МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 3, № 1

Volume 3, No. 1

Одеса – 2013
Odesa – 2013

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

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

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

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

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

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

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 734 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 734 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 5-12

МЕТОД ВЫЯВЛЕНИЯ СИММЕТРИЧНОГО КЛОНИРОВАНИЯ ПРИ ФАЛЬСИФИКАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

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

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

Предлагается теоретически обоснованная модификация метода выявления результатов одного из наиболее часто используемых при фальсификациях цифровых изображений инструментов, реализованных в большинстве графических редакторов – клонирования, разработанного авторами ранее. Базовый метод основан на анализе сингулярных чисел блоков матрицы изображения. Предложенная модификация позволяет эффективно выявлять замещающие области, симметрично отраженные по вертикали/горизонтали и/или подвергнутые повороту на угол, кратный 90°, что подтверждается приведенными результатами вычислительных экспериментов. Разработанный метод может быть эффективно использован для выявления фальсификации цифрового видео.

Ключевые слова: фальсификация цифровых изображений, клонирование, симметричное клонирование, фотомонтаж, матрица, сингулярное число

Введение

Цифровые изображения (ЦИ) в настоящее время стали неотъемлемой частью бытовой и профессиональной деятельности человека. Развитие цифровой техники для создания и редактирования ЦИ, а также общедоступность графических редакторов обуславливает необходимость усовершенствования существующих и создания новых методов выявления нарушений целостности ЦИ.

Часто при обработке ЦИ, в частности, при их фальсификации, возникает необходимость дублирования или удаления каких-либо объектов. Удобнее всего с точки зрения сохранения надежности восприятия получаемого изображения использовать для этого фрагменты того же изображения: замещающие области (ЗО) выбираются, как правило, вблизи обрабатываемого объекта, чтобы минимизировать отличия света/тени, яркости/контрастности. И в случае дублирования объекта, и в случае его сокрытия происходит копирование групп пикселей из одной части изображения в другую путем параллельного переноса. Данная операция часто производится с помощью инструмента, реализованного в большинстве графических редакторов, называемого Штамп (Клон). Разновидностью клонирования является симметричное клонирование (СК) – зеркальное отображение клонированной области в горизонтальной/вертикальной плоскостях.

В настоящий момент в открытой печати широко обсуждаются вопросы разработки методов и алгоритмов, целью которых является выявление клонированных участков ЦИ, однако существующие современные методы и алгоритмы не лишены значительных недостатков: большинство из них требует значительных вычислительных затрат [1–5], самые эффективные из них (алгоритмы SIFT и SURF [6, 7]) недостаточно эффективны для объектов простой формы и без ярко выраженной текстуры, а также в случае

клонированных участков малого размера, ориентированы на форматы хранения изображения [8].

Все вышесказанное оставляет важной и актуальной задачу разработки принципиально новых методов и алгоритмов выявления клонированных участков изображения.

Цель статьи и постановка исследований

В [9] на основе общего подхода к анализу состояния и технологии функционирования информационных систем [10] был разработан новый метод выявления клонированных областей. Идея метода состояла в нахождении блоков матрицы изображения, имеющих одинаковые сингулярные числа (СНЧ), реализуемая при помощи анализа матрицы клонирования [9]. В связи с тем, что основная информация ЦИ несется низкими частотами, которые, в свою очередь, отвечают, в основном, наибольшим СНЧ [11], с целью уменьшения вычислительных затрат для выявления клонированных блоков, полученных в результате стандартного разбиения матрицы, в разработанном в [9] методе анализ ЦИ проводится путем попарного сравнения на равенство значений сумм 4 наибольших СНЧ блоков между собой. При использовании данного метода для выявления СК было установлено, что при малых размерах замещающей области (ЗО) он является недостаточно эффективным.

Целью работы является повышение эффективности выявления клонированных замещающих областей, симметрично отраженных и/или подвергнутых повороту на угол, кратный 90°, путем модификации метода выявления клонирования, основанного на общем подходе к анализу состояния и теории функционирования информационной системы [9].

Для достижения цели необходимо решить следующие *задачи*:

1) Обосновать теоретически характерные свойства СНЧ симметрично клонированных блоков матрицы цифрового изображения.

2) Исследовать особенности проявления свойств сингулярных чисел блоков матрицы цифрового изображения в случае симметричного клонирования и/или поворота на угол, кратный 90°, в системе чисел с плавающей точкой.

3) Адаптировать метод выявления клонирования для эффективного выделения клонированных замещающих областей, симметрично отраженных и/или подвергнутых повороту на угол, кратный 90°.

Основная часть

Математически СК области ЦИ представляет собой умножение матрицы клонированной области на матрицу перестановок. Имеет место следующая теорема.

Теорема. Симметричное клонирование не меняет сингулярных чисел подматрицы матрицы цифрового изображения, которая (подматрица) отвечает замещающей области.

Доказательство. Математически СК для части ЦИ с $k \times k$-матрицей A может быть представлено в матричном виде как: AP (при горизонтальном отражении); PA (при вертикальном); PAP (при отражении по обоим направлениям одновременно), где P — $k \times k$-матрица перестановок [12]:

$$P = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & \dots & 0 & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

Пусть

$$A = U\Sigma V^T \tag{1}$$

— сингулярное разложение матрицы A, где U, V — ортогональные $k \times k$-матрицы левых и правых сингулярных векторов соответственно, а Σ — диагональная матрица СНЧ A [12]. Тогда для AP с учетом (1) и симметричности P будет иметь место равенство:

$$AP = U\Sigma V^T P = U\Sigma\left(PV\right)^T. \tag{2}$$

Поскольку для матрицы PV имеет место равенство:

$$\left(PV\right)^T\left(PV\right) = V^T PPV = I,$$

где I — единичная матрица соответствующего размера, то (2) представляет сингулярное разложение матрицы AP, сингулярные числа которой представлены диагональю Σ, т.е. совпадают с СНЧ матрицы A.

Для матриц PA и PAP с учетом (1) аналогично получим:

$$PA = \left(PU\right)\Sigma V^T, \tag{3}$$

$$PAP = P\left(U\Sigma V^T\right)P = \left(PU\right)\Sigma\left(PV\right)^T, \tag{4}$$

при этом для матрицы PU имеет место равенство:

$$\left(PU\right)^T\left(PU\right) = U^T PPU = I,$$

т.е. PU, как и PV является ортогональной, а значит (3), (4) представляют сингулярные разложения матриц PA и PAP соответственно, откуда видно, что СНЧ этих матриц совпадают с СНЧ матрицы A, что и требовалось показать.

Таким образом, теоретически доказано, что СК не меняет СНЧ ЗО. Однако, как уже было упомянуто выше, на практике при тестировании разработанного в [9] метода для выявления областей СК возникало значительное количество ошибок первого рода. Для наглядности проиллюстрируем это на примере.

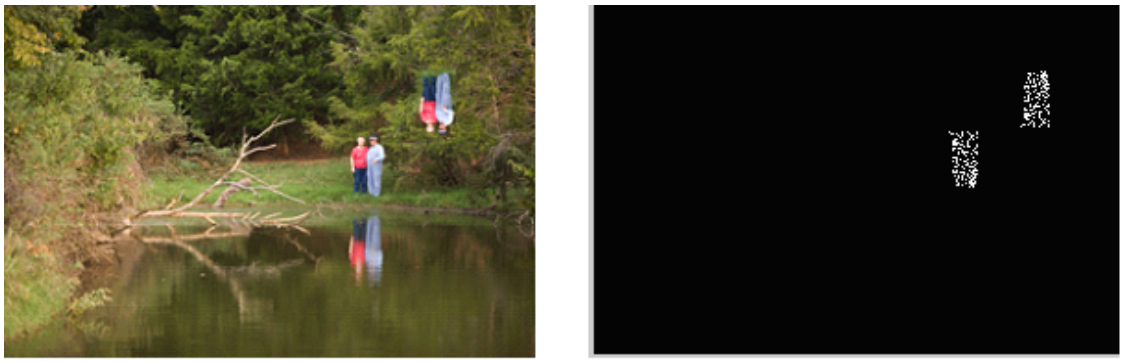
Для выявления СК, как и в случае клонирования без каких-либо дальнейших отражений и поворотов замещающей области, поставим в соответствие ЦИ матрицу клонирования (МК), каждый элемент которой соответствует одному блоку и равен нулю в случае несовпадения значения суммы четырех наибольших СНЧ данного блока со значениями сумм остальных блоков, 1 в случае выявления совпадений. Области, содержащие единицы в МК, соответствуют искомой области фальсификации ЦИ, а также той его части, которая являлась прототипом ЗО.

Фальсифицируем ЦИ способом клонирования одной части ЦИ – замещающей области, в другую часть этого же изображения, отразив при этом клонированную ЗО по горизонтали (рис. 1(а)), повернув ЗО против часовой стрелки на 90° (рис. 2(а)). Отражение по вертикали, а также поворот в любом из направлений на угол, кратный 90°

принципиально не меняет поведения элементов МК. На МК, соответствующей фальсифицированному ЦИ, представленной в виде бинарного изображения (рис. 1(б), 2(б)), ЗО и ее прототип в целом нашли свое отражение. Однако внутри ЗО оказались блоки, которые, будучи клонированными, не определены как таковые. В случае малого размера ЗО это принципиально может привести к пропуску фальсифицированного ЦИ – ошибке I рода.

Как доказано выше, отражение матрицы по любому из оговоренных направлений не меняет ее СНЧ, однако программная реализация разработанного метода выявления клонирования требует учета особенностей машинной арифметики. Эти особенности приводят к тому, что, в силу накопления вычислительной погрешности, для некоторых симметрично клонированных блоков их СНЧ могут отличаться друг от друга, причем это отличие, в общем случае, сравнимо с ошибкой округления (табл. 1).

Аналогичная картина для СНЧ блоков матрицы ЦИ имеет место и в случае поворота блока на угол, кратный 90°.



а **б**

Рис. 1. Выявление фальсификации: а – фотомонтаж на основе симметричного клонирования; б – МК фальсифицированного ЦИ

а **б**

Рис. 2. Выявление фальсификации: а – фотомонтаж на основе поворота клонированного участка на угол, кратный 90°; б – МК фальсифицированного ЦИ

Таблица 1.

Отличия сингулярных спектров симметрично клонированных блоков

№ СНЧ	СНЧ симметрично клонированного блока	СНЧ прототипа симметрично клонированного блока
1	383.826924389038	383.826924389040
2	38.8159972854393	38.8159972854394
3	12.7508929678442	12.7508929678442
4	11.2552643837216	11.2552643837216
5	9.17239356953573	9.17239356953573
6	6.16090100655953	6.16090100655953
7	4.61823508109017	4.61823508109020
8	0.725686359495353	0.725686359495354

Для эффективного выявления ЗО проведена модификация метода, разработанного в [9], в результате которой его основные шаги выглядят следующим образом.

1) Разбить матрицу F ЦИ на пересекающиеся 8×8-блоки

$$F_{ij},$$

$$i = 1,2\ldots,\left[(n-7)/8\right],\ j = 1,2\ldots,\left[(m-7)/8\right],$$

так, чтобы каждый блок отличался от соседнего на один столбец (строку).

2) Построить матрицу S с элементами

$$s_{ij} = \sum_{k=1}^{4}\sigma_k\ ,$$

$$i = 1,2\ldots,\left[(n-7)/8\right],\ j = 1,2\ldots,\left[(m-7)/8\right],$$

где $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ – наибольшие СНЧ соответствующего блока F_{ij}.

3) Построить МК C с элементами c_{ij}, $i = 1,2\ldots,\left[(n-7)/8\right]$, $j = 1,2\ldots,\left[(m-7)/8\right]$, каждый из которых отвечает блоку F_{ij} ЦИ. Для определения c_{ij} сравнить s_{ij} попарно со всеми элементами матрицы S:

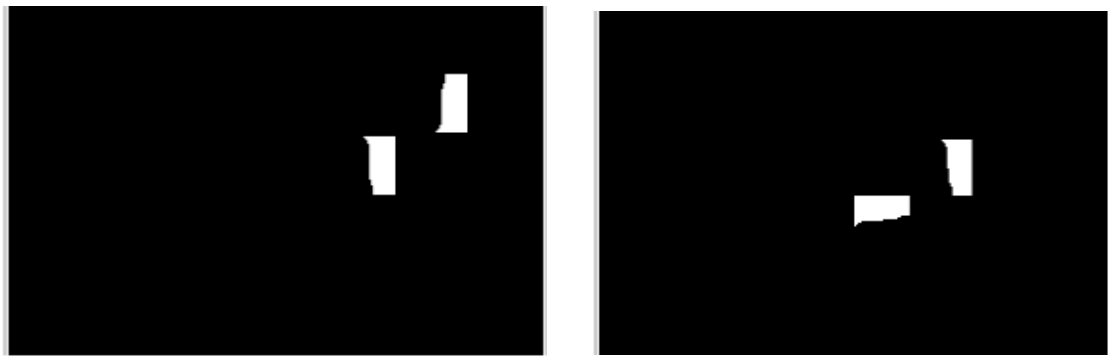
если для s_{ij} найдется элемент $s_{kl}, k\neq i\vee l\neq j$, матрицы S, что $\left|s_{ij}-s_{kl}\right|<\delta$, где δ — значение порога,

то $c_{ij}=1$,

иначе $c_{ij}=0$.

4) Элементы $c_{ij}=1$ матрицы C соответствуют клонированным блокам ЦИ.

Значение порога $\delta = 10^{-7}$ было получено экспериментально, при этом было установлено, что увеличение δ приводит к увеличению количества ошибок II рода, уменьшение – к увеличению количества ошибок I рода. Результаты работы модифицированного метода выявления клонированных областей для фотомонтажей, представленных на рис. 1(а), 2(а), отражены на рис. 3, что наглядно демонстрирует повышение эффективности базового метода (сравн. с рис. 1(б), 2(б)).



а **б**

Рис. 3. Выявление фальсификации: а – МК фальсифицированного ЦИ, представленного на рис. 1(а); б – МК фальсифицированного ЦИ, представленного на рис. 2(а)

Для анализа эффективности модифицированного метода выявления клонирования (ММВК) был проведен вычислительный эксперимент с использованием ЦИ в форматах с потерями и без потерь: 600 ЦИ, полученных без привлечения профессиональных фотографов фотокамерами различного качества (множество V_1), 200 ЦИ из базы NRCS [13]**,** являющейся традиционной при тестировании различных алгоритмов, работающих с ЦИ. В ходе эксперимента симметрично отраженные клонированные ЗО имели различные конфигурации и размеры, в том числе и равные одному блоку 8×8 пикселей. Симметричное отражение клонированных ЗО проводилось по горизонтали, по вертикали. Также ММВК был протестирован для случаев, где ЗО была подвергнута повороту на угол, кратный 90° в направлении как по часовой, так и против часовой стрелки. Результаты вычислительного эксперимента с изображениями, размер ЗО в которых не привязывался к размеру ЦИ и не зависел от размера блоков стандартного разбиения его матрицы, а также в случае размера ЗО, равного размеру блока 8×8 пикселей, приведены в таблице 2.

Таблица 2.

Анализ эффективности ММВК

		Отражение/Угол поворота (град.)	V_1				V_2			
			TIFF	JPEG	JPEG 2000 БП	JPEG 2000 СП	TIFF	JPEG	JPEG 2000 БП	JPEG 2000 СП
Ошибки, %	I рода	Горизонтальное	0.3	0.3	0.3	0.3	0.6	0.3	0.3	0.3
		Вертикальное	0.3	0.3	0.6	0.3	0.3	0.3	0.3	0.3
		90°	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3
		180°	0.3	0.3	0.3	0.3	0.3	0.3	0.3	0.3
		270°	0.3	0.3	0.3	0.3	0.3	0.3	0,3	0.3
	II рода		9.9				8.5			

Таким образом, проведенный эксперимент подтвердил высокую эффективность ММВК в выявлении объекта клонирования даже в том случае, когда ЗО сравнима с размерами одного блока 8×8 стандартного разбиения матрицы ЦИ.

ММВК инвариантен к формату хранения ЦИ, используемых при проведении фотомонтажа, и успешно адаптирован для выявления симметрично отраженных

клонированных ЗО, а также клонированных ЗО, подвергнутых повороту на угол, кратный 90°.

Вычислительная сложность ММВК определяется полиномом четвертой степени, что является приемлемым с точки зрения его практического применения.

Замечание. При использовании для несанкционированного изменения ЦИ инструмента графических редакторов Штамп (Клон) часто в качестве постобработки используется коррекция цвета для клонированной области. Такая операция приведет к изменению СНЧ блоков, содержащихся в ЗО. Однако это изменение будет носить строго определенный характер, позволяющий адаптировать ММВК для выявления клонирования в этом случае. Результаты исследования данного способа фальсификации изображения в настоящий момент готовятся авторами к печати.

Выводы

Предложенная в данной работе модификация метода выявления клонирования, основанного на общем подходе к анализу состояния и технологии функционирования информационной системы, дала возможность эффективно использовать его для выявления фальсификации цифрового изображения, осуществленной путем отражения клонированных замещающих областей по вертикали и/или горизонтали, а также поворота их в любом направлении на угол, кратный 90°.

Эффективность модифицированного метода выявления клонирования не зависит от формата хранения цифрового изображения, использованного для фальсификации: количество ошибок I рода составило 0.3–0.6%, II рода – 8,5–9.9%.

Разработанный метод может быть использован для выявления клонированных областей в цифровом видео. В этом случае анализу подвергаются матрицы ключевых кадров видеопоследовательности.

Список литературы

1. Dybala, B. Detecting Filtered Cloning in Digital Images / B. Dybala, B. Jennings, D. Letscher // MM&Sec'07 Proceedings of the 9th workshop on Multimedia & Security, September 20–21, Dallas, Texas, USA. — 2007. — PP. 43–50.
2. Pan, X. Region Duplication Detection Using Image Feature Matching / X. Pan, S. Lyu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol. 5, No. 4. — PP.857–867.
3. Wang, J. Detection of image region duplication forgery using model with circle block / J. Wang, *et al*. // MINES'09 Proceedings of the 2009 International Conference on Multimedia Information Networking and Security, November 18–20. – 2009. – Vol. 1. — PP. 25–29.
4. Баранов, П.Е. Использование треугольных блоков для определения области фальсификации в изображениях / П.Е. Баранов, Е.Ю. Лебедева // Інформаційна безпека. — 2011. — № 2(6). — С. 139–144.
5. Myna, A.N. Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping / A.N. Myna, M.G. Venkateshmurthy, C.G. Patil // ICCIMA'07 Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007). — Vol. 3. — PP. 371–377.
6. Bay, H. SURF: Speeded Up Robust Features / H. Bay, *et al.* // Computer Vision and Image Understanding. — 2008. — Vol. 110, No. 3. — PP. 346–359.
7. Lowe, D.G. Distinctive Image Features from Scale-Invariant Keypoints / D.G. Lowe // International Journal of Computer Vision. — 2004. — Vol. 60, Iss. 2. — PP. 91–110.
8. Нариманова, Е.В. Условия проявления DQ-эффекта / Е.В. Нариманова // Інформаційна безпека. — 2010. — № 1(3). — С. 15–22.
9. Зорило, В.В. Выявление клонирования как фальсификации цифрового изображения / В.В. Зорило // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Тематичний випуск «Системний аналіз, управління та інформаційні технології». — Х.: НТУ «ХПІ», 2011. — № 35 — С. 31–38.

10. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
11. Кобозева, А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А. Кобозева // Искусственный интеллект. — 2007. — №4. — С. 531–538.
12. Бахвалов, Н.С. Численные методы [Текст] : учебное пособие для студентов физико-математических специальностей вузов / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — 8-е изд. — М. : Физматлит ; Л. : Невский диалект, 2000. — 622 с.
13. NRCS Photo Gallery: *[Электронный ресурс]* // United States Department of Agriculture. Washington, USA. Режим доступу: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).

МЕТОД ВИЯВЛЕННЯ СИМЕТРИЧНОГО КЛОНУВАННЯ ПРИ ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО ЗОБРАЖЕННЯ

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

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

Пропонується теоретично обґрунтована модифікація методу, який був розроблений авторами раніше, виявлення результатів одного з найбільш часто використовуваних при фальсифікаціях цифрових зображень інструментів, реалізованих в більшості графічних редакторів – клонування. Базовий метод заснований на аналізі сингулярних чисел блоків матриці зображення. Запропонована модифікація дозволяє ефективно виявляти заміщаючі області, симетрично відображені по вертикалі/горизонталі та/або піддані повороту на кут, кратний 90°, що підтверджується наведеними результатами обчислювальних експериментів. Розроблений метод може бути ефективно використаний для виявлення фальсифікації цифрового відео.

Ключові слова: фальсифікація цифрових зображень, клонування, симетричне клонування, фотомонтаж, матриця, сингулярне число

METHOD OF SYMMETRIC CLONING DETECTION IN THE FALSIFIED DIGITAL IMAGES

Alla A. Kobozeva, Victoria V. Zorilo, Olena Yu. Lebedyeva

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

This paper focuses on the modification of cloning detection method based on the analysis of singular values of digital image matrices' blocks. This modification gives an opportunity to detect symmetric cloning and/or digital image copy-past areas, replaced areas rotated on 90 degree. Proposed method can be effectively used for detecting of digital video falsification.

Keywords: image falsification, cloning, symmetric cloning, image forgery, matrix, singular value

УДК 621.391.7

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 13-21

МОЖЛИВІСТЬ ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю.Є. Яремчук

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

Запропоновано метод цифрового підписування, що базується на математичному апараті рекурентних V_k -послідовностей. Аналіз показав, що в цілому метод має приблизно такий же рівень криптографічної стійкості та обчислювальної складності, що і відомі аналоги, але за певних умов метод забезпечує значне підвищення швидкості виконання процедури перевірки підпису, а також підвищення стійкості всього процесу цифрового підписування.

Ключові слова: захист інформації, криптографія, автентифікація, цифрове підписування, рекурентні послідовності

Вступ

На сьогодні для вирішення задачі забезпечення цілісності інформаційних контентів використовують два типи криптографічних протоколів – автентифікації та цифрового підписування [1–4]. На відміну від протоколів автентифікації, які, в основному, спрямовані на забезпечення автентифікації учасників взаємодії, протоколи цифрового підписування забезпечують автентифікацію повідомлень. При цьому цифровий підпис повинен гарантувати, по-перше, що повідомлення надсилаються від достовірного відправника, по-друге, що повідомлення надходять в неспотвореному вигляді, і, по-третє, повинен забезпечувати гарантію одержувачу того, що відправник в подальшому не зможе відмовитись від свого підпису.

В загальному вигляді в схемі цифрового підписування [4] існує два учасника – відправник-підписант та одержувач-перевіряльник. Відправник (або центр довіри) генерує два ключа – загальнодоступний відкритий ключ K_1 та відповідний йому секретний ключ K_2. При формуванні підпису для повідомлення M відправник обчислює цифровий підпис DS від M, використовуючи ключ K_2. При перевірці підпису одержувач перевіряє підпис DS від повідомлення M, використовуючи ключ K_1.

Серед існуючих схем цифрового підписування найбільшого поширення отримали рандомізовані схеми з додаванням повідомлення. До таких схем в першу чергу відносяться методи Ель-Гамаля, Шнорра, DSA, ГОСТ 34.10 [1–3]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації.

Крім того, існують задачі, в яких процедуру перевірки підпису необхідно здійснювати в реальному часі від великої кількості власників і тому необхідність виконання складних обчислень в існуючих методах цифрового підписування створює перевіряльнику в таких випадках певні незручності. До такого роду задач відносяться задачі авторизації та ідентифікації під час здійснення трансакцій в електронних платіжних системах та в системах стільникового зв’язку, забезпечення веб-трансакцій

між клієнтом та сервером, організації банківських трансакцій, організації мобільної комерції, авторизації електронних повідомлень та інші. В таких задачах перевіряльник за одиницю часу може отримувати велику кількість запитів на перевірку підпису, що, в свою чергу, може створювати для нього проблему перенавантаження.

В цьому зв'язку певний інтерес викликає апарат на основі рекурентних послідовностей [5, 6], який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач. Так в роботі [7] представлено метод автентифікації сторін взаємодії, який базується на рекурентних V_k-послідовностях і забезпечує спрощення обчислень з боку перевіряльника.

Виходячи з цього, актуальною є розробка методу цифрового підписування на основі рекурентних послідовностей, який би забезпечував спрощення обчислень процедури перевірки підпису при забезпеченні достатнього рівня криптостійкості.

Мета статті і постановка задач дослідження

Метою роботи є дослідження можливості цифрового підписування на основі рекурентних V_k-послідовностей із забезпеченням спрощення обчислень під час перевірки підпису та достатнього рівня криптографічної стійкості.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1) Розглянути математичний апарат рекурентних V_k-послідовностей з можливістю побудови швидкісного методу цифрового підписування;

2) Провести порівняльний аналіз запропонованого методу з відомими аналогами щодо криптостійкості та обчислювальної складності.

Метод цифрового підписування на основі рекурентних V_k-послідовностей

В [5] розглянуто V_k-послідовність, яка складається з V_k^+-послідовності та V_k^--послідовності.

V_k^+-послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \tag{1}$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k — цілі числа; n і k — цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k v_{n+k-1,k}}{g_1}. \tag{2}$$

V_k^--послідовністю називається послідовність чисел, що обчислюються за формулою (5) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \ldots = v_{-k,k} = 0$ для $k > 2$.

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [6]

$$v_{n+m,k} = v_{m+(k-2),k} v_{n,k} + g_1 \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} v_{n-k+i,k} \,. \quad (3)$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [5]

$$v_{n-m,k} = v_{-m+(k-2),k} v_{n,k} + g_1 \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} v_{n-k+i,k} \,. \quad (4)$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють розробити методи цифрового підписування на їх основі.

Суть методу цифрового підписування, що пропонується (заявка на корисну модель № u 2013 06323 від 22.05.2013 р.), базується на використанні властивості (3) V_k-послідовності, яка дозволяє використовувати її для обчислення елементу $v_{n+m,k}$, а також для обчислення елементу $v_{-n+m,k}$. Крім того властивість (3) дозволяє реалізувати процедуру обчислення елементу $v_{n \cdot m,k}$. Так само на основі властивості (4) можна реалізувати процедуру обчислення елементу $v_{-n \cdot m,k}$. Все це дає можливість створення такого методу цифрового підписування.

Спочатку відправник-підписант (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. При цьому він випадковим чином вибирає секретний ключ a, за допомогою якого обчислює, а потім передає одержувачу-перевіряльнику відкритий ключ $v_{-a+i,k}$, $i = \overline{-k,-1}$.

При формуванні цифрового підпису для повідомлення M відправник-підписант вибирає випадкове число b, обчислює $v_{b,k}$, визначає значення x як $x = v_{b,k}$ та обчислює хеш-значення r як $r = h(x, M)$ за допомогою обраної функції хешування h від повідомлення M та значення x. Далі він визначає значення s як $s = b + ar$. Після цього отриману множину цілих чисел $\{r; s\}$ він перетворює у цифровий підпис вигляду $DS = (0 \,\|\, r \,\|\, 0 \,\|\, s)$ і передає його разом з повідомленням M одержувачу.

При перевірці цифрового підпису одержувач спочатку обчислює $v_{-a \cdot r+i,k}$, $i = \overline{-(k-1),0}$, на основі відкритого ключа – елементів $v_{-a+i,k}$, $i = \overline{-k,k-2}$, та отриманого від підписанта значення r, а потім на основі отриманого від підписанта значення s він обчислює елементи $v_{s+i,k}$, $i = \overline{-1,k-2}$.

Після цього на основі усіх обчислених підписантом елементів він обчислює значення x' як $x' = v_{-a \cdot r+s,k}$, використовуючи залежність (3), а потім обчислює хеш-значення r' як $r' = h(x', M)$ та перевіряє, чи виконується $r \stackrel{?}{=} r'$. Якщо так, то підпис приймається, в іншому випадку – відкидається.

Не важко пересвідчитись, що для підпису, згенерованого згідно цього методу, перевірка $r \stackrel{?}{=} r'$ завжди буде виконуватись.

Виходячи з цього схема цифрового підписування за даним методом буде мати такий вигляд (рис. 1).

Операція за модулем в схемі цифрового підписування використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Обчислення елементу $v_{b,k} \bmod p$ відправник може виконати попередньо, заздалегідь до безпосереднього формування цифрового підпису з повідомлення M.

В запропонованому методі цифрового підписування основні обчислення виконуються згідно залежності (3). Обчислення елементу $v_{n+m,k}$ згідно цієї залежності здійснюється на основі елементів $v_{n+i,k}$, $i=\overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i=\overline{-1,k-2}$.

В разі необхідності отримання певного послідовного набору елементів V_k-послідовності у кількості більшої ніж k, достатньо отримати будь-які послідовні k з них, оскільки інші можуть бути обчислені згідно формул (1) або (2) на основі вже отриманих.

Також в методі одержувачу слід виконувати обчислення елементів $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$, які можна здійснювати згідно представленого в роботі [7] методу обчислення елементів $v_{-m\cdot n,k}$.

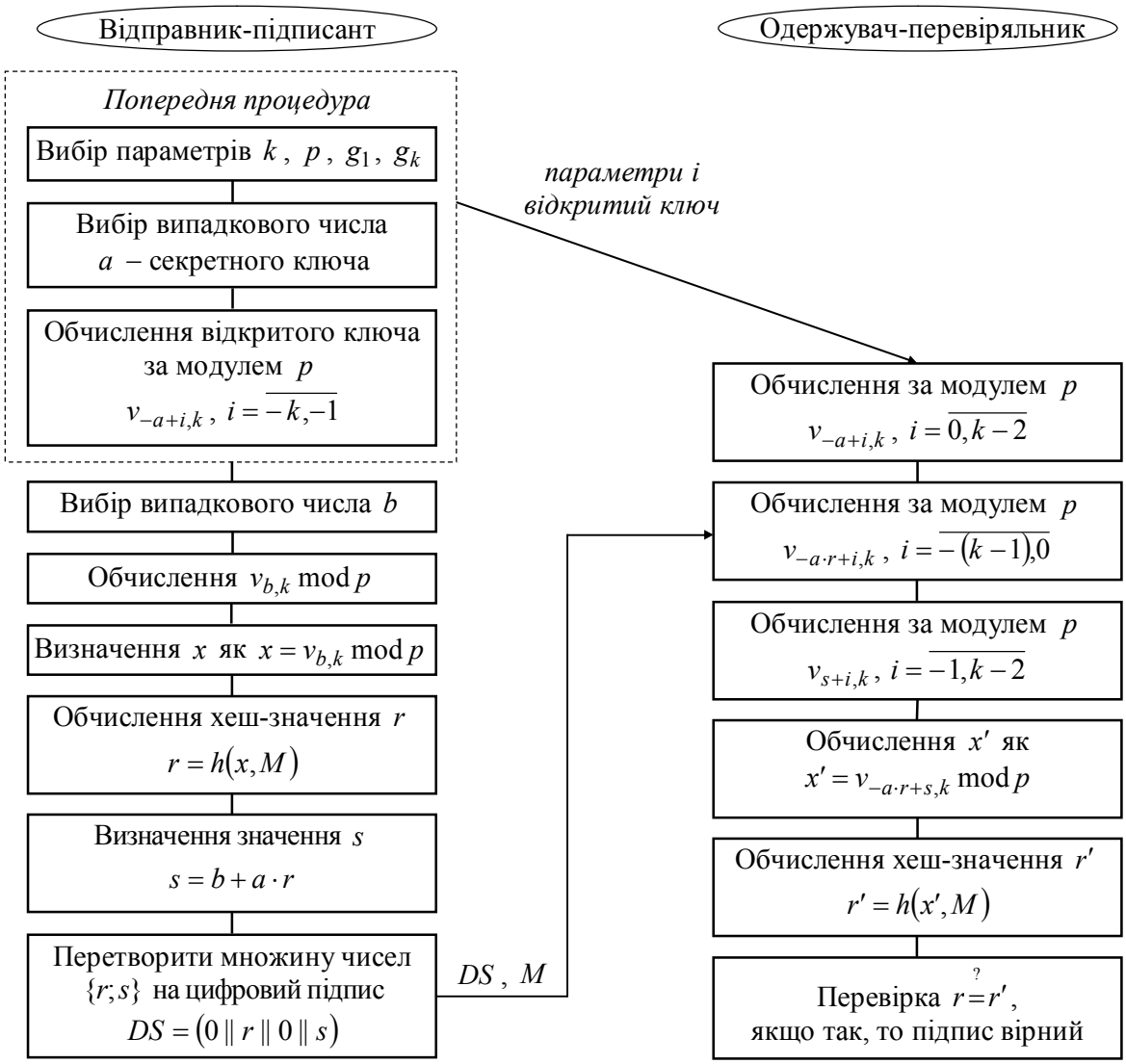


Рис. 1. Схема цифрового підписування на основі елементів V_k-послідовності.

Визначивши як можуть отримуватись елементи V_k -послідовності, що використовуються в методі цифрового підписування, отримаємо такий протокол цифрового підписування.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати g_1, g_k.

П.4. Відправнику передати параметри Одержувачу.

П.5. Відправнику вибрати випадкове число a — секретний ключ.

П.6. Відправнику обчислити відкритий ключ за модулем p $v_{-a+i,k}$, $i=\overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П.7. Відправнику передати відкритий ключ $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, Одержувачу.

П.8. Одержувачу обчислити за модулем p $v_{-a+i,k}$, $i=\overline{0,k-2}$, за формулою (1).

П.9. Відправнику вибрати випадкове число b.

П.10. Відправнику обчислити $v_{b,k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.11. Відправнику визначити x як $x = v_{b,k} \bmod p$.

П.12. Відправнику обчислити хеш-значення r як $r = h(x, M)$ за допомогою обраної функції хешування h від повідомлення M та значення x.

П.13. Відправнику визначити значення s як $s = b + ar$.

П.14. Відправнику перетворити множину цілих чисел $\{r; s\}$ у цифровий підпис вигляду $DS = (0 \| r \| 0 \| s)$ і передати його разом з повідомленням M Одержувачу.

П.15. Одержувачу обчислити за модулем p $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$, використовуючи алгоритм прискореного обчислення елементів $v_{-m\cdot n,k}$.

П.16. Одержувачу обчислити за модулем p елементи $v_{s+i,k}$, $i=\overline{-1,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.17. Одержувачу обчислити $x' = v_{-a\cdot r+s,k} \bmod p$ згідно залежності (3).

П.18. Одержувачу обчислити хеш-значення r' як $r' = h(x', M)$.

П.19. Одержувачу перевірити, чи виконується $r \overset{?}{=} r'$, якщо так, то підпис вважати вірним.

У п.2 проводиться вибір параметру p, який є модулем при обчисленнях в представленому протоколі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

У п.3 відбувається вибір параметрів g_1, g_k. Оскільки значення будь-якого числа в розробленому протоколі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

У п.10 протоколу цифрового підписування відправнику необхідно здійснювати обчислення $v_{b,k} \bmod p$, а у п.16 одержувачу необхідно здійснювати обчислення за модулем p елементів $v_{s+i,k}$, $i=\overline{-1,k-2}$. Ці обчислення можна здійснювати за одним з

алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які представлено в роботі [5].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, що виконуються у п.6 протоколу цифрового підписування, на основі одного з запропонованих у тій же роботі [5] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п.15 Одержувачу необхідно обчислювати за модулем p елементи $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$. Для цього можна використати алгоритм прискореного обчислення елементів $v_{-m\cdot n,k}$, який представлено в роботі [7].

Не важко помітити, що у випадку, якби $k=1$, запропонований метод цифрового підписування став би дуже подібним на метод Шнорра.

Згідно відомого протоколу цифрового підписування Шнорра [1] центр довіри або відправник вибирає і відкрито публікує два простих числа p і q: $q \mid p-1$ та число $g \neq 1$: $g^q \equiv 1 (\mathrm{mod}\, p)$. Потім він вибирає випадкове число $a<q$ як секретний ключ та обчислює $y=g^{-a} \bmod p$ – відкритий ключ, який передається одержувачу. Після цього протокол цифрового підписування реалізується таким чином.

На етапі формування підпису відправник вибирає випадкове число $b<q$ та обчислює $x=g^b \bmod p$ (ці обчислення можуть бути виконані і попередньо). Далі, з отриманого значення x та повідомлення M, що підписується, він здійснює хешування за допомогою функції h, обчислюючи значення $r=h(x,M)$. Потім відправник обчислює $s=(b+ar) \bmod q$ і надсилає повідомлення M з підписом (r,s) одержувачу.

На етапі перевірки підпису одержувач обчислює $x'=g^s y^r \bmod p$ і перевіряє, чи виконується рівняння $r \stackrel{?}{=} h(x',M)$. Якщо так, то підпис приймається, інакше – відкидається.

Проведемо аналіз запропонованого методу цифрового підписування на основі елементів V_k-послідовності та порівняємо його з відомим методом цифрового підписування Шнорра.

Здійснювати криптоаналіз запропонованого методу цифрового підписування на основі V_k-послідовності зловмисник може на основі відомих параметрів k, p, g_1, g_k, відкритого ключа $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, чисел r, s цифрового підпису та повідомлення M, які передаються від відправника до одержувача. Відповідно згідно методу Шнорра зловмиснику відомі параметри p, q, g, відкритий ключ $g^{-a} \bmod p$, а також повідомлення M з підписом (r,s), які передаються одержувачу відправником.

З [6] видно, що складність отримання зловмисником індексу елемента рекурентної V_k-послідовності, обчисленого за модулем, є принаймні не меншою, ніж отримання числа степеня з результату модулярного піднесення до степеня. Враховуючи це, можна стверджувати, що криптографічна стійкість запропонованого методу знаходиться приблизно на тому ж рівні, принаймні є не меншою, ніж й відомого аналогу.

Перевагою запропонованого методу цифрового підписування на основі рекурентних послідовностей перед відомими методами щодо стійкості є також можливість змінювати параметр k, що, в свою чергу, дає можливість підвищувати криптостійкість за рахунок збільшення складності виконання протоколу цифрового підписування. Окрім того, до переваг запропонованого методу цифрового підписування

слід віднести й те, що він має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Проведемо тепер аналіз запропонованого методу цифрового підписування щодо обчислювальної складності.

Аналіз запропонованого та відомого методів цифрового підписування показує, що згідно запропонованого методу необхідно чотири рази проводити обчислення елементів V_k-послідовності за прискореним алгоритмом, а саме обчислення за модулем p різних наборів елементів з $v_{-a,k}$, $v_{b,k}$, $v_{-a\cdot r,k}$ та $v_{s,k}$. Стільки ж, чотири, необхідно виконувати піднесень до степеня за модулем p згідно відомого методу Шнорра: g^{-a}, g^b, g^s та y^r.

В роботі [5] проведено дослідження складності виконання алгоритмів прискореного обчислення елементів V_k-послідовності, з якого видно, що складність обчислення елементу цієї послідовності із заданим індексом має приблизно такий же рівень як і піднесення до заданого степеня того ж порядку, що й індекс. Виходячи з цього, запропонований метод цифрового підписування на основі V_k-послідовності в цілому має приблизно такий же рівень обчислювальної складності, що і відомий метод Шнорра.

Однак, важливою перевагою запропонованого методу на основі V_k-послідовностей є те, що за необхідністю процедуру перевірки підпису можна значно спростити, якщо обчислення елементів $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, здійснювати не одержувачу, а відправнику, і передавати потім ці елементи перевіряльнику замість індексу s (заявка на корисну модель № u 2013 06322 від 22.05.2013 р.). Тоді відправнику необхідно буде передавати більшу кількість чисел і виконувати три обчислення елементів V_k-послідовності за прискореним алгоритмом замість двох. Однак такий варіант методу буде мати дві суттєвих переваги, по-перше, підвищиться стійкість методу, оскільки тепер зловмиснику замість індексу s буде відомий набір елементів $v_{s,k} \bmod p$ обчислених за цим індексом, і, по-друге, значно спроститься процедура перевірки підпису, оскільки в такому випадку одержувачу необхідно буде виконувати лише одне обчислення елементів V_k-послідовності за прискореним алгоритмом.

Висновки

На основі математичного апарату рекурентних V_k-послідовностей запропоновано метод цифрового підписування, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. Представлено протокол реалізації методу, а також проведено аналіз його криптографічної стійкості та обчислювальної складності у порівнянні з відомим аналогом.

Аналіз показав, що в цілому криптографічна стійкість і обчислювальна складність запропонованого методу знаходяться приблизно на тому ж рівні, що і відомого аналогу, але при цьому запропонований метод за певних умов дозволяє значно спрощувати обчислення процедури перевірки підпису, а також підвищувати стійкість всього процесу цифрового підписування.

Крім того запропонований метод дозволяє змінювати стійкість методу залежно від параметру k-го порядку послідовності, а також має простішу процедуру завдання параметрів у порівнянні з відомими аналогами.

Список літератури

1. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. — 5th ed. — N.Y.: CRC Press, 1996. — 816 p.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] = Applied cryptography. Protocols, algorithms and source code in C : [Пер. с англ.] / Б. Шнайер. — М. : ТРИУМФ, 2003. — 815 с.
3. Молдавян, Н.А. Теоретический минимум и алгоритмы цифровой подписи : учеб. пособие по направлению «Прикладные математика и физика» / Н.А. Молдовян. — СПб. : БХВ-Петербург, 2010. — 289 с.
4. Введение в криптографию: новые математические дисциплины [Текст] : учеб. для вузов / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др.: Под ред. В.В. Ященко. — СПб. : Питер ; М. : МЦНМО, 2001. — 287 с.
5. Яремчук, Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань [Текст] / Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. — 2013. — Т. 15, № 1. — С. 14–22.
6. Яремчук, Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю.Є. Яремчук // Захист інформації. — 2012. — № 4. — С. 120–127.
7. Яремчук, Ю.Є. Методи автентифікації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2013. — Вип. 1(25). — С. 39–48.

ВОЗМОЖНОСТЬ ЦИФРОВОГО ПОДПИСАНИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.Е. Яремчук

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

Предложен метод цифрового подписания, который основывается на математическом аппарате рекуррентных V_k –последовательностей. Анализ показал, что в целом метод имеет приблизительно такой же уровень криптографической стойкости и вычислительной сложности, что и известные аналоги, но при определённых условиях метод обеспечивает значительное повышение скорости выполнения процедуры проверки подписи, а также повышение стойкости всего процесса цифрового подписания.

Ключевые слова: защита информации, криптография, аутентификация, цифровое подписание, рекуррентные последовательности

POSSIBILITY OF DIGITAL SIGNING BASED ON RECURRENT SEQUENCES

Yuri E. Yaremchuk

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

We suggested a method of digital signing based on mathematical apparatus of recurrent V_k sequences. The analysis shows that, overall, the method has approximately the same level of cryptographic reliability and computational complexity as the known analogues. However, under certain circumstances, the method provides for a significant speed increase of signature checking procedures, as well as increase of reliability of the whole digital signature process.

Keywords: informational security, cryptography, authentication, digital signature, recurrent sequences

УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 22-34

МЕТОД ИДЕНТИФИКАЦИИ И ЛОКАЛИЗАЦИИ МАСШТАБИРОВАНИЯ В ЦИФРОВОМ ИЗОБРАЖЕНИИ

Е.А. Трифонова

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

На основании общего подхода, который предоставляет возможность для решения задачи обнаружения несанкционированного вмешательства в цифровой сигнал, предлагается новый метод идентификации и локализации масштабирования в цифровом изображении.

Ключевые слова: цифровое изображение, несанкционированное вмешательство, интерполяция, сингулярные числа

Введение

С развитием цифровых и IT-технологий в целом, а также благодаря разработанному богатому инструментарию различных графических редакторов, добиться реалистичной графической фальсификации стало значительно проще, а значит существенно сложнее стала задача доказательства подлинности и идентификации несанкционированного вмешательства в цифровой сигнал, решение которой во многих областях, таких как судебная экспертиза, медицинская диагностика, военная разведка, электронный документооборот и др. имеет определяющее значение. В связи с этим активно разрабатываются методы детектирования фальсификации цифровых сигналов, основной упор в которых направлен на обнаружение и локализацию основных геометрических преобразований цифрового сигнала. Наибольшее внимание уделено кадрированию как наиболее простому и самому распространенному способу фальсификации.

Следующим по распространенности использования среди преднамеренных геометрических модификаций цифровых сигналов считается масштабирование. Методы детектирования данного типа несанкционированного вмешательства, которые находятся в открытом доступе, не лишены значительных недостатков. Метод, предложенный в [1], осуществляет детектирование исключительно масштабирования, которое было построено на основании линейной или кубической интерполяции, при этом примененное ко всему изображению целиком. В [2–4] проводится исследование нормализованной энергии цифрового сигнала для детектирования масштабирования аналогично предыдущему методу – на ограниченном наборе ядер интерполяции.

Таким образом, актуальной остается проблема не просто детектирования, а построения метода локализации и идентификации масштабирования среди других геометрических преобразований, представляющих собой несанкционированное вмешательство в цифровой сигнал.

Цель исследования и постановка задачи

В [5] на основе теории возмущений и матричного анализа был разработан общий подход, который предоставляет возможность для решения задачи обнаружения и идентификации несанкционированного вмешательства в цифровой сигнал.

В соответствии с данными основами определены математические параметры, несущие в себе информацию о состоянии, а их возмущения – информацию об изменении состояния цифрового сигнала. Различные способы возмущения (в частности, различные способы несанкционированного вмешательства) цифрового сигнала приводят к различным характерным возмущениям математических параметров, которые сигнализируют о соответствующем возмущающем воздействии.

Целью данной работы является проведение анализа математических параметров и их возмущений для установления свойств, характеризующих локацию и способ возмущающего воздействия (несанкционированного вмешательства) на цифровой сигнал.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) Установить свойства, определяющие информационную структуру математических параметров, позволяющие обнаружить несанкционированное вмешательство в цифровой сигнал;

2) Установить свойства, определяющие информационную структуру математических параметров, позволяющие идентифицировать несанкционированное вмешательство в цифровой сигнал.

Основная часть

Масштабирование цифрового сигнала можно рассматривать как несанкционированное вмешательство, являющееся возмущением, основанным на замещении части основного сигнала (ОС), сигналом (ЗО) с измененными размерами (рис. 1).

а **б**

Рис. 1. Цифровое изображение: а – основной сигнал; б – результирующий сигнал с ЗО

Изменение размера дискретизированного сигнала производится за счет изменения количества элементов, приходящихся на обрабатываемую зону сигнала, и размещение их во времени и в пространстве в соответствии с первоначальной частотой дискретизации. При этом происходит увеличение или уменьшение размеров этого сигнала в зависимости от того, увеличивается или уменьшается количество его элементов. Поэтому процесс изменения количества элементов, составляющих обрабатываемый сигнал, может быть рассмотрен как процедура вторичной дискретизации этого сигнала. Как известно, вторичная дискретизация – это преобразование первичного дискретного сигнала во вторичный дискретный сигнал с использованием промежуточного сглаживания интерполяцией.

Сущность проблемы интерполяции состоит в отыскании значений сигнала в некоторых промежуточных точках между известными его элементами с целью сохранения, а иногда и улучшения качества исходного сигнала при осуществлении преобразований. Поскольку изменение размеров дискретизированного сигнала осуществляется

на основании интерполяции, следовательно, необходимо провести исследование ее влияния на свойства математических параметров для решения задачи обнаружения и идентификации данного типа несанкционированного вмешательства.

Влияние интерполяции, используемой для изменения размера, на сингулярные числа блоков матрицы цифрового сигнала

Интерполянт чаще всего ищут в виде свертки дискретного сигнала с ядром интерполяции. Наиболее распространенными и реализованными для использования являются следующие ядра интерполяции:

- прямоугольное ядро;
- треугольное ядро;
- кубическое ядро;
- ядра Ланцоша.

После применения любого ядра интерполяции для изменения размеров исходного цифрового сигнала будем рассматривать, аналогично случаю сжатия, два возможных способа получения сигнала: частичное интерполирование, которое не предполагает округление и введения во множество допустимых значений элементов интерполянта, в отличие от полного интерполирования.

Построение интерполянта в условиях отсутствия информации о ядре интерполирования и коэффициенте масштабирования является необратимой процедурой для исходного цифрового сигнала и приводит к некоторым закономерным особенностям сингулярных чисел (СНЧ) блоков, полученных после предварительного стандартного разбиения матриц цифрового сигнала.

Для иллюстрации этих особенностей в среде *MathWorks* MATLAB был проведен вычислительный эксперимент, в котором обработке подвергались различные цифровые сигналы, для которых были применены различные алгоритмы интерполяции.

Согласно ранее проведенному эксперименту [5], лишь малая часть общего числа блоков (ОЧБ) матриц, соответствующих цифровым изображениям и цифровым аудио, хранимым без потерь, имеет нулевые СНЧ.

Пусть цифровой сигнал подвергся частичной интерполяции, то есть после применения некоторого алгоритма интерполирования с целью изменения размеров цифрового сигнала не проведены округления и введения во множество допустимых значений. Как показывает результат проведенного эксперимента, у полученных матриц цифровых сигналов все блоки содержат нулевые СНЧ. Такая ситуация закономерна, поскольку в результате применения любого алгоритма интерполирования элементы интерполянта представляют собой линейные комбинации исходных значений матрицы для сохранения того же самого значения ранга матрицы при увеличении ее размера.

Таким образом, проведенный вычислительный эксперимент для анализа СНЧ блоков цифровых сигналов показал, что количество нулевых СНЧ блоков является свойством, которое предоставляет возможность различать, а именно локализовать, блоки цифрового сигнала исходного и подвергшегося интерполяции.

Восстановление влияния частичной интерполяции на сингулярные числа блоков матрицы цифрового сигнала

Пусть исходный цифровой сигнал подвергся частичной интерполяции, но в результате сохранения значения его отсчетов неизбежно, для соответствия определённому формату, будут округлены и введены в определенный диапазон, то есть будет осуществлена полная интерполяция.

Несмотря на то, что операция округления, применимая к значениям цифрового сигнала, представляет собой незначительное возмущение матрицы, и СНЧ являются нечувствительными к возмущающим воздействиям, но значения СНЧ станут все же ненулевыми. Поэтому для отличия исходного от цифрового сигнала, полученного в результате интерполяции, имеет смысл анализировать матрицу, соответствующую частично интерполированной.

Пусть для некоторого блока матрицы A размером 8×8, например, цифрового изображения, проведена процедура частичной интерполяции с некоторым интерполяционным ядром для масштабирования в k раз. Получена матрица I размером $8k \times 8k$. Тогда матрица после полной интерполяции II такая что

$$I = II + \Delta, \tag{1}$$

где Δ — действительная матрица $8k \times 8k$, значения которой из $[-0.5; 0.5)$, т.е.

$$\max|II - I| \le 0.5. \tag{2}$$

Рассмотрим сингулярное разложение I

$$I = U\Sigma V^T = \sum_{i=1}^{8k} \sigma_i u_i v_i^T, \tag{3}$$

где

U и V — ортогональные матрицы левых и правых сингулярных векторов соответственно,

Σ — диагональная матрица СНЧ [6].

Поскольку матрица получена в результате частичного интерполирования, то содержит нулевые СНЧ. Тогда вектора левого и правого сингулярных базисов, соответствующие нулевым СНЧ, не вносят своего вклада при построении матрицы I:

$$I = \sum_{i=1}^{8k-r} \sigma_i u_i v_i^T, \tag{4}$$

где r – количество нулевых СНЧ.

Сингулярное разложение матрицы II, полученной после полного интерполирования, не содержит нулевых СНЧ, все вектора правого и левого сингулярных базисов вносят свой вклад в формирование матрицы II

$$II = \overline{U}\,\overline{\Sigma}\,\overline{V}^T = \sum_{i=1}^{8k} \overline{\sigma}_i \overline{u}_i \overline{v}_i^T. \tag{5}$$

Тогда неравенство (2),учитывая (4) и (5) можно представить

$$\max\left|\sum_{i=1}^{8k} \overline{\sigma}_i \overline{u}_i \overline{v}_i^T - \sum_{i=1}^{8k-r} \sigma_i u_i v_i^T\right| \le 0.5. \tag{6}$$

Для выяснения влияния округления на изменение сингулярного спектра и изменения левого (правого) сингулярного базиса в среде *MathWorks* MATLAB был проведен вычислительный эксперимент. Рассмотрению подвергались левые (правые) сингулярные базисы матриц I и II, полученные в результате частичной и полной

интерполяции U и $\overline{U}$. Для определения изменения вычислен косинус угла между советующими векторами U и $\overline{U}$.

Согласно результатам эксперимента, изменение после округления претерпевают сингулярные вектора, соответствующие нулевым СНЧ. Остальные вектора остаются без изменений, составляя

$$\cos\left(u_i, \bar{u}_i\right) = 1, \quad i = [1;8k],$$

лишь в редких случаях образуя

$$\cos\left(u_i, \bar{u}_i\right) = -1, \quad i = [1;8k].$$

Сингулярный спектр в результате округления больше не содержит нулевых значений. Следовательно, неравенство (6), можно представить в следующем виде:

$$\max\left| \sum_{i=8k-r+1}^{8k} \bar{\sigma}_i \bar{u}_i \bar{v}_i^T \right| \le 0.5. \qquad (7)$$

На основании полученного неравенства можно определить максимальное количество СНЧ, обнуление которых не приводит к изменению матрицы, полученной в результате полной интерполяции.

Основные шаги метода определения максимального количества нулевых сингулярных чисел:

1) Построение для блока размером $n \times n$ сингулярного разложения матрицы $II = \overline{U}\overline{\Sigma}\overline{V}^T$, $t = n$.

2) Предположение, что t-е СНЧ не является нулевым вследствие округления.

3) Обнуление t-го СНЧ, т.е. $\sigma_t = 0$.

4) Вычисление $\Delta = \max\left| \sum_{i=t}^{n} \bar{\sigma}_i \bar{u}_i \bar{v}_i^T \right|$.

5) Сравнение:

если $\Delta \le 0.5$,

то $t = t - 1$ и переход на шаг 2,

иначе t — максимальное количество нулевых СНЧ.

Рассмотрим матрицу A изображения размером 64×64 (рис. 2), которая не содержит нулевых СНЧ. В результате частичного интерполирования получим действительную матрицу I изображения размером 128×128. Она содержит 64 нулевых СНЧ. После применения полного интерполирования матрица II (изображение на рис. 3) не содержит ни одного нулевого СНЧ.

Рис. 2. Тестируемое цифровое изображение 64×64 пикселя

Для определения максимального количества нулевых СНЧ воспользуемся методом, предложенным выше. Результаты всех шагов представлены в таблице 1. На каждом шаге последовательно обнулялось σ_t значение сингулярного спектра и вычислялось Δ.

Таблица 1.

Результаты работы метода определения максимального количества нулевых СНЧ

t	Δ	t	Δ	t	Δ	t	Δ	t	Δ	t	Δ	t	Δ
1	0.0009	**21**	0.1112	**41**	0.2900	**61**	0.4642	**81**	2.9928	**101**	15.2839	**121**	67.8800
2	0.0034	**22**	0.1070	**42**	0.2907	**62**	0.4632	**82**	3.0628	**102**	15.6700	**122**	81.2210
3	0.0078	**23**	0.1095	**43**	0.2906	**63**	0.4644	**83**	3.1125	**103**	17.5803	**123**	86.0424
4	0.0079	**24**	0.1256	**44**	0.2942	**64**	0.4801	**84**	3.5059	**104**	21.6161	**124**	95.3361
5	0.0117	**25**	0.1350	**45**	0.3080	**65**	0.5049	**85**	4.3512	**105**	19.5070	**125**	101.383
6	0.0192	**26**	0.1335	**46**	0.3088	**66**	0.5067	**86**	4.2971	**106**	20.2455	**126**	101.047
7	0.0252	**27**	0.1337	**47**	0.3090	**67**	0.4998	**87**	4.3563	**107**	22.1476	**127**	115.119
8	0.0340	**28**	0.1388	**48**	0.3253	**68**	0.6279	**88**	6.2148	**108**	23.1458	**128**	164.000
9	0.0365	**29**	0.1742	**49**	0.3577	**69**	0.6718	**89**	6.2961	**109**	24.6010		
10	0.0367	**30**	0.1732	**50**	0.3580	**70**	0.7379	**90**	7.5489	**110**	25.8038		
11	0.0462	**31**	0.1702	**51**	0.3779	**71**	1.0105	**91**	8.4585	**111**	34.5827		
12	0.0601	**32**	0.1985	**52**	0.3741	**72**	1.2732	**92**	9.1461	**112**	34.6749		
13	0.0566	**33**	0.2156	**53**	0.3833	**73**	1.2855	**93**	11.2848	**113**	34.1513		
14	0.0608	**34**	0.2021	**54**	0.3974	**74**	1.5047	**94**	12.0659	**114**	39.0169		
15	0.0660	**35**	0.2145	**55**	0.3994	**75**	1.5215	**95**	12.1474	**115**	40.5433		
16	0.0685	**36**	0.2785	**56**	0.4033	**76**	1.8387	**96**	13.2470	**116**	47.3842		
17	0.0797	**37**	0.2788	**57**	0.4336	**77**	1.8932	**97**	13.2246	**117**	55.4794		
18	0.0828	**38**	0.2627	**58**	0.4396	**78**	1.9767	**98**	13.4397	**118**	58.8119		
19	0.0868	**39**	0.2846	**59**	0.4238	**79**	2.5708	**99**	13.9699	**119**	59.2001		
20	0.1051	**40**	0.3022	**60**	0.4680	**80**	2.8014	**100**	14.1332	**120**	59.2362		

При обнулении σ_{65} значение $\Delta > 0.5$, являющееся сигналом, что обнуление σ_{65} приводит к изменению исследуемой матрицы. Следовательно, максимальное количество нулевых СНЧ для данной матрицы 64, что совпадает с количеством нулевых СНЧ данной матрицы, полученной при частичной интерполяции.

Рис. 3. Изображение 128×128, полученное в результате полной интерполяции

Замечание. Необходимо подчеркнуть особенности, связанные с применением интерполяции, возникающие в частотной области.

Рассмотрим матрицу изображения (рис. 2), но для наглядности только ее часть. Построим соответствующие матрицы с помощью частичной билинейной интерполяции и полной интерполяции. Для каждой из них определим их частотное представление.

Для матрицы частичной интерполяции характерно возникновение нулевых строк и нулевых столбцов, образующих так называемую решетку, которая становится регулярной в случаях увеличения коэффициента масштабирования (табл. 2), и совершенно пропадает для матрицы полной интерполяции (табл. 3), не оставляя даже намека, по сравнению с матрицей нулевых СНЧ блоков (МНСЧБ), на применение несанкционированного вмешательства.

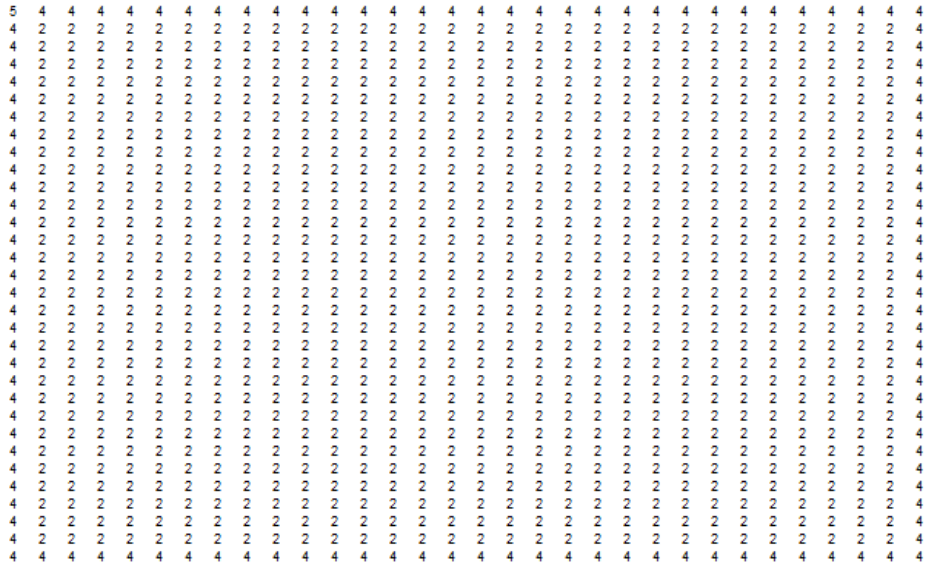
Исследование свойств СНЧ блоков, полученных при различных способах разбиения цифрового сигнала, подвергшегося интерполяции с целью изменения размеров

На основании проведенных выше исследований установлено, что количество нулевых СНЧ является свойством, которое локализует и сигнализирует о применении несанкционированного вмешательства.

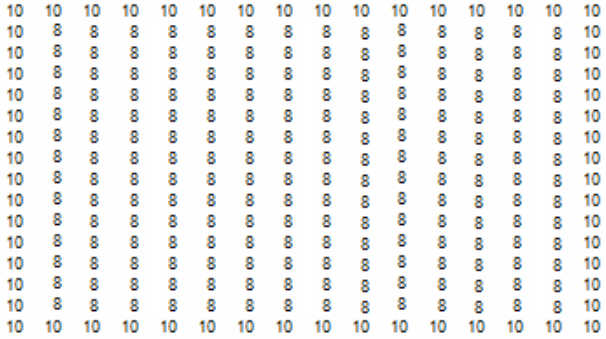
Для идентификации несанкционированного вмешательства, основанного на интерполяции с целью изменения размеров цифрового сигнала, необходимо установить отличительные свойства, определяющие информационную структуру математических параметров.

Рассмотрим блок матрицы A размером 64×64. После применения интерполяции, например, с ядром Ланцоша получена матрица размером 256×256 (рис. 4(а)). Для матрицы применена последовательно разбивка на блоки 8×8, 16×16, 32×32, и построены соответствующие МНСЧБ (рис. 4(б-г)), каждый элемент которой, определялся как максимальное количество нулевых СНЧ блока, на основании метода, полученного выше.

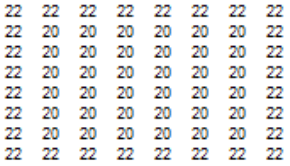
а



б



в



г

Рис. 4. Применение интерполяции с ядром Ланцоша: а – блок 256×256 изображения, полученный в результате интерполяции с ядром Ланцоша; б – МНСЧБ при разбиении на блоки 8×8; в – МНСЧБ при разбиении на блоки 16×16; г – МНСЧБ при разбиении на блоки 32×32

Таблица 2.

Частотное представление матрицы цифрового изображения, полученной в результате частичной интерполяции

0.0573984	-0.0018369	-0.3002841	0.1541174	0.1445389	-0.2144409	1.672219	-2.00E-14	-3.0253353	0.7188361	-0.9464867	-2.1685964	10.75758	0.2333964	-60.076537	472.75
0.0010706	-0.1200685	0.0052254	0.8229028	-0.1086945	-1.1688831	0.2826934	3.05E-15	-0.5114415	3.9182606	0.7117659	-11.579122	-0.1871969	15.256112	-1.1205079	-13.641808
-0.0014926	-0.0012384	0.1879083	-0.0518122	-0.5710025	0.0690461	1.7290214	-3.36E-15	-3.1281009	-0.2314524	3.7391058	0.7290536	-6.7317535	0.1573507	1.5622404	-0.413919
-0.0005678	-0.0042237	-0.0317706	-0.0856768	0.1617245	0.4440755	-1.3343298	4.40E-16	2.4140349	-1.4886037	-1.0590236	1.2055639	1.1381701	0.5366702	0.5942956	-1.71587
-0.0011673	-0.0001359	0.01149	-0.0994369	0.1339906	0.2574451	-0.5798022	1.40E-15	1.0489631	-0.8629923	-0.8774131	1.3991832	-0.4116238	0.0172707	1.221782	-0.1971451
0.0011902	0.0048234	0.0201541	-0.0718949	-0.1283018	0.1464145	0.0396038	1.42E-15	-0.0716501	-0.490802	0.8401607	1.0116381	-0.7220128	-0.6128691	-1.2457617	-1.2391708
0.0006027	-0.0003125	0.0236635	-0.013076	-0.0161261	0.0174253	0.0842611	-3.57E-16	-0.152443	-0.0584122	0.1055987	0.1839929	-0.8477365	0.039711	-0.6308598	-0.9843728
-0.0001902	0.0030685	-0.0097331	-0.0134033	0.0163571	0.1148763	-0.1044485	-2.53E-16	0.1889655	-0.3850814	-0.1071115	0.188599	0.3486855	-0.3898933	0.1990773	-0.1346894
6.67E-16	-2.34E-15	-1.69E-15	7.77E-16	2.92E-15	-2.73E-15	-1.33E-15	2.22E-15	-5.55E-16	3.00E-15	7.49E-16	-1.22E-15	3.03E-15	-5.11E-15	-4.00E-15	-7.11E-15
0.0001051	-0.0016961	0.0053799	0.0074085	-0.0090412	-0.0634965	0.0577327	7.81E-16	-0.1044485	0.2128493	0.0592046	-0.1042459	-0.1927318	0.215509	-0.1100377	0.074448
-0.0001798	9.32E-05	-0.0070592	0.0039008	0.0048107	-0.0051983	-0.0251365	-4.60E-16	0.0454763	0.0174253	-0.0315019	-0.0548882	0.2528941	-0.0118464	0.1881961	0.293655
-0.0001818	-0.0007366	-0.0030777	0.0109791	0.0195931	-0.0223591	-0.0060479	-7.28E-16	0.0109418	0.0749509	-0.1283018	-0.1544882	0.1102593	0.0935918	0.1902415	0.189235
8.30E-05	9.66E-06	-0.0008166	0.0070668	-0.0095224	-0.0182961	0.0412053	-9.96E-17	-0.0745475	0.061331	0.0623558	-0.0994369	0.0292532	-0.0012274	-0.0868294	0.0140107
1.58E-05	0.0001179	0.0008868	0.0023916	-0.0045143	-0.0123958	0.0372461	1.00E-15	-0.0673847	0.0415525	0.0295613	-0.0336518	-0.0317706	-0.0149805	-0.016589	0.0478963
1.17E-05	9.75E-06	-0.0014789	0.0004078	0.0044939	-0.0005434	-0.0136077	4.24E-16	0.0246188	0.0018216	-0.0294275	-0.0057378	0.0529802	-0.0012384	-0.0122951	0.0032576
-1.02E-06	0.0001147	-4.99E-06	-0.0007862	0.0001038	0.0011168	-0.0002701	6.98E-16	0.0004886	-0.0037436	-0.00068	0.0110629	0.0001789	-0.014576	0.0010706	0.0130337

Таблица 3.

Частотное представление матрицы цифрового изображения, полученной в результате полной интерполяции

0.6025719	0.6729244	-0.671272	0.0386325	1.0040881	0.0381725	1.6975908	0.4375	-3.40751	0.0185264	-0.718823	-2.216432	11.020629	-0.351422	-60.60318	473.6875
-0.233181	-0.055762	0.50445	0.6452143	0.3993378	-0.8412637	-0.6276938	0.4848859	-0.5141748	4.1514467	0.6259714	-12.510681	0.378684	15.501493	-1.378428	-13.73713
-0.2408	0.0011163	0.8431782	0.3144622	-0.3286613	-0.3735298	1.8155516	0.1774259	-3.1593948	-0.3909813	3.893537	0.54161	-6.945363	0.1306119	1.1933141	0.047292
-0.531184	-0.123297	0.1291306	-0.3653816	-0.1350312	0.8996655	-1.6551975	-0.0999273	2.4913774	-1.3788598	-0.9114939	1.2048759	1.0982676	0.6192826	0.9617878	-2.110194
-0.247604	0.3560922	-0.17094	-0.1584709	-0.0681466	0.2441448	0.0884707	-0.1971451	0.8559373	-1.0540189	-0.8909929	1.6780777	-0.54161	0.1158911	1.3521073	-0.197145
0.22232	0.0139676	-0.096511	-0.2225949	-0.1404607	-0.0185959	-0.0157446	-0.1204595	-0.0920755	-0.0162109	0.7539069	0.988077	-0.516591	-0.642712	-1.663585	-1.787157
0.3749095	0.084709	0.00968	0.0427323	-0.0232246	-0.1098731	0.4936457	0.0071426	-0.5160329	-0.0394366	0.1665789	0.2094686	-0.968871	-0.225004	-1.209394	-0.968903
0.1586997	0.0106678	-0.139418	-0.0841124	-0.08816	0.5152759	-0.0102481	0.0730244	-0.0368472	-0.7832067	0.060161	0.2637561	0.6813575	-0.882453	0.2712688	0.0295308
0.0947235	-0.080968	-0.141601	0.1294956	0.2165275	-0.124274	-0.2883073	0.0625	0.324122	0.0390048	-0.3009234	-0.1493097	0.2136236	0.2336744	-0.077306	-0.1875
-0.006937	0.0390631	0.0658861	-0.0091681	0.0251503	-0.381189	0.1351185	0.0351431	-0.165502	0.3567846	0.197395	0.2207633	-0.784308	0.2200741	-0.129187	0.3413374
-0.203936	-0.121451	0.0001792	0.0117023	0.0139302	-0.0760483	-0.4008396	0.0359082	0.4136189	-0.0732614	-0.0405295	-0.130843	0.4606781	0.3635143	0.9109275	0.4102956
-0.166105	-0.057053	0.1938568	0.0795813	-0.0561744	0.1155595	0.0034545	0.0448345	0.063764	-0.1331754	-0.1900049	-0.4841156	-0.113678	0.6470671	1.092487	0.5994663
-0.006171	-0.088429	0.2095927	-0.1780777	0.0586532	0.2298089	-0.4026556	0.0140107	0.1208644	0.1004015	0.1993844	-0.2834709	0.0408545	-0.157298	-0.413398	0.0140107
0.029885	0.0782993	0.0449902	-0.115665	0.2622017	0.0583888	-0.1997474	-0.0602782	0.138849	0.1354951	-0.2884042	-0.0553953	-0.243637	-0.142158	-0.241123	0.4456686
-0.1091614	0.0827765	0.2231567	-0.325179	-0.514774	0.4107954	0.2617017	-0.1185522	-0.0942768	-0.2300236	0.172168	0.3087404	0.4302423	-0.212272	0.1790756	0.0048782
-0.060834	-0.298209	0.1052355	0.3139758	-0.2019511	-0.1392752	0.1492218	-0.0971006	-0.034395	0.0396066	0.1603446	0.1918304	-0.348119	0.1369295	0.288342	-0.019337

Полученные МНСЧБ, не зависимо от алгоритма интерполяции, коэффициента масштабирования и способа построения разбиения на блоки, характеризуются одинаковой информационной структурой. Элементы МНСЧБ последней и первой строчки, последнего и первого столбца всегда принимают значения, большие по сравнению с остальными элементами, образуя пограничный контур.

Метод обнаружения возмущения цифрового сигнала, основанного на интерполяции, используемой для изменения размера цифрового сигнала

На основании полученных результатов построим практический метод обнаружения и идентификации несанкционированного вмешательства в цифровой сигнал возмущением, основанным на интерполяции, которая используется для изменения размера цифрового сигнала. Рассмотрим цифровые сигналы, полученные современными цифровыми фотокамерами, диктофонами и др. Среди них как сигналы с измененными размерами, полученными в результате интерполяции, так и не подвергшиеся масштабированию. Пусть часть ОС, заменяется ЗО с измененными размерами (для большей наглядности получаемых ниже выводов никакая последующая обработка сигнала не производится). Такое возмущение цифрового сигнала, основанное на интерполяции, пример которого на основе изображения (рис. 5(а)) демонстрирует несанкционированное вмешательство, представлено на (рис. 5(б)), сохраняется без потерь. Графическое представление МНСЧБ результирующего цифрового изображения наглядно демонстрирует подобласти несанкционированного вмешательства данного типа при разбиении на блоки 16×16 (рис. 5(в)) и при разбиении на 32×32 (рис. 5(г)).

Таким образом, основные шаги метода, обнаружения и идентификации несанкционированного вмешательства интерполяцией с целью изменения размеров, следующие:

1) Построение матрицы цифрового сигнала.

2) Разбиение полученной матрицы стандартным образом на блоки 8×8.

3) Построение для I МНСЧБ M, на основании метода определения максимального количества нулевых СНЧ.

4) Обнаружение: выделение в M прямоугольных областей, таких что:

- $O_1, O_2, ..., O_m$ — большинство элементов, которых имеют нулевое значение;
- $Z_1, Z_2, ..., Z_p$ — большинство элементов, которых имеют ненулевое значение.

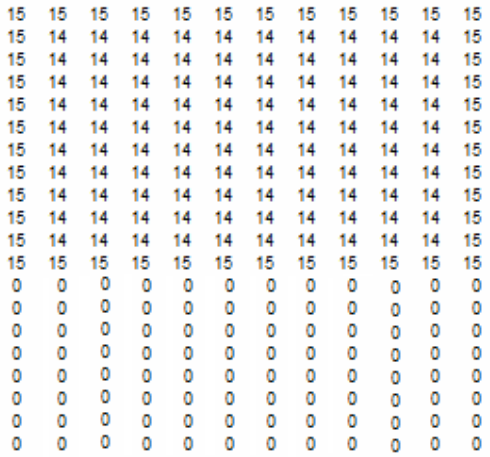
5) Идентификация:

- $O_1, O_2, ..., O_m$ — являются результатом «copy-paste» из цифрового сигнала;
- области из $Z_1, Z_2, ..., Z_p$, которые содержат пограничный контур, являются результатом несанкционированного вмешательства интерполяцией с целью изменения размеров.

а

б

в



г

Рис. 5. Фальсификация с применением интерполяции с ядром Ланцоша: а – исходное цифровое изображение; б – изображение, полученное в результате несанкционированного вмешательства интерполяцией; в – МНСЧБ при разбиении на блоки 16×16; г – МНСЧБ при разбиении на блоки 32×32

Выводы

В данной работе проведено исследование свойств математических параметров цифрового сигнала для установления информационной структуры, позволяющей локализовать и идентифицировать возмущение, основанное на интерполяции. Показано, что количество нулевых СНЧ блоков матрицы цифрового сигнала является свойством, на

основании которого осуществляется локализация, а наличие пограничного контура идентифицирует данный тип несанкционированного вмешательства. Результатом проделанной работы стало создание практического метода для обнаружения и идентификации несанкционированного вмешательства, основанного на интерполяции с целью изменения размеров цифрового сигнала.

Список литературы

1. Gallagher, A.C. Detection of Linear and Cubic Interpolation in JPEG Compressed Images / A.C. Gallagher // Proceedings of the 2nd Canadian conference on Computer and Robot Vision, May 9–11, 2005. — 2005. — PP. 65–72.
2. Feng, X. An energy-based method for the forensic detection of re-sampled images / X. Feng, G. Doërr, I.J. Cox // 2011 IEEE International Conference on Multimedia and Expo (ICME), July 11-15, Barcelona, Spain. — 2011. — PP. 1–6.
3. Uccheddu, F. Detection of Resampled Images: Performance Analysis and Practical Challenges / F. Uccheddu, *et al.* // Proceedings of the 18th European Signal Processing Conference (EUSIPCO-2010), August 23–27, 2010. — 2010. — PP. 1675–1679.
4. Yamasaki, T. Detecting Resized JPEG Images by Analyzing High Frequency Elements in DCT Coefficients / T. Yamasaki, T. Matsunami, K. Aizawa // 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, October 15–17, Darmstadt, Germany. — 2010. — PP. 567–570
5. 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. В. Даля. — 2008. — № 8(126), Ч. 1. — С. 62–72.
6. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.

МЕТОД ЛОКАЛІЗАЦІЇ ТА ІДЕНТИФІКАЦІЇ МАСШТАБУВАННЯ В ЦИФРОВОМУ ЗОБРАЖЕННІ

К.О. Трифонова

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

На підставі загального підходу, який надає можливість для вирішення задачі виявлення та ідентифікації несанкціонованого втручання в цифровий сигнал, пропонується новий метод локалізації і ідентифікації масштабування в цифровому зображенні.

Ключові слова: несанкціоноване втручання, інтерполяція, сингулярні числа

METHOD OF LOCATION AND IDENTIFICATION SCALING IN DIGITAL IMAGE

Ekaterina A. Trifonova

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

In this paper, based on a common approach, which provides an opportunity to address the problem of detection and identification of digital signal tampering, a new method for localization and identification of scale in a digital image is proposed.

Keywords: unauthorized alteration, interpolation, the singular values

Mathematics Subject Classification (2010) 74A10

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 35-42

THE STRESS STATE OF THE CONICAL LAYERED MEDIUM

Nataly D. Vaysfel'd

Odessa I.I. Mechnikov National University,
2 Dvoryanskaya str., Odessa, 65082, Ukraine; e-mail: vaysfeld@onu.edu.ua

An infinite conic layered cone which represents sequence of conical adjacent funnels, inserted one into another, is considered. Each of these funnels differs by their shear modulus. Conditions of an ideal contact are fulfilled between the adjacent conical surfaces. An external conical surface is loaded by tangent torsion stress. An exact solution of corresponding one-dimensional boundary problem is constructed in domain of Mellin's transformation, which is applied directly to the torsion equation. A formulating of boundary conditions in the matrix form allows to obtain recurrent type relations for unknown constants of a general solution for each layer. The proposed solving method leads to the exact solution which is independent of the layers' number. Mellin's transformation is inversed to finish the construction of the formulas for displacements and stress.

Keywords: conical layered medium, integral transformation, vector boundary problem

Introduction

An interest to the stress state of conical layered medium investigations is due to development of corresponded mathematical methods for such a problems' solving, and to a wide range of practical applications of the investigation's results in an engineering.

A lot of present day works are dedicated to a numerical approach to the solving the problems on a stress state of layered mediums ([1–3]), but numerical methods are not very effective in this case, because during layered mediums' modeling it is necessary to change a distance between the grid's points. That is why working up of an analytical solving methods is actual. Last time in the papers [4, 5] a new approach to the solving of inhomogeneous medium problems based on the further development of the factorization method was proposed for an investigation and application of block structures. For the analytical solution's construction the multilayered step model is used during the stress state analysis of the layered materials in three-dimensional case [6]. A new effective method of the axisymmetrical mixed problems' solving for stratified mediums is developed in [7]. An exponential model reducing the problem to the integral equation is worked out for functionally-gradient materials by [8, 9]. Dynamic problems for the inhomogeneous mediums are also actively investigated during past time [10–12].

The torsion of a conical body under static and dynamic loadings is investigated [13–16].

A new analytical method of a conical layered medium investigation was proposed by G. Popov in [17, 18]. An initial problem in terms of Lame's equations is reduced to the one-dimensional problem. The integral transformation with respect to space coordinates is applied directly to the equilibrium equations but not to their representations through the harmonic or other functions as they do it traditionally. In the transformations' domain the exact solution of the problem is constructed with a help of matrix differential calculus, and besides it is constructed independently of the layers' quantity. This approach is used for a solving of the torsion problem for a conical layered elastic cone.

The formulation of the initial boundary value problem

The torsion of the elastic circular infinite cone $0 < r < \infty, 0 < \theta < \omega_n, -\pi \le \varphi < \pi$ (r, θ, φ — the spherical system of coordinates) is considered. The cone's shear module G stepwise changes on the conical surfaces $\theta = \omega_j$, $j = \overline{1, n-1}$. The external surface $\theta = \omega_n$ is loaded by the tangent torsion stresses. Let's set the layer $\omega_{j-1} < \theta < \omega_j$ and input the designation for its shear modulus G_j and the displacement $u_\varphi^j(r,\theta) = w_j(r,\theta)$, $j = \overline{1, n-1}$. At the problem's formulation Lame's equations are reduced to one equation relative to the displacement $w_j(r,\theta)$ [19]

$$\left[r^2 w_j'(r,\theta)\right]' + \frac{\left[\sin\theta w_j^{\bullet}(r,\theta)\right]^{\bullet}}{\sin\theta} - \frac{w_j(r,\theta)}{\sin^2\theta} = 0, \quad 0 < r < \infty, \quad \omega_{j-1} < \theta < \omega_j, \quad j = \overline{1, n} \tag{1}$$

Here and further the stroke denotes the derivative with respect to the variable r and the dot – the derivative with respect to the variable θ. The nonzero stress are defined by the formulas [19]

$$r\tau_{r\varphi}^{(j)}(r,\theta) = G_j\left[rw_j'(r,\theta) - w_j(r,\theta)\right], \quad r\tau_{\theta\varphi}^{(j)}(r,\theta) = G_j\left[w_j^{\bullet}(r,\theta) - ctg\theta w_j(r,\theta)\right]. \tag{2}$$

The boundary condition is defined by the equality

$$\tau_{\theta\varphi}^{(n)}(r,\omega_n) = q(r) \quad \text{or} \quad G_n\left[w_n^{\bullet}(r,\omega_n) - ctg\omega_n w_n(r,\omega_n)\right], \quad 0 < r < \infty. \tag{3}$$

The conditions of the ideal contact are fulfilled between the two adjacent layers with the different shear moduli

$$w_j(r,\omega_j) = w_{j+1}(r,\omega_j), \quad r\tau_{\theta\varphi}^{(j)}(r,\omega_j) = r\tau_{\theta\varphi}^{(j+1)}(r,\omega_j), \quad j = \overline{1, n-1}. \tag{4}$$

The last equality can be written in the form, taking into consideration the relations (2)

$$G_j\left[w_j^{\bullet}(r,\omega_j) - ctg\omega_j w_j(r,\omega_j)\right] = G_{j+1}\left[w_{j+1}^{\bullet}(r,\omega_j) - ctg\omega_j w_{j+1}(r,\omega_j)\right], \quad j = \overline{1, n-1}. \tag{5}$$

It is necessary to estimate and to investigate the cone's stress state.

The scheme of the problem solution

The Mellin's integral transformation is applied to the relations (1), (3)-(5)

$$w_{j,s}(\theta)=\int_0^{\infty} w_j(r,\theta)r^{s-1}dr,$$
$$\operatorname{Re} s>0,\quad \omega_{j-1}<\theta<\omega_j,\quad j=\overline{1,n}. \tag{6}$$

As a result, one obtains the one-dimensional boundary problem

$$\frac{\left[\sin\theta w^{\bullet}_{j,s}(r,\theta)\right]^{\bullet}}{\sin\theta}+s(s-1)w_{j,s}(\theta)-\frac{w_{j,s}(\theta)}{\sin^2\theta}=0,\quad \omega_{j-1}<\theta<\omega_j,\quad j=\overline{1,n}; \tag{7}$$

$$G_n\left[w^{\bullet}_{n,s}(\omega_n)-ctg\omega_n w_{n,s}(\omega_n)\right]=q_s,\quad q_s=\int_0^{\infty} q(r)r^{s-1}dr; \tag{8}$$

$$w_{j,s}(\omega_j)=w_{j+1,s}(\omega_j),$$
$$G_j\left[w^{\bullet}_{j,s}(\omega_j)-ctg\omega_j w_{j,s}(\omega_j)\right]=G_{j+1}\left[w^{\bullet}_{j+1,s}(\omega_j)-ctg\omega_j w_{j+1,s}(\omega_j)\right],\quad j=\overline{1,n-1}. \tag{9}$$

One may be sure that the general solution of the equation (7) is the linear combination of Legendre's functions [20]

$$w_{j,s}(\theta)=C_j^0(s)P_{s-1}^1(\cos\theta)+C_j^1(s)Q_{s-1}^1(\cos\theta),$$
$$j=\overline{2,n},\quad \omega_{j-1}<\theta<\omega_j, \tag{10}$$

where $C_j^0(s)$, $C_j^1(s)$ ($j=\overline{2,n}$) are unknown constants, $P_{s-1}^1(\cos\theta)$, $Q_{s-1}^1(\cos\theta)$ are Legendre's functions. For the case $j=1$ the general solution of the equation (7) is given by the formula

$$w_{1,s}(\theta)=C_1^0(s)P_{s-1}^1(\cos\theta),$$
$$0<\theta<\omega_1. \tag{11}$$

The substitution of the equalities (10) in the conditions (9) leads to the relations

$$C_j^0(s)P_{s-1}^1(\cos\omega_1)+C_j^1(s)Q_{s-1}^1(\cos\omega_j)=C_{j+1}^0(s)P_{s-1}^1(\cos\omega_1)+C_{j+1}^1(s)Q_{s-1}^1(\cos\omega_j),$$
$$G_j\left[C_j^0(s)P_{s-1}^*(\omega_j)+C_j^1(s)Q_{s-1}^*(\omega_j)\right]=G_{j+1}\left[C_{j+1}^0(s)P_{s-1}^*(\omega_j)+C_{j+1}^1(s)Q_{s-1}^*(\omega_j)\right], \tag{12}$$
$$j=\overline{2,n-1}.$$

One must understand here that $P_s^*(\omega_j)$, $Q_s^*(\omega_j)$ are the correspondences

$$P_{s-1}^*(\theta)=P_{s-1}^2(\cos\theta)-ctg\theta P_{s-1}^1(\cos\theta),$$

$$Q^{*}_{s-1}(\theta)=Q^{2}_{s-1}(\cos\theta)-ctg\theta Q^{1}_{s-1}(\cos\theta)$$

Instead of the relation (12) for the case $j=1$ the conjugation's formulas (9) because of the equality (11) take the form

$$\begin{aligned} &C^{0}_{1}(s)P^{1}_{s-1}(\cos\omega_1)=C^{0}_{2}(s)P^{1}_{s-1}(\cos\omega_1)+C^{1}_{2}(s)Q^{1}_{s-1}(\cos\omega_1),\\ &G_1C^{0}_{1}(s)P^{*}_{s-1}(\omega_1)=G_2\left[C^{0}_{2}(s)P^{*}_{s-1}(\omega_1)+C^{1}_{2}(s)Q^{*}_{s-1}(\omega_1)\right]. \end{aligned} \tag{13}$$

One must proceed from the conjugations' condition (9). Let's input into consideration the matrices and the vectors

$$\mathbf{C}_j(s)=\begin{pmatrix} C^{0}_{j}(s)\\ C^{1}_{j}(s)\end{pmatrix},\quad j=\overline{2,n},$$

$$\mathbf{C}_1(s)=\begin{pmatrix} C^{0}_{1}(s)\\ 0\end{pmatrix}, \tag{14}$$

$$\mathbf{g}_j=\begin{pmatrix} 1 & 0\\ 0 & G_j\end{pmatrix},\quad j=\overline{1,n};$$

$$\begin{aligned} &\mathbf{R}_j(s)=\begin{pmatrix} P^{1}_{s-1}(\cos\omega_j) & Q^{1}_{s-1}(\cos\omega_j)\\ P^{*}_{s-1}(\omega_j) & Q^{*}_{s-1}(\omega_j)\end{pmatrix},\quad j=\overline{1,n-1},\\ &\mathbf{R}^{0}_{1}(s)=\begin{pmatrix} P^{1}_{s-1}(\cos\omega_j) & 0\\ P^{*}_{s-1}(\omega_j) & 0\end{pmatrix}. \end{aligned} \tag{15}$$

One can write the conjugation's conditions (12) with regard of these matrices and vectors in the form

$$\begin{aligned} &\mathbf{g}_j\mathbf{R}_j(s)\mathbf{C}_j(s)=\mathbf{g}_{j+1}\mathbf{R}_j(s)\mathbf{C}_{j+1}(s),\\ &j=\overline{2,n-1}. \end{aligned} \tag{16}$$

For the case $j=1$ the conjugation's condition correspondently to the relation (13) is written

$$\mathbf{g}_1\mathbf{R}^{0}_{1}(s)\mathbf{C}_1(s)=\mathbf{g}_2\mathbf{R}_1(s)\mathbf{C}_2(s). \tag{17}$$

One can obtain from the formulas (16), (17) the relations that connect the coefficients on the two adjacent layers

$$\begin{aligned} &\mathbf{C}_{j+1}(s)=\mathbf{R}^{-1}_{j}(s)\mathbf{g}^{-1}_{j+1}\mathbf{g}_j\mathbf{R}_j(s)\mathbf{C}_j(s),\\ &j=\overline{2,n-1}; \end{aligned} \tag{18}$$

$$\mathbf{C}_2(s)=\mathbf{R}^{-1}_{1}(s)\mathbf{g}^{-1}_{2}\mathbf{g}_1\mathbf{R}^{0}_{1}(s)\mathbf{C}_1(s). \tag{19}$$

The matrix $\mathbf{\Omega}_1^0(s)=\mathbf{R}_1^{-1}(s)\mathbf{g}_2^{-1}\mathbf{g}_1$ after calculations of the inverse matrices in it can be represented in the form

$$\mathbf{\Omega}_1^0(s)=\begin{pmatrix}\Phi_{11}^0(s) & \Phi_{12}^0(s)\\ \Phi_{21}^0(s) & \Phi_{22}^0(s)\end{pmatrix}=-\sin\omega_1\begin{pmatrix}Q_{s-1}^*(\omega_1) & -G_1^*Q_{s-1}^1(\cos\omega_1)\\ -P_{s-1}^*(\omega_1) & G_1^*P_{s-1}^1(\cos\omega_1)\end{pmatrix},$$
$$G_1^*=\frac{G_1}{G_2}. \tag{20}$$

One must use the relation, that defines Wronsky's determinant for Legendre's functions (3.4(25), [20]), during obtaining of this formula. Taking into consideration the equalities (15), (20) one can rewrite the formula (19)

$$\mathbf{C}_2(s)=\mathbf{\Omega}_1^0(s)\begin{pmatrix}P_{s-1}^1(\cos\omega_1)\\ P_{s-1}^*(\omega_1)\end{pmatrix}\mathbf{C}_1^0(s)=$$
$$=-\begin{pmatrix}Q_{s-1}^*(\omega_1) & -G_1^*Q_{s-1}^1(\cos\omega_1)\\ -P_{s-1}^*(\omega_1) & G_1^*P_{s-1}^1(\cos\omega_1)\end{pmatrix}\begin{pmatrix}P_{s-1}^1(\cos\omega_1)\\ P_{s-1}^*(\omega_1)\end{pmatrix}\frac{\mathbf{C}_1^0(s)}{(\sin\omega_1)^{-1}}. \tag{21}$$

Introducing the designation

$$\mathbf{\Omega}_j(s)=\mathbf{R}_j^{-1}(s)\mathbf{g}_{j+1}^{-1}\mathbf{g}_j\mathbf{R}_j(s), \tag{22}$$

formula (18) can be represented in the form

$$\mathbf{C}_{j+1}(s)=\mathbf{\Omega}_j(s)\mathbf{C}_j(s),$$
$$j=\overline{2,n-1}. \tag{23}$$

The equality $\mathbf{C}_n(s)=\mathbf{\Omega}_{n-1}(s)\mathbf{C}_{n-1}(s)$ leads from the formula (23), which is why one can obtain

$$\mathbf{C}_n(s)=\mathbf{\Omega}_{n-1}(s)\mathbf{\Omega}_{n-2}(s)\ldots\mathbf{\Omega}_2(s)\mathbf{C}_2(s),\quad n\geq 3, \tag{24}$$

(when $n=2$ the formula (21) is correct). Introducing the matrix

$$\mathbf{\Phi}_n(s)=\mathbf{\Omega}_{n-1}(s)\mathbf{\Omega}_{n-2}(s)\ldots\mathbf{\Omega}_2(s)\mathbf{\Omega}_1^0(s)=\begin{pmatrix}\Phi_{11}(s) & \Phi_{12}(s)\\ \Phi_{21}(s) & \Phi_{22}(s)\end{pmatrix}, \tag{25}$$

with the help of formulas (24), (19) and (25) one obtains the correspondence

$$\mathbf{C}_n(s)=\begin{pmatrix}C_n^0(s)\\ C_n^1(s)\end{pmatrix}=\mathbf{\Phi}_n(s)\begin{pmatrix}P_{s-1}^1(\cos\omega_1) & C_1^0(s)\\ P_{s-1}^*(\omega_1) & C_1^0(s)\end{pmatrix}. \tag{26}$$

Let's satisfy the boundary condition (3), that can be represented with regard of (10) in the form

$$G_n\left[C_n^0(s)P_{s-1}^*(\omega_n)+C_n^1(s)Q_{s-1}^*(\omega_n)\right]=q_s \tag{27}$$

As a result of the formula (26), one can obtain

$$C_1^0(s)\left[G_n\Delta_n(s)\right]^{-1}q_s,$$

$$\Delta_n = P_{s-1}^*(\omega_n)\left[\Phi_{11}(s)P_{s-1}^1(\cos\omega_1)+\Phi_{12}(s)P_{s-1}^*(\omega_1)\right]+ \tag{28}$$

$$+Q_{s-1}^*(\omega_n)\left[\Phi_{21}(s)P_{s-1}^1(\cos\omega_1)+\Phi_{22}(s)P_{s-1}^*(\omega_1)\right].$$

With the help of the formula (21) one constructs $\mathbf{C}_2(s)$, and the rest of the coefficients must be found with the relation (23). For example, $\mathbf{C}_3(s)=\Omega_2(s)\mathbf{C}_2(s)$ and so on. Mellin's transformations of the displacements can be written by the formulas (10), (11). The required displacements are obtained from the formulas

$$w_j(r,\theta)=\frac{1}{2\pi i}\int_{\gamma-i\infty}^{\gamma+i\infty}\left[C_j^0(s)P_{s-1}^1(\cos\theta)+C_j^1(s)Q_{s-1}^1(\cos\theta)\right]r^{-s}ds,$$

$$w_1(r,\theta)=\frac{1}{2\pi i}\int_{\gamma-i\infty}^{\gamma+i\infty}C_1^0(s)P_{s-1}^1(\cos\theta)r^{-s}ds,\quad j=\overline{2,n}. \tag{29}$$

where γ is the small positive quantity.

Conclusions

1) The problem of the conical layered medium torsion is solved by a new approach. The core of the proposed method is in a direct application of the integral transformation to the equilibrium equations (to the torsion equation in this case), instead of an applying it to the well known different representations of these equations through the harmonic or any other functions as it is done traditionally. The further reduction of initial problem's boundary conditions in the transformation space to the vector form allows the construction of the exact solution, where coefficients are calculated by the recurrent formula.

2) The exact solution of the torsion problem for the conical layered elastic cone is obtained when on the external layer the torsion stress are given. The conditions of the ideal contact are fulfilled on the adjacent layers.

3) The proposed approach allows to obtain the solution of the axisymmetrical problem for the elastic conical layered medium when the conditions of the ideal contact are fulfilled on the adjacent layers.

References

1. Stephens, L.S. Finite Element Analysis of the Initial Yielding Behavior of a Hard Coating/Substrate System With Functionally Graded Interface Under Indentation and Friction / L.S. Stephens, Y. Liu and E.I. Meletis // Journal of Tribology. — 1999. — Vol. 122, Iss. 2. — PP. 381–387.
2. Birk, C. A modified scaled boundary finite element method for three-dimensional dynamic soil-structure interaction in layered soil / C. Birk, R. Behnke // International Journal for Numerical Methods in Engineering. — 2012. — Vol. 89, Iss. 3. — PP. 371–402.
3. Kim, K.S. Green's Function Approach to Solution of Transient Temperature for Thermal Stresses of Functionally Graded Material / K.S. Kim, N. Noda // JSME International Journal Series A Solid Mechanics and Material Engineering. — 2001. — Vol. 44, No. 1. — PP. 31–36.

4. Бабешко, В.А. О проблеме блочных структур академика М.А.Садовского / В.А. Бабешко, О.М. Бабешко, О.В. Евдокимова // Доклады академии наук. — 2009. — Том 427, № 4. — С. 480–485.
5. Бабешко, В.А. К теории блочного элемента / В.А. Бабешко, О.М. Бабешко, О.В. Евдокимова // Доклады академии наук. — 2009. — Том 427, № 2. — С. 183–187.
6. Kulchytsky-Zhyhailo, R.D. Approximate method for analysis of the contact temperature and pressure due to frictional load in an elastic layered medium / R.D. Kulchytsky-Zhyhailo, A.A. Yevtushenko // International Journal of Solids and Structures. — 1998. — Vol. 35, Iss. 3–4. — PP. 319–329.
7. Аналитические решения смешанных осесимметричных задач для функционально-градиентных сред [Текст] : монография / С.М. Айзикович, В.М. Александров [и др.]. — М. : Физматлит, 2011. — 192 с.
8. Ke, L.L. Two-dimensional contact mechanics of functionally graded materials with arbitrary spatial variations of material properties / L.L. Ke, Y.S. Wang // International Journal of Solids and Structures. — 2006. — Vol. 43, Iss. 18–19. — PP. 5779–5798.
9. Ke, L.L. Two-dimensional sliding frictional contact of functionally graded materials / L.L. Ke, Y.S. Wang // European Journal of Mechanics – A/Solids. — 2007. — Vol. 26, Iss. 1. — PP. 171–188.
10. Mykhas'kiv, V.V. Effective dynamic properties of 3D composite materials containing rigid penny-shaped inclusions / V.V. Mykhas'kiv, O.M. Khay, *et al.* / Waves in Random and Complex Media. — 2010. — Vol. 20, No.3. — PP. 491–510.
11. Ватульян, А.О. Фундаментальные решения для ортотропной упругой среды в случае установившихся колебаний / А.О. Ватульян, Е.М. Чебакова // Прикладная механика и техническая физика. — 2004. — Том 45, № 5. — С. 131–139.
12. Калинчук, В.В. Динамика поверхности неоднородных сред [Текст] : монография / В.В. Калинчук, Т.И. Белянкова. — М. : Физматлит, 2009 (Чебоксары). — 312 с.
13. Budayev, B.V. Torsion of a circular cone with static and dynamic loading / B.V. Budayev, N.F. Morozov, M.A. Narbut // Journal of Applied Mathematics and Mechanics. — 1994. — Vol. 58, Iss. 6. — PP. 1097–1100.
14. Мехтиев, М.Ф. Асимптотическое поведение решения осесимметричной задачи теории упругости для трансверсально-изотропного полого конуса / М.Ф. Мехтиев, Н.А. Сардарова, Н.И. Фомина // Известия Российской академии наук. Механика твердого тела. — 2003. — № 2. — С. 61–70.
15. Улитко, А.Ф. Векторные разложения в пространственной теории упругости [Текст] : методический материал / А.Ф. Улитко. — К. : Академпериодика, 2002. — 341 с.
16. Popov, G. The steady-state oscillations of the elastic infinite cone loaded at a vertex by a concentrated force / G. Popov, N. Vaysfel'd // Acta Mechanica. — 2011. — Vol. 221, Iss. 3–4. — PP. 261–270.
17. Попов, Г.Я. К решению краевых задач механики и математической физики для слоистых сред / Г.Я. Попов // Известия Академии наук Армянской ССР. Механика. — 1978. — Том XXXI, № 2. — С. 34–47.
18. Попов, Г.Я. Концентрация упругих напряжений возле штампов, разрезов, тонких включений и подкреплений / Г.Я. Попов. — М. : Наука, 1982. — 344 с.
19. Nowacki, W. Teoria sprezystosci / W. Nowacki. — Warszawa: PWN, 1970. — 769 p.
20. Bateman, H. Higher Transcendental Functions. Vol. 2. / H. Bateman, A. Erdelyi. — New York: The McGraw-Hill, 1953. — 396 p.

НАПРУЖЕНИЙ СТАН КЛИНУВАТО-ШАРУВАТОГО СЕРЕДОВИЩА

Н.Д. Вайсфельд

Одеський національний університет імені І.І. Мечникова,
вул. Дворянська, 2, Одеса, 65082, Україна; e-mail: vaysfeld@onu.edu.ua

Розглядається нескінченний шаруватий конус, що заповнює область, що представляє собою послідовність воронок-шарів, вставлених одна в іншу. Модуль зсуву конуса стрибкоподібно змінюється на конічних поверхнях. Між сусідніми шарами з різними модулями зсуву виконуються умови ідеального контакту. До зовнішньої поверхні конуса прикладені дотичні напруження. Потрібно визначити зміщення конуса, що задовольняють рівнянню кручення при крайових умовах, а також дослідити напруги, що виникають на поверхні конічних шарів. Для розв'язання задачі застосовується інтегральне перетворення по радіальній координаті. Отримана одновимірна задача розв'язана точно за допомогою побудованих рекурентних формул, що пов'язують константи загальних рішень кожного шару. Застосування зворотного перетворення завершує побудову точного рішення. Задача деталізована для окремих випадків шаруватості.

Ключові слова: клинувато-шарувате середовище, інтегральне перетворення, векторна крайова задача

НАПРЯЖЕННОЕ СОСТОЯНИЕ КЛИНОВИДНО-СЛОИСТОЙ СРЕДЫ

Н.Д. Вайсфельд

Одесский национальный университет имени И.И. Мечникова,
ул. Дворянская, 2, Одесса, 65082, Украина; e-mail: vaysfeld@onu.edu.ua

Рассматривается бесконечный слоистый конус, заполняющий область, представляющую собой последовательность воронок-слоев, вставленных одна в другую. Модуль сдвига конуса скачкообразно меняется на конических поверхностях. Между соседними слоями с различными модулями сдвига выполняются условия идеального контакта. К внешней поверхности конуса приложены касательные напряжения. Требуется определить смещения конуса, удовлетворяющие уравнению кручения при краевых условиях, а также исследовать напряжения, возникающие на поверхности конических слоев. Для решения задачи применяется интегральное преобразование по радиальной координате. Полученная одномерная задача решена точно с помощью построенных рекуррентных формул, связывающих константы общих решений каждого слоя. Применение обратного преобразования завершает построение точного решения. Задача детализирована для частных случаев слоистости.

Ключевые слова: клиновидно-слоистая среда, интегральное преобразование, векторная краевая задача

УДК 681.32.019.3

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 43-49

ГИСТОГРАММНЫЙ СПОСОБ ГЕНЕРИРОВАНИЯ СЛУЧАЙНЫХ ЧИСЕЛ В ЗАДАЧАХ ИССЛЕДОВАНИЯ НАДЕЖНОСТИ

С.В. Ленков[1], А.В. Селюков[2], В.О. Браун[1], В.Н. Цыцарев[1], Ю.В. Березовская[3]

[1] Военный институт Киевского национального университета имени Тараса Шевченко,
ул. Ломоносова, 81, Киев, 03680, Украина; e-mail: lenkov_s@ukr.net
[2] Государственное предприятие «Научный центр точного машиностроения»,
ул. Бориспольская, 9, Киев, 02099, Украина; e-mail: selukov@3g.ua
[3] Киевский национальный университет имени Тараса Шевченко,
ул. Владимирская, 60, Киев, 01601, Украина; e-mail: kjv@univ.kiev.ua

Разработан способ ускоренного генерирования случайных чисел с заданным законом распределения, названный гистограммным. Приведены результаты исследований гистограммного датчика случайных чисел. Даны рекомендации по использованию гистограммных датчиков случайных чисел.

Ключевые слова: случайные числа, гистограмма, датчики, быстродействие, закон распределения

Введение

При исследовании надежности сложных технических систем часто единственным методом эффективного решения задачи остается метод имитационного статистического моделирования [1, 2]. Применение метода статистического моделирования неизбежно предполагает использование различных датчиков (генераторов) случайных чисел, с помощью которых генерируются случайные реализации наработки до отказа отдельных элементов исследуемой технической системы. Статистические модели разрабатываются, как правило, для решения различных оптимизационных задач надежности, в которых требуется многократное получение оценок показателей надежности и качества системы, для которой требуется найти оптимальные значения ее параметров. Поэтому наряду с требованиями точности и адекватности датчиков случайных чисел к ним предъявляются также и требования по быстродействию.

Цель статьи

В [3, 4] разработаны датчики случайных чисел для наиболее часто используемых в задачах надежности законов распределения.

Целью настоящей статьи является разработка нового способа ускоренного генерирования случайных чисел с заданным законом распределения, который мы назвали *гистограммным способом*.

Основная часть

Обычно случайные числа с заданным законом распределения генерируются методом обратной функции, согласно которому вначале генерируется случайная

величина (с. в.) ρ, подчиненная равномерному распределению в интервале [0,1]. Затем получается с. в. ξ, имеющая заданное распределение, путем решения уравнения

$$F_\xi(\xi) = \rho, \tag{1}$$

где $F_\xi(t)$ — функция распределения с. в. ξ.

Если уравнение (1) удается решить в аналитическом виде, то с. в. ξ получается непосредственно из выражения

$$\xi = F_\xi^{-1}(\rho), \tag{2}$$

где $F_\xi^{-1}(t)$ — функция, обратная по отношению к функции $F_\xi(t)$.

К сожалению, уравнение (1) не всегда можно решить аналитически, и для его решения приходится применять какие-либо численные методы, что, естественно, требует определенных затрат машинного времени.

Идея гистограммного способа генерирования с. в. заключается в замене функции распределения (ФР) $F_\xi(t)$ ее линейной аппроксимацией, заданной на некотором множестве дискретных точек ее аргумента, то есть ее гистограммой.

Вместо функции $F(t)$ в (1) и (2) нам удобнее использовать функцию надежности (ФН) $P(t)$, которая с функцией $F(t)$ связана соотношением $P(t) = 1 - F(t)$. Гистограмма ФН $P(t)$ в памяти компьютера представляется совокупностью значений (массивом) $\{P_i\}$, где $P_i = P(t_i)$. Будем полагать, что гистограмма построена на множестве равноотстоящих точек аргумента $\{t_i = i \cdot \Delta;\ i = \overline{1, N_\Delta}\}$, где Δ — интервал дискретности; N_Δ — число точек, в которых построена гистограмма (рис. 1). Граничное значение области определения гистограммы $T_{\max}$ будем определять из уравнения

$$P(T_{\max}) = \gamma, \tag{3}$$

где γ — малая величина, подбираемая экспериментально.

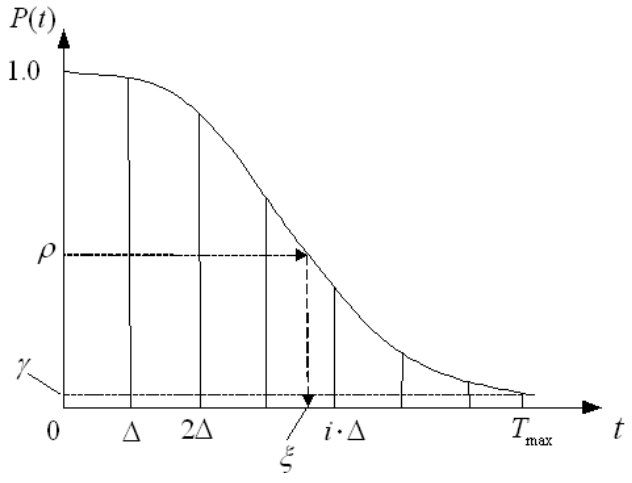


Рис.1. К пояснению принципа работы гистограммного генератора случайных чисел

Количество точек аппроксимации N_Δ задается из соображений обеспечения требуемой точности датчика. Величина Δ после определения $T_{\max}$ вычисляется по формуле $\Delta = \frac{T_{\max}}{N_\Delta}$.

Для получения с. в. ξ, подчиненной $P(t)$, нужно сделать следующее:

1) получить равномерно распределенную в интервале [0, 1] с. в. ρ, и

2) рассчитать приближенное значение с. в. ξ по формуле:

$$\xi = t_{i+1} - \frac{\rho - P_{i+1}}{P_i - P_{i+1}}\Delta, \quad i = \overline{0, N_\Delta - 1}. \tag{4}$$

В (4) предполагается, что $P(t_0) = P(0) = 1$.

Очевидно, что точность приближения закона распределения с. в. ξ к заданному закону распределения $P(t)$ будет зависеть от точности аппроксимации $\{P_i\}$, которая, в свою очередь, зависит от γ и N_Δ. Экспериментально установлено, что вполне приемлемая для практики точность гистограммного датчика обеспечивается при $\gamma \approx 0.001$ и $N_\Delta \approx 30$.

Далее приводятся результаты исследований характеристик гистограммного датчика в сравнении с соответствующими «точными» датчиками. В качестве «точных» датчиков для сравнительного анализа были взяты датчики диффузионного немонотонного (*DN*) и экспоненциального (*E*) распределений. Эти датчики подробно описаны в [4] и называются соответственно *DNGEN* и *EGEN*. Построенные нами для этих же распределений гистограммные датчики названы соответственно *DNGEN_G* и *EGEN_G*.

Датчик *DNGEN* генерирует с. в., подчиняющиеся *DN*-распределению, ФР которого имеет следующий вид [3,4]:

$$DN(t;\mu,\nu) = \Phi\left(\frac{\frac{t}{\mu} - 1}{\nu\sqrt{\frac{t}{\mu}}}\right) + \exp\left(\frac{2}{\nu^2}\right)\Phi\left(-\frac{\frac{t}{\mu} + 1}{\nu\sqrt{\frac{t}{\mu}}}\right), \tag{5}$$

где

$\Phi(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z}\exp\left(-\frac{x^2}{2}\right)dx$ — нормированная функция нормального распределения;

μ и ν — параметры распределения: μ — параметр масштаба, совпадающий с математическим ожиданием, ν — параметр формы (коэффициент вариации).

Датчик *EGEN* генерирует с. в., подчиняющиеся *E*-распределению с ФР

$$E(t;\mu) = 1 - \exp\left(-\frac{t}{\mu}\right). \tag{6}$$

E-распределение является однопараметрическим с коэффициентом вариации $\nu = 1$.

Для исследования датчиков была разработана программа для ПК, с помощью которой генерируются заданным датчиком последовательности случайных чисел (выборки) заданного объема. Программа разработана в системе программирования Delphi [5], в которой имеется встроенная функция `Random`, предназначенная для генерирования с. в. с равномерным распределением в интервале [0,1]. По полученным

выборкам в программе вычисляются оценки математического ожидания $M[\bullet]$ и коэффициента вариации $V[\bullet]$ оценок параметров распределения, для которого генерируются с. в. Вычисляются также оценки коэффициента парной корреляции между выборками $K[X,Y]$, где $X=\{x_i\}$ и $Y=\{y_i\}$ — две различные выборки одной и той же с. в.

С помощью разработанной программы получаются и отображаются на экране ПК гистограммы распределений относительного числа попаданий с. в. в различные интервалы области ее определения. Эти гистограммы предназначены только для визуализации генерируемых с. в. и никак не связаны с гистограммами ФН, использующимися при генерации с. в. гистограммным способом.

Расчеты были произведены для параметров *DN*-распределения $\mu=1$ и $\nu=0.5$, и параметра *E*-распределения $\mu=1$. Относительные ошибки ε_μ и ε_ν вычислялись по формулам:

$$\varepsilon_\mu=(\mu-\overline{\mu})\times\frac{100}{\mu},$$
$$\varepsilon_\nu=(\nu-\overline{\nu})\times\frac{100}{\nu}, \qquad (7)$$

где $\overline{\mu}$ и $\overline{\nu}$ — выборочные оценки параметров μ и ν соответственно.

На рис. 2 показана гистограмма, построенная для равномерно распределенных случайных чисел, получаемых с помощью функции `Random`. На рис. 3 приведены такие же гистограммы для случайных чисел, полученных при помощи «точных» и гистограммных датчиков (объем выборки $N=1000$).

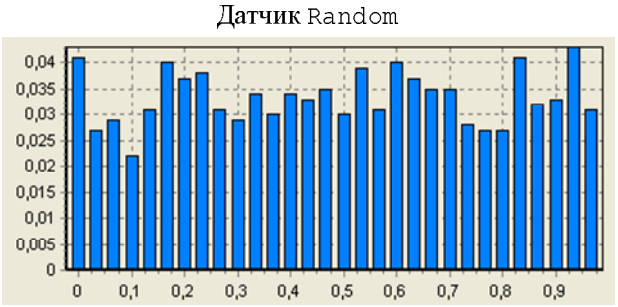
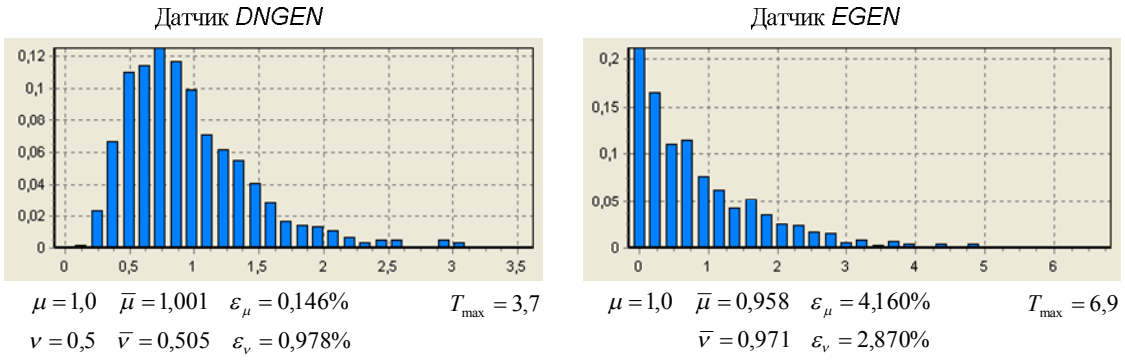


Рис. 2. Гистограмма равномерно распределенных случайных чисел в интервале [0,1]

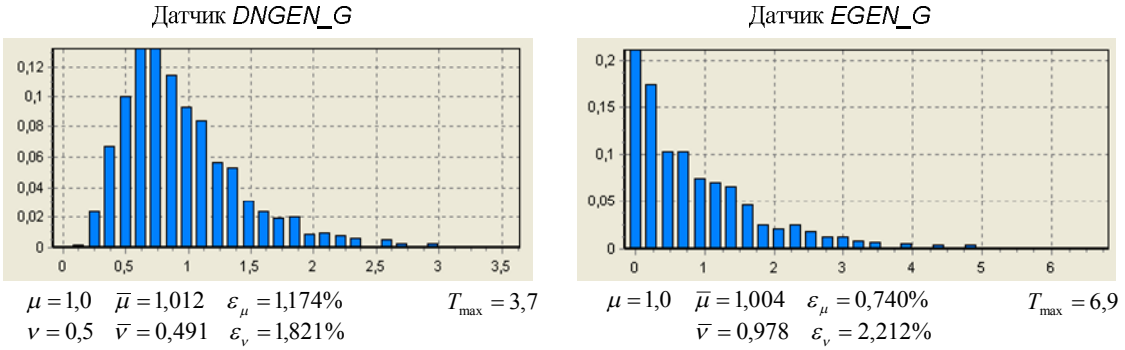
В табл. 1 представлены оценки $M[\bullet]$ и $V[\bullet]$ показателей μ и ν (и соответствующие ошибки ε), полученные по результатам моделирования 30 выборок объемом $N=1000$ каждая.

Следует отметить, что указанные в табл. 1 значения являются случайными реализациями соответствующих оценок, которые изменяются от эксперимента к эксперименту в пределах ошибок ε.

По полученным результатам можно сделать вывод о том, что точные и гистограммные датчики примерно одинаковы по характеристикам точности. Поэтому замена «точных» датчиков их гистограммными аналогами в статистических моделях не приводит к сколько-нибудь заметному ухудшению точности результатов моделирования.



а



б

Рис. 3. Примеры гистограмм распределения случайных чисел, генерируемых с помощью «точных» и гистограммных датчиков: а – «точные» датчики; б – гистограммные датчики ($N_\Delta = 30$)

Таблица 1.

Характеристики датчиков случайных чисел

Показатель	*DN*-распределение		*E*-распределение	
	DNGEN	*DNGEN_G*	*EGEN*	*EGEN_G*
Математическое ожидание среднего $M[\bar{\mu}]$	0.994	0.999	1.003	0.997
Математическое ожидание коэффициента вариации $M[\bar{\nu}]$	0.496	0.495	0.998	0.990
Относительная ошибка среднего ε_μ, %	0.511	0.021	0.318	0.277
Относительная ошибка коэффициента вариации ε_ν, %	0.658	0.868	0.161	0.908
Коэффициент вариации среднего $V[\bar{\mu}]$	0.018	0.015	0.033	0.025
Коэффициент вариации коэффициента вариации $V[\bar{\nu}]$	0.030	0.026	0.028	0.032
Коэффициент парной корреляции $K[X,Y]$	0.046	0.039	0.026	0.038

Для сравнительной оценки быстродействия «точных» и гистограммных датчиков были произведены расчеты по той же программе (с помощью которой получены данные табл. 1) для больших объемов генерируемых выборок, при которых затраты машинного времени на вычисления становятся ощутимыми. Результаты таких расчетов представлены в табл. 2 (данные получены для процессора AMD Athlon II X2 245, 2.90 ГГц).

Таблица 2.

Показатели быстродействия датчиков случайных чисел

Размер выборки N	Время счета для различных датчиков			
	DNGEN	*DNGEN_G*	*EGEN*	*EGEN_G*
0.1×10^6	13″	3″	3″	3″
0.5×10^6	1′8″	16″	15″	15″
10^6	2'16″	33″	30″	31″
5×10^6	11′29″	2′45″	2′29″	2′33″

По полученным данным хорошо видно, что применение гистограммных датчиков случайных чисел дает существенный выигрыш в скорости счета в случае «сложных» законов распределения. «Сложность» закона распределения здесь понимается в смысле потребности большого объема вычислений для генерирования с. в. К таким «сложным» законам распределения, по-видимому, можно отнести и *DN*-распределение. В случае «простых» законов распределения, к таковым можно отнести *E*-распределение, выигрыш при использовании гистограммного способа практически отсутствует.

Заключение

В заключение можно сделать общий вывод о том, что при разработке статистических моделей, в которых необходимо генерировать случайные величины, подчиняющиеся «сложным» законам распределения, целесообразно использовать гистограммные датчики случайных чисел.

Список литературы

1. Ушаков, И.А. Вероятностные модели надежности информационно-вычислительных систем [Текст] / И.А. Ушаков. — М. : Радио и связь, 1991. — 132 с.
2. Надежность и эффективность в технике [Текст] : справочник в 10 т. / Ред. совет: В.С. Авдуевский (пред.) и др. — М. : Машиностроение, 1986. — .
   Т. 3 : Эффективность технических систем / Под ред. В.Ф. Уткина, Ю.В. Крючкова. — 1988. — 328 с.
3. Стрельников, В.П. Оценка и прогнозирование надежности электронных элементов и систем [Текст] : сборник научных трудов / В.П. Стрельников, А.В. Федухин. — К. : Логос, 2002. — 486 с.
4. Федухин, А.В. К вопросу о статистическом моделировании надежности / А.В. Федухин, Н.В. Сеспедес-Гарсия // Математичні машини і системи. — 2006. — № 1. — С. 156–163.
5. Архангельский, А.Я. Программирование в Delphi 6 [Текст] : монография / А.Я. Архангельский. — М. : Бином, 2002. — 1117 с.

ГІСТОГРАМНИЙ СПОСІБ ГЕНЕРУВАННЯ ВИПАДКОВИХ ЧИСЕЛ В ЗАДАЧАХ ДОСЛІДЖЕННЯ НАДІЙНОСТІ

С.В. Лєнков[1], О.В. Сєлюков[2], В.О. Браун[1], В.М. Цыцарєв[1], Ю.В. Березовська[3]

[1] Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81а, Київ, 03680, Україна; e-mail: lenkov_s@ukr.net
[2] Державне підприємство «Науковий центр точного машинобудування»,
вул. Бориспільська, 9, Київ, 02099, Україна; e-mail: selukov@3g.ua
[3] Київський національний університет імені Тараса Шевченка,
вул. Володимирська, 60, Київ, 01601, Україна; e-mail: kjv@univ.kiev.ua

Розроблено спосіб прискореного генерування випадкових чисел із заданим законом розподілу, названий гістограмним. Наведено результати досліджень гістограмного датчика випадкових чисел. Надано рекомендації щодо використання гістограмного датчиків випадкових чисел.
Ключові слова: випадкові числа, гістограма, датчики, швидкодія, закон розподілу

HISTOGRAM METHOD FOR GENERATING RANDOM NUMBERS IN RELIABILITY RESEARCH TASKS

Sergey V. Lenkov[1], Oleksandr V. Selyukov[2], Vadim O. Brown[1], Vadim M. Tsytsaryev[1], Julia V. Berezovska[3]

[1] Military Institute, Taras Shevchenko National University of Kyiv,
81-A Lomonosov str., Kyiv, 03680, Ukraine; e-mail: lenkov_s@ukr.net
[2] Scientific center of precision engineering, State enterprise,
9 Boryspilska str., Kyiv, 02099, Ukraine; e-mail: selukov@3g.ua
[3] Taras Shevchenko National University of Kyiv
64 Volodymyrs'ka str., Kyiv, 01601, Ukraine; e-mail: kjv@univ.kiev.ua

This paper focuses on development of rapid method for random numbers generation according to a given distribution. Developed method named «Histogram». The results of histogram method for generating random numbers research are presented. Recommendations on the use of histogram sensors are given.
Keywords: random numbers, histogram, sensors, processing speed, distribution law

УДК 004.415.056.5(075)

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 50-60

АМАЛЬГАМИ, ПОВНОТА ДІАГРАМ ТА ПІДОБ'ЄКТИ МНОЖИН В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

І.М. Павлов

Національний технічний університет України «Київський політехнічний інститут»,
просп. Перемоги, 37, Київ, 03056, Україна; e-mail: pavlov@ukr.net

У статті розглядаються математичні моделі взаємовідносин множин та підмножин на основі аналізу категорій логіки з метою подальшого проведення аналізу загроз на системи захисту інформації. Наведено опис зворотного образу, ядерних відношень та амальгам у множинах систем захисту інформації.

Ключові слова: амальгами, множина, підмножина, об'єкти, підоб'єкти, функції, система захисту інформації

Вступ

Наявні математичні моделі процесів нападу на інформацію та її захисту, на яких ґрунтуються оцінки рівня захищеності інформації у системах захисту інформації, не враховують динаміку зміни множин можливих несанкціонованих втручань і варіацій їх параметрів як у реальному масштабі часу, так і у процесі експлуатації інформаційних систем.

Моделювання у загальному розумінні та моделювання процесів нападу на інформацію у конкретному випадку є одним із ефективних методів дослідження поведінки технічних об'єктів при реалізації антагоністичних прагнень суб'єктів інформаційного конфлікту.

У [1, 2] авторами запропоновані основи категорійного апарату теорії множин, які дозволяють пояснити процес взаємовідносин множин загроз и множин системи захисту інформації, на якому можна будувати різни математичні моделі з метою аналізу систем інформаційного обміну в системах критичного застосування.

Мета дослідження

Під час моделювання процесів нападу на інформацію та процесів блокування таких нападів у будь-яких конфліктних множинах виникає проблема опису конфлікту з метою розкриття тих або інших напрямків побудови різних множин у системах захисту інформації для найбільш ефективного перекриття множин загроз живучими множинами механізмів захисту [3], для чого необхідний опис зворотного образу, ядерних відношень та амальгам у множинах систем захисту інформації, що і є *метою* цієї статті.

Основна частина

У множинах та підмножинах коамальгамою або зворотнім образом пари $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$ β-стрілок з загальним кінцем можна уявити межу у β-діаграми, яка представлена на рис. 1.

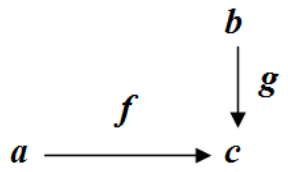


Рис. 1. β-діаграма пари стрілок $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$

Конус для цієї діаграми складається з 3-х стрілок f', h, g', для яких комутативна діаграма, надана на рис. 2(а).

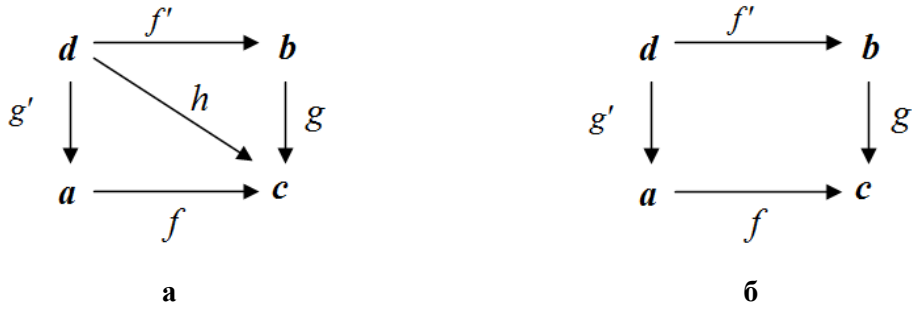


Рис. 2. Комутативні діаграми пари $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$: а – з 3-х стрілок f', h, g'; б – з 2-х стрілок f', g'

Це означає, що $h = g^{\circ} f' = f^{\circ} g'$. Тому можна казати, що конусом є пара $a \overset{g'}{\leftarrow} d \overset{f'}{\rightarrow} b$ β-стрілок, для яких квадрат, наданий на рис. 2(б), комутативний, тобто $f^{\circ} g' = g^{\circ} f'$.

Таким чином, згідно визначення універсальності конусу, зворотнім образом пари $a \overset{f}{\rightarrow} c \overset{g}{\leftarrow} b$ буде пара β-стрілок $a \overset{g'}{\leftarrow} d \overset{f'}{\rightarrow} b$, яка має наступні властивості [4, 5]: $f^{\circ} g' = g^{\circ} f'$, та для будь-яких $a \overset{h}{\leftarrow} e \overset{j}{\rightarrow} b$, таких, що $f^{\circ} h = g^{\circ} j$, існує і при тому тільки одна стрілка $k : e \rightarrow d$, яка задовольняє рівнянню $h = g'^{\circ} k$ і $j = f'^{\circ} k$.

Іншою мовою, для будь-яких h і j, для яких зовнішній квадрат (тобто кордон наведеної на рис. 3 діаграми) комутативний, мається одне доповнення цієї діаграми стрілкою k, при якому уся діаграма стає комутативною.

Зовнішній квадрат f, g, f', g' цієї діаграми ще має назву декартового квадрату. У цьому випадку можна казати, що f' — зворотній образ f відносно g і що f' отримується підйомом f вдовж g, а g' — зворотній образ g відносно f і отримується підйомом g вдовж f.

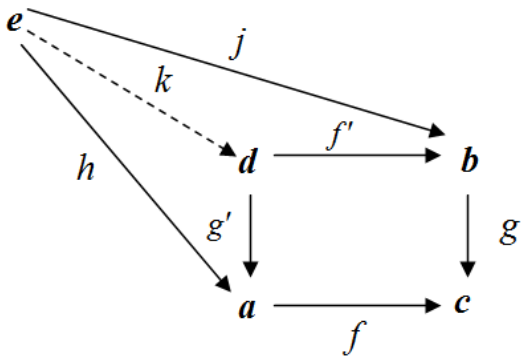


Рис. 3. Комутативні діаграми пари зворотного образу $a \overset{h}{\leftarrow} e \overset{j}{\rightarrow} b$ для рівнянь $h = g'^{\circ}k$ і $j = f'^{\circ}k$

У **Set** [6] зворотній образ двох теоретико-множинних функцій f і g визначається рівняннями (рис. 4):

$$D = \{\langle x, y\rangle : x \in A,\ y \in B \text{ і } f(x) = g(y)\}$$
$$f'(\langle x, y\rangle) = y, \quad g'(\langle x, y\rangle) = x. \tag{1}$$

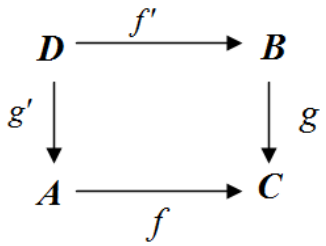


Рис. 4. Комутативна діаграма теоретико-множинних функцій

Таким чином, D є підмножиною добутку $A \times B$, а f' і g' — функції проектування. І D — є добутком A і B над C $\left(A \underset{C}{\times} B\right)$.

Якщо $f : A \rightarrow B$ — довільна функція і C — деяка підмножина у B, то можна уявити *прообразом множини* C при відображенні f (ще позначають, як $f^{-1}(C)$) підмножину у A, яка складається з усіх тих елементів $x \in A$, для яких $f(x) \in C$, тобто:

$$f^{-1}(C) = \{x : x \in A \text{ і } f(x) \in C\}. \tag{2}$$

Формула (2) представлена діаграмою, наведеною на рис. 5.

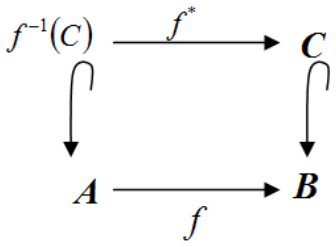


Рис. 5. Комутативна діаграма прообразу множини C при відображенні f

У діаграмі, яка наведена на рис. 5, стрілки із зігнутими кінцями визначають включення, а f^* визначається рівнянням $f^*(x) = f(x)$ для $x \in f^{-1}(C)$. Тобто f^* — обмеження функції f на $f^{-1}(C)$ є декартовим квадратом у категорії **Set**. Таким чином, прообраз C при відображенні f отримується підйомом C вздовж f (рис. 6).

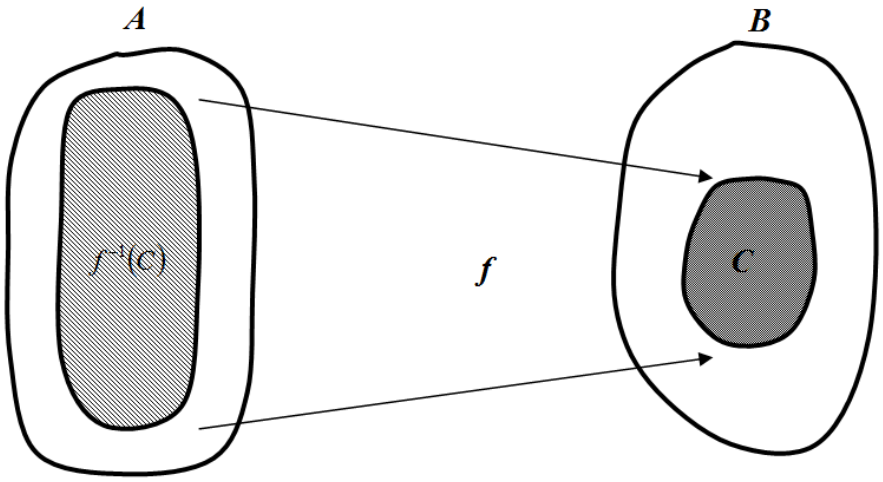


Рис. 6. Діаграма прообразу C при відображенні f

Поставимо у відповідність кожній функції $f : A \to B$ відношення еквівалентності на A і позначимо через R_f. Таке відношення ще має назву *ядерного відношення* або *ядра функції f*, і визначимо:

$$R_f = \{\langle x, y\rangle : x \in A \text{ і } y \in A \text{ і } f(x) = f(y)\},$$
$$\text{або } xR_f y \text{, якщо і тільки, коли } f(x) = f(y). \tag{3}$$

Тоді діаграма бути мати вигляд, наведений на рис. 7, де $p_1(\langle x, y\rangle) = x$ і $p_2(\langle x, y\rangle) = y$ декартов квадрат, тобто R_f отримується підйомом f вдовж самого себе.

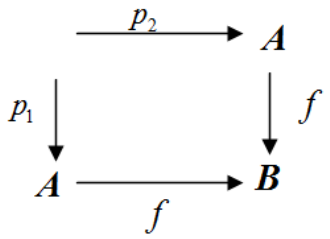


Рис. 7. Комутативна діаграма епі-моно-розкладання стрілок

На цій основі можна підтвердити лему про квадрати, коли діаграма, яка надана на рис. 8, комутативна, тоді якщо два малих квадрата декартові, то зовнішній прямокутник також декартовий (нижня і верхня сторони якого є композиціями відповідно нижніх і верхніх сторін малих квадратів).

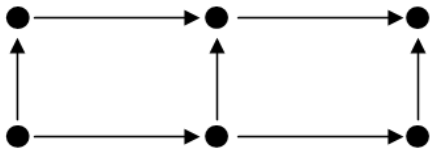


Рис. 8. Комутативна діаграма квадрату

Якщо зовнішній прямокутник і правий квадрат декартові, то декартовий і лівий квадрат. Відповідно, якщо прямокутник перевернути на 90°, то коли зовнішній прямокутник і ніжній квадрат декартові, то верхній квадрат теж декартовий.

У вільній категорії (рис. 9(а)) стрілка $f : a \to b$ мономорфна, тоді і тільки тоді, коли квадрат декартовий; якщо квадрат декартовий (рис. 9(б)), і f — монострілка, то g також мономорфна.

а **б**

Рис. 9. Комутативні діаграми квадратів множин: а – у вільній категорії; б – якщо квадрат декартовий

Поняття амальгами є двійковим по відношенню до поняття зворотного образу.

Амальгамою є пари стрілок $a \overset{f}{\leftarrow} c \overset{g}{\rightarrow} b$ з загальним початком [7], як надано на рис. 10.

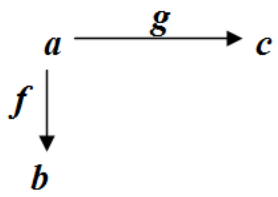


Рис. 10. Діаграма пари стрілок $a \overset{f}{\leftarrow} c \overset{g}{\rightarrow} b$

У категорії **Set** амальгама отримується побудовою диз'юнктивного об'єднання $b+c$ і ототожненням $f(x)$ з $g(x)$ для кожного $x \in a$ (тобто амальгама співпадає з коприрівнювачем пари композицій $a \overset{f}{\rightarrow} b \mapsto b+c$, $a \overset{g}{\rightarrow} c \mapsto b+c$).

Таким чином β може бути повною, якщо у ній діаграма має межу. Двійковим образом категорії β є коповнота, якщо кожна β-діаграма має комежу. А біповною є категорія, яка є одночасно повною і коповною.

Кінцевою може бути діаграма, яка має кінцеву кількість об'єктів і кінцеве число стрілок між ними. Таким чином, категорія може бути кінцево повною, якщо вона має межу будь-якої діаграми. А кінцево коповною може бути діаграма, яка має комежу і є кінцевою. Таким чином і визначається кінцева біповнота.

Для даних множин A і B можна утворити у **Set** сукупність B^A усіх функцій, визначених на A, які приймають значення B, тобто:

$$B^A = \{f : f - \text{функція із } A \text{ у } B\}. \qquad (4)$$

Щоб визначити B^A у стрілках необхідно асоціювати з множиною B^A спеціальну стрілку

$$ev : B^A \times A \to B. \qquad (5)$$

Категорний опис B^A базується на тому факті, що спеціальна стрілка має властивості універсальності серед усіх функцій вигляду $C \times A \overset{g}{\rightarrow} B$.

Для будь-якої такої функції g існує одна і тільки одна функція $\hat{g} : C \to B^A$, для якої діаграма, яка надана на рис. 11, є комутативною.

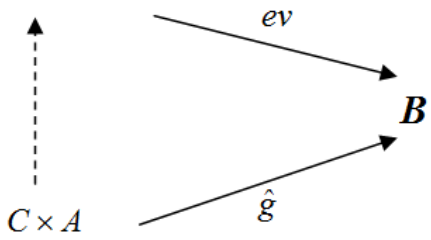


Рис. 11. Комутативна діаграма функторного добутку функцій

На діаграмі на парі $\langle c,a\rangle \in C\times A$ значення функції дорівнює:

$$\hat{g}\times id_A = \langle \hat{g}(c), id_A(a)\rangle = \langle \hat{g}(c), a\rangle . \qquad (6)$$

Таке визначення функції $\hat{g}$ зумовлено тою обставиною, що при кожному фіксованому c функція g визначає відображення $A\to B$, яке отримується, якщо перший елемент упорядкованих пар, які є аргументом функції g, покласти рівним c, у той-же час, як другий буде пробігати множину A. Іншою мовою, для цього $c\in C$ визначається $g_c : A\to B$ правилом $g_c(a) = g(\langle c,a\rangle)$ для кожного $a\in A$.

Функція $\hat{g}$ визначається рівнянням $\hat{g}(c) = g_c$ для $c\in C$. Для вільної пари $\langle c,a\rangle \in C\times A$ справедливим є рівняння:

$$ev(\langle \hat{g}(c), a\rangle) = g_c(a) = g(\langle c,a\rangle). \qquad (7)$$

Вимога комутативності діаграми, яка наведена на рис. 11, тобто правильності рівняння (7) означає, що $\hat{g}(c)$ повинна бути функцією, яка для цього a дає $g(\langle c,a\rangle)$, тобто $\hat{g}(c)$ повинна співпадати з визначеної вище g_c.

Якщо множина A є підмножиною множини B, то функція включення $A\mapsto B$ ін'єктивна і тому мономорфна. З іншого боку, вільна мономорфна функція $f : C\mapsto B$ визначає підмножину множини B, при якій $\mathrm{Im}\, f = \{f(x) : x\in C\}$ (рис. 12). Тобто, f індуцирує бієкцію між C та $\mathrm{Im}\, f$. Далі отримуємо $C\cong \mathrm{Im}\, f$.

Таким чином, область визначення мономорфної функції ізоморфна деякій підмножині області значень цієї функції. Іншою мовою, область визначення є, з точністю до ізоморфізма, підмножиною області значень.

Підмножиною або підоб'єктом β-об'єкта d або підоб'єктом у d є мономорфна β-стрілка $f : a\mapsto d$ з кінцем d.

Якщо D — довільна множина, то множина усіх підмножин $\mathrm{P}(D)$ є *множиною-степеню* множини D.

Таким чином, $\mathrm{P}(D) = \{A : A \text{ підмножина множини } D\}$.

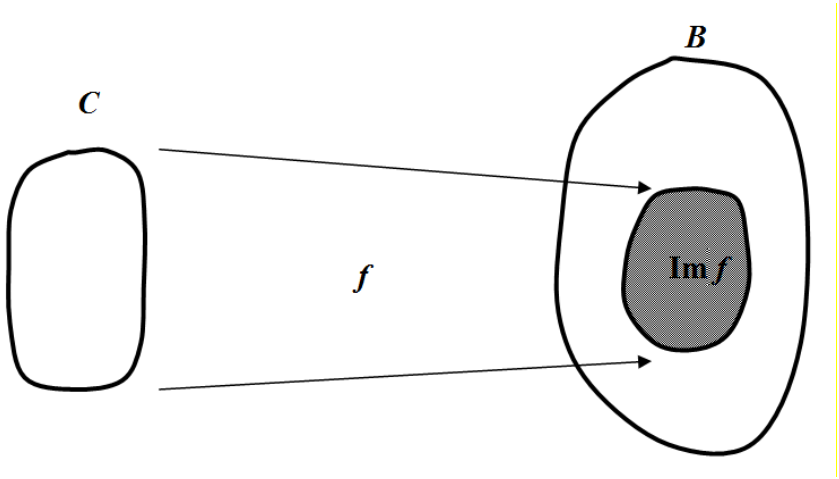


Рис. 12. Діаграма $f : C\mapsto B$, при якій $\mathrm{Im}\, f = \{f(x) : x\in C\}$

Відношення теоретико-множинного включення є частковим порядком на множині-степені $\mathrm{P}(D)$, тобто пара $(\mathrm{P}(D),\subseteq)$ утворює частково-упорядочену множину, яку можна уявляти як категорію, у якій стрілка $A \to B$ мається тільки тоді, коли $A \subseteq B$. При наявності стрілки $A \to B$ діаграма, яка надана на рис. 13(а), комутативна.

а **б**

Рис. 13. Комутативні діаграми: а – при $A \subseteq B$, $A \subseteq B, D$; б – при $f : a \mapsto d$, $g : b \mapsto d$, $h : a \to b$

Це підказує визначення відношення включення між підоб'єктами об'єкта *d*. Для заданих підоб'єктів $f : a \mapsto d$ і $g : b \mapsto d$ покладемо $f \subseteq g$ тоді і тільки тоді, коли існує β-стрілка $h : a \to b$, при якій діаграма, яка наведена на рис. 13(б), комутативна, тобто $f = g^{\circ}h$. Така стрілка *h* буде мономорфною, тобто буде підоб'єктом об'єкта *b*, що посилює аналогію з теоретико-множинним випадком. Таким чином, $f \subseteq g$ тоді і тільки тоді, коли *f* проходить через *g*.

Поняття включення на підоб'єктах підмножин можна розглядати наступним чином:

Відношення рефлективності при $f \subseteq f$, так як $f = f \circ 1_a$ (рис. 14).

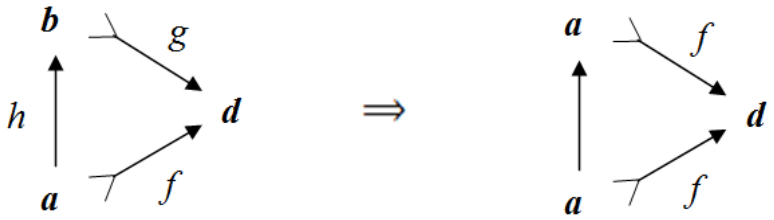


Рис. 14. Комутативні діаграми рефлективності

Відношення транзитивності: якщо $f \subseteq g$ і $g \subseteq f$, то $f \subseteq k$, так як з $f = g \circ h$ і $g = k \circ i$ виходить $f = k \circ (i \circ h)$ (рис. 15).

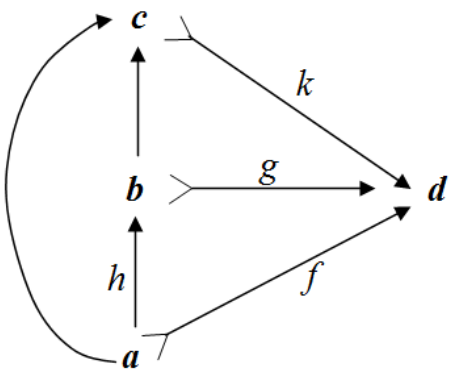


Рис. 15. Комутативна діаграма транзитивності

Якщо $f \subseteq g$ і $g \subseteq f$, то f і g пропускається друг через друга, як надано на рис. 16, то $f = g \circ h$, $g = f \circ i$.

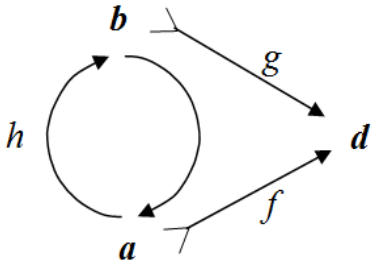


Рис. 16. Діаграма тотожності підмножин при $f \subseteq g$ і $g \subseteq f$

У цьому випадку $h : a \to b$ буде ізострілкою, а i — зворотною до неї. Таким чином, якщо $f \subseteq g$ і $g \subseteq f$, то стрілки f і g мають ізоморфні початки. Тому їх ще називають *ізоморфними підоб'єктами* ($f \cong g$). Відношення ізоморфності є відношенням еквівалентності. Кожна стрілка $f : a \mapsto d$ визначає клас еквівалентності:

$$[f] = \{g : f \cong g\}. \tag{8}$$

При цьому утворюється множина:

$$Sub(d) = \{[f] : f \text{ є 1 монострілкою і } cod\ f = d\}.$$

Тобто, елементи множини $Sub(d)$ є підоб'єктами. Тому підоб'єктами об'єкту d вважаються класи еквівалентності монострілок з кінцем у d.

Для визначення відношення включення на введених об'єктах, визначимо $[f] \subseteq [g] \Rightarrow f \subseteq g$.

Для визначення залежності класів еквівалентності від самих множин та підмножин розглянемо наступне твердження: якщо $[f]=[f']$ і $[g]=[g']$, то $f \subseteq g$, при $f' \subseteq g'$. Тобто відношення тотожності стійке відносно ізоморфності підоб'єктів.

Підоб'єкти об'єкту d утворюють частково упорядковану множину $(Sub(d),\subseteq)$. Дійсно, якщо $[f]\subseteq[g]$ і $[g]\subseteq[f]$, то $f \subseteq g$ і $g \subseteq f$, відповідно $f \cong g$, з чого витікає, що $[f]=[g]$.

В подальшому вираз $f \cong g$ буде використовуватися, коли вважається, що f і g є одним і тим же підоб'єктом, а вираз $f = g$ буде визначати, що f і g у дійсності є однією і тою ж стрілкою.

Висновки

Описуючи категорію підмножин, необхідно повернутися до поняття елементів множин. Елемент x множини $A(x \in A)$ можна ототожнити з одноелементною підмножиною $\{x\}$ множини A і, відповідно, зі стрілкою $\{x\}\mapsto A$ з кінцевого об'єкта $\{x\}$ у A. Зворотно функція $f:1\to A$ визначає у категорії **Set** елемент з A, а саме f-образ єдиного елементу кінцевого об'єкта 1. Якщо категорія β має кінцевий об'єкт 1, то елементом β-об'єкта a є будь-яка β-стрілка $x:1\to a$. При цьому $x:1\to a$ завжди буде моно стрілкою.

У подальшому виникає питання про властивості елементів у **Set.** Чи повинен будь-який об'єкт, який є не початковим, мати елементи? Чи можливо охарактеризувати мономорфні і епіморфні стрілки у термінах елементів їх початку і кінця? Усі ці питання необхідно розглядати у комплексі, розкриваючи імена стрілок та визначаючи класифікацію підоб'єктів, з метою подальшого розкриття питань взаємодії множин та підмножин загрозливих впливів на об'єкти та підоб'єкти множин механізмів захисту інформації [8].

Список літератури

1. Бірюков, В.О. Композиція і категорії функцій систем загроз в областях систем захисту інформації / В.О. Бірюков, І.М. Павлов // Захист інформації. – 2013. – № 1. – С. 28–37.
2. Павлов, І.М. Морфізм функцій і бієктивність об'єктів при проекції множин загроз та областей систем захисту інформації / І.М. Павлов // Сучасний захист інформації. — 2013. — № 1. — С. 36–45.
3. Павлов, І.М. Проектування комплексних систем захисту інформації [Текст] : підруч. для студ. вищ. навч. закл., які навчаються за галуззю знань «Інформаційна безпека» / І.М. Павлов, В.О. Хорошко ; Держ. служба спец. зв'язку та захисту інформації, Військ. ін-т телекомунікацій та інформатизації Нац. техн. ун-ту України «Київ. політехн. ін-т», Держ. ун-т інформ.-комунікац. технологій. — К. : ВІТІ : ДУІКТ, 2011. — 244 с.
4. Manes, E.G. Category Theory Applied to Computation and Control / E.G. Manes // Proceedings of the 1st International symposium, San Francisco, February 25–26, 1974. Edited by E.G. Manes. — Berlin : Springer-Verlag, 1975. — 245 p.
5. Попов, М.М. Аксіоматична теорія множин. Частина І: Система аксіом ZFC і вступ до теорії моделей / М.М. Попов ; Чернівецький національний університет імені Юрія Федьковича. — Чернівці, 2011. — 79 с.
6. Grayson, R. Heyting-valued models for intuitionistic set theory / R. Grayson // Lecture Notes in Mathematics. — 1979. — Vol. 753. — PP. 402–414.
7. Плоткин, Б.И. Универсальная алгебра, алгебраическая логика и базы данных : монография / Б.И. Плоткин. — М. : Наука, 1991. — 446 с.
8. Павлов, И.Н. Формальное описание процесса проектирования комплексных систем защиты информации в информационно-телекоммуникационных системах [Текст] / И.Н. Павлов, Г.Д. Радзивилов // Вісник ДУІКТ. — К. : 2010. — Т. 8, № 1. — С. 84–93.

АМАЛЬГАМЫ, ПОЛНОТА ДИАГРАММ И ПОДОБЪЕКТОВ МНОЖЕСТВ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

И.Н. Павлов

Национальный технический университет Украины «Киевский политехнический институт»,
просп. Победы, 37, Киев, 03056, Украина; e-mail: pavlov@ukr.net

В статье рассматриваются математические модели отношений множеств и подмножеств на основе анализа категорий логики с целью дальнейшего проведения анализа угроз на системы защиты информации. Приведено описание обратного образа, ядерных отношений и амальгам в множествах систем защиты информации.
Ключевые слова: амальгамы, множества, подмножества, объекты, подобъекты, функции, система защиты информации

AMALGAMS, COMPLETENESS OF DIAGRAMS AND SUB-OBJECTS OF SETS IN INFORMATION SECURITY SYSTEMS

Igor M. Pavlov

National Technical University of Ukraine «Kyiv Polytechnic Institute»,
37 Peremogy Ave., Kyiv, 03056, Ukraine; e-mail: pavlov@ukr.net

This paper focuses on mathematical models of the relationship between sets and subsets based on analysis of the logic categories for further analyze threatening impacts on information security systems. The description of the pullback, nuclear relations and amalgams in the sets of information security systems are given.
Keywords: amalgams, sets, subsets, objects, sub-objects, functions, information security system

УДК 621.372

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 61-68

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЭКРАНИРОВАННОГО РАСПРЕДЕЛЁННОГО ФИЛЬТРА

В.В. Козловский[1], **Р.М. Лысенко**[2]

[1] Государственный университет информационно-коммуникационных технологий,
ул. Соломенская, 7, Киев, 03680, Украина; e-mail: valerey@ukr.net
[2] Национальный технический университет Украины «Киевский политехнический институт»,
просп. Победы, 37, Киев, 03056, Украина

Разработана математическая модель экранированного распределённого фильтра низких частот на основе теории восьмиполюсников, проведено ее исследование при различных исходных данных. Даны рекомендации для моделирования процессов фильтрации.

Ключевые слова: фильтр низких частот, восьмиполюсник, экранированные линии передачи, амплитудно-частотная характеристика, каналы утечки информации

Введение

Для предотвращения утечки информации по цепям питания в настоящее время широко используются фильтры низких частот (ФНЧ) [1], которые рассчитываются методами теории линий передач без учёта влияния экрана, что приводит к ошибкам в реализации амплитудно-частотных характеристик фильтров. В работе [2] для построения ФНЧ предложено использовать более точную концептуальную модель фильтра, которая представляет собой соединение восьмиполюсников. Однако математический анализ данной модели отсутствует.

Целью статьи является разработка математической модели распределённого ФНЧ на основе теории восьмиполюсников и её исследование при различных исходных данных.

Основная часть

В целях определённости рассмотрим ФНЧ, составленный из однородных отрезков линий передачи. При этом различие в волновых сопротивлениях каждой секции фильтра достигается включением диэлектрических вставок с различными диэлектрическими проницаемостями.

Сопоставим ФНЧ на отрезках экранированных линий передачи восьмиполюсник рис. 1.

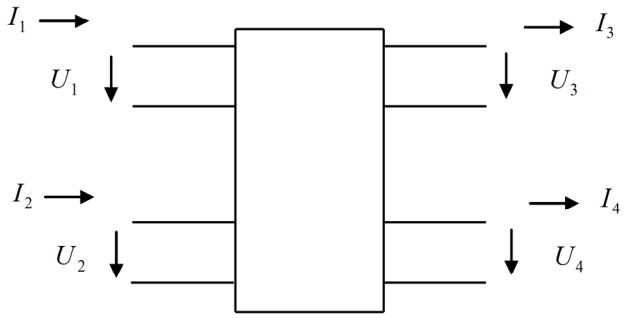


Рис. 1. Схема восьмиполюсника

Запишем уравнения восьмиполюсника через систему A- параметров:

$$\left.\begin{aligned} U_1 &= A_{11}U_3 + A_{12}U_4 + A_{13}I_3 + A_{14}I_4 \\ U_2 &= A_{21}U_3 + A_{22}U_4 + A_{23}I_3 + A_{24}I_4 \\ I_1 &= A_{31}U_3 + A_{32}U_4 + A_{33}I_3 + A_{34}I_4 \\ I_2 &= A_{41}U_3 + A_{42}U_4 + A_{43}I_3 + A_{44}I_4 \end{aligned}\right\} \qquad (1)$$

Составим математическую модель фильтра в предположении, что к плечам 3 и 4 подключены в общем случае комплексные сопротивления R_3, R_4 (рис. 2)

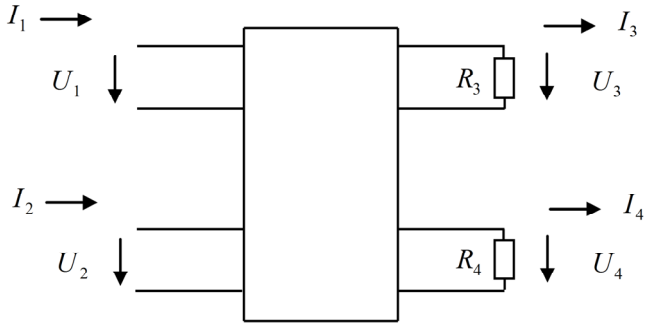


Рис. 2. Схема нагруженного восьмиполюсника

Выразим напряжения U_3, U_4 через напряжения возбуждения U_1, U_2. В этом случае граничные условия запишутся в виде

$$\begin{aligned} U_3 &= I_3R_3, \\ U_4 &= I_4R_4. \end{aligned} \qquad (2)$$

С учётом (2) из уравнений (1) имеем:

$$U_1 = A_{11}U_3 + A_{12}U_4 + A_{13}G_3U_3 + A_{14}G_4U_4 = (A_{11} + A_{13}G_3)U_3 + (A_{12} + A_{14}G_4)U_4,$$

$$U_2 = A_{21}U_3 + A_{22}U_4 + A_{23}G_3U_3 + A_{24}G_4U_4 = (A_{21} + A_{23}G_3)U_3 + (A_{22} + A_{24}G_4)U_4, \quad (3)$$

$$G_3 = \frac{1}{R_3}, \quad G_4 = \frac{1}{R_4}.$$

Из системы уравнений (3) находим

$$U_3 = \frac{b_{22}U_1 - b_{12}U_2}{\Delta},$$

$$U_4 = \frac{b_{11}U_2 - b_{21}U_1}{\Delta}, \quad (4)$$

где

$$b_{11} = A_{11} + A_{13}G_3,$$

$$b_{12} = A_{12} + A_{14}G_4,$$

$$b_{21} = A_{21} + A_{23}G_3, \quad (5)$$

$$b_{22} = A_{22} + A_{24}G_4,$$

$$\Delta = b_{11}b_{22} - b_{12}b_{21}.$$

Воспользовавшись соотношениями (4), составим математическую модель трёхсекционного экранированного ФНЧ (рис. 3), где $Z_{в1}, Z_{в2}, Z_{в3}$ — волновые сопротивления неэкранированных линий передачи, $\Theta_1, \Theta_2, \Theta_3$ — электрические длины секций. Считаем, что сопротивления нагрузок фильтра равны 50 м.

Для симметричного ФНЧ

$$Z_{в1} = Z_{в3}, \quad \Theta_1 = \Theta_3. \quad (6)$$

В этом случае цепная матрица передачи ФНЧ (рис. 3) равна произведению матриц передачи каждого звена:

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} =$$

$$= \begin{bmatrix} \cos\Theta_1 & jZ_{в1}\sin\Theta_1 \\ \frac{j}{Z_{в1}}\sin\Theta_1 & \cos\Theta_1 \end{bmatrix} \begin{bmatrix} \cos\Theta_2 & jZ_{в2}\sin\Theta_2 \\ \frac{j}{Z_{в2}}\sin\Theta_2 & \cos\Theta_2 \end{bmatrix} \begin{bmatrix} \cos\Theta_1 & jZ_{в1}\sin\Theta_1 \\ \frac{j}{Z_{в1}}\sin\Theta_1 & \cos\Theta_1 \end{bmatrix} \quad (7)$$

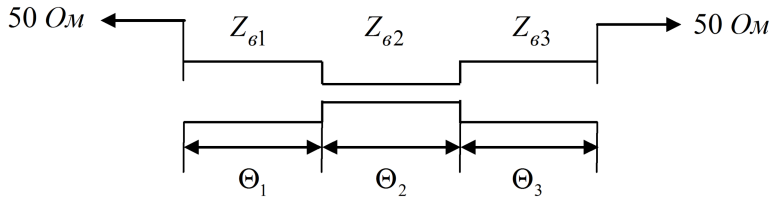


Рис. 3. Симметричный трёхступенчатый ФНЧ

Для симметричной цепи затухание определяется известной формулой [3]

$$L_A = 10\lg\left[1+\frac{1}{4}\left(\frac{A_{12}}{jR}-\frac{A_{21}R}{j}\right)^2\right],\ \partial Б. \qquad (8)$$

Обозначим $\Theta_1 = \Theta_3 = \Theta$, $\Theta_2 = m\Theta$. Из анализа зависимостей (рис. 4) следует, что наибольшая область заграждения наблюдается при $m = 1$ ($Z_{в1} = Z_{в3} = 11{,}6$ Ом, $Z_{в2} = 144$ Ом).

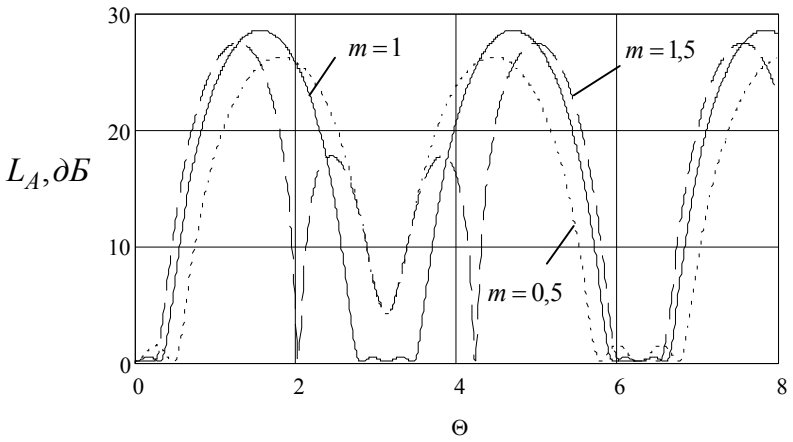


Рис. 4. Зависимость затухания ФНЧ рис. 3 от электрической длины

Рассмотрим влияние экрана на характеристики ФНЧ в предположении, что фильтр реализован на основе двухпроводной линии (рис. 5).

Исходные данные конструкции ФНЧ, рассчитанного на основе двухпроводной неэкранированной линии – $a = 3$ мм, $d = 0.5$ мм.

Волновое сопротивление $Z_{в1} = Z_{в3} = 11.6$ Ом реализуется включением диэлектрической шайбы с относительной диэлектрической проницаемостью $\varepsilon_{r1} = 656$. Волновому сопротивлению $Z_{в2} = 144$ Ом соответствует диэлектрическая шайба с $\varepsilon_{r2} = 4.26$.

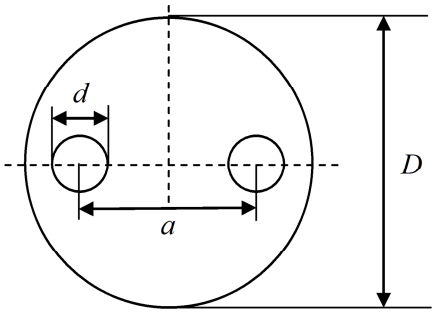


Рис. 5. Двухпроводная экранированная симметричная линия проводников

При наличии круглого экрана (рис. 5) диаметром $D = 6$ мм волновые сопротивления экранированной линии составляют:

- при нечётном возбуждении

$$Z_{oo1} = Z_{oo3} = 9.228 \text{ Ом}, \quad Z_{oo2} = 114.512 \text{ Ом};$$

- при чётном возбуждении

$$Z_{oe1} = Z_{oe3} = 14.217 \text{ Ом}, \quad Z_{oe2} = 176.421 \text{ Ом}.$$

В этом случае восьмиполюсная модель (схема) ФНЧ приобретает вид представленный на рис. 6.

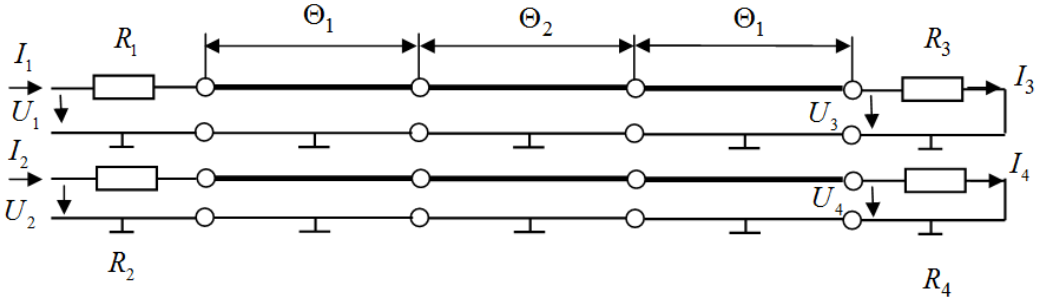


Рис. 6. Схема трёхступенчатого ФНЧ на связанных линиях

Амплитудно-частотную характеристику (АЧХ) будем оценивать отношением мощностей, поглощаемых нагрузками R_3, R_4, к мощности источников возбуждения. В соответствии со схемой рис. 6 матрица A восьмиполюсника, расположенного левее сопротивлений R_3, R_4, равна

$$A_\Sigma = A_R A_1 A_2 A_1, \tag{9}$$

где A_R — A-матрица восьмиполюсника, состоящего из внутренних сопротивлений R_1, R_2 источников возбуждения [2]; A_1, A_2 — A-матрицы связанных линий, имеющих электрические длины Θ_1, Θ_2 соответственно (рис. 6).

Таким образом, для схемы рис. 6 напряжения на нагрузках описываются формулами (4), (5), где под элементами матрицы A_{ij} понимаются элементы матрицы A_Σ (9). По напряжениям U_1, U_2, U_3, U_4 из (1) и (2) находим токи I_1, I_2, I_3, I_4.

Мощности источников возбуждения:

$$P_{e1} = \mathrm{Re}\left(U_1 \overset{*}{I}_1 \right), \qquad P_{e2} = \mathrm{Re}\left(U_2 \overset{*}{I}_2 \right). \tag{10}$$

Мощности, поглощаемые нагрузками R_3, R_4:

$$P_{R_3} = \mathrm{Re}\left(U_3 \overset{*}{I}_3 \right), \qquad P_{R_4} = \mathrm{Re}\left(U_4 \overset{*}{I}_4 \right). \tag{11}$$

Фильтрующие свойства фильтра будем оценивать коэффициентом передачи по мощности K, равным отношению мощности нагрузок к мощности источников или затуханием L

$$K = \frac{P_{R_3} + P_{R_4}}{P_{e1} + P_{e2}}, \quad L, \quad \text{дБ} = 10 \lg \frac{1}{K}. \tag{12}$$

На рис. 7 показаны характеристики ФНЧ на связанных линиях, рассчитанные при следующих исходных данных: все нагрузки (рис. 6) равны 50 Ом, электрические длины всех секций равны между собой $x = \omega t = \Theta_1 = \Theta_2 = \Theta_3$, где t — время задержки одной секции связанных линий, напряжения $U_1 = 1B$, $U_2 = U_1 e^{j\varphi}$. Проведенный анализ показал, что изменение диаметра внешнего проводника D, а также фазового сдвига φ от 0 до 2π слабо влияет на характеристики ФНЧ (рис. 7).

Из анализа зависимостей рис. 7 следует, что при $\omega t = k\pi, k = 1,2,...$ ФНЧ имеет паразитные (нерабочие) полосы пропускания, которые образуют несанкционированные каналы утечки информации. Просчёт характеристик ФНЧ при различных конструктивных параметров линий показал, что протяжённость областей заграждения при всех номерах k одинакова и является максимальной при равенстве электрических длин секций фильтра. При различных электрических длинах секций степень изрезанности затухания фильтра возрастает и при этом возрастает количество паразитных полос пропускания, то есть возрастает количество частотных каналов утечки информации. Общая картина получается аналогичной рис. 4.

Если нагрузки ФНЧ (рис. 6) различны или являются комплексными, то АЧХ фильтра с учётом экрана и без него сильно отличаются друг от друга. В этом случае при синтезе ФНЧ следует обязательно учитывать влияние экрана.

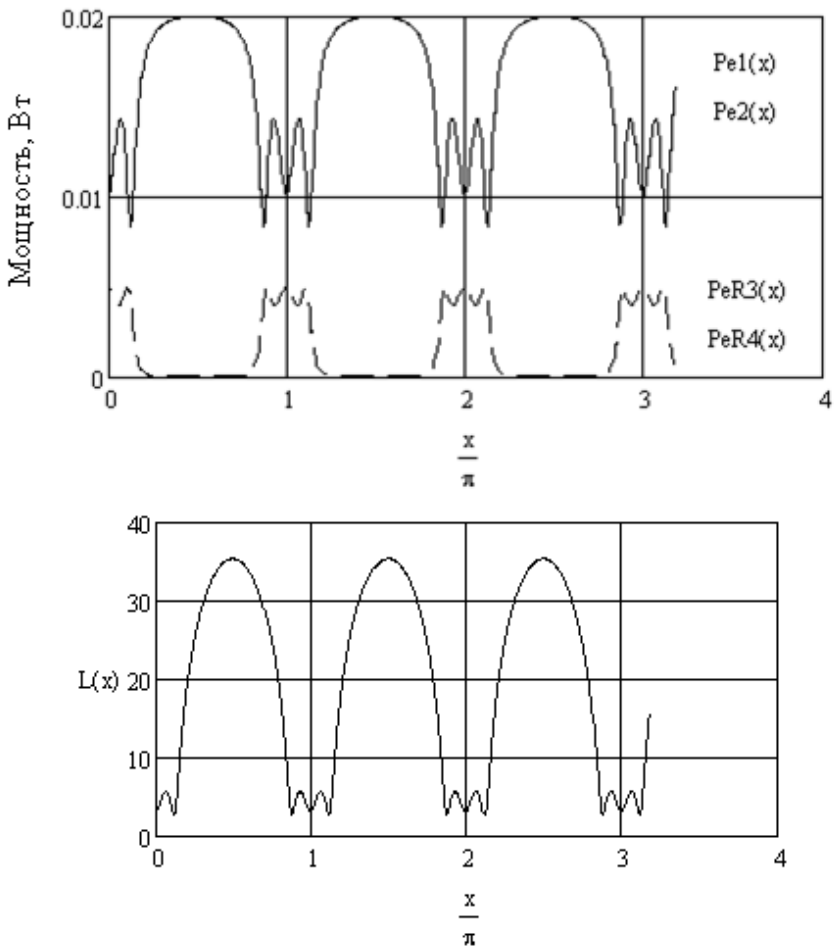


Рис. 7. Характеристики трёхступенчатого ФНЧ на связанных линиях

Выводы

Разработана математическая модель фильтров низких частот, позволяющая учитывать влияние экранирования на процесс фильтрации. Эквивалентная схема модели представляет собой каскадное соединение восьмиполюсников, в общем случае нагруженных на четыре различные комплексные нагрузки.

При моделировании процессов фильтрации, происходящих в реальных системах, следует иметь в виду, что

- внутренние сопротивления источников возбуждения должны быть одинаковыми (или мало отличаться друг от друга), когда расстояние между источниками значительно меньше длины возбуждающей волны;
- если расстояние между источниками соизмеримо с длиной волны, то комплексные сопротивления источников могут сильно отличаться друг от друга. Такая ситуация может возникнуть в сверхскоростных системах передачи информации, в которых геометрия устройства соизмерима с длиной информационной волны.

Очевидно, что всё сказанное справедливо и для сопротивлений нагрузок ФНЧ.

Список литературы

1. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. — К. : ЮНИОР, 2003. — 505 с.
2. Козловский, В.В. Концептуальная модель СВЧ канала утечки информации по цепи питания / В.В. Козловский, Р.М. Лысенко // Сучасний захист інформації. — 2013. — № 1. — С. 12–18.
3. Маттей, Д.Л. Фильтры СВЧ, согласующие цепи и цепи связи [Текст] : в 2-х т. : пер. с англ. / Д.Л. Маттей, Л. Янг, Е.М.Т. Джонс ; ред.: Л.В. Алексеев, Ф.В. Кушнир. — М. : Связь, 1971–1972.
Т. 1. — 1971. — 493 с.

МАТЕМАТИЧНА МОДЕЛЬ ЕКРАНОВАНОГО РОЗПОДІЛЕНОГО ФІЛЬТРА

В.В. Козловський[1], Р.М. Лисенко[2]

[1] Державний університет інформаційно-комунікаційних технологій,
вул. Солом'янська, 7, Київ, 03680, Україна; e-mail: valerey@ukr.net
[2] Національний технічний університет України «Київський політехнічний інститут»,
просп. Перемоги, 37, Київ, 03056, Україна

Розроблено математичну модель екранованого розподіленого фільтра низьких частот на основі теорії восьмиполюсників, проведено її дослідження при різних вхідних даних. Дано рекомендації для моделювання процесів фільтрації.
Ключові слова: фільтр низьких частот, восьмиполюсник, екрановані лінії передачі, амплітудно-частотна характеристика, канали витоку інформації

MATHEMATICAL MODEL OF SHIELDED DISTRIBUTED FILTER

Valery V. Kozlovsky[1], Roman M. Lysenko[2]

[1] State University of Information and Communication Technologies,
7 Solomenskaya str., Kyiv, 03680, Ukraine; e-mail: valerey@ukr.net
[2] National Technical University of Ukraine «Kyiv Polytechnic Institute»,
37 Peremogy Ave., Kyiv, 03056, Ukraine

This paper focuses on development of mathematical model for shielded distributed low-pass filter based on eight-terminal circuit theory. The proposed model is assessed using different initial data. Recommendations for the simulation of filtration are given.
Keywords: low-pass filter, eight-terminal circuit, shielded transmission line, amplitude and frequency characteristics, information leakage channels

УДК 004.281:681.3

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 69-74

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ СИСТЕМ ЗАХИСТУ В МЕРЕЖАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

В.О. Хорошко, Ю.Є. Хохлачова

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

У даній статті розглянуто положення, які дозволяють сформулювати чи отримати ряд надзвичайно важливих для вирішення задачі захисту інформаційних ресурсів систем спеціального призначення умов, обмежень та оптимальних значень найбільш загальних параметрів системи захисту.

Ключові слова: захист інформації, системи захисту, мережі передачі інформації, захист інформаційних ресурсів

Вступ

Інформаційна безпека, поряд із економічною, військовою та іншими, займає одне з найважливіших місць у національній безпеці будь-якої держави. Забезпечення такої безпеки – складна наукомістка і багатогранна проблема.

Водночас необхідно чітко бачити протиріччя, що пов'язані з впровадженням інформаційних технологій взагалі і, зокрема, в системах спеціального призначення (ССП). З одного боку, автоматизація процесів збору, передачі, оброблення, збереження і відображення інформації істотно підвищує можливості органів керування, а з іншого боку – призводить до зростання залежності керування від надійності функціонування засобів автоматизації і надійності захисту інформації від несанкціонованого доступу і завад [1].

Тому величина шкоди ССП може бути визначеною у вигляді:

$$M\theta_2 = \sum_{i=1}^{i=n} p_{ві} \Delta T_{ki} C_i \,, \tag{1}$$

де

C_i — шкода за рахунок простою відповідних ресурсів ССП під час контролю в умовних одиницях в одиницю часу,

ΔT_{ki} — тривалість *i*-того виду контролю,

$p_{ві}$ — ймовірність виявлення і подальшої протидії загрозі *i*-го типу.

З урахуванням цього можна записати:

$$M\theta = M\theta_1 + M\theta_2 = \sum_{i=1}^{i=n} \left[G_i \left(T_{ki} - \Delta T_{ki} \right) \left(1 - p_{ві} \right) + p_{ві} C_i \Delta T_{ki} \right], \tag{2}$$

де $M\theta_1$ — максимальна величина можливої загальної шкоди.

Аналіз цього виразу дозволяє зробити висновок про те, що він може бути прийнятим як цільова функція системи технічного захисту інформації (ТЗІ).

У разі виявлення в процесі контролю факту порушення цілісності, здійснюється її поновлення із застосуванням резервних копій відповідної інформації. Характеристиками процесу поновлення є тривалість власне поновлення ($\Delta t_{пі}$) та ймовірність виникнення його необхідності; $p_{ві}$ — ймовірність виявлення порушення цілісності. Тоді математичне сподівання тривалості поновлення дорівнює:

$$\Delta t_{пі} p_{ві} + O(1 - p_{ві}) = \Delta t_{пі} p_{ві}.$$

Тобто тривалість усього процесу контролю та поновлення є винятковою величиною і визначається тривалістю власне процесу контролю $\Delta t_{кі}$, та тривалістю поновлення $\Delta t_{пі}$ з ймовірністю $p_{ві}$. Середнє значення величини $\Delta T_{кі}$, його математичне сподівання можна визначити як:

$$\Delta T_{кі} = \Delta t_{кі} + \Delta t_{пі} p_{ві}. \qquad (3)$$

Основна частина

Цільова функція (1), окрім умов доцільності застосування системи ТЗІ від загроз того чи іншого типу, дає змогу здійснити спробу знаходження оптимальних параметрів системи захисту – характеристик системи ТЗІ, наприклад, в сенсі максимуму шкоди, яка запобігається завдяки застосуванню системи захисту [2]. Зрозуміло, що величина цільової функції залежить від параметрів, які не є залежними від характеристик системи ТЗІ, але впливають на них, та і від параметрів, які не є залежними від помережної реалізації системи ТЗІ – їх характеристик. Деякі з них можуть бути параметрами управління, тобто тими параметрами, які можуть змінюватися залежно від умов застосування системи ТЗІ. Ці параметри залежать від типу загроз.

На інформаційні ресурси ССП, а також технічні засоби захисту цієї системи впливають виходи за межі допустимих значень температури, вологості, радіаційного чи електромагнітного випромінювання.

Стійкість ССП до загроз визначається її надійністю, що забезпечується відповідними заходами, які включають засоби контролю та поновлення цілісності системи. Значної уваги для забезпечення стійкості ССП приділяється протидії випадковим або зловмисним спробам несанкціонованого доступу (НСД), або штучним загрозам, під якими розуміються заборонені дії користувачів, по відношенню до ресурсів ССП [3].

Спроби НСД можуть вплинути на ССП лише після подолання засобів управління доступом та відповідних засобів забезпечення тієї чи іншої функціональної послуги.

Таким чином, інформаційні ресурси ССП потребують захисту від спроб НСД, а також безпосередніх впливів.

Припустимо, що потоки кожного з типів загроз є найпростішими з інтенсивностями $\gamma_{зі}$, тоді ця інтенсивність дорівнює сумі інтенсивностей загроз штучних $\gamma_{ші}$ та природних γ_i, так що:

$$\gamma_{зі} = \gamma_{ші} + \gamma_i.$$

Звернемо увагу на те, що під величиною γ_i, на наш погляд, слід розглядати ту частину потоків відмов ССП з загальною інтенсивністю γ, яка створює лише загрози *i*-го типу, так що:

$$\gamma = \sum_{i=1}^{i=n} \gamma_i \ .$$

Слід враховувати те, що $p_{ві}$ — ймовірність виявлення і подальшої протидії загрози *i*-го типу є ймовірністю складної події, яка полягає в тому, що система ТЗІ запобігає (не допускає) впливу цієї загрози, чи встановила факт її впливу і ліквідувала відповідні наслідки.

Для вирішення першої задачі використовується система управління (обмеження) доступом до інформаційних ресурсів ССП, що забезпечується адміністратором безпеки. Стійкість (в розумінні імовірності неподолання) p_{gi} системи управління доступом визначається стійкістю процесів ідентифікації та автентифікації адміністратора, як користувача з найширшими повноваженнями [Same]. Останнє визначається можливостями системи ідентифікації та кількістю можливих варіантів паролів і надійністю їх конфіденційного збереження.

Оскільки штучні загрози можуть впливати тільки в разі їх не виявлення засобами управління доступом, то інтенсивність цих загроз, які впливають на засоби забезпечення відповідної функціональної послуги ССП, зменшується до

$$\gamma_{ші}\left(1 - p_{gi}\right).$$

Друга задача (установки факту впливу загрози і ліквідації відповідних наслідків) вирішується шляхом перевірки цілісності та доступності інформації і її поновлення, в разі виявлення такого порушення. Тому з урахуванням застосування відповідних засобів захисту – засобів забезпечення відповідної функціональної послуги ССП результуюча інтенсивність загроз γ_{pi} може бути розрахованою як:

$$\gamma_{pi} = \left[\gamma_{ші}\left(1 - p_{gi}\right) + \gamma_i\right]\left(1 - p_{ві}\right), \tag{4}$$

де $p_{ві}$ — ймовірність виявлення (усунення) засобами забезпечення відповідно функціонально послуги ССП загрози відповідного типу.

Будемо вважати закон розподілу ймовірностей впливу на ресурси пуассонівським [4]. Тоді ймовірність впливу на *i*-ий ресурс хоча б однієї загрози відповідного типу $p_{зі}$ на інтервалі $\left(T_{ki} - \Delta T_{ki}\right)$ при умові застосування системи ТЗІ, тобто коли система захисту не виявила і, зрозуміло, не протидіяла цій загрозі, дорівнює:

$$p_{зі} = 1 - p_{oi} = 1 - \exp\left\{-\left(T_{ki} - \Delta T_{ki}\right)\left[\left(\gamma_{mi}\left(1 - p_{gi}\right) + \gamma_i\right)\left(1 - p_{ві}\right)\right]\right\},$$

де p_{oi} — ймовірність відсутності впливів, або наявність рівня нуля впливів.

Якщо підставити (3) в (1) з урахуванням (2), то величину шкоди можна записати у вигляді:

$$\begin{aligned} M\theta_i = {} & G_i\left(T_{ki} - \Delta T_{ki}\right)\left[1 - \exp\left\{-\left(T_{ki} - \Delta T_{ki}\right)\left[\left(\gamma_{mi}\left(1 - p_{gi}\right) + \gamma_i\right)\left(1 - p_{ві}\right)\right]\right\}\right] + \\ & + C_i \Delta T_{ki} \exp\left\{-\left(T_{ki} - \Delta T_{ki}\right)\left[\left(\gamma_{ші}\left(1 - p_{gi}\right) + \gamma_i\right)\left(1 - p_{ві}\right)\right]\right\}, \end{aligned} \tag{5}$$

Як слідує з останнього виразу, величина шкоди є функцією достатньо великого числа змінних. Серед цих змінних величини $G_i, C_i, \gamma_{ші}$ та γ_i є незалежними не тільки

від дій адміністратора безпеки, але і від характеристик підсистеми захисту ССП в цілому, тобто принципово не можуть розглядатися як параметри управління. Величини p_{oi}, $p_{вi}$ та ΔT_{ki} є залежними від якості розроблених та застосованих засобів управління доступом та засобів забезпечення відповідної функціональної послуги ССП і не можуть бути зміненими оперативно, але під час розробки системи ТЗІ їх значення принципово можна змінювати, тому ці параметри слід розглядати як параметри неоперативного управління. Після цих зауважень стає зрозумілим, що параметром оперативного управління слід вважати лише величину періоду контролю T_{ki}.

Слід показати, що ця функція має мінімум в точці:

$$T_{ki} = \Delta T_{ki} + d\,, \tag{6}$$

де величина ΔT визначається відповідно [3],

$$d = \frac{1}{z} + 0.5\sqrt{s}\,,$$

$$s = \Delta T_{ki}^2\left(1 + \frac{4C_i}{G_i}\right) + 4\left(\frac{1}{z^2} + \frac{C_i \Delta T_{ki}}{G_i z}\right),$$

а величина

$$z = \left\{\left[\gamma_{ші}\left(1 - p_{gi}\right) + \gamma_i\right]\left(1 - p_{вi}\right)\right\}$$

є не що інше, як результуюча інтенсивність загроз ($z = \gamma_{pi}$).

Отриманий результат має чітке і зрозуміле тлумачення [5]. Величина шкоди при зміні періоду контролю T_{ki} є мінімальною при такому його значенні, яке перевищує середнє значення його тривалості ΔT_{ki} на величину d яка, в свою чергу, визначається інтенсивністю потоку загроз, величинами шкод G_i та C_i характеристиками системи ТЗІ.

Вираз для розрахунку мінімального значення шкоди при цьому має вигляд:

$$\min M\theta_1 = G_i d\left[1 - \exp\left(-dz\right)\right] + C_i \Delta T_{ki} \exp\left(-dz\right),$$

з якого її легко розрахувати при відомих значеннях.

Цікавим є результат пошуку оптимального значення тривалості контролю ΔT_{ki}.

Неважко показати, що точка:

$$\Delta T_{ki} = \frac{\left[\left(2G_i T_{ki} z + \left(C_i - C_i T_{ki} z\right)\right)\right]}{\left[z_z\left(G_i - C_i\right)\right]} = \Delta T_{ki0\,pt}$$

є точкою максимуму шкоди. При цьому оптимальне значення тривалості контролю перевищує значення тривалості його періоду $\Delta T_{ki0\,pt} > T_{ki}$. Таке значення тривалості контролю є неможливим, але цей факт дозволяє зробити наступний, важливий для практики висновок: на інтервалі від $\Delta T_{ki} = 0$ до $\Delta T_{ki} = \Delta T_{ki0\,pt}$ значення шкоди із збільшенням ΔT_{ki} зростає, або чим меншим є значення тривалості контролю ΔT_{ki} тим меншим є значення шкоди у вигляді (3). Іншими словами, при побудові, проектуванні

чи виборі засобів ТЗІ перевагу слід віддавати таким засобам, які мають найменший час виконання операцій контролю.

Пошук екстремуму цільової функції (4) по результуючій інтенсивності загроз z призводить до висновку, що при надійних (високоефективних) системах управління доступом та виявлення і усунення загроз, коли на інтервал роботи ССП довжиною $(T_{ki} - \Delta T_{ki})$ попадає менше ніж один вплив, який є пропущений системою управління доступом і не виявленим та не усуненим системою контролю, тобто при виразі:

$$(T_{ki} - \Delta T_{ki})\left[\gamma_{ші}(1 - p_{gi}) + \gamma_i\right](1 - p_{ві}) < 1 \qquad (7)$$

величина шкоди є залежною лише від параметрів T_{ki} та ΔT_{ki} і має екстремуми в точках, які є близькими до

$$\Delta T_{ki0\,pt} = T_{ki}, \qquad \Delta T_{ki0\,pt} = T_{ki} / C .$$

Останній результат лише підтверджує вже отримані висновки і, при цьому його цінність полягає хіба що в підтвердженні адекватності моделі реальним процесам, пов'язаним з ТЗІ.

Якщо розглядати вираз (7) як таке обмеження при (4), що при певних умовах [4] перетворюється на окрему цільову функцію, тоді отримаємо важливі для практики вимоги щодо допустимих значень:

1) Тривалості періоду контролю (з урахуванням раніше отриманого результату щодо величини ΔT_{ki} (T_{ki}):

$$T_{ki} < \frac{1}{\left(\gamma_{mi}(1 - p_{gi}) + \gamma_i\right)(1 - p_{ві})}. \qquad (8)$$

2) Або щодо результуючої інтенсивності впливів загроз

$$\left[\gamma_{ші}(1 - p_{gi}) + \gamma_i\right](1 - p_{ві}) < \frac{1}{T_{ki}}. \qquad (9)$$

Умова (8) дозволяє визначити вимоги щодо тривалості періоду контролю T_{ki} при відомих інтенсивностях загроз γ_i, $\gamma_{ші}$ та реалізованих в системі ТЗІ ймовірностях p_{gi} та $p_{ві}$.

В свою чергу, умова (9) при заданій тривалості періоду контролю T_{ki} дозволяє визначити вимоги щодо таких параметрів системи ТЗІ як ймовірності p_{gi} та $p_{ві}$ при відомих інтенсивностях загроз γ_i, $\gamma_{ші}$.

З виразу (4) можна отримати значення екстремумів цієї ж функції і по будь-яким іншим параметрам неоперативного управління.

Висновки

Таким чином, розглянуті положення, які дозволяють сформулювати чи отримати цілу низку надзвичайно важливих для вирішення задачі захисту інформаційних ресурсів ССП: умов, обмежень та оптимальних значень найбільш загальних параметрів системи захисту, але не дають змоги сформулювати більш конкретні вимоги щодо складу та параметрів системи захисту чи її складових.

Список літератури

1. Основи надійності інформаційних систем [Текст] : підручник / С.М. Головань [та ін.]. — Луганськ : Ноулідж, 2012. — 334 с.
2. ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт [Текст] = Техническая защита информации. Порядок проведения работ : стандарт. — Введ. с 1997-07-01. — К. : Держстандарт України, 1997. — 27 с.
3. Василенко, В.С. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах *[Електронний ресурс]* / В.С. Василенко, О.С. Бордюк, С.М. Полонський. — Режим доступу: http://www.rusnauka.com/11_EISN_2010/Informatica/64068.doc.htm (Дата звернення 14.03.2013 р.)
4. Справочник по вероятностным расчетам [Текст] / Г.Г. Абезгауз [и др.]. — 2-е изд., испр. и доп. — М. : Воениздат, 1970. — 536 с.
5. Відновлення та оптимізація інформації в системах прийняття рішень [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напрямом «Інформаційна безпека» / В.Л. Баранов [та ін.] ; Державний ун-т інформаційно-комунікаційних технологій. — К. : ДУІКТ, 2009. — 132 с.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ СИСТЕМ ЗАЩИТЫ В СЕТЯХ ПЕРЕДАЧИ ИНФОРМАЦИИ

В.А. Хорошко, Ю.Е. Хохлачева

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

В данной статье рассмотрены положения, позволяющие сформулировать или получить ряд важнейших для решения задачи защиты информационных ресурсов систем специального назначения: условий, ограничений и оптимальных значений наиболее общих параметров системы защиты.

Ключевые слова: защита информации, системы защиты, сети передачи информации, защите информационных ресурсов

OPTIMIZATION OF PARAMETERS FOR DEFENCE SYSTEMS IN DATA TRANSMISSION NETWORK

Vladimir O. Khoroshko, Yulia E. Khokhlachova

National Aviation University,
1 Kosmonavta Komarova Ave., Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

This article discusses provisions that allow to formulate or to get a number of extremely important conditions, constraints, and the optimal values of the most common parameters of protection for solving the problem of protecting information resources in special use systems.

Keywords: information security, security systems, data transmission network, protection of information resources

УДК 355.40

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 75-81

МОДЕЛЬ ЛІНГВІСТИЧНОЇ БАЗИ ДАНИХ В СИСТЕМАХ АВТОМАТИЧНОЇ ОБРОБКИ ПРИРОДНОМОВНОЇ ТЕКСТОВОЇ ІНФОРМАЦІЇ

І.В. Замаруєва, В.Б. Толубко, Л.О. Литвиненко, О.Ю. Ніколаєвський

Військовий інститут Київського національного університету імені Тараса Шевченка,
просп. Глушкова, 2, корпус 8, Київ, 03680, Україна

У статті запропоновано модель лінгвістичної бази даних як складової лінгвістичного забезпечення систем автоматичної обробки природномовної текстової інформації. Відмінність запропонованої моделі полягає у відокремленні знань про мову від знань про світ (предметну область). Розроблена модель лінгвістичної бази даних у порівнянні з іншими має значно менший обсяг словників, формат представлення даних дозволяє моделювати закономірності як флективних мов, так й аналітичних, здатна забезпечувати обробку природномовного тексту для різних прикладних задач.

Ключові слова: лінгвістична база даних, лінгвістичне забезпечення, системи автоматичної обробки текстової інформації, мовна система, семіотична система

Вступ

Лінгвістичне забезпечення є невід'ємною складовою систем автоматичної обробки природномовної текстової інформації (ПМТІ). До таких систем сьогодні відносять системи машинного перекладу, інформаційно-пошукові системи, системи автоматичного індексування й класифікації ПМТІ, автоматичного реферування тощо. Ядром лінгвістичного забезпечення є лінгвістична база даних (ЛБД), яка складається із різноманітних словників заданого формату і забезпечує задачі автоматичної обробки ПМТІ.

Досвід побудови ЛБД свідчить, що визначення форматів словникових статей є окремою дослідницькою задачею, оскільки від повноти урахування лексико-граматичних характеристик в кінцевому рахунку залежить якість автоматичної обробки ПМТІ. Аналіз підходів до побудови ЛБД [1–4] показав, що вони орієнтовані здебільшого як на вузьку предметну область, так і на обмежену кількість задач автоматичної обробки (наприклад, автоматична класифікація ПМТІ, машинний переклад). Недоліком такого підходу є те, що розроблені словникові бази не можуть бути замінними як між собою, так і використовуватися в інших задачах обробки ПМТІ, які на сьогодні виникають (наприклад, в інформаційно-аналітичних системах з обробки ПМТІ). В той же час ЛБД моделює закономірності мовної системи, які не залежать від предметної області та розв'язуваних задач автоматичної обробки ПМТІ.

Мета статті і постановка задачі дослідження

Метою статті є розробка моделі ЛБД, яка б задовольняла вимогам незалежності від предметної області, мови представлення тексту, розв'язуваної задачі автоматичної обробки тексту.

При постановці задачі дослідження автори виходили з таких міркувань: архітектура ЛБД визначається об'єктом моделювання і задачами щодо його автоматичного опрацювання.

Об'єктом моделювання є природномовний текст. При цьому текст розглядається як об'єкт різних рівнів опрацювання: як знакова система (тобто правила графемного оформлення тексту), як лінгвістична система (тобто знання про мову, якою представлений текст) і як система знань про світ (предметну область). Кожний рівень має свої особливості, свої засоби виразу і, отже, припускає наявність специфічних методів обробки. Універсальними задачами опрацювання тексту є аналіз, прагматична інтерпретація й синтез.

Автори розрізняють лінгвістичну базу даних, яка представляє формальний запис знань про вхідну мову, та інформаційну базу даних (ІБД), яка представляє формальний запис знань про світ (прикладну область). До останньої можна віднести, наприклад, електронні перекладні словники в системах машинного перекладу, тезауруси в інформаційно-пошукових системах тощо.

Лінгвістична база даних представляється четвіркою:

$$LBD =: \langle G, Lm, Lsyn, Lsam \rangle,$$

де

G – словники для аналізу й синтезу графемної структури тексту;

Lm – словники для аналізу й синтезу морфологічного рівня мовної системи;

$Lsyn$ – словники для аналізу й синтезу синтаксичного рівня мовної системи;

$Lsam$ – словники для аналізу й синтезу семантичного рівня мовної системи.

До словників висуваються наступні вимоги: формат представлення граматичної інформації кожного рівня представлення словників є входом для аналізу наступного рівня, аналітичні словники будуються із урахуванням потреб синтетичних словників. Ми не розглядаємо задачу прагматичної інтерпретації, оскільки коректність цієї задачі залежить від ІБД.

Запропонована модель експериментально досліджена на текстах, представлених російською, українською та англійською мовами. Для кожної вхідної мови будується окрема ЛБД, але формати представлення даних є уніфікованими, що дозволяє їх реалізацію у багатомовних системах машинного перекладу, оскільки в ЛБД представлена як аналітична, так і синтетична складова. Далі розглянемо детальніше структуру і зміст словників кожного рівня.

Виклад основного матеріалу дослідження

Структура і зміст словників, що забезпечують автоматичний аналіз вхідного тексту на знаковому рівні його представлення. Кінцевою метою розпізнавання на графемному рівні представлення тексту є побудова графемної структури тексту, яка включає виділення на множині рядків і графем вхідного тексту таких семантично самостійних одиниць тексту: фрагментів (дискурсів), речень, синтагм, лексем; визначення типів (класів) перелічених одиниць тексту та встановлення відношень між ними в певному вхідному тексті [5].

В основу класифікатора графем покладені такі ознаки: тип знаку (цифра, буква, синтаксичний знак, службовий знак тощо), належність до алфавіту (латиниця, кирилиця, виключно російська, виключно українська), розмір літер (прописна, заголовна), фонетичні ознаки (голосна, приголосна). Аналітичний словник цього знакового рівня представлення тексту задає правила утворення лексем. Правила утворення лексем для російської мови представлені в таблиці 1.

Таблиця 1.

Правила утворення лексем для російської мови

Код класу	Найменування лексеми	Опис правила	Приклад
L01	Слово з малої літери	([а-я]+)	танк
L02	З великої літери	([А-Я][а-я]*)	Михаил
L03	Іншомовне слово	[a-zA-Z]+	tomahawk
L04	Неповна лексема	([а-я]+)-	полу-
L05	Слово через дефіс	([а-я]+)-([а-я]+)	полу-автоматический
L06	Слово з латинської літери	[A-Z]-([а-я]+)	U-образный
L08	Неповне позначення	-[0-9]+[A-Z]+	-104G
L09	Ціле число	[0-9]+	1945
L07	Позначення	([0-9А-Яа-я]+[-./]+[0-9А-Яа-я]+)|([0-9A-Za-z]+[-./]+[0-9A-Za-z]+)	МиГ-27; F.82
L10	Дробове число	[0-9]+[,.][0-9]+	143.7
L11	Дата	[0-9]+[-./][0-9]+[-./][0-9]+	03.07.1993
L12	Числов. прикметник	[0-9]+-[а-я]+	5-и
L13		"	"
L14	Скорочення	[цкнгшщхфпрлджчсмтб]+[.]	г.
L15	Скорочене ім’я	[А-Я] [цкнгшщзхфвпрлджчсмтб] + [.]| [А-Я] [.]	Дж.
L20	Спец. символ	[№@#$%^&*]	#
L21	Абревіатура	[А-Я]{2,}	США
L23	Повне ім’я	L15+ L02	Дж. Буш
L25	Складне скорочення	[цкнгшщзхфвпрлджчсмтб]+/[цкнгшщзхфвпрлджчсмтб]+	м/с
L30		([А-Я][а-я]*)-([А-Я][а-я]*)	Гаусса-Остроградского
L31		([А-Я][а-я]*)-([а-я]+)	
L32	Електронне посилання	((http|ftp)\:\/\/[a-z0-9./-]+)	http://univ.kiev.ua
L33	Електронна адреса	^(\w+([_.]{1}\w+)*@\w+([_.]{1}\w+)*\.[A-Za-z]{2,3}[;]?)*$	info@univ.kiev.ua

Синтетичний словник знакового рівня задає правила транслітерації, такий словник використовується в системах машинного перекладу для забезпечення перекладу власних назв, які не мають аналогів у мові, якою перекладається текст (наприклад: «Верховна Рада» англ. «*Verchovna Rada*»). У лівому полі такого словника послідовність букв мови-оригіналу, правому полі послідовність букв мови-перекладу. Довжина ланцюга букв визначається однозначністю передачі фонетичного звучання власної назви і коливається від 1 до 5.

Структура і зміст словників морфологічного рівня мовної системи. На цьому рівні аналізуються лише лексеми класів *L01***,** *L02***,** *L05* (див. табл. 1), тобто ті класи, для яких можна визначити лексико-граматичну інформацію. Даний рівень представлений словозмінною та словотвірною моделями мови.

Словозмінна модель визначається задачами автоматичного опрацювання текстів на морфологічному рівні:

1) Автоматичний морфологічний аналіз (АМА) – приписування граматичної інформації словоформам вхідного тексту.

2) Лематизація словоформ – приведення словоформи з тексту до початкової форми.

3) Синтез словоформ (синтезувати словоформу з початкової форми у відповідну необхідну форму для вживання у перекладеному тексті).

Для забезпечення першої задачі укладається аналітичний морфологічний словник, для 2 і 3 синтетичний морфологічний словник.

У розроблюваній ЛБД використано флективний підхід за словником квазізакінчень, який будується автоматично. Вхідними даними для процедури автоматичної побудови словника квазіфлексій є обернений словник словоформ певної вхідної мови з відповідною лексико-граматичною інформацією. До словника словоформ висуваються такі вимоги:

- лексика словника не містить службових частин мови і числівника (у тому числі й порядкового), оскільки дана лексика не визначає предметну галузь, має досить обмежений обсяг (близько 1 тис. словоформ), а тому автори вважають, що такий словник доцільно подавати у вигляді словника словоформ);
- лексико-граматична інформація повинна мати єдину граматичну параметризацію для російської, української та англійської мов та максимально враховувати функціональні особливості словоформи в тексті, формальний запис (код) лексико-граматичної інформації має забезпечувати незалежний доступ до кожної окремої граматичної категорії.

З метою забезпечення другої вимоги розроблено позиційно-цифрове кодування лексико-граматичної інформації [6]. Першим кодом (до символу «*») йде зазначення лексико-граматичного класу, а надалі граматичні характеристики у фіксованому порядку (рід, число, відмінок, особа, вид, стан, ступінь, час, істотність). Кожна граматична характеристика має певний набір параметрів, яким відповідає цифра від 0 до 9. При чому, для всіх характеристик значення 0 та 9 є загальними, а саме 0 – не визначається для даної словоформи взагалі, 9 – невизначена характеристика. Цифри від 1 до 8 мають конкретні значення для кожної характеристики. Наприклад, категорія «*число*» має такі характеристики: 1 – однина, 2 – множина, 3 – тільки однина, 4 – тільки множина. Якщо словоформа має декілька морфологічних значень (присутня омонімія) – то усі можливі комбінації задаються через символ «/». Наприклад, російській словоформі «*стекло*» буде відповідати така словникова стаття:

стекло 1*311000002/1*314000009/8*313021001/8*314021009/8*316021002/

Процес побудови словника квазіфлексій полягає в тому, що розглядаються словоформи з кінця слова в алфавітному порядку. Квазіфлексією в даному разі виступає набір літер з кінця слова. Починається процес з визначення найбільш часто вживаного коду (набору кодів) для однієї останньої літери – наприклад, літери «*а*». Надалі визначається найбільш вживаний код для квазіфлексії «*ба*», якщо він співпадає з кодом для «*а*», то така квазіфлексія не вноситься до словника, інакше – закінчення вноситься до словника та процес продовжується. Якщо на якомусь етапі визначиться, що для більш коротка квазіфлексія відповідає такому самому набору кодів, що і інше, яке включає таку квазіфлексію, то більша за розміром квазіфлексія видаляється зі словника. Такий прохід робиться по всім літерам алфавіту. На виході ми отримуємо словник квазіфлексій у вигляді власне квазіфлексій та відповідних їм визначених наборів кодів.

Лематизаційний словник являє собою словник квазіфлексій, ліва частина представляє мінімальну послідовність букв, яку необхідно відкинути від слова, а права частина – необхідно мінімальний фрагмент коду, на підставі якого розпізнана лексема

приводиться до початкової форми та послідовність букв, яку необхідно додати. Наприклад, російська словоформа *«полка»* має два набори граматичної інформації:

1) іменник жіночого роду, називного відмінку, однини;
2) іменник чоловічого роду, родового відмінку однини.

Стаття лематизаційного словника квазіфлексій для словоформи *«полка»* буде мати такий вигляд: *лка 1*1:лк/1*2:лка*.

Парадигматичний словник квазіфлексій будується аналогічно. В правій частині послідовність букв, яку необхідно відкинути від слова в початковій формі, а в лівій – парадигма цього слова. Нижче представлений фрагмент лематизаційного парадигматичного словника квазіфлексій для української мови.

а 1*2/а/и/і/у/ою/і/о/и/б/ів/ам/и//ів/ах/и/

б 1*11/б/ба//бу/бу//бові/б//ба/бом/бі/бе/би/бів/бам/би//бів/бами/бах/

йиб
2*11/бий/бого/бому/бий//бого/бим/бому//бім/ба/бої/бій/бу/бою/бій/бе/бого/бому/бе/бим/бому//бім/бі/бих/бим/бі//бих/бими/бих/

аб 1*41/ба/би/бі/бу/бою/бі/бо/би/б/бам/би//б/бами/бах/

Оскільки парадигматичний словник має значно більшу довжину рядка, то власне квазіфлексію виділено жирним шрифтом. Через риску подається парадигма слова у фіксованому порядку відповідно до кожного лексико-граматичного класу.

Структура і зміст словників синтаксичного рівня мовної системи. Словники цього рівня визначають правила синтаксичної сполучуваності в межах речення. Вхідними даними для побудови словників синтаксичної сполучуваності є дані морфологічного аналізу. Декларативне представлення правил синтаксису вхідної мови поділяється на контекстні синтаксичні правила, правила виокремлення присудка і підмета та правила виокремлення другорядних членів речення.

До контекстних синтаксичних правил відносять правила: узгодження, керування, прилягання. Формат опису правил представлений в таблиці 2.

В таблиці 2 знаком «+» показано за якою позицією застосовується правило перетинання значень морфологічного коду, 2 у позиції відмінок означає, що у другої словоформи має бути родовий відмінок, С1 – правило узгодження, У1-У2 – правила керування, П1 – правило прилягання.

Таблиця 2.

Формат опису правил

Який клас	З яким класом	рід	число	відмінок	Порядковий № гол. сл.	Синтаксичний тип	Приклад
2*	1*	+	+	+	(2)	С1	державні органи
23*	1*			2	(2)	У1	від форми
1*	1*			2	(1)	У2	генератор шуму
14*	8*				(2)	П1	швидко біг

Аналогічно задаються інші правила. Декларативне представлення правил синтаксису у вигляді уніфікованих таблиць дає можливість спростити алгоритм обробки на синтаксичному рівні мовної системи, звівши його фактично до обробки даних таблиці. Крім того це дає можливість одним модулем обробляти тексти,

представлені різними мовами, оскільки результат обробки залежить не від алгоритму обробки, а від коректності даних, представлених в таблиці.

Структура і зміст словників семантичного рівня мовної системи. Оскільки семантика тексту сильно корелюється з представленням знань про світ (предметну область), які ми включаємо до ІБД, то ми пропонуємо в ЛБД включати лише обмежений словник – словник, який не увійшов до словника квазізакінчень (це так звані службові частини мови: частка, прийменник, займенник, сполучник; до цього словника ми також відносимо числівник). Такий підхід обумовлений тим, що перелічені класи слів не характеризують предметну область і визначають допоміжну функцію у розумінні тексту. Крім того такий словник є обмежений обсягом – не перевищує 2 тис. словникових статей. Для виконання вимоги узгодженості словників ЛБД та ІБД для представлення семантичної інформації розроблено семантичний позиційно-цифровий код, який за форматом збігається із морфологічним кодом, але має інше змістове наповнення. Словникова стаття має такий вигляд: у левій частині словоформа у правій – код її семантичного класу, який відокремлюється знаком «*» від значень відповідних їй семантичних характеристик. Семантичні характеристики представлені 9-позиційним кодом, де перша позиція – час (як семантична категорія), 2 – простір; 3 – кількість; 4 – якість; 5 – предметність; 6 – явище; 7 – процес; 8 – стан; 9 – властивість. Значення кожної категорії визначаються на інтервалі [0;9], при цьому 0 і 9 мають фіксовані інтерпретації значень: 0 – не визначається; 9 – невизначено. Наприклад, російському слову «*возле*», буде відповідати така словникова стаття:

возле 25*010000000,

де 25* – означає семантичний клас відношення; 1 у другій позиції, що слово характеризується часом з конкретним значенням «*знаходитися в Q-межах*».

Висновки

Таким чином, запропонована модель ЛБД здатна забезпечувати обробку природномовного тексту для різних прикладних задач. За рахунок розмежування ЛБД по рівням мовної системи є змога використовувати лише окремі словники, так наприклад, для інформаційно-пошукових систем достатньо словників морфологічного рівня. Розмежування ІБД і ЛБД дозволяє значно спростити процедуру ведення електронних перекладних словників, звівши їх до формату слово – перекладний відповідник. Обсяг запропонованої моделі ЛБД значно менший. За рахунок використання словників квазізакінчень (як аналітичних, так і синтезуючих) обсяг всіх словників ЛБД не перевищує 25 тис. словникових одиниць. Декларативне представлення синтаксичних правил дозволяє покращити якість перекладу, оскільки повну синтаксичну структуру на сьогодні не будує жодна система перекладу, а збільшення обсягу словникових статей (близько 4 млн. в системі RETRANS) не дозволяє гарантувати обробку нового тексту.

Список літератури

1. Дарчук, Н.П. Комп’ютерна лінгвістика (автоматичне опрацювання тексту) [Текст] : підруч. для студ. вищ. навч. закл. / Н.П. Дарчук ; Київ. нац. ун-т ім. Т. Шевченка. — К. : Київ. ун-т, 2008. — 351 с.
2. Белоногов, Г.Г. Автоматизированные информационные системы [Текст] / Г.Г. Белоногов, В.И. Богатырев ; под общ. ред. К.С. Тараканова. — М. : Советское радио, 1973. — 328 с.
3. Grishman, R. TIPSTER text phase II architecture design / R. Grishman // TIPSTER’96 Proceedings of a workshop on held at Vienna, Virginia: May 6-8, 1996. — PP. 249–305.

4. Грязнухина, Т.О. Система автоматичного морфологічного аналізу українського наукового тексту / Т.О. Грязнухина, М.В. Нікула // Проблеми українізації комп'ютерів. Матеріали 2-ої Міжнар. конф. — Київ, 1993. — С. 42–46.
5. Балабін, В.В. Доморфемна обробка текстів в системах машинного перекладу / В.В. Балабін, І.В. Замаруєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — 2008. — Вип. 11. — С. 78–84.
6. Пампуха, І.В. Побудова та використання словника квазізакінчень / І.В. Пампуха, Л.О. Литвиненко, О.Ю. Ніколаєвський та ін. // Збірник наукових праць Військового институту КНУ ім. Тараса Шевченка. — К., 2008. — № 14. — С. 154–158.

МОДЕЛЬ ЛИНГВИСТИЧЕСКОЙ БАЗЫ ДАННЫХ В СИСТЕМАХ АВТОМАТИЧЕСКОЙ ОБРАБОТКИ ЕСТЕСТВЕННО-ЯЗЫКОВОЙ ТЕКСТОВОЙ ИНФОРМАЦИИ

И.В. Замаруева, В.Б. Толубко, Л.А. Литвиненко, А.Ю. Николаевский

Военный институт Киевского национального университета имени Тараса Шевченко,
просп. Глушкова, 2, корпус 8, Киев, 03680, Украина

В работе предложена модель организации лингвистической базы данных как составляющей лингвистического обеспечения систем автоматической обработки естественно-языковой текстовой информации. Особенность предложенной модели состоит в отделении знаний о языковой системе от знаний о мире (предметной области). Разработанная модель лингвистической базы данных по сравнению с известными характеризуется значительно меньшими объемами словарей, формат представления данных позволяет моделировать закономерности как флективных языков, так и аналитических. Она способна обеспечивать обработку естественно-языкового текста для различных прикладных задач.

Ключевые слова: лингвистическая база данных, лингвистическое обеспечение, системы автоматической обработки текстовой информации, языковая система, семиотическая система

MODEL OF LINGUISTIC DATA BASE IN AUTOMATIC PROCESSING OF NATURAL LANGUAGE TEXT SYSTEMS

Irina V. Zamaruieva, Vladimir B. Tolubko, Leonid O. Lytvynenko, Oleksandr Yu. Nikolaevsky

Military Institute, Taras Shevchenko National University of Kyiv,
2 Glushkova Ave., build. 8, Kyiv, 03680, Ukraine

The paper presents the model of the organization of the linguistic database as part of linguistic support of the automatic processing of natural language text information. The peculiarity of the proposed model is to separate the knowledge of the language system of knowledge about the world (domain). The developed model of a linguistic database in comparison with known characterized by significantly lower volumes of dictionaries, data format allows you to simulate patterns as inflected languages and analytical. It is able to provide the processing of natural language text for a variety of applications.

Keywords: linguistic database, linguistic software, automatic text processing, language system, semiotic system

УДК 004.7:681.31

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 82-90

КРИТЕРІЇ ОЦІНКИ РІВНЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ З ВРАХУВАННЯМ ЇХ АРХІТЕКТУРИ

І.З. Якименко

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: iyakymenko@mail.ru

В статті розглядається проблематика оцінки рівня захисту комп'ютерних мереж з врахуванням коефіцієнта емерджентності. Вперше розроблено критерій, який дозволяє оптимально встановити відповідність характеристик емерджентності мережі і її коефіцієнтів захисту. Згідно запропонованого підходу можна визначити необхідний рівень захисту інформаційних потоків в комп'ютерних мережах, який потрібен для певного класу архітектури.

Ключові слова: коефіцієнт емерджентності, комп'ютерні мережі, рівень захисту, коефіцієнт захисту, архітектури комп'ютерних мереж

Вступ

Сучасні комп'ютерні мережі інтенсивно вдосконалюються на основі нових теоретичних положень опрацювання інформаційних потоків при реалізації алгоритмів формування, перетворення, ідентифікації та покращення автентифікації користувачів інформаційних систем. При цьому, на сучасному етапі розвитку комп'ютерних мереж (КМ) виникає ряд проблем та науково-технічних задач, пов'язаних з підвищенням інформаційної стійкості КМ та швидкодії алгоритмів шифрування/дешифрування. Досвід використання відомих алгоритмів шифрування та розвиток теорії алгоритмів, які широко застосовуються в практиці на основі важко оборотних функцій хешування, факторизації, модулярних та інших операцій вже наблизилися до границь своїх потенційних можливостей і в загальному не можуть бути основою розвитку та вдосконалення засобів захисту інформаційних потоків (ІП) в сучасних та проектованих КМ. Крім того, виникає проблема комплексного підходу щодо забезпеченості необхідного рівня захисту ІП з врахуванням коефіцієнту емерджентності КМ [1–4].

Застосування інформаційних технологій у медицині відбувається в межах певних правових норм, які є правовим забезпеченням технології. Одним з важливих питань застосування інформаційних технологій є забезпечення конфіденційності інформації про пацієнта. Перелік відомостей про пацієнта, що не підлягають розголошенню, визначено статтею 286 Цивільного кодексу України та статтею 40 Закону України «Основи законодавства України про охорону здоров'я» (від 19 листопада 1992 р. № 2801-XI). Серед цих відомостей є і дані, якими оперують медичні інформаційні системи: результати медичного обстеження, діагноз.

Для технічного захисту інформації згідно ДСТУ 33961-96 та міжнародного стандарту застосовуються програмні засоби для ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації; засоби розмежування доступу користувачів до інформації та технічних засобів автоматизованих систем.

Сучасні комерційні медичні інформаційні системи володіють набором засобів та технологій як для розмежування доступу, так захисту баз даних.

Розвиток телемедицини та розподілених систем опрацювання медичної інформації ставить нові задачі оцінки потоків інформації в мережі як глобальній, так і

локальній, за залежність рівня захищеності від архітектури мережі та просторової віддаленості учасників обміну інформацією. Складність у вирішення цієї задачі вносить і стрімкий розвиток бездротових мереж та мобільних пристроїв, що все ширше застосовуються для збору діагностичної інформації про пацієнта.

Виходячи з вищесказаного, *метою* роботи є розробка критерію оцінки рівня захисту інформаційних потоків від несанкціонованого доступу з врахуванням коефіцієнту емерджентності, що дозволить встановлювати взаємно однозначну закономірність між захистом та типом архітектури мережі.

Дослідження архітектур комп'ютерних мереж

Дослідження та аналіз архітектур розподілених комп'ютерних систем, які використовуються в локальних, проблемно-орієнтованих та спеціалізованих комп'ютерних мережах, дозволяє визначити наступні класи їх архітектур, представлених в табл. 1, до яких належать: одноріневна, багаторівнева, безпровідна, з відкритим оптичним каналом [15]. Основним показником ефективності архітектур розподілених комп'ютерних систем є коефіцієнт емерджентності, який визначається згідно рівняння 1 [4, 8–11, 14]:

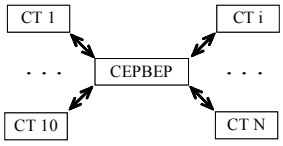
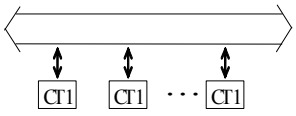
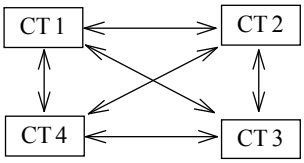
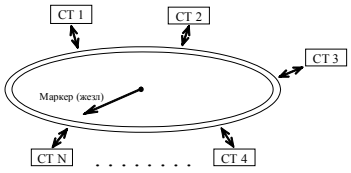
$$K_e = \frac{n_з}{n_e}, \qquad (1)$$

де $n_з$ — число зв'язків, n_e — число компонентів.

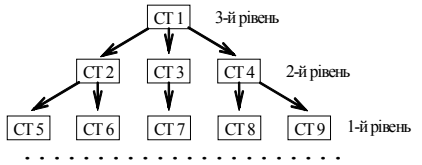
З табл. 1 видно, що найкращими показниками емерджентності характеризуються наступні архітектури: мережно-ієрархічна; систолічна; безпровідна безретрансляційна; безпровідна зірково-магістральна; зірково-магістральна. На рис. 1 показана гістограма коефіцієнтів емерджентності різних типів архітектур КМ.

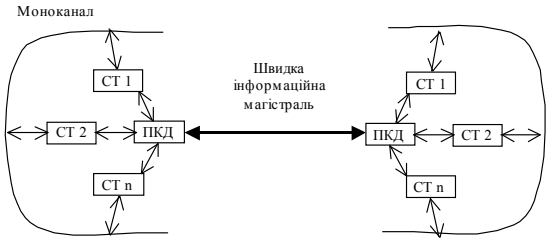
Таблиця 1.

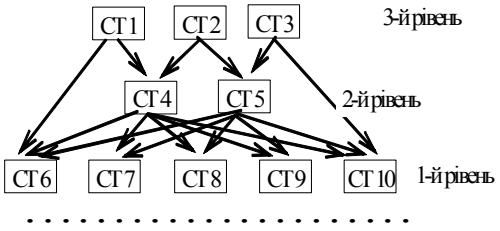
Тип та архітектура комп'ютерних мереж

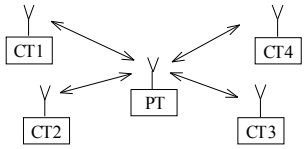
№	Тип та архітектура КМ	
	Одноріневі архітектури	
1	1. Зіркова  $K_e = 3$	2. Моноканал  $K_e = 1$
2	3. Систолічна  $K_e = 10$	4. Кільцева  $K_e = 1$

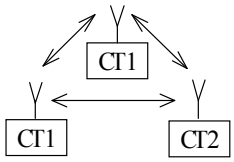
Продовження таблиці 1.

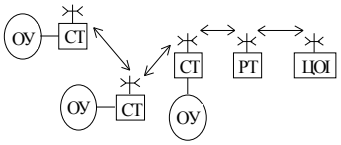
<table>
<tr><td colspan="4">Багаторівневі архітектури</td></tr>
<tr><td>3</td><td>5. Ієрархічна
 

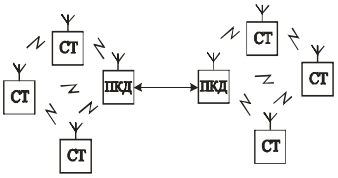
$K_e = 1$</td><td colspan="2">6. Зірково-магістральна
 

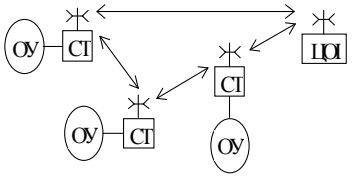
$K_e = 10$</td></tr>
<tr><td>4</td><td colspan="3">7. Мережно-ієрархічна
 

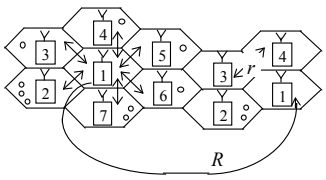
$K_e = 10$</td></tr>
<tr><td colspan="4">Безпровідні архітектури</td></tr>
<tr><td>5</td><td>8. З пасивним ретранслятором
 

$K_e = 3$</td><td>9. Безретрансляційна
 

$K_e = 10$</td><td>10. З активним ретранслятором
 

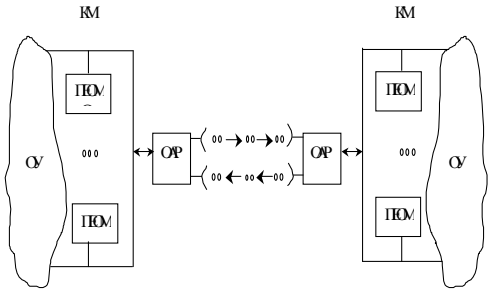
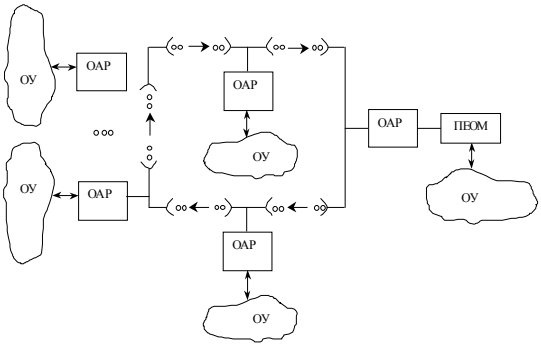
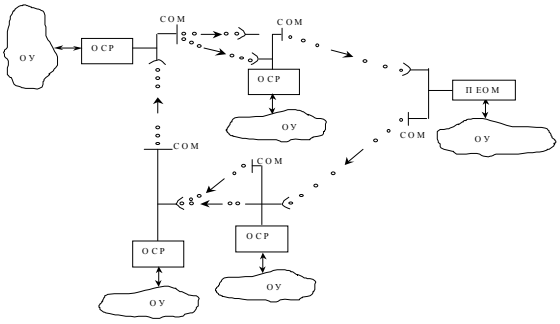
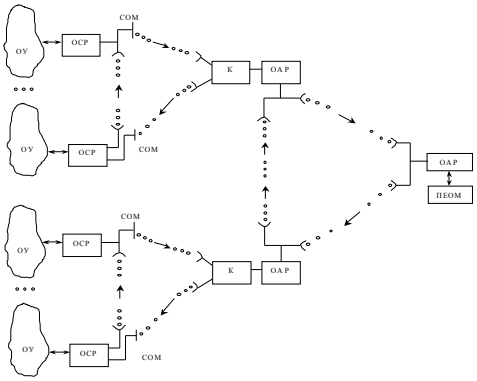
$K_e = 4$</td></tr>
<tr><td>6</td><td>11. Зірково-магістральна
 

$K_e = 10$</td><td>12. З активним ретранслятором та кільцевою структурою
 

$K_e = 6$</td><td>13. Сотова
 

$K_e = 6$</td></tr>
</table>

Продовження таблиці 1.

	Архітектури КМ з відкритими оптичними каналами зв'язку	
7	14. Високошвидкісна дуплексна  $K_e = 1$	15. Середньошвидкісна кільцева  $K_e = 3$
8	16. Низькошвидкісна кільцева  $K_e = 3$	17. Розгалужена  $K_e = 4$

Аналіз рис. 1 показує, що високим рівнем емерджентності характеризуються багаторівневі зірково-магістральні та мережно-ієрархічні КМ, а також безпровідні КМ з активними ретрансляторами.

У роботах [1, 2, 4] показано, що найбільш перспективною архітектурою КМ є безпровідна зірково-магістральна архітектура яку доцільно використовувати для забезпечення необхідного рівня захисту.

Рис. 1. Ефективність мережевих архітектур за параметром емерджентності. Однорівневі: 1 – зіркова; 2 – моноканал; 3 – кільцева; 4 – систолічна; багаторівневі: 5 – ієрархічна; 6 – зірково-магістральна; 7 – мережно-ієрархічна; безпровідні: 8 – з пасивним ретранслятором; 9 – безретрансляційні; 10 – з активним ретранслятором; 11 – зірково-магістральна; 12 – з активним ретранслятором та кільцевою структурою; 13 – сотова; з відкритими оптичними каналами зв'язку: 14 – високошвидкісна дуплексна; 15 – середньошвидкісна кільцева; 16 – низькошвидкісна кільцева; 17 – розгалужена

Критерій оцінки необхідного рівня захисту інформаційних потоків в комп'ютерних мережах

Оцінка архітектур та ІП в КМ на основі коефіцієнта емерджентності найкраще відображає структурну організацію КМ. В той же час, дана оцінка не відображає умов необхідного рівня захисту ІП КМ від несанкціонованого доступу [12, 13], що потребує їх класифікації з врахуванням вразливості, умов захисту та характеру секретності ІП, які можуть циркулювати в різних архітектурах. Спроба такої систематизації виконана у роботі [7]. У табл. 2 на основі експертних оцінок коефіцієнта захисту $K_з$ приведена класифікація мереж по характеру секретності та необхідного рівня захисту ІП від несанкціонованого доступу.

На основі оцінок коефіцієнта емерджентності КМ $K_е$ та коефіцієнта захисту ІП $K_з$ запропоновано критерій (забезпечення рівня захисту):

$$K_{зе} = \frac{K_з}{K_е}, \qquad (2)$$

який одночасно враховує необхідний рівень захисту ІП з врахуванням їх топологій та коефіцієнта емерджентності.

Слід зауважити, що архітектури КМ з врахуванням коефіцієнта емерджентності можна поділити на п'ять груп. До першої групи відносяться мережі з $K_е = 1$, до другої з $K_е = 2.5$, третьої $K_е = 4$, четвертої $K_е = 6$, п'ятої $K_е = 10$. У табл. 3 приведені показники критерію $K_{зе}$ забезпечення певного рівня захисту з врахуванням інтелекту мережі.

Таблиця 2.

Класифікація мереж по характеру секретності та захисту

№ п/п	Класифікація СКС по характеру секретності та захисту	$K_з$
1	Державного значення: служба безпеки України, національний банк України, Система Президента України, та ін.	10
2	Банківські системи	9
3	Відомчі системи (системи стратегічних об'єктів, військові)	8
4	Екологічно-небезпечні (атомні, нафтогазові та ін.)	7
5	Транспортні	6
6	Мережі медичних лікувальних закладів	5
7	Інтернет	4
8	Регіональні комп'ютерні мережі	3
9	Низові комп'ютерні мережі	2
10	Інформаційно-вимірювальні керуючі системи	1

Таблиця 3.

Показники критерію $K_{зе}$ забезпечення певного рівня захисту з врахуванням коефіцієнту емерджентності мережі

$K_з$ \ $K_е$	1	2.5	4	6	10
10	0.1	0.25	0.4	0.6	1
9	0.11	0.28	0.44	0.67	1.11
8	0.125	0.3125	0.5	0.75	1.25
7	0.14	0.36	0.57	0.86	1.43
6	0.167	0.42	0.67	1	1.67
5	0.2	0.5	0.8	1.2	2
4	0.25	0.625	1	1.5	2.5
3	0.33	0.83	1.33	2	3.33
2	0.5	1.25	2	3	5
1	1	2.5	4	6	10

Приведені на рис. 2 дослідження дозволяють встановити відповідність характеристик емерджентності мережі і її коефіцієнтів захисту для забезпечення оптимального рівня $K_{зе}$.

Рис. 2. Оцінка критерію $K_{зе}$ відповідно до характеристик емерджентності мережі та її коефіцієнтів захищеності.

Результати досліджень показали, що для забезпечення необхідного рівня захисту інформаційних потоків в комп'ютерних мережах необхідно вибирати такий клас архітектур, для яких співвідношення коефіцієнту захищеності та емержентності мережі наближається до 1.

Висновки

Аналіз та дослідження архітектур та трафіків КМ на основі оцінки їх емерджентності показує, що найбільш перспективною архітектурою мережевих технологій опрацювання інформаційних потоків є зірково-магістральна. Архітектури існуючих КМ, типу ієрархічних та багаторівневих, характеризуються нижчим рівнем емерджентності та рівнем трафіку у порівнянні з зірково-магістральною. Однак магістральні архітектури ще не є достатньо поширеними і тиражованими у світовій практиці і розглядаються як перспективні. Таким чином, вдосконалення мережевих технологій захисту інформаційних потоків на основі сучасних архітектур КМ не можуть в повній мірі забезпечити ефективність формування та опрацювання інформаційних потоків для захисту інформації. Вперше отриманий критерій оцінки рівня захисту який дозволяє встановити відповідність характеристик емерджентності мережі і її коефіцієнтів захисту. На його основі було встановлено, що для забезпечення необхідного рівня захисту інформаційних потоків в комп'ютерних мережах необхідно вибирати такий клас архітектур, для яких співвідношення коефіцієнту захищеності та інтелектуальності мережі наближається до 1.

Список літератури

1. Столлингс, В. Беспроводные линии связи и сети [Текст] / В. Столлингс ; пер. с англ. А.В. Высоцкий [и др.]. — М. ; СПб. ; К. : Издательский дом «Вильямс» ; СПб. ; К. : [б.и.], 2003. — 638 с.
2. Таненбаум, Э. Компьютерные сети [Текст] = Computer Networks / Э. Таненбаум ; пер. с англ. В. Шрага. — 4-е изд. — Санкт-Петербург : Питер, 2008. — 991 с.
3. Столлингс, В. Структурная организация и архитектура компьютерных систем: Проектирование и производительность [Текст] = Computer organization and architecture:

Designing and Performance : монография / В. Столлингс; [Пер. с англ. и ред. В.Т. Тертышного]. — 5-е изд. — М. : Вильямс, 2002. — 892 с.
4. Мартин, Дж. Планирование развития автоматизированных систем [Текст] = Strategic data-planning methodologies / Дж. Мартин ; пер. с англ. С.М. Круговой ; под ред. В.М. Савинкова. — М. : Финансы и статистика, 1984. — 195 с.
5. Олифер, В.Г. Компьютерные сети [Текст] : принципы, технологии, протоколы: учеб. пособие / В.Г. Олифер. — 3-е изд. — СПб. : Питер, 2008. — 958 с.
6. Буров, Є.В. Комп'ютерні мережі [Текст] : монографія / Є.В. Буров; за ред. В. Пасічника. — 2-ге вид., оновл. і доп. — Л. : [б. и.], 2003. — 566 с.
7. Защита информации в телекоммуникационных системах: учебник / В.Г. Кулаков, А.Б. Андреев, А.В. Заряев и др. — Воронеж: Воронежский институт МВД России, 2002. — 300 с.
8. Hartley, R.V.L. Transmission of information / R.V.L. Hartley // The Bell System Technical Journal. — 1928. — Vol. 7. — PP. 535–563.
9. Shannon, C.E. A Mathematical Theory of Communication / C.E. Shannon // The Bell System Technical Journal. — 1948. — Vol. 27. — PP. 379–423, 623–656.
10. Шэннон, К. Работы по теории информации и кибернетике [Текст] : монография / К. Шеннон; пер. с англ. под ред. Р.Л. Добрушина, О.Б. Лупанова ; с предисл. А.Н. Колмогорова. — М. : Иностр. лит., 1963. — 829 с.
11. Луценко, Е.В. Количественные меры возрастания эмерджентности в процессе эволюции систем (в рамках системной теории информации) / Е.В. Луценко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. — Краснодар: КубГАУ, 2006. — № 5(21).
12. Васильцов, І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними [Текст]: монографія / І.В. Васильцов. — Кременець : Вид. центр КОГРІ, 2009. — 264 с.
13. Васильцов, І.В. Класифікація сучасних атак спеціального виду на реалізацію / І.В. Васильцов, Л.О. Дубчак // Захист інформації. — 2007. — № 4. — С. 10–21.
14. Николайчук, Я.М. Теорія джерел інформації [Текст] : монографія / Я.М. Николайчук. — Т. : ТНЕУ, 2008. — 536 с.
15. Якименко, І.З. Фундаментальні основи структуризації та опрацювання інформаційних потоків в комп'ютерних мережах / І.З. Якименко // Вісник Хмельницького національного університету. Серія: «Технічні науки». — 2011. — № 3. — С. 265–271.

КРИТЕРИИ ОЦЕНКИ УРОВНЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ С УЧЕТОМ ИХ АРХИТЕКТУРЫ

И.З. Якименко

Тернопольский национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: iyakymenko@mail.ru

В статье рассматривается проблематика оценки уровня защиты компьютерных сетей с учетом коэффициента эмерджентности. Впервые разработан критерий, позволяющий оптимально установить соответствие характеристик эмерджентности сети и ее коэффициентов защиты. Согласно предложенному подходу можно определить необходимый уровень защиты информационных потоков в компьютерных сетях, который необходим для определенного класса архитектур.
Ключевые слова: коэффициент эмерджентности, компьютерные сети, уровень защиты, коэффициент защиты, архитектуры компьютерных сетей

EVALUATION CRITERIA OF NETWORKS PROTECTION LEVEL TAKING INTO ACCOUNT ITS ARCHITECTURE

Igor Z. Yakymenko

Ternopil National Economic University,
11 Lvivska str., Ternopil, 46020, Ukraine; e-mail: iyakymenko@mail.ru

This paper focuses on problems of evaluation of the networks protection level taking into account the emergence coefficient. Criterion that allowed to set optimally correspondence between network emergency and protection level was first developed. According to the proposed approach, it is possible to identify the necessary protection level of information streams in computer networks that required for specific class of architectures.
Keywords: emergency coefficient, computer networks, security level, protection coefficient, architecture of computer networks

УДК 004.942

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 91-97

ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЧНИХ СИСТЕМАХ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Л.О. Дубчак

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

У даній статті розглянуто метод захисту інформації, що передається в телемедичних мережах, шляхом вибору алгоритму шифрування даних на основі нечіткої логіки. Побудована нечітка система дозволяє здійснювати адекватний захист даних в реальному часі, враховуючи поточний стан самої комп'ютерної системи.

Ключові слова: нечітка система, телемедицина, захист інформації, DES, RSA, криптоалгоритм на основі еліптичних кривих

Вступ

Телемедицина – це галузь медицини, яка використовує телекомунікаційні та електронні інформаційні (комп'ютерні) технології для надання медичної допомоги і послуг в сфері охорони здоров'я в точці необхідності (в тих випадках, коли географічна відстань є критичним фактором) [1]. Глобальна мережа Інтернет в даному випадку є засобом зв'язку між клієнтом та комп'ютерною системою медичного закладу. Звідси випливають усі проблеми захисту інформації, що використовується в телемедицині, з точки зору інформаційної системи та мережі.

Як правило, інформаційна система включає [2]: прикладне програмне забезпечення (ППЗ), яке відповідає за зв'язок системи з клієнтом; системи управління базами даних (СУБД); операційну систему для обслуговування ППЗ та СУБД; мережу, яка забезпечує взаємодію всіх вузлів інформаційної системи. Найнебезпечнішими для таких інформаційних систем є несанкціонований доступ до паролів чи конфіденційної інформації, порушення прав доступу, атаки типу «відмова в обслуговуванні», «пряма» атака, віруси, сучасні атаки по побічних каналах витоку інформації. Несанкціонований доступ полягає у підборі чи викраденні пароля або підміні IP-адреси законного користувача системи. До цього виду атак вразливі усі компоненти інформаційної системи.

Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації [3]:

- контроль доступу;
- розширення парольного захисту;
- шифрування;
- використання брандмауерів.

Атака типу «відмова в обслуговуванні» полягає у створенні неправильного пакету даних чи передачі великої кількості пакетів даних по мережі з метою блокування роботи контролера домена, що зупиняє роботу комп'ютерної системи. Для захисту компонентів інформаційної системи застосовуються спеціальні програми виявлення такого типу атак чи міжмережеві екрани [4].

Комп'ютерний вірус – комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати

шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Для захисту від вірусів на даний час існує багато антивірусних програм, що захищає інформаційну систему від пошкодження.

Побічними каналами витоку інформації під час передачі пакетів даних по мережі є електромагнітне випромінювання, час виконання алгоритмів шифрування та реакція системи на спеціально внесені помилки. Для протидії таким атакам використовуються, як правило, архітектурна та операційна надлишковість, тобто додаткові апаратні та програмні засоби [3, 5].

Постановка завдання дослідження

Загалом можна визначити наступні методи захисту інформаційної системи від втрати чи викриття конфіденційної інформації [2].

Установка перешкоди – метод фізичного перешкоджання шляху зловмиснику до інформації, що захищається, у тому числі спроб з використанням технічних засобів знімання інформації і дії на неї.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

- ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);
- автентифікацію (встановлення автентичності) об'єкту або суб'єкта після пред'явленого їм ідентифікатору;
- перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);
- дозвіл і створення умов роботи в межах встановленого регламенту;
- реєстрацію (протоколювання) звернень до ресурсів, що захищаються;
- реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Проте, застосування всіх відомих методів захисту даних інформаційної системи не гарантує збереження цілісності даних, тому розробка нових підходів залишається актуальною задачею.

Одним із шляхів розв'язку цього завдання є застосування нечіткої логіки до побудови системи захисту інформації.

Нечітка система вибору алгоритму захисту інформації

Для здійснення захисту інформації в телемедицині необхідно визначити рівень доступу поточного клієнта до інформаційної системи. Крім того, варто враховувати ризик виникнення атаки через поточний канал передачі інформації, який може визначатися співвідношенням кількості звернень даного клієнта до кількості збоїв під час передачі даних через його канал.

На даний час відомі симетричні та асиметричні криптоалгоритми. Найпоширеніші серед них – симетричний DES, асиметричний RSA на основі еліптичних кривих [5].

Загальна схема вибору алгоритму захисту інформації зображена на рисунку 1. В даному випадку в якості критеріїв вибору виступають рівень доступу клієнта до інформації (*access*) та ризик виникнення атаки при передачі інформації поточному клієнту (*risk*), а підсистемою вибору є система обробки нечіткої інформації на основі механізму Мамдані. Виходом такої системи є один з криптоалгоритмів, відповідний вхідним критеріям вибору, застосовуючи який, комп'ютерна система забезпечить свою оптимальну роботу.

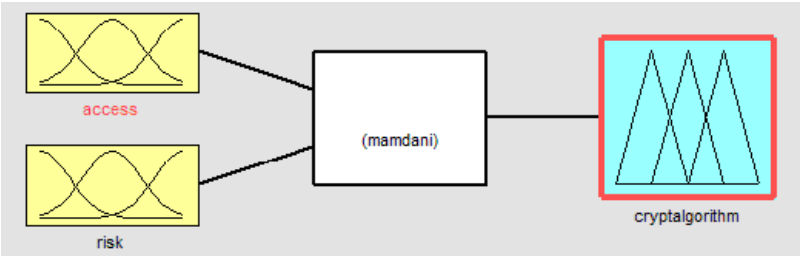


Рис. 1. Загальна схема оптимального вибору методу модулярного експоненціювання для розподілу доступу клієнтів комп'ютерної системи

В інженерних задачах застосовується, як правило, механізм нечіткого висновку Мамдані [6, 7]. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій [8]:

1) процедура фазифікації: визначаються степені істинності, тобто значення функцій належності $MF_i(x)$ для лівих частин кожного *i*-го правила (передумов);

2) нечіткий висновок. Спочатку визначаються мінімальний рівень «відсічення» для лівої частини кожного з правил $A_i = \min(MF_i(x))$, а потім знаходяться «усічені» функції належності висновку $B_i = \min(A_i, B_i)$;

3) композиція або об'єднання отриманих «усічених» функцій, для чого використовується максимальна композиція нечітких множин $MF(y) = \max(B_i(y))$;

4) дефазифікація або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод. Геометричний зміст такого значення – центр ваги для кривої функції належності отриманого виходу.

Застосовуючи засіб *Fuzzy Logic Toolbox* середовища *MathWorks* MATLAB 7.7.0 (R2008b) [9], можна побудувати запропоновану нечітку систему вибору криптоалгоритму.

Значення функцій належності вхідних змінних *access* та *risk* задається трапецевидною функцією, що визначається четвіркою чисел (a,b,c,d), які позначають абсциси вершин трапеції:

$$MF(x) = \begin{cases} \dfrac{b-x}{b-a}, a \le x \le b \\ 1, b \le x \le c \\ \dfrac{x-c}{d-c}, c \le x \le d \\ 0, \text{в інших випадках} \end{cases}.$$

Функція належності виходу *cryptoalgorithm* задається трикутною формою, яка залежить від трьох змінних (a,b,c) (абсциси вершин трикутника) [9]

$$MF(x)=\begin{cases}\dfrac{b-x}{b-a}, a\le x\le b\\ \dfrac{x-c}{c-b}, b\le x\le c\\ 0, \text{в інших випадках}\end{cases},$$

при чому в даному випадку має місце випадок симетричної трикутної функції належності, тобто $(b-a)=(c-b)$.

Функції належності для змінних *access* та *risk*, подані на рисунках 2 та 3, відповідно. Вони поділені на три інтервали кожна для точного опису змінних, зокрема, для опису рівня доступу до інформації застосовується змінна *low*, що позначає низький рівень доступу (може надаватися, наприклад, новим клієнтам), *middle* - середній рівень та *high* - високий рівень доступу (може надаватися адміністратору інформаційної системи).

Для задання рівня ризику виникнення атаки пропонуються змінні *low*, *middle* та *high*, що відповідають низькому, середньому та високому рівню.

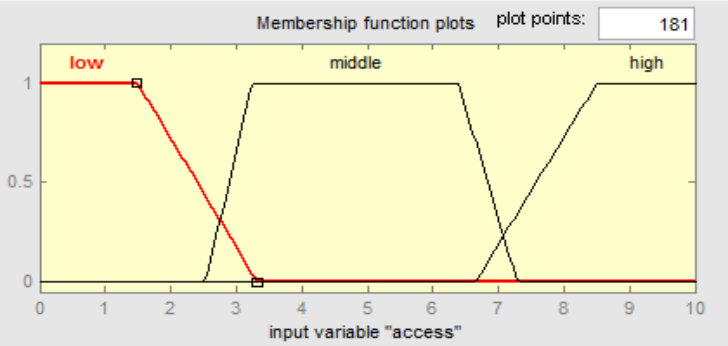


Рис. 2. Функції належності змінної *access*

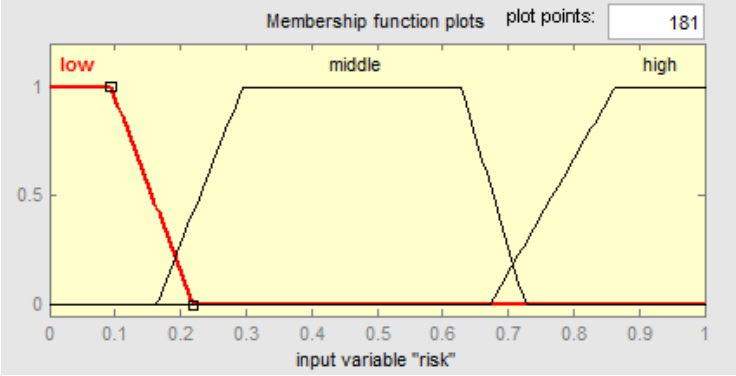


Рис. 3. Функції належності змінної *risk*

Функції належності для вихідної змінної *cryptoalgorithm* зображено на рисунку 4. Вони позначаються однаковими інтервалами на осі ординат для точного визначення центру ваги, що позначає нечіткий висновок системи. *None* позначає відсутність необхідності застосування алгоритму захисту інформації (наприклад, у випадку, коли до інформаційної системи звертається адміністратор), *DES*, *RSA* та *EC* – криптоалгоритм DES, RSA та на основі еліптичних кривих, відповідно. Кожен з цих алгоритмів має свої переваги і недоліки, свій рівень стійкості та продуктивності, які описані в [5].

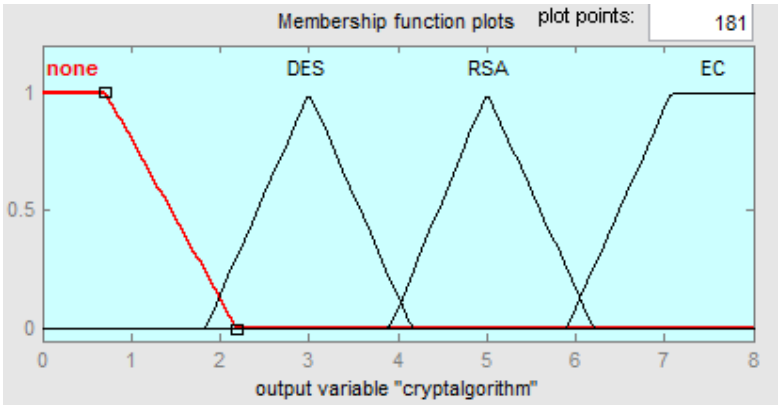


Рис. 4. Функції належності змінної *method*

База знань для побудови даної нечіткої моделі складається з правил типу «якщо — то» [9], усі вхідні змінні мають по три нечітких стани і ще один стан, коли значення вхідної змінної не задане системою. Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий, тому кількість правил нечіткого висновку досліджуваної системи $N = 4 \times 4 - 1 = 15$. База правил розробленої нечіткої системи має вигляд, зображений на рисунку 5 і задається наступним чином:

1) **IF** (access is low) **AND** (risk is low) **THEN** (cryptalgorithm is RSA)
2) **IF** (access is low) **AND** (risk is middle) **THEN** (cryptalgorithm is RSA)
3) **IF** (access is low) **AND** (risk is high) **THEN** (cryptalgorithm is EC)
4) **IF** (access is low) **THEN** (cryptalgorithm is EC)
5) **IF** (access is middle) **AND** (risk is low) **THEN** (cryptalgorithm is DES)
6) **IF** (access is middle) **AND** (risk is middle) **THEN** (cryptalgorithm is DES)
7) **IF** (access is middle) **AND** (risk is high) **THEN** (cryptalgorithm is EC)
8) **IF** (access is middle) **THEN** (cryptalgorithm is RSA)
9) **IF** (access is high) **AND** (risk is low) **THEN** (cryptalgorithm is none)
10) **IF** (access is high) **AND** (risk is middle) **THEN** (cryptalgorithm is DES)
11) **IF** (access is high) **AND** (risk is high) **THEN** (cryptalgorithm is EC)
12) **IF** (access is high) **THEN** (cryptalgorithm is none)
13) **IF** (risk is low) **THEN** (cryptalgorithm is DES)
14) **IF** (risk is middle) **THEN** (cryptalgorithm is RSA)
15) **IF** (risk is high) **THEN** (cryptalgorithm is EC)

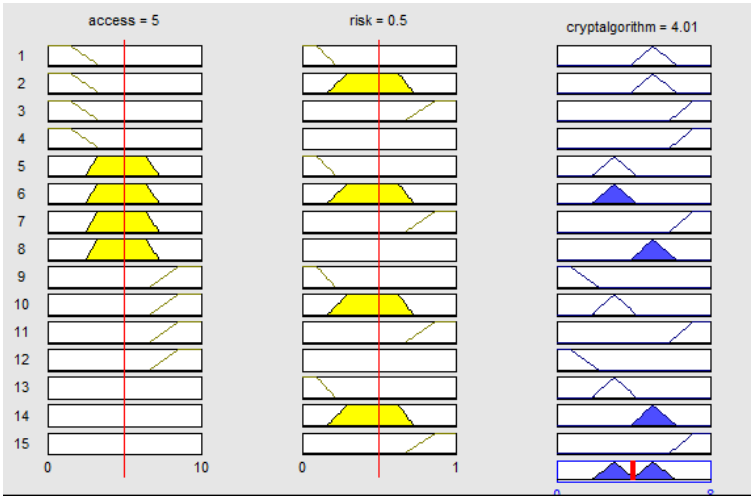


Рис. 5. База правил нечіткої системи вибору криптоалгоритму

Поверхня значень розробленої нечіткої системи вибору алгоритму захисту інформації в телемедицині зображена на рисунку 6.

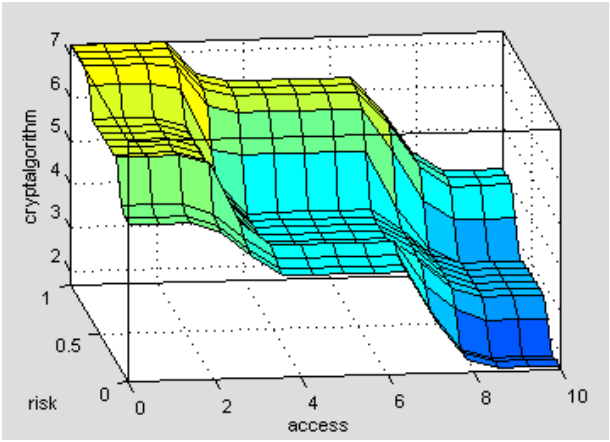


Рис. 6. Поверхня значень нечіткої системи вибору криптоалгоритму

Дослідження бази правил (див. рис. 5) та поверхні значень (див. рис. 6) запропонованої нечіткої системи показали правильність її роботи.

Висновок

В даній статті запропоновано систему захисту інформації в телемедичній системі, яка базується на нечіткому висновку Мамдані. Розроблена нечітка система дозволяє застосувати оптимальний для кожного клієнта криптоалгоритм в реальному часі, що забезпечить найкращу роботу всієї інформаційної системи в цілому.

Список літератури

1. Владзимирский, А.В. Телемедицина [Текст] : [монография] / А.В. Владзимирский. — Донецк : НОУЛИДЖ, 2011. — 436 с.
2. Лукацкий, А. Атаки на информационные системы. Типы и объекты воздействия / А.Лукацкий // Электроника: Наука, Технология, Бизнес. — 2000. — № 1. — С. 16–21.

3. Васильцов, І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними [Текст]: монографія / І.В. Васильцов. — Кременець : Вид. центр КОГРІ, 2009. — 264 с.
4. Дубчак, Л.О. Атаки на сучасні інформаційні системи та методи захисту проти них / Л.О. Дубчак // Materiály IX mezinárodní vědecko-praktická konference «Vědecký pokrok na přelomu tysyachalety – 2013». — Praha Publishing House «Education and Science» s.r.o, 2013. — PP. 3–5.
5. Романец, Ю.В. Защита информации в компьютерных системах и сетях : 2 изд., перераб. и доп. / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин ; ред. В.Ф. Шаньгин. — Москва : Радио и связь, 2001. — 376 с.
6. Ross, T.J. Fuzzy Logic with Engineering Applications / T.J. Ross. — New York : McGraw-Hill, 1995. — 600 p.
7. Штовба, С.Д. Введение в теорию нечетких множеств и нечеткую логику / С.Д. Штовба. — Винница : Изд-во ВГТУ, 2001. — 198 с.
8. Бережная, М.А. Методы проектирования нечетких устройств принятия решений на основе программируемых логических интегральных микросхемах. / М.А. Бережная // Технология приборостроения. — 2009. — № 2. — С. 16–23.
9. Лазарєв, Ю.Ф. Моделювання динамічних систем у Matlab. Електронний навчальний посібник / Ю.Ф. Лазарєв — К.: НТУУ «КПІ», 2011. — 421 с.

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ НА ОСНОВЕ НЕЧЁТКОЙ ЛОГИКИ

Л.О. Дубчак

Тернопольский национальный экономический университет,
ул. Львовская, 11, 46020, Тернополь, e-mail: dlo@tneu.edu.ua

В статье рассмотрен метод защиты информации, передаваемой в телемедицинских сетях, путем выбора алгоритма шифрования данных на основе нечёткой логики. Построенная нечёткая система позволяет осуществлять адекватную защиту данных в реальном времени, учитывая текущее состояние самой компьютерной системы.
Ключевые слова: нечёткая система, телемедицина, защита информации, DES, RSA, криптоалгоритм на основе эллиптических кривых

INFORMATION SECURITY IN TELEMEDICINE SYSTEMS BASED ON FUZZY LOGIC

Lesya O. Dubchak

Ternopil National Economical University,
11 Lvivska str., 46020, Ternopil, e-mail: dlo@tneu.edu.ua

In this article the method of protecting information, transmitted in telemedicine networks, by selecting encryption algorithm based on fuzzy logic had been proposed. Proposed fuzzy system allows for adequate protection of data in real time, considering the current state of the computer system.
Keywords: fuzzy systems, telemedicine, information security, DES, RSA, crypto algorithm based on elliptic curves

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 3, номер 1, 2013. Одеса – 98 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 3, номер 1, 2013. Одесса – 98 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 3, No. 1, 2013. 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 №7 від 30.04.2013)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: immm.ukraine@gmail.com