

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 5, № 4

Volume 5, No. 4

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 - 6460P 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

ОСНОВИ НОВОГО ПІДХОДУ ДО ВИЯВЛЕННЯ РЕЗУЛЬТАТІВ КЛОНУВАННЯ В ЦИФРОВОМУ ЗОБРАЖЕННІ В УМОВАХ ЗБУРНИХ ДІЙ А.А. Кобозєва, С.М. Григоренко	303	BASICS OF A NEW APPROACH TO IDENTIFY CLONING RESULTS IN DIGITAL IMAGES IN DISTURBING INFLUENCES Kobozeva A., Grygorenko S.
СИСТЕМА АВТОМАТИЗОВАНОГО ПОШУКУ ГОЛОСІВ О.В. Рибальський, В.І. Соловійов, А.Н. Шабля, В.В. Журавель	312	AUTOMATED SYSTEM VOICE SEARCH Rybalskiy O., Solovyov V., Chablis A., Zhuravel V.
СТРУКТУРНІ ВЛАСТИВОСТІ ПРОРІДЖЕНИХ МАТРИЦЬ ЕКВІВАЛЕНТНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШТОК Н.І. Кушніренко, В.Я. Чечельницький	318	STRUCTURAL PROPERTIES OF THINNED MATRICES OF THE EQUIVALENCE CLASS PERFECT BINARY ARRAYS Kushnirenko N., Chechelnytskiy V.
МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ УМОВ УТВОРЕННЯ ФРАКТАЛЬНИХ СТРУКТУР ПРИ ВОДОНАПІРНОМУ РЕЖИМІ НАФТОДОБУТКУ С. А. Положаєнко, Мухіалдін Хасан Моха	325	MATHEMATICAL FORMALIZATION OF TERMS OF FORMATION OF FRACTAL STRUCTURES AT MODE OF PRESSURE OF WATER OF OIL PRODUCTION Polozhaenko S., Muhialdin Hassan Moha
СИНТЕЗ СИНЕРГЕТИЧНОГО УПРАВЛІННЯ ПОПИТОМ АГЕНТІВ НА КОНТЕНТ У СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ К.В. Молодецька	330	THE SYNTHESIS OF SINERGISTICAL MANAGEMENT OF AGENTS DEMAND ON CONTENT IN SOCIAL INTERNET SERVICES Molodetska K.
МОДЕЛІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІЗ ЗАПІЗНЮВАННЯМ РЕАГУВАННЯ НА ІНЦИДЕНТИ І.В. Кононович, Д.А. Маєвський, Р.С. Подобний	339	MODELS OF SYSTEM OF THE CIBERSECURITY PROVIDING WITH DELAY OF REACTION ON INCIDENTS Kononovich I., Mayevskiy D., Podobniy R.
ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ КРИПТОГРАФІЧНОГО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ О.В. Задерейко, О.В. Троянський	347	PROGRAM AND TECHNICAL ASPECTS OF CRYPTOGRAPHIC DEFENCE OF DATA STORAGE Zadereyko A., Troyanskiy A.

ОЦІНЮВАННЯ ПОКАЗНИКІВ
ПРИЗНАЧЕННЯ НЕЛІНІЙНИХ
РАДІОЛОКАТОРІВ
Ю.Ф. Зіньковський, М.І. Прокоф'єв

353 EVALUATION INDICATORS PURPOSE
NONLINEAR RADAR
Zinkovskiy Y., Prokofiev M.

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНО-
СИСТЕМНИХ ВЛАСТИВОСТЕЙ
ПРОЦЕСУ РЕАЛІЗАЦІЇ
ВИМІРЮВАНЬ ЗАДАНОЇ
НАДІЙНОСТІ
А.А. Березовський, В.С. Дмитренко

362 DESIGN OF INFORMATIVE-SYSTEM
PROPERTIES OF PROCESS OF
REALIZATION OF MEASUREMENTS OF
THE SET RELIABILITY
Berezovskiy A., Dmitrienko V.

УДОСКОНАЛЕННЯ
СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ,
ЗАСНОВАНОГО НА АНАЛІЗІ
ПРОСТОРОВОЇ ОБЛАСТІ ЦИФРОВИХ
КОНТЕЙНЕРІВ
Г.В. Ахмамет'єва

367 IMPROVEMENT OF THE
STEGANALYTIC METHOD, BASED
ON THE ANALYSIS OF THE SPATIAL
DOMAIN OF DIGITAL CONTAINERS
Akhmamet'ieva G.

ЕКСПЕРИМЕНТАЛЬНЕ
ДОСЛІДЖЕННЯ ПРОГРАМНОЇ
РЕАЛІЗАЦІЇ МЕТОДІВ
МОДУЛЯРНОГО
ЕКСПОНЕНЦІЮВАННЯ
М.М. Касянчук, І.З. Якименко,
Т.М. Долинюк, Н.А. Рендзеняк

376 EXPERIMENTAL STUDY OF
PROGRAM IMPLEMENTATION OF
METHODS OF MODULAR
EXPONENTIAL
Kasianchuk M., Yakymenko I.,
Dolynyuk T., Rendzenyak N.

СТІЙКЕ ПРЕЦИЗІЙНЕ
МОДЕЛЮВАННЯ ОПЕРАТОРА
ЗАПІЗНЕННЯ
О.А. Стопакевич, А.О. Стопакевич

383 PRECISION RACK DESIGN
OPERATOR DELAY
Stopakevych O., Stopakevych A.

ПРИСКОРЕНИЙ АЛГОРИТМ
ОДНОСТОРОННЬОГО ГАЛУЖЕННЯ
ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ
ЛІНІЙНОГО ПРОГРАМУВАННЯ З
БУЛЕВИМИ ЗМІННИМИ
Б.І. Юхименко

389 SINGLE ACCELERATE THE
ALGORITHM BRANCHES FOR
SOLVING LINEAR PROGRAMMING
PROBLEMS WITH BOOLEAN
VARIABLES
Ukhimenko B.

ОСНОВЫ НОВОГО ПОДХОДА К ВЫЯВЛЕНИЮ РЕЗУЛЬТАТОВ КЛОНИРОВАНИЯ В ЦИФРОВОМ ИЗОБРАЖЕНИИ В УСЛОВИЯХ ВОЗМУЩАЮЩИХ ВОЗДЕЙСТВИЙ

А.А. Кобозева, С.Н. Григоренко

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

В работе предложены основы нового подхода к выявлению результатов клонирования, проведенного в цифровом изображении, в условиях дополнительных возмущающих воздействий на изображение после клонирования, в качестве которых могут рассматриваться сжатие с потерями, наложение шума, размытие и т.д. Подход основан на выявлении сравнимости частей поверхности, которая ставится в соответствие анализируемому изображению, отвечающих клону и его прообразу. Поверхность определяется графиком интерполяционного сплайна, приближающего функцию изображения, при этом элементы матрицы изображения рассматриваются как узлы интерполяции. Обоснованно, что в качестве основной количественной характеристики такой сравнимости целесообразно использовать объем цилиндрического тела с образующей, параллельной оси OZ, ограниченного сверху соответствующей частью графика интерполирующей функции, снизу – плоскостью XOY.

Ключевые слова: цифровое изображение, клонирование, нарушение целостности, матрица цифрового изображения, интерполяционный сплайн, возмущающие воздействия.

Введение

Современный уровень развития информационных технологий привел к небывалой легкости осуществления неавторизованных модификаций цифровых контентов. Сегодня только ленивый не пробует свои силы в изменении, дополнении, «улучшении» имеющихся оригинальных фотографий, видеороликов при помощи таких широко распространенных программных сред, как Photoshop, Gimp и др. Однако эти модификации не всегда имеют безобидные, развлекательные цели. Высокопрофессиональные подделки, или результаты фальсификации, цифровых контентов могут привести к серьезным негативным последствиям как для отдельно взятых людей, так и для общества в целом, при использовании их в деле пропаганды, в виде вещественных доказательств в судебных разбирательствах, при создании «черного пиара» для «нежелательных» оппонентов и т.д. Все это приводит к необходимости проведения экспертизы целостности цифровых контентов для возможности их использования в целях, отличных от развлекательных.

Одним из наиболее широко и часто используемых способов изменения цифровых изображений (ЦИ), которые и рассматриваются далее в статье, является клонирование, реализованное во всех графических редакторах. При клонировании одна область изображения (прообраз) копируется и вставляется в другую область (клон) этого же изображения, заменяя собой его оригинальную часть. Такой способ фальсификации

часто используется в случае, когда с ЦИ убирается «ненужный» объект, либо изменяется взаимное расположение объектов.

Распространенность упомянутого способа нарушения целостности ЦИ привела к необходимости разработки эффективных методов выявления его результатов [1-4]. Однако, не смотря на то, что активность ученых в этой области велика, рассматриваемая задача не имеет окончательного удовлетворительного решения. Один из основных недостатков существующих методов связан со следующим. При проведении фальсификации ЦИ нарушитель для сокрытия факта клонирования с большой вероятности выполнит (незначительную) постобработку клона, прообраза (коррекция цвета, яркости и др.) или ЦИ в целом (например, размытие с малым радиусом, наложение шума и др.). Кроме того, учитывая нарастающий с каждым днем объем передаваемой, хранимой, обрабатываемой информации и связанную с этим необходимость сохранения информации в форматах с потерями, фальсифицированные ЦИ с большой вероятностью также будут сохранены с потерями. Эффективный метод выявления результатов клонирования должен работать в условиях перечисленных выше возмущающих воздействий, вносящих дополнительные (к клонированию) изменения в изображение. В настоящий момент существуют методы, работающие в условиях коррекции цвета, яркости области клона [5,6], размытия ЦИ [7], эффективность которых недопустимо снижается в случае, когда фальсифицированное ЦИ сохраняется в формате с потерями; инвариантность по отношению к формату сохранения измененного изображения декларируется в [2,3], однако эти методы оказываются бессильными в случае, когда область клонирования не содержит контуров, что часто имеет место на практике, когда, например, при помощи клонирования «скрывается» объект, присутствующий на оригинальном ЦИ; в открытой печати не было найдено разработок, эффективных в условиях нескольких возмущающих воздействий на ЦИ, осуществляемых после выполненного клонирования.

Все вышесказанное говорит об актуальности усовершенствования имеющихся, разработки новых методов и реализующих их алгоритмов для выявления результатов клонирования в ЦИ, подвергнутом дополнительным возмущениям после осуществления клонирования.

Цель статьи и постановка заданий

Целью работы является разработка основ нового подхода к решению задачи выявления (областей) нарушения целостности ЦИ, полученного путем клонирования, в условиях дополнительных к клонированию возмущающих воздействий на измененное ЦИ.

Под дополнительными возмущающими воздействиями далее будем понимать сохранение ЦИ в форматах с потерями, наложение различных шумов, размытие ЦИ, фильтрация и т.д. Предполагается, что область клонирования/прообраза не подвергается никакой постобработке отдельно от всего измененного ЦИ.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1. Установить качественную характеристику ЦИ, одинаковую/сравнимую для областей клона и его прообраза в условиях дополнительных возмущающих воздействий. Обеспечить нечувствительность этой характеристики к малым изменениям входных данных (фальсифицированного при помощи клонирования ЦИ);
2. Найти количественную оценку установленной при решении задачи 1 качественной характеристики клона/прообраза; обеспечить ее нечувствительность к возмущениям исходных данных.

Основная часть

Клонирование в ЦИ без последующей обработки области клона или в условиях его незначительной обработки приводит к смысловому, зрительному повторению некоторой части ЦИ – прообраза. Даже если изображение потом претерпело дополнительные возмущающие воздействия, сходство клона и его прообраза в целом в нашем восприятии остается. Необходимо отметить, что дополнительные изменения в уже фальсифицированное ЦИ, которые нарушитель будет вносить в него с целью замаскировать клонирование, не могут быть значительными, иначе такие изменения сами по себе привлекут внимание эксперта, что, очевидно, не входит в цели нарушителя [7]. Наша зрительная система, мозг, не смотря на то, что не в состоянии заметить различия яркостей в несколько градаций, изменения ширины линии контура на 1-2 пикселя, уловить незначительное понижение контрастности изображения, изменения, связанные с размытием ЦИ с малым радиусом и т.д., оказываются способными выловить сходство частей изображения, их идентичность даже в случае их неполного совпадения, анализируя ЦИ в целом, уделяя особое внимание тем его частям, которые по тем или иным причинам оказываются «под подозрением». Таким образом, при выявлении областей клонирования на ЦИ больший смысл имеет поиск не совпадающих (при постобработке ЦИ такой поиск будет безрезультатным), а мало отличающихся между собой областей. Характеристика ЦИ, используемая для этого, должна быть малочувствительной (нечувствительной) к малым изменениям изображения (к изменениям входных данных).

Не ограничивая общности рассуждений, для простоты изложения далее рассматриваются изображения в градациях серого.

Любое ЦИ является результатом дискретизации области определения $D \subset R^2$ и квантования значений некоторой функции двух переменных $f(x, y), (x, y) \in D$ [8] (при работе с ЦИ функция $f(x, y)$ в явном виде отсутствует), результатом чего служит $n \times m$ – матрица F с элементами $f_{ij} \in \{0, 1, \dots, 255\}, i = \overline{1, n}, j = \overline{1, m}$, а наглядным представлением может служить трехмерная поверхность, являющаяся графиком функции $g(x, y)$, приближающей $f(x, y)$ на множестве D с использованием элементов F , в частности, $g(x, y)$ может выступать интерполяционным сплайном, использующим элементы F как узлы интерполирования, что и предполагается ниже. Формально геометрическая структура, аналитические характеристики поверхностей, отвечающих изображениям, отличающимся незначительно (имеется ввиду значения яркости соответствующих пикселей), также будут мало отличаться друг от друга (сравните рис.1(б) с рис.1(в) и 1(г)), а вот части поверхности, соответствующие клону и его прообразу в отсутствии какой-либо постобработки окажутся идентичными (рис.1(б)). Действительно, если $g(x, y)$ - интерполяционный сплайн нулевой степени, то сделанный вывод о малых изменениях структуры поверхности, отвечающей ЦИ, при его малых изменениях является очевидным. Рассмотрим вариант, когда $g(x, y)$ - интерполяционный сплайн 1-ой степени. После дискретизации области D и квантования значений функции $f(x, y)$ элементы изображения – пиксели имеют целочисленные координаты $(x, y), x, y \in Z$, что приводит к тому, что координаты соседних пикселей могут отличаться лишь на 1 (рис.2).

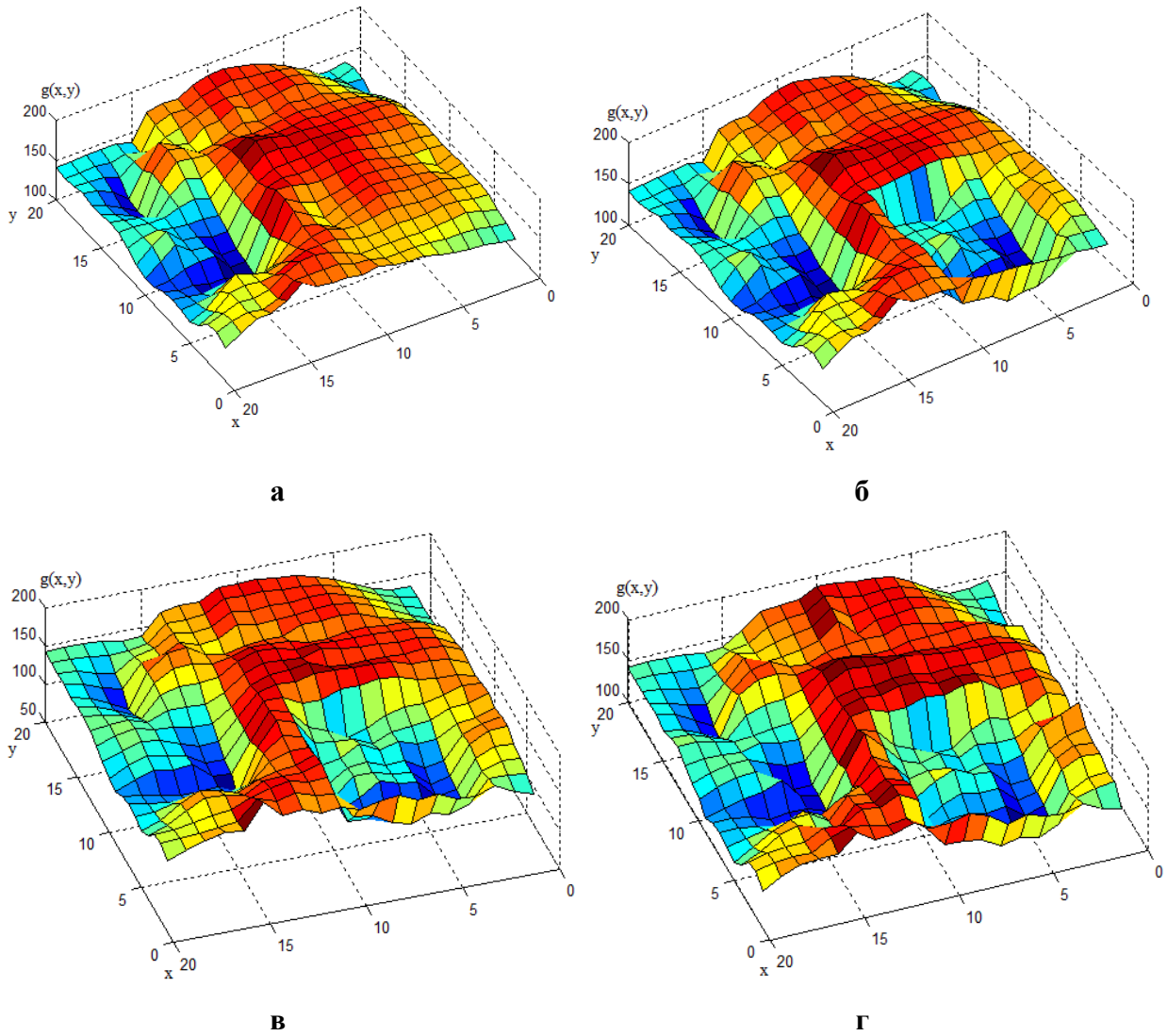


Рис. 1. Поверхности, отвечающие ЦИ: а – оригинальное ЦИ; б – ЦИ после клонирования и сохранения в формате без потерь (Tif); в - ЦИ после клонирования и сохранения в формате с потерями (Jpeg); г – ЦИ после клонирования с последующим наложением гауссовского шума с дисперсией 0.0001 и нулевым матожиданием и сохранением в Jpeg

Для определения коэффициентов уравнения плоскости $z = ax + by + c$, проходящей через три не лежащих на одной прямой соседних пикселя с координатами (x_1, y_1) , (x_2, y_2) , (x_3, y_3) и соответствующими значениями яркости z_1, z_2, z_3 необходимо решить систему линейных уравнений:

$$\begin{cases} ax_1 + by_1 + c = z_1, \\ ax_2 + by_2 + c = z_2, \\ ax_3 + by_3 + c = z_3 \end{cases} \quad (1)$$

с матрицей $A = \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix}$, являющейся хорошо обусловленной. Действительно,

$\det A = (x_2 - x_1)y_3 + (x_1 - x_3)y_2 + (x_3 - x_2)y_1$. Для соседних трех узлов интерполяции, не лежащих на одной прямой, совпадение значений абсцисс наблюдается для пары узлов.

Если для определенности, не ограничивая общности рассуждений, предположить, что $x_2 = x_1$, то $x_3 - x_2 = x_3 - x_1 = -(x_1 - x_3) \neq 0$, а $\det A = (x_1 - x_3)y_2 + (x_3 - x_2)y_1 = (x_1 - x_3)(y_2 - y_1) \neq 0$, поскольку, если $x_2 = x_1$, то обязательно $y_2 \neq y_1$. Более того, различие несовпадающих абсцисс/ординат по абсолютной величине здесь может быть равно только единице. Таким образом, $|\det A| = 1$, матрица системы далека от вырожденной, а потому является хорошо обусловленной [9], а значит система (1) является нечувствительной к изменениям исходных данных, т.е. при малых изменениях z_1, z_2, z_3 коэффициенты интерполирующей плоскости изменятся незначительно.

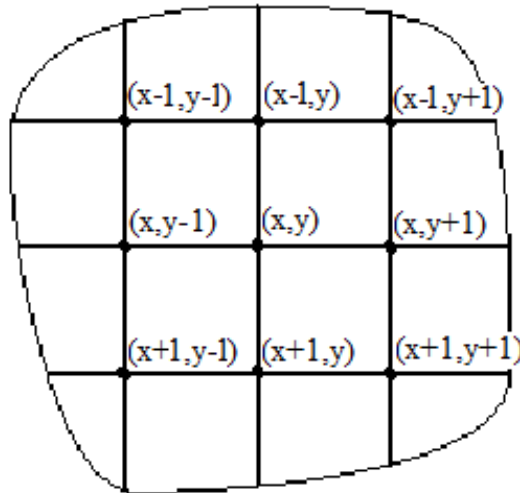


Рис. 2. Фрагмент области D после дискретизации с указанием соседей пикселя с пространственными координатами (x, y)

Рассмотрение интерполяционных сплайнов более высокой степени не является принципиальным для решения задачи, поставленной в настоящей работе, хотя с учетом имеющей место зависимости между координатами узлов-соседей, приведет к тем же результатам относительно чувствительности.

Таким образом, задача построения интерполяционного сплайна для функции, являющейся результатом дискретизации и квантования $f(x, y)$, является нечувствительной к изменениям входных данных – изменению значений яркости пикселей ЦИ. Но даже в случае нечувствительности малые изменения с $g(x, y)$ и соответствующей поверхностью конечно произойдут. Необходимо определить параметр, который бы характеризовал поверхность (часть поверхности) в целом и при этом был бы нечувствительным к малым изменениям характеристик поверхности (к изменениям входных данных). Одним из параметров, характеризующих поверхность в целом, является объем тела, ограниченного этой поверхностью (в случае ее замкнутости), либо цилиндрического тела с образующей, параллельной оси аппликат, ограниченного поверхностью (незамкнутой) и координатной плоскостью $ХОУ$. В нашем случае имеет место второй вариант, поскольку поверхность, отвечающая ЦИ, не может быть замкнутой. Вычисление объема тела V , отвечающего ЦИ, порождаемому функцией $f(x, y)$, $(x, y) \in D$, проведем в соответствии с формулой:

$$V = \iint_D g(x, y) dx dy, \quad (2)$$

где $g(x, y)$ - интерполяционный сплайн, построенный по узлам, являющимся элементами матрицы F . Как известно [9], задача численного интегрирования является нечувствительной к малым изменениям входных данных (изменению подинтегральной функции), что подтверждает целесообразность выбора параметра V для решения задачи, рассматриваемой в работе.

При помощи введенного объема можно характеризовать не только ЦИ в целом, но и его части. Если, например, $P \subset D$, $K \subset D$ - области прообраза и клона соответственно, то им также можно поставить в соответствие следующие интегралы: $V_P = \iint_P g(x, y) dx dy$, $V_K = \iint_K g(x, y) dx dy$. Если после клонирования область клона и прообраза не подвергалась никакой постобработке, то:

$$\iint_P g(x, y) dx dy = \iint_K g(x, y) dx dy, \quad (3)$$

если постобработка (как оговорено выше – незначительная) ЦИ имела место, то

$$\iint_P g(x, y) dx dy \approx \iint_K g(x, y) dx dy. \quad (4)$$

Для численного вычисления двойных интегралов (2)-(4), которые существуют в силу непрерывности на области интегрирования подинтегральной функции $g(x, y)$, в качестве составной квадратурной формулы рассмотрим соответствующие интегральные суммы, отвечающие разбиению области интегрирования в соответствии с рис.3: частичная область, полученная в результате разбиения произвольной $L \subset D$, представляет из себя квадрат, в центре которого находится соответствующий пиксель. Не ограничивая общности рассуждений, в соответствии с [8], где координаты рядом стоящих пикселей отличаются максимально на единицу (рис.2), может считать, что длина стороны каждого квадрата, а потому и его площадь S_{ij} равны 1. Тогда:

$$\iint_L g(x, y) dx dy \approx \sum_{(i, j) \in L} g(i, j) S_{ij} = \sum_{(i, j) \in L} g(i, j). \quad (5)$$

В формуле (5) намеренно используются $(i, j) \in L$ для обозначения местоположения соответствующего пикселя в пределах области L , чтобы подчеркнуть целые значения координат и связь с индексами элементов матрицы F . Формула (5) представляет из себя составную квадратурную формулу для вычисления интегралов в (2)-(4). Необходимо отметить, что для (5) не имеет значения степень интерполяционного сплайна $g(x, y)$, используемого при приближении $f(x, y)$.

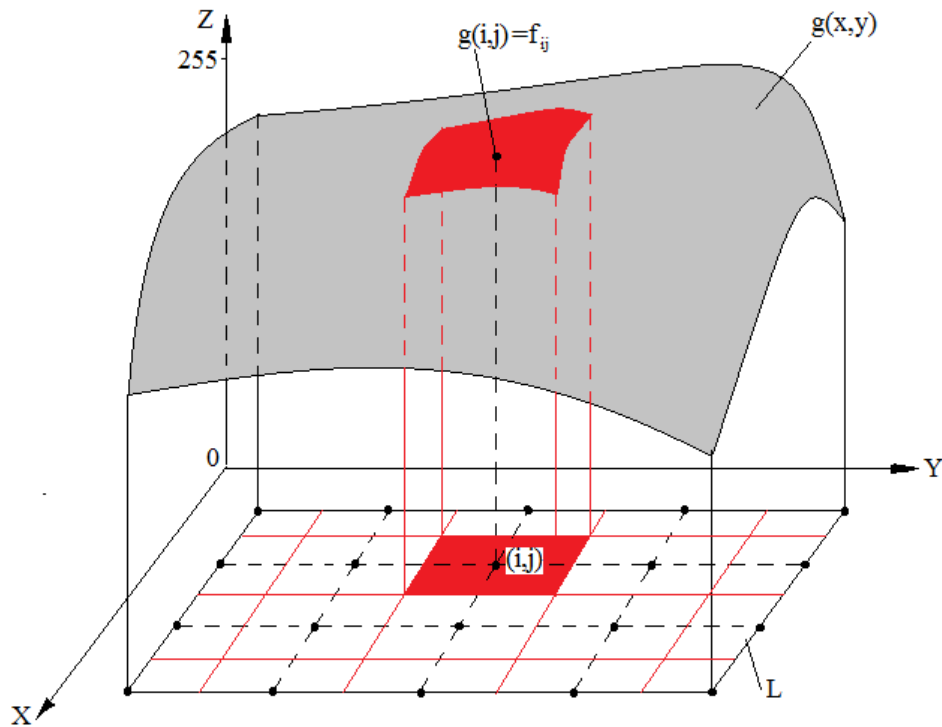


Рис. 3. Построение составной квадратурной формулы для вычисления интегралов (2)-(4)

На практике, с учетом того, что используемые в (5) значения $g(x,y)$ в узлах интерполирования $(x,y) = (i,j)$ совпадают со значениями соответствующих элементов матрицы F , получаем, что

$$\iint_L g(x,y) dx dy \approx \sum_{(i,j) \in L} f_{ij}. \quad (6)$$

Таким образом, как следует из (6) для областей клона и его прообраза должно выполняться соотношение:

$$\sum_{(i,j) \in K} f_{ij} \approx \sum_{(i,j) \in P} f_{ij}. \quad (7)$$

Соотношение (7) является основой для организации поиска клонированных областей и их прообразов в ЦИ, претерпевшем возмущения после проведения клонирования.

Для разработки соответствующего метода необходимо определить степень возможного количественного отличия $\sum_{(i,j) \in K} f_{ij}$ от $\sum_{(i,j) \in P} f_{ij}$ при различных возмущающих воздействиях, которые могут иметь место при постобработке измененного ЦИ, кроме того, с учетом геометрической схожести частей поверхности, которая ставится в соответствие ЦИ, отвечающих клону и прообразу, в качестве дополнительных количественных характеристик можно задействовать значения локальных экстремумов, глобальных минимума и максимума, направлений векторов градиента в характерных точках функции $g(x,y)$ и т.д.

Выводы

В работе предложены основы нового подхода к выявлению результатов клонирования, проведенного в ЦИ, в условиях возможных дополнительных возмущающих воздействий на изображение после клонирования. Основной идеей подхода является фиксация имеющей место визуальной схожести областей клона и прообраза даже в случае наличия дополнительных возмущений изображения. Подход основан на выявлении геометрической сравнимости частей поверхности, которая ставится в соответствие анализируемому ЦИ, отвечающих клону и его прообразу. Показано, что для поверхности, являющейся графиком функции $g(x, y)$, приближающей функцию изображения $f(x, y)$, в случае, когда $g(x, y)$ является интерполяционным сплайном, использующим в качестве узлов интерполирования результат дискретизации и квантования $f(x, y)$, задача нахождения такой поверхности является нечувствительной к малым изменениям значений яркости пикселей ЦИ. Нечувствительным к малым возмущениям $g(x, y)$ также является задача вычисления двойного интеграла от упомянутой функции по соответствующей области, значение которого и рассматривается как основная количественная характеристика поведения $g(x, y)$ в условиях рассматриваемой задачи.

Сравнимость частей поверхности, отвечающих клону и его прообразу, устанавливается путем выявления малого отличия сумм значений яркостей пикселей, принадлежащих соответствующим областям.

Список литературы

1. Лебедева, Е.Ю. Метод локализации и идентификации оригинальной и клонированной областей изображения / Е.Ю. Лебедева // Информатика та математичні методи в моделюванні. — 2014. — Том 4. — №1. — С. 76 – 84.
2. Huang, H. Detection of copy-move forgery in digital images using SIFT algorithm / H. Huang, W.Guo, Y. Zhang // IEEE Pacific-Asia Workshop on Computational Intell. and Industrial Application. — 2008. — Vol.2. — P. 272-276.
3. Pooja, S. Detecting Region Duplication Forgery in Digital Image using SIFT Features / S.Pooja, S.Kotkar, S. Shriramwar // International Journal of Current Engineering and Technology. — 2014. — Vol.4. — №3. — P.1437-1440.
4. Pan, X. Region duplication detection using image feature matching / X. Pan, S. Lyu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol.5. — №4. — P. 857–867.
5. Кобозева, А.А. Основы метода выявления клонированных участков изображения, подвергнутых коррекции яркости / А.А. Кобозева, Е.Ю. Лебедева // Сучасна спеціальна техніка. — 2013. — №3. — С.17 – 24.
6. Кобозева, А.А. Основы метода выявления клонированных участков изображения, подвергнутых коррекции цвета / А.А. Кобозева, Е.Ю. Лебедева // Збірник наукових праць Військового інституту КНУ ім.Т.Шевченка. — 2013. - №44. — С.96-102.
7. Зорило, В.В. Метод выявления результатов размытия цифрового изображения / В.В.Зорило, А.А.Кобозева // Сучасна спеціальна техніка. — 2010. - №3(22). — С.72-82\
8. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.
9. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студ. физико-математических спец. вузов; Рекомендовано МО РФ / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 6-е изд. — М. : БИНОМ. Лаборатория знаний, 2008. — 636 с.

ОСНОВИ НОВОГО ПІДХОДУ ДО ВИЯВЛЕННЯ РЕЗУЛЬТАТІВ КЛОНУВАННЯ В ЦИФРОВОМУ ЗОБРАЖЕННІ В УМОВАХ ЗБУРНИХ ДІЙ

А.А. Кобозєва, С.М. Григоренко

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

У роботі запропоновані основи нового підходу до виявлення результатів клонування, проведеного в цифровому зображенні, в умовах додаткових збурних дій на зображення після клонування, у якості яких можуть розглядатися стиск із втратами, накладання шуму, розмиття й т.д. Підхід заснований на виявленні порівнянності частин поверхні, що ставиться у відповідність аналізованому зображенню, які відповідають клону і його прообразу. Поверхня визначається графіком інтерполяційного сплайна, що наближає функцію зображення, при цьому елементи матриці зображення розглядаються як вузли інтерполяції. Обґрунтовано, що у якості основної кількісної характеристики такої порівнянності доцільно використовувати об'єм циліндричного тіла з твірною, паралельною осі OZ, обмеженого зверху відповідною частиною графіка інтерполяційної функції, знизу - площиною XOY.

Ключові слова: цифрове зображення, клонування, порушення цілісності, матриця цифрового зображення, інтерполяційний сплайн, збурні дії.

BASICS OF A NEW APPROACH TO IDENTIFY CLONING RESULTS IN DIGITAL IMAGES IN DISTURBING INFLUENCES

A.A. Kobozeva, S.N. Grygorenko

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

In this paper it is proposed basics of a new approach to identify cloning results, conducted in digital images, in additional disturbing influences conditions in a digital image after cloning, that may be considered as lossy compression, add noise, blur, etc. The approach is based on identifying the comparability of the surface parts, which is put into correspondence the analyzed image appropriate clones and its preimage. The surface is determined by the graph of the interpolation spline, approaching the function of the image, and the elements of the image are regarded as the interpolation nodes. It is proved that as the main quantitative characteristics of such comparability is advisable to use the volume of a cylindrical body with generator parallel to the axis OZ, bounded from above corresponding part of the interpolation function graph, bounded below - plane XOY.

Keywords: digital image, cloning, violating the integrity, digital image matrix interpolation spline, disturbing influences.

СИСТЕМА АВТОМАТИЗИРОВАННОГО ПОИСКА ГОЛОСОВ

О.В. Рыбальский¹, В.И. Соловьев², А.Н. Шабля³, В.В. Журавель⁴

¹Национальная академия внутренних дел,

пл. Соломянская, 1, Киев, 03056, Украина; e-mail: rybalsky_ol@mail.ru

²Национальный университет им. В. Даля,

ул. Советская, 51, Северодонецк, 93400, Украина; e-mail: mettilyd@mail.ru

³Одесский научно-исследовательский институт судебных экспертиз МЮ Украины,

ул. Ланжероновская, 21, Одесса, 65044, Украина; e-mail: alik.shablya@gmail.cjm

⁴Государственный научно-исследовательский экспертно-криминалистический центр МВД Украины,

ул. Б. Окружная, 4а, Киев, 03056, Украина; e-mail: fonoscopia@ukr.net

Рассмотрен отдельный вид экспертных материалов цифровой звукозаписи - фонограммы, содержащие сообщения, поступающие в дежурные части ОВД Украины, среди которых могут быть ложные. Для указанных экспертных материалов решаются задачи идентификации по параметрам сигналов речи личности, подозреваемой в предоставлении ложного сообщения, в случае ее задержания или наличия образцов ее голоса, полученных оперативным путем, а также выявления в базе данных голосов фигурантов с близкими параметрами сигналов устной речи для установления потенциальных подозреваемых в предоставлении ложной информации, для чего разработана автоматизированная система быстрого поиска подозреваемых.

Ключевые слова: база данных, голос, идентификация, фигурант, цифровая фонограмма

Вступление

Материалы звукозаписи составляют значительную часть доказательств, используемых при расследовании и рассмотрении в суде дел, связанных с коррупцией, взяточничеством, вымогательством, рэкетом, похищениями людей и тому подобное [1-3].

Но существуют особенные цифровые фонограммы, содержащие сообщения, поступающие в дежурные части ОВД Украины. Они образуют отдельный вид экспертных материалов цифровой звукозаписи. Это объясняется тем, что при их экспертизе всегда используют цифровую копию фонограммы и не проводят экспертизу оригинальности и подлинности фонограмм. Еще одна особенность таких фонограмм – малая длительность записываемых сообщений. Принимая во внимание, что в настоящее время значительную часть таких фонограмм составляют ложные сообщения относительно ожидаемых терактов, перед экспертными подразделениями МВД Украины предстала проблема помощи в розыске и следствии выявлением подозреваемых в таких правонарушениях экспертным путем.

Основными задачами такой экспертизы являются:

- идентификация по параметрам сигналов речи личности, подозреваемой в предоставлении ложного сообщения, в случае ее задержания или наличия образцов ее голоса, полученных оперативным путем;
- выявление в базе данных голосов фигурантов с близкими параметрами сигналов устной речи для установления потенциальных подозреваемых в предоставлении ложной информации.

Успешное решение этих задач может быть обеспечено соответствующими экспертными подразделениями Государственного научно-исследовательского экспертно-криминалистического центра (ГНИЭКЦ) МВД Украины. Для облегчения их выполнения требовалась разработка автоматизированной системы быстрого поиска подозреваемых в имеющейся базе голосов для последующей идентификации личности по физическим параметрам сигналов ее устной речи.

В настоящее время такая система разработана. Она была подвергнута испытаниям и предоставлена на апробацию в ГНИЭКЦ и Одесский НИИ судебных экспертиз.

Основная часть

В системе предусматривается автоматическое разделение голосов дежурного работника ОВД и заявителя. Такая функция во многих случаях исключает необходимость предыдущей подготовки экспертом записей, поступающих или уже зафиксированных в базе данных. Однако ее применение не обеспечивает гарантированного разделения голосов в фонограммах, записанных на одноканальной аппаратуре. Поэтому введение этой опции в программу не исключает необходимости технически и методически предусмотреть возможность проведения предыдущей подготовки записей, зафиксированных в базе данных. Такой подготовкой является разделение голосов экспертом, и такая опция также предусмотрена в программе.

Также следует отметить, что система является поисковой, поэтому результаты поиска отнюдь не тождественны идентификации личности по голосу, поскольку являются лишь результатом ранжирования по степени близости отдельных параметров голосовых сигналов. Также следует отметить, что сравнения физических параметров голосов всегда носят вероятностный характер, который определяется величиной вероятностей ошибок I и II рода. В системе использован метод ранжирования по величине ошибки I рода. Проведенные эксперименты с использованием первой версии программы AVATAR показали, что при поиске разных образцов голоса одного человека, записанного на разных фонограммах, величина вероятности ошибки I рода не превышает значения 0,08. Результаты поиска предоставляются в виде ранговой таблицы. В процессе ввода фонограмм в базу данных производится расчет параметров сигналов зафиксированных на них голосов.

Первоначально расчет параметров голосов и ранжирование проводилось только по частоте основного тона. Но при расчете ранговой таблицы весьма часто случалось так, что хотя на ее первой позиции размещалась фонограмма с записью голоса диктора, голос которого записан и на образцовой фонограмме, однако на последующих позициях находились фонограммы с голосами других дикторов. И это несмотря на то, что в базе было несколько фонограмм с записью голоса искомого диктора. Но при этом во всех экспериментах на первую позицию, как правило, приходился голос диктора, который записан и на образцовой фонограмме. Это квалифицировалось авторами, как существенный недостаток программы.

Была создана программа, использующая ранжирование не только по частоте основного тона, но по дополнительным признакам, имеющим индивидуальный характер. В результате отработки предлагаемого метода были отобраны три метода ранжирования по признакам, содержащимся в голосовых сигналах, пригодные для построения окончательного варианта системы. К ним относятся:

- вычисление близости кривых функций двумерной плотности вероятности для частоты основного тона и расположению в спектре семи формант, выделяемых из речи, зафиксированной на фонограмме;
- вычисление близости кривых функций плотности вероятности для каждого из этих признаков отдельно;

■ вычисление меры близости абсолютных максимумов спектров формант, выделяемых из речи, зафиксированной на фонограмме.

Особенностью разработанного метода является спектральный анализ фрагментов речи на малых временных интервалах (20-30 мс). Для этого используется вейвлет-преобразование, в частности, используется вейвлет Морле. Фрагменты речи сканируются вейвлетом Морле с минимально возможным смещением окна сканирования. Величина этого смещения обратна частоте дискретизации. В каждом временном окне вычисляется преобразование на основе вейвлета Морле. Определяется частота основного тона – F_b как корреляционная функция максимумов вейвлет преобразования в каждом окне. Важно отметить, что частота основного тона F_b определяется для каждого временного окна.

Таким образом, для фрагмента речи длительностью, например, 1 сек при частоте дискретизации 11025 Гц и размере окна анализа 20 мс, массив частот основного тона составляет величину порядка десять тысяч отсчетов, что весьма существенно при статистических оценках.

Аналогично, в каждом временном окне рассчитывается и спектр. Особенностью применяемого метода расчета спектра является то, что расчет спектральных характеристик проводится с разрешающей способностью 1 Гц (неортогональные преобразования в малом временном окне, для чего использована теория каркасов [4]). В спектре каждого временного окна выделяются максимумы первых семи формант.

Для вычисления близости кривых функций двумерной плотности вероятности рассчитывается функция F_f – функция характеристик голоса. Эта функция является нелинейной эмпирической функцией зависимостей амплитуды и частоты максимумов формант.

Диапазон частот основного тона F_b разбивается на интервалы в диапазоне от 80 до 600 Гц. Аналогично на частотные интервалы в диапазоне от 80 до 2500 Гц разбиваются значения F_f .

Для всех фрагментов речи определяется двумерная плотность вероятностей по двум координатам – частоте основного тона F_b и функции характеристик голоса F_f (см. рис. 1). Таким образом, в основу системы заложен комбинированный метод оценки на основе частоты основного тона и спектральных характеристик. Степень близости двух характеристик голоса определяется абсолютными разностями между двумерными плотностями вероятностей.

Разумеется, что проекции двумерных плотностей вероятностей на каждую из одномерных осей координат дает распределение частоты основного тона F_b и распределение функции характеристик голоса F_f , которые также можно представить в виде отдельных зависимостей. Это позволяет произвести вычисление близости кривых функций плотности вероятности для каждого из этих признаков отдельно.

Точность оценки частоты основного тона в вариантах фрагментов речи с явно выраженными участками частоты основного тона определяется произведением $D_t \cdot F_t$, где D_t – период дискретизации речевого файла.

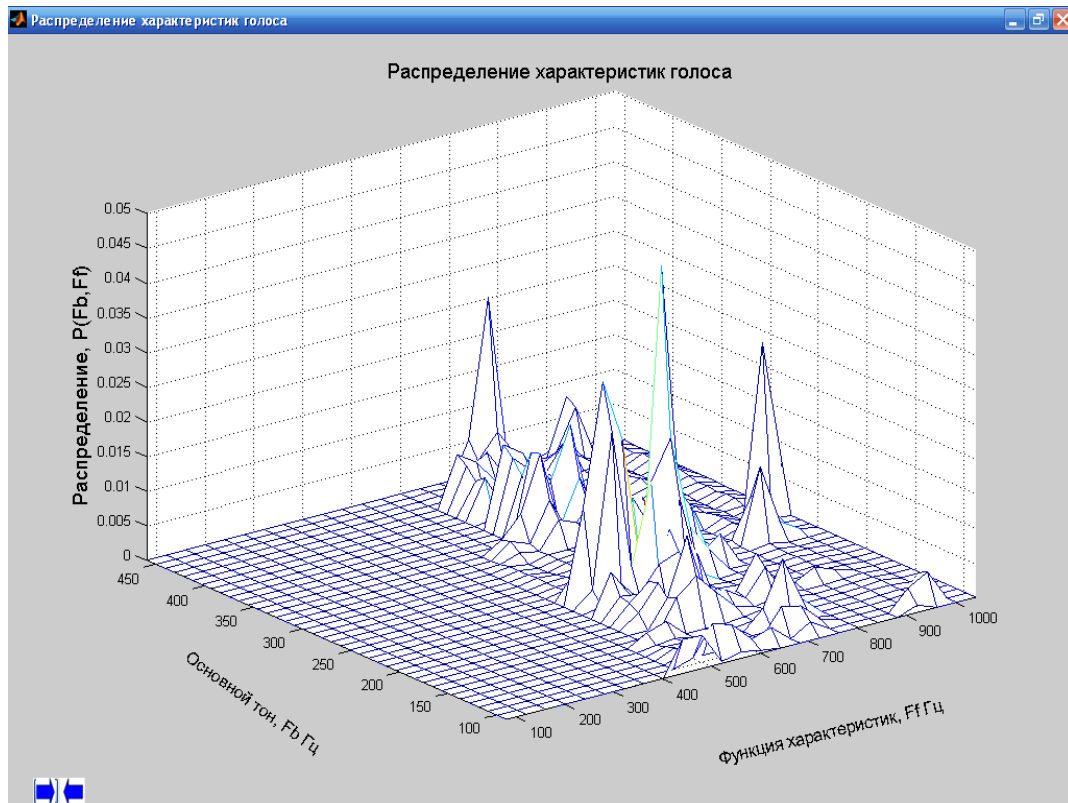


Рис. 1. Двумерная функция плотности вероятности характеристик голоса

Для ранжирования по плотностям распределения основного тона F_t и функциям характеристик голоса F_f в качестве меры близости используется величина, эквивалентная критерию согласия Колмогорова:

$$F_n(x) = \frac{1}{n} \sum_{i=1}^n IX_i \leq x, \quad (1)$$

где $IX_i \leq x$ показывает, попала ли величина X_i в область $(-\infty, x]$ при условии, что

$$IX_i \leq x = \begin{cases} 1, & X_i \leq x; \\ 0, & X_i > x; \end{cases} \quad (2)$$

Для вычисления меры близости абсолютных максимумов спектров формант, выделяемых из речи, зафиксированной на фонограмме, используется критерий

$$S_i = \text{abs}\{\max[P_1(x_1, x_2) - \max P_2(x_1, x_2)]\}, \quad (3)$$

где $P_1(x_1, x_2), P_2(x_1, x_2)$ – двумерные плотности вероятностей для двух разных записей с аргументами, как частоты основного тона, так и характеристик голоса, сравниваемых отдельно.

Результаты поиска голосов с близкими характеристиками представляются в виде ранговых таблиц. Пример таблицы для ранжирования по плотностям вероятностей основного тона F_t и функциям характеристик голоса F_f показан на рис. 2.

Следует отметить, что все вычисления характеристик голоса осуществляются для фрагментов записей, содержащих речевые сигналы. Разделение на паузы и фрагменты речи в системе осуществляется автоматически на основе двух критериев – уровня нормируемого аудиосигнала и наличия фрагмента записи, содержащего звуки речи. Система выделения звуков, является вспомогательной системой, встроенной в систему.

Она осуществляет общее разделение фрагментов, в которых присутствуют звуки речи, на основе специального метода, близкого к методологии скрытых марковских цепей и не является предметом рассмотрения данной статьи.

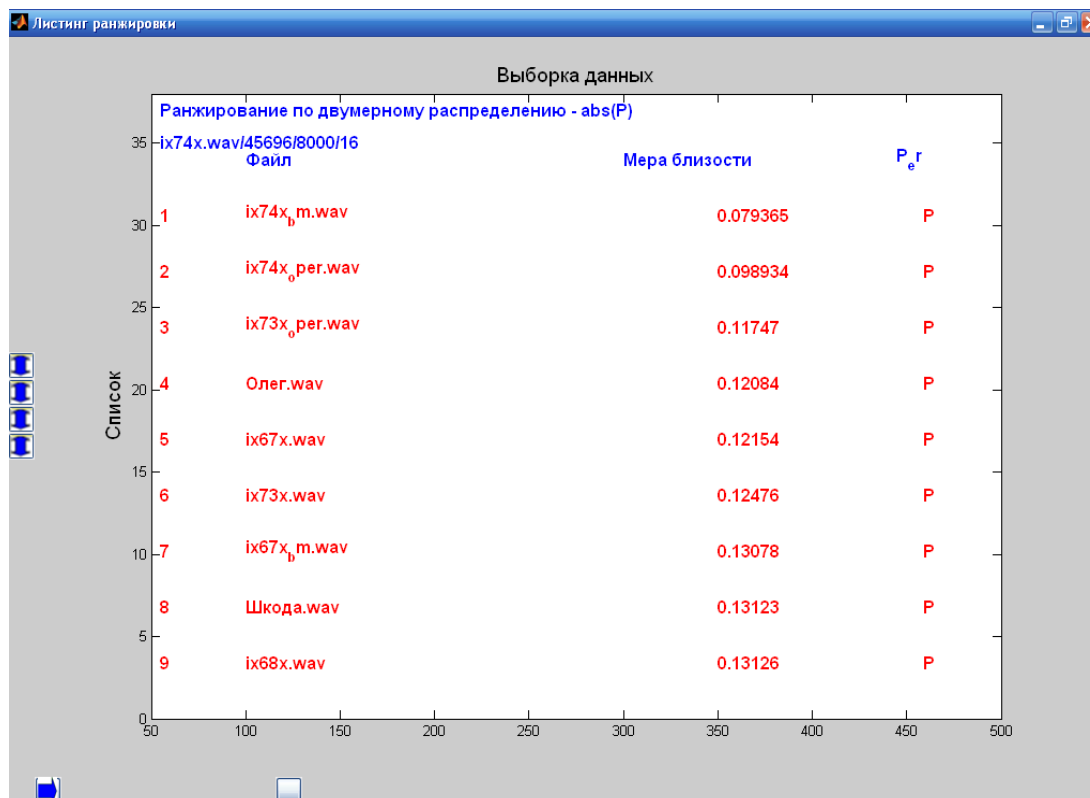


Рис. 2. Пример ранжирования характеристик голоса по двумерному распределению

Выводы

Создана система, обеспечивающая автоматический поиск по базе данных личностей с голосами, наиболее близкими к голосу фигуранта, записанного на образцовой фонограмме, что призвало повысить эффективность работы экспертных подразделений МВД Украины.

Список литературы

1. Кобозева, А.А. Матричный анализ - основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // Вісник Східноукраїнського національного університету ім. Володимира Даля. – 2008. – №8(126), ч.1. – С. 62-72.
2. Рыбальский, О.В. Комплексный подход к экспертизе подлинности материалов цифровой звукозаписи / О.В. Рыбальский, А.А. Кобозева, И.А. Струк, Е.А. Трифонова // Вісник Східноукраїнського національного університету ім. Володимира Даля. – 2009. – №6(136), ч.1. – С. 75-79.
3. Кобозева, А.А. Разработка общей теории выявления следов цифровой обработки сигналов и ее реализация аппаратно-программным комплексом «Теорема-М» / А.А. Кобозева, О.В. Рыбальский, В.И. Соловьев // Сучасна спеціальна техніка. – 2010. – №1(20). – С. 5-14.
4. Малла, С. Вэйвлеты в обработке сигналов: Пер. с англ. / С. Мала. – М.: Мир, 2005. – 671 с.

СИСТЕМА АВТОМАТИЗОВАНОГО ПОШУКУ ГОЛОСІВ

О.В. Рибальський¹, В.І. Соловйов², А.Н. Шабля³, В.В. Журавель⁴¹Національна академія внутрішніх справ,
пл. Солом'янська, 1, Київ, 03056, Україна; e-mail: rybalsky_ol@mail.ru²Національний університет ім. В. Даля,
вул. Радянська, 51, Сєвєродонецьк, 93400, Україна; e-mail: mettilyd@mail.ru³Одеський науково-дослідний інститут судових експертиз МЮ України,
вул. Ланжеронівська, 21, Одеса, 65044, Україна; e-mail: alik.shablya@gmail.cjm⁴Державний науково-дослідний експертно-криміналістичний центр МВС України,
вул. Б. Окружна, 4а, Київ, 03056, Україна; e-mail: fonoscopia@ukr.net

Розглянуто окремий вид експертних матеріалів цифрового звукозапису - фонограми, що містять повідомлення, які надходять в чергові частини ОВС України, серед яких можуть бути хибні. Для зазначених експертних матеріалів вирішуються задачі ідентифікації за параметрами сигналів мови особистості, підозрюваної у наданні неправдивого повідомлення, у разі її затримання або наявності зразків її голосу, отриманих оперативним шляхом, а також виявлення в базі даних голосів фігурантів з близькими параметрами сигналів усного мовлення для встановлення потенційних підозрюваних у наданні неправдивої інформації, для чого розроблена автоматизована система швидкого пошуку підозрюваних.

Ключові слова: база даних, голос, ідентифікація, фігурант, цифрова фонограма

AUTOMATED SYSTEM VOICE SEARCH

O.V. Rybalskiy¹, V.I. Solovyov², A.N. Chablis³, V.V. Zhuravel⁴¹National Academy of Internal Affairs,
1, Solomenskaya Sq., Kiev, 03056, Ukraine; e-mail: rybalsky_ol@mail.ru²National University. Dal,
51, Soviet st., Severodonetsk, 93400, Ukraine; e-mail: mettilyd@mail.ru³Odessa scientific research institute of forensic examinations Justice of Ukraine,
21, Lanzheronovskaya st., Odessa, 65044, Ukraine; e-mail: alik.shablya@gmail.cjm⁴State Research Forensic Center Interior Ministry of Ukraine,
4a, B. District st., Kiev, 03056, Ukraine; e-mail: fonoscopia@ukr.net

Is considered a separate type of digital audio expert materials - soundtrack containing messages received in the duty of MIA of Ukraine, among which may be false. For these expert materials solved the problem of identification of parameters of speech signals of the individual suspected of providing false messages in the event of detention or the availability of samples of its votes obtained by surgery and to identify the database votes defendants with similar parameters of signals of speech to determine potential suspected of providing false information, which developed the automated system of quick search of suspects.

Keywords: database, voice authentication, suspected, digital phonogram

STRUCTURAL PROPERTIES OF THINNED MATRICES OF THE EQUIVALENCE CLASS PERFECT BINARY ARRAYS

N.I. Kushnirenko, V.Y. Chechelnytskiy

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

The paper discusses the properties of perfect binary arrays and their thinned matrices when the cyclic shifts of rows and/or columns are performed. The relationship between the cyclic shifts parameters of generator array and its thinned matrices found, the location of thinned matrices when performing operation of interleaving revealed. The discovered properties of equivalence class thinned matrices will allow design of the cost-effective schemes of generators for perfect binary arrays of different orders. Such schemes can be used for cryptographic transmission of information, for broadband signals construction and other purposes.

Keywords: perfect binary array, thinned matrices, generator PBA, cyclic shift parameters, equivalence class PBA generator

Introduction

In recent years, a lot of domestic and foreign scientific papers are dedicated to the issues of Perfect Binary Arrays (PBA) application. Such structures are widely used to solve various problems of radio engineering, for example: synthesis of antenna aperture, perfect time-frequency codes design, new classes of block error-correcting codes design, new classes of orthogonal, biorthogonal and minimax noise-like signals with the multiloop cyclic shift property design, encryption tasks and so forth [1, 2]. However, the theory of the PBA requires further research. In particular, the task of an efficient PBA generator design, which takes into consideration structural properties of the PBA and their thinned matrices, must be solved.

The PBA is two-dimensional matrix of size $N \times N$ [2]

$$P(N) = \|p_{i,j}\|, \quad (1)$$

where $p_{i,j} \in \{+1, -1\}$ — elements of PBA;

$i = \overline{0, N-1}$ — numbers of rows of PBA;

$j = \overline{0, N-1}$ — numbers of columns of PBA;

which has an ideal two-dimensional periodic autocorrelation function (2D PACF)

$$R(N) = \|r_{m,n}\| = \begin{bmatrix} N^2 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}, \quad (2)$$

where $m = \overline{0, N-1}$ — numbers of 2D PACF rows;

$n = \overline{0, N-1}$ — numbers of 2D PACF columns.

Elements of 2D PACF (2) of P0BA are calculated using an equation

$$r_{m,n} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} p_{i,j} p_{i+m,j+n} = \begin{cases} N^2, & \text{when } m = n = 0; \\ 0, & \text{others } m \text{ and } n, \end{cases} \quad (3)$$

while values $i+m$ and $j+n$ are calculated modulo N .

An example of the PBA $P(4)$ size of 4×4 and its 2D PACF $R(4)$ respectively given below

$$P(4) = \begin{bmatrix} + & + & - & - \\ + & + & + & + \\ - & + & + & - \\ - & + & - & + \end{bmatrix}, \quad R(4) = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (4)$$

Here and further the elements of PBA «+1» and «-1» denoted as «+» and «-» respectively.

It is known the PBAs of order $N = 2^k$ and $N = 3 \cdot 2^k$, where $k = 1, 2, 3, 4, \dots, k$ — non-negative integer [3].

Research, given in this paper was performed within the Research work "Methods of informational security in broadband telecommunication systems", which is carried out by Information Security Department, Odessa National Polytechnic University.

The aim of the research

The research is devoted to the consideration of the properties of the equivalence class perfect binary arrays thinned matrices while the cyclic shifts of its rows and/or columns are performed. Such properties are able to simplify design of the equivalence class PBA generator.

The following problems must be solved to achieve this:

1. Evaluate the mutual properties of the PBAs and its thinned matrices while the cyclic shifts of their rows and/or columns are performed.
2. Determine the relationship between the cyclic shift parameters of generator PBA and the cyclic shift parameters of thinned matrices.
3. Determine the relationship between the cyclic shift parameters of generator PBA and the location of thinned matrices when interleaving is performed.

Main Body

It is known [1], that each PBA of arbitrary order N can be a generator (base) to build the equivalence class of PBAs — $E(N)$ -class. Such class can be obtained from a generator matrix by means of cyclic shifts of its rows and/or columns. Thus, if any arbitrary PBA is chosen as a generator, on its basis an $E(N)$ -class can be constructed and the power of it is given by

$$S_{E(N)} = N^2. \quad (5)$$

The union of all equivalence classes of PBA enables to construct a complete $U(N)$ -class of PBAs. The random selection of any PBA from each $E(N)$ -class as a base allows to construct the generator class of PBAs — $\Pi(N)$ -class, the power of which when $N = 2^k > 4$ is given by [3]

$$S_{\Pi(N)} = \begin{cases} 7^{(k-1)/2} \cdot 3^{(k-1)/2} \cdot 2^{2^{k+1}-2(k+1)}, & \text{если } k \text{ нечетное;} \\ 7^{(k-2)/2} \cdot 3^{k/2} \cdot 2^{2^{k+1}-2(k+1)}, & \text{если } k \text{ четное.} \end{cases} \quad (6)$$

The power of generator $\Pi(2)$ -class of PBAs is $S_{\Pi(2)} = 2$, the power of $\Pi(4)$ -class — $S_{\Pi(4)} = 12$.

Consider the next PBA as a generator

$$P_0(4) = \begin{bmatrix} - & + & - & - \\ + & + & + & - \\ - & + & - & - \\ - & - & - & + \end{bmatrix}, \quad (7)$$

where the subscript denotes its belonging to one of equivalence classes.

On the basis of given PBA (7) by means of cyclic shift of rows and/or columns operations the corresponding $E(4)$ -class (Table 1) was constructed.

Table 1.

Equivalence $E(4)$ -class of PBAs

	$k2 = 0$	$k2 = 1$	$k2 = 2$	$k2 = 3$
$k1 = 0$	$P_0^{[0,0]}(4) = \begin{bmatrix} - & + & - & - \\ + & + & + & - \\ - & + & - & - \\ - & - & - & + \end{bmatrix}$	$P_0^{[0,1]}(4) = \begin{bmatrix} + & - & - & - \\ + & + & - & + \\ + & - & - & - \\ - & - & + & - \end{bmatrix}$	$P_0^{[0,2]}(4) = \begin{bmatrix} - & - & - & + \\ + & - & + & + \\ - & - & - & + \\ - & + & - & - \end{bmatrix}$	$P_0^{[0,3]}(4) = \begin{bmatrix} - & - & + & - \\ - & + & + & + \\ - & - & + & - \\ + & - & - & - \end{bmatrix}$
$k1 = 1$	$P_0^{[1,0]}(4) = \begin{bmatrix} - & - & - & + \\ - & + & - & - \\ + & + & + & - \\ - & + & - & - \end{bmatrix}$	$P_0^{[1,1]}(4) = \begin{bmatrix} - & - & + & - \\ + & - & - & - \\ + & + & - & + \\ + & - & - & - \end{bmatrix}$	$P_0^{[1,2]}(4) = \begin{bmatrix} - & + & - & - \\ - & - & - & + \\ + & - & + & + \\ - & - & - & + \end{bmatrix}$	$P_0^{[1,3]}(4) = \begin{bmatrix} + & - & - & - \\ - & - & + & - \\ - & + & + & + \\ - & - & + & - \end{bmatrix}$
$k1 = 2$	$P_0^{[2,0]}(4) = \begin{bmatrix} - & + & - & - \\ - & - & - & + \\ - & + & - & - \\ + & + & + & - \end{bmatrix}$	$P_0^{[2,1]}(4) = \begin{bmatrix} + & - & - & - \\ - & - & + & - \\ + & - & - & - \\ + & + & - & + \end{bmatrix}$	$P_0^{[2,2]}(4) = \begin{bmatrix} - & - & - & + \\ - & + & - & - \\ - & - & - & + \\ + & - & + & + \end{bmatrix}$	$P_0^{[2,3]}(4) = \begin{bmatrix} - & - & + & - \\ + & - & - & - \\ - & - & + & - \\ - & + & + & + \end{bmatrix}$
$k1 = 3$	$P_0^{[3,0]}(4) = \begin{bmatrix} + & + & + & - \\ - & + & - & - \\ - & - & - & + \\ - & + & - & - \end{bmatrix}$	$P_0^{[3,1]}(4) = \begin{bmatrix} + & + & - & + \\ + & - & - & - \\ - & - & + & - \\ + & - & - & - \end{bmatrix}$	$P_0^{[3,2]}(4) = \begin{bmatrix} + & - & + & + \\ - & - & - & + \\ - & + & - & - \\ - & - & - & + \end{bmatrix}$	$P_0^{[3,3]}(4) = \begin{bmatrix} - & + & + & + \\ - & - & + & - \\ + & - & - & - \\ - & - & + & - \end{bmatrix}$

In Table 1 parameters $k1$ and $k2$ denote number of cyclic shifts of base PBA's rows down and number of cyclic shifts of columns to the left respectively. Let denote by $P_0^{[k1,k2]}(4)$ any PBA belonging to an equivalence $E(4)$ -class.

An arbitrary square PBA $P(N) = \|p_{i,j}\|$ of order N can be thinned in the spatial coordinates [4] in order to obtain four matrices

$$\left. \begin{aligned} A(N/2) &= \|a_{m,n}\|, \\ B(N/2) &= \|b_{m,n}\|, \\ C(N/2) &= \|c_{m,n}\|, \\ D(N/2) &= \|d_{m,n}\|, \end{aligned} \right\}, \quad m = \overline{0, N/2-1}, \quad n = \overline{0, N/2-1}. \quad (8)$$

Let call these structures the thinned matrices. The dimension of such matrices is $N/2 \times N/2$.

The elements of thinned matrices are calculated using the next equation

$$\left. \begin{aligned} a_{m,n} &= p_{2i,2j}, \\ b_{m,n} &= p_{2i,2j+1}, \\ c_{m,n} &= p_{2i+1,2j}, \\ d_{m,n} &= p_{2i+1,2j+1} \end{aligned} \right\}, \quad \left. \begin{aligned} i &= \overline{0, N/2-1}, \quad m = \overline{0, N/2-1}, \\ j &= \overline{0, N/2-1}, \quad n = \overline{0, N/2-1} \end{aligned} \right\}, \quad (9)$$

where i — number of PBA's row;

j — number of PBA's column;

m — number of thinned matrix row;

n — number of thinned matrix column.

Consider an operation of thinning in spatial coordinates and obtaining the thinned matrices $A(N/2)$, $B(N/2)$, $C(N/2)$, $D(N/2)$ on the example of PBA of order $N=4$. The elements of PBA are located as follows

$$P(4) = \begin{bmatrix} p_{0,0} & p_{0,1} & p_{0,2} & p_{0,3} \\ p_{1,0} & p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,0} & p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,0} & p_{3,1} & p_{3,2} & p_{3,3} \end{bmatrix}. \quad (10)$$

Operation of thinning PBA (10) in spatial coordinates leads to the construction of four thinned matrices, which constitute the PBA

$$A(N/2) = A(2) = \begin{bmatrix} p_{0,0} & p_{0,2} \\ p_{2,0} & p_{2,2} \end{bmatrix} = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix}, \quad (11)$$

$$B(N/2) = B(2) = \begin{bmatrix} p_{0,1} & p_{0,3} \\ p_{2,1} & p_{2,3} \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix}, \quad (12)$$

$$C(N/2) = C(2) = \begin{bmatrix} p_{1,0} & p_{1,2} \\ p_{3,0} & p_{3,2} \end{bmatrix} = \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix}, \quad (13)$$

$$D(N/2) = D(2) = \begin{bmatrix} p_{1,1} & p_{1,3} \\ p_{3,1} & p_{3,3} \end{bmatrix} = \begin{bmatrix} d_{0,0} & d_{0,1} \\ d_{1,0} & d_{1,1} \end{bmatrix}. \quad (14)$$

Opposite is also true. The square PBA $H(N) = \|h_{i,j}\|$ of order N can be constructed from four thinned matrices (11)–(14) of order $N/2$ by means of spatial interleaving of thinned matrices elements, which is an inverse of the thinning (9).

Equation to calculate elements of PBA using the thinned matrices $A(N/2)$, $B(N/2)$, $C(N/2)$, $D(N/2)$ is given below

$$\left. \begin{aligned} h_{2i,2j} &= a_{m,n}, \\ h_{2i,2j+1} &= b_{m,n}, \\ h_{2i+1,2j} &= c_{m,n}, \\ h_{2i+1,2j+1} &= d_{m,n} \end{aligned} \right\}, \quad \left. \begin{aligned} i &= \overline{0, N/2-1}, m = \overline{0, N/2-1}, \\ j &= \overline{0, N/2-1}, n = \overline{0, N/2-1} \end{aligned} \right\}. \quad (15)$$

While performing the operation of interleaving (15), the thinned matrices can be permuted. The number of these permutations is $4! = 24$. Thus, by means of permutations of four thinned matrices $A(N/2)$, $B(N/2)$, $C(N/2)$, $D(N/2)$ and the operation of interleaving, 24 PBAs can be constructed.

In this way, if for construction of PBA the permutation of thinned matrixes $A(N/2)B(N/2)C(N/2)D(N/2)$ is used, the elements of resulting PBA will be located as shown below

$$P(4) = \begin{bmatrix} a_{0,0} & b_{0,0} & a_{0,1} & b_{0,1} \\ c_{0,0} & d_{0,0} & c_{0,1} & d_{0,1} \\ a_{1,0} & b_{1,0} & a_{1,1} & b_{1,1} \\ c_{1,0} & d_{1,0} & c_{1,1} & d_{1,1} \end{bmatrix}.$$

If another permutation is used, e.g. $A(N/2)C(N/2)B(N/2)D(N/2)$, the elements of resulting PBA will be located as follows

$$P(4) = \begin{bmatrix} a_{0,0} & c_{0,0} & a_{0,1} & c_{0,1} \\ b_{0,0} & d_{0,0} & b_{0,1} & d_{0,1} \\ a_{1,0} & c_{1,0} & a_{1,1} & c_{1,1} \\ b_{1,0} & d_{1,0} & b_{1,1} & d_{1,1} \end{bmatrix}.$$

For example, for the PBA (7) the thinned matrices look as follows

$$A(N/2) = A(2) = \begin{bmatrix} - & - \\ - & - \end{bmatrix}, \quad (16)$$

$$B(N/2) = B(2) = \begin{bmatrix} + & - \\ + & - \end{bmatrix}, \quad (17)$$

$$C(N/2) = C(2) = \begin{bmatrix} + & + \\ - & - \end{bmatrix}, \quad (18)$$

$$D(N/2) = D(2) = \begin{bmatrix} + & - \\ - & + \end{bmatrix}. \quad (19)$$

Consider the relationship between the cyclic shift parameters k_1 and k_2 of generator PBA and the cyclic shift parameters of its thinned matrices. Then consider location of thinned matrices after the cyclic shifts of generator PBA will be performed.

Let parameters a_1, b_1, c_1, d_1 and a_2, b_2, c_2, d_2 denote the number of cyclic shifts of thinned matrices' $A(N/2)$, $B(N/2)$, $C(N/2)$, $D(N/2)$ rows down and columns to the left respectively.

For brevity the thinned matrices will be denoted by A, B, C , and D .

As follows from Table 1 and equation (9) and taking into account (16)–(19), the following combinations of thinned matrices can be obtained (Table 2).

Similar studies have been conducted to PBA of larger orders, in particular for $N = 6$ and $N = 8$ that can more clearly illustrate the results presented below.

Table 2.

E(4)-class of PBAs presented as combinations of thinned matrices

	$k_2 = 0$	$k_2 = 1$	$k_2 = 2$	$k_2 = 3$
$k_1 = 0$	$A^{[0,0]} B^{[0,0]} C^{[0,0]} D^{[0,0]}$	$B^{[0,0]} A^{[0,1]} D^{[0,0]} C^{[0,1]}$	$A^{[0,1]} B^{[0,1]} C^{[0,1]} D^{[0,1]}$	$B^{[0,1]} A^{[0,0]} D^{[0,1]} C^{[0,0]}$
$k_1 = 1$	$C^{[1,0]} D^{[1,0]} A^{[0,0]} B^{[0,0]}$	$D^{[1,0]} C^{[1,1]} B^{[0,0]} A^{[0,1]}$	$C^{[1,1]} D^{[1,1]} A^{[0,1]} B^{[0,1]}$	$D^{[1,1]} C^{[1,0]} B^{[0,1]} A^{[0,0]}$
$k_1 = 2$	$A^{[1,0]} B^{[1,0]} C^{[1,0]} D^{[1,0]}$	$B^{[1,0]} A^{[1,1]} D^{[1,0]} C^{[1,1]}$	$A^{[1,1]} B^{[1,1]} C^{[1,1]} D^{[1,1]}$	$B^{[1,0]} A^{[1,1]} D^{[1,0]} C^{[1,1]}$
$k_1 = 3$	$C^{[0,0]} D^{[0,0]} A^{[1,0]} B^{[1,0]}$	$D^{[0,0]} C^{[0,1]} B^{[1,0]} A^{[1,1]}$	$C^{[0,1]} D^{[0,1]} A^{[1,1]} B^{[1,1]}$	$D^{[0,1]} C^{[0,0]} B^{[1,1]} A^{[1,0]}$

As follows from Table 2, there exist only four possible combinations of thinned matrices A, B, C , and D with different number of their cyclic shifts of rows or/and columns, in particular

$$A^{[a_1, a_2]} B^{[b_1, b_2]} C^{[c_1, c_2]} D^{[d_1, d_2]}, \quad B^{[b_1, b_2]} A^{[a_1, a_2]} D^{[d_1, d_2]} C^{[c_1, c_2]},$$

$$C^{[c_1, c_2]} D^{[d_1, d_2]} A^{[a_1, a_2]} B^{[b_1, b_2]}, \quad D^{[d_1, d_2]} C^{[c_1, c_2]} B^{[b_1, b_2]} A^{[a_1, a_2]}.$$

Combinations of thinned matrices permutations depend on whether the cyclic shift parameters k_1 and k_2 of generator PBA are odd or even. The Table 3 illustrates such relationship.

Table 3.

 Combinations of thinned matrices depending on the parameters k_1 and k_2

k_1	k_2	Combinations of thinned matrices
even	even	$A^{[a1,a2]} B^{[b1,b2]} C^{[c1,c2]} D^{[d1,d2]}$
even	odd	$B^{[b1,b1]} A^{[a1,a2]} D^{[d1,d2]} C^{[c1,c2]}$
odd	even	$C^{[c1,c2]} D^{[d1,d2]} A^{[a1,a2]} B^{[b1,b2]}$
odd	odd	$D^{[d1,d2]} C^{[c1,c2]} B^{[b1,b2]} A^{[a1,a2]}$

In addition, there is a dependence of the cyclic shifts parameters of thinned matrices A , B , C , and D on parity of the cyclic shifts parameters k_1 and k_2 of generator PBA. Let consider such relationship in detail (Table 4)

Table 4.

The cyclic shifts parameters of thinned matrices

k_1, k_2	$a1, a2$	$b1, b2$	$c1, c2$	$d1, d2$
even	$k_1 / 2$	$k_1 / 2$	$k_1 / 2$	$k_1 / 2$
odd	$(k_1 + 1) / 2$	$(k_1 - 1) / 2$	$(k_1 + 1) / 2$	$(k_1 - 1) / 2$

For example, if following cyclic shifts parameters of PBA are given: $k_1=2, k_2=1$, then according to the Table 3 the cyclic shifts of rows and columns of generator PBA by k_1 and k_2 elements respectively lead to the structure $B^{[b1,b1]} A^{[a1,a2]} D^{[d1,d2]} C^{[c1,c2]}$. The cyclic shifts parameters of thinned matrices ($a1, a2$), ($b1, b2$), ($c1, c2$), ($d1, d2$) can be determined from Table 4. In this way, the following PBA is obtained

$$B^{[1,0]}(N/2) A^{[1,1]}(N/2) D^{[1,0]}(N/2) C^{[1,1]}(N/2),$$

that corresponds to the Table 2.

Conclusions

The properties of PBA and their thinned matrices while the cyclic shifts of rows and/or columns are performed are discussed. The relationship between the cyclic shifts parameters of generator PBA and the cyclic shifts parameters of thinned matrices discovered. Moreover, the relation between the cyclic shifts parameters of generator PBA and location of thinned matrices when performing operation of interleaving revealed.

The results obtained in this study can be utilized in the design of the equivalence class PBA generator which can be used for cryptographic transmission of information, for broadband signals construction and other purposes.

The equivalence class PBA generator can be constructed in various ways:

- store in memory all the PBA of equivalence class and use the switch to select the desired PBA, in this case it is possible to reach a minimum hardware complexity, but it requires a large amount of expensive memory elements;
- store generator PBA in memory and using shift registers obtain the necessary number of rows and then columns shifts; this method has a very low performance;
- use other known methods, each of which has a high hardware complexity or poor performance.

The results presented in this paper will allow the construction of equivalence class PBA generator with stored in memory thinned matrices. Such approach will drastically reduce the complexity of the cyclic shift device since the number of elements in matrices decreases four

times. Furthermore, such a device can be implemented on the basis of switches. It allows performing necessary number of cyclic shifts of rows and columns in one clock cycle. Thus, the discovered properties of thinned matrices of equivalence class will allow creating cost-effective schemes of generators for PBAs of different orders.

References

1. Мазурков, М.И. Классы эквивалентных и порождающих совершенных двоичных решеток для CDMA-технологий / М.И. Мазурков, В.Я. Чечельницкий // Радиоэлектроника (Изв. вузов). — 2003. — Т. 46. — № 5. — С. 54–63.
2. Kushnirenko, N.I. Digital modulation method based on perfect binary arrays / N.I. Kushnirenko, V.Ya. Chechelnytskyi // Труды Одесского политехнического университета. — 2014. — Вып. 1 (43). — С. 218–224.
3. Чечельницкий, В.Я. Метод построения порождающего класса совершенных двоичных решеток порядка $N=2^k$ / В.Я. Чечельницкий // Труды Одесского политехнического университета. — Спецвып. — 2006. — С. 84–92.
4. Чечельницкий, В.Я. Взаимосвязь прореженных матриц совершенных двоичных решеток порядка $N=2^k$ / В.Я. Чечельницкий // Труды Одесского политехнического университета. — 2007. — Вып. 1 (27). — С. 168–171.

СТРУКТУРНІ ВЛАСТИВОСТІ ПРОРІДЖЕНИХ МАТРИЦЬ ЕКВІВАЛЕНТНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШІТОК

Н.І. Кушніренко, В.Я. Чечельницький

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

У роботі розглянуті властивості досконалих двійкових решіток та їх проріджених матриць при виконанні операції циклічного зсуву рядків і/або стовпців. Знайдено взаємозв'язок між параметрами циклічних зсувів породжувальної решітки та її проріджених матриць, встановлено їх розташування при виконанні операції перемежування. Виявлені властивості проріджених матриць еквівалентного класу дозволять створити економічні схеми генераторів досконалих двійкових решіток різних порядків, які можна використовувати для криптографічної передачі інформації, для побудови різних широкосмугових сигналів та інших цілей.

Ключові слова: досконала двійкова решітка, проріджена матриця, породжувальна ДДР, параметри циклічного зсуву, генератор еквівалентного класу ДДР

СТРУКТУРНЫЕ СВОЙСТВА ПРОРЕЖЕННЫХ МАТРИЦ ЭКВИВАЛЕНТНОГО КЛАССА СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК

Н.И. Кушниренко, В.Я. Чечельницкий

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

В работе рассмотрены свойства совершенных двоичных решеток и их прореженных матриц при выполнении операции циклического сдвига строк и/или столбцов. Найдена взаимосвязь между параметрами циклических сдвигов порождающей решетки и ее прореженных матриц, установлено их расположение при выполнении операции перемежения. Обнаруженные свойства прореженных матриц эквивалентного класса позволят создать экономичные схемы генераторов совершенных двоичных решеток различных порядков, которые можно использовать для криптографической передачи информации, для построения различных широкополосных сигналов и других целей.

Ключевые слова: совершенная двоичная решетка, прореженная матрица, порождающая СДР, параметры циклического сдвига, генератор эквивалентного класса СДР

МАТЕМАТИЧЕСКАЯ ФОРМАЛИЗАЦИЯ УСЛОВИЙ ОБРАЗОВАНИЯ ФРАКТАЛЬНЫХ СТРУКТУР ПРИ ВОДОНАПОРНОМ РЕЖИМЕ НЕФТЕДОБЫЧИ

С. А. Положаенко, Мухиалдин Хассан Моха

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

Выполнен качественный анализ условий образования фрактальных структур фильтрационного потока при вытеснении нефти водой в режимах реальной нефтедобычи. Анализ позволил установить связь между фрактальной структурой фильтрационного потока и устойчивостью фронта вытеснения, что обуславливается скоростью продвижения последнего. Формализация динамики продвижения фронта вытеснения нефти водой при их взаимной фильтрации позволила получить выражение для критической скорости, определяющее область устойчивости фронта вытеснения и начало образования фрактальных структур в фильтрующей системе «нефть - вода».

Ключевые слова: фильтрационный поток, водонапорный режим нефтедобычи, фронт вытеснения, скорость продвижения фронта вытеснения, фрактальная структура.

Введение

В ряде работ последних лет, посвященных исследованию фильтрационных процессов жидкостей в пористых средах [1-5], обращено внимание на образование фрактальных структур фильтрационного потока (ФП) и их качественное влияние на характер процесса фильтрации. Это влияние, как установлено, может осуществляться за счет фрактальной структуры пористой среды [6] или гетерогенного поведения фильтрующей системы [7]. Вместе с тем показано [7], что гетерогенные жидкости, в частности, эмульсии, обладают динамической фрактальной структурой, которая определяется взаимодействием между частицами, что происходит со снижением концентрации дисперсной фазы.

Несмотря на имеющиеся значительные результаты в области определения фрактальных характеристик различных реологических процессов [8-11], остается нерешенным ряд важных теоретических и прикладных задач, связанных, в частности, с взаимной фильтрацией несмешивающихся жидкостей.

Целью работы является исследование условий образования фрактальных структур при вытеснении нефти водой (т.е. в условиях водонапорного режима нефтедобычи) и формализация при этом фронта вытеснения.

Основная часть

В настоящее время около 90% товарной нефти добывается с применением заводнения [12, 13], причем количество закачиваемой воды в пласт значительно превышает уровень добычи нефти [14, 15]. Тем не менее, средний уровень коэффициента нефтеотдачи не превышает (40...50)%, что предопределяет актуальность поиска новых воздействий на нефтяную залежь.

Техническим противоречием при заводнении нефтяного месторождения является то, что поддержание необходимых градиентов пластового давления требует закачки значительных объемов воды, а это, в свою очередь, приводит к нарушению *устойчивости фронта вытеснения* (ФВ) (т.е. фронта раздела фаз «нефть - вода») и раннему прорыву воды к добывающим скважинам. Последнее обстоятельство резко снижает коэффициент нефтедобычи и уровень рентабельности промысловых работ. Преодоление указанного противоречия возможно приданием процессу фильтрации гетерогенного характера, например, образование из несмешивающихся в ходе реологии фильтрующихся жидкостей (нефти и воды) *гетерогенной системы* за счет добавления в закачиваемую воду поверхностно-активных веществ (ПАВ), в частности, эмульсий и полимеров [16, 17]. Как показывают проведенные исследования устойчивости ФВ фаз «нефть - вода» в условиях ячейки Хелле-Шоу [18], добавление ПАВ к фильтрующимся жидкостям обуславливает образование фрактальной структуры флюида (водо-нефтяной системы) в виде «вязких пальцев» («viscous fingering») [19-21] и стабилизирует ФВ.

Анализ и обобщение имеющихся литературных данных экспериментальных исследований скоростей движения ФВ «ньютоновской» (вязкой) нефти водой [16, 17] позволяют прийти к следующему. Для фрактальных структур ФП при скорости v_ϕ последнего в диапазоне $v_\phi = (10^{-3} \dots 2 \times 10^{-3})$ м/с ФВ практически устойчив. При $v_\phi < 10^{-3}$ м/с и $v_\phi > 2 \times 10^{-3}$ м/с наблюдается значительное нарушение устойчивости ФВ. На основании проведенных обобщений построена зависимость «безводной» нефтеотдачи (отсутствует прорыв воды в добывающую скважину) от скорости движения ФВ. Очевидно, что «безводная» нефтеотдача характерна лишь для области устойчивости ФВ. Иными словами, желаемый режим разработки нефтяного месторождения, при котором достигается максимальная нефтеотдача, достигается в условиях устойчивости фронта раздела фаз «нефть - вода», что исключает прорыв воды в добывающую скважину. Указанная выше зависимость представлена на рис. 1 в виде функции «безводного» коэффициента вытеснения η_6 от скорости движения ФВ v_ϕ , т.е. $\eta_6 = f(v_\phi)$.

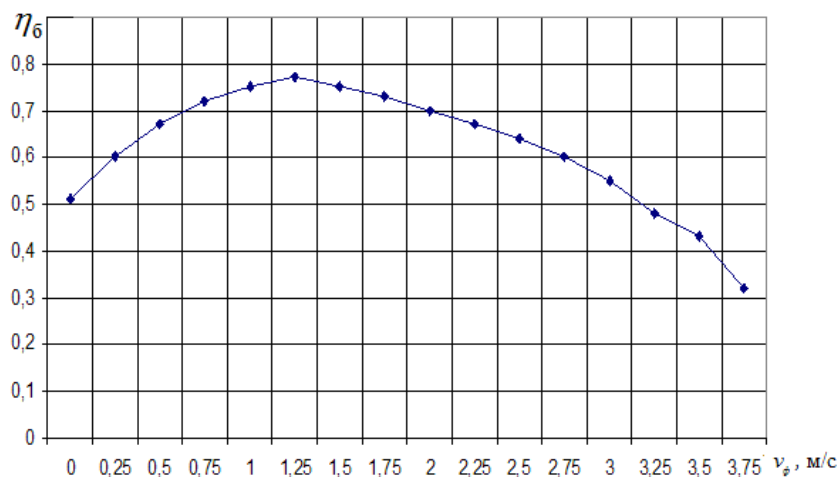


Рис. 1. Зависимость «безводного» коэффициента вытеснения η_6 от скорости v продвижения ФВ v

Выполним формализацию динамики продвижения ФВ нефти водой при их взаимной фильтрации в условиях образования фрактальных структур ФП. Качественные явления, определяющие динамику в данном случае, состоят в следующем. Молекулярно-поверхностные силы на границе раздела фаз «нефть - вода» действуют в направлении уменьшения площади поверхности потока (т.е. в направлении, обратном действию гидродинамических сил). Поэтому, когда молекулярно-поверхностные силы преобладают

над гидродинамическими силами, форма ФВ определяется радиусом кривизны с центром, расположенным в вытесняемой жидкости (нефти). Данное состояние соответствует участку $v_{\phi} < 10^{-3}$ м/с на рис. 1. Образование подобных структур объясняется [21] неоднородностью по размеру пор среды (толще пласта), в которой происходит фильтрационное движение. Вместе с тем, возникающая неустойчивость ФВ при этом может быть объяснена [16] доминированием возмущающего воздействия (градиента пластового давления, обусловленного закачиванием воды) над капиллярным давлением (капиллярными силами) в центре потока. В противном случае стабилизация (устойчивость) ФВ является следствием подавления возмущений поверхностным натяжением в зоне «отмыва» нефти водой. Когда поверхностные силы уравниваются гидродинамическими силами (возмущения в центре потока и у стенок капилляров имеют один порядок), ФВ становится практически устойчивым и имеет место картина, полученная в диапазоне скоростей $v_{\phi} = (10^{-3} \dots 2 \times 10^{-3})$ м/с.

В случае, если гидродинамические силы преобладают над поверхностными, максимальное значение скорости продвижения ФВ наблюдается в центре капилляра, а минимальная — на его стенках. Физически данная ситуация соответствует образованию «язычков» вытесняющей фазы (воды) в центре капилляра. На рис. 1 отражение указанного эффекта обусловлено резким падением «безводного» коэффициента вытеснения η_0 при скоростях продвижения ФВ $v_{\phi} > 2 \times 10^{-3}$ м/с.

Далее, будем считать, что молекулярно-поверхностные и гидродинамические силы уравновешены (т.е. скорость продвижения ФВ v_{ϕ} , определяемая градиентом пластового давления, равна скорости капиллярной пропитки $v_{\text{кл}}$). Поскольку скорость $v_{\text{кл}}$ определяется физико-химическими свойствами фильтрующихся жидкостей (их вязкостями и фракционным составом, в частности, для нефти), а также реологическими характеристиками среды (пористостью и проницаемостью), то для условий конкретного месторождения эта скорость практически неизменна. Исходя из этого, определим критическую скорость продвижения ФВ $v_{\phi 0}$, соответствующую предельному условию устойчивости фронтального вытеснения нефти водой, т.е. случаю $v_{\phi 0} = v_{\phi} = v_{\text{кл}}$.

Запишем для плоского капилляра закон Дарси (в форме Буссинеска [20]):

$$v = (b^2 \Delta P) / (12 \mu l), \quad (1)$$

где b и l — соответственно размеры поперечного сечения капилляра, ΔP — перепад (градиент) пластового давления, μ — вязкость вытесняющей фазы (воды); и уравнение Лапласа

$$\Delta P_k = 2 \sigma / b, \quad (2)$$

где ΔP_k — перепад капиллярного давления,

σ — поверхностное натяжение на границе раздела «стенка капилляра – фильтрующаяся жидкость».

Очевидно, что критическая скорость продвижения ФВ $v_{\phi 0}$ будет определяться условием $\Delta P = \Delta P_k$. Тогда, с учетом (1) и (2), получим

$$v_{\phi 0} = \sigma b / (6 \mu l). \quad (3)$$

Для реальных реологических условий нефтяных месторождений (например, пояса Гамбурцева [62]) величины, входящие в выражение (3), имеют следующие численные

значения параметров: $\sigma = 30 \times 10^{-3}$ Н/м, $b = 1,2 \times 10^{-4}$ м, $l = 0,24$ м, $\mu = 10^{-3}$ Па·с (вязкость воды). Их подстановка в (3) позволяет получить $v_{\phi 0} \approx 2,36 \times 10^{-3}$ м/с, что подтверждает проведенные рассуждения.

Скорость продвижения ФВ v_{ϕ} оказывает качественное влияние на фрактальные структуры «вязких пальцев», образующихся при неустойчивых ФВ. При вытеснении «легких» и «сверхлегких» нефтей (для которых плотность составляет $\rho \leq 800$ кг/м³) критическая скорость продвижения ФВ с учетом (3) будет соответствовать значениям $v_{\phi 0} < 10^{-3}$ м/с. Этому случаю, очевидно, будет соответствовать доминирующее развитие «вязкого пальца» вытесняемой жидкости (нефти), поскольку ее смачивающие свойства будут выше, чем у вытесняющей жидкости (воды). При вытеснении «тяжелых» нефтей (для которых плотность составляет $\rho > 900$ кг/м³) критическая скорость продвижения ФВ будет иметь значения $v_{\phi 0} > 2 \times 10^{-3}$ м/с, а фрактальные структуры будут практически зеркальным отражением первого случая: доминирующее развитие получит «вязкий палец» вытесняющей жидкости, т.к. скорость v_{ϕ} в центре фронта будет максимальной.

Вывод

Исследованы условия образования фрактальных структур при водонапорном режиме разработки нефтяных месторождений, которые обуславливают устойчивость фронта раздела фаз «нефть - вода». Получено выражение для критического значения скорости продвижения ФВ, позволяющее, в условиях реальных реологических характеристик месторождения, прогнозировать появление фрактальных структур типа «вязкий палец», а также качественно оценивать характерный вид последних.

Список литературы

1. Мандельбот, Б. Фрактальная геометрия природы / Б. Мандельбот. — М.-Ижевск: МКИ. — 2002. — 656 с.
2. Katz, A. J. Fractal Sandstone Pores: Implications between for Conductivity and Pore Formation / A.J. Katz, A.H. Thompson // Physical Review Letters. — 1985. — V. 54. — P. 1325 — 1332.
3. Динариев, О. Ю. Движение жидкостей и газов в пористых средах с фрактальной геометрией / О.Ю. Динариев // Известия РАН. Механика жидкостей и газа. — 1992. — № 5. — С. 101 — 109.
4. Мальшаков, А. В. Уравнения гидродинамики для пористых сред со структурой порового пространства, обладающей фрактальной геометрией / А.В. Мальшаков // Инженерно-физический журнал. — 1992. — Т. 62. — № 3. — С. 405 — 414.
5. Мейланов, Р. П. К теории фильтрации в пористых средах с фрактальной структурой / Р.П. Мейланов // Журнал технической физики. — 1996. — Т. 22. — Вып. 23. — С. 10 — 12.
6. Гийон, Э. Фракталы и перколяция в пористой среде / Э. Гийон, К.Д. Митеску, Ж.П. Юдлен, С. Ру // Успехи физических наук. — 1991. — Т. 161. — № 10. — С. 121 — 128
7. Зосимов, В. В. Динамическая фрактальная структура эмульсий, обусловленная движением и взаимодействием частиц. Численная модель / В.В. Зосимов // Журнал экспериментальной и теоретической физики. — 1997. — Т. 111. — Вып. 4. — С. 1314 — 1319.
8. Avnir, D. Chemistry in non integer dimensions between two and three. Fractal surfaces of adsorbents / D. Avnir, D. Farin, P. Pfeifer // The Journal of Chemical Physics. — 1983. — V. 7. — № 7. — P. 3566 — 3571.
9. Неймарк, А. В. Термодинамический метод расчета поверхностной фрактальной размерности / А.В. Неймарк // Журнал экспериментальной и теоретической физики. — 1990. — Т. 51. — Вып. 10. — С. 535 — 538.
10. Черкашинин, Г. Ю. Оценка фрактальной размерности дисперсных систем на основании уравнения, описывающего адсорбцию в микропорах / Г.Ю. Черкашинин, В.А. Дроздов // Журнал физической химии. — 1998. — Т. 72. — № 1. — С. 88 — 92.

11. Дункан, Г. Методы увеличения нефтеотдачи: практика проектирования, закачивания и эксплуатации скважин / Г. Дункан // Нефтегазовые технологии. — 1995. — № 2. — С. 11 — 16.
12. Suleimanov, B. A. Experimental Study of the Formation Structures During Oil Displacement / B. A. Suleimanov // Energy Sources. — 1995. — V. 17. — № 4. — P. 477— 483.
13. Азиз, Х. Математическое моделирование пластовых систем / Х. Азиз., Э. Сеттари.— М.: Недра, 1982. — 406 с.
14. Кричлоу Генри, Б. Современная разработка нефтяных месторождений - проблемы моделирования / Б. Кричлоу Генри. — М.: Недра, 1979.— 302с.
15. Сулейманов, Б. А. Экспериментальные исследования образования фрактальных структур при вытеснении несмешивающихся жидкостей на ячейке Хелле-Шоу / Б.А. Сулейманов // Инженерно-физический журнал. — 1996. — Т. 69. — № 2. — С. 229 — 236
16. Сулейманов, Б. А. Экспериментальные исследования образования фрактальных структур при вытеснении нефти / Б.А. Сулейманов // Азербайджанское нефтяное хозяйство. — 1993. — № 5. — С. 29 — 33.
17. Федер, Е. Фракталы / Е. Федер. — М.: Мир, 1991. — 254 с.
18. Котяхов, Ф. И. Основы физики нефтяного пласта / Ф.И. Котяхов. — М.: Энергия, 1996. — 364 с.
19. Мосолов, А. Б. Фрактальная гриффитова трещина / А.Б. Мосолов // Журнал технической физики. — 1991. — Т. 61. — Вып. 7. — С. 57 — 60.
20. Мосолов, А. Б. Фрактальный распад упругих полей при разрушении / А.Б. Мосолов // Журнал технической физики. — 1992. — Т. 62. — Вып. 6. — С. 23 — 32.
21. Кисленко, Б. Е. Об устойчивости водонефтяного контакта в однородной пористой среде / Б.Е. Кисленко // прикладная механика и техническая физика. — 1961. — № 6. — С. 194 — 195.

МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ УМОВ УТВОРЕННЯ ФРАКТАЛЬНИХ СТРУКТУР ПРИ ВОДОНАПІРНОМУ РЕЖИМІ НАФТОДОБУТКУ

С. А. Положаєнео, Мухіалдін Хасан Моха

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

Виконано якісний аналіз умов утворення фрактальних структур фільтраційного потоку при витісненні нафти водою в режимах реального нафтовидобудку. Аналіз дозволив встановити зв'язок між фрактальною структурою фільтраційного потоку та сталістю фронту витіснення, що зумовлено швидкістю просування останнього. Формалізація динаміки просування фронту витіснення нафти водою при їх взаємній фільтрації дозволила отримати вираз для критичної швидкості, що визначає область сталості фронту витіснення та початок утворення фрактальних структур у системі «нафта - вода», яка фільтрується.

Ключові слова: фільтраційний потік, водонапірний режим нафтодобутку, фронт витіснення, швидкість просування фронту витіснення, фрактальна структура.

MATHEMATICAL FORMALIZATION OF TERMS OF FORMATION OF FRACTAL STRUCTURES AT MODE OF PRESSURE OF WATER OF OIL PRODUCTION

S. A. Polozhaenko, Muhialdin Hassan Moha

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: polozhaenko@mail.ru

The high-quality analysis of terms of formation of fractal structures of filtration stream at ousting of oil by water in the modes of the real oil production is executed. The analysis allowed to set communication between the fractal structure of filtration stream and stability of front of ousting, that is determined by speed of advancement of the last. Did formalization of dynamics of advancement of front of ousting of oil by water during their mutual filtration allow to get expression for stalling speed, determining the region of stability of front of ousting and beginning of formation of fractal structures in the filtered system «oil - water».

Keywords: filtration stream, mode of pressure of water production, front of ousting, speed of advancement of front of ousting, fractal structure.

СИНТЕЗ СИНЕРГЕТИЧНОГО УПРАВЛІННЯ ПОПИТОМ АГЕНТІВ НА КОНТЕНТ У СОЦІАЛЬНИХ ІНТЕРНЕТ- СЕРВІСАХ

К.В. Молодецька

Житомирський національний агроєкологічний університет
вул. Старий бульвар, 7, Житомир, 10008, Україна; e-mail: kmolodetska@gmail.com

Соціальні інтернет-сервіси належать до класу нелінійних динамічних систем, тому явища соціальної комунікації характеризуються непрогнозованістю процесів взаємодії агентів внаслідок зовнішніх впливів і переходом системи в стан некерованого хаосу. Для досягнення системою стійкого стану як результату керованої самоорганізації агентів пропонується використати концепцію синергетичного управління взаємодією агентів у соціальних інтернет-сервісах. Синтезовано синергетичне управління взаємодією агентів у соціальних інтернет-сервісах, що дозволить підвищити стійкість віртуальних спільнот до деструктивних інформаційних впливів шляхом регуляризації попиту на контент. Наведено модельний приклад управління взаємодією агентів з метою синергетично керованого переходу віртуального співтовариства до заданого стану інформаційної безпеки.

Ключові слова: соціальний інтернет-сервіс, динамічний хаос, синергетичне управління, атрaktor, інформаційна безпека.

Вступ

Одним із основних сучасних засобів комунікації суспільства є соціальні інтернет-сервіси (СІС), які реалізують обмін інформацією, зберігання посилань і мультимедійних документів, створення та редагування публікацій тощо [1–5]. СІС застосовуються користувачами, яких називають агентами СІС, для реалізації особистісних і групових інтересів їх представників у віртуальному просторі. Сьогодні віртуальні спільноти і зокрема агенти СІС є об'єктами деструктивних інформаційних впливів з метою поширення контенту заданого змісту та впливу на суспільну думку [1–3]. В результаті у СІС виникають хаотично керовані вихідні дії агентів, а у випадку їх взаємного впливу і виконанні деяких визначених умов з'являються синергетичні ефекти [1, 3]. Такі ефекти породжують у високоорганізованих системах управління різного ієрархічного рівня нові і нехарактерні для СІС властивості, які називають емерджентними. Своєчасне встановлення сутності і змісту синергетичних ефектів у СІС, їх завчасне виявлення та прогнозування, є актуальною проблемою забезпечення інформаційної безпеки людини, суспільства та держави.

Аналіз останніх досліджень і публікацій

З динамічної теорії хаосу відомо, що задана поведінка системи досягається шляхом придушення в ній хаотичної динаміки нелінійних періодично збурюваних динамічних систем [5–8]. Класична задача управління динамічним хаосом у такому разі зводиться до вибору управляючого впливу, що стабілізує задану траєкторію в системі з

хаотичною поведінкою [6]. Такий вплив реалізується як періодичне збудження системи в розімкнутій формі – програмне управління, або у вигляді зворотного зв'язку за станом чи виходом. Недоліками таких управляючих впливів є привнесення в систему, що управляється, суттєвих змін в її динаміку в цілому і в саму систему зокрема.

Також при вивченні хаотично збуджуваних нелінійних динамічних систем встановлено, що задана поведінка в системі досягається за рахунок її самоорганізації, однією з необхідних умов виникнення якої є підтримання стану нерівноваги [6–8]. Завдяки процесам самоорганізації – теоретичній основі синергетики, можна виділити відносно невелику кількість параметрів порядку чи характеристик середовища, які визначають динаміку системи в цілому. Таким чином, наявність хаотичного атрактора забезпечує досягнення стійкого стану системи за незначних збурень системних параметрів.

В основу досліджень було покладено концепцію синергетичного управління процесами взаємодії агентів у СІС, що узагальнює відомі підходи до управління процесами взаємодії агентів та розвиває їх на клас нелінійних систем, які описуються на основі положень динамічної теорії хаосу [7, 8]. Вирішення проблеми синтезу синергетичного управління, що забезпечить виникнення процесів керованої самоорганізації агентів у СІС для досягнення заданого стану інформаційної безпеки віртуального співтовариства є актуальною.

Метою статті є підвищення стійкості віртуальних спільнот в СІС до деструктивних інформаційних впливів за рахунок синтезу синергетичного управління попитом агентів на відповідний контент.

Виклад матеріалу

Нехай у формалізованому вигляді взаємодія агентів у деякій СІС описується системою нелінійних диференціальних рівнянь вигляду [1]

$$\begin{cases} \frac{dx(t)}{dt} = ax - xy - bx^2; \\ \frac{dy(t)}{dt} = -cy + xy, \end{cases} \quad (1)$$

де $x(t)$ – процес, що описує попит агентів у СІС на відповідний контент для досліджуваної віртуальної спільноти;

$y(t)$ – процес, що описує пропозицію з надання відповідного контенту;

a – показник зміну швидкості попиту агентів у СІС на відповідний контент; якщо $a > 0$ – швидкість попиту зростає, $a < 0$ – швидкість попиту спадає;

b – показник зміни конкуренції агентів у СІС на публікацію контенту, аналогічного за сутністю та змістом;

c – показник зміни швидкості пропозиції з надання агентам взаємодії в СІС відповідного контенту.

У першому рівнянні системи нелінійних диференціальних рівнянь (1) компонент $-xy$ відображає швидкість споживання контенту користувачами СІС або задоволення попиту на відповідний контент, а в другому рівнянні системи (1) із додатним знаком описує швидкість росту пропозиції контенту в СІС за рахунок попиту на нього.

Дослідимо процес синергетичного управління процесами взаємодії агентів СІС з метою протидії інформаційним впливам шляхом штучного підтримання в агентів заданого рівня зацікавленості до відповідного контенту [1]. Для цього синтезуємо

синергетичне управління пропозицією контенту у СІС, для якого система нелінійних диференціальних рівнянь перетвориться до вигляду

$$\begin{cases} \frac{dx(t)}{dt} = ax - xy - bx^2; \\ \frac{dy(t)}{dt} = -cy + xy + u(x, y), \end{cases} \quad (2)$$

де $u(x, y)$ – синергетичне управління взаємодією агентів у СІС, що реалізується через зворотний зв'язок.

Закон управління $u(x, y)$ синтезуємо на основі заданого параметра порядку $\psi_v(x, y) = 0$, що гарантує протікання процесів самоорганізації в системі і появу бажаних синергетичних ефектів. Введемо в структуру системи динамічні інваріанти – атрактори, які враховують природні особливості СІС. Підтримання заданого рівня попиту агентів СІС і зміна цінності інформації, що становить інтерес, повинні змінюватись відповідно до логістичного рівняння:

$$\frac{dz(t)}{dt} = rz(k - z), \quad (3)$$

де r – коефіцієнт зростання попиту на контент;

k – гранична ємність інформаційного середовища, яка враховує цінність контенту.

Для наочної демонстрації механізмів насичення інформаційного середовища вираз (3) запишемо у вигляді:

$$\frac{dz(t)}{dt} = rkz \left(1 - \frac{z}{k} \right). \quad (4)$$

Відповідно до раніше запропонованої концепції [1], обраний атрактор повинен відображати консервативні закони збереження і дисипативні закони впорядкування, самоорганізації властивостей системи. Тому у формалізованому вигляді він набуває вигляду [6]:

$$\psi_v(x, y) = \psi_k(x, y) + \psi_d(x, y),$$

де $\psi_k(x, y)$ – консервативна складова або керований аспект взаємодії агентів у СІС;

$\psi_d(x, y)$ – дисипативна складова, яка визначає вигляд бажаної структури і зміну деякого показника взаємодії акторів СІС відповідно до заданого параметра порядку.

В якості консервативної складової оберемо рівень попиту на контент, який регулюється відповідним коефіцієнтом φ_1 . Дисипативну складову формалізуємо у вигляді правої частини диференціального рівняння логістичного типу (4), яке описує процес насичення інформаційного середовища із врахуванням цінності контенту, шляхом обмеження пропозиції контенту $y(t)$ до заданого рівня N і регуляризації коефіцієнтом φ_2 . Тоді параметр порядку $\psi_v(x, y)$ з урахуванням (4) набуває вигляду [5–8]:

$$\psi_v(x, y) = \varphi_1 x + \varphi_2 \left(1 - \frac{y}{N} \right), \quad (5)$$

де φ_1, φ_2 – коефіцієнти регуляризації попиту і пропозиції відповідного контенту агентів взаємодії в СІС;

N – рівень пропозиції контенту з урахуванням його цінності і визначає задану границю насичення інформаційного середовища.

Функція (5) на завершальному етапі переходу системи до керованого стану повинна бути рівна нулю, що дозволить запустити процеси спонтанної самоорганізації в системі [6]. Внаслідок чого система перейде на траєкторію руху вздовж заданого притягуючого атрактора. Для забезпечення перебігу в системі нелінійних диференціальних рівнянь (2) всіх перехідних процесів, які будуть запуснені завдяки прикладеному синергетичному управлінню за час T_v , макрозмінна (5) повинна задовольняти функціональному рівнянню [6]:

$$T_v \frac{d\psi_v(t)}{dt} + \psi_v(t) = 0. \quad (6)$$

Рівняння (6) є рівнянням Ейлера-Лагранжа, яке визначає точки сплеску синергетичного ефекту [1] для обраного атрактора $\psi_v(x, y)$. Виконання умови (6) забезпечить стійкість переходу до бажаного керованого стану в результаті синергетичного управління $u(x, y)$ взаємодією агентів у СІС.

Після підстановки макрозмінної (5) в рівняння (6), враховуючи початкову систему диференціальних рівнянь (1), отримаємо синергетичне управління :

$$u(x, y) = \frac{\varphi_1}{\varphi_2} N(ax - xy - bx^2) + \frac{1}{\varphi_2 T_v} N\psi_v(x, y) + cy - xy. \quad (7)$$

Синтезоване синергетичне управління переводить зображуючу точку системи (2) на стабілізуючий інваріант (5), рух вздовж якого описується диференціальним рівнянням:

$$\frac{dx_\psi}{dt} = x_\psi \left(a - N - x_\psi \left(\frac{\varphi_1}{\varphi_2} + b \right) \right). \quad (8)$$

Із рівняння (7) отримаємо значення точок сплеску синергетичного ефекту для попиту на контент агентів СІС x_v і пропозиції y_v , в яких система досягає бажаного стану на фазовій площині

$$x_v = \frac{a - N}{\frac{\varphi_1}{\varphi_2} N + b}, \quad y_v = \frac{\varphi_1}{\varphi_2} N \frac{a - N}{\frac{\varphi_1}{\varphi_2} N + b} + N. \quad (9)$$

У результаті підстановки синтезованого управління (7) система нелінійних диференціальних рівнянь (2) набуває вигляду

$$\begin{cases} \frac{dx(t)}{dt} = ax - xy - bx^2; \\ \frac{dy(t)}{dt} = \frac{\varphi_1}{\varphi_2} N(ax - xy - bx^2) + \frac{N}{\varphi_2 T_v} \left(\varphi_1 x + \varphi_2 \left(1 - \frac{y}{N} \right) \right). \end{cases} \quad (10)$$

Слід відмітити, що в синтезованій замкненій системі (10) з урахуванням синергетичного управління пропозиція контенту у СІС $y(t)$ не залежить від показника c зміни швидкості пропозиції з надання агентам взаємодії в СІС відповідного контенту.

Виконаємо моделювання попиту і пропозиції на контент агентів СІС засобами пакету прикладних програм MathCad. В стані динамічного хаосу системи нелінійних диференціальних рівнянь (1) графік зміни попиту і пропозиції контенту в СІС та фазовий портрет системи для параметрів $a = b = 0,25$, $c = 0,4$ подано на рис. 1.

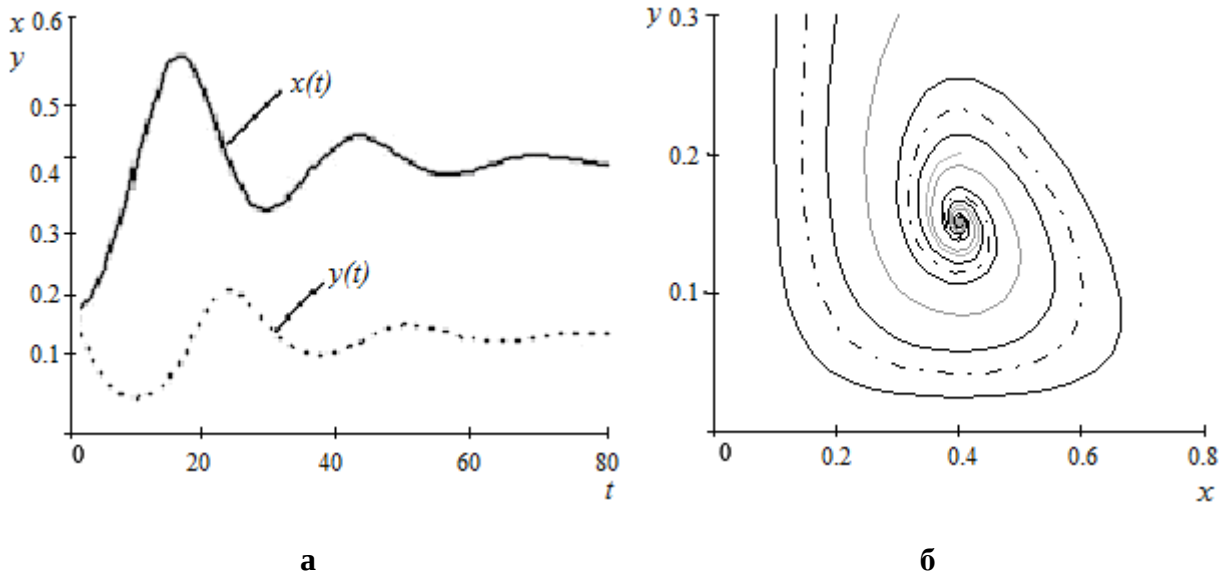


Рис. 1. Система у стані динамічного хаосу: а - графік зміни попиту і пропозиції інформації в СІС; б - фазовий портрет системи

Із фазового портрету нелінійної системи диференціальних рівнянь (1) (рис. 1, б) видно, що вона переходить до керованого стану в точці, для якої пропозиція контенту в СІС дорівнює $y = 0,15$, а попит агентів на нього $x = 0,4$ і цей стан досягається не одразу, а за деякий проміжок часу.

Синергетичне управління попитом на контент $x(t)$ агентів СІС досягається варіюванням значень параметрів N і φ_1 , φ_2 синтезованої системи нелінійних диференціальних рівнянь (10). Контроль рівня пропозиції контенту в СІС $y(t)$ реалізується зміною граничної ємності інформаційного середовища N шляхом обмеження поширення інформації заданого змісту у віртуальних спільнотах і врахуванням природної властивості зменшення цінності інформації в часі [9, 10]. Результати розрахунку значень точки сплеску синергетичного ефекту для T_v подано в табл. 1.

Таблиця 1.

Залежність фазових координат точки сплеску синергетичного ефекту від граничної ємності інформаційного середовища

Коефіцієнти регуляризації попиту φ_1, φ_2	Гранична ємність інформаційного середовища N	Точка сплеску синергетичного ефекту (x_v, y_v)	
		x_v	y_v
$\varphi_1 = \varphi_2 = 1$	0,05	0,67	0,08
	0,10	0,49	0,14
	0,15	0,25	0,19
	0,20	0,11	0,22
	0,25	0	0,25

Візуалізація результатів розрахунків для синтезованої замкнутої системи нелінійних диференціальних рівнянь (11) виконана при параметрах системи рівних $T_v = 1$, $\varphi_1 = \varphi_2 = 1$, $N = 0,17$ подана на рис. 2.

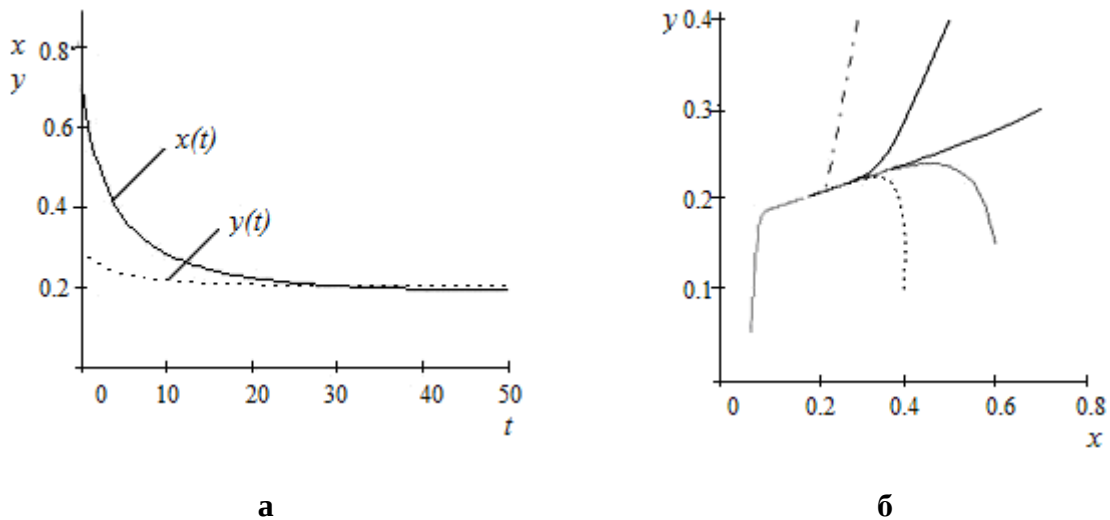


Рис. 2. Керована система управління взаємодією агентів у СІС зміною параметра N : а - графік зміни попиту і пропозиції контенту в СІС; б - фазовий портрет системи

Отже, зміна попиту агентів СІС на контент $x(t)$ досягається варіюванням значень граничної ємності інформаційного середовища N . Аналіз фазового портрету (рис. 2, б) показує, що система переходить від хаосу до керованого стану і фазові траєкторії синтезованої системи (11) організовано прямують до обраного параметра порядку $\psi_v(x, y) = 0$. На цьому інваріантному різноманітті міститься точка сплеску синергетичного ефекту із фазовими координатами $x_v = 0,19$ і $y_v = 0,21$, в якій досягається обмеження попиту агентів $x(t)$ на відповідний контент у СІС.

Для регулювання попиту агентів використовуємо значення параметрів φ_1 і φ_2 синтезованої системи нелінійних диференціальних рівнянь (11). Нехай гранична ємність інформаційного середовища дорівнює $N = 0,17$ і $T_v = 1$. Розрахункові значення точки сплеску синергетичного ефекту подано в табл. 2.

Таблиця 2.

Залежність фазових координат точки сплеску синергетичного ефекту від коефіцієнтів регуляризації попиту φ_1 і φ_2

Гранична сміність інформаційного середовища $N = const$	Коефіцієнт регуляризації попиту φ_1	Коефіцієнт регуляризації попиту φ_2	Точка сплеску синергетичного ефекту (x_v, y_v)	
			x_v	y_v
$N = 0,17$	0,2	$\varphi_2 = 1$	0,28	0,18
	0,4		0,25	0,19
	0,6		0,23	0,19
	0,8		0,21	0,20
	1		0,19	0,20
	$\varphi_1 = 1$	0,2	0,07	0,23
		0,4	0,12	0,22
		0,6	0,15	0,21
		0,8	0,17	0,21
		1	0,19	0,21

Візуалізація результатів розрахунків синергетичного управління взаємодією агентів у СІС для синтезованої замкнутої системи нелінійних диференціальних рівнянь (11) при параметрах системи рівних $T_v = 1$, $N = 0,17$, $\varphi_1 = 0,4$, $\varphi_2 = 0,5$ подана на рис. 3.

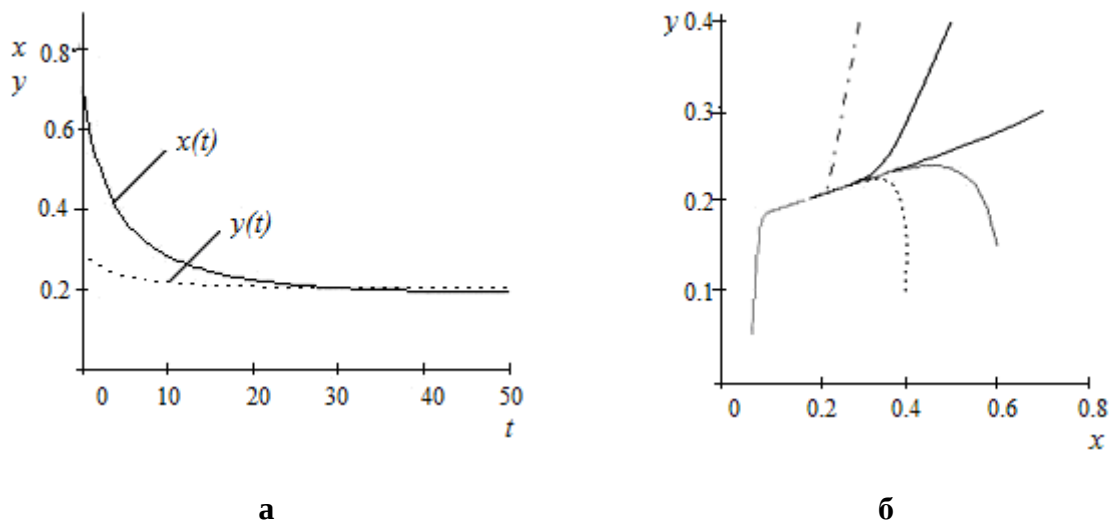


Рис. 3. Керована система управління взаємодією агентів у СІС зміною параметрів φ_1 і φ_2 : а - графік зміни попиту і пропозиції контенту в СІС; б - фазовий портрет системи

Для обраних значень параметрів синтезованої системи нелінійних диференціальних рівнянь (11) точка сплеску синергетичного ефекту, до якої прямують фазові траєкторії, має координати $x_v = 0,18$ і $y_v = 0,21$. У цій точці досягається бажаний синергетичний ефект у синтезованій системі.

Таким чином, результатом синергетичного управління взаємодією агентів у СІС є виникнення процесів самоорганізації, а система переходить від хаотичної динаміки до керованого стану. Фазові траєкторії системи організовано прямують до точки сплеску синергетичного ефекту (x_v, y_v) , яка належить інваріантному різноманіттю $\psi_v(x, y) = 0$. При синтезі синергетичного управління розв'язується пряма задача визначення

координат точки сплеску синергетичного ефекту, які розраховуються за формулами (9). Обернена задача синтезу полягає у визначенні параметрів системи із зворотним зв'язком (11) на основі бажаних координат точки сплеску синергетичного ефекту (x_v, y_v) , що визначаються для попередньо поставленого завдання взаємодії агентів у СІС.

Аналіз результатів моделювання синергетичного управління попитом агентів на контент в СІС показує, що досягнення бажаного синергетичного ефекту досягається зміною параметрів синтезованої нелінійної системи. При цьому для переходу фазової траєкторії системи до обраного притягуючого атрактора достатньо змінити тільки один із параметрів системи, що спрощує процес управління взаємодією агентів у СІС, яка належить до класу складних систем.

Висновки

Вказаний синергетичний ефект досягається за рахунок запуску процесів самоорганізації агентів у СІС. Точка сплеску синергетичного ефекту є притягуючим атрактором системи, на якому реалізується редукція ступенів свободи вихідної системи нелінійних диференціальних рівнянь і забезпечується спрощення процесу досягнення поставлених завдань взаємодії агентів у СІС. Ефективне управління взаємодією агентів здійснює синергетично керований перехід до заданого стану інформаційної безпеки віртуального співтовариства. Подальші дослідження будуть направлені на дослідження необхідних і достатніх умов реалізації синергетичного управління, що забезпечать стійкість досягнутого системою стану інформаційної безпеки.

Список літератури

1. Гришук, Р.В. Концепція синергетичного управління процесами взаємодії агентів у соціальних інтернет-сервісах / Р.В. Гришук, К.В. Молодецька // Безпека інформації. – 2015. – Т. 21. – Ч. II. – С. 123–130.
2. Сазанов, В.М. Социальные сети : Анализ – Технологии – Перспективы. Обзор : [електронний ресурс] / Сайт Лаборатории СВМ. – Режим доступу : http://ntl-cbm.narod.ru/CBM-NET/net_rew.doc (дата звернення: 17.04.15). – Назва з екрану.
3. Горбулін, В.П. Інформаційні операції та безпека суспільства : загрози, протидія, моделювання: [монографія] / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.
4. Castells, M. The Network Society : From Knowledge to Policy / M. Castells, G. Cardoso. – Washington, DC : Johns Hopkins Center for Transatlantic Relations, 2005. – 434 p.
5. Epstein, Joshua M. Nonlinear Dynamics, Mathematical Biology, and Social Science : lecture notes / Joshua M. Epstein. – Massachusetts : Addison-Wesley Publishing Company, 1997. – 164 p.
6. Колесников, А.А. Синергетическое методы управления сложными системами : теория системного синтеза / А.А. Колесников. – М. : Едиторал УРСС, 2005. – 228 с.
7. Андриевский, В.Р. Управление хаосом : методы и приложения : [в 2ч.]. / В. Р. Андриевский, А.Т. Фрадков // Автоматика и телемеханика. – 2003. – Ч I : Методы. – № 5. – С. 3–45.
8. Пригожин, И. Порядок из хаоса : Новый диалог человека с природой [пер. с англ.] / И. Пригожин, И. Стенгерс ; под. общ. ред. В.И. Аршинова, Ю.Л. Климонтовича, Ю.В. Сачкова. – М. : Наука, 1984. – 432 с.
9. Бурячок, В.Л. Політика інформаційної безпеки [Текст] : підручник / В.Л. Бурячок, Р.В. Гришук, В.О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.
10. Гришук, Р.В. Методика оцінювання рівня небезпеки кібернетичних загроз / Р.В. Гришук, С.В. Чернишук // Сучасний захист інформації. – 2013. – Спецвипуск. – С. 23–28.

СИНТЕЗ СИНЕРГЕТИЧЕСКОГО УПРАВЛЕНИЯ СПРОСОМ АГЕНТОВ НА КОНТЕНТ В СОЦИАЛЬНЫХ ИНТЕРНЕТ-СЕРВИСАХ

К.В. Молодецкая

Житомирский национальный агроэкологический университет
ул. Старый бульвар, 7, Житомир, 10008, Украина; e-mail: kmolodetska@gmail.com

Социальные интернет-сервисы принадлежат к классу нелинейных динамических систем, поэтому явления социальной коммуникации характеризуются непредсказуемостью процессов взаимодействия агентов в результате внешних воздействий и переходом системы в состояние неуправляемого хаоса. Для достижения системой устойчивого состояния как результата управляемой самоорганизации агентов предлагается использовать концепцию синергетического управления взаимодействием агентов в социальных интернет-сервисах. В статье синтезировано синергетическое управление взаимодействием агентов в социальных интернет-сервисах, что позволит повысить устойчивость виртуальных сообществ к деструктивным информационным влияниям путем регуляризации спроса на контент. Приведен модельный пример управления взаимодействием агентов с целью синергетически управляемого перехода виртуального сообщества к заданному состоянию информационной безопасности.

Ключевые слова: социальный интернет-сервис, динамический хаос, синергетическое управление, аттрактор, информационная безопасность.

THE SYNTHESIS OF SINERGISTICAL MANAGEMENT OF AGENTS DEMAND ON CONTENT IN SOCIAL INTERNET SERVICES

K.V. Molodetska

Zhytomyr National Agro-Ecological University
7, Sraryi Bulvar, , Zhytomyr, 10008, Ukraine; e-mail: kmolodetska@gmail.com

Social Internet services belong to the class of nonlinear dynamical systems, so the phenomenon of social communication processes are characterized by unpredictability of agents' interaction due to external influences and transition of the system into a state of uncontrolled chaos. To achieve a steady state of the system as a result of self-managed agents, it is suggested to use the concept of the synergistic management of agents' interaction in social networking services. The paper synthesized synergistic management of agents' interaction in social networking service that will enhance the resistance of virtual communities to destructive information impacts through regularization of the demand for content. As an example, the article presents a model of the management of agents' interaction in order to provide the synergistically managed transition to a given state of the information security of a virtual community.

Keywords: social networking service, dynamic chaos, synergistic management, attractor, information security.

МОДЕЛІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІЗ ЗАПІЗНЮВАННЯМ РЕАГУВАННЯ НА ІНЦИДЕНТИ

І.В. Кононович¹, Д.А. Маєвський², Р.С. Подобний²

¹Одеська національна академія харчових технологій
вул. Канатна, 112, Одеса, 65039, Україна; e-mail: kononovich@mail.ru

²Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net

Розглядається проблема впливу запізнювання реагування на інциденти із захищеністю інформаційних ресурсів в системах кібербезпеки інформаційного простору. Визначено, що динамічні властивості взаємодіючих систем типу «порушення безпеки – підтримка безпеки» досліджена ще недостатньо. Відомі інструментарії аналізу й оцінки захищеності інформації та результати досліджень не дають можливості враховувати вплив запізнювання реагування на інциденти з кібербезпекою. На основі аналізу теорії й моделей запізнювання та аналізу динаміки систем захисту інформації розроблена методика дослідження впливу запізнювання в системах кібербезпеки. Порівнюються моделі із запізнюванням Хатчинсона, Лоткі-Вольтерра та Аронсона. Методика та досліджені моделі дають можливість створювати більш гнучкі засоби виявлення, обробки та ліквідації наслідків інцидентів кібербезпеки та оцінювати рівень захищеності інформації на основі статистичних даних і на якісних оцінках, зроблених за допомогою нелінійних моделей із запізнюванням.

Ключові слова: захист інформації, інформаційна безпека, загрози, вразливість, атака, кібербезпека, ризики інформаційної безпеки, нелінійна динаміка, модель систем із запізнюванням

Вступ

Триваюче загострення критичної ситуації у сфері кібербезпеки високотехнологічних систем, критичних інформаційних ресурсів, інформаційного простору країни та кіберпростору вимагає вирішення багатьох наукових і технологічних проблем. Зростають різноманітність, складність і технологічність загроз та засобів впливу, збільшується кількість вразливостей елементів сучасного кіберпростору внаслідок його надзвичайної гнучкості. При цьому, існуючі засоби та заходи захисту не здатні в повному обсязі протидіяти наявній множині загроз. Згідно висловлювання Касперського настав час «важливості складних технологій (безпеки) в епоху складних атак» [1]. Тому загальною проблемою є вдосконалення та підвищення ефективності систем забезпечення інформаційної безпеки з урахуванням ризиків безпеки сучасного кіберпростору та високотехнологічних систем. Новою проблемою, яка стає темою досліджень, є використання в сфері кібербезпеки прогностичних можливостей нелінійної динаміки та синергетики, зокрема, врахування впливу запізнювання з прийняттям рішень та реагуванням на інциденти з кібербезпекою. Для побудови ефективних комплексних систем захисту інформації в інформаційно-комунікаційних системах необхідно проводити аналіз, моделювання та оцінку ризиків із врахуванням запізнювання реагування на порушення політики кібербезпеки.

Аналіз існуючих досліджень. Огляд теорії запізнювання стосовно систем синхронізації та інших галузей подано у [2]. Показано, що запізнювання у взаємодіях приводить до суттєвих змін і ускладненню динаміки ансамблю. Як найбільш типова

властивість таких систем відмічена «періодичність у залежності динамічних режимів системи від величини запізнювання». Періодичний характер залежності величини захищеності інформації у часі та залежності амплітуди захищеності від величини запізнювання реагування на інциденти з кібербезпекою прогнозовано у роботах з участю автора [3, 4]. Дана робота є продовженням і узагальненням цих робіт. Складні системи удосконалюються завдяки процесам інтеграції, конвергенції й уніфікації, які стимулюються застосуванням інформаційних технологій. Інтегральний підхід «до множини різних ризиків» безпеки обґрунтовується у [5]. Для дослідження динаміки захищеності інформаційних ресурсів почали використовувати моделі динамічних систем, які мають аналоги різної природи: фізичної, хімічної, біологічної, соціальної, економічної, інформаційної тощо. Застосовується математичний апарат, який став класичним для вивчення моделей розповсюдження інфекційних хвороб, біологічних та інших об'єктів [6]. Огляд сучасного стану аналітичних моделей розповсюдження червів та оцінки впливу запізньованих заходів з протидії мережевим хробакам зроблено в [7]. Детальні математичні дослідження систем із запізнюванням, що моделюють задачу типу «хижак-жертва» на основі рівнянь Хатчинсона проведені у [8]. Однією з головних причин ризиків інформаційної безпеки є «людський фактор» і, зокрема, запізнювання в прийнятті нагальних рішень щодо застосування заходів і засобів захисту. Запізнювання виникає як технологічне, соціальне і психологічне явище. Нові покоління технологій непередбачено виявляються вразливими. Потрібен час для вироблення протидії. Необхідне відповідне навчання користувачів, фахівців та осіб, що приймають рішення. Запізнювання може виникати внаслідок звикання до технологій і недооцінки ризиків. Запізнювання прийняття рішень щодо захисту інформації стало одним із важливих проблем безпеки. Вплив запізнювання прийняття заходів захисту інформації на ризики інформаційної безпеки науковцями і практиками досліджено недостатньо. Існуючі оцінки захищеності інформації у переважній більшості базуються на статистичних підходах, орієнтуються на статичні моделі і слабо враховують динамічний характер взаємодій у кіберпросторі. Відомий інструментарій аналізу та оцінки ризиків не дає можливості враховувати вплив запізнювання у прийнятті рішень щодо заходів захисту інформації з урахуванням їх динаміки.

Метою роботи є розробка в рамках системного аналізу методів дослідження та аналіз впливу запізнювання у прийнятті рішень із захисту інформації на рівень захищеності інформаційних ресурсів за допомогою порівняння моделей із запізнюванням на основі рівняння Хатчинсона, моделі Лоткі-Вольтерра та системи рівнянь Аронсона і виділення найбільш типових властивостей, які характерні для систем із запізнюванням у зв'язках.

Системи із запізнюванням за характером взаємодії можна поділити на наступні класи. Системи із внутрішніми взаємодіями, які отримали назву систем із внутрішньовидовою конкуренцією за ресурси. Характерним прикладом таких систем є модель на основі рівняння Хатчинсона. Системи із природною (ймовірнісною) міжсистемною взаємодією, які називають міжвидовою конкуренцією. Реакції обох систем пропорційні дії противної сторони. Типовим прикладом таких систем є модель Лоткі-Вольтерра. Системи із коливальною регулярною міжсистемною взаємодією, так звані, системи із синхронізацією. Амплітудна динаміка таких систем вивчена Аронсоном на «взаємній синхронізації двох автогенераторів» [2]. На основі численних даних моделювання є підстави вважати, що в усіх випадках взаємодія системи «зловмисник – захисник» відбувається коливальним способом.

Внутрішньо-системні запізнювання. Рівняння Хатчинсона

Системи забезпечення інформаційної безпеки є системами із часовим запізнюванням. В них результат впливу або ліквідації цього впливу проявляється не

відразу, а через певний час τ – час запізнювання. Розглянемо вплив запізнювання з прийняття і виконання рішень щодо заходів захисту інформації на ризик інформаційної безпеки. У найпростіших випадках ризик пропорційний частоті вдалих атак, які привели до завдання шкоди. Тоді частота вдалих атак може бути мірою ризику інформаційної безпеки. «Рівнянням із запізнюванням прийнято називати рівняння відносно невідомої функції $x(t)$, що пов'язує швидкість зміни функції $x(t)$ з її значеннями в поточний момент часу t та з її значеннями в певний момент часу $t-\tau$, де постійна $\tau > 0$ » [9]. Дослідимо вплив запізнювання з прийняття рішень щодо захисту інформації на частоту атак за допомогою простої моделі – рівняння Хатчинсона:

$$N'(t) = r(1 - \frac{N(t-\tau)}{K})N(t), \quad (1)$$

де: τ – час запізнювання.

Найпростішим дискретним аналогом рівняння Хатчинсона є рівняння [10]:

$$N_{n+1} = r(1 - N_{n-\tau}/K)N_n \quad (2)$$

де $\tau \in \{0, 1, 2, \dots\}$, приймає дискретні значення

Якщо у (1) покласти $\tau = 0$, то рівняння Хатчинсона перетворюється у рівняння Ферхюльста [11]. Рівняння (1) і (2) мають просту інтерпретацію для систем забезпечення інформаційної безпеки. Маємо: динамічний процес у системі з обмеженим обсягом однорідних інформаційних ресурсів K , наприклад, у мережі є K однакових, вразливих до атак, типових комп'ютерів; t – час; n – величина дискретного відліку часу (модельний час). У системі відбувається боротьба за ресурси. Змінна N відображає поточне число реалізованих загроз. Параметр r – коефіцієнт росту кількості вдало реалізованих атак. Параметр r/K – коефіцієнт стримування росту кількості атак, або коефіцієнт внутрішньо-системної конкуренції. Він характеризує процес «опору середовища». Опір середовища пояснюється, по-перше, обмеженими доступними ресурсами, а, по-друге, тим, що кількість ресурсів (неуражених активів) поновлюється внаслідок впровадження засобів та заходів захисту, які, проте, можуть мати нові вразливості.

Оскільки потік реалізованих атак є дискретним потоком подій, то для аналізу моделі Хатчинсона доцільно вибрати відображення (2). Порядок проведення математичного експерименту наступний. Задаємо кількість інформаційних ресурсів – K . Для кожної пари параметрів r і τ знаходимо рівняння руху

$$N_{i+1}(r, \tau) = r(1 - N_{i-\tau}/K)N_i; \quad i = [1, 2, \dots, i_{\max}] \quad (3)$$

Далі знаходимо функцію, яка описує поверхню:

$$M(r, \tau) = \max(N_{i+1}(r, \tau)). \quad (4)$$

Недолік моделі запізнювання у системі інформаційної безпеки на основі рівняння Хатчинсона полягає у тому, що коефіцієнт опору середовища не змінюється і не залежить від зовнішніх факторів. Коефіцієнт відновлення комп'ютерів не залежить від кількості атак. Такий недолік усувається у наступній моделі.

Запізнювання при стохастичній міжсистемній взаємодії. Модель Лоткі-Вольтерра

Цю модель інтерпретовано в термінах систем інформаційної безпеки і запропоновано автором для вивчення систем безпеки із запізнюванням у роботі [4]. Модель представлена у наступному вигляді. Введені позначення: x – кількість атак на комп'ютерну мережу, що виконуються зловмисниками, це аналог «жертв»; y –

кількість операцій, що виконуються захисниками комп'ютерної мережі, це аналог «хижаків». Середнє значення цих величин позначимо великими літерами, відповідно – X_c, Y_c . Динаміка чисельності взаємодіючих популяцій захисника $x(t)$ та хижака $y(t)$ моделюється системою рівнянь [8]:

$$\begin{cases} \dot{x}(t) = r_x \left[1 + a \left(1 - \frac{y(t)}{Y_c} \right) - \frac{x(t-h_x)}{X_c} \right] x(t), \\ \dot{y}(t) = r_y \left[\frac{x(t)}{X_c} - \frac{y(t-h_y)}{Y_c} \right] y(t) \end{cases}, \quad (5)$$

де r_x та r_y – мальтузіанські коефіцієнти росту;

h_x та h_y – середній час запізнювання, відповідно, аналізу (планування) атаки хакером й впровадження засобів протидії та пошуку вразливості захисником;

X_c та Y_c – середні кількості операцій-атак та з ліквідації атак, відповідно;

a – коефіцієнт тиску захисників на хакерів, який визначає ефективне зменшення середньої кількості дій хакерів за умови збільшення активності захисників.

Коефіцієнт тиску захисників на хакерів – a визначає ефективне зменшення кількості операцій хакерів по плануванню, підготовці та здійсненню атак. Його можна визначити неявно:

$$X_c(a) = X_c(0)/(1+a). \quad (6)$$

Для спрощення моделі (5) при чисельному розрахунку зменшують кількість параметрів за допомогою заміни. Слідуючи [12; формули (3), (4)], робимо заміни: $t = h_x \tau$, $x(h_x \tau) = X N_1(\tau)$, $y(h_y \tau) = Y N_2(\tau)$, і далі, позначивши $\lambda_1 = r_x h_x$, $\lambda_2 = r_y h_y$, $h = h_y/h_x$, та знову перепозначивши τ через t , отримуємо

$$\begin{cases} \dot{N}_1(t) = \frac{\lambda_1}{1+a} [1 + a(1 - N_2(t)) - N_1(t-1)] N_1(t), \\ \dot{N}_2(t) = \lambda_2 [N_1(t) - N_2(t-h)] N_2(t). \end{cases} \quad (7)$$

Звернемо увагу, що рівняння (7) можна вивести із рівняння Хатчинсона (1), при $K=1$, у яке включаються додаткові члени $(\lambda_1 a N_2(t) N_1(t))$, $(\lambda_2 N_1(t) N_2(t))$, щоб «описати пригнічуючі впливи, які чиняться кожним видом на свого конкурента» [13].

При проведенні математичного експерименту величину запізнювання дій хакера можна вважати незмінною і змінювати запізнювання дій «захисника». Можна зафіксувати також параметри активності хакера та тиску на нього: $\lambda_1 = \text{const}$; $a = \text{const}$. Для кожної пари параметрів λ_2 і h знаходимо рівняння руху $N_1(t, \lambda_2, h)$, вирішуючи систему рівнянь (7) чисельним способом; знаходимо функцію, яка описує поверхню

$$M(r, \tau) = \max(N_1(t, \lambda_2, h)). \quad (8)$$

Основні труднощі математичного експерименту полягають у знаходженні раціональних інтервалів зміни параметрів λ_2 і h та фіксації параметрів λ_1, a . Нас цікавлять випадки, коли можна попередити максимальні ризики інформаційної безпеки.

Запізнювання при регулярній міжсистемній взаємодії. Системи із синхронізацією

Аналізувати запізнювання у системі кібербезпеки з позицій синхронізації має сенс за таких причин. Моделювання показує, що інтенсивність атак та інтенсивність впливу

на порушення політики безпеки (реагування на інциденти з кібербезпекою) мають тенденцію до коливального характеру. Тому корисно визначити як параметри синхронізуючого коливального процесу протидії атакам впливають на коливальний процес самих атак і виробити відповідні заходи зменшення останніх. Вважається, що модель взаємодії із запізнюванням Аронсона є найбільш універсальною, на відміну від моделей Хатчинсона і Лоткі-Вольтерра. Як і раніше, нас цікавить опис процесів із амплітудною динамікою.

У [2] розглядається ансамбль із двох зв'язаних систем Ван-дер-Поля. Такий ансамбль описується наступною системою рівнянь для амплітуд і фаз:

$$\begin{cases} dr_1/dt = r_1(1 - k\gamma - r_1^2) + r_2\gamma \cos \varphi, \\ dr_2/dt = r_2(1 - k\gamma - r_2^2) + r_1 \cos \varphi, \\ d\varphi/dt = \Delta + q_1 r_1^2 - q_2 r_2^2 - (r_1/r_2 + r_2/r_1) \sin \varphi. \end{cases} \quad (9)$$

Тут r_1 та r_2 – амплітуда коливань автогенераторів; відповідно – це кількість атак і кількість відновлених комп'ютерів;

$\varphi = \theta_1 - \theta_2$ – різниця фаз коливань;

γ – сила зв'язку;

k – тип зв'язку (задамо $k = 1$);

Δ – параметр, що визначає частотне розлаштування між автогенераторами;

q_1 та q_2 – задають залежність частоти коливань від амплітуди у незв'язаних системах.

«Найбільш цікавим ефектом, який виявлено у системі (9), являється так зване вимирання коливань. Даний ефект полягає у тому, при зв'язуванні автогенераторів коливання в них припиняються і амплітуди r_i приймають нульові значення. З точки зору фазового простору, цей ефект відповідає стійкому в цілому стану рівноваги на початку координат» [2]. З точки зору кібербезпеки, такий ефект можна трактувати як існування умов, за яких активність порушників кібербезпеки можна звести до нульового значення. У [2] показано, що стан рівноваги може бути стійким лише за умови $|\Delta| > 2/k$.

«Простір параметрів системи (9) розбивається на три області з якісно різною поведінкою, ([2, рис. 3а]). За малих розлаштувань Δ та великих силах зв'язку γ у системі спостерігається синхронізація, при якій автогенератори коливаються з постійною різницею фаз. За великих розлаштувань і слабких зв'язках динаміка системи являється асинхронною – різниця фаз автогенераторів необмежено зростає. У випадку великих розлаштувань та сильних зв'язках у системі відбувається вимирання коливань» [2].

Таким чином, ефект взаємодії із запізнюванням полягає у тому, що взаємодія між системами «часто приводить до якісної зміни динаміки системи в цілому [2]». Ритми взаємодії систем узгоджуються і налаштовуються одне до одного. Синхронізація нелінійних систем різної природи часто виявляється заснованою на якісно схожих між собою динамічних механізмах.

Результати математичних експериментів

Для прикладу і для виявлення типових властивостей моделей із запізнюванням розглянемо модель на основі рівняння Хатчинсона. Після аналізу нерухомих точок, досліджуємо рівняння руху. На серії рис. 5, а, б, в, г наведені рівняння руху, отримані за формулою (3) у залежності від коефіцієнту росту – r та величини запізнювання – τ . Маємо відповідно: а – швидко зменшувану кількість атак; б – виникнення затухаючих

коливань; в – регулярний коливальний процес; г – детермінований хаос. Далі досліджувався вплив на максимальну кількість реалізованих атак у залежності від коефіцієнту росту – r та величини запізнювання – τ (рис. 6.). На графіку відображені значення максимуму кількості реалізованих атак лише в області стійкості моделі. На рис. 7 наведено фактичні затримки T у залежності від коефіцієнту росту – r та величини запізнювання – τ . Фактична затримка оцінюється модельним часом від початку моделювання, до першого максимуму. Отримані результати носять не кількісний, а якісний характер. «Так, стало цілком ясно, що навряд чи можливий ефективний кількісний аналіз (навіть при використанні ЕОМ з їх колосальними можливостями) природної екосистеми навіть у «малому», без чого важко розраховувати на побудову яких-небудь більш або менш адекватних прогнозів щодо динаміки цих систем у «цілому»» [14, с. 8]. Кількісні оцінки можливі лише після уточнення моделей та доведення їх адекватності на основі широкого експериментального та статистичного матеріалу.

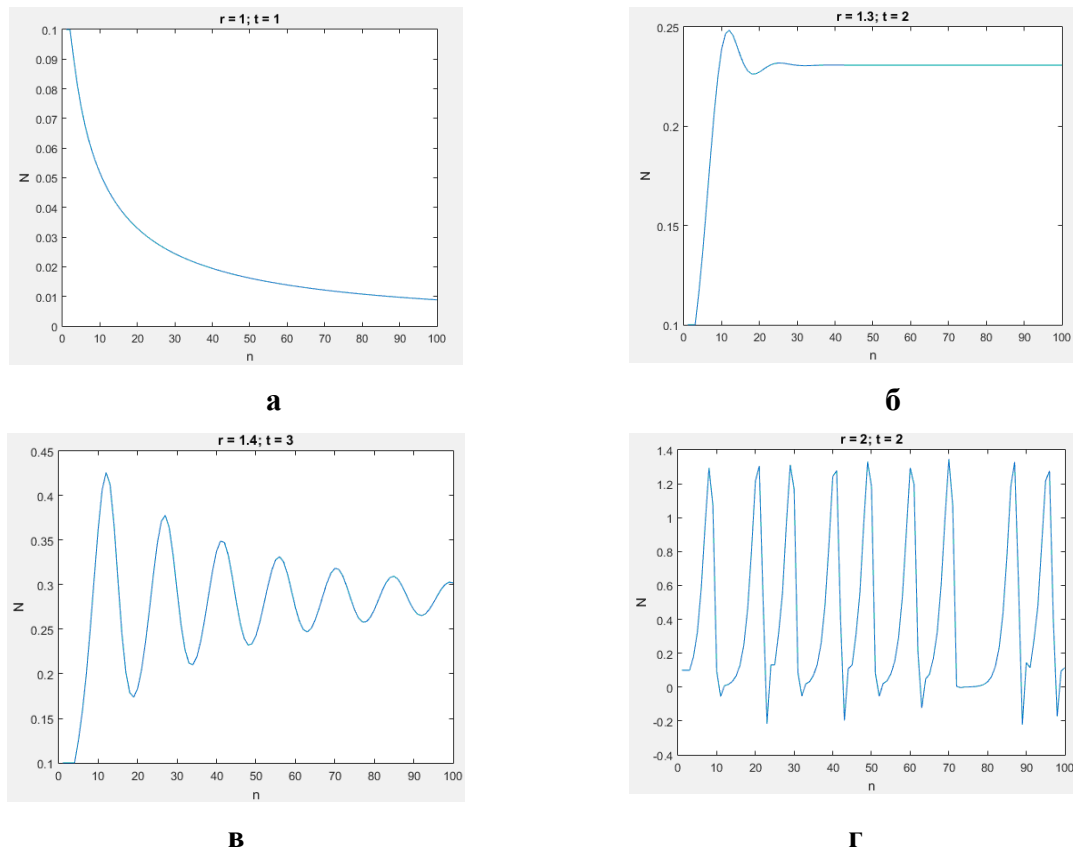


Рис. 5. Графіки рівняння руху в моделі Хатчинсона.

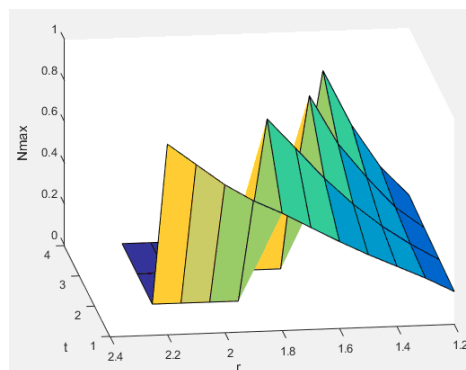


Рис. 6. Залежність максимальної кількості реалізованих атак від коефіцієнту росту – r та величини запізнювання – τ в моделі Хатчинсона

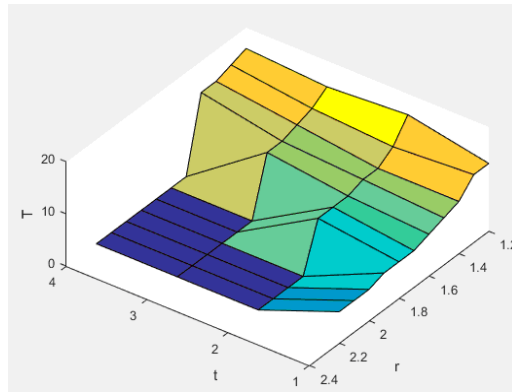


Рис. 7. Залежність фактичної затримки реагування від коефіцієнту росту – r та величини запізнювання – τ в моделі Хатчинсона

Висновки

В рамках системного аналізу розроблено методи дослідження та проведено якісний аналіз впливу запізнювання у прийнятті рішень із захисту інформації на рівень захищеності інформаційних ресурсів за допомогою порівняння моделей із запізнюванням на основі рівняння Хатчинсона, моделі Лоткі-Вольтерра та системи рівнянь, досліджених Аронсоном. Виділені найбільш типові властивості, які характерні для систем із запізнюванням у взаємозв'язках. Темою подальших досліджень може стати експериментальна та статистична перевірка адекватності моделей на реальних системах.

Список літератури

1. Отчет «Лаборатории Касперского»: Java под ударом – эволюция эксплойтов в 2012-2013 гг. – 26 с. – Режим доступа: http://www.securelist.com/ru/analysis/208050816/Otchet_Laboratorii_Kasperskogo_Java_pod_udarom_evolyutsiya_eksplotov_v_2012_2013_gg.
2. Клиньшов, В.В. Синхронизация автоколебательных сетей с запаздывающими связями / В.В. Клиньшов, В.И. Некоркин // УФН. СПб.: – 2013. – Т. 183. – № 12. – С. 1323 – 1336.
3. Кононович, В.Г. Вплив затримки прийняття заходів із захисту інформації на ризики інформаційної безпеки / В.Г. Кононович, І.В. Кононович, Ю.В. Копитін, С.В. Стайкуца // Безпека інформації. – Київ: НАУ, 2014. – Т. 20. – № 1. – С. 83 – 91.
4. Кононович, І.В. Динаміка кількості інцидентів інформаційної безпеки / І.В. Кононович // Інформатика та математичні методи в моделюванні. – Одеса, 2014. – Т. 3. – №3. – С. 35-43.
5. Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. – М.: РАН, 2000. – 249 с. – Режим доступа: <http://risk.keldysh.ru/risk/risk.htm>.
6. Захарченко, А.А. Черводинамика: причины и следствия / А.А. Захарченко // Защита информации. Конфидент. – 2004. – №2. – С. 50–55.
7. Котенко, И.В. Аналитические модели распространения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. Вып. 4. – СПб.: Наука. 2007. – С. 208-224. – Режим доступа: <http://www.proceedings.spiiras.nw.ru/data/src/2007/04/00/spyproc-2007-04-00-15.pdf>.
8. Кашенко, С.А. Релаксионные колебания в системе с запаздываниями, моделирующей задачу «хищник–жертва» / С.А. Кашенко // Модели и анализ информационных систем. – 2013. – Т. 2. – № 1 (2013) – Ярославль. – С. 52-98.
9. Тарасевич, Ю.Ю. Избранные вопросы математического моделирования и численных методов. – Режим доступа: <http://window.edu.ru/resource/936/38936/files/aspu03.pdf>.
10. Гусаров, А.Н. Модель запаздывания действия антивирусов при распространении в сетях компьютерных угроз / А.Н. Гусаров, Д.О. Жуков // Известия ОрелГТУ. Серия «Информационные системы и технологии». – 2008. – № 1-2/269(544). – С. 67–72.
11. Долгий, Ю.Ф. Математические модели динамических систем с запаздыванием : учеб. пособие / Ю.Ф. Долгий, П.Г. Сурков. – Екатеринбург : Изд-во Урал, ун-та, 2012. – 122 с.

12. Шампайн, Л.Ф. Решение обыкновенных дифференциальных уравнений с использованием МАТЛАБ: Учебное пособие / Л.Ф. Шампайн, И. Гладвел, С. Томпсон. Пер. с англ. – СПб.: Издательство «Лань», 2009. – 304 с. (Учебники для вузов. Специальная литература).
13. Дж. М. Смит. Модели в экологии / Дж. М. Смит. – М.: Мир, 1976. – 183 с.
14. Тутубалин, В.Н. Математическое моделирование в экологии: Историко-методологический анализ. Монография / В.Н. Тутубалин, Ю.М. Барабашева, А.А. Григорян и др. // – М.: Языки русской культуры, 1999. – 208 с.

МОДЕЛИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ С ЗАПАЗДЫВАНИЕМ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

І.В. Кононович¹, Д.А. Маевський², Р.С. Подобний²

¹Одесская национальная академия пищевых технологий
ул. Канатная, 112, Одесса, 65039, Украина; e-mail: kononovich@mail.ru

²Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net

Рассматривается проблема влияния запаздывания реагирования на инциденты с защищенностью информационных ресурсов в системах кибербезопасности информационного пространства. Известные инструментарию анализа и оценки защищенности информации и результаты исследований не дают возможности учитывать влияние запаздывания реагирования на инциденты с кибербезопасностью. На основе анализа теории и моделей запаздывания и анализа динамики систем защиты информации разработана методика исследования влияния запаздывания в системах кибербезопасности. Сравниваются модели с запаздыванием Хатчинсона, Лотки-Вольтерра и Аронсона. Методика и исследованные модели дают возможность оценивать уровень защищенности информации на основе статистических данных и качественных оценок, выполненных с помощью нелинейных моделей с запаздыванием.

Ключевые слова: защита информации, информационная безопасность, угрозы, уязвимость, атака, кибербезопасность, риски информационной безопасности, нелинейная динамика, модель систем с запаздыванием

MODELS OF SYSTEM OF THE CIBERSECURITY PROVIDING WITH DELAY OF REACTION ON INCIDENTS

I.V. Kononovich¹, D.A. Mayevskiy², R.S. Podobniy²

¹Odessa national academy of food technologies
112, Rope Str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

²Odessa national polytechnic university,
1, Shevchenko Str, Odessa, 65044, Ukraine; e-mail: konrac1993@gmail.com

The problem of influencing of delay of reaction on incidents with protected of informative resources in the systems of cybersecurity informative space is examined. It is certain that dynamic properties of the interactive systems of type of security «breach is support of safety» is yet not enough explored. Known tools of analysis and estimation of protected of information and the results of researches do not enable to take into account influence of delay of reaction on incidents with cybersecurity. On the basis of analysis of theory and models of delay and analysis of dynamics of the systems of defence of information the developed method of research of delay in the systems of cybersecurity. Models with the Chatshinson, Aronson and Lotki-Volterra delay are compared. A method and explored models enable to create more flexible facilities of exposure, treatment and liquidation of consequences of incidents of cybersecurity and to estimate the level of protected of information on the basis of statistical information and on the high-quality estimations done by nonlinear models with the delay.

Keywords: information security, information security, threat, vulnerability, attack, cyber security, information security risks, nonlinear dynamics model systems with delay

PROGRAM AND TECHNICAL ASPECTS OF CRYPTOGRAPHIC DEFENCE OF DATA STORAGE

A.V. Zadereyko, A.V. Troyanskiy

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; email: alexander.zadereyko@opu.ua,
alexander.zadereyko@gmail.com

Data storage defense is an aggregate of problems, interlinked with the use of cryptographic program facilities of the different setting. For the decision of this task - using free of charge cross platform cryptographic TrueCrypt software with the opened source code, allows to make coding of information «on the fly». The analysis of TrueCrypt software possibilities is executed. The algorithm for defense of data storage with practical application TrueCrypt software is developed. The productivity comparative analysis of the personal computer with/out cryptographic TrueCrypt software is resulted. Actual absence of the productivity decline is showed. Independent audit considered cryptographic TrueCrypt software did not expose the greatest threats his vulnerability. Personal author's 10-years experience in exploitation TrueCrypt software for defense of data storage allows to assert a blamelessness, reliability and stability of it work.

It's shown that cryptographic TrueCrypt software and its subsequent modifications, is the most effective measure, which allows preventing the losses of confidential information of users, placed on the personal computer and external data storage.

Keywords: cryptographic defense, cryptographic software, TrueCrypt, cryptocontainer, defense of carriers of data, coding of information «on the fly».

The essence of a problem

Ensuring the protection of the users of personal computers (PCs) in practice is a set of problems closely related with using software and hardware for various purposes. [1]

The most common feature of the operation PC users in different organizations is practically nobody does not restrict access to them. This inevitably leads to the fact that a "unit" PCs have access uncontrolled number of users. Such a "multi-user" mode of operation eventually gives rise to the need to protect data as stored on a PC, so data users themselves.

The solution of this problem is argued by objective reasons, determining the importance of ensuring the protection of user information:

- rapid growth of the number of PCs;
- widespread use of PCs in various spheres of human activity;
- accumulation of large amounts of data on PC;
- expansion of the users range who have access to PC;
- availability PC connecting to LAN or corporate network with Internet access.

A partial solution to this problem can be realized by using their individual user information data storage - flash cards, portable hard disks, etc.

However, it did not really solve the problem of protecting information from unauthorized access, "third parties" by hackers or malicious software (software) when connecting individual carriers to the PC. Furthermore, it should also be noted that these devices trust important information is unsafe. First of all because there is the risk of data loss (physical or mechanical), especially if recorded on the data storage any confidential

information of high importance, the consequences of such a loss can appear to be the most sorrowful.

In this regard, the task of ensuring reliable protection of user data is current as ever.

Latest research and publications analysis have taken the initiative towards solving the problem.

The most common methods of protecting information on connected data storage in a customer environment include:

1. Create a hidden partition [2];
2. Create an archive, locked password [3];
3. Restrict access to files / folders. [4]

These methods of information protection have a number of drawbacks. The presence of hidden partitions easily installed by comparing the actual and the real capacity of the storage medium.

Creating archives locked password, inevitably increases:

- the probability of a lack of software on the PC;
- long time of creating and extracting;
- the probability of an incorrect input (random) password when creating an archive;
- The probability of a partial data loss in the process of creating an archive

especially grows when using flash cards (due to exceeding the number of read-write cycles guaranteed by the manufacturer) [5].

Restrict access to files/folders is performed, usually with the help of additional software: Folder Crypto Password; Secure Folder; Hide Folder; Lock Folder, etc. or built-in operating system (OS). In this case, access to the protected data is limited to OS administrative means, which in itself is unreliable.

Conclusions and prospects for further research in this direction

In connection with the above, it can be concluded that a reliable protection for user data only option is to use any encryption in real time. This allows to realize continuous operation of the encryption/decryption algorithm of traffic from the PC to the data storage medium during recording/reading [6].

The purpose of the article

Consider the feasibility of cryptographic protection data storage users.

The basic material of the presentation

To solve this problem almost perfect free, cross-platform cryptographic TrueCrypt software open source encryption of data "on the fly» (On-the-fly encryption). Under the encrypted "on the fly" is to be understood that all data is encrypted and decrypted before the direct appeal to them (read, execute, or save). The data is encrypted in its entirety, including the file headers, the contents, metadata, etc. [7].

Considered software allows to create a file cryptocontainers, encrypt partitions themselves HDD, including OS, as well as removable storage devices: USB-drives and external HDD.

The benefits of encryption software TrueCrypt [8]:

- the ability to use a portable (portable version);

- software works with Microsoft Windows, starting with 2000 / XP / 7 (x32 / x64), GNU / Linux (32- and 64-bit versions of the kernel 2.6 or compatible) and Mac OS X (10.4 Tiger and above);
- use strong encryption algorithm - AES-256, Serpent, and Twofish with the possibility of a mutual combination);
- real-time encryption, and it is not noticeable to the user;
- pre-boot authentication to encrypt the system partition HDD;
- the possibility of creating separate file of cryptocontainers, including dynamically expanding in the data storage with NTFS file system;
- creation cryptocontainers in the "cloud storage";
- cryptocontainers may look like an ordinary file with any extension, for example, txt, doc (x), mp3, img, iso, mpg, avi, etc., with or without enlargement;
- full encryption of the contents of devices – HDD and removable data storage;
- creation of hidden volumes, including and the hidden OS;
- the OS cannot determine the presence of TrueCrypt volumes - they are just a set of random data and identify them with TrueCrypt software does not seem possible (not counting method termorectum cryptoanalysis);
- ensure that the two levels of plausible deniability of the encrypted data is one of the most important features of the software TrueCrypt. Their operating principle is the ability to create an encrypted carrier with two passwords - password of the available real data, and the second - the other data [9]. Thus, in a situation where the encrypted user's data storage formally withdrawn, the user can open the second password, wherein all important data that are available at present the password will remain hidden.
- change passwords and key files for the TrueCrypt software volume without loss of encrypted data;
- create an encrypted virtual drive;
- ability to use TrueCrypt software on PC as a normal user.

TrueCrypt practical use for storage devices protection (see Fig. 1):

1. Removable storage device (external HDD or flash card) is to be divided into two partition [2]. The size of the first partition is determined by TrueCrypt size and makes 2-5 Mb.
2. Copy a TrueCrypt portable variant into the first partition.
3. Start TrueCrypt and implement the encryption of the second partition.
4. Mount the encrypted partition onto a Disk.
5. Perform the information transfer onto a Disk.
6. Umount Disk into the encrypted partition.

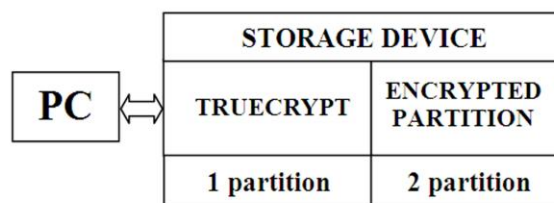


Fig.1. Structure of the encrypted storage device

Comparative analysis of the PC performance with using the TrueCrypt software

Pictures 1-3 show the results of an experimental study of the effect on PC performance when running encryption TrueCrypt software using PC stationary and its mobile version (Laptop) [10].

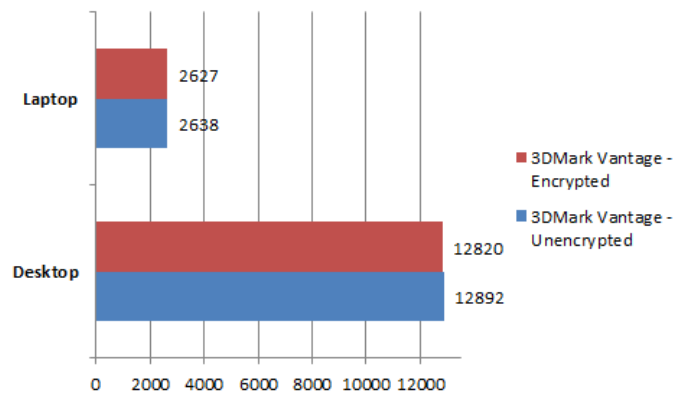


Fig. 1. Comparative performance PC video adapters.

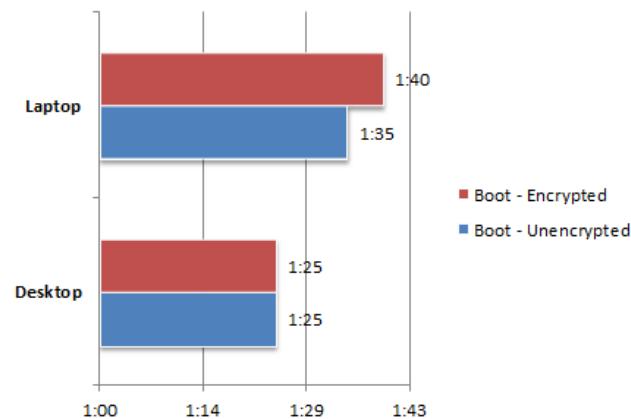


Fig. 2. Load time OS analysis with/without using Truecrypt software data encryption.

As seen from the diagrams shown in Picture 1 and Picture 2, the performance of your PC video card is not reduced, and the boot time is increased by Laptop versions using SDD.

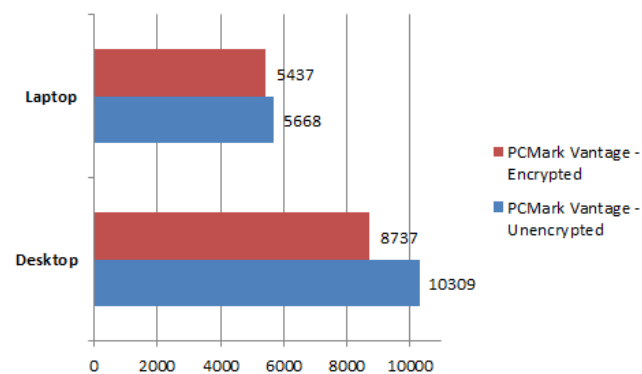


Fig. 3. Comparative analysis of the PC performance with using PCMark.

As seen from the diagrams shown in Picture 3, there is a drop in performance version of Laptop PCs with SSD (-15%). At the same time, the initial speed of SSDs is so high that they still outperform PC HDD, lost in the PCMark only 4%.

Comparative tests were carried out on the PC the following configurations: PC laptop performance (Laptop) - AMD Phenom II X4 905 (2.5 GHz), 6GB DDR3 1600 MHz, Radeon HD6870 OC 1GB DDR5, 120GB RunCore Pro V 2.5 "SATA III SSD; Stationary PCs - Intel Core2 Quad CPU Q9000 @ 2.00 GHz, 6 GB of RAM DDR2, ATI Mobility Radeon HD 4650, Seagate Momentus XT 500GB HDD.

Conclusions and prospects for further research in this direction

Currently, the development of encryption TrueCrypt software was further developed in the form of individual cryptographic software: CipherShed [11] and VeraCrypt [12]. The basis for the collection of the original code base TrueCrypt software. This cryptographic software successfully developed and supported. Moreover, they fixed some bugs encryption TrueCrypt software [13].

It should also be noted that the formats of cryptocontainers VeraCrypt software become incompatible with TrueCrypt software. For comparison, cryptocontainers CipherShed software compatible with TrueCrypt software.

Independent audit considered encryption TrueCrypt software, conducted by iSEC Partners showed that its code was found in a total of 11 members of security threats. 4 of them have an average level of danger, another 4 - low, remaining in principle, difficult to classify due to their insignificance. More detailed results of the audit were published in a document posted on site - opencryptoaudit.org [14, 15].

10-year author's experience in the encryption operation with TrueCrypt software to protect the data storage suggests perfection, reliability and stability of the examination on. Thus, the use of encryption TrueCrypt software considered and its modifications, is the most effective measure that prevents leakage of confidential user information placed on your PC and external data storage.

References

1. Methods and tools for the protection of information in computer systems: Proc. benefits for students. Executive. Proc. institutions / Pavel Borisovich Horev. - M.: Publishing center "Academy", 2005. - 360 c.
2. Hidden partition. [Electronic resource]. // Access: <http://cyberhound.ru/windows/zaschita/skrytye-razdely-zhestkogo-diska.html>. - Title from the screen.
3. Creation of encrypted archives. [Electronic resource] // Access: <https://the-bosha.ru/2010/06/19/zashifrovannye-archivi-v-linux/>. - Title from the screen.
4. How to prevent access to the folder or file. [Electronic resource] // Access: http://www.vashmirpc.ru/publ/sistema/kak_zapretit_dostup_k_papke_ili_fajlu/2-1-0-75. - Title from the screen.
5. The facts: how many write cycles at the stick? [Electronic resource] // Access: <http://hi-news.ru/periferiya/fakty-skolko-ciklov-zapisi-u-fleshki.html>. - Title from the screen.
6. Protecting information on removable disks. [Electronic resource] // Access: <http://wd-x.ru/protect-info-on-removable-drives/>. - Title from the screen.
7. Features of national conspiracy: encrypt drives using Luks / dm-crypt, Truecrypt and Encfs. [Electronic resource] // Access: <https://xakep.ru/2011/03/14/54794/>. - Title from the screen.
8. «TrueCrypt» - program for encryption. [Electronic resource] // Access: <https://test.ru/tools/truecrypt/>. - Title from the screen.
9. Deniable encryption. [Electronic resource] // Access: https://ru.wikipedia.org/wiki/Отрицаемое_шифрование. - Title from the screen.
10. What is the Performance Impact of System Encryption With TrueCrypt. [Electronic resource]. // Access: <http://www.digitalcitizen.life/what-performance-impact-system-encryption-truecrypt>. - Title from the screen.
11. CipherShed. [Electronic resource] // Access: <https://ciphershed.org>. - Title from the screen.

12. Veracrypt: improved version of Truecrypt. [Electronic resource] // Access: <https://xakep.ru/2014/10/14/veracrypt/>. - Title from the screen.
13. VeraCrypt. [Electronic resource] // Access: - <https://veracrypt.codeplex.com>. - Title from the screen.
14. The audit source TrueCrypt: serious threats have been identified. [Electronic resource] // Access: <http://www.3dnews.ru/818668/print>. - Title from the screen.
15. The second phase of the audit is completed TrueCrypt: four vulnerabilities identified. [Electronic resource] // Access: <http://webware.biz/?p=3370>. - Title from the screen.

ПРОГРАМНО-ТЕХНІЧНІ АСПЕКТИ КРИПТОГРАФІЧНОГО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ

О.В. Задерейко, О.В. Троянський

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

Захист носіїв інформації є сукупністю проблем, тісно зв'язаних з використанням криптографічних програмних засобів різного призначення. Для вирішення цього завдання застосовується безкоштовне, кроссплатформене криптографічне програмне забезпечення (ПО) TrueCrypt з відкритим кодом, що дозволяє здійснювати шифрування даних «на льоту». Виконаний аналіз можливостей ПО TrueCrypt. Розроблений алгоритм практичного вживання ПО TrueCrypt для захисту носіїв інформації. Приведено порівняльний аналіз продуктивності персонального комп'ютера з/без використанням ПО TrueCrypt, який показав фактичну відсутність зниження продуктивності. Незалежний аудит розглянутого криптографічного ПО TrueCrypt не виявив найвищих погроз його уразливості. Особистий 10-ти річний досвід авторів з експлуатації ПО TrueCrypt для захисту носіїв інформації дозволяє затверджувати бездоганність, надійність і стійкість його роботи.

Показано, що вживання криптографічного ПО TrueCrypt і його подальших модифікацій, є найбільш ефективною мірою, яка дозволяє запобігти витоку конфіденційної інформації користувачів, розміщеної на персональних комп'ютерах та зовнішніх носіях.

Ключові слова: криптографічний захист, криптографічне програмне забезпечення, TrueCrypt, криптоконтейнер, захист носіїв інформації, шифрування даних «на льоту».

ПРОГРАММНО-ТЕХНИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ НОСИТЕЛЕЙ ИНФОРМАЦИИ

А.В. Задерейко, А.В. Троянский

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

Защита носителей информации представляет собой совокупность проблем, тесно связанных с использованием криптографических программных средств различного назначения. Для решения этой задачи применяется бесплатное, кроссплатформенное криптографическое программное обеспечение (ПО) TrueCrypt с открытым исходным кодом, позволяющее осуществлять шифрование данных «на лету». Выполнен анализ возможностей ПО TrueCrypt. Разработан алгоритм практического применения ПО TrueCrypt для защиты носителей информации. Приведен сравнительный анализ производительности персонального компьютера с/без применением ПО TrueCrypt, который показал фактическое отсутствие снижения производительности. Независимый аудит рассмотренного криптографического ПО TrueCrypt не выявил наивысших угроз его уязвимости. Личный 10-ти летний опыт авторов в эксплуатации ПО TrueCrypt для защиты носителей информации позволяет утверждать безупречность, надежность и устойчивость его работы.

Показано, что применение криптографического ПО TrueCrypt и его последующих модификаций, является наиболее эффективной мерой, которая позволяет предотвратить утечки конфиденциальной информации пользователей, размещенной на персональных компьютерах и внешних носителях.

Ключевые слова: криптографическая защита, криптографическое программное обеспечение, TrueCrypt, криптоконтейнер, защита носителей информации, шифрование данных «на лету».

ОЦІНЮВАННЯ ПОКАЗНИКІВ ПРИЗНАЧЕННЯ НЕЛІНІЙНИХ РАДІОЛОКАТОРІВ

Ю.Ф. Зінковський, М.І. Прокоф'єв

Національний технічний університет України «Київський політехнічний інститут»
просп. Перемоги, Київ, 03056, Україна; e-mail: krasan@ukr.net

Для сертифікації/експертизи нелінійних радіолокаторів в якості єдиного імітатора закладного пристрою запропоновано двозаходову плоску спіральну антену з узгодженим нелінійним навантаженням, оскільки він задовольняє наступним вимогам: широкосмуговий; має еліптичну поляризацію; конструктивно здатний до високої відтворюваності параметрів; забезпечує спрямовану передачу потужності; володіє високим коефіцієнтом корисної дії; забезпечує заданий рівень узгодження з нелінійним елементом. Наведено приклад оцінювання значень параметра максимальна дальність дії нелінійних радіолокаторів.

Ключові слова: нелінійна радіолокація, імітатор закладного пристрою, широкосмугова антена.

Вступ

Технологія нелінійної радіолокації в сфері технічного захисту інформації (ТЗІ) застосовується для виявлення, локалізації та ідентифікації радіоелектронних закладних пристроїв (ЗП), призначених для несанкціонованого отримання (перехоплення) інформації. Такі ЗП мають у своєму складі напівпровідникову елементну базу з нелінійними характеристиками (мікросхеми, транзистори, діоди тощо), здатну змінювати спектральний склад інформаційного сигналу [1]. Тому під час проведення пошуку ЗП їх слід розглядати як джерела перевипромінювання зонduючого сигналу (ЗС), в результаті чого виникають нові спектральні складові – гармоніки, кратні частоти ЗС або комбінаційні частоти. При цьому, якщо в досліджуваному середовищі присутні утворення виду «метал-окисел-метал» (МОМ-структури), окислені контакти, погано спаяні або зварені з'єднання, то вони теж діють як нелінійні розсіювачі (НРс) [2].

Типовий метод нелінійної радіолокації включає прийом сигналів відгуку від ЗП на другій або на другій і третій гармоніках зонduючого сигналу, обробку та оцінювання їх рівнів для виявлення та локалізації ЗП оператором. Це обумовлено тим, що зазвичай ЗП, які містять напівпровідникові компоненти, мають на другій гармоніці рівень сигналу відгуку на 20-30 дБ більший, ніж на третій гармоніці. Для розсіювачів контактного типу (МОМ-структур), як правило, справедливим є зворотнє співвідношення.

У серійних нелінійних радіолокаторах (НР) застосовують ЗС в діапазоні частот, що наближений до 900 МГц. Такий вибір ЗС пов'язаний з компромісом у вирішенні наступного протиріччя: з одного боку, чим нижче частота ЗС, тим краще його проникаюча здатність в середовище, в якому потай можуть бути змонтовані ЗП; з іншого боку – чим вище частота випромінювання, тим вужча діаграма спрямованості антени НР при фіксованих геометричних розмірах, а значить велика щільність потоку потужності ЗС.

Максимальна відстань (пошукова відстань), на якій виявлення ЗП ефективне, як правило, обмежена значенням 0,7 м. Глибина виявлення ЗП у досліджуваному середовищі може досягати декількох десятків сантиметрів. Наприклад, НР серії

«Циклон» виявляють напівпровідникові компоненти в залізобетонних стінах товщиною до 0,3 м, цегляних і дерев'яних – до 0,6 м [3].

НР, що обладнані тільки антенами з лінійною поляризацією, мають можливість виявляти ЗП при сканування поверхні, як мінімум, у двох напрямках, а за наявності у НР випромінюючої антени з круговою поляризацією пошук ЗП здійснюють незалежно від розташування НР.

Поширена технологія нелінійної радіолокації, яка пов'язана з імпульсним випромінюванням ЗС. Відомо, що виявляюча здатність НР зростає зі збільшенням потужності ЗС. Однак, діючі санітарні норми і правила експлуатації обмежують дозволені рівні потужності ЗС НВЧ діапазону. Застосування імпульсного НР дозволяє, з одного боку, реалізувати високі рівні потужності ЗС і, отже, підвищити ефективність виявлення, а з іншого – істотно знизити середню потужність випромінювання до величини, що задовольняє санітарним нормам. Так при імпульсній потужності 150 Вт і шпаруватості 1500, середня потужність випромінювання НР складе 100 мВт, а рівень задніх пелюсток діаграми спрямованості випромінюючої антенної системи буде послаблений відносно головної пелюстки на 20 дБ. Чутливість приймального тракту НР не перевищує мінус 160 дБВт. Для приймальної антени частотного діапазону близького до 1800 МГц (для приймання НР другої гармоніки частоти ЗС) з діаграмою спрямованості не більше 30° і коефіцієнтом підсилення близько 10 дБ "дальня" зона починається від 2 м.

Постановка задачі

При сертифікації/експертизі (СЕ) нелінійних радіолокаторів раціональними є їх випробування за показниками призначення методом порівняння. Наявність взаємних зв'язків між показниками призначення НР в значній мірі полегшує і спрощує проведення СЕ НР. Суть методу порівняння полягає в тому, що один з типів НР приймають за «еталон» і по відношенню до нього проводять порівняння за показниками призначення решти видів НР. У результаті проведення серії випробувань виявляються зразки НР, що мають значні відхилення значень показників призначення від середніх значень [4, 5].

Користуючись даними, отриманими у результаті таких випробувань, можна визначити «середні» значення параметрів щодо ефективності використання НР, їх розкид, криву розподілу відхилень від «еталона», а також виявити ті НР, які слід піддати більш детальному дослідженню у разі сумірних з допусками відхилень.

Для оцінки НР раціональним є врахування взаємних зв'язків між показниками призначення. Такі показники НР як дальність виявлення (I) ЗП і роздільна здатність (II) НР при виявленні ЗП мають високу взаємозалежність. Показники призначення НР, щодо якого проводиться СЕ, відповідають «еталону», якщо координати, що визначають значення показників I і II, потрапляють в заштриховану область (рис. 1).

Процедура СЕ включає проведення оцінки показника I. Якщо отримане значення лежить в межах інтервалу $\pm a_I$, то НР вважається «прийнятим» і перевірка по другому показнику не проводиться. Якщо при зміні показника I отримується значення, що лежить за межами $\pm a_I$, але в межах $\pm b_I$, то проводиться перевірка по показнику II. Якщо при зміні показника I розкид значень параметра більший ніж $\pm b_I$, то СЕ НР не є успішною.

Визначення меж $\pm a$, $\pm b$ проводиться, якщо відомі допуски по показникам I і II та величини взаємних зв'язків. Наявність взаємних зв'язків між показниками I і II призводить до того, що координати точки, що належать I і II, будуть охоплювати не весь прямокутник $klmn$, а смугу, що відтинається по осях відрізками. Таким чином,

$a_I = 3(\sigma_I - \sigma_{I,II})$, $b_I = 3\sigma_I$, якщо оцінювання виконуються за першим показником, і $a_{II} = 3(\sigma_{II} - \sigma_{II,I})$, $b_{II} = 3\sigma_{II}$ при оцінюванні за другим показником, де σ_I , σ_{II} , $\sigma_{I,II}$, $\sigma_{II,I}$ – дисперсії для показників I, II та їх взаємодії.

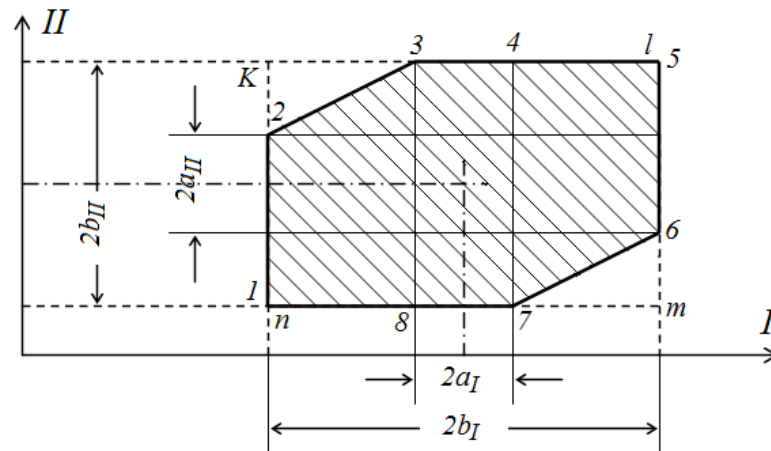


Рис. 1. Взаємна залежність між значеннями показників призначення НР: I – дальність виявлення ЗП, II – роздільна здатність НР

Виграш, що має місце в цьому випадку, визначається співвідношенням площ, які визначають на рис.1 ступінь взаємної залежності параметрів:

$$\eta = \frac{S_{8,3,4,7}}{S_{1,2,3,5,6,7}} = \frac{(\sigma_I - \sigma_{I,II})\sigma_{II,I}}{\sigma_I\sigma_{II} - (\sigma_{II} - \sigma_{II,I})(\sigma_I - \sigma_{I,II})}. \text{ В окремому випадку, при } \sigma_I = \sigma_{II} = \sigma_0 \text{ та}$$

$$\sigma_{I,II} = \sigma_{II,I} = \sigma_K: \eta = \frac{(\sigma_0 - \sigma_K)\sigma_K}{\sigma_0^2 - (\sigma_0 - \sigma_K)^2} < 30\%. \text{ Методики визначення значень показників}$$

призначення (дальність дії, роздільна здатність, вибірковість тощо) показані у [6].

Таким чином, враховуючи вище зазначене, для СЕ нелінійних радіолокаторів необхідною є оцінка значень показників призначення за вибіркою різних типів НР. Як приклад, наводимо оцінку значень показника НР - максимальна відстань виявлення нелінійних розсіювачів (НРс).

Основна частина

Введемо співвідношення, що дозволяє оцінити за непрямыми вимірами максимальну відстань виявлення НРс нелінійним радіолокатором [6...8].

Нехай відстань між антеною передавача НР та НРс буде рівною R_1 , а між НРс та антеною приймача НР – R_2 . Амплітуда електрорушійної сили (ЕРС), наведена полем зонduючого сигналу, дорівнює

$$E_0 = h_D \cdot \sqrt{\frac{P_T \cdot G_T \cdot W}{2\pi \cdot R_1^2}}, \quad (1)$$

де h_D – діюча довжина розсіювача; P_T , G_T – потужність передавача НР і коефіцієнт спрямованої дії його антени; $W = 120\pi$ – хвильовий опір вільного простору.

Потужність сигналу, перевипромінена НРс на k -й гармоніці становить

$$P_{BC_k} = I_k^2 \cdot R_{\Sigma k} = \frac{E_0^2 \cdot R_{\Sigma k}}{(R_{\Sigma k} + Z_{Дk})^2}, \quad (2)$$

де I_k – амплітуда струму k -ї гармоніки, викликана дією ЕРС E_0 , $Z_{Дk}$ – сумарний опір нелінійних елементів НРс за k -ю гармонікою струму, що протікає через них; $R_{\Sigma k}$ – опір випромінювання НРс на k -й гармоніці.

При підстановці (1) в (2) одержимо

$$P_{BC_k} = \frac{\lambda^2 \cdot P_T \cdot G_T \cdot W \cdot R_{\Sigma k}}{2\pi^3 \cdot R_1^2 \cdot (R_{\Sigma k} + Z_{Дk})^2}. \quad (3)$$

Потужність сигналу на виході антени приймача НР за умови ідеального її узгодження з приймачем на k -й гармоніці дорівнює:

$$P_{ПРk} = \frac{P_{BC_k} \cdot G_{ПР} \cdot \lambda^2}{2 \cdot k^2 (4\pi)^2 \cdot R_2^2}, \quad (4)$$

де $G_{ПР}$ – коефіцієнт спрямованої дії антени приймача НР на k -й гармоніці.

При підстановці (4) в (3) одержимо рівняння для визначення добутку відстаней між передавачем НР та НРс і приймачем НР та НРс, при яких здійснюється надійне приймання НР сигналу відгуку на k -й гармоніці:

$$R_1 \cdot R_2 = \sqrt{\frac{P_T \cdot G_T \cdot G_{ПР} \cdot W \cdot R_{\Sigma k} \cdot \lambda^4}{64 \cdot \pi^5 \cdot k^2 \cdot P_{ПРk} \cdot (R_{\Sigma k} + Z_{Дk})^2}}. \quad (5)$$

Розрахунок за (5) передбачає використання у якості НРс для оцінювання показників НР єдиного імітатора ЗП. Штатний калібрувальний розсіювач, відносно якого виконується налаштування в «польових» умовах конкретного НР, у більшості випадків є резонансним та налаштованим на частоту ЗС НР. Таким чином, він ефективно поглинає енергію зондуючого сигналу певного НР і перевипромінює достатньо потужні за рівнем продукти нелінійних перетворень на 2/3 гармоніках у порівнянні з випромінюваннями вузькосмугових сторонніх джерел та спектральних складових відгуків МОМ-структур. Оскільки робоча частота ЗС для різних типів НР лежить у широкому діапазоні частот (600...1000) МГц, то штатні резонансні імітатори НРс по різному поглинатимуть однаковий за потужністю зондуючий сигнал від різних НР. Таким чином, для об'єктивного порівняння єдиний імітатор НРс повинен задовольняти наступним вимогам: бути широкосмуговим; мати кругову або еліптичну поляризацію; конструктивно здатним до високої відтворюваності параметрів; забезпечувати спрямовану передачу потужності; мати високий коефіцієнт корисної дії (ККД); забезпечувати заданий рівень узгодження з нелінійним навантаженням.

У якості антенних структур імітатора НРс перспективними є спіральні антени, оскільки вони широкосмугові та мають еліптичну поляризацію [9].

Для конструювання плоских спіральних антен (ПСА) використовують спіралі двох видів: рівнокутних логарифмічних і арифметичних (архімедових). Гілки спіралей можуть бути виготовлені як провідники, розташовані на діелектричній основі, або як прорізи у провідній площині. Зазвичай плоскі спіралі мають дві гілки і залежно від фазових співвідношень в точці збудження можуть випромінювати в двох режимах:

осьовому (направленому) і ненаправленому. Якщо дві гілки спіралі збуджуються в протифазі, то виникає режим осьового випромінювання, при якому головна пелюстка діаграми спрямованості розташована уздовж осі спіралі. Режим ненаправленого випромінювання, при якому поле максимальне в площині спіралі, має місце при синфазному збудженні її гілок.

Принцип роботи плоскої антени, виготовленої як архімедова спіраль, базується на твердженні, що її випромінювання визначається в основному тим витком, де струми в суміжних елементах спіралі майже синфазні. За межами основного випромінюючого витка існують додаткові витки, конструктивні параметри яких кратні параметрам основного. Однак експериментальні дані показують, що ці смужки випромінюють лише малу частину енергії. При зміні довжини хвилі основний випромінюючий виток автоматично переміщується уздовж радіуса спіралі, зберігаючи постійність своєї електричної довжини.

Спіральні антени з коефіцієнтом перекриття по частоті від 1,5 до 10 дозволяють формувати діаграми односпрямовані (ДС) шириною ($90^\circ \dots 180^\circ$) з коефіцієнтом спрямованої дії (КСД) (2...8).

Розглянемо широкопasmовий імітатор закладного пристрою, в якості антенної структури якого є двозаходова ПСА з нелінійним навантаженням, розрахована на діапазон частот 0,8...3 ГГц. Досліджуємо двозаходову ПСА з максимальним радіусом 26 мм, виконану з фольгованого текстоліту і навантажену на діод типу КД-522А, що під'єднаний до спіралей в точках А і В (рис. 2).

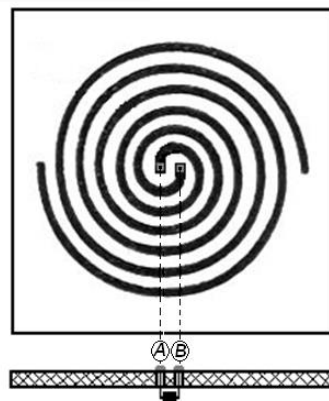


Рис. 2. Імітатор НРс на базі плоскої двозаходової спіральної антени

Геометричні параметри випромінюючої структури: кількість входів — 2; початковий радіус 22...26 мм; кількість витків 2...3. У смузі частот 0,8...3 ГГц діаграма спрямованості зазнає змін, про що свідчать результати розрахунків на рис. 3,4. Коефіцієнт спрямованої дії на частоті 1 ГГц становить (6,5...2,5) дБ при ширині головної пелюстки ДС ($90^\circ \dots 120^\circ$).

КСД на частоті 2 ГГц становить (2,0...0,5) дБ при ширині головної пелюстки ДС ($120^\circ \dots 160^\circ$). На частотах понад 2 ГГц спостерігається зниження КСД, обумовлене розширенням головної пелюстки ДС.

У табл. 1 для п'яти різних типів серійних НР (y_1 — «ОНЕГА 3»; y_2 — «NR 900М»; y_3 — «NR 900Е»; y_4 — «РОДНИК 23»; y_5 — «ЦИКЛОН М1А») наведені результати розрахунків за (5) (при $R_1 = R_2 = R$) максимальної відстані виявлення імітатора НРс на базі двозаходової ПСА із узгодженим нелінійним перетворювачем (діод КД522А). У табл. 2, для тих же типів НР наведені результати експериментальних досліджень з визначення максимальної відстані виявлення зразків імітатора НРс на базі двозаходової ПСА з узгодженим у навантаженні діодом КД522А (вимірювання проводились у

площині, перпендикулярній основній площині досліджуваних зразків ПСА).

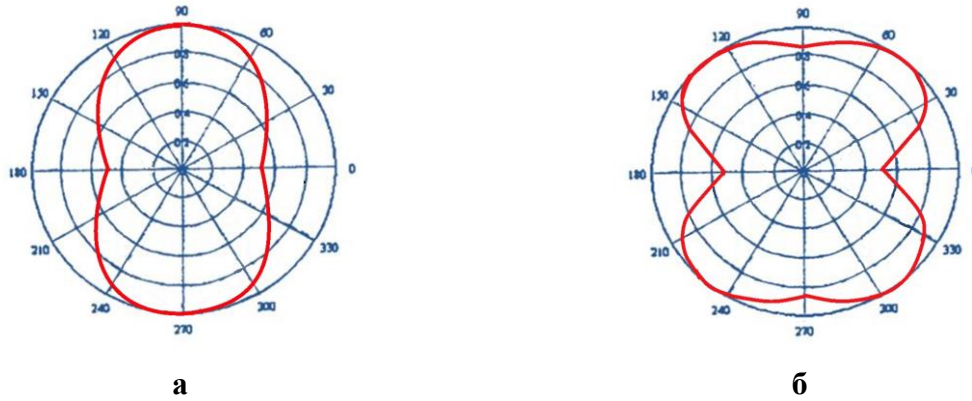


Рис. 3. ДС ПСА, розрахована в наближенні заданого струму для частоти: а – 1 ГГц; б - 2 ГГц

Таблиця 1.

Розраховані значення максимальної відстані виявлення широкосмугового імітатора ЗП

Досліджуваний пристрій	Розрахована максимальна відстань виявлення об'єкта для різних НР, м					Середнє значення
	y_1	y_2	y_3	y_4	y_5	
НРс на базі ПСА	1,91	2,17	2,08	1,86	2,24	2,05

Таблиця 2.

Експериментальні значення максимальної відстані виявлення зразків імітатора ЗП

Досліджуваний зразок, на базі ПСА	Максимальна відстань виявлення об'єкта різними НР, м					Середні зн-ня по імітаторам НРс
	y_1	y_2	y_3	y_4	y_5	
Зразок №1	1,73	1,80	1,76	1,62	2,00	1,78
Зразок №2	1,68	1,76	1,83	1,59	2,05	1,78
Зразок №3	1,62	1,82	1,85	1,66	1,98	1,79
Зразок №4	1,65	1,73	1,74	1,71	1,96	1,76
Зразок №5	1,66	1,82	1,71	1,70	1,94	1,77
Зразок №6	1,71	1,75	1,73	1,57	2,03	1,76
Зразок №7	1,74	1,87	1,84	1,63	1,91	1,80
Зразок №8	1,69	1,79	1,75	1,65	1,96	1,77
Середні зн-ня для НР	1,69	1,79	1,78	1,64	1,98	

Дослідження максимальної відстані виявлення імітаторів НРс на базі двозаходової ПСА з узгодженим нелінійним навантаженням проводилися для восьми зразків імітаторів ЗП з метою перевірки якості відтворювання їх параметрів (табл. 2).

За результатами експериментальних досліджень (табл. 2) на рис. 5 представлена кумулятивна функція розподілу максимальної відстані виявлення розробленого імітатора НРс серійними НР [10]. З рисунку представленої кумулятивної функції можна зробити висновок, що закон розподілу з високою довірчою вірогідністю є нормальним.

Перевірка гіпотези щодо виду функції розподілу за критерієм Шапіро-Уїлка згідно ISO 5479-97 теж підтверджує, що розподіл у вибірці є нормальним і не відхиляється від нього при рівні значимості $\alpha = 0,05$.

Нормальний закон розподілу та мінімальні розходження середніх значень максимальної відстані виявлення для різних зразків ширококутових імітаторів НРс (відповідність критеріям Фішера за довірчої ймовірності 99,8 % [10]) свідчить про високу якість відтворення параметрів імітаторів НРс на базі двозаходової ПСА з узгодженим нелінійним навантаженням, а тому їх можна вважати за еталонні.

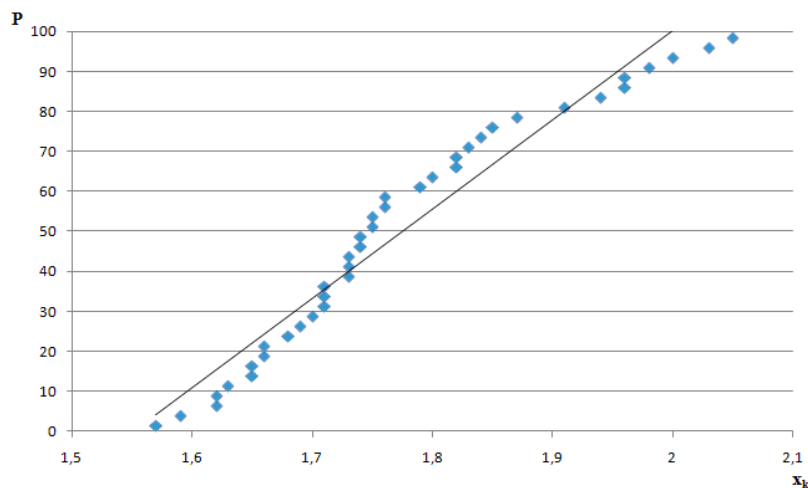


Рис. 4. Кумулятивна функція P розподілу значень максимальної відстані виявлення імітатора ЗП серійними нелінійними радіолокаторами (x_k – експериментально виміряні значення)

Розбіжність результатів отриманих шляхом розрахунків та натурального експерименту можна пояснити впливом на розраховані значення похибки непрямих вимірювань δ_1 , а для експериментально отриманих значень похибкою:

- δ_2 , обумовленою невисоким рівнем відношення сигнал/шум на вході приймачів НР (енергетична похибка);
- δ_3 , через недосконалість екранування приймачів НР від зовнішніх і внутрішніх завад (похибка недостатнього екранування);
- δ_4 впливу перевідбиття від землі та навколишніх предметів вимірювального майданчика (похибка перевідбиття).

Повна похибка непрямих вимірювань показника призначення Y , значення якого залежить від прямовимірюваних величин $x_1, x_2, x_3, \dots$, $Y = f(x_1, x_2, x_3, \dots)$, дорівнює

$\delta_1 = \sqrt{a_{x_1}^2 \Delta x_1^2 + a_{x_2}^2 \Delta x_2^2 + a_{x_3}^2 \Delta x_3^2}$, де $\Delta x_1 = \sqrt{\Delta x_1^2 + \theta_{x_1}^2}$, $\Delta x_2 = \sqrt{\Delta x_2^2 + \theta_{x_2}^2}$, $\Delta x_3 = \sqrt{\Delta x_3^2 + \theta_{x_3}^2}$ – повні похибки аргументів; $\theta_{x_1}, \theta_{x_2}, \theta_{x_3}$ – приладові похибки аргументів функцій, що є незалежними випадковими величинами; $\Delta x_1, \Delta x_2, \Delta x_3$ – випадкові похибки аргументів функцій, що не залежать від приладових похибок; $a_{x_1} = \left. \frac{\partial f}{\partial x_1} \right|_{\overline{x_1}, \overline{x_2}, \overline{x_3}}$, $a_{x_2} = \left. \frac{\partial f}{\partial x_2} \right|_{\overline{x_1}, \overline{x_2}, \overline{x_3}}$,

$a_{x_3} = \left. \frac{\partial f}{\partial x_3} \right|_{\overline{x_1}, \overline{x_2}, \overline{x_3}}$ – часткові похідні функцій, що розраховані в точці $(\overline{x_1}, \overline{x_2}, \overline{x_3})$. Вони

мають сенс вагових множників, бо показують, з якою вагою випадкові або приладові похибки аргументів функцій входять відповідно у випадкову та приладову похибки самої функції (в нашому випадку $\delta_1 \leq 10\%$).

Систематичні складові експериментальних похибок можуть бути апроксимовані залежностями наступного виду:

$$\delta_2 = m_1 \left[\frac{P_{\text{пр}} R^2 \lambda^2}{P_k S_k S_{\text{пр}}} \sqrt{\left(\frac{P_k S_k S_{\text{пр}}}{P_{\text{пр}} R^2 \lambda^2} + \gamma \right) \frac{\Delta f}{F}} \right], \quad \delta_3 = m_2 \left[\frac{A_{\text{пр}} G_k \lambda^2}{\pi R^2 S_k} \sqrt{\left(\frac{2\pi^2 S_k R^2}{A_{\text{пр}} G_k \lambda^2} + \gamma \right) \frac{\Delta f}{F}} \right],$$

$$\delta_4 = m_3 \left(\frac{4S_\sigma}{4\pi S_\sigma + R^2} \right),$$

де $P_k G_k$ – енергопотенціал джерела перевипромінювання (НРс) на k -й гармоніці; $P_{\text{пр}}$ – чутливість приймача НР; $S_k, S_{\text{пр}}$ – відповідно ефективні площі антен ПСА з НРс на k -й гармоніці та приймача на частоті сигналу, що приймається НР; $\Delta f, F$ – ширина смуги частот, що займає випромінюваний НРс сигнал, і ширина смуги пропускання приймача НР відповідно; γ – коефіцієнт прямокутності смуги пропускання приймача; $A_{\text{пр}}$ – площа екранованої поверхні корпусу приймача НР, що схильна до дії радіозавад; S_σ – середнє значення ефективної поверхні розсіювання (ЕПР) «землі» і фона на частоті приймання; $m_1 \div m_3$ – масштабні коефіцієнти, значення яких підбирається дослідним шляхом за результатами метрологічних експериментів, що передбачають створення нормованих електромагнітних полів, вимірювання потужності випромінювань та оцінку відповідних похибок. Загальний вплив похибок $\delta_2, \delta_3, \delta_4$ не перевищує 20%.

Таким чином, середнє значення максимальної відстані виявлення імітатора ЗП, розраховане за непрямыми вимірами, становитиме $2,05 \pm 0,20$ м, а отримане експериментально – $1,77 \pm 0,35$ м.

Висновок

При сертифікації та експертизі таких засобі ТЗІ загального призначення як нелінійні радіолокатори доцільним є їх випробування за показниками призначення методом порівняння. Наявність взаємних зв'язків між показниками призначення в значній мірі полегшує і спрощує проведення випробувань НР. Оцінювання значень показників призначення НР необхідно проводити за результатами порівняння різних типів НР. Для СЕ НР в якості єдиного імітатора ЗП доцільно використати двозаходову плоску спіральну антену (ПСА) з узгодженим нелінійним навантаженням, оскільки він задовольняє наступним вимогам: ширококутовий; має еліптичну поляризацію; конструктивно здатний до високої відтворюваності параметрів; забезпечує спрямовану передачу потужності; має високим коефіцієнт корисної дії; забезпечує заданий рівень узгодження з НРс. Запропонований імітатор завдяки ширококутовості та еліптичній поляризації за рахунок нелінійних перетворень перевипромінює досить значні рівні сигналів на 2/3 гармоніках зондуємого сигналу у порівнянні з резонансними калібрувальними розсіювачами. Це дає можливість навіть у польових умовах чітко калібрувати НР на досить великих відстанях при будь-якій просторовій орієнтації. Розбіжність результатів оцінювання максимальної відстані виявлення ширококутового імітатора, отриманих шляхом розрахунків за непрямыми вимірами та натурального експерименту, можна пояснити впливом похибки непрямих вимірювань, а

для експериментально отриманих значень – похибками, обумовленими недостатнім екрануванням та перевідбиттям (енергетичними).

Список литературы

1. Вернигоров, Н.С. Практические применения нелинейного радиолокатора / Н. С. Вернигоров // Безопасность от А до Я. – 1998. – № 2-3. – С. 14–15.
2. Беляев, В.В. Состояние и перспективы развития нелинейной радиолокации / В.В. Беляев, А.Т. Маюнов, С.Н. Разиньков // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. – 2002. – № 6. – С. 59–78.
3. Хорошко, В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков – К. : «Юниор», 2003. – 504с.
4. Калабухов, В. А. Нелинейная радиолокация: принципы сравнения / В. А. Калабухов, Д. В. Ткачев // Специальная техника. – 2001. – № 2. – С. 28.
5. Вернигоров, Н.С. К вопросу о принципе сравнения в нелинейной радиолокации / Н.С. Вернигоров, Т. В. Кузнецов // ИНФОРМОСТ Радиоэлектроника и Телекоммуникации. – 2002. – № 3(21). – С. 7–14.
6. НД ТЗІ 1.4.–002–08 «Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань».
7. Авдеев, В.Б. Методический аппарат для оценки эффективности средств нелинейной радиолокации и противорадиолокации / В. Б. Авдеев, С. Н. Паньчев, Д. В. Сенькевич // Вестник Воронежского государственного технического университета. – 2007. – Т. 3. – № 4. – С. 115–119.
8. Вернигоров, Н.С. Влияние антенно-фидерного тракта нелинейного объекта на дальность обнаружения в нелинейной локации / Н. С. Вернигоров, В. Б. Харин // Радиотехника и электроника. – 1997. – Т. 42. – № 12. – С. 1267.
9. Юрцев, О.А. Спиральные антенны / О. А. Юрцев, А. В. Рунов, А. Н. Казарин. – М. : Сов. радио, 1974. – 224 с.
10. Радченко, С.Г. Математическое моделирование технологических процессов в машиностроении. – К. : ЗАО «Укрспецмонтажпроект», 1998. – 274 с.

ОЦЕНКА ПОКАЗАТЕЛЕЙ НАЗНАЧЕНИЕ НЕЛИНЕЙНЫХ РАДИОЛОКАТОРА

Ю. Ф. Зинковский, М. И. Прокофьев

Национальный технический университет Украины «Киевский политехнический институт»
просп. Победы, Киев, 03056, Украина; e-mail: krasan@ukr.net

Для сертификации/экспертизы нелинейных радиолокаторов в качестве единственного имитатора закладного устройства предложено двухзаходная плоскую спиральную антенну согласованную нелинейной нагрузкой, поскольку он удовлетворяет следующим требованиям: широкополосный; имеет эллиптическую поляризацию; конструктивно способен к высокой воспроизводимости параметров; обеспечивает направленную передачу мощности; обладает высоким коэффициентом полезного действия; обеспечивает заданный уровень согласования с нелинейным элементом. Приведен пример оценки значений параметра максимальная дальность действия нелинейных радиолокаторов.

Ключевые слова: нелинейная радиолокация, имитатор закладного устройства, широкополосная антенна.

EVALUATION INDICATORS PURPOSE NONLINEAR RADAR

Y.F. Zinkovskiy, M.I. Prokofiev

National Technical University of Ukraine “Kyiv Polytechnic Institute”
Victory Ave., Kyiv, 03056, Ukraine; e-mail: krasan@ukr.net

For nonlinear radar certification/expertise the two-armed plane spiral antenna with matched nonlinear load is proposed as a single simulator of secret intelligence device because it serves the following requirements: broadband; has elliptical polarization; structurally capable of high reproducibility parameters; aimed at providing transmission capacity; has high efficiency; provides a set level of conformity with the nonlinear element. Due to it the normative estimation of the maximum coverage range of the nonlinear radar is made.

Keywords: nonlinear radar, simulator backfill device wideband antenna.

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНО-СИСТЕМНИХ ВЛАСТИВОСТЕЙ ПРОЦЕСУ РЕАЛІЗАЦІЇ ВИМІРЮВАНЬ ЗАДАНОЇ НАДІЙНОСТІ

А.А. Березовський, В.С. Дмитренко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: aberezovskiy@soyus-corp.com

Виділено групу оцінок надійності на кожному етапі здійснення вимірювань, для яких сформовано фактори, що визначають точність та достовірність процесу оцінювання. Досліджено похибки вимірювань, зокрема, системні регулярні та методичні. Побудовано «зони» перерозподілу значущості факторів, які впливають на точність та достовірність вимірювань.

Ключові слова: інформаційні системи, інформаційно-вимірювальні системи, оцінки надійності та достовірності вимірювань, похибки вимірювань.

Вступ

Інформаційні та інформаційно-вимірювальні системи (ІВС) набувають всебічного застосування у всіх сферах діяльності людини: техніці, науці, транспорті, суспільному житті тощо. Від якості (точності) та надійності функціонування цих систем у значній мірі залежить достовірність отриманої за їх допомогою інформації та прийняття на підставі останньої подальших рішень. З огляду на зазначене, дослідження надійності функціонування інформаційних та ІВС набуває першочергового значення. Одним з дієвих та ефективних (з точки зору матеріальних витрат) шляхів розв'язання задачі дослідження якісних характеристик вказаного класу систем є моделювання.

Основна частина

З інформаційно-системної аксіоматики формалізації процесу реалізації вимірювань заданої надійності слід виділити оцінку надійності на кожному етапі здійснення вимірювань (зокрема: фіксація величини, що вимірюється, первинним датчиком; перетворення первинної інформації у вигляді неелектричної фізичної величини в електричний сигнал; передача електричного сигналу з певними параметрами по каналу зв'язку; прийом електричного сигналу з каналу зв'язку, його перетворення та інформаційна обробка, тощо), яка характеризує хід вимірювань з метою з'ясування питань щодо досягнення вимірюваннями необхідних (достовірних) значень, а саме: $ПН_i, i = \overline{1, n}$ (n – число задіяних етапів процесу вимірювань). Крім того слід з'ясувати, наскільки достовірно виконано оцінку. Береться до уваги, що кожний етап процесу вимірювань завершується підтвердженням виконанням вимог стосовно надійності $ПН_{ij} \in [ПН_{ij}]_\gamma, i = \overline{1, n}$ з урахуванням довірального інтервалу значень показників надійності при довірчальній вірогідності γ . Останнє співвідношення має сенс лише в «інформаційній системі координат» j -го етапу

процесу вимірювань, оскільки об'єктом, що підлягає оцінюванню, є результат вимірювань саме на j -му етапі.

Виходячи з цих положень, необхідно враховувати дві групи факторів, що визначають точність та достовірність оцінки значень PH_{ij} . Це фактори, які визначають точність та достовірність оцінки (ТДО) значень PH в «інформаційній системі координат» (ІСК) j -го етапу вимірювань, та фактори, які визначають ТДО в «ІСК» завершального етапу процесу вимірювань. При цьому, факторами першої групи виявляються: ступінь відповідності моделі, за якою здійснюється оцінювання PH , до результату вимірювань на j -му етапі; адекватність, достовірність та точність вихідної (вимірювальної) інформації, що використовується для оцінки PH_{ij} ; адекватність, достовірність та точність метода оцінки PH (припущення метода, точність обчислювальних процедур, точність обробки результатів). До факторів другої групи можна віднести: ступінь відповідності (адекватності) результату j -го етапу вимірювань кінцевому результату вимірювань (завершальному значенню). Причому, для кількісного виразу ролі факторів другої групи можна використати шкалу так званого «інформаційного коефіцієнта адекватності», який пропонується представляти наступним чином: $0 \leq \eta_j \leq 1, j = \overline{1, s}$.

Основними методами дослідження надійності результатів вимірювань на етапах процесу вимірювань є розрахункові методи [1, 2]. Їх реалізація має на увазі використання існуючого в даній предметній області розрахункового апарату та інформації щодо вірогідносних властивостей вихідних величин. Тому в рамках факторів першої групи, які визначають ТДО значень PH_{ij} формуються (за традиційною класифікацією [3]) похибки систематичні та випадкові.

Загальним видом похибок для методів, які використовуються для оцінки PH систем вимірювання, що проектується, виявляються систематичні, регулярні похибки, і ці похибки утворюються через неточність математичного опису процесу вимірювань, спрощенню вихідної фізичної картини інформаційних процесів – тобто являють собою методологічні похибки. Вказаний вид систематичних похибок, що притаманний факторам першої групи, повинен розглядатися лише в тій мірі, в якій можливо виразити відмінність етапного результату процесу вимірювань і тих математичних описів (математичних моделей), які використовуються на конкретному етапі вимірювань для виконання досліджень та розрахунків. В іншому випадку цей вид похибок повинен розглядатися в рамках факторів другої групи.

В числі з розглянутим видом систематичних похибок, методам оцінки PH процесу вимірювань можуть відповідати і інші види методичних похибок. Так, для методів статистичного моделювання властиві методичні похибки, що зумовлені використанням наближених процедур чисельного інтегрування вихідних диференціальних рівнянь, обмеженістю обсягів статистичних випробовувань, наближенням розподілів «вихідних» величин теоретичними функціями розподілу у вигляді відомих законів або розкладів у ряди (наприклад, Грама-Шарл'є та інш.). В рамках факторів першої групи, які визначають ТДО значень PH_{ij} окремих вимірювань, наявними є загальні для всіх методів оцінки надійності, що використовуються, випадкові похибки, які, в свою чергу, породжено неповним представленням про можливий випадковий характер фізичних явищ процесу вимірювання та передачі вимірювальної інформації, обмеженість та різноманітність вихідної статистичної інформації про них. Всі перераховані похибки, так само як і похибки методичного характеру, пов'язані з неточністю математичного опису процесу вимірювань (або апаратних засобів, за допомогою яких здійснюються вимірювання та передається вимірювальна інформація), можуть бути враховані розрахунковим шляхом або за допомогою експертних оцінок.

Аналіз розглянутих систематичних та випадкових похибок, що відносяться до факторів першої групи, і які визначають ТДО $ПН$, дозволяють визначити в «системі координат» j -го етапу вимірювань відповідність вимогам досягнутого рівня надійності (достовірності). Ці вимоги виконано, якщо оцінки $ПН_j \in [НП]_{\gamma}$. Однак, даний аналіз носить методичний характер у тому відношенні, що дає представлення щодо точності обчислення оцінок $ПН_j$ у межах «ІСК», що розглядається. Причому, оскільки розглянуті похибки першої групи є, в певних межах, керованими (зміна кроку інтегрування, збільшення обсягу статистичних випробовувань, варіювання числом експертів, тощо), то в рамках j -ї «системи координат» формується судження щодо виконання вимог відносно надійності.

Точність та достовірність оцінки $ПН_j$ результату здійснення вимірювань на j -му етапі визначаються з урахуванням похибок що відносяться до факторів другої групи. Ці похибки оцінюються інформаційним коефіцієнтом адекватності j -го перетворювача η_j . Причому, оцінка полягає у корегуванні значень довірливої вірогідності, з якою досягнуте на j -му етапі підтвердження процесу вимірювань вимогам по надійності може бути перенесено на наступні етапи $\gamma_{j+1} = \eta_j \cdot \gamma_j$.

На завершальних етапах вимірювального процесу використовуються моделі та методики оцінки досягнутого рівня надійності, адекватні щодо конкретної процедури вимірювань та апаратних засобів її реалізації. Вони обробляють фактичну експериментальну статистичну інформацію про хід процесу вимірювань. В своїх алгоритмах зазначені моделі реалізують накопичення та переробку інформації щодо надійності завершального етапу вимірювань, а також здійснюють оцінювання значень $ПН$ в інтервальній формі, що дозволяє постійно відстежувати міру ТДО.

В аналізі точності та достовірності оцінки $ПН$ певного процесу вимірювань, актуальними є питання: як співвідносяться фактори першої та другої групи, що визначають точність та достовірність $ПН$; які є можливості щодо підвищення точності та достовірності оцінки; як реалізувати витрати на підвищення точності та достовірності оцінювання. З метою формування відповідей на поставлені питання необхідно зіставити «долі недостовірності», які приходяться на фактори першої та другої групи. При цьому необхідно врахувати, що, оскільки міру точності та достовірності по факторах першої групи (інтервал значень, в якому повинні знаходитись показники, що оцінюються, та відповідна довірлива вірогідність) регламентовано необхідністю підтверджувати на кожному етапі вимірювального процесу $ПН_{ij} \in [НП_{ij}]_{\gamma}, i = \overline{1, n}$, то, у відношенні до цих факторів, не зовсім коректно ставити питання щодо підвищення точності та достовірності $ПН$. По відношенню до цих факторів необхідно розглядати задачі забезпечення перевірки виконання умов $ПН_{ij} \in [НП_{ij}]_{\gamma}, \overline{1, n}$ для варіантів конструкторських розробок та раціоналізації витрат на вимірювання за рахунок використання для оцінки $ПН$ адекватних j -му етапу інформаційних засобів. По відношенню до факторів другої групи зазначені питання сформульовано некоректно. Це означає, що можливі дії, спрямовані на підвищення достовірності оцінювання $ПН$ певного процесу вимірювань. При цьому, оскільки достовірність оцінювання в даному випадку залежить від усієї сукупності інформаційних засобів, що визначають глибину та якість вимірювань на j -му етапі, у відповідності до поставлених критеріїв, то й зусилля повинні бути всебічними, спрямованими по всіх інформаційних складових. Зокрема, необхідно розширення спектру математичного моделювання певних етапів або всього процесу вимірювання в цілому; реалізація оптимізаційних та імітаційних досліджень; використання ефективних програмних засобів (навіть створення САПР) тощо.

Наведені міркування можуть бути доповнені якісним представленням тенденцій (рис. 1), що відбивають взаємодію інтенсивності вимірювань з послідовною реалізацією міри адекватності η_j , яка може розглядатися як відбиток цільового спрямування на результат, що досягається, в виконанні вимірювань на певному їх етапі. На рис.1 зіставлено зони «недостовірності», що визначаються факторами першої (крива 1) та другої (крива 2) груп. Між кривими знаходиться зона, що характеризує перерозподіл значимості вказаних факторів, який відбувається за рахунок зміни інформативності певних етапів вимірювань (їх «вагових» коефіцієнтів), що знаходить відображення у підвищенні значень інформаційного коефіцієнту адекватності на величину $\Delta\eta_j$. Вказані зміни призводять до можливого виграшу у часі вимірювань на величину ΔT_j .

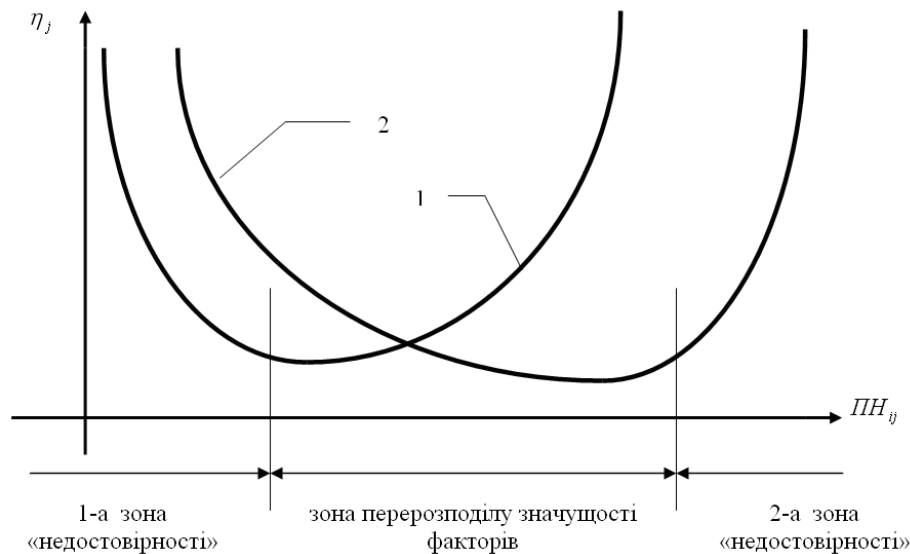


Рис. 1. Перерозподіл зон значущості факторів, що впливають на точність та достовірність вимірювань

Підвищення ТДО $ПН$ процесу вимірювань при переході з етапу на етап (за умови виконання вимоги: кожний етап закінчується підтвердженням правила $ПН_{ij} \in [НП_{ij}]_{\gamma}$) може досягатися за рахунок прийняття до уваги на наступному етапі достовірності оцінки, яку досягнуто на попередньому етапі та яка переноситься на етап, що розглядається, за правилом $\gamma_{j+1} = \gamma_j \eta_j$. При цьому, перенесення центра тяжіння щодо якості процесу вимірювань на попередні його етапи, спричиняє очевидний ефект: $\gamma_{j+1} = \gamma_j (\eta_j + \Delta\eta_j)$, $\Delta\gamma_{j+1} = \gamma_j \Delta\eta_j$, де $\Delta\gamma_{j+1}$ – прирощення достовірності, що переноситься на наступний етап вимірювань, за рахунок прирощення значень інформаційного коефіцієнта адекватності.

Важливим є перерозподіл «ролей», які відіграють похибки, що характеризують ТДО $ПН$ в залежності від тривалості процесу вимірювань. На початкових етапах похибки оцінки, що пов'язані з факторами другої групи, переважають над похибками, які характеризують фактори першої групи. Тому тут втрачає сенс перенос досягнутої достовірності на наступний етап вимірювань з метою підвищення точності оцінювання $ПН$. Разом з тим, підкреслене не відкидає актуальності в «ущільненні» проектних робіт початкових етапів вимірювання, оскільки можливим є суттєвий виграш в темпах реалізації процесу вимірювань, оскільки можливим є суттєвий виграш в темпах здійснення вимірювань і, таким чином, в раціоналізації витрат (апаратних або інформаційних) на вимірювання. При «просуванні» по етапах процесу вимірювань, по мірі зміни значущості факторів першої та другої груп, у зв'язку зі зближенням етапного

результату реалізації вимірювань, принциповим стає можливість обліку достовірності в оцінці *ПН* процесу вимірювань, яку досягнуто на попередньому етапі і яку задіяно у розрахунку *ПН* на поточному етапі процесу вимірювань. В даному випадку є задіяними значні складові загальних витрат на вимірювання, пов'язані із залученням інформаційних ресурсів, необхідних для точної та достовірної оцінки *ПН*.

Висновок

Показано, що в ході моделювання якісних характеристик інформаційних та ІВС можна дослідити систематичні та методичні похибки систем. При цьому моделювання дозволяє отримати об'єктивні характеристики, на відміну від часто застосованих експертних оцінок, заснованих на «суб'єктивізмі» експерта-людини.

Список літератури

1. Цветков, Э.И. Алгоритмические основы измерений / Э.И. Цветков. — СПб.: Энергоатомиздат, 1992. — 274 с.
2. Розенберг, В.Я. Введение в теорию точности измерительных систем / В.Я. Розенберг. — М.: Сов. Радио, 1975. — 327 с.
3. Телешевский, В.И. Рекуррентное робастное оценивание в автоматизированных измерительных информационных системах / В.И. Телешевский, Д.А. Мастеренко // Измерительная техника. 1997. — № 4. — С. 16–19.

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННО-СИСТЕМНЫХ СВОЙСТВ ПРОЦЕССА РЕАЛИЗАЦИИ ИЗМЕРЕНИЙ ЗАДАННОЙ НАДЕЖНОСТИ

А.А. Березовский, В.С. Дмитренко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: aberezovskiy@soyus-corp.com

Выделена группа оценок надежности на каждом этапе осуществления измерений, для которых сформированы факторы, что определяют точность и достоверность процесса оценивания. Исследованы ошибки измерений, в частности, системные регулярные и методические. Построены «зоны» перераспределения значимости факторов, которые влияют на точность и достоверность измерений.

Ключевые слова: информационные системы, информационно-измерительные системы, оценки надежности и достоверности измерений, ошибки измерений.

DESIGN OF INFORMATIVE-SYSTEM PROPERTIES OF PROCESS OF REALIZATION OF MEASUREMENTS OF THE SET RELIABILITY

A.A. Berezovskiy, V.S. Dmitrienko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: aberezovskiy@soyus-corp.com

The group of estimations of reliability is selected on every stage of realization of measurements which factors are formed for, that determine exactness and authenticity of evaluation process. The errors of measurements are investigational, in particular, system regular and methodical. The «areas» of redistribution of meaningfulness of factors which influence on exactness and authenticity of measurements are built.

Keywords: informative systems, informative-measurements systems, estimations of reliability and authenticity of measurements, errors of measurements.

УСОВЕРШЕНСТВОВАНИЕ СТЕГАНОАНАЛИТИЧЕСКОГО МЕТОДА, ОСНОВАННОГО НА АНАЛИЗЕ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ЦИФРОВЫХ КОНТЕЙНЕРОВ

А.В. Ахмаметьева

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

В работе предложена адаптация стеганоаналитического метода, разработанного автором ранее, основанного на учете различий в изменении количества блоков с одинаковыми значениями яркости цветовых матриц последовательности изображений/кадров видеопоследовательности в результате первичного и повторного внедрения дополнительной информации, для контейнеров, хранимых в форматах с потерями. Предложенный стеганоаналитический метод осуществляет анализ цифровых контентов в пространственной области и направлен на выявление наличия вложения дополнительной информации методом модификации наименьшего значащего бита с незначительной скрытой пропускной способностью (не более 0.5 бит/пиксель). Приведены результаты вычислительного эксперимента.

Ключевые слова: стеганоаналитический метод, метод модификации наименьшего значащего бита, пространственная область контейнера, цифровое изображение, цифровая видеопоследовательность, формат хранения с потерями

Введение

Постоянное развитие информационных, компьютерных технологий приводит к их проникновению во все сферы человеческой жизни, что, тем не менее, далеко не всегда благотворно для различных областей деятельности, в частности для безопасности государства, когда в антигосударственных целях могут применяться стеганографические системы, направленные на организацию скрытого канала связи, где обеспечивается сокрытие самого факта передачи секретной информации [1, 2]. В связи с этим чрезвычайно актуальным является развитие и усовершенствование стеганоанализа – составной части стеганографии, основной задачей которого является выявление факта присутствия или отсутствия в каком-либо цифровом контенте передаваемой скрытно информации [2, 3]. В настоящей работе в качестве контейнеров выступают цифровые изображения (ЦИ) и видеопоследовательности (ЦВ), результат внедрения дополнительной информации (ДИ) в контейнер далее называется стеганосообщением (СС).

Одним из наиболее распространенных стеганографических методов до настоящего момента остается метод модификации наименьшего значащего бита (LSB) [2], благодаря простоте реализации, возможности применения как в пространственной области, так и в области преобразований контейнера/СС, а также принципиальной возможности обеспечения высокой скрытой пропускной способности (СПС). Однако на сегодняшний момент с целью затруднения обнаружения пересылаемой скрыто информации метод LSB применяется и с малой СПС (не более 0.5 бит/пиксель). Большинство существующих стеганоаналитических комплексов, методов, алгоритмов

[1, 4-7] выполняют анализ цифровых контентов в области преобразования (частотной области, областях сингулярного/спектрального разложения соответствующих матриц и т.д.). Однако перевод цифрового контента в область преобразования естественным образом сопровождается накоплением вычислительной погрешности, что очевидно способствует снижению эффективности стеганоанализа, особенно при малой СПС стеганографического канала связи, что подтверждается на практике.

Анализ пространственной области цифровых контентов позволяет избежать как дополнительного накопления погрешностей вычисления, так и дополнительных временных затрат при переходе в область преобразований.

Таким образом, повышение эффективности стеганоанализа за счет обеспечения возможности его проведения в пространственной области при внедрении ДИ методом LSB с незначительной СПС в цифровые контейнеры (ЦИ, ЦВ) является актуальной задачей для современной стеганографии.

Цель статьи и постановка задач

Целью работы является повышение эффективности стеганоанализа при выявлении наличия/отсутствия ДИ, погруженной методом LSB с незначительной СПС (не более 0.5 бит/пиксель) в последовательность ЦИ/кадров видеопоследовательности, хранимых в форматах с потерями, путем усовершенствования стеганоаналитического метода, разработанного в [8], основанного на анализе ЦИ (кадров ЦВ) в пространственной области.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1. Получить оценки относительных изменений количества блоков с одинаковыми значениями яркости размером 4×4 матриц оригинальных ЦИ и СС;
2. Выявить отличия в оценках относительных изменений количества 4×4 -блоков с одинаковыми значениями яркости, полученных для ЦИ (кадров ЦВ) в формате без потерь и в формате с потерями [8], определить значения порогов относительных изменений для формата с потерями.

Основная часть

В качестве контейнеров будем рассматривать цветные ЦИ и ЦВ в формате с потерями, хранимые в соответствии с цветовой схемой RGB, которые представляются в виде совокупности трех двумерных матриц R , G , B – красной, зеленой и синей составляющих ЦИ соответственно.

В работе [8] были получены характерные особенности блоков матриц цифровых контентов, отвечающие конкретным выявленным возмущениям их сингулярных чисел (СНЧ) при погружении ДИ. Интерес для решения рассматриваемой задачи вызвали блоки вида:

$$A = \begin{pmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \ddots & \dots \\ a & a & \dots & a \end{pmatrix}, \quad a \in \{1, 2, 3, \dots, 255\}. \quad (1)$$

Для блоков вида (1) установлены и доказаны следующие свойства:

1. Единственное отличное от нуля СНЧ матрицы (1) принадлежит множеству N натуральных чисел;

2. Для $n \times n$ -матрицы A вида (1) максимальное СНЧ определяется по формуле $\lambda_1 = na \in \mathbb{N}$, для остальных СНЧ справедливо равенство $\lambda_2 = \lambda_3 = \dots = \lambda_n = 0$.

Установленные свойства имеют важное значение, поскольку внедрение ДИ методом LSB изменит значения яркости пикселей ЦИ, в результате чего сократится количество блоков вида (1), так как изменение хотя бы одного значения в матрице (1) приведет к увеличению ранга, и свойство 2 не будет выполнено.

На основе рассмотренных свойств в работе [8] был обоснован выбор 4×4 -блока и проведен вычислительный эксперимент на базе последовательности ЦИ/кадров ЦВ в формате без потерь (TIFF), на основе которого были сформулированы основные шаги стеганоаналитического метода и определены пороговые значения относительных изменений количества блоков вида (1) при первичном и вторичном погружении ДИ, которые позволяют отделить контейнер от СС.

В настоящей работе исследования количественной оценки наличия 4×4 -блоков вида (1) проводятся для ЦИ, хранимых в формате с потерями (JPG). В вычислительном эксперименте используется база изображений (БЦИ), включающая в себя 600 цветных ЦИ (схема RGB): 200 ЦИ из базы NRCS Photo Gallery [9] (группа 1), 200 высококачественных ЦИ, взятых из [10] (группа 2), 200 изображений, полученных непрофессиональными фотокамерами (группа 3). Из анализируемых групп ЦИ при пересылке по каналу общего пользования очевидно наименее привлекающими внимание будут изображения группы 3, как имеющие непосредственное отношение к отправителю/получателю, что делает такие ЦИ наиболее вероятными контейнерами при организации скрытого канала связи.

На первом шаге вычислительного эксперимента проводилась оценка количества блоков вида (1) в цветовых составляющих оригинальных ЦИ (контейнеров). Каждая цветовая компонента контейнера исследовалась отдельно. Результаты представлены в табл. 1. Было установлено, что в 2.2% от общего количества цветовых матриц (из $600 \cdot 3 = 1800$ матриц) не содержится 4×4 -блоков вида (1), тем не менее данный процент существенно ниже аналогичного количества для изображений в форматах без потерь [8], что вполне объясняется сжатием ЦИ: в результате частотных преобразований происходит округление коэффициентов ДКП до ближайшего целого, что приводит к унификации соседних близких по значению яркостей к их среднему значению. Отсутствие или незначительное количество 4×4 -блоков вида (1) говорит о наличии большого количества мелких деталей и перепадов яркости близлежащих пикселей в изображении. Как видно из табл. 1, в ЦИ группы 3 вообще не наблюдалось матриц, не содержащих блоков с одинаковыми значениями яркости.

Таблица 1.

Количество 4×4 -блоков вида (1) в цветовых составляющих оригинальных ЦИ в формате с потерями (JPG) относительно общего числа блоков (%)

Цветовая составляющая ЦИ	Группа 1			Группа 2			Группа 3		
	Мин-е значение	Макс-е значение	Среднее значение	Мин-е значение	Макс-е значение	Среднее значение	Мин-е значение	Макс-е значение	Среднее значение
R	0	44.0162	5.9681	0	30.4347	1.8399	0.0015	27.7792	2.8137
G	0	44.2113	5.9398	0	28.4236	1.8371	0.0015	29.8941	2.8233
B	0	46.4097	5.9874	0	26.5523	2.0404	0.0005	31.3935	3.0729

Внедрение ДИ методом LSB приводит к изменению количества 4×4 -блоков вида (1) в матрице ЦИ. Для установления количественной оценки этого изменения был проведен второй шаг вычислительного эксперимента, результаты которого приведены

в табл. 2, где СС сформированы на основе контейнеров из БЦИ при СПС 0.5, 0.25 и 0.1 бит/пиксель. В табл. 2 столбец, обозначенный I, соответствует используемому значению СПС (бит/пиксель); II – выбранной цветовой составляющей ЦИ; III₁, III₂ и III₃ – среднему значению относительного (по отношению к общему количеству блоков в матрице цветовой компоненты ЦИ (%)) количества блоков с одинаковыми значениями яркости по СС из групп 1, 2 и 3 соответственно; IV₁, IV₂ и IV₃ – относительному изменению среднего значения количества блоков с одинаковыми значениями яркости в сформированных СС по сравнению с оригинальными ЦИ для групп 1, 2 и 3 соответственно (%).

Изменения среднего значения количества блоков вида (1) $\bar{R}, \bar{G}, \bar{B}$ соответственно для красной, зеленой и синей цветовой компоненты оригинального контейнера по сравнению с СС вычисляются по формулам:

$$\bar{R} = \frac{|r^{(C)} - r^{(S)}|}{r^{(C)}} \cdot 100\%, \quad \bar{G} = \frac{|g^{(C)} - g^{(S)}|}{g^{(C)}} \cdot 100\%, \quad \bar{B} = \frac{|b^{(C)} - b^{(S)}|}{b^{(C)}} \cdot 100\%, \quad (2)$$

где $r^{(C)}, g^{(C)}, b^{(C)}$ – средние значения количества блоков в последовательности оригинальных ЦИ / кадрах ЦВ в красной, зеленой и синей компоненте соответственно;

$r^{(S)}, g^{(S)}, b^{(S)}$ – средние значения количества блоков в последовательности СС, сформированных погружением ДИ с одинаковой СПС в оригинальный контейнер, в красной, зеленой и синей компоненте соответственно.

Таблица 2.

Количество 4×4-блоков с одинаковыми значениями яркости в цветовых составляющих ЦИ-СС, сформированных для различных значений СПС, относительно общего числа блоков цветowych составляющих изображения (%)

I	II	Группа 1		Группа 2		Группа 3	
		III ₁	IV ₁	III ₂	IV ₂	III ₃	IV ₃
0.5	R	0.5175	91.3	0.6693	63.6	0.5595	80.1
	G	0.4623	92.2	0.6871	62.6	0.6919	75.5
	B	0.5229	91.2	1.0485	48.6	0.8847	71.2
0.25	R	0.5139	91.4	0.6616	64	0.5545	80.3
	G	0.4594	92.3	0.6789	63	0.6882	75.6
	B	0.5202	91.3	1.0254	49.7	0.8759	71.5
0.1	R	0.7495	87.4	0.7008	61.9	0.6599	76.5
	G	0.6827	88.5	0.7407	59.7	0.7744	72.6
	B	0.8027	86.6	1.0711	47.5	0.9799	68.1

Наиболее информативной характеристикой при анализе количества 4×4-блоков вида (1) является относительное изменение их количества при внедрении ДИ по сравнению с оригинальным ЦИ, поскольку абсолютное изменение количества таких блоков может быть незначительным либо вообще отсутствовать, и точно отделить оригинальный контейнер от СС здесь не представляется возможным. Табл. 2 показывает, как изменяется количество 4×4-блоков вида (1) (IV₁, IV₂ и IV₃ в табл. 2) при внедрении ДИ с СПС 0.5, 0.25 и 0.1 бит/пиксель в зависимости от анализируемой группы. При этом, как и в формате без потерь [8], происходящие изменения различны для разных групп ЦИ. Вполне естественно, что наименьшие изменения будут в группе 2, так как в нее входят высококачественные профессиональные ЦИ, а в изображениях худшего качества изменения более заметны. Следует отметить, что относительные

изменения в форматах с потерями на порядок выше, чем при аналогичном вычислительном эксперименте ЦИ в формате без потерь [8], что объясняется особенностями сжатия изображений.

Тем не менее, в реальных условиях стеганоанализ проводится при отсутствии оригинального изображения-контейнера, поэтому выясним, как изменится количество блоков с одинаковыми значениями в ЦИ-СС при повторном внедрении ДИ методом LSB с различными значениями СПС. Результаты эксперимента приведены в табл. 3, где столбец с обозначением II соответствует цветовой составляющей ЦИ-СС; III₁, III₂ и III₃ – среднему значению количества блоков с одинаковыми значениями яркости в СС, сформированных в результате повторного погружения ДИ методом LSB в ЦИ-СС из групп 1, 2 и 3 соответственно; IV₁, IV₂ и IV₃ – изменению среднего значения количества блоков с одинаковыми значениями яркости по сравнению с СС, сформированными в результате повторного погружения ДИ методом LSB в ЦИ-СС из групп 1, 2 и 3 соответственно (%). Здесь изменения среднего значения количества блоков вида (1) $\bar{R}, \bar{G}, \bar{B}$ соответственно для красной, зеленой и синей цветовой компоненты ЦИ-СС по сравнению с СС, сформированным повторным погружением ДИ, вычисляются по формулам:

$$\bar{R} = \frac{|r^{(s)} - r^{(\bar{s})}|}{r^{(s)}} \cdot 100\%, \quad \bar{G} = \frac{|g^{(s)} - g^{(\bar{s})}|}{g^{(s)}} \cdot 100\%, \quad \bar{B} = \frac{|b^{(s)} - b^{(\bar{s})}|}{b^{(s)}} \cdot 100\%, \quad (3)$$

где $r^{(\bar{s})}, g^{(\bar{s})}, b^{(\bar{s})}$ – средние значения количества блоков в последовательности СС, сформированных вторичным погружением ДИ в ЦИ-СС, в красной, зеленой и синей компоненте соответственно.

Для наглядной иллюстрации различий между изменениями при первичном погружении ДИ в оригинальное изображение и при повторном внедрении ДИ в СС, сформированные на основе погружения ДИ в оригинальные ЦИ с разными СПС, построим графики зависимости относительного изменения количества блоков вида (1) для красной компоненты (выбрана для примера) по каждой анализируемой группе (рис. 1).

Полученные результаты позволяют отделить последовательность незаполненных изображений-контейнеров от заполненных СС, поскольку относительные изменения при первичном и вторичном погружении ДИ количественно значительно отличаются друг от друга. Притом отличия по ЦИ в формате с потерями настолько значительны, особенно при первичной СПС 0.5 и 0.25 бит/пиксель, даже по сравнению с аналогичным вычислительным экспериментом, проведенным по ЦИ в формате без потерь [8], что дает возможность дать ответ с большой вероятностью, есть ли в анализируемой последовательности вложенная ДИ или нет. Как видно из табл. 3, в целом значения относительного изменения сравнимы друг с другом для СПС 0.5 и 0.25. В случае СПС 0.1 эти значения несколько выше, что, тем не менее, не повлияет на заключение об отсутствии/наличии ДИ, так как даже такие значения намного ниже тех, которые получаются при первичном погружении ДИ.

Таблица 3.

Оценки для абсолютного и относительного количества блоков с одинаковыми значениями яркости в цветовых составляющих ЦИ-СС, сформированных путем повторного внедрения ДИ в СС, полученные методом LSB для различных значений СПС, усредненные по всем изображениям из групп 1, 2 и 3 (%)

Первичная СПС СС (бит/пиксель)	СПС для повторного погружения ДИ в СС (бит/пиксель)	II	Группа 1		Группа 2		Группа 3	
			III ₁	IV ₁	III ₂	IV ₂	III ₃	IV ₃
0.5	0.5	R	0.5365	3.7	0.6900	3.1	0.5778	3.3
		G	0.4804	3.9	0.7099	3.3	0.7049	1.9
		B	0.5417	3.6	1.1030	5.2	0.9046	2.2
	0.25	R	0.5199	0.5	0.6760	1	0.5635	0.7
		G	0.4640	0.4	0.6947	1.1	0.6958	0.6
		B	0.5250	0.4	1.0685	1.9	0.8930	0.9
	0.1	R	0.5184	0.2	0.6721	0.4	0.5614	0.3
		G	0.4628	0.1	0.6901	0.4	0.6934	0.2
		B	0.5241	0.2	1.0567	0.8	0.8885	0.4
0.25	0.5	R	0.5200	1.2	0.6769	2.3	0.5645	1.8
		G	0.4638	1	0.6947	2.3	0.6959	1.1
		B	0.5254	1	1.0699	4.3	0.8944	2.1
	0.25	R	0.5777	12.4	0.6741	1.9	0.5749	3.7
		G	0.4875	6.1	0.6984	2.9	0.7066	2.7
		B	0.5803	11.6	1.0501	2.4	0.8946	2.1
	0.1	R	0.5150	0.2	0.6643	0.4	0.5562	0.3
		G	0.4602	0.2	0.6816	0.4	0.6896	0.2
		B	0.5212	0.2	1.0333	0.8	0.8794	0.4
0.1	0.5	R	0.5186	30.8	0.6724	4.1	0.5612	15
		G	0.4625	32.3	0.6907	6.8	0.6934	10.5
		B	0.5243	34.7	1.0579	1.2	0.8877	9.4
	0.25	R	0.5148	31.3	0.6640	5.3	0.5560	15.7
		G	0.4601	32.6	0.6814	8	0.6900	10.9
		B	0.5211	35.1	1.0337	3.5	0.8782	10.4
	0.1	R	1.0912	45.6	0.7364	5.1	0.7839	18.8
		G	1.1485	68.2	0.7823	5.6	0.8281	6.9
		B	1.1111	38.4	1.1345	5.9	1.0726	9.5

На основе полученных результатов основные шаги стеганоаналитического метода, направленного на выявление наличия/отсутствия вложения ДИ в последовательности из P ЦИ $C_1, C_2, \dots, C_P$ с цветовыми составляющими $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ (или видеопоследовательности из P кадров $C_1, C_2, \dots, C_P$), следующие:

1. Для каждого $C_i, i = \overline{1, P}$ вычислить $r_i^{(C)}, g_i^{(C)}, b_i^{(C)}$ – относительное количество 4×4 -блоков в $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ по отношению к общему количеству 4×4 -блоков в матрице цветовой составляющей (в %) соответственно.

2. Внедрить в $R_i^{(C)}, G_i^{(C)}, B_i^{(C)}$ методом LSB некоторую ДИ – случайно сформированную бинарную последовательность с СПС T бит/пиксель. Результат – S_i с цветовыми составляющими $R_i^{(S)}, G_i^{(S)}, B_i^{(S)}$.

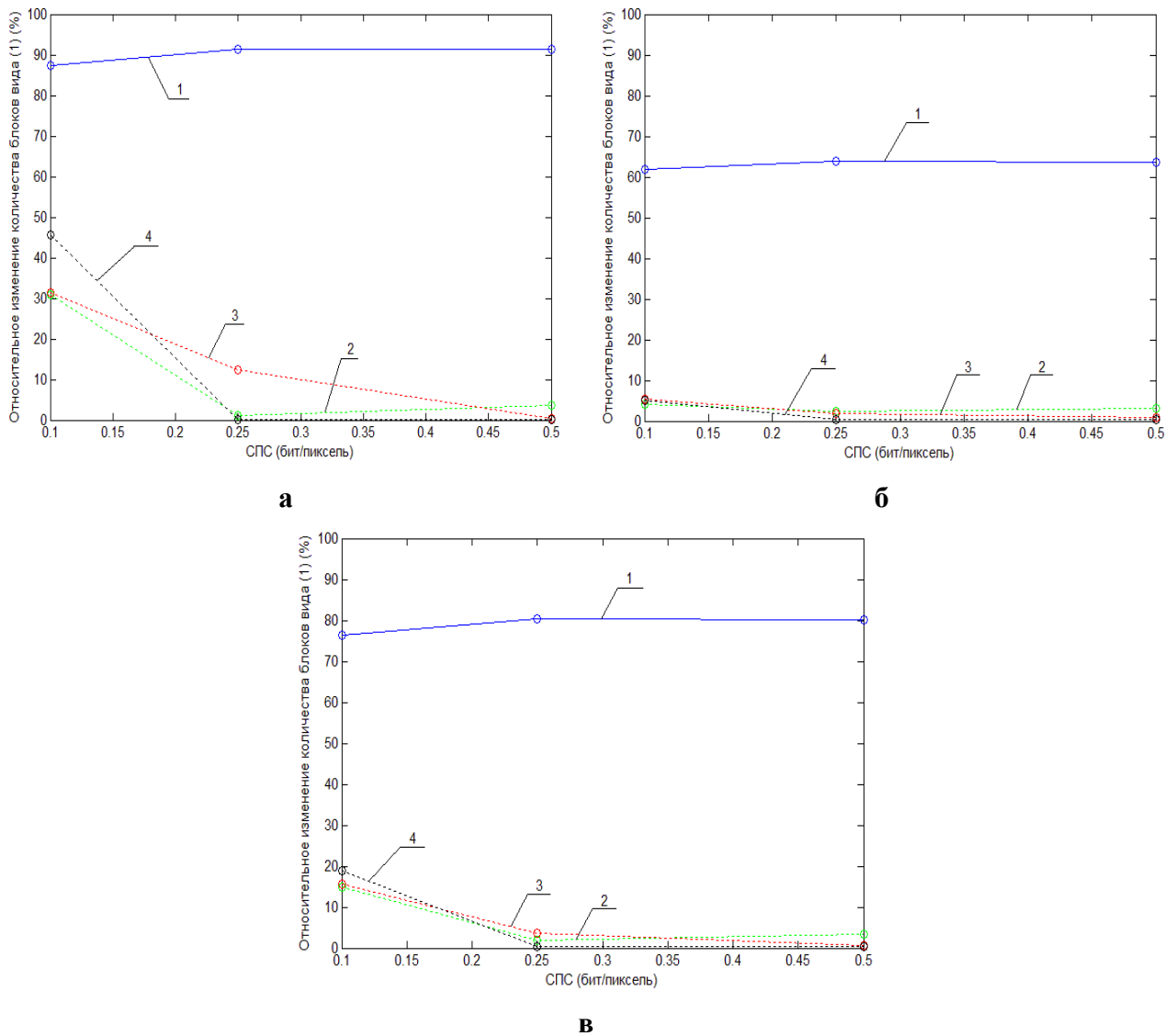


Рис. 1. Зависимость относительного изменения количества блоков вида (1) в матрицах ЦИ от СПС метода LSB, использованного для стеганопреобразования: 1 – для СС при внедрении ДИ в оригинальное ЦИ; 2 – для СС, полученного путем повторного внедрения ДИ в СС, сформированное методом LSB с СПС 0.5 бит/пиксель; 3 – для СС, полученного путем повторного внедрения ДИ в СС, сформированное методом LSB с СПС 0.25 бит/пиксель; 4 – для СС, полученного путем повторного внедрения ДИ в СС, сформированное методом LSB с СПС 0.1 бит/пиксель; а – ЦИ из группы 1; б – ЦИ из группы 2; в – ЦИ из группы 3

3. Для каждого $S_i, i = \overline{1, P}$ вычислить $r_i^{(S)}, g_i^{(S)}, b_i^{(S)}$ – относительное количество 4×4 -блоков в $R_i^{(S)}, G_i^{(S)}, B_i^{(S)}$ по отношению к общему количеству 4×4 -блоков в матрице цветовой составляющей (в %) соответственно.

4. Определить средний процент 4×4 -блоков вида (1) по анализируемой последовательности $C_1, C_2, \dots, C_P$ и сформированной последовательности $S_1, S_2, \dots, S_P$ по формулам:

$$r^{(C)} = \frac{1}{P} \sum_{i=1}^P r_i^{(C)}, \quad g^{(C)} = \frac{1}{P} \sum_{i=1}^P g_i^{(C)}, \quad b^{(C)} = \frac{1}{P} \sum_{i=1}^P b_i^{(C)};$$

$$r^{(S)} = \frac{1}{P} \sum_{i=1}^P r_i^{(S)}, \quad g^{(S)} = \frac{1}{P} \sum_{i=1}^P g_i^{(S)}, \quad b^{(S)} = \frac{1}{P} \sum_{i=1}^P b_i^{(S)}.$$

5. Вычислить относительное изменение количества 4×4 -блоков вида (1) каждой цветовой составляющей $\bar{R}, \bar{G}, \bar{B}$ анализируемой последовательности $C_1, C_2, \dots, C_P$ по отношению к среднему значению количества 4×4 -блоков вида (1) последовательности $S_1, S_2, \dots, S_P$ по формуле (2).

6. Детектирование вложения ДИ:

Если $\bar{R} < T_R$, то $C_1, C_2, \dots, C_P$ содержит вложенную ДИ в красной цветовой составляющей;

Если $\bar{G} < T_G$, то $C_1, C_2, \dots, C_P$ содержит вложенную ДИ в зеленой цветовой составляющей;

Если $\bar{B} < T_B$, то $C_1, C_2, \dots, C_P$ содержит вложенную ДИ в синей цветовой составляющей,

где T_R, T_G, T_B – пороговые значения для каждой цветовой составляющей.

По результатам проведенного эксперимента в качестве пороговых значений относительного изменения количества блоков вида (1) в матрицах оригинальных ЦИ по сравнению с СС для формата с потерями предлагается принять $T_R = 32$, $T_G = 33$, $T_B = 35.5$ (для красной, зеленой, синей составляющих ЦИ соответственно). Если в качестве контейнеров при организации скрытого канала связи использовать ЦИ группы 3, то можно предполагать эффективность предложенного метода.

Выводы

В работе усовершенствован разработанный в [8] стеганоаналитический метод, направленный на выявление результатов вложения ДИ методом LSB с незначительной СПС (не более 0.5 бит/пиксель) для контейнеров, хранимых в формате без потерь, путем расширения данного метода на контейнеры, хранимые в формате с потерями.

В качестве контейнеров разработанный метод анализирует последовательности ЦИ или последовательные кадры видеопоследовательности в случае организации скрытого канала связи. Метод основан на учете различий относительных изменений количества блоков с одинаковыми значениями яркости цветовой составляющей ЦИ/кадра видеопоследовательности в результате первичного и повторного погружения ДИ. Данные различия отлично проявляются для контейнеров, хранимых в формате с потерями, особенно для тех из них, которые получены непрофессиональными фото и видеокамерами.

В настоящее время автором проводится уточнение количественных порогов T_R , T_G , T_B для контейнеров, хранимых в формате с потерями, что в дальнейшем позволит разработать эффективный стеганоаналитический алгоритм, реализованный на основе усовершенствованного метода.

Список литературы

1. Бобок, И.И. Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями / И.И. Бобок // Сучасний захист інформації. – 2011. – №2. – С. 50-60.
2. Стеганография, цифровые водяные знаки и стеганоанализ : [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: Вузовская книга, 2009. – 220 с.
3. Bohme, R. Advanced statistical steganalysis / R. Bohme. – Springer, 2010. – 302 p.
4. Alimoradi, D. The effect of correlogram properties on blind steganalysis in JPEG images / D. Alimoradi, M. Hasanzadeh // Journal of computing and security. – 2014. – Vol. 1. – No.1. – Pp. 39-46.

5. Visavalia, S.R. Improving blind image steganalysis using genetic algorithm and fusion technique / Sarita R. Visavalia, Amit Ganatra // Journal of computer science. – 2014. – Vol. 1. – Pp. 40-46.
6. Yamini, B. Blind steganalysis: to analyse the detection rate of stego images using different steganalytic techniques with support vector machine classifier / B. Yamini, R. Sabitha // International journal of computer applications. – 2014. – No. 2. – Pp. 22-25.
7. Manjunath, C. Added and subtracted feature level video steganalysis in neighbor adaptive embedded / C. Manjunath, Mis.B. Sowjanya // International journal of professional engineering studies. – 2015. – Vol. 5. – Issue 2. – Pp. 308-316.
8. Кобозева, А.А. Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь / А.А. Кобозева, А.В. Ахметьев, А.А. Ефименко // Інформаційна безпека. – 2014. – №1(13). – С. 31-42.
9. NRCS Photo Gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата обращения: 26.07.2012).
10. WallpapersCraft: [Електронний ресурс] // Широкоформатные обои на рабочий стол, картинки, фото. Режим доступа: <http://wallpaperscraft.ru/> (Дата обращения: 21.11.2014).

УДОСКОНАЛЕННЯ СТЕГНОАНАЛІТИЧНОГО МЕТОДУ, ЗАСНОВАНОГО НА АНАЛІЗІ ПРОСТОРОВОЇ ОБЛАСТІ ЦИФРОВИХ КОНТЕЙНЕРІВ

Г.В. Ахметьєва

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

У роботі запропоновано адаптацію стеганоаналітичного методу, розробленого автором раніше, заснованого на врахуванні розходжень у зміні кількості блоків з однаковими значеннями яскравості кольорних матриць послідовності зображень/кадрів відео послідовності в результаті первинної й повторної вбудови додаткової інформації, для контейнерів, збережених у форматах з втратами. Запропонований стеганоаналітичний метод здійснює аналіз цифрових контентів у просторовій області та направлений на виявлення наявності вкладення додаткової інформації методом модифікації найменшого значущого біта з незначною прихованою пропускнуною спроможністю (не більше 0.5 біт/піксель). Наведені результати обчислювального експерименту.

Ключові слова: стеганоаналітичний метод, метод модифікації найменшого значущого біта, просторова область контейнера, цифрове зображення, цифрова відеопослідовність, формат зберігання з втратами

IMPROVEMENT OF THE STEGANALYTIC METHOD, BASED ON THE ANALYSIS OF THE SPATIAL DOMAIN OF DIGITAL CONTAINERS

A. V. Akhmet'ieva

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: anna-odessitka@mail.ru

The paper presents the adaptation of steganalytic method developed earlier by the author, based on the accounting of differences in the change of the number of blocks with the equal color brightness values of color matrices of sequence of images / frames of a video sequence as a result of primary and repeated insertion of additional information for containers in losses formats. The proposed steganalytic method analyzes digital content in the spatial domain and is aimed to detect the presence of the embedding of additional information by modification of the least significant bits with a small hidden capacity (not more than 0.5 bit / pixel). Results of computational experiment are shown.

Keywords: Steganalytic method, method of the modification of the least significant bit, the spatial domain of the container, a digital image, a digital video sequence, losses format

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ МЕТОДІВ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ

М.М. Касянчук, І.З. Якименко, Т.М. Долинюк, Н.А. Рендзеняк

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: kasyanchuk@ukr.net, jiz@tneu.edu.ua

Виконання арифметичних операцій над багаторозрядними числами є досить важливою задачею сучасної теорії чисел та асиметричної криптографії. У роботі проведено експериментальне дослідження часової складності модулярного експоненціювання з використанням середовища програмування Python 3.4.0 різними методами: пониження степеня за допомогою виділення квадратів (бінарний), кубів (3-арний), системи залишкових класів та її модифікованої досконалої форми. Операції виконувалися над числами різної розрядності та з різною вагою Хемінга. Показано, що при малих розрядностях найбільшою швидкістю характеризується метод пониження степенів за допомогою кубів. Починаючи з 1024 біт найменший час для виконання операції модулярного піднесення до степеня витрачається при застосуванні методу модифікованої досконалої форми системи залишкових класів. При дослідженні часової складності модулярного експоненціювання в залежності від ваги Хемінга встановлено, що найбільший час затрачується, коли вага Хемінга максимальна. При її зменшенні час виконання різко зменшується і надалі залишається майже постійним.

Ключові слова: асиметрична криптографія, модулярне експоненціювання, пониження степеня, модифікована досконала форма системи залишкових класів, часова складність, вага Хемінга.

Вступ

Розробка стійких систем захисту інформаційних потоків забезпечується високою продуктивністю при реалізації на основі обчислювальних термінальних пристроїв в комп'ютерних мережах існуючих мережових протоколів [1], заборонаю функціонування системи в обхід підсистем захисту та розмежуванням доступу [2]. Найбільш трудомісткими з точки зору обчислювальної реалізації протоколів мережового обміну є виконання операцій модулярної арифметики, зокрема, модулярного експоненціювання, над багаторозрядними числами [3], розрядність яких значно перевищує розрядність процесорів. Особливо це стосується асиметричної криптографії [4], наприклад, криптосистем RSA, Ель-Гамала, протоколів обміну ключем та електронного цифрового підпису [5] тощо.

Складність використання протоколів обміну ключами та рівень захищеності прямо пропорційна розрядності чисел, якими вони оперують. На сьогоднішній день для досягнення прийнятної рівня захищеності вказаних криптографічних застосувань необхідна розрядність чисел становить щонайменше 1024 біт [6] з перспективою її зростання в найближчі роки до 2048 та 4096 біт. Це неминуче призведе до зменшення швидкодії виконання алгоритмів модулярного експоненціювання та виникнення небезпеки переповнення розрядної сітки. З особливою гостротою ця проблема стоїть для малорозрядних вбудованих мікропроцесорів та мікроконтролерів [7]. Тому постає

задача вибору найбільш швидкого алгоритму піднесення до степеня великорозрядних чисел за модулем при використанні комп'ютерів загального та спеціального призначення.

Слід зазначити, що на даний момент розроблено багато методів різної обчислювальної складності для модулярного множення та експоненціювання [3] (стандартний, бінарний, Монтгомері, Карацуби-Офмана тощо). Однак теоретичні дослідження обчислювальної складності не завжди показують реальну картину щодо швидкодії обчислень, оскільки не враховують усіх факторів, які впливають на роботу комп'ютера, зокрема, звертань до пам'яті, особливостей завантаженості процесора, його розрядності та розпаралелення обчислень тощо.

Тому *метою* нашої роботи є знаходження, порівняння та аналіз часу модулярного експоненціювання, виконаних за допомогою різних алгоритмів для чисел різної розрядності на комп'ютері із заданими параметрами.

Основна частина

Для досліджень було обрано комп'ютер HP ProBook 4540S, з процесором Intel i5, тактова частота 2,3 GHz, оперативна пам'ять 6 GB, операційна система Linux Mint 17.1, середовище програмування Python 3.4.0. Вибір останнього зумовлений його модульністю та можливістю повторного використання коду [8]. Це є інтерпретована об'єктно-орієнтована мова програмування високого рівня з динамічною семантикою. Структури даних високого рівня разом із динамічною семантикою та динамічним зв'язуванням роблять її привабливою для швидкої розробки програм, а також як засіб поєднання існуючих компонентів. Інтерпретатор Python та стандартні бібліотеки доступні як у скомпільованій, так і у вихідній формах на всіх основних платформах. В мові програмування Python підтримується декілька парадигм програмування, зокрема: об'єктно-орієнтована, процедурна, функціональна та аспектно-орієнтована [9]. Безсумнівною її перевагою є можливість роботи з великорозрядними числами (до 4096 біт).

Вибір методів зумовлювався часом модулярного експоненціювання, який для різних методів мав бути приблизно одного порядку, та можливістю виконання операцій над великорозрядними числами (до 4096 біт). В зв'язку з цим не досліджувалися методи прямого піднесення до степеня, при якому вже для 16-бітних чисел відбувалося переповнення розрядної сітки, та множення справа наліво або зліва направо, що вимагало виконання $x-1$ операцій множення (x – показник степеня) і, відповідно, збільшувався час обчислень. З цієї ж причини не був використаний метод системи залишкових класів (СЗК), коли модуль p є добутком декількох простих співмножників ($p = p_1 \cdot p_2 \cdot \dots \cdot p_n$), і його потрібно факторизувати, що приводило до істотного збільшення часової складності. Отже, для дослідження були вибрані чотири методи:

- бінарний або метод пониження степеня за допомогою квадратів [3], який описується виразом:

$$N = a^x \bmod p = (a^{x-2x_1} a_1^{x_1-2x_2} \dots a_i^{x_i-2x_{i+1}} \dots) \bmod p = \left(\prod_{i=0}^{\lfloor \log_2 x \rfloor} a_i^{x_i-2x_{i+1}} \right) \bmod p, \quad (1)$$

де $a_0 = a$, $x_0 = x$, $a_i = a_{i-1}^2 \bmod p$; $x_i = \left\lfloor \frac{x_{i-1}}{2} \right\rfloor$;

- метод пониження степеня за допомогою кубів (3-арний) [2], який можна записати аналогічно (1):

$$N = a^x \bmod p = (a^{x-3x_1} a_1^{x_1-3x_2} \dots a_i^{x_i-3x_{i+1}} \dots) \bmod p = \left(\prod_{i=0}^{\lfloor \log_3 x \rfloor} a_i^{x_i-3x_{i+1}} \right) \bmod p,$$

де $a_0 = a$, $x_0 = x$, $a_i = a_{i-1}^3 \bmod p$; $x_i = \lfloor x_{i-1}/3 \rfloor$;

■ використання СЗК [10], коли основа степеня розбивається на залишки від ділення на попарно взаємно прості модулі, далі відбувається пониження степеня бінарним методом і відновлення десяткового запису числа. Всю процедуру можна описати виразом:

$$N = a^x \bmod p = \left(\sum_{i=1}^k m_i M_i a_i \right) \bmod p, \quad (2)$$

де $a_i = (a \bmod p_i)^{x_i} \bmod p_i$, $p = \prod_{i=1}^k p_i$, $M_i = \frac{p}{p_i}$, $m_i = M_i^{-1} \bmod p_i$, $a_0 = a$, k – кількість модулів. Пошук оберненого елемента відбувається за допомогою алгоритму Евкліда та його наслідку;

■ використання модифікованої досконалої форми (МДФ) СЗК [11], згідно якої модулі підбрані таким чином, що $m_i = M_i \bmod p_i = \pm 1$. Це дозволяє уникнути виконання громіздкої операції пошуку оберненого елемента за модулем та множення в (2) на базисні числа m_i , що, відповідно, приводить до зменшення часу обчислень.

Для модулярного піднесення до степеня $a^x \bmod p$ в залежності від розрядності n та кількості одиниць у двійковому записі числа (ваги Хемінга) параметри a , x та p визначалися таким чином: $a = r(n-3, \Delta)$, $x = r(n, \Delta)$, де цілочисельна функція

$$r(n, \Delta) = 2^n - 1 - \lfloor RND \cdot \lfloor \Delta \cdot n / 100 \rfloor \rfloor,$$

n – розрядність чисел, над якими виконуються операції, $0 < RND < 1$ – випадкова величина, заданий параметр Δ набуває дискретних значень 0, 10, 30, 50 та 80.

Останній вказує, що при $\Delta = 0$ вага Хемінга чисел $a = 2^n - 1$ та $x = 2^{n-3} - 1$ дорівнює їх розрядності. Збільшення цього параметра означає, що $\Delta\%$ молодших розрядів у двійковому записі a та x може змінитися випадковим чином під дією функції RND .

Для кожного методу піднесення до степеня використовувався один і той самий модуль, який залежить від розрядності числа x і є добутком трьох попарно взаємно

простих співмножників $p = p_1 \cdot p_2 \cdot p_3$, що утворюють МДФ СЗК: $p_1 = 2^{\lfloor \frac{n}{3} \rfloor + 1}$, $p_2 = 2p_1 - 1$, $p_3 = 2p_1 + 1$. Слід відмітити, що модуль p перевищує діапазон обчислень, який визначається відповідною розрядністю n , приблизно у 8-16 разів. Усі розрахунки для кожного випадку проводилися 10 разів і визначався середній час виконання модулярного експоненціювання (в мікросекундах). Отримані результати наведені в таблиці 1 (у першому стовпчику 1 – пониження степеня за допомогою квадратів, 2 – за допомогою кубів, 3 – СЗК, 4 – МДФ СЗК).

Як слідує з таблиці, швидкість піднесення до степеня за модулем істотно залежить від методу, яким воно виконується. Так, при малих розрядностях (до 256 включно) методи СЗК та МДФ СЗК істотно поступаються в часі двом іншим (приблизно в 2-4 рази), а найшвидше модулярне експоненціювання виконується методом пониження степеня за допомогою кубів. Це ж стосується випадку, коли $n = 512$ і $\Delta = 0$. Для інших Δ і тієї ж розрядності мінімальний час буде при використанні бінарного методу, а СЗК та МДФ СЗК вже відстають приблизно в 1,5 раза і, починаючи з $n = 1024$ вони дають мінімальний час. На рисунку 1 в логарифмічній шкалі представлено графіки залежності часу виконання операції модулярного

експоненціювання різними методами від розрядності чисел для $\Delta = 0$, тобто для чисел з максимальним значенням ваги Хемінга.

Таблиця 1.

Час виконання операції модулярного експоненціювання різними способами

Розрядність	8	16	32	64	128	256	512	1024	2048	4096
$\Delta = 0$										
1	14	24	55	108	254	746	2251	10727	64628	405196
2	12	23	44	91	200	655	2162	11987	75411	466016
3	58	83	159	299	628	1430	3430	10366	37564	216596
4	62	72	150	266	610	1340	3195	9956	36861	208496
$\Delta = 10$										
1	10	18	39	81	179	487	1955	9452	61290	404806
2	9	17	34	66	148	445	1997	10055	68190	458023
3	43	58	114	211	456	997	2858	9266	34831	199364
4	40	53	105	193	451	969	2563	8417	34413	198145
$\Delta = 30$										
1	10	18	38	78	177	487	1919	9353	60907	403917
2	9	17	35	68	146	441	2038	10097	68163	457405
3	43	61	115	211	458	998	2848	9009	34768	199534
4	40	53	103	193	443	974	2546	8409	34378	197433
$\Delta = 50$										
1	11	18	37	79	177	494	1954	9465	61187	404641
2	8	17	33	67	146	442	1978	10224	68165	457931
3	44	61	113	211	459	1004	2847	9108	34826	199136
4	40	53	103	193	442	965	2553	8443	34361	197780
$\Delta = 80$										
1	10	17	37	78	181	492	1918	9419	60949	404217
2	9	18	33	67	146	444	2015	10074	68148	458093
3	42	61	112	209	458	1001	2856	9086	34738	199704
4	40	51	101	194	440	974	2560	8394	34355	197588

Слід зазначити, що при інших значеннях Δ залежності мають приблизно такий самий характер, тому вони не наведені. З рисунка видно, що графіки для СЗК та МДФ СЗК практично збігаються. Це пов'язано з тим, що при переведенні чисел із СЗК в десяткову систему числення для модулів, які утворюють МДФ СЗК і використовуються в дослідженні, потрібна мала кількість ітерацій при застосуванні алгоритму Евкліда, його наслідку та китайської теореми про залишки.

На рисунку 2 наведено графіки залежності часу виконання модулярного піднесення до степеня різними методами від значення ваги Хемінга Δ при найбільш поширеній на даний час розрядності $n = 1024$.

Як видно з рисунка, всі графіки мають приблизно однаковий характер. Найбільший час затрачається при максимальній вазі Хемінга ($\Delta = 0$). При зменшенні останньої час різко зменшується і надалі залишається майже постійним, здійснюючи невеликі коливання відносно деякого значення.

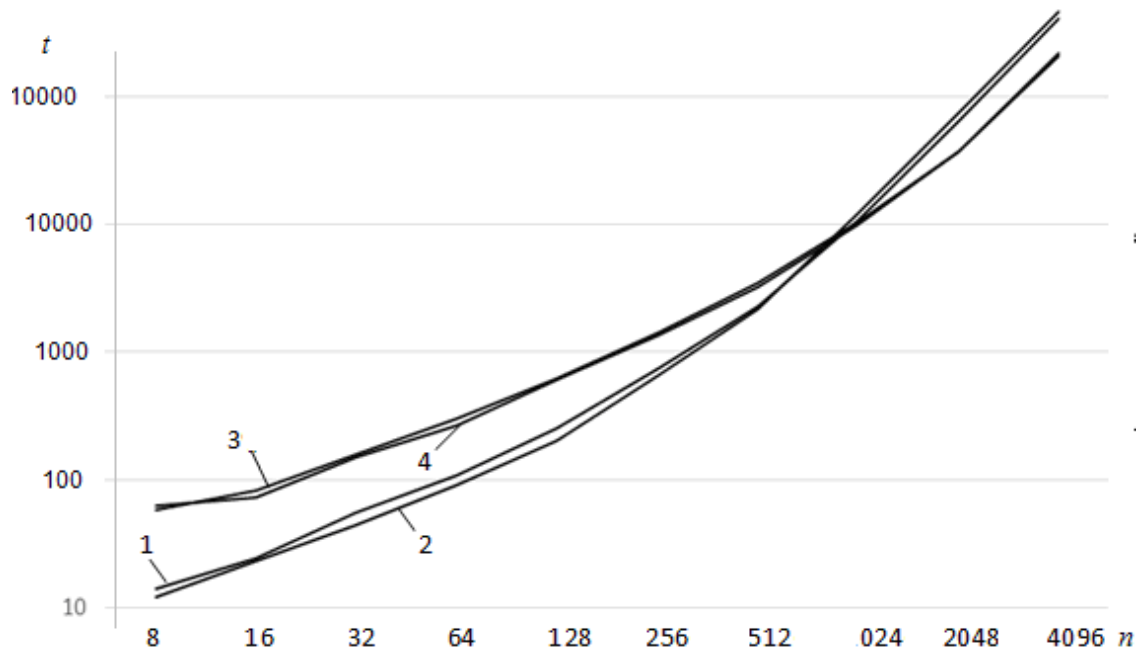


Рис. 1. Графіки залежності часу виконання операції модулярного експоненціювання різними методами від розрядності чисел для $\Delta=0$ (1 – пониження степеня за допомогою квадратів, 2 – за допомогою кубів, 3 – використання СЗК, 4 – використання МДФ СЗК)

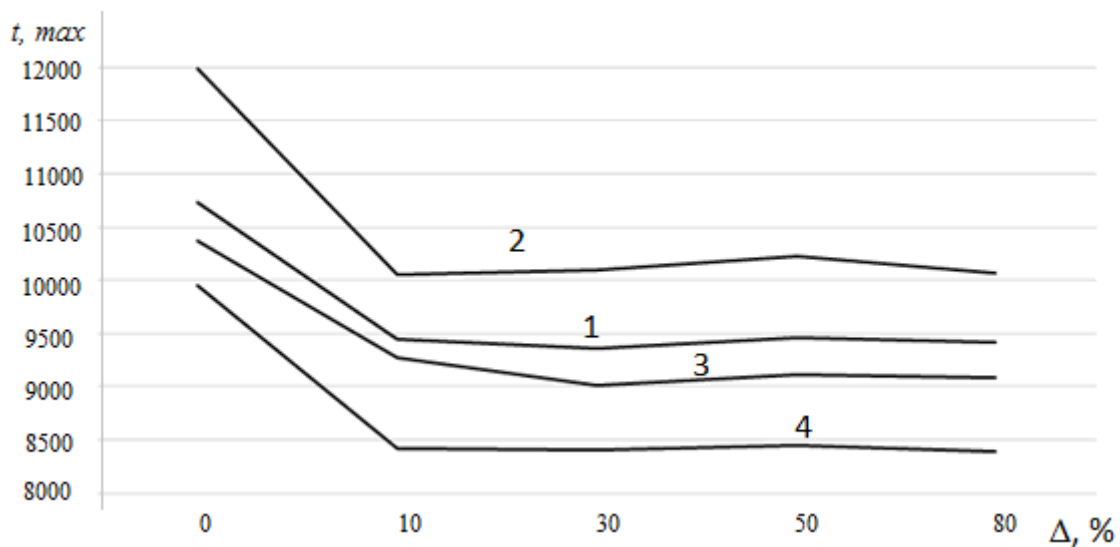


Рис. 2. Графіки залежності часу виконання модулярного піднесення до степеня різними методами від значення ваги Хемінга Δ при $n=1024$ (1 – пониження степеня за допомогою квадратів, 2 – за допомогою кубів, 3 – використання СЗК, 4 – використання МДФ СЗК)

Висновки

У роботі проведено експериментальне дослідження програмної реалізації різних методів модулярного експоненціювання. Показано, що при малих розрядностях найбільшою швидкістю характеризується метод пониження степенів за допомогою кубів. Починаючи з 1024 біт найменший час для виконання операції модулярного

піднесення до степеня витрачається при застосуванні методу МДФ СЗК. Досліджено часову складність модулярного експоненціювання в залежності від ваги Хемінга. Встановлено, що найбільший час затрачається, коли вага Хемінга максимальна. При її зменшенні час виконання різко зменшується і надалі залишається майже постійним.

Список літератури

1. Горбенко, І. Д. Захист інформації в інформаційно- телекомунікаційних системах / І.Д. Горбенко, Т.О.Гриненко. - Харків: ХНУРЕ, 2004. - 368 с.
2. Норткатт, С. Обнаружение вторжений в сеть / С. Норткатт, Д. Новак. – М.: Лори, 2001. – 384 с.
3. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел. / В.К. Задірака, О.С. Олексюк. – К.: КИ, 2003. – 264 с.
4. Задірака, В.К. Комп'ютерна криптологія / В.К. Задірака, О.С. Олексюк. – Тернопіль, Київ, 2002. – 504 с.
5. Вербіцький, О.В. Вступ до криптології / О.В. Вербіцький. – Львів: ВНТЛ, 1998. – 247 с.
6. Петренко, А.Б. Аналіз часових атак на апаратний шифратор персонального засобу криптографічного захисту інформації «Шипка» / А.Б. Петренко, О.С. Шматок, С.А. Шматок, Є.О. Агеєнко // Наукоємні технології. - 2014. - № 2 (22). - С. 187-191.
7. Schindler, W. A timing attack against rash with the chinese remainder theorem / W. Schindler // Cryptographic Hardware and Embedded System. - 2000. - № 2. - P. 109–124.
8. Stewart, J. Python for Scientists / J. Stewart. - Cambridge: Cambridge University Press, 2014 - 230 p.
9. Downey, A. How to Think Like a Computer Scientist. Learning with Python / A. Downey, J. Elkner, C. Meyers. - Wellesley: Green Tea Press, 2012. - 243 p.
10. Николайчук, Я.М. Теорія джерел інформації / Я.М. Николайчук. – Тернопіль: ТзОВ «Терно–граф», 2010. – 536 с.
11. Касянчук, М. Алгоритм знаходження системи модулів модифікованої досконалої форми системи залишкових класів / М.М. Касянчук, Я.М. Николайчук, І.З. Якименко, Л.М. Тимошенко, Т.М. Долинюк // Матеріали Міжнародної науково-практичної конференції «Сучасні інформаційні та електронні технології». - Одеса, 26 — 30 травня 2014 р. – С. 115-116.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ МЕТОДОВ МОДУЛЯРНОГО ЭКСПОНЕНЦИРОВАНИЯ

М.Н. Касянчук, И.З. Якименко, Т.Н. Долинюк, Н.А. Рендзеняк

Тернопольский национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: kasyanchuk@ukr.net, jiz@tneu.edu.ua

Выполнение арифметических операций над многоразрядными числами является весьма важной задачей современной теории чисел и асимметричной криптографии. В работе проведено экспериментальное исследование временной сложности модулярного экспоненцирования с использованием среды программирования Python 3.4.0 различными методами: понижение степени посредством выделения квадратов (бинарный), кубов (3-арный), системы остаточных классов и ее модифицированной совершенной формы. Операции выполнялись над числами различной разрядности и с разным весом Хемминга. Показано, что при малых разрядностях наибольшей скоростью характеризуется метод понижение степеней с помощью кубов. Начиная с 1024 бит наименьшее время для выполнения операции модулярного возведения в степень расходуется при применении метода модифицированной совершенной формы системы остаточных классов. При исследовании временной сложности модулярного экспоненцирования в зависимости от веса Хемминга установлено, что наибольшее время затрачивается, когда вес Хемминга максимален. При его уменьшении время выполнения резко уменьшается и в дальнейшем остается почти постоянным.

Ключевые слова: асимметричная криптография, модульное экспоненцирование, понижение степени, модифицированная совершенная форма системы остаточных классов, временная сложность, вес Хемминга.

EXPERIMENTAL STUDY OF PROGRAM IMPLEMENTATION OF METHODS OF MODULAR EXPONENTIAL

M.M. Kasianchuk, I.Z. Yakymenko, T.M. Dolynyuk, N.A. Rendzenyak

Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: kasyanchuk@ukr.net, jiz@tneu.edu.ua

The arithmetic operations on multi-digital numbers performing is assigned as the mportant task of modern numerical theory and asymmetric cryptography. Present work was devoted to experimental study of time complexity of modular exponential with using of Python 3.4.0 programming platform by various methods, among them depleted of degree using selection of squares (binary), cubes (tertiary) residual classes system and its modified perfect shape. The operations were performed on different bit numbers and with different Hemets' weight. It is shown that at low bit the greatest rate of reduction method is characterized by using the powers of cubes. Since 1024 bit the least time to perform of operation of modular exponentiation power was exploited under the application of method of modified form of perfect system of residual classes. Under the evaluation of time complexity of modular exponential depending on Hemets' weight it was shown that most time was spent, when the Hemets'weight is maximal. With its reducing runtime drastically reduced and remained almost constant.

Keywords: asymmetric cryptography, modular exponential, degree depleted, residual classes system and its modified perfect shape, time complexity, Hemets' weight.

ОБ УСТОЙЧИВОМ ПРЕЦИЗИОННОМ МОДЕЛИРОВАНИИ ОПЕРАТОРА ЗАПАЗДЫВАНИЯ

А.А. Стопакевич¹, А.А. Стопакевич²

¹Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, Украина;

²Одесская национальная академия связи им. Попова,
ул. Кузнечная, 1, Одесса, Украина; e-mail: stopakevich@gmail.com

Исследуются особенности моделирования оператора запаздывания с использованием рядов Тейлора и Паде. Целью исследования является определение границ устойчивости аппроксимации запаздывания рядом Тейлора при увеличении числа членов ряда. Научной значимостью работы является уточнение условий применимости ряда Тейлора для аппроксимации оператора запаздывания, что стало особенно актуально в связи с распространением современных программных пакетов, позволяющих прецизионное моделирование сложных систем. Для определения границ устойчивости использован критерий Рауса. Проведено вычисление распределения корней аппроксимации для различного количества членов ряда и величины времени запаздывания. Получен вывод, что доказательства сходимости соответствующего функционального ряда недостаточно и, сходимость никак не гарантирует устойчивости аппроксимации на основе ряда.

Практическим значением результатов является обоснование требования исследования не только сходимости функционального ряда, но и его устойчивости в зависимости от порядка аппроксимации и параметров аппроксимируемого оператора.

Ключевые слова: аппроксимация, ряд, Тейлор, устойчивость, экспонента, оператор, запаздывание.

Введение

Проблема повышения точности моделирования сложных систем стала одной из наиболее актуальных в связи с широким распространением таких современных программных средств как, например, Matlab, Mathcad, Maple [1-2]. Однако, оказывается, что иногда стремление к высокой точности моделирования того или иного объекта приводит к потере устойчивости модели.

Одним из наиболее распространенных элементов моделей сложных систем является оператор чистого запаздывания [3], представляемый при использовании преобразования Лапласа экспонентой от отрицательной величины запаздывания, умноженной на оператор Лапласа [4]. Известно, что во многих публикациях экспонента, особенно матричная, определяются через ряд Тейлора [5-7], имеется множество работ, в которых точность аппроксимации экспоненты связывается с числом взятых членов ряда Тейлора, причем, чем больше взято членов, тем точнее аппроксимация [8-9]. Для повышения скорости сходимости аппроксимации (что известно практически, хотя и не доказано теоретически), на основе ряда Тейлора построена дробно-рациональная аппроксимация Паде [10].

Цель работы

Целью работы является исследование соотношения точности аппроксимации оператора запаздывания и устойчивости этой аппроксимации при использовании ряда Тейлора и аппроксимации Паде.

Основная часть

Общеизвестно, что экспонента аппроксимируется рядом Тейлора в виде:

$$e^{\alpha \cdot x} = \sum_{k=0}^{\infty} \frac{(\alpha \cdot x)^k}{k!}.$$

В соответствии с указанной аппроксимацией в теории систем экспоненту запаздывания, то есть оператор, полученный в результате преобразования Лапласа задержки сигнала на время τ , записывают в виде:

$$e^{-\tau \cdot s} = \frac{1}{\sum_{k=0}^n \frac{(\tau \cdot s)^k}{k!}},$$

где s – оператор Лапласа.

Однако оказывается, что такое представление не вполне корректно. При $n > 4$ выражение в правой части теряет устойчивость. Причем, граница устойчивости не зависит от времени запаздывания.

Докажем это аналитически для уравнения пятого порядка

$$e^{-\tau \cdot s} = \frac{1}{\frac{\tau^5}{120} s^5 + \frac{\tau^4}{24} s^4 + \frac{\tau^3}{6} s^3 + \frac{\tau^2}{2} s^2 + \tau \cdot s + 1}.$$

Для этого составим таблицу Рауса [4] (табл. 1).

Таблица 1.

Таблица Рауса для уравнения 5 порядка

Вспомогательные коэффициенты	Основные коэффициенты		
	$c_{11} = \tau^5 / 120$	$c_{12} = \tau^3 / 6$	$c_{13} = \tau$
	$c_{21} = \tau^4 / 24$	$c_{22} = \tau^2 / 2$	$c_{23} = 1$
$r_3 = c_{11} / c_{21} = 0.2 \cdot \tau$	$c_{31} = c_{12} - \tau_3 \cdot c_{22} = 0.4 \cdot \tau^4$	$c_{32} = c_{13} - \tau_3 \cdot c_{23} = 0.8 \cdot \tau$	
$r_4 = c_{21} / c_{31} = 5 \cdot \tau / 48$	$c_{41} = c_{22} - \tau_4 \cdot c_{32} = 5 \cdot \tau^2 / 12$	$c_{42} = c_{23} - \tau_4 \cdot c_{33} = 1$	
$r_5 = c_{31} / c_{41} = 0.96 \cdot \tau$	$c_{51} = c_{32} - \tau_5 \cdot c_{42} = -0.16 \cdot \tau$		
$r_6 = c_{41} / c_{51} = -2.6 \cdot \tau < 0$			

Поскольку $r_6 < 0$, то полином пятого порядка не устойчив. Можно показать, что неустойчивы и все полиномы более высокого порядка. И этот вывод не зависит от величины запаздывания. Для иллюстрации данного утверждения, вычислим и представим на рис. 1 распределение корней аппроксимации экспоненты для $n = 4, 5, 10, 20, 100, 1000$ и для $\tau = 0.1, 1, 5, 10, 50, 100$.

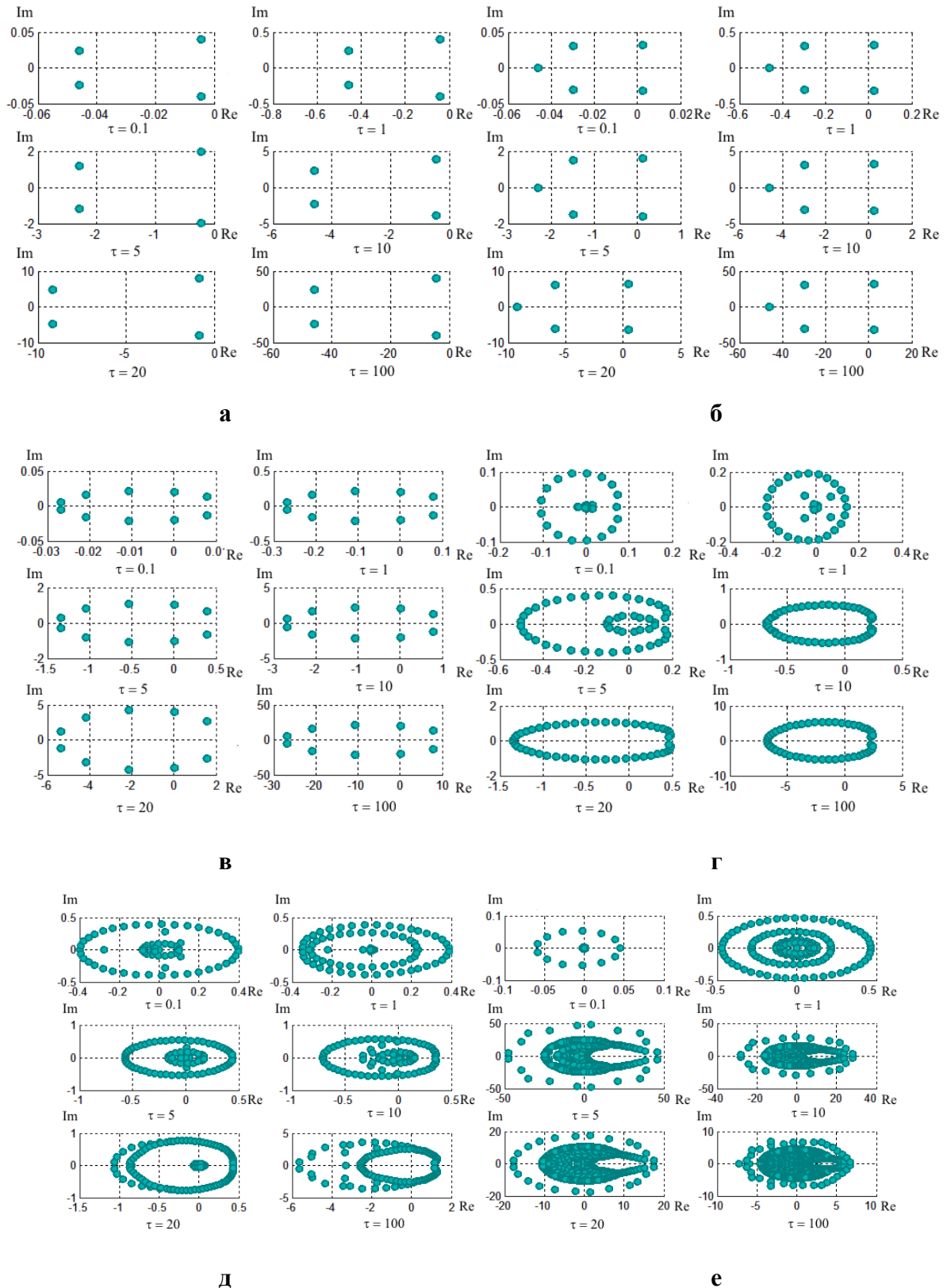


Рис. 1. Распределение корней экспоненты запаздывания при различных n : а – $n = 4$; б – $n = 5$; в – $n = 10$; г – $n = 20$; д – $n = 100$; е – $n = 1000$

Исследуем более подробно, как ведут себя корни s_i при изменении порядка аппроксимации. На рис. 2 и 3 показано изменение максимальной действительной части корня $\max(\text{real}(s_i))$, минимальной действительной части корня $\min(\text{real}(s_i))$, максимальной мнимой части корня $\max(\text{imag}(s_i))$, максимального размаха между

максимальной и минимальной действительными частями корней. Из рисунков видно, что с ростом порядка аппроксимации максимальное расстояние между максимальной и минимальной действительными частями корней растет, устремляясь к бесконечности. Скорость роста зависит от времени запаздывания экстремально, то есть она увеличивается при росте запаздывания от 0.1 до 5 и уменьшается при дальнейшем росте запаздывания.

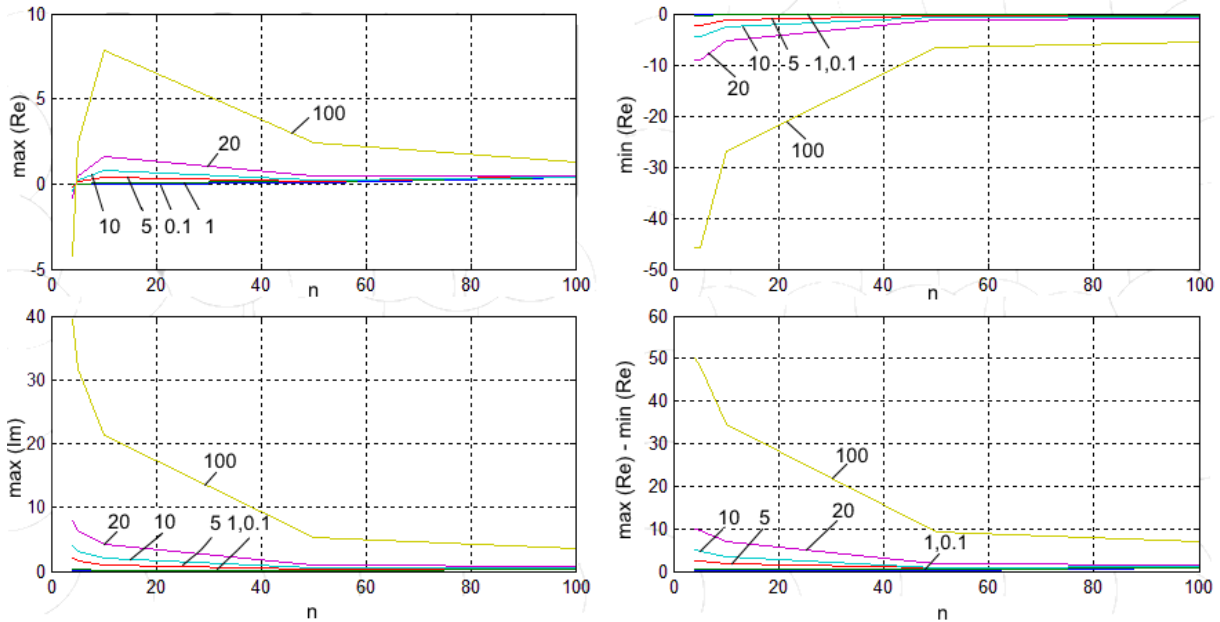


Рис. 2. Поведение корней в функции порядка аппроксимации при $n=5..100$ и различных τ

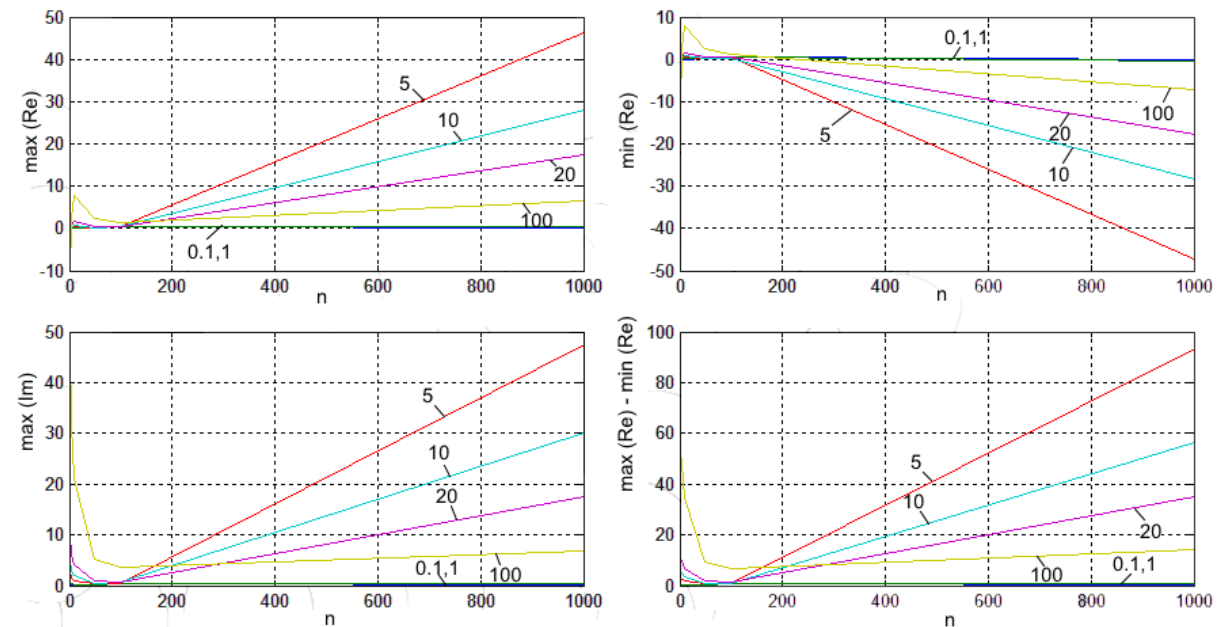


Рис. 3. Поведение корней в функции порядка аппроксимации при $n=5..1000$ и различных τ

Интересно отметить, что построенная на том же ряде Тейлора аппроксимация Паде имеет значительно больший запас устойчивости. Так для указанного выше набора времен запаздывания симметричная аппроксимация Паде устойчива до 75 порядка.

Причем, как и в случае ряда Тейлора, устойчивость не зависит от времени запаздывания. Однако, при порядке 75 корни оказываются настолько близкими к мнимой оси, что численное моделирование показывает неустойчивый процесс. Так что реальным порядком, при котором аппроксимация сходится, является 70. И действительно, с увеличением порядка постепенно улучшается качество аппроксимации.

Результаты исследования

Результаты исследования границ устойчивости аппроксимации оператора запаздывания рядом Тейлора показывают, что количество допустимых членов ряда для аппроксимации экспоненциальной функции равно пяти, с его превышением теряется устойчивость аппроксимации. Анализ корней при изменении порядка аппроксимации показывает, что с ростом порядка аппроксимации максимальное расстояние между максимальной и минимальной действительными частями корней растет, устремляясь к бесконечности. В то же время использование симметричной аппроксимации Паде дает устойчивое решение, не зависящее от времени запаздывания, при большом порядке теоретически равном 75, а практически - 70. Точность аппроксимации Паде с увеличением числа членов, как и ожидалось, плавно увеличивается.

Выводы

При использовании аппроксимации операторов доказательства сходимости соответствующего функционального ряда недостаточно и, собственно, сходимость никак не гарантирует применимости ряда. Помимо сходимости необходимо исследовать устойчивость и ее поведение в зависимости от порядка аппроксимации и, возможно, параметров аппроксимируемого оператора.

Список литературы

1. Алексеев, В.Р. Решение задач вычислительной математики в пакетах MathCAD 12, MATLAB 7, Maple 9 / В.Р. Алексеев, О.В. Чеснокова. – М.: ИТ-Пресс, 2006. – 360 с.
2. Коробейников, А.Г. Разработка и анализ математических моделей с использованием MATLAB и Maple / А.Г. Коробейников. – СПб.: СПбГУ ИТМО, 2010. – 280 с.
3. Бесекерский, В.А. Теория систем автоматического управления / В.А. Бесекерский, Е.П. Попов. – СПб.: Профессия, 2003. – 395 с.
4. Огнев, С.П. Вариантные аппроксимации звена запаздывания. / С.П. Огнев // Сборник научных трудов SWorld. Технические науки. – 2011. – Вып.3. – С. 25-29.
5. Лаврентьев, М. А. Методы теории функций комплексного переменного / М.А. Лаврентьев, Б. В. Шабат. – М.: Наука, 1987. – 425 с.
6. Moler, C. Nineteen Dubious Ways to Compute the Exponential of a Matrix, Twenty-Five Years Later. Society for Industrial and Applied Mathematics / C. Moler, C. Loan // SIAM Rev. – 2003. – Вып. 45. – С. 3-49.
7. Shao, M. Aggressively truncated Taylor series method for accurate computation of exponentials of essentially nonnegative matrices / M. Shao, W. Gao, J. Xue // SIAM. J. Matrix Anal. & Appl. – 2014. – Вып. 35. – С. 317–338.
8. Ильин, В. А. Математический анализ, ч. 1 / В.А. Ильин, В. А. Садовничий, Бл. Х. Сендов. – М.: Проспект, 2004. – 590 с.
9. Thomas, G. Calculus and Analytic Geometry / G. Thomas, R. Finney. – Boston, Ma: Addison Wesley, 1996. – 650 с.
10. Бейкер, Дж. Аппроксимации Паде / Дж. Бейкер, П. Грейвс-Моррис. – М.: Мир, 1986.
11. Макаров, И.М. Линейные автоматические системы / И.М. Макаров, Б.М. Менский. – М.: Машиностроение, 1977. – 370 с.

СТІЙКЕ ПРЕЦИЗІЙНЕ МОДЕЛЮВАННЯ ОПЕРАТОРА ЗАПІЗНЕННЯ

О.А. Стопакевич, А.О. Стопакевич

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

Досліджуються особливостей моделювання оператора запізнення із використанням рядів Тейлора і Паде. Метою дослідження є визначення меж стійкості апроксимації запізнення рядом Тейлора при збільшенні кількості членів ряду. Науковою значимістю роботи є уточнення умов застосування ряду Тейлора для апроксимації оператора запізнення, що стало особливо актуально в зв'язку із поширенням сучасних програмних пакетів, які дозволяють прецизійне моделювання складних систем. Для визначення меж стійкості використано критерій Рауса. Був проведений розрахунок розподілення корнів апроксимації для різної кількості членів ряду і величини часу запізнення.

Отримано висновок, що доказу збіжності відповідного функціонального ряду недостатньо, і, збіжність ніяк не гарантує стійкості апроксимації на основі ряду. Практичним значенням результатів роботи є обґрунтування вимоги дослідження не тільки збіжності функціонального ряду, але і його стійкості в залежності від порядку апроксимації і параметрів апроксимуючого оператора.

Ключові слова: апроксимація, ряд, Тейлор, стійкість, експонента, оператор, запізнення.

PRECISION RACK DESIGN OPERATOR DELAY

O.A. Stopakevych, A.O. Stopakevych

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

The article is devoted to the research of delay operator modeling features using Taylor and Pade series. The purpose of the research is to determine the stability boundaries for approximation of the delay operator by Taylor series when the number of terms in the series is increasing. The scientific significance of the research states the Taylor series applicability conditions for the delay operator modelling. The conditions are important for modern software that allows precise modeling of complex systems. The Routh criterion is used to determine the stability boundaries. The calculations of the delay operator approximation poles for different number of series terms and the delay value were made.

The scientific value of the research is the conclusion that the proof of corresponding functional series convergence is insufficient to use this series in modelling systems. The convergence of series does not guarantee the approximation stability and, respectively, applicability of the series.

The practical value of the work results is grounded on the requirement to investigate not only convergence of the series, but also the approximation stability taking into account the approximation order and the operator parameters.

Keywords: approximation, series, Taylor, stability, Pade, operator, time delay, modelling.

УСКОРЕННЫЙ АЛГОРИТМ ОДНОСТОРОННЕГО ВЕТВЛЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ С БУЛЕВЫМИ ПЕРЕМЕННЫМИ

Б.И. Юхименко

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

В работе приведен ускоренный алгоритм решения задачи линейного программирования с булевыми переменными. Алгоритм относится к классу алгоритмов метода ветвей и границ с односторонним ветвлением. Особенностью является то, что приведен способ получения исходного варианта решения и способ приоритетного ранжирования компонент вектора решения. Дан пример определения оптимального решения согласно предполагаемому алгоритму.

Ключевые слова: отсеивание, приоритетная очередь, одностороннее ветвление.

Введение

Принятие решений в любой сфере деятельности человека неизбежная процедура. Решение всегда выбирается так, чтобы оно было более эффективным, а в некоторых случаях и оптимальным. Такое решение достигается путем сравнения отдельных альтернативных решений, количество которых может быть как бесконечным, так и конечным. С математических позиций конечное множество решений имеют дискретные задачи оптимизации. Дискретная оптимизация, как область науки, является постоянно развивающейся и привлекает множество специалистов. В настоящее время насчитывается большое количество алгоритмов, методов и подходов решения задач данного класса.

Цель статьи

Значительное место среди методов решения задач дискретной оптимизации занимают комбинаторные методы. В своей сущности эти методы используют конечность множества вариантов. Комбинаторные методы наиболее простые и достойны в практической реализации. Хорошо известный метод ветвей и границ [1] также относится к классу комбинаторных методов, является переборным методом, по своей сложности относится к классу NP -полных алгоритмов. В них полный перебор вариантов заменяется частичным перебором. Эффективность алгоритмов предопределяется выделением подмножества перебираемых (перспективных) вариантов. Чем это подмножество содержит меньше вариантов, тем алгоритм работает эффективнее в смысле скорости сходимости. Любой способ увеличения отсеивания вариантов в какой-то степени улучшает скорость сходимости. В данной статье приводится алгоритм метода ветвей и границ с односторонним ветвлением. Увеличение отсеивания неперспективных вариантов, в первую очередь, получается за счет изначального определения исходного варианта. Приведена очередь приоритетов

компонент вектора решений. Это упрощает перебор вариантов и ускоряет получение оптимального.

Анализ основных исследований и публикаций

В известных алгоритмах метода ветвей и границ для решения задачи целочисленного линейного программирования (ЦЛП) отсеивание неперспективных вариантов ведется различными способами.

В алгоритме Лэнд и Дойч [2], имеющего в основе симплекс метод, поочередно исключаются нецелочисленные значения в районе оптимального значения нецелочисленной компоненты. Пусть эта компонента x_k . Множество вариантов делится на два подмножества. В одном подмножестве будут рассматриваться варианты, в которых $x_k \leq [x_k]$, а во втором – $x_k \geq [x_k] + 1$ - где $[x_k]$ - целая часть x_k . Варианты, в которых компоненты x_k находится в интервале $[x_k] < x_k < [x_k] + 1$ не будут рассматриваться.

В алгоритме Литла и др. [3] для решения задачи о коммивояжере, которого можно считать предком метода ветвей и границ в целом, предусмотрено довольно сильное правило отсеивания вариантов. Подмножество вариантов, содержащее неперспективный переезд между парой городов, довольно часто безвозвратно исключается из рассмотрения. Не перспективность переезда оценивается потерей доли значения целевой функции в случае не включения рассматриваемой пары в цикл объезда городов.

В классических алгоритмах метода вервей и границ, использующих правило расширения – суждения множества вариантов [4] для получения оценок и последовательное построение решения [5] как средство разбиения множества вариантов на подмножества отсеивание вариантов осуществляется за счет удачно подобранного способа конкретизации переменных. В работе [6] экспериментально было показано, что на скорость сходимости значительной степени влияет процедура определения компоненты, включаемой в решение и являющейся параметром разбиения множества вариантов на подмножества. На отсеивание вариантов также влияет точность получаемых оценок. Признак оптимальности, практически не подвергавшийся обновлению от момента появления метода, выражается через оценки подмножеств вариантов. Чем ближе значение оценки подмножества к значению целевой функции варианта, тем больше подмножеств исключается из рассмотрения и быстрее выявляется оптимальность варианта.

Алгоритм Балаша [7] с так называемым односторонним ветвлением имеет другой способ отсеивания вариантов. Конкретизируются только единичные компоненты вектора решений. Компоненты принимают нулевые значения, если они не могли стать единичными по следующим причинам. Во-первых, из-за жесткости системы ограничений. Вторая причина состоит в том, что присвоение единичного значения не позволит улучшить значение целевой функции по сравнению с уже имеющимся рекордом. Предложенный автором алгоритма способ выбора компонент-претендентов на значение «1», довольно хороший и оптимальное решение получается быстро. Прием, заменяющий признак оптимальности, не достаточен. Процедура подтверждения того, что найденный вариант оптимальный, часто более вычислительноемкий, чем сама процедура его определения.

Способ отсеивания вариантов, стоящий во главе признака оптимальности в алгоритмах с односторонним ветвлением, полностью зависит от поиска перспективных компонент, которым будет присвоено значение «1». Модификации таких алгоритмов «усиливающих» процедуру отсеивания вариантов, увеличит скорость сходимости.

Нижче буде приведено алгоритм з одностороннім ветвленим. Алгоритм навеян ідеями алгоритма Балаша, однак має деякі особливості, що покращують швидкість збіжності. Спочатку визначається варіант рішення, значення цільової функції якого розглядається як рекорд. Процедура визначення початкового варіанта в обчислювальному сенсі нескладна. В основу цієї процедури закладено спосіб упорядкування за перспективністю компонент вектора рішень. Сама перспективність оцінюється величиною сумарних неувязок в системі обмежень, помноженою на відносну величину відповідуючої компоненти вектора цільової функції. Такого типу упорядкування компонент використовувалося в алгоритмі з двохстороннім ветвленим і значно збільшило швидкість збіжності [6]. Решта частина алгоритму це підтвердження оптимальності отриманого варіанта. Якщо варіант виявиться не оптимальним, то йде його покращення, використовуючи ті ж оцінки перспективності компонент. Не перспективні компоненти відсіваються.

Основная часть

Алгоритм використовується для рішення задач ЦЛП в постановці

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

при обмеженнях

$$\begin{aligned} \sum_{j=1}^n a_{ij} x_j &\leq b_i, \quad i = \overline{1, m}; \\ x_j &\in \{0, 1\} \quad j = \overline{1, n}, \end{aligned}$$

де всі a_{ij} , b_i і c_j є неотрицательними числами.

Введемо деякі позначення і твердження. Індеси компонент, претендентів на значення «1» складають множину V_j^k , де k крок алгоритму

$$V_j^k = \{j / (b_i^k - a_{ij}) \geq 0, \quad \forall_i\};$$

Оцінка перспективності компонент x_j для $j \in V_j^k$ визначається за формулою

$$p_j = \sum_{i=1}^m (b_i - a_{ij}) \cdot \sqrt{c_j / \min c_j}, \quad j \in V_j^k.$$

За величиною p_j визначається черга пріоритетності компонент x_j , що приймають значення «1». Індеси j складають множину PX і визначають пріоритетну чергу компонент x_j . Множина PX є домінуючою при побудові вектора $X = \{x_j\}_{j=\overline{1, n}}$ на будь-якому рівні роботи алгоритму. Значення цільової функції $R = \sum_{j=1}^n c_j x_j$ називається рекордом, якщо воно найбільше серед уже розглянутих варіантів.

B – вектор правых частей в системе ограничений, B^k – рабочий вектор, используемый на k -ом шаге алгоритма. Во второй части алгоритма используются еще два массива: $\tilde{P}$ – индексы нулевых компонент, имеющихся в варианте X и $\bar{X}$ – рабочий вариант решения задачи.

Ниже приводится описание самого алгоритма, состоящего из двух частей:

- определение исходного варианта и рекорда;
- проверка отсутствия лучшего варианта и формирования нового варианта.

Первая часть

Шаг 1. Формирование массива оценок перспективности компонент вектора решений $P = \{p_j\} \quad j = \overline{1, n}$;

Шаг 2. Упорядочение компонент p_j массива P в порядке не возрастания и формирование массива индексов $PX = \{j_i\}_{i=\overline{1, n}}$.

Шаг 3. Определение варианта решений $X = \{x_j\}_{j=\overline{1, n}}$.

3.1. $\kappa = 1$; $b_i^k = b_i \quad \forall_i$;

3.2. $j = PX(k)$;

3.3. если $(b_i^k - a_{ij}) \geq 0 \quad \forall_i$, то $x_j = 1$; $b_i^k = (b_i^k - a_{ij}) \quad \forall_i$ и к 3.5;

3.4. $x_j = 0$;

3.5. $k = k + 1$; если $k \leq n$, то к 3.2;

3.6. вычисление рекорда $R = \sum_{j=1}^n c_j x_j$.

Вторая часть алгоритма, связанная с проверкой о возможности улучшения варианта X и если это возможно, то улучшение.

Шаг 1. Формирование массива $\tilde{P}$ индексов нулевых компонент варианта X .

1.1. $j = 1$; $l = 0$;

1.2. если $x_j > 0$, то 1.4;

1.3. $l = l + 1$; $P_l = j$;

1.4. $j = j + 1$, если $j \leq n$, то 1.2;

Шаг 2. Исходные условия.

$k = 1$;

2.1. $Z = 0$; $\bar{x} = \emptyset$;

2.2. $b_i^k = b_i \quad \forall_i$;

2.3. $j = \tilde{P}(k)$; $\bar{x}_j = 1$;

2.4. $b_i^k = (b_i^k - a_{ij}) \quad \forall_i$;

Шаг 3. Формирование множества хороших компонент.

3.1. $V_j^k = \{r = \overline{1, n} / (b_i^k - a_{ir}) \geq 0 \quad \forall_i\}$;

3.2. если $V_j^k = \emptyset$, то шаг 7;

Шаг 4. Формирование варианта решения.

$s = 1$;

4.1. $r = P_x(s)$;

4.2. если $(r = j)$ или $(r \in V_j^k)$, то шаг 5;

4.3. $\bar{x}(r) = 1$; $Z = Z + C_r$; $b_i^k = (b_i^k - a_{ir}) \quad \forall_i$; $V_j^k = V_j^k - r$;

4.4. если $V_k^k = \emptyset$, то шаг 5;

4.5. если $Z + \sum_{j \in V_j^k} c_j \leq R$, то шаг 7;

Шаг 5. $s = s + 1$; если $s \leq n$, то 4.1;

Шаг 6. Если $Z > R$, то $R = Z$; $X = \bar{X}$;

Шаг 7. $k = k + 1$; если $k \leq l$, то 2.1;

Шаг 8. R и X являются результатом.

Пример. Найти оптимальное решение задачи в постановке

$$Z = \max (4x_1 + 7x_2 + 2x_3 + x_4 + 3x_5 + 5x_6)$$

при ограничениях

$$\begin{cases} 2x_1 + 5x_2 + x_3 + 2x_4 + 3x_5 + 4x_6 \leq 14 \\ 4x_1 + 3x_2 + 2x_3 + 4x_4 + 2x_5 + 3x_6 \leq 11 \\ x_j \in \{0,1\} \quad j = \overline{1,6}. \end{cases}$$

Таблица 1.

Последовательное решение рассматриваемого примера

Переменная и значение	b_i^k	Z	V_j^k	Ситуация
$x_2 = 1$	12 7	7	$\{1,3,4,5,6\}$	
$x_6 = 1$	8 4	$7+5=12$	$\{1,3,4,5\}$	
$x_1 = 4$	2 0	$12+4=16$	$\emptyset$	$x = (110001)$; $R = 16$.
$x_3 = 1$	13 9	2	$\{1,2,4,5,6\}$	$\tilde{P} = \{3,4,5\}$
$x_2 = 1$	8 6	$2+7=9$	$\{1,4,5,6\}$	
$x_6 = 1$	4 3	$9+5=14$	$\{4,5\}$	$(14+1+3) > 16$
$x_5 = 1$	1 1	$14+3=17$	$\emptyset$	$x = (011011)$; $R = 17$.
$x_4 = 1$	12 7	1	$\{1,2,3,5,6\}$	$\tilde{P} = \{4,5\}$
$x_2 = 1$	7 4	$1+7=8$	$\{1,3,5,6\}$	
$x_6 = 1$	3 1	$8+5=13$	$\emptyset$	$13 < 17$
$x_5 = 1$	10 8	3	$\{1,2,3,4,6\}$	$\tilde{P} = \{5\}$
$x_2 = 1$	5 5	$3+7=10$	$\{1,3,4,6\}$	
$x_6 = 1$	1 2	$10+5=15$	$\{3\}$	$15+7=22$ улучшений нет $\tilde{P} = \emptyset$

Оценка перспективности каждой искомой величины

$$P_1 = (14 - 2 + 11 - 4) \cdot \sqrt{4} = 19\sqrt{4} = 38.0;$$

$$P_2 = 17\sqrt{7} = 45.0;$$

$$P_3 = 22\sqrt{2} = 31.1;$$

$$P_4 = 19\sqrt{0.5} = 13.4;$$

$$P_5 = 20\sqrt{3} = 34.6;$$

$$P_6 = 18\sqrt{5} = 40.2.$$

$$P_x = \{2, 6, 1, 5, 3, 4\}.$$

Оптимальное решение $X = (0\ 1\ 1\ 0\ 1\ 1)$; $Z = 17$.

Заключение

Приведенный алгоритм имеет ряд положительных моментов по сравнению с алгоритмами с односторонним ветвлением. К ним относится определение изначального варианта решения и рекорда – значение целевой функции. Далее, приведенная очередность включения в решении компонент с единичными значениями также значительно улучшает скорость сходимости. Сам перебор вариантов построен на замене нулевых значений вектора решений поочередно единичными, что значительно уменьшает количество перебираемых вариантов. Проведенный пока не большой числовой эксперимент дал утешительные результаты. Конечно, проверить работу необходимо на большом количестве числовых задач и, по возможности, дать теоретическое обоснование в смысле скорости сходимости. Работа над алгоритмом продолжается.

Список литературы

1. Корбут, А.А. Дискретное программирование / А.А. Корбут, Ю.Ю. Финкельштейн. – М.: Наука, 1969. – 368 с.
2. Land, A.H. An automatic method of solving discrete programming problems / A.H. Land, A. G. Doig // *Econometrica*, 1960. – V. 28. – №3. – С. 497-520.
3. Little, J.D. C. An algorithm for the traveling salesman problem / K.G. Murty, D. W.Sweeney, C. Karel // *Operat. Res.*, 1963. – Т. 11. – №6. – С. 972-989.
4. Шкурба, В.В. Конструктивные подходы к решению задач дискретной оптимизации / В. В. Шкурба // В кн. «IV симпозиум по экстремальным задачам» Тезисы докладов, Каунас, 1969. – С. 15-17.
5. Михалевич, В.С. Последовательные алгоритмы оптимизации и их применение, I, II / В.С. Михалевич // *Кибернетика*. – 1965. – №1. – С. 45-55; №2. – С. 85-89.
6. Юхименко, Б.И. Сравнительная характеристика алгоритмов метода ветвей и границ для решения задач целочисленного линейного программирования / Б.И. Юхименко, Ю.Ю. Козина // *Тр. Одес. политехн. ун-та*. – 2005. – Вып. 2. – С. 199-204.
7. Balas, E. An additive algorithm for solving linear programs with zero-one variables / E. Balas // *Operat. Res.* – 1965. – V.13. – №4. – С. 517-546.

**ПРИСКОРЕНИЙ АЛГОРИТМ ОДНОСТОРОННЬОГО ГАЛУЖЕННЯ ДЛЯ ВИРІШЕННЯ
ЗАВДАНЬ ЛІНІЙНОГО ПРОГРАМУВАННЯ З БУЛЕВИМИ ЗМІННИМИ**

Б.І. Юхіменко

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

В роботі даний невеликий огляд комбінаторних методів, які представлені в початкових виданнях. Наведені передумови до необхідності удосконалення математичного апарату розв'язання задач цілочисельного лінійного програмування. Основною розробкою є алгоритм з одностороннім гілкуванням для розв'язання задачі лінійного програмування з булевими змінними. Дана покрокова структура алгоритму, вирішений числовий приклад.

Ключові слова: відсіювання, пріоритетна черга, одностороннє розгалуження.

**SINGLE ACCELERATE THE ALGORITHM BRANCHES FOR SOLVING LINEAR
PROGRAMMING PROBLEMS WITH BOOLEAN VARIABLES**

B.I. Ukhimenko

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

The paper presents a short review of combinatorial methods presented in the primary publications. Preconditions are listed for the need to improve conditions of the mathematical tool of solving problems of integer linear programming. A one-way branching algorithm is the main development is for solving problems of linear programming with Boolean variables. The paper presents turn-based structure of the algorithm, was solved a numerical example.

Keywords: screening, priority queue, unilateral branching.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 5, номер 4, 2015. Одеса – 98 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 5, номер 4, 2015. Одесса – 98 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 5, No. 4, 2015. Odesa – 98 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №3 від 08.12.2015)

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