УДК 004.056, 681.513.5

В.Б. Чередниченко[1], К.Е. Чередниченко[2].

[1]*Сумська філія Харківського національного університету внутрішніх справ, Суми*
[2]*Сумський державний університет, Суми*

БІОМЕТРИЧНІ МЕТОДИ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Одним з напрямків захисту інформаційних систем є оснащення приміщень з комп'ютерною технікою і процедур відкриття програмних засобів та баз даних пристроями доступу. У статті розглянуто властивості статичних біометричних методів ідентифікації особи та величини параметрів FAR і FRR для різних типів систем доступу. Запропоновано рекомендації щодо напрямків застосування цих методів у системах захисту інформації.

Ключові слова: *біометричні методи, дактилоскопія, термограма, сітківка ока, райдужна оболонка, ідентифікація, FAR, FRR.*

Вступ

У теперішній час розвиток комп'ютерної техніки та технологій призвів до впровадження інформаційних систем практично на усіх підприємствах, в організаціях, наукових установах, силових структурах, тощо. Сьогодні різні види інформації – наукова, технічна, технологічна, фінансова, тощо – накопичуються у електронній формі та використовуються співробітниками через комп'ютерні мережі. Зважаючи на шкоду, яку може завдати несанкціонований доступ до таких даних чи їх спотворення, на перший план виходять проблеми захисту інформаційних систем загального (цивільного) та спеціального (військового та правоохоронного) призначення. При аналізі загроз безпеці інформації одним з чинників є втручання людини у роботу апаратних або програмних засобів з метою порушення конфіденційності або цілісності інформації [1]. Зовнішнім впливам звичайно протидіють за допомогою різноманітних програмно – технічних методів захисту. Внутрішні загрози обумовлені діями власного персоналу або осіб, що проникли на об'єкт. Оскільки на підприємстві кількість приміщень з комп'ютерною технікою може сягати кількох десятків, у такій же ступені зростають труднощі забезпечення інформаційної безпеки. Відомим засобом протидії стороннім втручанням є процедури вводу паролю доступу. Але вони мають ряд недоліків, через що їх ефективність часто вважається недостатньою. В останній час досягнуто успіхів у розробці біометричних методів ідентифікації та аутентифікації, які можуть перешкодити проникненню сторонніх осіб ззовні та забезпечити значно надійніший захист від несанк-ціонованих дій всередині інформаційної системи [2].

Біометричним методам присвятили свої роботи Лакин Г.Ф., Кухарев Г. А., Варецький Я. Ю., Романець Ю.В., Тимофеєв П.А., Дубчак О.В., Підгайна К.І., Казарин М.Н., Брюхомицкий Ю.А., Вакуленко А., Іванов А.И., Дзюба О., Чернодуб А., Колесников А. В., Лавданський А. О., Ц. Мацумото, Хоанг Чунг Киен, Ч. Стюарт, та інші.

Метою даної роботи є огляд сучасних біометричних методів ідентифікації особи та рівня їх розвитку, а також можливостей використання цих технологій у системах захисту інформації.

Основна частина

У теперішній час методи ідентифікації з використанням «ручного» набору паролю замінюються на більш надійні: пластикові беджі, смарт – карти з введенням додаткового паролю, «інтелектуальні» картки з мікрочіпом, тощо. Ці засоби характеризуються набагато вищим ступенем захисту від підбору, копіювання, фальсифікації ключових даних порівняно з ручним вводом. Але всі карткові методи мають принциповий недолік – перевіряється перетинання рубежу захисту предметом ідентифікації, а не особою, яка має право доступу. При цьому картка може бути викрадена, загублена, підроблена, передана, тощо.

Єдиним беззаперечним способом ідентифікації на сьогодні є виявлення за допомогою технічних пристроїв біологічних характеристик особи та перевірка їх відповідності заздалегідь сформованим особистим шаблонам.

Біометрика (англ. Biometrics) – це методи ідентифікації особи, що використовують фізіологічні параметри людини – відбитки пальців або долоні, зображення обличчя, райдужну оболонку або сітківку ока, голос, ДНК, тощо. Використання цих технологій має певну історію, а їх «друге народження» почалось після відомих терористичних атак 11 вересня 2001 р. Результатами стали бурхливий розвиток біометричних технологій та їх широке впровадження у системи безпеки різноманітного призначення. Відбулося значне здешевлення такої апаратури при підвищенні безпомилковості її роботи. Звичайно біометричні методи розділяють на статичні, коли відповідні ознаки особи практично не змінюються у часі, та динамічні, які використовують дані про особливості поведінки людини.

Для систем захисту інформації цінність представляють в основному статичні методи, що фіксують незмінні характеристики особи, притаманні їй від народження.

Дактилоскопічний метод базується на унікальності та незмінності протягом життя відбитків пальців людини, що доведено криміналістичною наукою та підтверджено експертною практикою. На відбитку пальця знаходяться *мінуції* – унікальні для кожного узору точки зміни структури папілярних ліній – їх закінчення, роздвоєння, розрив, тощо. Система визначає для кожної мінуції ії координати і орієнтацію папілярних ліній у цій точці. Еталонний відбиток містить приблизно 70 мінуцій. Оцінку *(K)* результату порівняння відбитків та еталону можна обчислювати за формулою:

$$K = \frac{D^2 \times 100\%}{pq}$$

де D – кількість збігів мінуцій зчитаного та еталонного відбитків,

p, q – кількість мінуцій еталону та відбитку [3].

Дактилоскопічні датчики бувають різних типів:

– оптичні,
– оптико – волоконні,
– роликові,
– напівпровідникові,
– зарядові (capacitive – DC),
– ємнісні (capacitive - AC),
– термочутливі,
– радіочастотні,
– ультразвукові,
– мультиспектральні,
– протяжні різних типів, тощо.

Відповідно різняться їх експлуатаційні характеристики та вартість.

Дактилоскопічний метод розпізнання займає приблизно половину ринку систем доступу. Достатньо вказати, що майже третина сучасних ноутбуків оснащена вбудованою системою зчитування відбитків пальця, такі датчики вмонтовують у клавіатури ПК, Миші, флеш - накопичувачі, замки дверей, тощо.

Для оцінки якості біометричних систем ідентифікації введено такі характеристики:

– імовірність допуску особи, яка не має права доступу (False Acceptance Rate - FAR), це найбільш небажаний результат, який повинен бути мінімізованим;

– імовірність відмови особі, яка має право доступу (False Rejection Rate - FRR), такий помилковий результат можна виправити.

Ці характеристики взаємопов'язані – чим менше одна, тим більше друга. Точка, у якій ці дві помилки рівні, називається EER (Equal Error Rates). Чим менша величина EER, тим вище безпомил-ковість системи доступу. Наведемо характеристики деяких систем дактилоскопічного доступу (табл.1) [4]:

Таблиця 1

Характеристики систем дактилоскопічного доступу

№	Модель (фірма)	Вірогідність FAR %	Вірогідність, FRR %
1	FingerScan (Identix)	0,0001	1,0
2	TouchNet (Identix)	0,001	1,0
3	FIU (Sony)	0,1	1,0
4	Дакто (Россия)	0,000001	0,01
5	Кордон (Россия)	0,0001	1,0

Термін ідентифікації відбитку дактосистемою коливається від 0,5 до 5 сек., звичайно це припустима величина. Можна відмітити, що датчик найбільш якісної системи №4 виробляється на Чернігівському заводі радіоприладів, Україна. Реальні показники якості систем можуть погіршуватись у процесі експлуатації через забруднення датчика чи пальця, або через слабко виражені папілярні узори у людей фізичної праці, або через пошкодження пальця (іноді умисні), тощо.

Треба констатувати розповсюдженість думки про легкість створення дактилоскопічного муляжу та обману таких систем. У джерелах описаний експеримент спеціаліста по безпеці з університету Йокогами (Японія) Цутому Мацумото (Tsutomu Matsumoto). Він виготовив муляж пальця, за допомогою якого у 2002 р. на кількох різних сканерах одержав вірогідність помилкового допуску FAR у 70-95% [5], що є вкрай негативним. Також описаний експеримент з протилежним результатом, проведений після 2004 р. компанією «Ревер», Москва. Муляж власноручного виготовлення перевірявся на трьох сканерах та на Миші з

дактилоскопічним датчиком. У серіях по 100 спроб ні одна з трьох систем не сприйняла підроблений муляж у якості відбитка пальця. Тільки датчик Миші один раз за серію зчитав фальшивий відбиток, але при ідентифікації його з еталонним записом у базі даних система дала відмову у доступі [6]. Для протидії муляжам тепер успішно використовують сканери, які додатково реагують на температуру, пульс, вологість живого пальця. Питання «обману» дактилоскопічних систем не є темою даної статті.

Закінчуючи розгляд дактилоскопічного методу, слід вказати на успішно працюючу в Україні та Білорусі автоматизовану дактилоскопічну систему «Дакта – 2000», а в Російській Федерації функціонує аналогічна система «Папілон». Державні бази даних зберігають дактилоскопічну інформацію про мільйони осіб за десятипальцевою схемою та успішно перевіряють сліди пальців з місць нерозкритих злочинів по масиву дактилокарт.

Ідентифікація за формою обличчя – за допомогою відеокамери будується 2D або 3D образ обличчя, при цьому виявляються контури брів, очей, носа, губ, підборіддя, вух та ін. Потім між ними обчислюється відстань і будується множина варіантів у залежності від повороту обличчя, нахилу, зміни міміки. Достовірність такого порівняння оцінюється у 86- 93%. Для сканування потрібна камера високої роздільної здатності, щоб відстань між центрами зіниць була еквівалентна 200 пікселям, та відповідне освітлення і певна відстань до обличчя [7]. Тут існують труднощі розпізнання особи, пов'язані з окулярами, накладними вусами, бородою, гримом, тощо. Але для систем доступу на об'єкти цей недолік можна вважати несуттєвим.

Ідентифікація за термограмою обличчя – базується на неповторності розподілу на обличчі кровоносних судин, які виділяють тепло. Для сканування необхідна термочутлива камера інфра-червоного діапазону. Система може працювати в цілковитій темряві, на результати розпізнання не впливають переохолодження обличчя або його перегрів, природне старіння шкіри, пластичні операції, грим, накладні елементи [8]. Цей метод, на відміну від попереднього, дозволяє розрізняти близнят, його вважають ефективнішим за 2D або 3D сканування.

Ідентифікація за сітківкою ока – цей метод базується на унікальності малюнку судин очного дна. При скануванні всередину ока направляється пучок світла (іноді інфрачервоного), а обличчя повинно бути розташоване з високою точністю відносно сканера, що можна визнати незручністю методу. Але такі системи майже не дають помилкового допуску FAR та мають низьку похибку помилкової відмови зареєстрованій особі FRR. Недоліком методу є негативний вплив деяких захворювань ока (катаракти або глаукоми) на розпізнання особи. Також розповсюджена небезпідставна думка, що регулярне підсвічування ока шкодить здоров'ю.

Малюнок райдужної оболонки ока – він має високу унікальність. Сканування відбувається шляхом фотографування обличчя та виділення на ньому райдужної оболонки, зображення якої перетворюється на цифровий код. Необхідна камера високої роздільної здатності, але фото може бути зроблено непомітно для особи. Деякі захворювання викликають появу пігментних плям або зміну кольору райдужної оболонки, тому для верифікації використовують чорно - біле зображення. Негативно впливають на ідентифікацію незначні травми ока, безсоння, великі фізичні навантаження. За даними фірм – виробників похибка помилкового допуску особи FAR у таких системах досягає 0,0001% [8].

Ідентифікація за характеристиками долоні – робиться тривимірний відбиток кисті руки (геометрія кисті, об'єм пальців, нерівності долоні, розміщення складок шкіри, тощо). Другий метод базується на знятті термограми розташування судин на зовнішній стороні долоні. Такий малюнок характеризується неповторністю та стабільністю протягом усього життя, невеликі порізи або забруднення не є перешкодою для порівняння. Останній з цих методів безконтактний та досить надійний і перспективний для систем доступу, особливо для ідентифікації vip – персон на робочому місці [7].

Використання ДНК – коду людини – вважається найточнішим біометричним методом, але він потребує добре оснащеної біологічної лабораторії та порівняно великого проміжку часу для одержання результату. У системах доступу цей метод не використовується.

У якості підсумка наведемо порівняльні характеристики біометричних систем, побудованих з використанням розглянутих вище методів ідентифікації (табл. 2) [9]:

Слід зазначити, що у таблиці представлені типові значення характеристик, які при однаковому методі розпізнання можуть помітно відрізнятись для різних моделей (табл. 1).

Висновки

Розглянуті біометричні пристрої доцільно використовувати у системах захисту інформації. Наприклад, описана дактилоскопічна система (Futronic), яка складається з напівпро-відникового сканеру розміром з сірникову коробку та з програми, що вбудовується у меню входу до операційної системи, які виконують ідентифікацію шести користувачів за відбитком пальця та вводом паролю через клавіатуру (вартість комплекту до 100 дол.). Можна виконувати ідентифікацію осіб за райдужкою ока або/та формою обличчя, якщо використовувати вбудовану у ноутбук або зовнішню відеокамеру і придбати спеціальну програму.

Таблиця 2

Порівняльні характеристики біометричних систем

№ з/п	Модель	Біометричний метод	% на ринку	Вірогідність несанкціонованого допуску, FAR %	Вірогідність помилкового не-допуску, FRR %
1	Eyedentify ICAM	Сітківка ока	1%	0,0001	0,4
2	Iriscan	Райдужка ока	7%	0,0008	0,0007
3	FingerScan	Відбиток пальця	58%	0,0001	1,0
4	Veriprint 2100	-//-	-//-	0,001	0,01
5	BioMet	Геометрія руки	7%	0,1	0,1
6	Vocord (2D)	Геометрія обличчя	18%	0,01	0,2
7	Geometrix (3D)	-//-	-//-	0,001	0,01
8	Hitachi VeinID	Вени руки	1%	0,0008	0,01

Якщо показник помилкового допуску FAR недостатній для конкретної системи, доцільно застосувати перевірку по двох чи більше пальцях, або по райдужкам двох очей, або по райдужці та формі обличчя – без значного підвищення вартості обладнання. Значно вищу ефективність дає одночасне застосування двох систем, заснованих на різних біометричних методах – дактилоскопічному, термографічному, за райдужкою ока або рисами обличчя, тощо.

Можливими проблемами біометричних (та усіх інших) систем доступу є імовірність перехоплення інформації під час її передачі від сканера до бази даних, а також несанкціонований доступ до масиву еталонних записів, що зберігається у комп'ютері. Одним з засобів протидії цим загрозам є кодування відповідних даних.

Список літератури

1. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно – телекомуніка-ційних систем [Текст] / В. Л. Бурячок // Захист інформації. НАУ. - К. – 2011. - №3. – С. 1-9.

2. Болл, Р. Руководство по биометрии [Текст] / Болл Р.М., Коннел Дж.Х., Панканти Ш., Ратха Н.К., Сеньор Э.У. – М. : Техносфера, 2007. - 368 с. - ISBN 978-5-94836-109-3, 0-387-40089-3.

3. Гарасим, Ю. Дослідження та аналіз перспектив-них технологій ідентифікації особи в захищених корпоративних мережах зв'язку [Текст] / Ю. Р. Герасим, Т. Б. Крет. // Системи обробки інформації. / Харківський університет Повітряних Сил. – 2010, вип. 3(84). – С. 7-10. – ISSN 1681-7710.

4. Барсуков В. С. Новая информационная технология: «Стеганографическая дактилоскопія» [Електронний ресурс] / Информационная система «Техника для спецслужб». – Режим доступу: http://www.bnti.ru/showart.asp?aid=602&lvl=04.08.03.

5. Евангели, А. Биометрические технологии. [Електронний ресурс] - журнал "BYTE", №4 (68), 2004.– Режим доступу: http://www.bytemag.ru/articles/detail.php?ID=6675.

6. Маковский Е.И. «Обман» биометрических систем доступа, использующих дактилоскопическую идентификацию личности [Електронний ресурс] / компания «РЕВЕР». – Режим доступу: http://www.rewer. ru /Snoski/Statii/obman.htm.

7. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. [Текст] // Математичні машини і системи / Інститут проблем математичних машин і систем НАН України. – 2011. - №1. – С. 39- 45. – ISSN 1028-9763.

8. Лисенко А.М., Мельник О.С. Застосування біометричних систем для ідентифікації особи [Текст] // Вісник Київського національного університету ім. Т.Шевченка, серія «Юридичні науки». – 2004. - №60- 62. – С. 87 – 91.

9. Лукашенко, В. Сравнительный анализ специализированных систем управления доступом на базе биометрии. [Текст] / В. М. Лукашенко, О.С. Вербицкий, С.А.Мощенко, Ю.Ю.Терещенко, Е.П. Лукацкая // Современные информационные технологи.- 2010. - [Електронний ресурс] - Режим доступу: www.rusnauka.com/35_OINBG_2010/Informatica/76318.doc.htm

Надійшла до редколегії 30.03.2012

Рецензент: д-р техн. наук, проф. О.А. Борисенко, Сумський державний університет, Суми.

БИОМЕТРИЧЕСКИЕ МЕТОДЫ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

В.Б. Чередниченко, К.Э. Чередниченко

Одним из направлений защиты информационных систем является оснащение помещений с компьютерной техникой и процедур открытия программных средств и баз данных устройствами доступа. В статье рассмотрены свойства статических биометрических методов идентификации личности и величины параметров FAR и FRR для различных типов систем доступа. Предложены рекомендации по направлениям применения этих методов в системах защиты информации.

***Ключевые слова**: биометрические методы, дактилоскопия, термограмма, сетчатка глаза, радужная оболочка, идентификация, FAR, FRR.*

BIOMETRIC METHODS IN INFORMATION SECURITY SYSTEMS

V.B. Cherednyhenko, K.E. Cherednychenko

One of the areas of protection of information systems is to equip rooms with computer equipment and procedures for opening the software and database access devices. The article deals with the properties of static biometric identification methods and the values of parameters FAR and FRR for different types of access systems. Recommendations on areas of application of these techniques in information security systems.

***Keywords**: biometrics, fingerprinting, thermograms, retina, iris, identification, FAR, FRR.*