Висновки. Згідно методу побудови засобів, що автоматизують процеси доменного аналізу представленого розширення RTPA, яке демонструється на прикладі розробки програмного забезпечення авіаційного тренажера. Метод може використовуватися для побудови засобів, які автоматизують інші процеси доменної інженерії.

ЛІТЕРАТУРА

1. Сидоров Н.А. Восстановление, повторное использование и переработка программного обеспечения. I. // УСим – К.- 1998.- №3.- С.74-83.
2. Wartik S., Prieto-Diaz R. Criteria for comparing reuse-oriented domain analysis approaches.- Software productivity consortium, 1991. Hp. 31-67.
3. Dudnyk V., Ryabokin U., Mendzebrovskiy I. Method of domain analysis to information support of aircraft.- National Aviation University, Ukraine.- 2012.- p.p. 1.10.1-1.10.19
4. Сидоров Н.А., Мендзебровский И.Б., Рябоконь Ю.Н. Метод построения средств доменного анализа на основе формальных спецификаций в RTPA. Вестник Восточноукраинского национального университета им . Даля.- №4.- 2012.- С. 52-57.
5. Wang Y. Software engineering foundations: a software science perspective.- Auerbach Publications, 2008, p. 1200.
6. STARS. Organization Domain Modeling (ODM) Guidebook Version 2.0. STAR Technical Report D613-55159, STARS Technology Center, Arlington VA, July 1996.
7. Sidorov N., Khomenko V., Nedovodeev V. Reengineering of the air simulators legacy software.- Proc. Of the NAU.- №2.- 2008.- P. 28-35.
8. Сидоров Н.А., Недоводеев В.Т., Сердюк И.П., Хоменко В.А., Сидоров Е.Н. Реинженерия наследуемого программного обеспечения информационно – моделирующих тренажерных комплексов. УС и М.- 4. - 2008. - с.68-75.

Надійшла: 5.10.2012 р.

Рецензент: д.т.н., професор Петров О.С,

УДК 004.942.001.57 **Молодецька К.В.**

МОДЕЛЬ ТЕПЛОВОГО ПОЛЯ СМАРТ-КАРТИ МОДУЛЯ АУТЕНТИФІКАЦІЇ В КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ

Запропоновано аналітичну модель теплового поля модуля смарт-карти пристрою аутентифікації, побудовану із використанням методу на основі алгебричних властивостей диференціальних спектрів. Виконано порівняння отриманих результатів із іншими відомими методами.

Ключові слова: захист інформації, теплове поле, модуль аутентифікації, диференціальні перетворення.

На сьогодні відома велика кількість різнопланових загроз безпеки інформації в комп'ютеризованих системах [1–2]. В останні роки на основі сучасних методів здійснюються нові види криптоаналітичних атак, метою яких є визначення деталей виконання криптографічних перетворень. До таких методів відносять атаки на комп'ютеризовані системи за допомогою вимірювання рівня енергоспоживання, випромінювання та використання інших побічних каналів. Такі атаки можуть здійснюватися проти різних алгоритмів шифрування з відкритим ключем в пристроях аутентифікації, що забезпечені системами протидії вторгненню [1]. Як приклад атаки на смарт-карту розглянемо випадок, коли порушник має на меті несанкціоноване отримання секретних ключів, які знаходяться всередині модуля, захищеного від вторгнення. Порушник не здатний до здійснення криптоаналізу алгоритмів чи протоколів і не може зламати систему протидії вторгненню.

Альтернативними варіантами атаки є таймінг-аналіз, який полягає у визначенні часу, необхідного модулю для виконання певних операцій і подальшого встановлення інформації про ключ, або вимірювання кількості тепла, що виділяється у модулі, та визначення місцезнаходження джерела випромінювання. Атаки на основі вимірювання випромінюваної теплової енергії були використані для розкриття секретів усіх карт, що є на ринку [1–2]. Теплове поле такого модуля описується диференціальним рівнянням з частинними похідними з початковими і граничними умовами. Моделювання теплових полів виконується

із використанням чисельних методів розв'язання й потребує виконання значного об'єму обчислень на ЕОМ. В даний час аналітичні і чисельно-аналітичні методи розв'язання крайових задач недостатньо розвинені і вимагають подальших досліджень.

Аналіз останніх досліджень і публікацій [3–8] показав, що моделювання фізичних полів може бути виконано в аналітичному або чисельно-аналітичному вигляді на основі використання одномірних диференціальних перетворень [4–7]. Недолік цих методів полягає в залежності складності аналітичного опису фізичного поля в області зображень від похибки моделювання фізичного процесу в області оригіналів. Математична модель фізичного поля в області диференціальних перетворень має вигляд диференціального спектру, де похибка моделювання фізичного процесу в області оригіналів безпосередньо залежить від кількості дискрет [5]. Складність аналітичного опису дискрет диференціального спектру зростає із збільшенням номера дискрети. Тому моделювання фізичних полів в аналітичному вигляді виконують з використанням декількох початкових дискрет диференціального спектру, а це обмежує точність моделювання фізичних полів в області оригіналів. В зв'язку з цим виникає завдання зниження похибки моделювання фізичних полів у випадку використання обмеженої кількості дискрет диференціального спектру. Пропонується підвищити точність моделювання фізичних полів шляхом використання методу на основі алгебричних властивостей диференціальних спектрів.

Мета статті полягає в розробці аналітичної моделі теплового поля смарт-карти модуля аутентифікації для її подальшого застосування при побудові захищених модулів в комп'ютеризованих системах.

Розглянемо задачу моделювання теплового поля в тонкій прямокутній пластинці смарт-карти ABCE. Потрібно знайти стаціонарну температуру внутрішніх точок пластинки. Ця задача зводиться до розв'язку крайової задачі Лапласа:

$$\frac{\partial^2 u(x,y)}{\partial x^2}+\frac{\partial^2 u(x,y)}{\partial y^2}=0, \tag{1}$$

зі змішаними граничними умовами:

$$u\big|_{AB}=0,\ u\big|_{CD}=1,\ \left.\frac{\partial u}{\partial \nu}\right|_{BC\cup AED}=0, \tag{2}$$

де ν – нормаль до межі.

Розіб'ємо область Ω на дві зони Ω_1 і Ω_2 й позначимо через S границю поділу області на зони (рис. 1). Зона Ω_1 обмежена прямокутником BCDF, а зона Ω_2 – прямокутником AEDF. На першому етапі виконаємо моделювання в зоні Ω_1. При цьому використаємо дві моделі зміщених диференціальних перетворень по змінній y.

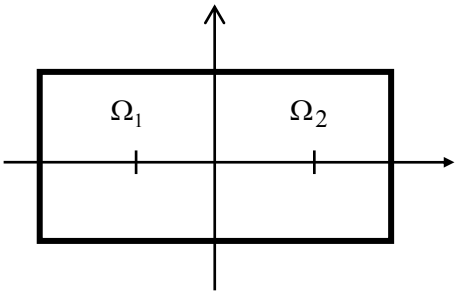

Рис. 1. Область моделювання смарт-карти

Прямий диференціальний спектр нижньої половини зони Ω_1 будуємо в точці $y_{1\nu}=-0,5$ згідно виразів [5]:

$$U_1(x,k)=\frac{H_1^k}{k!}\left[\frac{\partial^k u_1(x,y)}{\partial y^k}\right]_{y=y_{1\nu}=-0,5},\ u_1(x,y)=\sum_{k=0}^{\infty}\left(\frac{y-y_{1\nu}}{H_1}\right)^k U_1(x,k), \tag{3}$$

а зворотний диференціальний спектр верхньої половини зони Ω_1 будуємо в точці $y_{2\nu}=0,5$:

$$\overline{U}_1(x,k)=\frac{\overline{H}_1^k}{k!}\left[\frac{\partial^k u_1(x,y)}{\partial y^k}\right]_{y=y_{2\nu}=0,5},\ \overline{u}_1(x,y)=\sum_{k=0}^{\infty}\left(\frac{y-y_{2\nu}}{\overline{H}_1}\right)^k \overline{U}_1(x,k), \tag{4}$$

де $U_1(x,k)$, $\overline{U}_1(x,k)$ – диференціальні зображення функції $u_1(x,t)$; H_1 – довільна додатна стала; k – цілочисловий аргумент, який приймає значення 0, 1, 2, 3, …, ∞.

Таким чином рівняння теплового поля (1) в області зображень приймає вигляд:

$$U_1(x,k+2)=-\frac{H_1^2}{(k+1)(k+2)}\frac{d^2U_1(x,k)}{dx^2},\ \overline{U}_1(x,k+2)=-\frac{\overline{H}_1^2}{(k+1)(k+2)}\frac{d^2U_1(x,k)}{dx^2}. \tag{5}$$

Прямий диференціальний спектр згідно із рекурентною формулою (3) запишемо як:

$$U_1(x,0)=1,\ U_1(x,1)=H_1\varphi_1(x),\ U_1(x,2)=0,\ U_1(x,3)=-\frac{H_1^3}{3!}\ddot{\varphi}_1(x), \tag{6}$$

де $\varphi_1(x)$ – невідома функція аргументу x і введено позначення $\ddot{\varphi}_1(x)=\dfrac{d^2\varphi_1(x)}{dx^2}$.

Зворотний диференціальний спектр визначимо за виразом (4):

$$\overline{U}_1(x,0)=0,\ \overline{U}_1(x,1)=\overline{H}_1\psi_1(x),\ \overline{U}_1(x,2)=0,\ \overline{U}_1(x,3)=-\frac{\overline{H}_1^3}{3!}\ddot{\psi}_1(x), \tag{7}$$

де $\psi_1(x)$ – невідома функція аргументу x, а $\ddot{\psi}_1(x)=\dfrac{d^2\psi_1(x)}{dx^2}$.

Застосуємо обернені диференціальні перетворення (3) і (4) для диференціальних спектрів (6) та (7) відповідно:

$$u_1(x,y)=1+(y-y_{1\nu})\varphi_1(x)-\frac{(y-y_{1\nu})^3}{6}\ddot{\varphi}_1(x),\ \overline{u}_1(x,y)=(y-y_{2\nu})\psi_1(x)-\frac{(y-y_{2\nu})^3}{6}\ddot{\psi}_1(x). \tag{8}$$

Вздовж осі Ox при $y=0$ повинна виконуватися умова спряження диференціальних спектрів в точці $U_1(x,y=0)=\overline{U}_1(x,y=0)$ [5]. Підставляючи в неї вирази (8) при $y=0$, $y_{1\nu}=-0,5$, $y_{2\nu}=0,5$ отримаємо:

$$1+0,5\varphi_1(x)-\frac{1}{48}\ddot{\varphi}_1(x)=-0,5\psi_1(x)+\frac{1}{48}\ddot{\psi}_1(x). \tag{9}$$

Також повинна виконуватися умова спряження диференціальних спектрів по похідним $\left.\dfrac{\partial U_1}{\partial y}\right|_{y=0}=\left.\dfrac{\partial\overline{U}_1}{\partial y}\right|_{y=0}$. Диференціюючи вирази (8) по y і підставляючи $y_{1\nu}=-0,5$, $y_{2\nu}=0,5$ отримаємо:

$$\varphi_1(x)-\frac{1}{8}\ddot{\varphi}_1(x)=\psi_1(x)-\frac{1}{8}\ddot{\psi}_1(x). \tag{10}$$

Із умов спряження вздовж осі *Ox* при $y=0$ отримуємо систему звичайних диференціальних рівнянь (9)–(10). Загальний розв'язок системи лінійних звичайних диференціальних рівнянь має вигляд:

$$\varphi_1(x) = -1 - C_1 e^{-2\sqrt{2}x} - C_2 e^{2\sqrt{2}x} + C_3 e^{-2\sqrt{6}x} + C_4 e^{2\sqrt{6}x},$$
$$\psi_1(x) = -1 + C_1 e^{-2\sqrt{2}x} - C_2 e^{2\sqrt{2}x} + C_3 e^{-2\sqrt{6}x} + C_4 e^{2\sqrt{6}x}, \quad (11)$$

де C_1, C_2, C_3, C_4 – сталі інтегрування.

Сталі інтегрування для зони Ω_1 при $y \in [0;0,5]$ позначимо через $\overline{C}_i$, причому $C_i \neq \overline{C}_i$, $i = \overline{1,4}$. Параметри C_i та $\overline{C}_i$ визначаються із умов спряження зон Ω_1 і Ω_2, а також із заданих граничних умов (2). Таким чином, маємо:

$$C_1 = C_2 e^{-4\sqrt{2}}, \; C_3 = C_4 e^{-4\sqrt{6}}, \; \overline{C}_1 = \overline{C}_2 e^{-4\sqrt{2}}, \; \overline{C}_3 = \overline{C}_4 e^{-4\sqrt{6}}. \quad (12)$$

Із врахуванням (12) розв'язок крайової задачі в області Ω_1 приймає вигляд:

$$u_1(x,y) = 0,5 - y - (y+0,5)\left\{C_2\left[1 - \frac{4}{3}(y+0,5)^2\right]\left(e^{-2\sqrt{2}(x+2)} + e^{2\sqrt{2}x}\right) - \right.$$
$$\left. - C_4\left[1 - 4(y+0,5)^2\right]\left(e^{-2\sqrt{6}(x+2)} + e^{2\sqrt{6}x}\right)\right\} \quad для \quad y \in [0;-0,5]; \quad (13)$$

$$\overline{u}_1(x,y) = 0,5 - y + (y-0,5)\left\{\overline{C}_2\left[1 - \frac{4}{3}(y+0,5)^2\right]\left(e^{-2\sqrt{2}(x+2)} + e^{2\sqrt{2}x}\right) + \right.$$
$$\left. + \overline{C}_4\left[1 - 4(y-0,5)^2\right]\left(e^{-2\sqrt{6}(x+2)} + e^{2\sqrt{6}x}\right)\right\} \quad для \quad y \in [0;0,5]. \quad (14)$$

На другому етапі виконаємо аналогічним чином моделювання в зоні Ω_2. Використаємо дві моделі зміщених диференціальних спектрів по змінній *y*. Прямий диференціальний спектр нижньої половини зони Ω_2 будуємо в точці $y_{1\nu} = -0,5$, а зворотний диференціальний спектр верхньої половини зони Ω_2 будуємо в точці $y_{2\nu} = 0,5$, позначивши через H_2 крок моделювання. Виконаємо побудову прямого та зворотного диференціальних спектрів, використовуючи граничну умову (2):

$$U_2(x,0) = \varphi_2(x), \; U_2(x,1) = 0, \; U_2(x,2) = -\frac{H_2^2}{2}\ddot{\varphi}(x), \; U_2(x,3) = 0, \quad (15)$$

де $\varphi_2(x)$ – невідома функція аргументу *x*; $\ddot{\varphi}_2(x) = \dfrac{d^2\varphi_2(x)}{dx^2}$;

$$\overline{U}_2(x,0) = 0, \; \overline{U}_2(x,1) = \psi_2(x)\overline{H}_2, \; \overline{U}_2(x,2) = 0, \; \overline{U}_2(x,3) = -\frac{\overline{H}_2^3}{3!}\ddot{\psi}_2(x), \quad (16)$$

де $\psi_2(x)$ – невідома функція аргументу *x*; $\ddot{\psi}_2(x) = \dfrac{d^2\psi_2(x)}{dx^2}$.

Вздовж осі *Ox* при *y=0* повинна виконуватися умова спряження диференціальних спектрів у точці спряження $U_2(x, y=0) = \overline{U}_2(x, y=0)$ та за похідними $\left.\dfrac{\partial U_2}{\partial y}\right|_{y=0} = \left.\dfrac{\partial \overline{U}_2}{\partial y}\right|_{y=0}$.

Система рівнянь для умов спряження має вигляд:

$$\varphi_2(x) - \frac{1}{8}\ddot{\varphi}_2(x) = -0,5\psi_2(x) + \frac{1}{48}\ddot{\psi}_2(x),$$
$$-0,5\ddot{\varphi}_2(x) = \psi_2(x) - \frac{1}{8}\ddot{\psi}_2(x). \quad (17)$$

Розв'язок системи (17) має вигляд:

$$\psi_2(x) = a_1 e^{p_1 x} + a_2 e^{p_2 x} + a_3 e^{p_3 x} + a_4 e^{p_4 x},$$

$$\varphi_2(x) = a_1 e^{p_1 x}\left[-\frac{3}{4} + \frac{5}{96}p_1^2\right] + a_2 e^{p_2 x}\left[-\frac{3}{4} + \frac{5}{96}p_2^2\right] + a_3 e^{p_3 x}\left[-\frac{3}{4} + \frac{5}{96}p_3^2\right] + a_4 e^{p_4 x}\left[-\frac{3}{4} + \frac{5}{96}p_4^2\right]. \quad (18)$$

Підставляємо (18) в вирази для оберненого диференціального перетворення (3)–(4) при $y_{1\nu} = -0,5$ та при $y_{2\nu} = 0,5$:

$$u_2(x,t) = A\left(a_1 e^{p_1 x} + a_2 e^{p_2 x}\right) + B\left(a_3 e^{p_3 x} + a_4 e^{p_4 x}\right) \quad при \quad y \in [0;-0,5], \quad (19)$$

$$\bar{u}_2(x,t) = (y-0,5)\left\{\bar{A}\left(\bar{a}_1 e^{p_1 x} + \bar{a}_2 e^{p_2 x}\right) + \bar{B}\left(\bar{a}_3 e^{p_3 x} + \bar{a}_4 e^{p_4 x}\right)\right\} \quad при \quad y \in [0;0,5], \quad (20)$$

де введено наступні позначення:

$$A = \left[-\frac{3}{4} + \frac{5}{96}p_1^2\right]\left[1 - \frac{p_1^2}{2}(y+0,5)^2\right], \quad B = \left[-\frac{3}{4} + \frac{5}{96}p_3^2\right]\left[1 - \frac{p_3^2}{2}(y+0,5)^2\right],$$
$$\bar{A} = \left[1 - \frac{p_1^2}{6}(y-0,5)^2\right], \quad \bar{B} = \left[1 - \frac{p_2^3}{6}(y-0,5)^2\right]. \quad (21)$$

Параметри a_j, $\bar{a}_j$, $j = \overline{1,4}$ визначаємо із умови спряження зон Ω_1 і Ω_2, а також із граничної умови на грані *AE*:

$$a_1 = e^{-2p_1} a_2, \quad a_3 = e^{-2p_3} a_4, \quad \bar{a}_1 = e^{-2p_1}\bar{a}_2, \quad \bar{a}_3 = e^{-2p_3}\bar{a}_4. \quad (22)$$

Якщо записати умови спряження зон Ω_1 і Ω_2 вздовж осі *Oy* та в граничну умову на грані *BC* ввести позначення $v_1(x,y)\big|_{x=-1}$ і в граничну умову на грані *AE* $v_2(x,y)\big|_{x=1}$:

$$v_1(x,y)\big|_{x=-1} = \left.\frac{\partial u_1(x,y)}{\partial x}\right|_{x=-1} = 0, \; v_2(x,y)\big|_{x=1} = \left.\frac{\partial u_2(x,y)}{\partial x}\right|_{x=1} = 0,$$

отримаємо систему:

$$\begin{cases} u_1(x,y)\big|_{x=0} = u_2(x,y)\big|_{x=0}, \\ v_1(x,y)\big|_{x=0} = v_2(x,y)\big|_{x=0}, \end{cases} \quad при \quad y \in [0;-0,5]; \quad \begin{cases} \bar{u}_1(x,y)\big|_{x=0} = \bar{u}_2(x,y)\big|_{x=0}, \\ \bar{v}_1(x,y)\big|_{x=0} = \bar{v}_2(x,y)\big|_{x=0}, \end{cases} \quad при \quad y \in [0;0,5]. \quad (23)$$

Умови спряження (23) переведемо в область зображень по змінній *y* та надаючи цілочисловому аргументу *k* значення 0 і 1 у виразі отримаємо систему рівнянь для визначення параметрів C_2, C_4, a_2, a_4, $\bar{C}_2$, $\bar{C}_4$, $\bar{a}_2$, $\bar{a}_4$. Із властивостей диференціальних перетворень [6] слідує, що перше рівняння системи (23) зліва в області зображень може бути представлене у вигляді:

$$u_1(x,y)\big|_{\substack{x=0\\y=0}} = u_2(x,y)\big|_{\substack{x=0\\y=0}}. \quad (24)$$

Підставляючи в (24) вирази (13) і (19), враховуючи (21), отримаємо рівняння:

$$0,5 - \frac{C_2}{3}\left(e^{-4\sqrt{2}} + 1\right) = A_0 a_2\left(e^{-2p_1} + 1\right) + B_0 a_4\left(e^{-2p_3} + 1\right), \quad (25)$$

де згідно виразу (21):

$$A_0 = A\big|_{y=0} = \left(-\frac{3}{4} + \frac{5}{96}p_1^2\right)\left(1 - \frac{p_1^2}{8}\right), \quad B_0 = B\big|_{y=0} = \left(-\frac{3}{4} + \frac{5}{96}p_3^2\right)\left(1 - \frac{p_3^2}{8}\right).$$

Із рівняння (25) знайдемо параметр C_2:

$$C_2 = \frac{3}{1+e^{-4\sqrt{2}}}\left[\frac{1}{2} - A_0 a_2\left(1+e^{-2p_1}\right) - B_0 a_4\left(1+e^{-2p_3}\right)\right].$$

На основі визначення прямих диференціальних спектрів по змінній *y* вираз другого рівняння системи (23) зліва можна записати у вигляді $\left.\frac{\partial u_1(x,y)}{\partial y}\right|_{\substack{x=0\\y=0}} = \left.\frac{\partial u_2(x,y)}{\partial y}\right|_{\substack{x=0\\y=0}}$.

Диференціюючи по y відповідні вирази (13) і (19) із подальшою підстановкою визначаємо із нього параметр C_4:

$$C_4 = \frac{1}{2(1+e^{-4\sqrt{6}})}\left[A^* \frac{p_1^2}{2}\left(1+e^{-2p_1}\right)a_2 + B^* \frac{p_3^2}{2}\left(1+e^{-2p_3}\right)a_4 - 1\right],$$

де введено позначення:

$$A^* = -\frac{3}{4} + \frac{5}{96}p_1^2,\ B^* = -\frac{3}{4} + \frac{5}{96}p_3^2.$$

Розкриття третього і четвертого рівнянь системи (23) в області диференціальних зображень вимагає подвійного диференціювання виразів спочатку по x, а потім по y. Використовуючи властивості диференціальних перетворень можна визначити параметри a_2 і a_4:

$$a_2 = \frac{1}{D_{11}}\left(D_{01} - D_{12}a_4\right),\ a_4 = \frac{D_{02}D_{11} - D_{21}D_{01}}{D_{11}D_{22} - D_{21}D_{12}},$$

де:

$$D_{01} = \sqrt{2}\left(1-e^{-4\sqrt{2}}\right), \qquad D_{02} = 2\sqrt{6}\left(1-e^{-4\sqrt{2}}\right),$$

$$D_{11} = A_0\left[2\sqrt{2}\left(1-e^{-4\sqrt{2}}\right)\left(1+e^{-2p_1}\right) - p_1\left(1+e^{-4\sqrt{2}}\right)\left(e^{-2p_1}-1\right)\right],$$

$$D_{12} = B_0\left[2\sqrt{2}\left(1-e^{-4\sqrt{2}}\right)\left(1+e^{-2p_3}\right) - p_3\left(1+e^{-4\sqrt{2}}\right)\left(e^{-2p_3}-1\right)\right],$$

$$D_{21} = A^* p_1^2\left[\sqrt{6}\left(1-e^{-4\sqrt{6}}\right)\left(1+e^{-2p_1}\right) - \frac{p_1}{2}\left(1+e^{-4\sqrt{6}}\right)\left(e^{-2p_1}-1\right)\right],$$

$$D_{22} = B^* p_3^2\left[\sqrt{6}\left(1-e^{-4\sqrt{6}}\right)\left(1+e^{-2p_3}\right) - \frac{p_3}{2}\left(1+e^{-4\sqrt{6}}\right)\left(e^{-2p_3}-1\right)\right].$$

Визначення параметрів $\bar{a}_2$, $\bar{a}_4$, $\bar{C}_2$, $\bar{C}_4$ виконується аналогічним чином. Вираз для сталої $\bar{C}_2$:

$$\bar{C}_2 = \frac{3}{1+e^{-4\sqrt{2}}}\left[\frac{1}{2} + \frac{\bar{A}_0}{2}\left(e^{-2p_1}+1\right)\bar{a}_2 + \frac{\bar{B}_0}{2}\left(e^{-2p_3}+1\right)\bar{a}_4\right],\ \bar{A}_0 = \bar{A}\Big|_{y=0} = 1 - \frac{p_1^2}{24},$$

$$\bar{B}_0 = \bar{B}\Big|_{y=0} = 1 - \frac{p_3^2}{24},$$

Стала $\bar{C}_4$ визначається як:

$$\bar{C}_4 = \frac{-1}{2(1+e^{-4\sqrt{6}})}\left(1 + \left(\bar{A}_0 - \frac{p_1^2}{12}\right)\left(1+e^{-2p_1}\right)\bar{a}_2 + \left(\bar{B}_0 - \frac{p_3^2}{12}\right)\left(1+e^{-2p_3}\right)\bar{a}_4\right).$$

Параметри $\bar{a}_2$, $\bar{a}_4$ розраховуються із наступних виразів відповідно:

$$\bar{a}_2 = \frac{1}{\bar{D}_{11}}\left(\bar{D}_{01} - \bar{D}_{12}\bar{a}_4\right),\ \bar{a}_4 = \frac{\bar{D}_{02}\bar{D}_{11} - \bar{D}_{21}\bar{D}_{01}}{\bar{D}_{11}\bar{D}_{22} - \bar{D}_{21}\bar{D}_{12}},$$

де введено такі позначення:

$$\bar{D}_{01} = \sqrt{2}\left(1-e^{-4\sqrt{2}}\right),\ \bar{D}_{11} = \bar{A}_0\left[\frac{p_1}{2}\left(1+e^{-4\sqrt{2}}\right)\left(e^{-2p_1}-1\right) - \sqrt{2}\left(1-e^{-4\sqrt{2}}\right)\left(e^{-2p_1}+1\right)\right],$$

$$\bar{D}_{02} = 2\sqrt{6}\left(1-e^{-4\sqrt{6}}\right),\ \bar{D}_{12} = \bar{B}_0\left[\frac{p_3}{2}\left(1+e^{-4\sqrt{2}}\right)\left(e^{-2p_3}-1\right) - \sqrt{2}\left(1-e^{-4\sqrt{2}}\right)\left(e^{-2p_3}+1\right)\right],$$

$$\bar{D}_{21} = \left[p_1\left(1-\frac{p_1^2}{8}\right)\left(1+e^{-4\sqrt{6}}\right)\left(e^{-2p_1}-1\right) - 2\sqrt{6}\left(\bar{A}_0 - \frac{p_1^2}{12}\right)\left(1-e^{-4\sqrt{6}}\right)\left(1+e^{-2p_1}\right)\right],$$

$$\overline{D}_{22}=\left[p_3\left(1-\frac{p_3^2}{8}\right)\left(1+e^{-4\sqrt{6}}\right)\left(e^{-2p_3}-1\right)-2\sqrt{6}\left(\overline{B}_0-\frac{p_3^2}{12}\right)\left(1-e^{-4\sqrt{6}}\right)\left(1+e^{-2p_3}\right)\right].$$

Підстановка параметрів C_2, C_4, $\overline{C}_2$ і $\overline{C}_4$ у вирази (13)–(14) повністю визначає розв'язок задачі в зоні Ω_1. Аналогічно, підстановка параметрів a_2, a_4, $\overline{a}_2$ і $\overline{a}_4$ в вирази (19) –(20) дозволяє отримати аналітичний розв'язок крайової задачі в зоні Ω_2.

Також було виконано порівняння результатів моделювання теплового поля (1) методом на основі алгебричних властивостей диференціальних спектрів з результатами розв'язку задачі в [4] із застосуванням методу R-функцій [8] та результатами моделювання методом на основі алгебричних властивостей диференціальних спектрів [5]. Отримані результати подано на рис. 2.

Застосування методу моделювання фізичних полів на основі алгебричних властивостей диференціальних спектрів дозволило отримати аналітичну модель теплового поля.

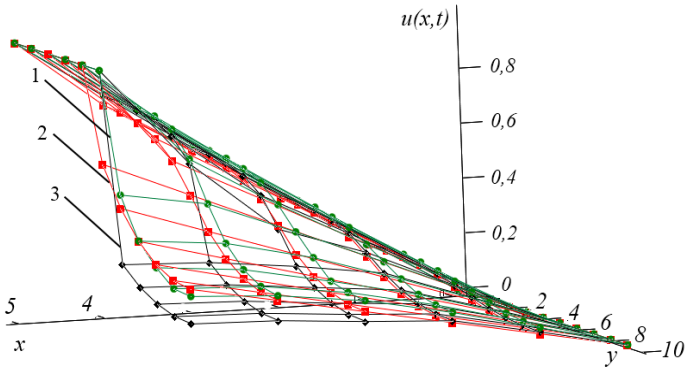

Рис. 2. Результати моделювання теплового поля смарт-карти:
1 – моделювання системою одномірних диференціальних спектрів;
2 – метод R-функцій; 3 – метод на основі алгебричних властивостей

Отримана в аналітичному вигляді математична модель теплового поля смарт-карти може розглядатися як модель технічного каналу витоку інформації і у подальшому застосовуватися при створенні захищених модулів аутентифікації в комп'ютеризованих системах.

ЛІТЕРАТУРА

1. Персиков А.В. Защита информации в телекоммуникационных системах: Учебник в 2х томах [Текст] / А.В. Персиков, В.В. Поповский. – Харьков: ООО "Компания СМИТ", 2006. – Т. 2. – 292 с.
2. Малюк А.А. Введение в защиту информации в автоматизированных системах [Текст] / А.А. Малюк, С.В. Пазизин, Н.С. Погожин – М.: Горячая линия-Телеком, 2001. – 148 с.
3. Бахвалов Н.С. Численные методы [Текст] / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. – М.: БИНОМ, 2003. – 632 с.
4. Баранов В.Л. Метод моделювання фізичних процесів на основі диференціальних перетворень нелінійних крайових задач / В.Л. Баранов, С.В. Водоп'ян, Р.М. Костюченко // Вісник ЖДТУ. – 2007. – №2 (41). – С. 59–65.
5. Баранов В.Л. Метод моделювання фізичних полів і процесів на основі прямих і зворотних диференціальних спектрів / В.Л. Баранов, Р.М. Костюченко, К.В. Молодецька // Вісник ЖДТУ. – 2009. – №2 (49). – С. 59–68.
6. Пухов Г.Е. Дифференциальные спектры и модели / Пухов Г.Е. – Киев: Наук. думка, 1990. – 184 с.
7. Пухов Г.Е. Дифференциальные преобразования и математическое моделирование физических процессов / Пухов Г.Е.. – Киев: Наук. думка, 1986. – 158 с.
8. Рвачев В.Л. Алгебра логики и интегральные преобразования в краевых задачах / В.Л. Рвачев, А.П. Слесаренко. – Киев: Наук. думка, 1976. – 288 с.

Надійшла: 8.10.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.