УДК 621.8:681.5

«БІОКОН» - СИСТЕМА БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

О.М. Різник, Д.О. Дзюба, А.М. Чернодуб
Інститут проблем математичних машин і систем НАН України
e-mail: neuro@immsp.kiev.ua

1. Вступ

Захист інформаційних систем колективного користування від несанкціонованого втручання потребує контролю доступу до їх терміналів (робочих місць). Існує широкий спектр засобів такого контролю - від найпростіших типу ключа, пароля або ПІН-кода до високотехнологічних біометричних методів ідентифікації особи користувача, основаних на використанні унікальності рисунку папілярних ліній пальців, райдужної оболонки ока, або генетичного коду особи. Серед біометричних методів, що досягли стадії практичного застосування найбільш надійним можна вважати метод ідентифікації особи за рисунком райдужної оболонки. Але цей метод досить незручний у використанні, тому найбільш поширеним є дактилоскопічний метод ідентифікації за відбитками пальців. Він забезпечує високу точність ідентифікації при мінімальних незручностях для користувачів. Зростанню його популярності сприяє масове виробництво дешевих дактилоскопічних сенсорів та поява відповідних комерційних комп'ютерних програм.

Слід зазначити, що дактилоскопічний метод не дає повної гарантії від помилок [1]. Відомі випадки фальсифікації дактилоскопічних відбитків з використанням муляжів, які існуючі сенсори не відрізняли від пальців живої людини. Нові удосконалені моделі сенсорів дозволяють помітно зменшити ризик фальсифікації, але в цілому ця проблема залишається відкритою. Для її вирішення необхідно збільшувати обсяг та різноманітність даних, використовуваних для ідентифікації особи. Цього можна досягти, наприклад, користуючись відбитками кількох пальців, вводячи їх в певній послідовності, відомій лише користувачу. Можна також використовувати додаткові біометричні ознаки, такі як зображення обличчя, або тембр голосу. Ризик помилки за додатковими ознаками може бути набагато більшим, ніж за відбитками пальців, але оскільки функція цих ознак є допоміжною, то точність ідентифікації практично не зменшиться

Для повного захисту інформаційної системи від несанкціонованого втручання ідентифікація особи користувача має забезпечуватись при виконанні ним будь-яких дій на робочому місці. Звичайно таку ідентифікацію проводять лише при відкритті доступу до робочого місця, а в подальшому захист робочого місця від стороннього втручання покладається на користувача. У випадку відлучення користувача доступ до робочого місця залишається відкритим, тому для виключення можливості стороннього втручання необхідний постійний контроль присутність користувача, та автоматичне блокування доступу у випадку відлучення. Для розблокування доступу має виконуватись повторна ідентифікація особи користувача. Така організація захисту дозволяє комбінувати різні засоби контролю і досягати компромісу між вимогами до високого рівня захисту інформаційної системи та мінімуму незручностей для її користувачів.

Висловлені положення були покладені в основу розробки системи біометричної ідентифікації «БІОКОН», створеної у відділі нейротехнологій Інституту проблем математичних машин і систем НАН України і призначеної забезпечувати надійний захист від несанкціонованого доступу у великих інформаційних системах та системах прийняття колективних рішень.

2. Структура системи

«БІОКОН» включає робочу програму та базу біометричних даних про користувачів. Копії робочої програми розміщені на робочих місцях – персональних комп'ютерах, що виконують функції терміналів інформаційної системи колективного користування. База біометричних даних зберігається централізовано на сервері цієї системи. Інформація про порушення доступу, виявлені робочими програмами, надходять в підсистему безпеки інформаційної системи колективного користування.

В системі «БІОКОН» реалізовано три способи ідентифікації особи користувача:

- за допомогою індивідуальної магнітної картки;
- за відбитком пальця;
- за зображенням обличчя.

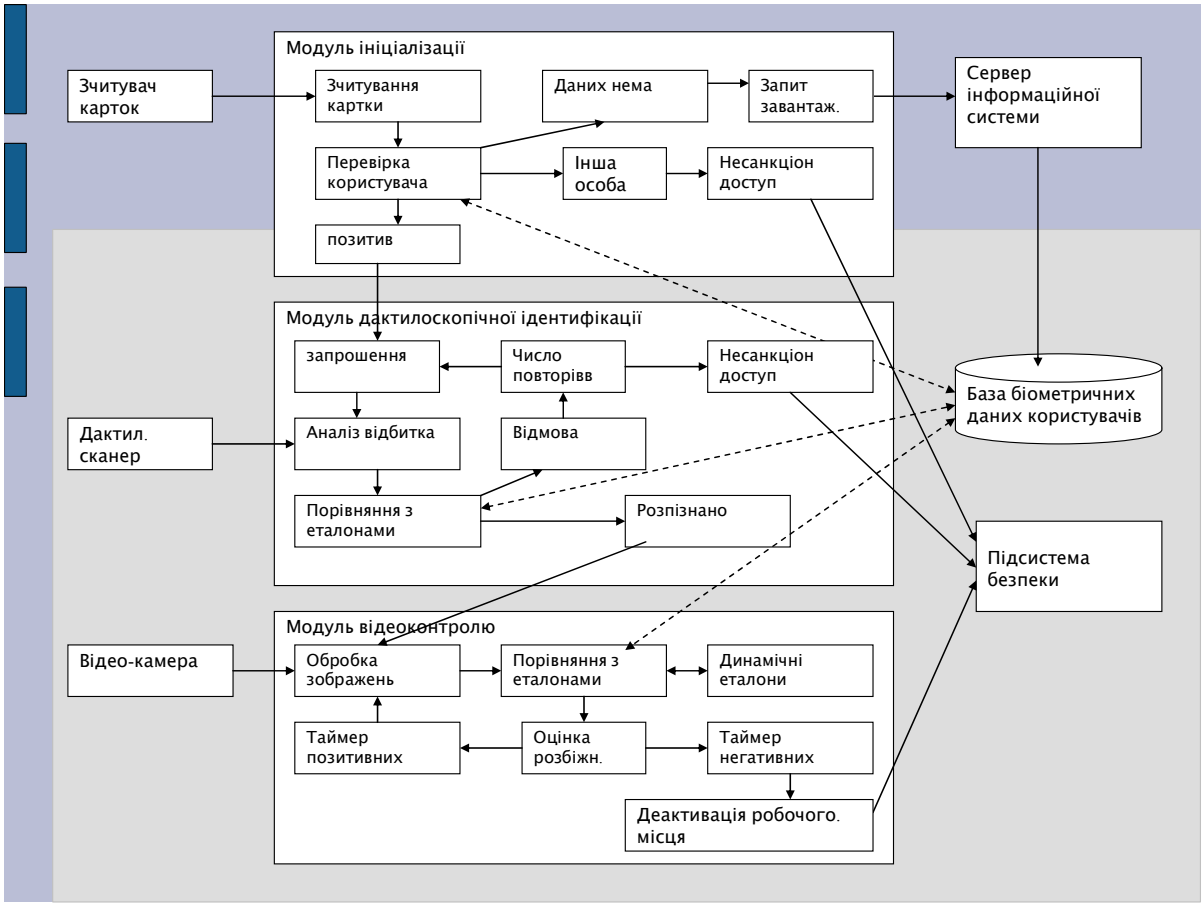

Рис.1. Структура системи біометричної ідентифікації особи користувача.

Відповідно робоча програма має три модулі:

Модуль ініціалізації «І», який здійснює перевірку магнітної картки користувача.

Модуль «Д», що виконує дактилоскопічну ідентифікацію (за відбитком пальця).

Модуль «З», що виконує ідентифікацію зображення обличчя користувача.

Рішення про дозвіл доступу власника магнітної картки до терміналу приймається при наявності позитивних відповідей всіх трьох модулів. Кожен модуль має спеціалізоване програмне забезпечення та відповідний пристрій для одержання даних про користувача:

- зчитувач магнітної картки;
- дактилоскопічний сенсор;
- відео-камеру.

3. Режими роботи

«БІОКОН» має три робочих режими:

- Реєстрація біометричних даних користувача;
- Верифікація особи користувача;
- Контроль присутності користувача на робочому місці.

Режим реєстрації призначений для одержання та збереження ідентифікаційних даних про користувачів інформаційної системи. Реєстрація може виконуватись на будь-якому терміналі інформаційної системи під контролем служби безпеки інформаційної системи. В цьому режимі «БІОКОН» одержує дані від дактилоскопічного сенсора та відеокамери, формує внутрішнє представлення біометричного портрету користувача, яке разом з даними його ідентифікаційної магнітної картки та датою реєстрації передає в Централізований банк ідентифікаційних даних (ЦБІД) інформаційної системи. При реєстрації в одному файлі даних може бути зафіксовано кілька екземплярів біометричного портрету користувача (до 10, залежно від їх якості). Число екземплярів визначається шляхом перевірки правильності розпізнавання при повторному введенні біометричної інформації. На рис.2. представлено реакцію дактилоскопічного модуля при недостатньому числі екземплярів біометричного портрету користувача.

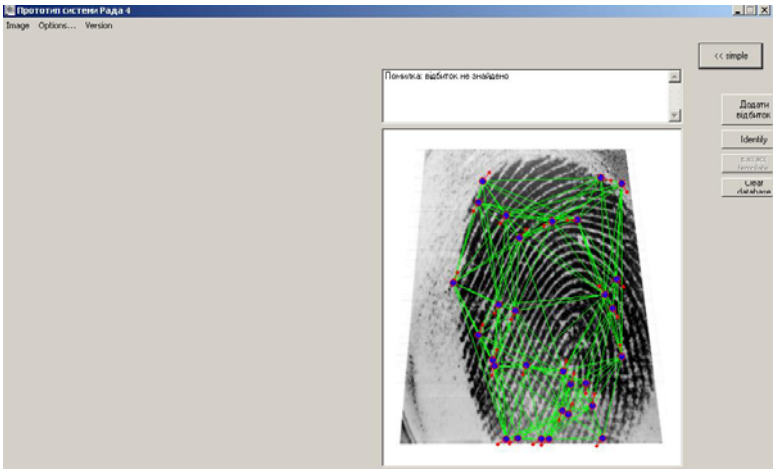

Рис.2. Реакція модуля дактилоскопічної ідентифікації в режимі реєстрації.

Режим верифікації призначений для встановлення відповідності особи, яка користується ідентифікаційною магнітною карткою власникові цієї картки. Верифікація виконується шляхом порівняння даних, одержаних за допомогою дактилоскопічного сенсора та відеокамери з біометричним портретом власника магнітної картки, зафіксованим при реєстрації користувача, який зберігається в ЦБІД інформаційної системи. При позитивній верифікації користувач отримує доступ до інформаційної системи, тобто відбувається активація терміналу. У випадку негативного результату, на екран терміналу надходить повідомлення: «НЕСПІВПАДІННЯ», що дозволяє повторну спробу верифікації. Якщо повторна верифікація дає негативну відповідь, то ситуація розглядається як спроба несанкціонованого доступу до системи. Відповідне повідомлення надсилається в службу безпеки, яка одержує також останні дані, зафіксовані дактилоскопічним сенсором та відеокамерою даного робочого місця.

Режим контролю присутності користувача на робочому місці здійснюється програмою модуля «З», яка одержує послідовні кадри з відеокамери, виявляє зображення обличчя користувача, представляє його у внутрішньому форматі та порівнює з біометричними даними, що зберігаються в ЦБІД. Порівняння виконується за допомогою нейронної мережі в послідовності, представленій на рис.3. При негативних результатах

порівняння аналізується послідовність змін зображення обличчя. При зникненні зображення користувача, або виявленні значного відхилення послідовності його рухів від природної поведінки, а також тривалому повторенні негативних результатів порівняння доступ до робочого місця блокується, а в службу безпеки надсилається повідомлення про причину блокування робочого місця.

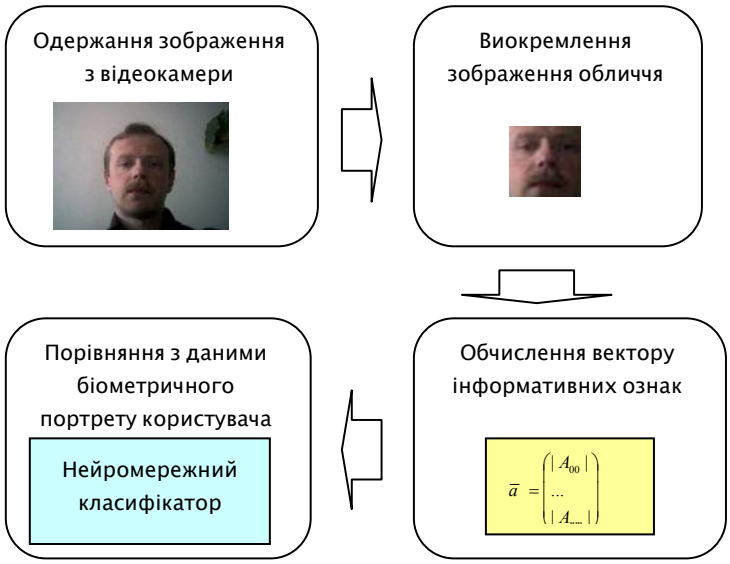

Рис. 3. Послідовність операцій модуля «З» при ідентифікації зображення.

4. Реалізація системи «БІОКОН»

Система «БІОКОН» реалізована в середовищі Windows і може встановлюватись на персональному комп'ютері з операційною системою Windows 2000, Windows XP або Windows Vista тощо. Прототип системи створено на базі міні-ноутбука з сенсорним екраном Samsung Q1 Ultra, обладнаним процесором Intel A110 з тактовою частотою 800 МГц та 1 Гб оперативної пам'яті. У режимі функціонування під управлінням Windows XP SP2 системою використовується 80-90% процесорного часу та 300-320 Mb оперативної пам'яті. Для роботи системи розпізнавання відбитків пальців додатково використовується програмне забезпечення Griaule Biometrics Fingerprint SDK [2]. Для коректної роботи системи розпізнавання облич необхідно забезпечити стаціонарність освітлення робочого місця з яскравістю відбитого світла приблизно еквівалентного денному освітленню.

Список використаної літератури

1. Болл Руд М., Коннел Джонатан Х., Панкатни Шарат, Ратха Налини К., Сеньор Єндрю У., "Руководство по биометрии", Москва: Техносфера, 2007.

2. http://www.griaule.com