УДК 004.056.52

Т.Ю. УТКІНА, О.С. ВЕРБИЦЬКИЙ, А.Г. ЛУКАШЕНКО
Черкаський державний технологічний університет

УЗАГАЛЬНЕНА БІОМЕТРИЧНА МОДЕЛЬ ДОСТУПУ ДО МІКРОПРОЦЕСОРНОЇ СИСТЕМИ КЕРУВАННЯ СПЕЦІАЛІЗОВАНОГО ЛАЗЕРНОГО ТЕХНОЛОГІЧНОГО КОМПЛЕКСУ

Запропонована узагальнена біометрична модель доступу за відбитком пальця. Визначений метод для виявлення резерву в основних технічних параметрах компонентів розроблюваної біометричної системи доступу до мікропроцесорної системи керування спеціалізованого лазерного комплексу, на основі теорії неповної подібності та розмірностей. Виявлений енергетичний резерв в ІС пам'яті SRAM. Запропонована база даних комп'ютерних компонентів, що прискорює процес створення біометричних систем безпеки будь-якої складності.

The general biometric model of access on the imprint of finger is offered. The method to identify the reserve of the main technical parameters of components of the developed biometric system for access to the microprocessor system of control the specialized laser complex, is defined on the basis of theory of incomplete similarity and dimensions. The power reserve is revealed in memory IC of SRAM. The database of these computer components is offered that accelerates the process of creation of the biometric systems of safety of any complication.

Ключові слова: біометрична система доступу, мікропроцесорна система керування, спеціалізований лазерний технологічний комплекс.

Вступ. Актуальність теми

Спеціалізовані лазерні технологічні комплекси (СЛТК) знаходять все більш широке застосування у науці, різних галузях виробництва: машинобудівній, електротехнічній, приладобудівній, автомобільній тощо.

Відмінною особливістю застосування лазерів у виробничих процесах є значне перевищення безпечного рівня енергії (потужності) випромінювання та невидимість для людського ока лазерного випромінювання.

Поряд з технологічними і технічними аспектами забезпечення надійності та функціональної безпеки СЛТК, як складної організаційно-технічної системи не менш важливу роль відіграє людський фактор, в якості однієї з характеристик якого виступає рівень професійної підготовки працівників. Оскільки неналежний рівень кваліфікації працівників несе загрозу несанкціонованого доступу до мікропроцесорної системи керування СЛТК, що в результаті може призвести до непередбачуваних наслідків.

Отже, при проектуванні СЛТК задача запобігання несанкціонованому втручанню як при експлуатації технологічного лазерного обладнання, так і при організації моніторингу доступу до мікропроцесорної системи керування відповідає актуальності.

Постановка задачі

Метою роботи є розробка узагальненої біометричної моделі доступу до мікропроцесорної системи керування СЛТК, яка передбачає створення бар'єра для будь-якого несанкціонованого втручання (заборону доступу) в процес функціонування. При фізичному моделюванні комп'ютерних компонентів мета роботи – визначити метод створення їх бази даних з найкращими технічними характеристиками.

Розв'язання проблемної задачі

1. Розробка узагальненої моделі біометричної системи доступу

Для досягнення поставленої мети необхідно визначити:

- існуючі сучасні комп'ютерні компоненти біометричної системи доступу;
- метод створення бази даних основних комп'ютерних компонентів.

В роботі [1] пропонується включити до складу комп'ютерної системи контролю безпеки мікропроцесорної системи керування СЛТК біометричну систему доступу, де ознакою є відбитки пальця. Ця система є доступною завдяки простоті й дозволить реалізувати такі функції, як моніторинг входу, доступ до мікропроцесорної системи керування, реєстрацію спроб порушення та ін.

Для реалізації процедури ідентифікації людини за відбитками пальців, як правило, використовують спеціалізовані дактилоскопічні *сканери* однієї з відомих фірм-виробників: "Bio-link Technologics", "Bioscrypt", "Precise Biometries", "Neurotechnologiya", "Digital Persona", "Ethentica", "Indentix", "Staflink", "Veridicom" тощо. При обранні *перетворюючого пристрою* особливу увагу звертають на такі відмінні риси, як висока роздільна здатність, малі габарити і мала вага, висока швидкість сканування, а також стійкість до механічних і кліматичних впливів.

В якості *обчислювального пристрою*, що реалізує функцію обробки зчитаної інформації, звичайно використовують мікропроцесор, або мікроконтролер, або цифровий сигнальний процесор (DSP-процесор). При цьому під обробкою інформації мається на увазі поліпшення зображення, нормалізація, формування зразка, порівняння зразка з отриманим зображенням тощо. З усіма цими завданнями біометричних систем доступу як найкраще справляються *DSP-процесори*, оскільки залишають запас продуктивності, необхідний для майбутніх вдосконалень. Архітектура DSP-процесорів розроблена для виконання складних математичних алгоритмів (наприклад, операцію множення/додавання за один цикл). Роздільні шини доступу до пам'яті команд й даних дозволяють одночасно отримувати команди і операнди, що також збільшує

швидкість обчислень. Отже, *DSP-процесори* сприяють створенню біометричної системи доступу з малими габаритами, високою продуктивністю та низькою ціною [2– 6].

Для збереження бази даних зразків відбитків пальців, з якими проводиться порівняння в момент запиту доступу, використовуються *мікросхеми пам'яті* RAM- або Flash-типу, або сервер даних за допомогою вихідного інтерфейсу.

Якщо біометрична система доступу представляє собою *вбудований пристрій*, то, як правило, зв'язок з сервером здійснюється за *допомогою USB-інтерфейсу*. Причому, деякі мікропроцесори вже містять у своєму складі USB-інтерфейс, і в цьому випадку необхідний лише фізичний рівень USB. Якщо ж біометричний пристрій працює в мережі, зв'язок з сервером організується за допомогою вихідного інтерфейсу RS232, або RS485, або Ethernet чи ін.

На підставі аналізу існуючих сучасних комп'ютерних компонентів пропонується узагальнена модель біометричної системи доступу до мікропроцесорної системи керування СЛТК, яка представлена на рис. 1.

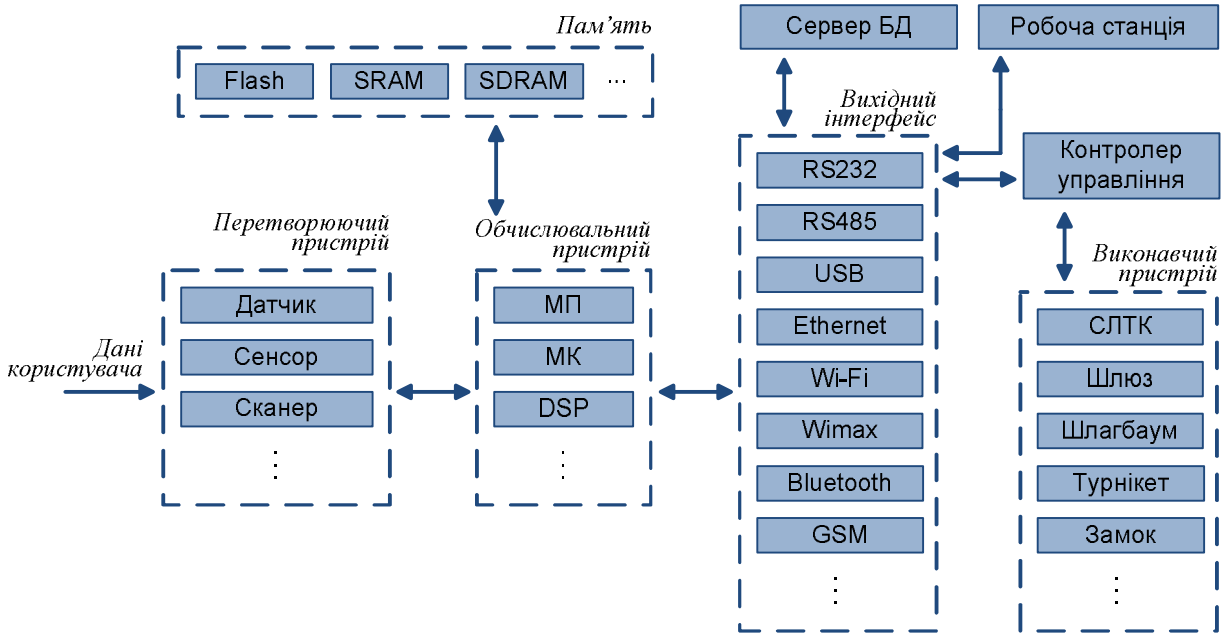

Рис. 1. Узагальнена модель біометричної системи доступу до мікропроцесорної системи керування СЛТК

З рис. 1 видно, що на базі запропонованої узагальненої моделі можливо побудувати відкриту для інтеграції з вже існуючим обладнанням, із розмежуванням прав доступу, розподілену біометричну систему доступу, де організацію зв'язку з віддаленими робочими станціями можна здійснювати за допомогою підключення до одного чи відразу до декількох вихідних інтерфейсів системи.

Наприклад, для об'єднання в одну мережу всіх точок доступу на підприємстві можна застосувати виділені лінії зв'язку Ethernet, або організувати спільну магістраль RS485 за рахунок відповідних перетворювачів (USB-RS485, LAN-RS485, GPRS-RS485) тощо.

Керування *виконавчими пристроями* здійснюється за допомогою контролера управління, зв'язок з яким відбувається по цифровому виділеному каналу, що, в свою чергу, унеможливлює несанкціонований доступ до приміщення шляхом перемикання дротів або імітації сигналу управління. Крім того, для об'єктів з підвищеними вимогами до безпеки пропонується застосовувати єдину систему енергозабезпечення периферійних пристроїв, де поряд з джерелами безперебійного живлення для сервера та комутаторів використовуються комутатори з підтримкою технології PoE (передача живлення 12 і 5 В по мережі Ethernet).

2. Визначення методу створення бази даних комп'ютерних компонентів для біометричних систем доступу

Для досягнення максимальної ефективності та експлуатаційної технологічності біометричної системи доступу до мікропроцесорної системи керування СЛТК необхідно використовувати високонадійні компоненти, які мають енергетичний резерв в існуючих мікросхемах.

Питанню визначення найкращих типів елементів пам'яті при проектуванні сучасних мікропроцесорних систем керування для СЛТК на базі теорії неповної подібності та розмірностей присвячено ряд робіт П.М. Алабужева, А.Н. Лебедєва, В.М. Лукашенко, Б.А. Шеховцова, А.П. Стахова та ін.

В роботах [7, 8] наведений алгоритм створення бази даних з використанням теорії неповної подібності та розмірностей, принципова відмінність якого базується на дотриманні подібності між оригіналом та моделлю тільки частини визначальних величин.

Послідовність рішення проблемної задачі включає наступні дії:

1. Визначення переліку основних технічних параметрів, який є адекватним для конкретного об'єкту, що розглядається.

2. Створення узагальненого математичного опису залежностей між параметрами об'єкту, що

розглядається.

3. Вибір методу визначення критеріїв подібності.

4. Створення критеріального рівняння.

5. Побудова знакової моделі.

Відомо, що більш перспективним є підхід щодо створення переліку визначальних величин за основними технічними параметрами елементів пам'яті, які характеризують енергетичні та швидкісні напрями пам'яті:

- $V_{об}$ – загальний об'єм пам'яті мікросхеми [біт];
- $V_{ряд}$ – довжина строки елемента пам'яті [біт];
- U – напруга споживання [В];
- I – струм споживання [мА];
- P_p – потужність розсіювання [мВт].

Потужність розсіювання обчислюється за формулою:

$$P_p = \frac{150 - T_C^o}{0.23}, \tag{1}$$

де T_c – максимальна температура, ^oC [7].

Для зниження апаратно-часових затрат потужним засобом є моделювання. Фізичне моделювання подібностей на основі аналізу розмірностей визначальних параметрів елементів пам'яті SRAM та використання π-теореми дозволяє просто реалізувати складні задачі при проектуванні сучасних мікропроцесорних систем керування для СЛТК. Перелік визначальних величин оригінала та моделі, аналіз розмірностей цих величин, наведених у табл. 1, дозволяють знайти умовні критерії подібності. Фізична модель відповідає п'яти умовам подібності двох об'єктів (оригіналу та моделі) завдяки їх фізичній однорідності [8].

Критеріальні співвідношення допомагають встановити якісні та кількісні зв'язки оригіналу й моделі, за допомогою яких можна отримати масштабні рівняння.

Достатньо складним процесом є побудова залежностей за відсутності математичного опису залежностей цих параметрів. Використання теорії розмірностей та пошуку критеріального рівняння дозволяє отримати узагальнений математичний опис залежності між параметрами мікросхем пам'яті, що набуває такого вигляду:

$$F(P_p, U, I, V_{об}, V_{ряд}) = 0. \tag{2}$$

Вибір методу визначення критеріїв подібності можна зробити на підставі стислого аналізу особливостей методів, що розглядаються.

Метод нульових ступенів представляє критерії у вигляді безрозмірного степеневого комплексу, який включає всі визначальні величини. Недоліком цього методу є складність.

Метод виключення розмірностей передбачає послідовне виключення із формул розмірностей визначальних величин всіх символів основних одиниць. Цей метод не набув широкого розповсюдження через неможливість виключення усіх символів основних одиниць.

В основі евристичного методу лежить підбір критеріїв подібності. Його відмітною особливістю є висока швидкість отримання результатів та проста реалізація. Тому для визначення критеріїв подібності в даному випадку як найкраще підходить евристичний метод [7].

При застосовуванні теорії неповної подібності та розмірностей визначальних величин за даними табл. 1, формули (2) та при використанні евристичного методу визначення умовних критеріїв подібності, критеріальне рівняння має наступний вигляд:

$$\Psi(P_p /(U \cdot I); V_{об} / V_{ряд}) = 0, \tag{3}$$

де $(V_{об}/V_{ряд})$ – коефіцієнт, величина якого пропорційна кількості адрес мікросхеми;

$(P_p/ (U{\cdot}I))$ – величина, яка характеризує енергетичний резерв мікросхеми.

Пропонується для визначення резерву взяти за основу такий комп'ютерний компонент розроблюваної біометричної системи доступу, як запам'ятовуючі пристрої типу SRAM. Це пов'язане з наявністю великої різноманітності на ринку запам'ятовуючих пристроїв типу SRAM, які сильно відрізняються за часом вибірки їх окремих комірок, обсягом інформації, що може зберігатися, та питомою вартістю зберігання однакового обсягу інформації.

Коефіцієнт $(V_{об}/V_{ряд})$ характеризує кількість адрес та їх контактів.

Отже, при зменшенні значення цього коефіцієнта:

- зменшується час вибірки, тобто збільшується швидкодія;
- підвищується надійність, завдяки збільшенню часу напрацювання до відмови;
- зростає відсоток виходу придатних виробів;
- зменшується собівартість мікросхем пам'яті;
- збільшується конкурентна спроможність ІС.

Величина $(P_p/ (U{\cdot}I))$ характеризує відношення між потужністю розсіювання та потужністю споживання, чим вона більша, тим кращими стають умови роботи мікросхеми та з'являється можливість її функціонального розширення за рахунок введення додаткових елементів.

Таблиця 1

Типи і перелік основних технічних параметрів елементів пам'яті SRAM

№	Тип ІС	$V_{об}$	Організація, $A \times V_{ряд}$	U, В	T_c, C^0	I, мА	P_p, мВт
1	K6E0804C1E	256K bit	64Kx4	5	70	70	0.9938
2	K6E0808C1C	256K bit	32Kx8	5	70	165	0.4216
3	K6E0808V1C	256K bit	32Kx8	3.3	70	90	1.1711
4	K6E0808V1E	256K bit	32Kx8	3.3	70	70	1.5057
5	K6R1004C1A	1M bit	256Kx4	5	70	150	0.4638
6	K6R1004C1D	1M bit	256Kx4	5	70	65	1.0702
7	K6R1004V1A	1M bit	256Kx4	3.3	70	130	0.8108
8	K6R1004V1B	1M bit	256Kx4	3.3	70	150	0.7027
9	K6R1004V1C	1M bit	256Kx4	3.3	85	68	1.2594
10	K6R1008C1A	1M bit	128Kx8	5	85	170	0.3325
11	K6R1008C1B	1M bit	128Kx8	5	70	160	0.4348
12	K6R1008C1C	1M bit	128Kx8	5	85	73	0.7743
13	K6R1008C1D	1M bit	128Kx8	5	85	65	0.8696
14	K6R1008V1A	1M bit	128Kx8	3.3	85	140	0.6117
15	K6R1008V1B	1M bit	128Kx8	3.3	85	160	0.5352
16	K6R1008V1C	1M bit	128Kx8	3.3	85	73	1.1731
17	K6R1008V1D	1M bit	128Kx8	3.3	85	65	1.3175
18	K6R1016C1A	1M bit	64Kx16	5	85	190	0.2975
19	K6R1016C1C	1M bit	64Kx16	5	85	93	0.6078
20	K6R1016V1A	1M bit	64Kx16	3.3	85	170	0.5038
21	K6R1016V1B	1M bit	64Kx16	3.3	85	200	0.4282
22	K6R1016V1D	1M bit	64Kx16	3.3	85	65	1.3175
23	K6R4004C1A	4M bit	1Mx4	5	85	150	0.3768
24	K6R4004C1B	4M bit	1Mx4	5	85	195	0.2899
25	K6R4004C1D	4M bit	1Mx4	5	70	65	1.0702
26	K6R4004V1B	4M bit	1Mx4	3.3	85	185	0.4629
27	K6R4004V1C	4M bit	1Mx4	3.3	85	130	0.6588
28	K6R4008C1A	4M bit	512Kx8	5	85	170	0.3325
29	K6R4008C1B	4M bit	512Kx8	5	85	210	0.2692
30	K6R4008C1C	4M bit	512Kx8	5	85	150	0.3768
31	K6R4008C1D	4M bit	512Kx8	5	85	65	0.8696
32	K6R4008V1B	4M bit	512Kx8	3.3	85	205	0.4178
33	K6R4008V1C	4M bit	512Kx8	3.3	85	135	0.6344
34	K6R4008V1D	4M bit	512Kx8	3.3	85	65	1.3175
35	K6R4016C1A	4M bit	256Kx16	5	85	210	0.2692
36	K6R4016C1B	4M bit	256Kx16	5	85	260	0.2174
37	K6R4016C1D	4M bit	256Kx16	5	85	65	0.8696
38	K6R4016V1B	4M bit	256Kx16	3.3	85	250	0.3426
39	K6R4016V1C	4M bit	256Kx16	3.3	85	140	0.6117
40	K6R4016V1D	4M bit	256Kx16	3.3	85	65	1.3175

На базі критеріального рівняння (3) та даних параметрів (табл. 1) пам'яті SRAM будується графік залежності між п'ятьма технічними параметрами мікросхем пам'яті, який зображено на рис. 2.

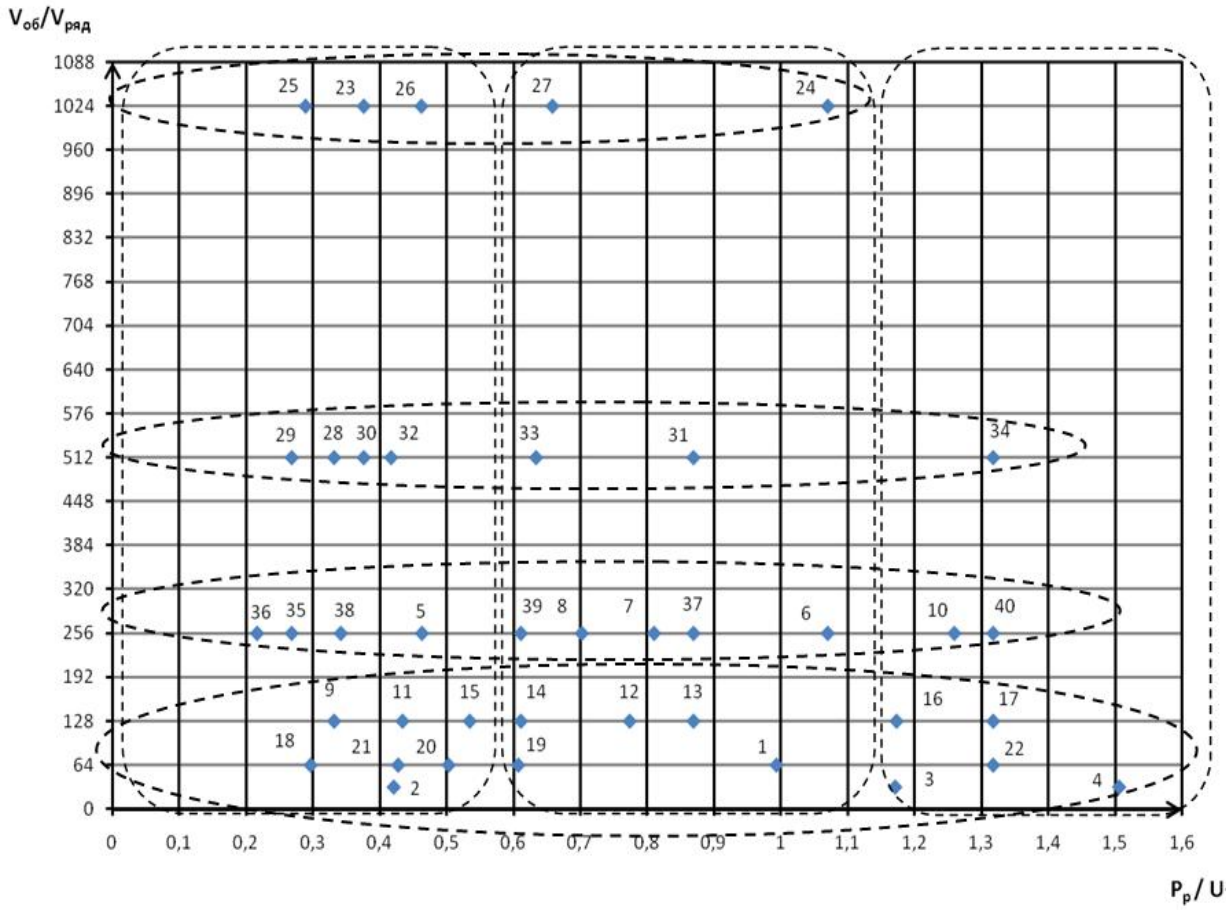

Рис. 2. Графік залежності основних технічних параметрів в безрозмірних координатах ($V_{об}/V_{ряд}$) та ($P_р$ / (U·I))

Примітка: на графіку цифри зазначених точок – 1, 2, …, 40 відповідають порядковому номеру мікросхем пам'яті, що наведені в табл. 1.

З графіка залежності видно, що найкращий енергетичний резерв мають елементи пам'яті, які знаходяться у правій вертикальній групі; відповідно до значення коефіцієнта ($V_{об}/V_{ряд}$) найкращими є елементи пам'яті, які знаходяться у нижній горизонтальній групі.

Отже, найкращими з боку надійності є елементи пам'яті типу K6E0808V1C, K6R1008V1C, K6R1008V1D, K6R1016V1D, а особливо K6E0808V1E. Але всі вони мають відносно низький загальний обсяг пам'яті (від 256 до 1024 Кбіт).

Тому, якщо при проектуванні необхідно обрати пам'ять з більшим загальним об'ємом, то рекомендується обирати елементи пам'яті типу K6R4016V1D, який має відносно високий енергетичний резерв та найбільший обсяг пам'яті серед розглянутих типів.

Проведений системний аналіз на основі теорії неповної подібності та розмірностей дозволяє пришвидшити процес визначення найкращих типів елементів пам'яті при проектуванні сучасних біометричних систем запобігання несанкціонованому доступу.

Крім того, виявлений резерв елементів пам'яті з енергетики дозволяє розкрити можливості підвищення надійності цих компонентів та визначити подальші напрями їх удосконалення.

Запропонований метод створення бази даних біометричних комп'ютерних компонентів забезпечить широкий вибір при проектуванні різноманітних систем контролю доступу у відповідності до вимог користувача, а застосування принципів системної інтеграції зробить можливим побудову або вдосконалення вже існуючих систем запобігання несанкціонованому доступу.

Висновки

Розроблена узагальнена біометрична модель доступу до мікропроцесорної системи керування СЛТК, яка відрізняється тим, що на її основі можна побудувати гаму агрегованих спеціалізованих біометричних систем доступу за принципом створення від складного, нехай і абстрактного, до більш простого та конкретного, для чого необхідно і достатньо лише вилучити з її складу зайві компоненти.

При фізичному моделюванні комп'ютерних компонентів визначений метод створення їх бази даних з найкращими технічними характеристиками, що сприяє досягненню максимальної ефективності та експлуатаційної технологічністю біометричної системи доступу до мікропроцесорної системи керування СЛТК.

Подальше дослідження слід проводити для визначення інформаційно-енергетичного резерву комп'ютерних компонентів за допомогою теорії неповної подібності та розмірностей. Широкий вибір біометричних комп'ютерних компонентів забезпечує можливість створення систем безпеки різної

складності: як систем контролю доступу до персонального комп'ютера або стільникового телефону, так й до систем безпеки, які охоплюють весь спектр завдань підприємства з територіально і структурно розподіленими об'єктами.

Література

1. Лукашенко В.М. Сравнительный анализ специализированных систем управления доступом на базе биометрии / В. М. Лукашенко, А.С. Вербицкий, С.А. Миценко и др. // Nauka i wykształcenie bez granic – 2010 : materiály VI Międzynárodowej naukowi-praktycznej konferencji. – Przemyśl : Nauka i studia, 2010. – Т. 22. – С. 9–12.

2. Мороз А.О. Біометричні технології. Методи дактилоскопії / А.О. Мороз // Математичні машини і системи. – 2011. – № 3. – С. 58–65.

3. Пантелейчук А. Использование DSP компании Texas Instruments в биометрических системах доступа [Электронный ресурс] / А. Пантелейчук // Новости электроники. – 2010. – № 2. – Режим доступу : http://www.compeljournal.ru/enews/2010/2/6.

4. Романов В.О. Биометрическая идентификация личности: современное состояние и перспективы развития в Украине / В.О. Романов, И.Б. Галелюка, П.С. Клочан // Электронные компоненты и системы. – 2010. – № 5. – С. 16–20.

5. Романов В.О. Технології аутентифікації особи за біометричними характеристиками / В. О. Романов, І. Б. Галелюка, П. С. Клочан // Комп'ютерні засоби, мережі та системи. – 2010. – № 9. – С. 54-61.

6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – СПб. : НиТ, 2004. – 384 с.

7. Лебедев А.Н. Моделирование в научно-технических исследованиях / А.Н. Лебедев. – М. : Радио и связь. – 1989. – 224 с.

8. Лукашенко А.Г. Виявлення резерву предмета дослідження на основі теорії неповної подібності та розмірностей / А.Г. Лукашенко, О.А. Кулигін, В.М. Лукашенко // Вісник Хмельницького національного університету. – 2009. – № 3. – С. 184–187.

Надійшла 16.11.2011 р.
Рецензент: д.т.н. Первунінський С.М.

УДК 621.3.029.6

Ю.В. ШИНКАРЕНКО, В.А. МИХАЙЛЕЦ
Киевский национальный университет технологий и дизайна

АНАЛИЗ НАПРЯЖЕННОСТИ МАГНИТНОГО ПОЛЯ ТЕРМОЭЛЕКТРОЛИТИЧЕСКОГО ПРЕОБРАЗОВАТЕЛЯ ВЛАЖНОСТИ ГАЗОВ
СООБЩЕНИЕ 2

В статье произведен анализ напряженности магнитного поля влагопреобразующего элемента, а также анализ дрейфа гигроскопического вещества в межэлектродном промежутке, при переносе электрических зарядов, вследствие воздействия на их транспортные процессы ортогональных электрического и магнитного полей преобразователя. Полученные результаты позволят разрабатывать конструкции влагопреобразующих элементов с улучшенными техническими характеристиками.

In the article an analysis of magnetic field strength of humidity-sensitive element has been performed, as well as an analysis has been made for the drift of absorbing material (humectants) within inter-electrode space (spark gap) while electric charges being transferred due to the transportation processes of abovementioned electric charges being affected by orthogonal electromagnetic fields of humidity transformer. This analysis will allow to developing the designs of humidity sensitive elements with enhanced operational and metrological capabilities.

Ключевые слова: термоэлектролитический преобразователь влажности газовых сред, влагопреобразующий элемент, принцип суперпозиции полей, ресурс, дрейф, напряженность магнитного поля, гигроскопическое вещество (сорбент), межэлектродный промежуток, радиальный интеграл.

Результаты исследования

МАГНИТНОЕ ПОЛЕ ВЛАГОПРЕОБРАЗУЮЩЕГО ЭЛЕМЕНТА С ОДНОСТОРОННИМ ПОДКЛЮЧЕНИЕМ ИСТОЧНИКА ТОКА

Если электрод имеет конечное и одинаковое по всей длине круглое сечение радиусом a, то напряженность магнитного поля внутри электрода на расстоянии x от его оси определяется по формуле [4]:

$$H = \frac{i}{4\pi a^2} \cdot x \qquad (33)$$

Тогда для расчета напряженности магнитного поля необходимо внести коррективы в сделанное в сообщении 1 рассмотрение магнитного поля влагопреобразующего элемента (ВПЭ) с учетом характера магнитного поля внутри электродов.