УДК 681.327.11

Н. В. Сачанюк-Кавецька
Вінницький Національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Визначення чутливості ідентифікаційної функції до зміни вхідних характеристик обробки зображень для розпізнавання суб'єктів у системах захисту інформації

Розглянуто особливості операції диференціювання логіко-часових функцій за змінною з метою визначення чутливості ідентифікаційної функції до зміни вхідних характеристик зображень, що використовуються для розпізнавання суб'єктів у системах захисту інформації, та основні властивості такої операції.

Ключові слова: *логіко-часова функція, похідна за змінною, розпізнавання зображень.*

Вступ

Використання інформаційних комп'ютерних систем для вирішення управлінських і підприємницьких завдань, стратегічного розвитку, підвищення ефективності адміністративної діяльності, планування і аналізу, реалізації у мережевому режимі різноманітних зв'язків підприємств з їхніми партнерами, клієнтами, владними структурами призвело до зростання інформаційних потреб, дало можливість не обмежувати інформаційні потоки та інформаційні процеси межами окремого підприємства і зумовило зростання інвестицій у комп'ютерні технології. Інформація та інформаційні системи, мережі, в яких вона функціонує, є важливими ресурсами організації [1]. Їхні доступність, цілісність і конфіденційність можуть мати особливе значення для забезпечення конкурентноспроможності організації, руху коштів, рентабельності, відповідності правовим нормам та іміджу організації. Водночас, унаслідок посилення залежності організацій від інформаційних, комунікаційних систем і послуг вони можуть стати більш вразливими до порушень режиму безпеки. Поширення інформаційних і комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості спеціалістів централізовано контролювати інформаційні системи та мережі. Тому актуальним є питання захисту інформації від несанкціонованих управлінських дій і доступу сторонніх осіб або програм до комп'ютерних даних.

Огляд проблем і постановка задачі створення засобів ідентифікації суб'єктів в системах захисту інформації

Система ідентифікації суб'єктів є одним із ключових моментів інфраструктури захисту від несанкціонованого доступу. Задачею систем ідентифікації є визначення та верифікація набору повноважень суб'єкта при доступі до інформаційних систем. Ідентифікація — це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). Існує три найпоширеніші види ідентифікації [2, 3]: парольна, апаратна та біометрична. При парольній ідентифікації кожен зареєстрований користувач будь-якої системи одержує набір персональних реквізитів, які він повторює при кожній спробі входу до системи. Перевага такого підходу — простота реалізації і використання, мінімізація витрат. Головним недоліком даного виду ідентифікації є величезна залежність надійності від користувачів. При апаратній ідентифікації визначення особистості користувача ґрунтується на якомусь «ключі», що перебуває в його ексклюзивному користуванні. Головною перевагою застосування апаратної ідентифікації є досить висока надійність. Слід відмітити, що найбільш серйозною небезпекою такої ідентифікації є можливість крадіжки зловмисниками токенів або карт (проксіміті, смарт, магнітних тощо) у зареєстрованих користувачів, плюс їхня висока ціна. Останнім часом досягнуто успіхів у розробці біометричних методів, що базуються на ідентифікації людини за унікальними, властивими тільки їй біологічними ознаками. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Головною перевагою біометричних технологій є найвища надійність (див. таблицю). Біометричним методам присвятили свої роботи Г.Ф. Лакин, Г.А. Кухарев, Я.Ю. Варецький, О.В. Дубчак, К.І. Підгайна, А.О. Лавданський, Ц. Мацумото, Києн Хоанг Чунг, Ч. Стюарт та інші. Можливими проблемами біометричних систем доступу є ймовірність перехоплення інформації під час її передачі від сканера до бази даних, а також несанкціонований доступ до масиву еталонних записів. Зрозуміло, що значно вищу ефективність дає застосування ідентифікації суб'єкта, що заснована на різних біометричних методах.

Порівняльні характеристики біометричних систем

№№ з/п	Модель	Біометричний метод	Імовірність несанкціонованого допуску	Імовірність помилкового допуску
1	Eyedentify ICAM	Сітківка ока	0,0001	0,4
2	Iriscan	Райдужка ока	0,0008	0,0007
3	FingerScan	Відбиток пальця	0,0001	1,0
4	BioMet	Геометрія руки	0,1	0,1
5	Vocord (2D)	Геометрія обличчя	0,01	0,2
6	Hitachi VeinID	Вени руки	0,0008	0,01

Такий підхід можна реалізувати в логіко-часовому середовищі, перетворивши всі параметри суб'єкта ідентифікації на логіко-часові функції (ЛЧФ) [4]. Далі ЛЧФ-характеристики ранжують за мірою важливості, а на основі синтезованих ознак формують ідентифікаційну ЛЧФ (фактично шифровані дані), яка є унікаль-

ною для даного суб'єкта. Ідентифікують суб'єкт шляхом порівняння отриманої ідентифікаційної функції з еталонними зразками бази знань. За умови неповної ідентифікації здійснюється розширення бази знань шляхом запису отриманого результату порівняння в пам'ять як нового зразка та визначення найбільш близького до отриманого еталонного зразка.

Однією з важливих проблем такої ідентифікації зображень є тестування чутливості логіко-часової ідентифікаційної функції по входу до зміни характеристик об'єкта, який ми ідентифікуємо. Оскільки розпізнавання базується на виділенні контурів зображення, що в свою чергу пов'язане з операцією диференціювання, то, як варіант, доцільно перевіряти чутливість ідентифікаційної функції, використовуючи поняття похідної ЛЧФ. Тому актуальною є розробка способу визначення істотних та неістотних характеристик, що формують ідентифікаційну функцію.

Метою даної статті є розробка способу, який дозволяв би визначати істотні та неістотні характеристики об'єкта розпізнавання, який описується ідентифікаційною ЛЧФ.

Основні положення

Існує три можливі класи ЛЧФ [4]:

1) функції, що між двома нулями приймають стале значення, позначають такі функції $f(t,t_1,T_1,a_1)$;

2) ЛЧФ, які мають m часових координат, причому відрізки їхнього існування не перетинаються, позначають такі функції $f(t,t_1,...,t_m,T_1,...,T_m,a_1,...,a_m)$;

3) монотонні функції (зростаючі чи спадні).

Одним із можливих способів подання функцій другого та третього класів є суперпозиція функцій першого класу, яка виконується за допомогою операції нерівнозначного віднімання ($|k|$), що базується на введеному попередньо понятті Δ-розбиття [3]:

$$f_1(t,t_{11},T_{11},a_1)|k|f_2(t,t_{21},T_{21},a_2)=\{(t-(t_1+i\Delta_i))\cdot|a_{i1}-a_{i2}|,\ t_1=\min(t_{11},t_{21})\},$$

де t_{11}, t_{21} — часові координати змінних; T_{11} та T_{21} — тривалості відрізків існування першої і другої функцій; a_1 та a_2 — відповідні амплітуди; i — кількість Δ-інтервалів в обраному часовому інтервалі, Δ_i — тривалість Δ-інтервалу; a_{i1}, a_{i2} — відповідні амплітуди на i-му Δ-інтервалі.

Результатом цієї операції буде знову ЛЧФ, яку можна назвати нерівнозначною різницею.

Наприклад, ЛЧФ

$$f(t,t_1,t_2,T_1,T_2,a_1,a_2)=\begin{cases}(t-t_1)a_1, & якщо \quad t_1\le t\le t_1+T_1\\ (t-t_2)a_2, & якщо \quad t_2\le t\le t_2+T_2\\ 0, & якщо \quad (t<t_1)\wedge(t_1+T_1<t<t_2)\wedge(t>t_2+T_2)\end{cases}$$

може бути подана так:

$$f(t,t_1,t_2,T_1,T_2,a_1,a_2) = f_1(t,t_1,T_1,a_1)\,|k|\,f_2(t,t_2,T_2,a_2),$$

де

$$f_1(t,t_1,T_1,a_1) = \begin{cases} (t-t_1)a_1, & якщо \quad t_1 \le t \le t_1+T_1, \\ 0, & якщо \quad (t<t_1)\wedge(t>t_1+T_1), \end{cases}$$

$$f_2(t,t_2,T_2,a_2) = \begin{cases} (t-t_2)a_2, & якщо \quad t_2 \le t \le t_2+T_2, \\ 0, & якщо \quad (t<t_2)\wedge(t>t_2+T_2). \end{cases}$$

Функції $f_1(t,t_1,T_1,a_1)$ та $f_2(t,t_2,T_2,a_2)$ будемо називати змінними. Враховуючи нові позначення, функцію з попереднього прикладу можна записати так:

$$f(t,t_1,t_2,T_1,T_2,a_1,a_2) = f_1(t,t_1,T_1,a_1)\,|k|\,f_2(t,t_2,T_2,a_2) = F(f_1,f_2).$$

Як спосіб тестування чутливості ЛЧФ $F(f_1,f_2,...,f_n)$ по входу можна запропонувати диференціювання цієї функції за змінною f_i, $i=\overline{1,n}$.

Нехай маємо функцію:

$$f(t,t_1,...,t_m,T_1,...,T_m,a_1,...,a_m) = f_1(t,t_1,T_1,a_1)\,|k|\,f_2(t,t_2,T_2,a_2)\,|k|\,...\,|k|\,f_m(t,t_m,T_m,a_m) = \\ = F(f_1,f_2,...,f_m).$$

Похідною ЛЧФ $F(f_1,f_2,...,f_m)$ за змінною f_i, $i=\overline{1,n}$, будемо називати нерівнозначну різницю цієї функції та $\overline{f_i}$, яку позначимо:

$$\frac{\partial F}{\partial f_i} = F\,|k|\,\overline{f_i}.$$

Можливий графічний результат такого диференціювання зображено на рис. 1.

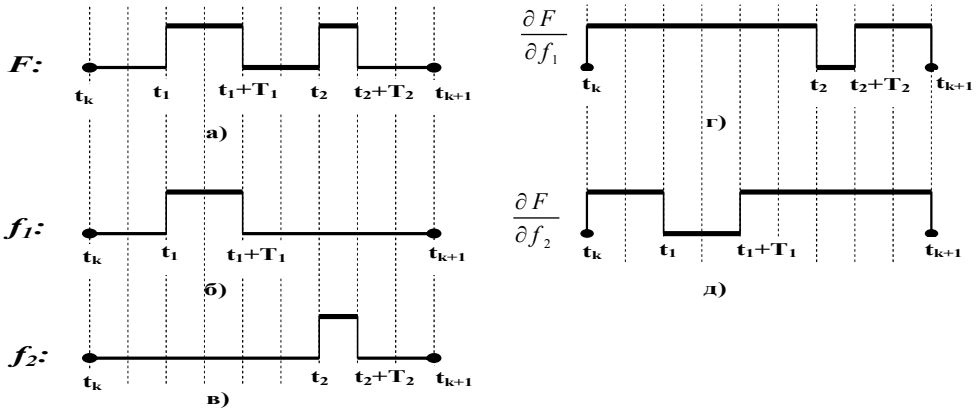

Рис. 1. Похідна ЛЧФ другого класу за змінною: а) початкова ЛЧФ; б), в) змінні початкової ЛЧФ; г) похідна ЛЧФ за першою змінною; д) похідна ЛЧФ за другою змінною

Зауваження.

1. Якщо позначити $a = \max\{a_1, a_2, ..., a_m\}$, то

$$\overline{f_i} = \begin{cases} (t - t_k)a, & якщо \quad t_k < t < t_i, \\ (t - t_i)|a - a_i|, & якщо \quad t_i \le t \le t_i + T_i, \\ (t - (t_i + T_i))a, & якщо \quad t > t_i + T_i. \end{cases}$$

2. Для функцій другого класу:

$$\frac{\partial F}{\partial f_i} = \begin{cases} (t - t_k)a, & якщо \quad t_k < t < t_1, \\ (t - t_1)|a - a_1|, & якщо \quad t_1 \le t \le t_1 + T_1, \\ (t - (t_1 + T_1))a, & якщо \quad t_1 + T_1 < t < t_2, \\ \vdots \\ (t - t_i)|2a_i - a|, & якщо \quad t_i \le t \le t_i + T_i, \\ (t - (t_i + T_i)), & якщо \quad t_i + T_i < t < t_{i+1}. \\ \vdots \end{cases}$$

3. Для класу монотонних функцій:

$$\frac{\partial F}{\partial f_i} = \begin{cases} (t - t_k)a, & якщо \quad t_k < t < t_1 \\ (t - t_1)|a - a_1|, & якщо \quad t_1 \le t \le t_1 + T_1, \\ (t - (t_1 + T_1))|a - a_2|, & якщо \quad t_1 + T_1 < t < t_2, \\ \vdots \\ (t - (t_1 + T_1 + ... + T_{i-1}))|2a_i - a|, & якщо \ t_1 + T_1 + ... + T_{i-1} \le t \le t_1 + T_1 + ... + T_{i-1} + T_i. \\ \vdots \end{cases}$$

Іноді виникає практична потреба розглянути похідну ЛЧФ за деякою ЛЧФ першого класу, яка не приймає участь у побудові ідентифікаційної функції.

Нехай маємо $f(t, t_1, ..., t_m, T_1, ..., T_m, a_1, ..., a_m) = F(f_1, f_2, ..., f_m)$ та деяку функцію $f_{m+1}(t, t_{m+1}, T_{m+1}, a_{m+1})$, $t_{m+1} \ne t_i, \quad i = \overline{1, m}$. Часова координата t_{m+1} може знаходитись або лівіше часової координати t_1, або правіше часової координати $t_m + T_m$, або знаходитися між часовими координатами даної ЛЧФ (відрізки існування не перетинаються). Тоді похідною ЛЧФ $F(f_1, f_2, ..., f_m)$ за змінною f_{m+1} будемо називати нерівнозначну різницю цієї функції та $\overline{f_{m+1}}$, яку позначимо:

$$\frac{\partial F}{\partial f_{m+1}} = F|k|\overline{f_{m+1}}.$$

Для знаходження інверсії функції $f_{m+1}(t, t_{m+1}, T_{m+1}, a_{m+1})$ оберемо $a = \max\{a_1, a_2, ..., a_m\}$, тоді:

$$\frac{\partial F}{\partial f_{m+1}} = \begin{cases} \vdots \\ (t - t_i)|a - a_i|, \quad якщо \quad t_i \le t \le t_i + T_i, \\ (t - (t_i + T_i))a, \quad якщо \quad t_i + T_i < t < t_{i+1}, \\ \vdots \\ (t - t_{m+1})|2a_{m+1} - a|, \quad якщо \quad t_{m+1} \le t \le t_{m+1} + T_{m+1}, \\ (t - (t_{m+1} + T_{m+1})), \quad якщо \quad t_{m+1} + T_{m+1} < t < t_p. \\ \vdots \end{cases}$$

Зауваження. Для збереження монотонності функцій t_{m+1} має знаходитися лівіше координати t_1 ($a_{m+1} < a_1, \quad t_{m+1} + T_{m+1} = t_1$), або t_{m+1} має знаходитися правіше координати t_m ($a_{m+1} > a_m$) для зростаючих функцій.

У першому випадку:

$$\frac{\partial F}{\partial f_{m+1}} = \begin{cases} (t - t_k)a, \quad якщо \quad t_k < t < t_{m+1}, \\ (t - t_{m+1})|a - a_{m+1}|, \quad якщо \quad t_{m+1} \le t \le t_1, \\ (t - t_1)|a - a_1|, \quad якщо \quad t_1 \le t \le t_1 + T_1, \\ (t - (t_1 + T_1))|a - a_2|, \quad якщо \quad t_1 + T_1 < t < t_1 + T_1 + T_2, \\ \vdots \end{cases}$$

а в другому випадку:

$$\frac{\partial F}{\partial f_{m+1}} = \begin{cases} (t - t_k)a, \quad якщо \quad t_k < t < t_1, \\ (t - t_1)|a - a_1|, \quad якщо \quad t_1 \le t \le t_1 + T_1, \\ \vdots \\ (t - (t_{m+1} + T_{m+1}))a, \quad якщо \quad t > t_{m+1} + T_{m+1}, \\ 0, \quad якщо \quad t_{m+1} \le t \le t_{m+1} + T_{m+1}. \end{cases}$$

Для спадних функцій формули будуть аналогічними з точністю до симетрії.

Можливий результат такого диференціювання показано на рис. 2.

Деякі властивості похідної ЛЧФ за змінною ілюструють наступні теореми.

Теорема 1.

$$\frac{\partial^2 F(f_1, f_2, ..., f_m)}{\partial f_{m+1}^2} = F(f_1, f_2, ..., f_m).$$

Доведення.

$$\frac{\partial F(f_1, f_2, ..., f_m)}{\partial f_{m+1}} = F(f_1, f_2, ..., f_m)|k|\overline{f_{m+1}},$$

а

$$\frac{\partial^2 F(f_1, f_2, ..., f_m)}{\partial f_{m+1}^2} = \left(F(f_1, f_2, ..., f_m)\middle|k\middle|\overline{f_{m+1}}\right)\middle|k\middle|\overline{f_{m+1}} = F(f_1, f_2, ..., f_m)\middle|k\middle|0 = F(f_1, f_2, ..., f_m).$$

Що і треба було довести.

Аналогічним чином можна довести, що

$$\frac{\partial^2 F(f_1, f_2, ..., f_m)}{\partial f_i^2} = F(f_1, f_2, ..., f_m), \quad i = \overline{1, m}.$$

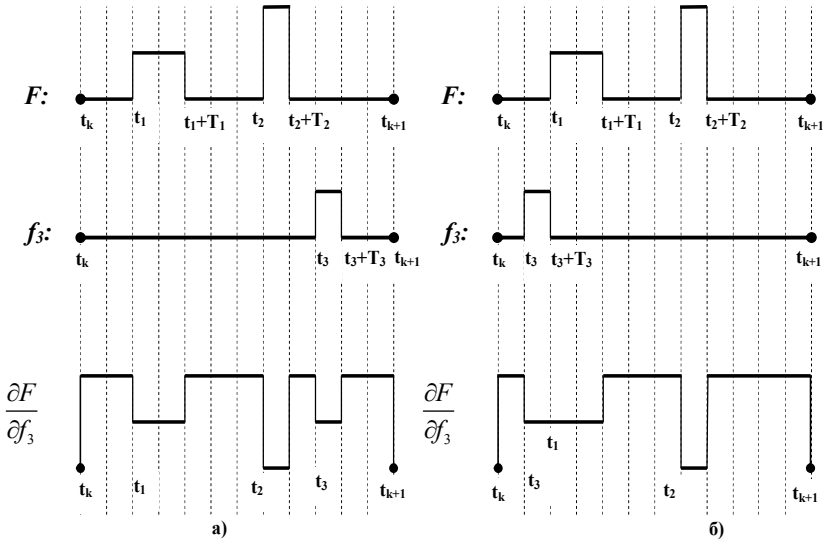

Рис. 2. Обчислення похідної ЛЧФ за змінною, що не входить у дану функцію:
а) випадок $t_3 > t_2 + T_2$; б) випадок $t_3 < t_1$

Теорема 2.

Нехай маємо дві ЛЧФ $F(f_1, f_2, ..., f_i, ..., f_n)$ та $F^*(f_1, f_2, ..., \overline{f_i}, ..., f_n)$. Тоді $\frac{\partial F^*}{\partial f_i} = F(f_1, f_2, ..., f_{i-1}, f_{i+1}, ..., f_n)$.

Доведення.

Доведемо теорему методом математичної індукції для класу монотонних функцій.

Доведемо базу індукції. Нехай маємо деяку зростаючу функцію $F(t, t_1, T_1, T_2, a_1, a_2)$, $a_1 < a_2$, $a_2 = 2a_1$. Дану ЛЧФ можна подати як нерівнозначну різницю функцій $f_1(t, t_1, T_1, a_1)$ та $f_2(t, t_1 + T_1, T_2, a_2)$, тобто:

$$F(f_1, f_2) = f_1(t, t_1, T_1, a_1)\middle|k\middle|f_2(t, t_1 + T_1, T_2, a_2) =$$

$$= \begin{cases} (t - t_1)a_1, & якщо \quad t_1 \le t \le t_1 + T_1, \\ (t - t_2)a_2, & якщо \quad t_1 + T_1 \le t \le t_1 + + T_1 + T_2, \\ 0, & якщо \quad (t < t_1) \wedge (t > t_1 + T_1 + T_2). \end{cases}$$

Тоді знайдемо, наприклад, ЛЧФ $F^*(f_1, \overline{f_2})$:

$$F^*(f_1, \overline{f_2}) = \begin{cases} (t - t_k)a_2, & якщо \quad t_k \le t < t_1, \\ (t - t_1)a_1, & якщо \quad t_1 \le t \le t_1 + T_{,1} \\ (t - (t_1 + T_1 + T_2))a_2, & якщо \quad t > t_1 + T_1 + T_2, \\ 0, & якщо \quad t_1 + T_1 \le t \le t_1 + T_1 + T_2 \end{cases}$$

і обчислимо похідну даної функції за змінною $f_2\left(t, t_1 + T_1, T_2, a_2\right)$. Згідно означення маємо

$$\frac{\partial F^*(f_1, \overline{f_2})}{\partial f_2} = \begin{cases} (t - t_1)\left|a_2 - a_1\right|, & якщо \quad t_1 \le t \le t_1 + T_1, \\ 0, & якщо \quad \left(t_k \le t < t_1\right) \wedge \left(t > t_1 + T_1\right), \end{cases}$$

оскільки

$$\overline{f_2} = \begin{cases} (t - t_k)a_2, & якщо \quad t_k \le t < t_1 + T_1, \\ (t - (t_1 + T_1 + T_2))a_2, & якщо \quad t > t_1 + T_1 + T_2, \\ 0, & якщо \quad t_1 + T_1 \le t \le t_1 + T_1 + T_2. \end{cases}$$

Тобто $\frac{\partial F^*(f_1, \overline{f_2})}{\partial f_2} = F(f_1)$.

Аналогічним чином можна показати, що $\frac{\partial F^*(\overline{f}_1, f_2)}{\partial f_1} = F(f_2)$.

Припустимо, що теорема має місце при $n = k$. Нехай

$$\frac{\partial F^*(f_1, f_2, ..., \overline{f_i}, ..., f_k)}{\partial f_i} = F(f_1, f_2, ..., f_{i-1}, f_{i+1}, ..., f_k).$$

Покажемо, що теорема має місце при $n = k + 1$. Враховуючи припущення маємо:

$$\frac{\partial F^*(f_1, f_2, ..., \overline{f_i}, ..., f_k, f_{k+1})}{\partial f_i} = \frac{\partial (F^*(f_1, f_2, ..., \overline{f_i}, ..., f_k)|k|f_{k+1})}{\partial f_i} =$$

$$= F(f_1, f_2, ..., f_{i-1}, f_{i+1}, ..., f_k)|k|f_{k+1} = F(f_1, f_2, ..., f_{i-1}, f_{i+1}, ..., f_k, f_{k+1}).$$

Згідно принципу математичної індукції теорема має місце для будь-якого натурального n.

Графічну ілюстрацію теореми 2 подано на рис. 3.

Можливість співставлення об'єкта ідентифікації відповідної ЛЧФ, що включає всі його біометричні характеристики дозволить істотно підвищити надійність ідентифікації. А математична обробка ідентифікаціної ЛЧФ та використання розробленої програми «Модель ЛЧФ» дозволяє в короткі терміни визначити най-

більш істотні характеристики об'єкта та прогнозувати зміни цієї функції відповідно до змін певних характеристик [5].

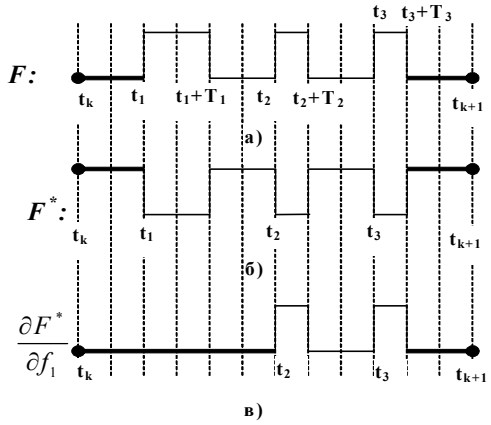

Рис. 3. Ілюстрація до теореми 2: а) початкова ЛЧФ; б) ЛЧФ F^* на наборі $\overline{f_1}, f_2, f_3$;
в) похідна ЛЧФ F^* за змінною f_1

Висновок

Похідна логіко-часової ідентифікаційної функції за змінною, яка не входить до цієї функції, дозволяє підвищити ефективність процесу розпізнавання суб'єктів для систем захисту інформації, шляхом введення нових істотних характеристик об'єкта ідентифікації і може використовуватись як алгоритм шифрування. Крім того, похідну за змінною можна використовувати для аналізу та діагностики комбінаційніх схем.

1. Устенко А.О., Василик І.І. Методи дослідження інформаційних потоків підприємств. *Науковий вісник Херсонського доржавного університету. Серія Економічні науки.* 2014. Вип. 9. Ч. 2. С. 218–222.

2. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів. *Інфокомунікаційні системи. Серія Системи обробки інформації.* 2013. Вип. 6 (113). С. 215–223.

3. Чередниченко В.Б., Чередниченко К.Е. Біометричні методи у системах захисту інформації. *Захист інформації в інформаційно–телекомунікаційних системах. Серія Системи обробки інформації.* 2012. Вип. 4(102). Т. 1. С. 145–148.

4. Сачанюк-Кавецька Н.В., Кожем'яко В.П. Елементи око-процесорної обробки зображень в логіко-часовому середовищі: монографія. Вінниця: УНІВЕРСУМ, 2004. 135 с.

5. Сачанюк-Кавецька Н.В. Математичне виділення контурів зображення в логіко-часовому середовищі: сб. статей научно-информационного центра «Знание» по материалам международной заочной научно-практической конференции: «Развитие науки в XXI веке». 2 часть. г. Харьков: сб. со статьями (уровень стандарта, академический уровень). Харьков: Научно-информационный центр «Знание», 2016. С. 91–97.

Надійшла до редакції 10.03.2017