перевіряється, до найближчих розподільних коробок, щитів, розташованих за межами ОІД.

На підготовчому етапі перевіряється відповідність метрологічних умов вимогам інструкції з експлуатації засобів контролю. Наступним кроком є перевірка АТЛ, яка починається з уточнення схем та паспортних даних та включає: загальну довжину лінії від розетки до найближчого розподільного щита за межами об'єкту перевірки, усі санкціоновані з'єднання (розподільні коробки, щити, паралельні відводи з позначенням довжини лінії від розеток до з'єднань). У разі потреби проводиться ідентифікація ліній, тобто перевірка відповідності фактично прокладених ліній наявним схемам трас прокладання комунікацій на ОІД.

Другий етап розпочинається із активації ТЗП, оснащених, наприклад, системою акустозапуску, з метою приведення їх в робочий стан. Цей етап націлений на виявлення активних ТЗП, які передають перехоплені повідомлення у вигляді радіосигналів чи самою АТЛ з використанням спеціальних форматів кодування і модуляції. На цьому етапі також можна виявити пристрої несанкціонованого отримання інформації, що реалізують методи "мікрофонного ефекту", високочастотного нав'язування чи підкачки.

Пошук проводиться радіовиявлювачами із функцією аналізу проводових ліній в діапазоні частот, який властивий для ТЗП з передачею інформації такими лініями. Радіовиявлювач за допомогою спеціальних адаптерів з комплексу пошукової апаратури безпосередньо або безконтактно підключається до проводових комунікацій на найближчому розподільному щиті (коробці тощо), що знаходиться за межами контрольованої зони та безпосередньо біля кінцевого обладнання.

Виявлення сигналів ТЗП здійснюється шляхом послідовного аналізу спектру вказаного діапазону частот. Аналіз доцільно проводити в окремих ділянках частотного діапазону, звертаючи увагу на сигнали найбільшої інтенсивності.

Ідентифікація виявлених сигналів на приналежність до сигналів ТЗП проводиться шляхом їх демодуляції та прослуховування, а також за наступними ознаками:

- наявність кореляції між створеним у приміщенні акустичним тестом та прийнятим демодульованим радіосигналом;
- поява та зникнення сигналу при знятті і покладенні слухавки телефонного апарата;
- поява і зникнення сигналу на початку та вкінці робочого дня;

- наявність акустичної "зав'язки" при прослуховуванні радіосигналу через динамік приймального пристрою у випадку його розміщення поблизу мікрофону ТЗП;
- наявність у прийнятого сигналу гармонійних складових.

Після ідентифікації виявленого сигналу, як сигналу ТЗП, проводиться локалізація його джерела пошуковими приладами, що реалізують методи неруйнівного контролю або візуально. Для проведення даного етапу робіт рекомендовано використовувати широкосмгові сканувальні приймачі з програмним забезпеченням, які дають змогу аналізувати сигнали в автоматичному режимі. Для визначення небезпечних сигналів потрібно встановити пороговий рівень 10 мВ. Сигнали в лінії, що перевищують даний рівень, можуть свідчити про можливість несанкціонованого отримання інформації такими методами як високочастотне нав'язування та високочастотна підкачка.

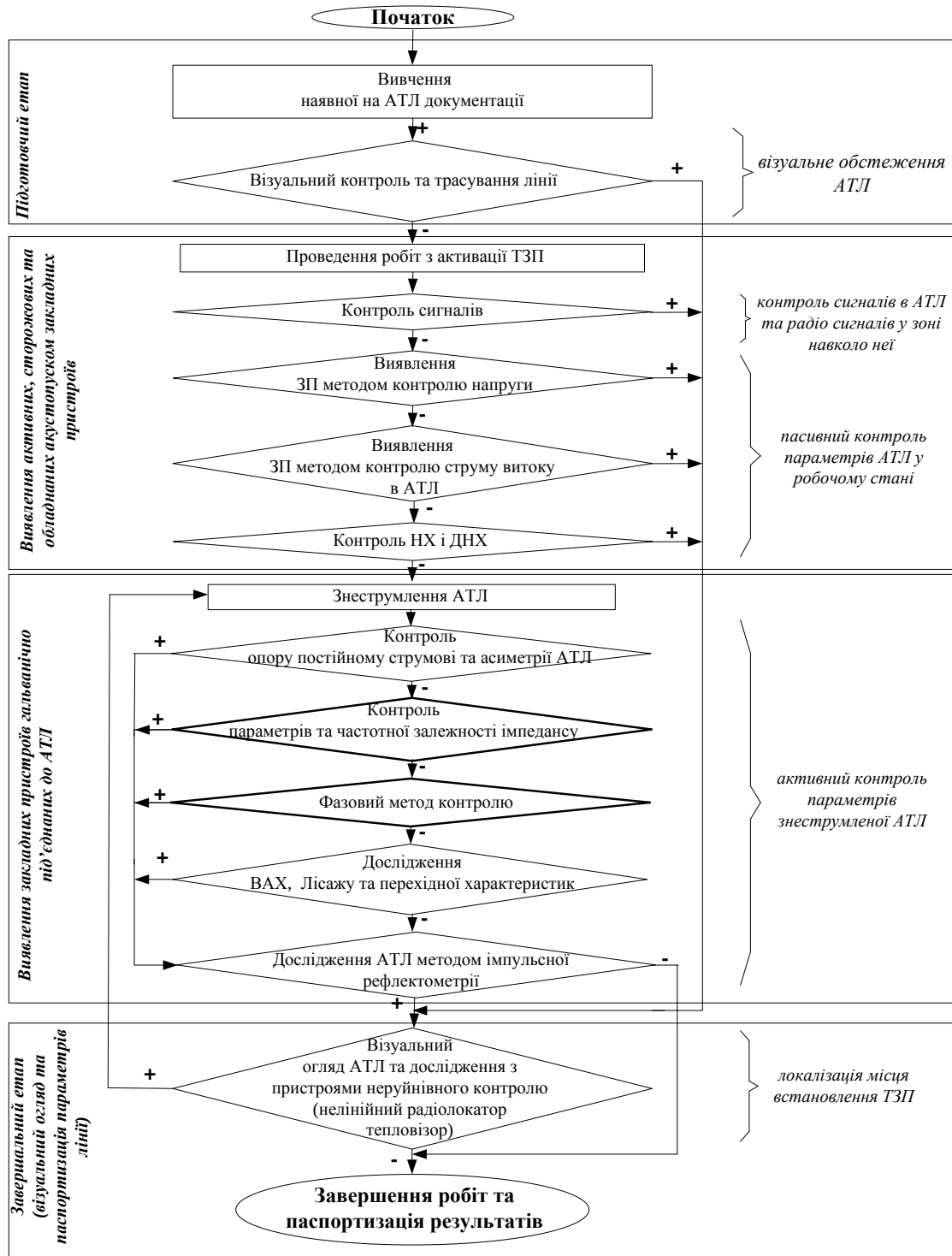


Рис. 3. Блок-схема алгоритму проведення робіт з виявлення ТЗП в АТЛ

Потрібно зазначити, що активовані закладні пристрої, можуть здійснювати запис інформаційних повідомлень на зовнішні запам'ятовуючі пристрої, тому не можуть бути виявлені шляхом контролю сторонніх сигналів. Для виявлення даної групи ТЗП в рамках другого етапу застосовуються методи контролю напруги, струму витоку та реєстрація навантажувальної характеристики. Отримані значення напруги живлення та струму шлейфу порівнюються із паспортними значеннями або з відповідними величинами на іншій лінії, що підключена до тієї ж АТС. Наприклад, різниця напруги живлення більше 1 В свідчить про можливу наявність ТЗП.

Дослідження навантажувальної характеристики дає змогу виявити наявність в досліджуваній телефонній лінії паралельно підключених ТЗП, що активуються підняттям слухавки і мають струм споживання не менше 0.1 мА. За перевищення струму шлейфу певного порогового рівня ТЗП активується, зумовлюючи стрибкоподібне збільшення струму споживання. Для кращого розпізнання моменту спрацювання ТЗП, використовують диференціальну навантажувальну характеристику. Допускається наявність зломів навантажувальної характеристики в першій третині кривої, що зумовлено неповним узгодженням вихідного опору пристрою із хвильовим опором лінії [7].

Перевірка телефонних ліній проводиться не лише у робочому режимі, але й у знеструмленому стані, причому достовірність результатів такого контролю зазвичай є вищою. Для перевірки необхідно відключити від ділянки лінії, що обстежуються: усіх відомих споживачів; всі санкціоновані паралельні відводи. Відключені паралельні відводи необхідно перевіряти як окремі ділянки лінії. При цьому, доцільно для порівняльного аналізу використовувати паспортні дані на проводіві комунікації ОІД та результати попереднього контролю.

Виявлення паралельно підключених ТЗП проводиться шляхом вимірювання опору ізоляції лінії за постійним струмом. За відсутності паралельних підключень опір ізоляції ділянки має перевищувати 20 МОм. Далі потрібно виміряти ємність розімкнутої лінії, а отримані результати порівняти з паспортними даними на лінію чи з результатами отриманими на аналогічній за типом лінії такої ж довжини.

Дослідження ліній на відсутність послідовно підключених ТЗП проводиться шляхом вимірювання асиметрії опору лінії. За відсутності сторонніх послідовних підключень опір ділянки має бути в межах одиниць-десятьків Ом залежно від її довжини і типу провідника. Крім того, потрібно виміряти індуктивність лінії в режимі короткого замикання на віддаленому кінці. Додатково рекомендується виконати вимірювання частотної залежності параметрів імпедансу лінії розімкнутої та замкнутої на віддаленому кінці.

З метою контролю лінії на предмет наявності компонентів з нелінійними характеристиками провести дослідження вольт-амперної характеристики лінії. Даний метод є ефективним за наявності у вхідному колі закладного пристрою напівпровідникових елементів, що характеризуються значною нелінійністю імпедансу. Вимірювання вольт-амперної характеристики може проводитись у двох режимах: з використанням джерел лінійно-зростаючої напруги на постійному і на змінному струмі.

Виявити наявність підключень з нелінійним вхідним імпедансом можна також шляхом візуального оцінювання зареєстрованої форми фігури Ліссажу. Оцінюється форма та кут нахилу до горизонтальної осі, відхилення цих параметрів свідчить про наявність додаткових резистивних елементів в лінії, а спотворення форми - про присутність напівпровідникових елементів. Також проводять дослідження перехідної характеристики, а візуальній оцінці піддаються такі її параметри, як монотонність, тривалість, форма. Для підвищення інформативності результатів контролю автори вважають за доцільне аналізувати не самі характеристики, а їх відхилення від зареєстрованих на «чистій лінії».

Для локалізації місця знаходження ТЗП використати метод імпульсної рефлектометрії. Перевірку необхідно проводити з боку розподільного щита, розподільної коробки, розташованих за межами об'єкта, що перевіряється [6]. У ході перевірки візуально, виходячи із аналізу форми відбитого сигналу, визначається неоднорідність імпедансу, що може свідчити про факт підключення до лінії. За видом та рівнем спотворень можна визначити ступінь неоднорідності лінії та відстань до неї.

Перевірка ліній на відсутність безконтактних ТЗП із індуктивним або ємнісним способом підключення проводиться методами неруйнівного контролю (нелінійний радіолокатор чи тепловізор) або візуального пошуку.

Висновки

Особливості будови та функціонування абонентської телефонної лінії дають змогу її використати не лише для перехоплення телефонних переговорів, а також як складову технічних каналів витоку мовної інформації із приміщення, де розташовано телефонний апарат.

Різноманітність методів і засобів ведення технічних розвідок на телефонних лініях, а також постійне удосконалення схемо-технічних та конструкторських рішень із маскувannya ТЗП вимагає пошуку нових принципів побудови засобів контролю АТЛ та удосконалення методик проведення пошукових робіт. Засоби контролю, побудовані на основі відомих методів, через обмежену чутливість не виявляють телефонних закладок із високими значеннями імпедансу. Тому актуальним є використання нових методів виявлення ТЗ та розроблення засобів контролю АТЛ на їх основі. Авторами запропоновано використання лінійного адаптера на основі незрівноваженої мостової схеми з регульованою чутливістю та каналом вимірювання фазового зсуву із підвищеною завадостійкістю.

Розроблена методика проведення інструментального контролю наявності несанкціонованих підключень до АТЛ враховує особливості будови, функціонування та способів використання сучасних ТЗП, що дає змогу оптимізувати порядок проведення пошукових робіт, скоротити час та знизити затрати, забезпечивши при цьому достовірність результатів контролю.

Список літератури

1. Дудикевич, В.Б. Захист засобів і каналів телефонного зв'язку: навч. посібник / В.Б. Дудикевич, В.В. Хома, Л.Т. Пархуць. - Львів: Видавництво Львівської політехніки, 2012. - 212 с.
2. Конахович, Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. - К.: «МК-Пресс», 2005. - 288 с.
3. Хорев, А.А. Класифікація електронних пристроїв перехоплення інформації / А.А. Хорев // Спецтехніка і зв'язок. - 2009. - №1. - С. 46-49.
4. Ленков, С.В. Методи і засоби захисту інформації. У 2-х томах / С.В. Ленков, Д.А. Перегудов, В.О. Хорошко. Під ред. В.А. Хорошко. - К.: Арій - Том I. Несанкціоноване отримання інформації, 2008. - 464 с.
5. Хома, В.В. Методи і засоби технічного захисту інформації на абонентських телефонних лініях / В.В. Хома // Вісн. Нац. ун-ту "Львів. політехніка". - 2009. - №639. - С. 87-93.
6. Іванюк, В.М., Аналіз перспективних напрямів удосконалення засобів виявлення закладних пристроїв у телефонних лініях / В.М. Іванюк, В.В. Хома // Вісн. Нац. ун-ту "Львів. політехніка". - 2013. - №774. - С. 92-96.
7. Іванюк, В. Фазовий метод виявлення закладних пристроїв у телефонних лініях / В. Іванюк, В. Хома // Захист інформації. - 2014. - т.16. - №3. - 243 с.
8. Іванюк, В.М. Пат. 108186 Україна, МПК2015.01 Н 04М 1/68, Н 04 L 12/22. Пристрій для виявлення несанкціонованого підключення до абонентської телефонної лінії [Текст] / В.М. Іванюк, В.В. Хома; заявник і власник Національний університет "Львівська політехніка"; опубл. 25.03.15, Бюл. № 6.

9. Иванюк, В.М. Пат. 108187 Україна, МПК2015.01 Н04М 1/68 (2006.01), Н04М 1/00. Пристрій для виявлення несанкціонованого підключення до абонентської телефонної лінії [Текст] / В.М. Иванюк, В.В. Хома; заявник і власник Національний університет "Львівська політехніка"; опубл. 25.03.15, Бюл. № 6.

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ВЫЯВЛЕНИЯ ЗАКЛАДНЫХ УСТРОЙСТВ НА АБОНЕНТСКОЙ ТЕЛЕФОННОЙ ЛИНИИ С УЧЕТОМ ВОЗМОЖНОСТЕЙ СОВРЕМЕННЫХ СРЕДСТВ КОНТРОЛЯ

В.В. Хома, В. М. Иванюк

Національний університет "Львівська політехніка",
ул. С. Бандеры, 12, г. Львов, 79013, Украина; e-mail: Volodymyr.V.Khoma@lpnu.ua;
e-mail: vitalikivaniuk@gmail.com

Статья посвящена вопросу структуризации методики проведения работ по выявлению устройств несанкционированного получения информации с абонентских телефонных линий. Проанализированы структура и функционирование современных телефонных закладных устройств и отмечены их основные демаскирующие признаки. Дана также сравнительная характеристика известных методов, применяемых для выявления несанкционированных подключений к телефонным линиям, указаны пути улучшения характеристик средств контроля. В этом контексте предложено использование линейного адаптера реализующего фазовый метод выявления телефонных закладных устройств, который обладает повышенной помехоустойчивостью. Разработана и представлена в виде блок-схемы методика проведения работ по выявлению несанкционированных подключений к телефонным линиям, которая учитывает возможности современных средств контроля и позволяет оптимизировать временные издержки.

Ключевые слова: абонентская телефонная линия, телефонное закладное устройство, демаскирующие признаки, методы выявления несанкционированных подключений, методика проведения поисковых работ, линейный адаптер.

IMPROVEMENT OF PROCEDURE FOR DETECTION OF TELEPHON BUGS WITH DUE CONSIDERATION OF MODERN MONITORING DEVICE CAPABILITES

V.V. Khoma, V.M.Ivanyuk

National University "Lviv Polytechnic",
Bandera str. 12, Lviv, 79013, Ukraine; e-mail: Volodymyr.V.Khoma@lpnu.ua
e-mail: vitalikivaniuk@gmail.com

The article is devoted to problem of structuring procedure to identify unauthorized devices for the information access on subscriber telephone lines. The structure and operating of modern drop-in-telephone bugs are analyzed and the basic give-away factors are discriminated. A comparison performance of well-known of methods used to detect unauthorized connections to telephone subscriber lines is given. Ways to improve performances of monitoring facilities are pointed. In this context, the using of linear adapter that implements the phase method to detection of drop-in-telephone bugs has been proposed. This device has a higher jamming resistance. A control flow chart of the procedure to identify unauthorized connections to telephone lines is developed and presented. This methodology takes account of modern control devices capabilities and offers the possibility to optimize of time expenditures.

Keywords: subscriber telephone line, drop-in-telephone bugs, give-away factors, methods of detecting unauthorized connections, procedure to identify, line adapter.

КОНТРОЛЬ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ МЕТОДАМИ ИДЕНТИФИКАЦИИ ПРИ НАТУРНОМ МОДЕЛИРОВАНИИ

Л.Л. Прокофьева, С.П. Савич, А.Н. Порпулит

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: proklu@mail.ru

Рассмотрены особенности организации вычислительного процесса для класса натуральных имитаторов, реализованных на аналого-цифровом (гибридном) вычислителе. Показана эффективность использования в гибридных натуральных имитаторах аналогового процессора в качестве динамической модели объекта, что обусловлено высоким быстродействием вследствие распараллеливания и неалгоритмических вычислений в ходе моделирования динамики. Предложен подход к контролю вычислительного процесса при натурном моделировании, основанный на методах идентификации, и получены конструктивные выражения оценки функционирования вычислительно-управляющих систем гибридных натуральных имитаторов.

Ключевые слова: вычислительный процесс, натурные вычислительно-моделирующие системы, аналоговый процессор, цифровой процессор, оперативный контроль, оценка функционирования, методы идентификации.

Введение

В последние годы в теории и практике моделирования развивается новое направление по созданию средств моделирования, базирующееся на сочетании концепций физического и квазианалогового моделирования. Основной особенностью такого рода средств моделирования, называемых натурными вычислительно-моделирующими системами (НВМС), является наличие в их составе реального моделирующего объекта (базового), сходного по физическому характеру с моделируемым объектом, и системы управления (УС или, в более общем случае, вычислительной управляющей системы — ВУС), предназначенной для выработки (вычисления) таких управляющих воздействий базового объекта, которые обеспечивают его эквивалентность моделируемому объекту. Возможности подобного рода средств моделирования достаточно полно характеризуются примерами НВМС подвижных объектов (в частности, натуральных имитаторов), в качестве которых можно привести следующие:

- летающие самолетные имитаторы, в которых обеспечивается совпадение поведения базового и моделируемого самолетов в реальных полетных условиях, что позволяет решать задачи как исследовательского характера (например, отработка систем управления проектируемых или разрабатываемых самолетов), так и тренировки и обучения летного состава;
- динамически эквивалентные имитаторы надводных и подводных судов, а также сухопутных передвижных средств (например, автомобилей), создание которых позволяет в условиях, близких к реальным, организовать полигонное обучение и тренировку экипажей по управлению в разнообразных ситуациях (маневры в портах и на трассах судоходства, движение в тумане и др.);

■ исследовательские комплексы высокоточных электромеханических систем локации, при создании которых одной из основных задач является разработка системы управления и законов определения управляющих воздействий, обеспечивающих заданное качество процессов наведения (слежения).

Высокие точностные требования приводят к тому, что отработка законов управления, например, процессами локации возможна лишь путем создания на базе ЭВМ системы моделирования, включающей собственно электромеханический объект, что обеспечивает полный учет и анализ значимости всех факторов, оказывающих влияние на точность наведения. Подобного рода системы моделирования предназначены, в частности, для проведения исследований по оценке правильности конструктивных решений, качества процессов локации и параметров законов управления.

Практическая необходимость создания НВМС (в том числе НВМС подвижных объектов) заключается в получении инструмента, позволяющего как существенно повысить экономичность и качество исследований сложных систем, так и более качественно организовывать процессы обучения, тренировки и профессионального отбора обслуживающего персонала.

Очевидно, что в процессе натурного моделирования следует обеспечить достоверность вычисленных управлений моделирующего (базового) объекта динамике реального (моделируемого) объекта.

Цель работы

Получение адекватных оценок функционирования вычислительно-управляющей системы натуральных имитаторов, реализованной на основе аналого-цифрового вычислителя.

Основная часть

В общем случае построение ВУС НВМС возможно с применением различных средств вычислительной техники. При этом различны и стратегии организации контроля вычислений.

Особый интерес в данном случае представляет использование в качестве динамической модели объекта аналоговый процессор (суть — аналоговая вычислительная машина — АВМ), обеспечивающий высокое быстродействие вследствие неалгоритмического вычислительного процесса в ходе моделирования [1, 2]. Однако, необходимость учета производных высоких порядков [3], приводит к тому, что исполнение ВУС НВМС сложных динамических объектов в аналоговом виде практически невозможно. В то же время, построение ВУС на базе аналого-цифровых вычислительных комплексов или с включением в их состав, так называемых аналоговых подпрограмм [4 — 8], является достаточно перспективным. Укажем также на вариант НВМС, базовый объект которого содержит аналоговый вычислитель. Сказанное обуславливает важность контроля вычислений, выполняемых аналоговыми средствами.

Как указывается в [9], задача оперативного контроля аналогового процессора является одной из важных проблем аналоговой вычислительной техники. Попытка решить указанную проблему с использованием аналоговой техники приводит к методам контроля, которые, в основном, ориентированы на контроль исправности отдельных элементов и узлов АВМ [9, 10]. Для контроля и диагноза неисправностей АВМ находит применение метод *избыточных переменных* [11] который не всегда

является эффективным при контроле решения уравнений, описывающих динамику управляемых нелинейных объектов.

В гибридных вычислительных системах (ГВС) возможно использование цифрового процессора (т.е. цифровой вычислительной машины — ЦВМ) для контроля АВМ. При этом осуществляется как построение контрольных и диагностических тестов АВМ с помощью ЦВМ [12, 13], так и контроль в процессе решения уравнений динамики [14, 15].

В [16] излагается метод диагностики неисправностей аналоговых моделей, описываемых системой линейных ОДУ с постоянными коэффициентами. Метод основан на решении обратной задачи и сводится к определению матрицы правой части решаемой системы по полученному решению. Диагностика неисправностей осуществляется сравнением идентифицированной матрицы решаемой системы (для моделирующего объекта) с заданной матрицей (для реального объекта). Все операции по диагностике неисправностей выполняются на ЦВМ. Данная процедура диагностики основана на аппроксимации переходного процесса линейной комбинацией экспоненциальных функций. При диагностике моделей нелинейных объектов применение описанного подхода сталкивается со значительными трудностями.

Контроль аналоговой модели сравнением аналогового решения с решением, полученным на ЦВМ, достаточно распространен, однако обладает такими недостатками, как необходимость преодоления трудностей численного решения исходной задачи в полной постановке на ЦВМ, существенные затраты машинного времени, невозможность установления причин возникновения ошибок.

Контроль, если он осуществляется путем прямого измерения, всегда представляет собой некоторую обратную задачу, в частности, задачу *оценки параметров* объекта по его выходным и входным воздействиям. В таком случае имеется возможность привлечь различные методы идентификации [17], которые обладают значительными возможностями для решения задач контроля динамических систем [18], в том числе и аналоговых моделей.

В формализованном виде, контроль на основе методов *параметрической идентификации* осуществляется следующим образом. По наблюдаемым переменным объекта оцениваются параметры его математической модели. И уже по результату сравнения полученных оценок параметров с заданными значениями принимается решение о состоянии объекта.

Применим данный подход к оцениванию функционирования вычислительно-управляющей системы натуральных имитаторов, реализованной на основе аналого-цифрового вычислителя. Предположим, что существует система уравнений той же структуры, что и моделируемая, но с другими (в общем случае переменными) параметрами $q = (q_1, \dots, q_m)^T$:

$$z = f(z, u^*, q, t), z(t_0) = z_0, \quad (1)$$

где $z = y_u + \Delta y$ — вектор, описывающий контролируемый объект, и параметры которого (при отсутствии ошибок в реализации уравнений динамики) совпадают с параметрами моделируемой системы. Путем измерения или расчета соответствующих величин формируется информация о входных u^* и выходных z сигналах объекта контроля. Наблюдаемый вектор $\bar{z}$ является в общем случае известной функцией векторов состояния z и управлений u^* . Если переменные непосредственно измеряются, то $\bar{z} = E_z + (v, u) = Eu^* + v$, где E — единичная матрица, v — аддитивный шум системы измерения. Шумы измерения зависят от точности «считывания» аналоговой информации или переменных в цифровой форме. В аналоговых моделях к

шумам измерения добавляются внутренние шумы самой модели. В системе измерения может производиться отделение сигнала от шумов, т.е. решаться задача фильтрации.

Результаты измерения предназначены для определения параметров математической модели (1), т.е. для проведения параметрической идентификации. По результатам, полученным с помощью идентификации, определяется по какому-либо критерию состояние объекта контроля. Для аналоговых моделей при обнаружении ошибки решается задача определения причины, вызвавшей ошибку, т.е. задача диагностики.

Использование средств аналоговой вычислительной техники для реализации контроля на основе идентификации приводит к большой избыточности оборудования, а точность оценок параметров при этом невысокая. В связи с этим методы контроля, ориентированные на применение ЦВМ, в частности, целесообразны при контроле аналоговых моделей в аналого-цифровых вычислительных комплексах (АЦВК). В этом случае по мере необходимости ЦВМ подключается к проверке аналоговой модели без вмешательства в ее работу.

Пусть объект контроля описывается уравнением

$$\dot{\psi} = f(z, u, q, t), y(t_0) = y_0. \quad (2)$$

а модель, используемая при идентификации, имеет вид

$$\dot{z} = f(z, u, \hat{q}, t), z(t_0) = z_0, \quad (3)$$

где $\hat{q} = (\hat{q}_1, \dots, \hat{q}_m)^T$ — вектор оценок параметров.

Обычно оценки параметров $\hat{q}$ определяются из условия минимума квадратичного функционала. Если известно с точностью до оценок параметров $\hat{q}$ аналитическое решение $z = \varphi(u, \hat{q}, t)$, то указанный функционал в матричной форме имеет вид

$$y(\hat{q}) = [b - A(\hat{q})]^T [b - A(\hat{q})], \quad (4)$$

где $b = [y(t_1), \dots, y(t_N)]^T$, $A(\hat{q}) = [\varphi(u, \hat{q}, t_1), \dots, \varphi(u, \hat{q}, t_N)]^T$.

Оценка $\hat{q}$ вектора параметров q находится из условия

$$\frac{\partial y(\hat{q})}{\partial(\hat{q})} = \frac{\partial A(\hat{q})}{\partial(\hat{q})} [b - A(\hat{q})] = 0. \quad (5)$$

Выражение (5) представляет собой систему нелинейных относительно $\hat{q}$ алгебраических уравнений, решением которой является искомая оценка вектора параметров q .

Определение оценок параметров $\hat{q}_i, i = \overline{1, m}$ из условия близости выходов объекта и модели, заданной в виде дифференциальных уравнений, приводит к нелинейным процедурам оценивания даже в том случае, когда модель объекта линейна по параметрам (из-за нелинейной зависимости решения от параметров).

Выводы

Получены аналитические выражения для определения оценок функционирования вычислительно-управляющей системы натуральных имитаторов, реализованной на основе аналого-цифрового вычислителя. Вычислительная процедура определения оценок

основана на методах параметрической идентификации и не требует прямых измерений векторов состояний натурной модели (имитатора) реального (моделируемого) объекта.

Однако, в ряде практических случаев, аналитическое решение сложных дифференциальных уравнений получить затруднительно (или, даже, невозможно) и для определения переменных z следует привлекать численные методы, что значительно усложняет процедуру идентификации.

Литература

1. Смолов, В.Б. Аналоговые вычислительные машины / В.Б. Смолов. — М.: Высшая школа, 1992. — 408 с.
2. Садчиков, П.И. Вычислительные устройства и системы / П. И. Садчиков, Ю. В. Шаповалов. — М.: Высшая школа, 1988. — 237 с.
3. Гноенский, Л.С. Математические основы теории управляемых систем / Л.С. Гноенский, Г.А. Каменский, Л.Э. Эльсгольд. — М.: Физматгиз, 1969. — 512 с.
4. Беки, Дж. Теория применения гибридных вычислительных систем / Дж. Беки, У. Карплюс. — М.: Мир, 1970. — 484 с.
5. Таненбаум, Э.С. Архитектура компьютера / Э.С. Таненбаум. — СПб.: Питер, 2007. — 848с.
6. Бройдо, В.Л. Архитектура ЭВМ и систем / В.Л. Бройдо, О.П. Ильина. — СПб.: Питер, 2009. — 720 с.
7. Новиков, Ю.В. Функциональные модули контрольно-измерительных систем / Ю.В. Новиков // Микропроцессорные средства и системы. — 1990.— №3.— С. 75 — 77.
8. Баррет, С.Ф. Встраиваемые системы / С.Ф. Баррет, Д. Дж. Пак. — М.: ДМК - пресс, 2007. — 640 с.
9. Бердяков, Г.И. Методы контроля аналоговых вычислительных машин / Г.И. Бердяков, И.М. Витенберг. — М.: Машиностроение, 1988. — 240 с.
10. Силаева, Т.А. Обеспечение надежного функционирования ЭВМ и систем / Т.А. Силаева. — М.: МАИ, 1993. — 146 с.
11. Мироновский, Л.А. О качестве контроля АВМ при использовании метода избыточных переменных / Л.А. Мироновский // Вопросы радиоэлектроники. — 1989. — Вып. 4. — С. 47 — 55.
12. Согомонян, Е.С. Самопроверяемые устройства и отказоустойчивые системы / Е.С. Согомонян, Е.В. Слабоков. — М.: Радио и Связь, 1989. — 208 с.
13. Курочкин, Ю.А. Надежность и диагностирование цифровых устройств и систем / Ю.А. Курочкин, А.С. Смирнов, В.А. Степанов. — СПб.: Питер, 1993. — 317 с.
14. Burrage, K. Numerical Methods for Second-Order Stochastic Differential Equations / K. Burrage, I. Lenane, G. Lythe // SIAM Journal on Scientific Computing. — 2007. — Vol. 29. — №. 1. — P. 245 – 264.
15. Kang, G. Efficient Implementation Techniques for Gracefully Degradable Multiprocessor Systems / G. Kang // IEEE Trans, on Contr. — 1995. — Vol. 44. — №. 4. — P. 503 — 517.
16. Верлань, А.Ф. Вычислительные процессы в системах управления и моделирования / А.Ф. Верлань, И.Е. Ефимов, А.В. Латышев. — Л.: Судостроение, 1989. — 244 с.
17. Мокін, Б.І. Математичні методи ідентифікації динамічних систем / Б.І. Мокін, В.Б. Мокін, О.Б. Мокін. — Вінниця: ВНТУ, 2010. — 260 с.
18. Евланов, Л. Г. Контроль динамических систем / Л.Г. Евланов — М.: Наука, 2009. — 431 с.

КОНТРОЛЬ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕСІВ МЕТОДАМИ ІДЕНТИФІКАЦІЇ ПРИ НАТУРНОМУ МОДЕЛЮВАННІ

Л. Л. Прокофьева, С. П. Савич, А. Н. Порпулит

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

Розглянуто особливості організації обчислювального процесу для класу натурних імітаторів, реалізованих на аналого-цифровому (гібридному) обчислювачі. Показано ефективність використання в гібридних натурних імітаторах аналогового процесору в якості динамічної моделі об'єкта, що обумовлено високою швидкістю внаслідок розпаралелювання та неалгоритмічних обчислень в ході моделювання динаміки. Запропоновано підхід до контролю за обчислювальним процесом при натурному моделюванні, заснований на методах ідентифікації та отримано конструктивні вирази оцінювання функціонування обчислювально-управляючих систем гібридних імітаторів.

Ключові слова: обчислювальний процес, натурні обчислювально-моделюючі системи, аналоговий процесор, цифровий процесор, оперативний контроль, оцінка функціонування, методи ідентифікації.

CONTROL OF CALCULABLE PROCESSES BY METHODS OF AUTHENTICATION AT MODEL DESIGN

L. L. Prokofieva, S. P. Savich, A. N. Porpulis

Odessa national polytechnic university,
1 Shevchenko Ave., Odessa 65044, Ukraine; e-mail:

The features of organization of calculable process for the class of the model imitators realized on an analog-digital (hybrid) calculator are considered. Efficiency of the use in the hybrid model imitators of analog processor as the dynamic model of object is shown, that is conditioned by the high fast-acting because of parallel and unalgorithmic calculations during the design of dynamics. Offered approach to the control of calculable process at the model design, based on the methods of authentication and structural expressions of estimation of functioning of the sensor-based systems of hybrid model imitators are got.

Keywords: calculable process, model calculable-designing systems, analog processor, digital processor, operative control, estimation of functioning, methods of authentication.

МОДЕЛЬ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАХИСТУ ПРОГРАМНОГО КОДУ ВІД НЕСАНКЦІОНОВАНИХ ЗМІН

А.Є. Кілін¹, В.Г. Кононович¹, І.В. Кононович², В.В. Беззубенко³

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

² Одеська національна академія харчових технологій,
вул. Канатна, 112, м. Одеса, 65039, Україна; e-mail: kononovich@mail.ru

³ Одеська національна академія зв'язку,
ул. Кузнечная, 1, Одеса, 65021, Україна; e-mail: vladimirbezzubenko@gmail.com

В роботі пропонується, додатково до існуючих, механізм захисту програмного коду від несанкціонованого змінювання. На цьому прикладі вдосконалюється загальна модель оцінки ефективності системи захисту. Алгоритм захисту заснований на стеганографічних підходах. Оцінка ефективності захисту проводиться за допомогою моделі вибору оптимального рівня захищеності за принципом «витрати на захист – ефективність». При цьому формалізуються типові залежності відшкодування збитків від рівня захищеності та залежності витрат на побудову системи безпеки від того ж рівня захищеності. Доводиться, що в загальному випадку доцільно обирати функцію Ципфа для залежності відшкодування збитків від рівня захищеності та одну з гіперболічних функцій для залежності витрат на побудову системи безпеки від того ж рівня захищеності. Введення названих функцій в модель вибору оптимального рівня захищеності дозволила перейти від якісних оцінок витрат на організацію системи безпеки до конкретних обчислень при математичному експерименті. Вдосконалена модель захисту та загальної оцінки ефективності системи захисту дозволить обґрунтовувати доцільність підвищення рівня захищеності програмного коду.

Ключові слова: захист програмного коду, несанкціоновані зміни, оцінка ефективності, рівень захищеності, моделювання, математичний експеримент.

Вступ

Дана робота відноситься до сфери забезпечення авторських прав на корисні моделі – програмне забезпечення і розглядає проблеми застосування та оцінки ефективності алгоритмічних і стеганографічних методів у комплексах захисту програмного коду від несанкціонованих змін.

Загальні методи та принципи захисту програмного коду розглянуті у відомій монографії [1]. Питання захисту програм від несанкціонованого тиражування, застосування стеганографії, аналізу засобів захисту та інструментів, які застосовуються при дослідженнях, а також методи оцінки ефективності захисту, розглянуті у [2]. Спостерігається вал науково-технічних матеріалів та пропонованих застосувань захисту програмного коду. З останніх робіт відмітимо [3; 4], де розглядається комбінований захист програмного забезпечення від несанкціонованих впливів та методи захисту програмного коду. Методи аналізу програм, захисту від аналізу та інструментарії виявлення змін викладені у навчальному посібнику [5]. Навики дослідження коду зловмисного програмного забезпечення, необхідні для розробки протидії, розглядаються в [6].

Класичною роботою по управлінню інформаційними ризиками та знаходженню економічно виправданої безпеки є книга [7]. Але залежності витрат на побудову

системи безпеки та залежності відшкодування збитків від досягнутого рівня захищеності досліджені недостатньо. Наприклад, витрати на компенсацію порушень політики безпеки вважаються лінійно залежними від рівня захищеності. Тому формалізація вказаних залежностей є актуальною задачею.

Метою роботи є розроблення стеганографічного, додаткового до алгоритмічних, механізму захисту програмного коду від несанкціонованих змін і вдосконалення моделі оцінки його ефективності за принципом оптимізації витрат на захист шляхом формалізації типових залежностей витрат на запобіжні заходи захисту та залежності витрат на відновлення втрат від рівня захищеності.

Стеганографічний спосіб захисту програмного коду

Для підвищення рівня захищеності програмного коду в комплексі системи захисту від несанкціонованих змін, додатково до існуючих засобів захисту, пропонується механізм захисту, заснований на стеганографічних методах. Основною метою тут є як захист від несанкціонованих змінень, так і захист самого коду. Наприклад, ми винайшли певний алгоритм і хочемо випускати програму, яка його використовує. Але при цьому ми хочемо, щоб сам алгоритм залишився секретом. Для цього нам необхідно цей алгоритм приховати всередині нашої програми. Вирішення цієї проблеми, у свою чергу, також веде до захисту від несанкціонованих змінень. Цей наслідок витікає із факту, що сам доступ до коду та, відповідно, змінення утруднені. Суть методу полягає в наступному.

Ділянки коду, що становлять підвищену цінність, будемо вбудовувати у стегано-контейнер. У ролі стеганоконтейнеру можуть виступати звичайні зображення, які у наш час є у багатьох програмних продуктах. Прихований код буде динамічно вийматися, компілюватися та виконуватися під час роботи програми. Таким чином, такий код буде існувати в його початковому вигляді лише під час виконання програми у динамічній пам'яті.

У якості стеганографічного метода добре підходить метод найменшого значущого біту, через його високу пропускну спроможність.

Модель оптимізації системи захисту за принципом «мінімізація витрат – ефективність»

Якісну модель оптимізації системи захисту інформаційного середовища підприємства за принципом «мінімізація витрат – ефективність» описав у своїй книзі Петренко [7]: «Взаємозв'язок між усіма витратами на безпеку, спільними витратами на безпеку та рівнем захищеності інформаційного середовища підприємства може бути представлена так, як це зображено на рис. 1.

Загальні витрати на безпеку складаються із витрат на запобіжні заходи, на контроль та відновлювання втрат (внутрішніх і зовнішніх). Із зміною рівня захищеності інформаційного середовища змінюються величини складових спільних витрат і, відповідно, їх сума – спільні витрати на безпеку».

Графіки побудовані із врахуванням наступних допущень: по-перше, при виконанні робіт по попередженню порушень політики безпеки (ППБ) у першу чергу виконуються роботи, які дають найбільший ефект по захисту інформаційного середовища; по-друге, залежності й активність атак не змінюються у часі, тоді економічний баланс не міняється.

Застосуємо дану якісну модель для оцінки ефективності механізму захисту програмного коду. Для цього проведемо і обґрунтуємо формалізацію складових залежностей для певних типових випадків. Крім того, необхідно дати відповідну

інтерпретацію моделі. «Будемо розглядати залежності витрат від відносного рівня захищеності x , який змінюється від 0 до 1. При цьому, $x=0$ відповідає незахищеній системі; $x=1$ відповідає високому рівню захищеності системи; $x<1$ означає, що абсолютно захищених систем у природі не існує.

Величина витрат – y також є відносною, що змінюється у інтервалі від 0 до 1. При визначенні відношення затрат на безпеку використовують яку-небудь базу вимірювань. Типовими базами вимірювання можуть бути: обсяг проданої продукції, якщо він не залежить від сезонних факторів або інших циклічних змін; обсяг виробництва; трудоемність, що представляється як величина оплати праці, безпосередньо витраченої на виробництво продукції, якщо вона має стабільний характер; обсяг ресурсів інформаційного середовища підприємства, тобто сукупна вартість власних ресурсів, які виділяються інформаційному середовищу підприємства, або величина витрат на заміну або відновлення працездатності тощо. База вимірювань не повинна залежати від поліпшення технологій, автоматизації виробничих процесів, зміни обслуговуючого персоналу. Порівнювані величини повинні братись у їх вартісному вираженні [7]».

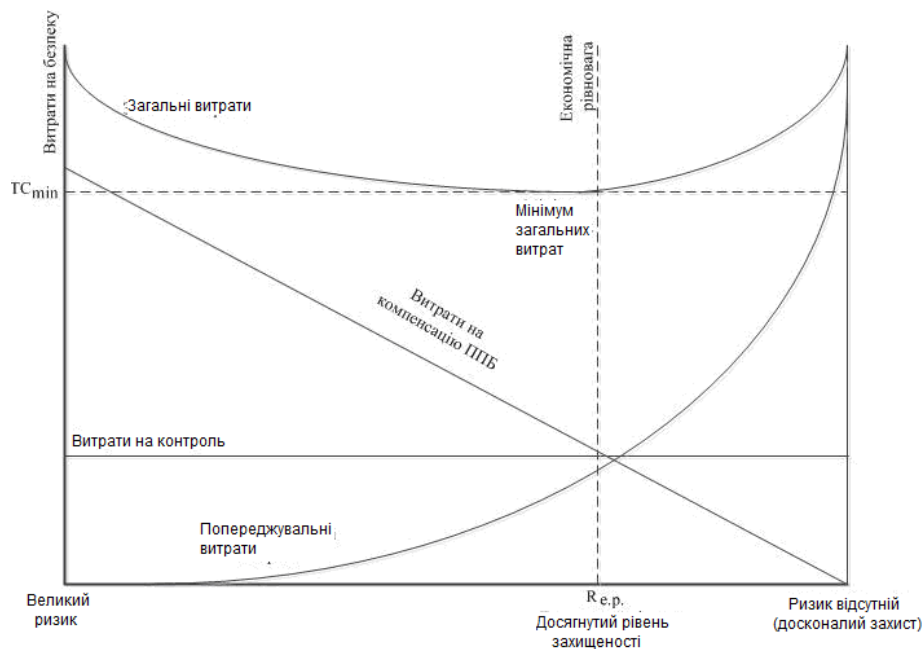


Рис.1. Модель оптимальних витрат на захист інформаційного середовища підприємства (модель запозичена із [7, рис. П7.4])

Витрати на компенсацію наслідків несанкціонованої зміни програмного коду. По суті ці витрати можна оцінювати величиною збитків від несанкціонованої зміни програмного коду. На рис. 1 ця залежність (витрати на компенсацію ППБ від рівня захищеності) лінійна. Це досить грубе наближення. В нашому випадку в реалізації загроз найбільше значення має людський фактор. Взаємодія людини з навколишнім середовищем має нелінійний характер. Реакція людини (її зору, слуху, нюху тощо) пропорційна логарифму подразнення. Скоріше за все, сприймання людиною рівня загроз або рівня витрат теж є нелінійним. Тому математичні формули для типових залежностей необхідно шукати серед стійких статистичних розподілів і залежностей. Такі розподіли дозволяють передбачати результати майбутніх випробувань у масових випадкових явищах.

Класичним є «нормальний розподіл», що впливає із закону великих чисел. У теорії ймовірностей існує центральна гранична теорема (теорема Ляпунова), що стосується граничних законів розподілу суми випадкових величин. Згідно цієї теореми

сума незалежних випадкових величин x_i ($i=1,2,\dots,n$), які мають будь-який розподіл, наближаються до нормального при необмеженому збільшенні величини n , якщо виконуються наступні умови: 1) всі величини мають скінчені математичні очікування m_i та дисперсії $M((x_i - m_i)^2) = D_i = \sigma_i^2$; 2) ні одна з величин по значенню різко не відрізняється від інших. Останнє породжує правило обробки статистичних даних, за якого найбільше та найменше значення відкидаються. Сказане означає, що кандидатом для формалізації залежності між нормованою величиною збитків при несанкціонованій зміні програмного коду та рівнем захищеності може служити нормальний (гаусів) розподіл при $m = 0$:

$$y_1 = \varphi(x) = \frac{k}{\sigma\sqrt{2\pi}} \exp\left(-x^2/2\sigma^2\right), x = \overline{0,1}, \quad (1)$$

де k – нормуючий коефіцієнт; σ – середньоквадратичне відхилення.

Але, незважаючи на широке розповсюдження нормального розподілу у науці й техніці, цей розподіл не підходить до опису згаданих залежностей. По-перше, пряма лінія на рис.1 більше підходить до опису залежності між нормованою величиною збитків та рівнем захищеності, ніж крива Гауса. По-друге, ця крива не може описувати соціальні явища в силу їх «негаусовості». Цей феномен пояснюється далі.

Другим кандидатом для формалізації залежності між нормованою величиною збитків та рівнем захищеності може служити експоненціальна функція

$$y_2(a, x) = \exp(-ax), x = \overline{0,1}, \quad (2)$$

де a – параметр.

Експоненціальна функція має важливу властивість. Швидкість зміни експоненціальної функції пропорційна значенню функції у цій точці. Завдяки цьому, вона застосовна для опису багатьох природних процесів. У даному разі експоненціальна функція показує, що зі збільшенням рівня захищеності втрати зменшуються. При $x=1$, $y(x) > 0$. Це певною мірою відповідає реальній ситуації. Абсолютно захищених систем не буває. І при високому рівні захищеності можливі втрати.

Теоретично можливі ситуації, коли подія настає, але це відбувається рідко, потенційна шкода невелика і тоді приймається рішення не захищатись від такої загрози. Можливі також загрози непереборної сили – стихійні лиха, теракти тощо. Експоненціальну функцію відбираємо для подальшого експериментального дослідження.

Останнім часом розвинуті теорії негаусових процесів, які можуть бути кращими кандидатами для формалізації залежностей. Стаціонарні розподіли значень змінних, у своїй масі, є не гаусовими, тобто не можуть бути описані розподілом Гауса та іншими гаусовими розподілами, що підпорядковуються центральною граничною теоремою теорії ймовірностей. За великих значеннях змінної воно має гіперболічну форму розподілу Ципфа, а в логарифмічних координатах розподіл Ципфа має вид прямої лінії. Ципфовими називають всякі розподіли, які мають при великих значеннях змінної вид розподілу Ципфа [9].

Негаусовість є загальною властивістю просторових та непросторових фрактальних структур. Негаусовими є часові структури, які утворюються відносно рідкими подіями, необмеженими у часі. Події, обмежені у часі, навпаки, розподілені більш гаусово. Там, де не існує обмежень значень змінної, розподіл виявляється негаусовим. Негаусові розподіли є більш поширеними, ніж гаусові. Наведемо деякі теоретичні відомості [10].

«Кількісні шкали поділяють на відкриті та закриті у залежності від того, чи обмежені зверху відносно значення вимірюваної величини. У випадку обмежених шкал, згідно центральної граничної теореми Ляпунова, отримують гаусові (нормальні) розподіли. Обмеження може бути із-за процедури вимірювання, наприклад, при визначенні тестових балів. Гранична теорема Гнеденко – Дебліна визначає умови для наближення розподілу нормованих сум однакового розподілених незалежних випадкових величин до стійких негаусових розподілів. Статистичні стаціонарні розподіли, які отримані за допомогою відкритих (необмежених) шкал, здебільшого мають довгі хвости, що описуються розподілом Ципфа (Парето):

$$y_3(\alpha, x) = \frac{C}{x^{1+\alpha}}, 0 < x_0 \leq x \leq J, 0 < \alpha < \infty, \quad (3)$$

де $y_3(x)$ – частість; α – показник розподілу Ципфа, який визначає його форму: чим α менше, тим більш довгохвостий даний розподіл; C – параметр, який забезпечує нормування відносно обсягу вибірки; x_0 та J – мінімальне та максимальне вибіркове значення x . Значення параметра α , як правило, невеликі».

Для розподілу Ципфа характерно відсутність математичного очікування; m наближається до нескінченності. Критерієм гаусовості чи негаусовості цих розподілів служить зміна величини дисперсії. Якщо на даній генеральній сукупності дисперсія (та моменти вищих порядків) суттєво зростає з об'ємом вибірки, то таку сукупність називають негаусівською, у іншому випадку – гаусівською.

На основі теореми Гнеденко-Дебліна можна говорити, що ймовірнісні негаусові розподіли є ципфовими розподілами з $\alpha < 2$, тоді як ципфовий розподіл з $\alpha > 2$ є гаусовим. Використання ципфового розподілу для формалізації залежності між нормованою величиною збитків та рівнем захищеності доцільно по таким причинам. Ципфовий розподіл характеризується різким спадом (більш крутим ніж у експоненті) і довгим хвостом. Крутий спад відповідає реальним даним по величині збитків. Невеликий початковий приріст захищеності викликає знаний спад активності зловмисників. Авторами доведено, що лише об'ява про забезпеченість захисту об'єкта зменшує число зловмисників на 80% [8]. Відомості щодо наявності захисту відсікає значну частину законослухняних споживачів від спроб незаконного використання продукту.

Витрати на запобіжні заходи захисту від несанкціонованої зміни програмного коду. Аналогічним способом розглянемо застосування показникової та параболічної функції. Для формалізації залежності між нормованою величиною витрат на запобіжні заходи та рівнем захищеності може служити експонента

$$y_4(b, x) = \exp(b(x-1)), x = \overline{0,1}, \quad (4)$$

де b – параметр.

Ряд процесів у природі (радіоактивний розпад, зростання кількості бактерій за певний проміжок часу тощо) описуються експонентою. Функція (4) зручна для формалізації тому, що при $x=0$ вона: $y_4(b,0) > 0$. Рівень захищеності починає зростати при певних початкових витратах, коли задіяна певна мінімальна функціонально повна множина заходів захисту. Наприклад тоді, коли повністю змонтовані всі елементи огорожі об'єкта.

Другим кандидатом для формалізації залежності між нормованою величиною витрат на запобіжні заходи та рівнем захищеності може служити параболічна функція

$$y_5(b, x) = bx^2, x = \overline{0,1}, \quad (5)$$

де b – параметр.

Парабола представляє собою найпростішу нелінійну функцію і має широке застосування у різних сферах, зокрема, у синергетиці. Для остаточного вибору типових функцій розподілу витрат на безпеку необхідні статистичні дані щодо цих витрат. Що стосується вибору таких функцій стосовно до конкретних об'єктів інформаційної діяльності, то вони можуть мати вельми специфічний характер.

Математичні експерименти із розподілами

Виявлення причин нанесення втрат, прийняття попередніх запобіжних заходів захисту, заходи підвищення рівня захищеності інформаційної системи повинні переслідувати мету – з найменшими витратами досягти найбільших результатів. Має сенс дослідити, як виглядають оптимальні витрати на оптимальну систему захисту у випадку, коли розглянуті розподіли матимуть місце у реальності. Постановка задачі формулюється так. Треба побудувати у трьохмірному просторі залежність

$$Y(a, b) = \min (y_i(a, x) + y_j(b, x)) \quad (6)$$

Із цієї побудови можна судити про можливий мінімум витрат на інформаційну безпеку. Інтервали змін параметрів a і b підбираються експериментально.

На рис. 2 представлені результати математичного експерименту, відповідно, для функцій $y_2(a, x)$ та $y_4(b, x)$. По осі z відкладається значення функції (6), по осям a і b відкладені, відповідно, параметри функцій (2) і (4).

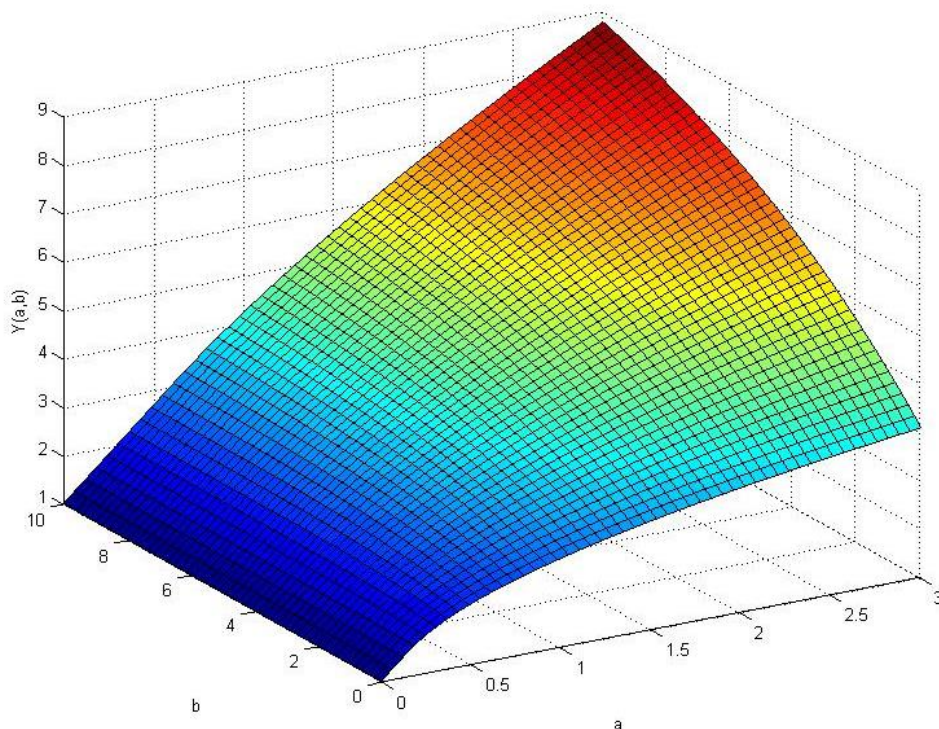


Рис.2. Розподіл оптимальних витрат на захист при експоненціальних функціях залежностей ризиків від витрат та затрат на захист

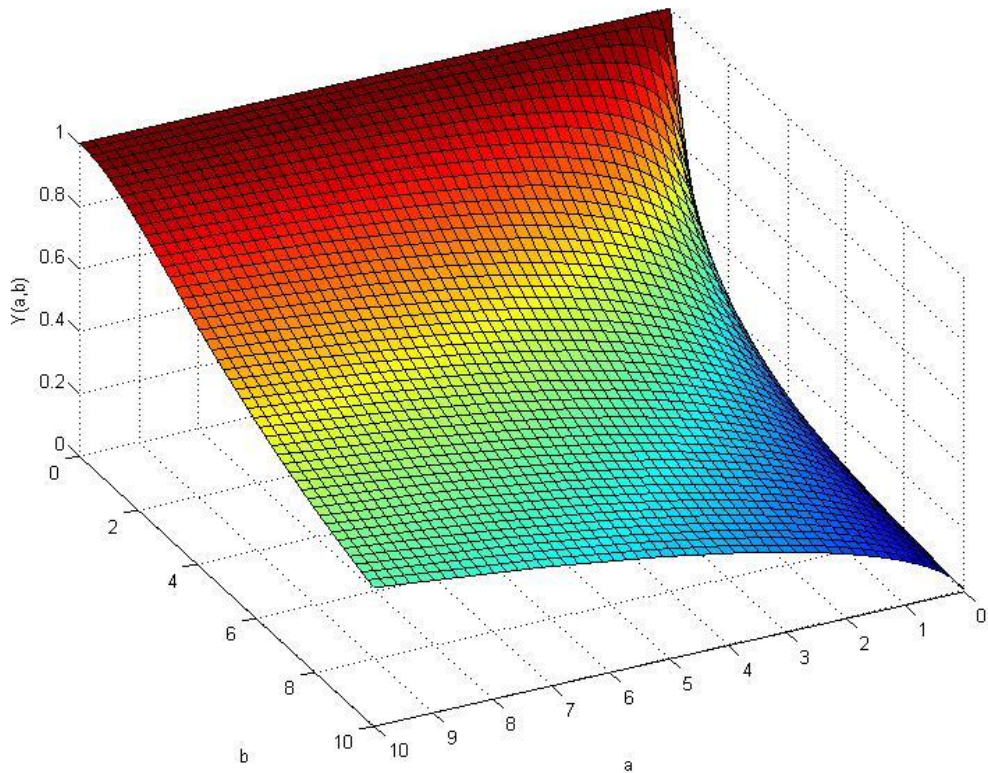


Рис. 3. Розподіл оптимальних витрат на захист при ципфових та експоненціальних функціях залежностей ризиків, відповідно, від витрат та затрат на захист

На рис. 3 представлені результати математичного експерименту, відповідно, для функцій $y_3(a, x)$ – ципфовий розподіл та $y_4(b, x)$ – експоненціальний розподіл. По осі z відкладається значення функції (6), по осям a і b відкладені, відповідно, параметри функцій (3) і (4).

Критерієм вибору функцій, придатних для формалізації залежності між нормованою величиною збитків (або витрат на систему захисту) та рівнем захищеності може служити наступний достовірний факт. Практикою доведено, що раціональна доля витрат на інформаційну безпеку можуть складати від 2% до 20% від обсягу продаж (або обороту). Більша доля витрат неефективна, бо знижує продуктивність основних виробничих функцій.

Висновки

В даній роботі розроблено стеганографічний, додатковий до алгоритмічних, механізм захисту програмного коду від несанкціонованих змін. Вдосконалена загальна модель оцінки ефективності системи захисту за принципом оптимізації витрат на захист. Проведена формалізація типових залежностей витрат на запобіжні заходи захисту та залежності витрат на відновлення втрат від рівня захищеності. Напрямок подальших досліджень повинні бути експериментальні дослідження статистики реальних витрат на інформаційну безпеку.

Список літератури

1. Казарин, О.В. Безопасность программного обеспечения компьютерных систем. Монография / О.В. Казарин. – М.: МГУЛ, 2003. – 212 с.
2. Скляр, Д.В. Искусство защиты и взлома информации / Д.В. Скляр. – СПб.: БХВ-Петербург, 2004. – 288 с. .
3. Десницкий, Д.А. Комбинированная защита программного обеспечения от несанкционированных воздействий / Д.А. Десницкий, И.В. Котенко // Изв. вузов. Приборостроение. – 2010. – Т.53. – №11. – С. 36-41.
4. Петров, А.С. Методы защиты программного кода / А.С. Петров, А.А. Петров // Системы обработки информации. – 2010. – № 3 (84). – С. 68-71.
5. Проскурин, В.Г. Защита программ и данных: уч. пособие / В.Г. Проскурин. – М.: Издательский центр «Академия», 2012. – 208 с.
6. Федоров, Д.Ю. Основы исследования безопасности программного обеспечения / Д.Ю. Федоров. – СПб.: СПГИЭУ, 2012. – 68 с.
7. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
8. Кононович, В.Г. Визначення ідентичності об'єктів у системі соціальної та інформаційної безпеки / В.Г. Кононович, І.В. Кононович, С.В. Стайкуца, О.О. Цвілій // Сучасний захист інформації. – 2015. – №1. – С. 19-27.
9. Яблонский, А.И. Математические модели в исследованиях науки / А. И. Яблонский. – М.: Наука, 1986. – 352 с.
10. Хайтун, С.Д. Феномен человека на фоне универсальной эволюции / С. Д. Хайтун. – М.: Книжный дом «ЛИБРОКОМ», 2009. – 536 с.

МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПРОГРАММНОГО КОДА ОТ НЕСАНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЙ

А.Е. Килин¹, В.Г. Кононович¹, И.В. Кононович², В.В. Беззубенко³

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

² Одесская национальная академия пищевых технологий,
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru

³ Одесская национальная академия связи,
ул. Кузнечная, 1, Одесса, 65021, Украина; e-mail:vladimirbezzubenko@gmail.com

В данной работе предлагается, дополнительно к существующим, механизм защиты программного кода от несанкционированного изменения та. На этом примере, усовершенствуется общая модель оценки эффективности системы защиты. Алгоритм защиты основан на стеганографических подходах. Оценка эффективности защиты проводится с помощью модели выбора оптимального уровня защищенности за принципом «затраты на защиту – эффективность». При этом формализуются типовые зависимости компенсации убытков от уровня защищенности и зависимости затрат на построение системы безопасности от того же уровня защищенности. Доказывается, что в общем случае целесообразно выбирать функцию Ципфа для зависимости компенсации убытков от уровня защищенности и экспоненциальную либо гиперболическую функцию для зависимости затрат на построение системы безопасности от того же уровня защищенности. Введение названных функций в модель выбора оптимального уровня защищенности позволила перейти от качественных оценок затрат на организацию системы безопасности к конкретным вычислениям при математическом экспериментировании. Усовершенствованная модель защиты и общей оценки эффективности системы защиты позволит обосновывать целесообразность повышения уровня защищенности программного кода.

Ключевые слова: защита программного кода, несанкционированные изменения, оценка эффективности, уровень защищенности, моделирование, математический эксперимент.

MODEL EVALUATION OF THE EFFECTIVENESS OF PROTECTION CODE FROM UNAUTHORIZED CHANGESA.E. Kilin¹, V.G. Kononovich¹, I.V. Kononovich², V.V. Bezzubenko³¹ Odessa National Polytechnic University

1, Shevchenko Ave, Odessa, 65044, Ukraine; e-mail: vl_kononovich@ukr.net

² Odessa National Academy Food Technologies

112, Kanatnaja str., Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

³ Odessa National Academy telecommunication,

1, Kuznechnaja str., Odessa, 65021, Ukraine; e-mail: vladimirbezzubenko@gmail.com

The additional mechanism of protection of programmatic code from the unauthorized change is offered in this work. The algorithm is based on steganographic techniques. Improving overall model of evaluation efficiency of the system protection. A model of choice of an optimum level of protection for the principle of "protection costs – efficiency." This formalized depending on the level of compensation for losses and security costs depending on the construction of the security system on the level of security. It proved the expediency of the function according to Cypf for compensation of losses from the level of protection and an exponential or hyperbolic function for the dependence of the cost of protection. Using these functions allowed to pass from qualitative assessments of the cost of protection to computing in mathematical experimentation. Advanced security model and an overall assessment of the effectiveness of the protection system allows you to substantiate the expediency of improving the security code.

Keywords: protection of software code, unauthorized modifications, performance evaluation, the level of security, modeling, mathematical experiment.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 5, номер 3, 2015. Одеса – 100 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 5, номер 3, 2015. Одесса – 100 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 5, No. 3, 2015. Odesa – 100 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №1 від 31.08.2015)

Адреса редакції: Одеський національний політехнічний університет,
проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: immm.ukraine@gmail.com

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

© Одеський національний політехнічний університет, 2015