- решать задачи аттестации КТЗИ;
- определять локальные источники излучений НМП, возникающие, например, в местах дефектов сварных швов экранирующих конструкций;
- проводить регламентированные мероприятия по обеспечению ЭМС радиокомплексов и отдельных технических средств в местах их компактного размещения;
- проводить исследования с целью обеспечения безопасности от угрозы технологического терроризма (поиска на защищаемом объекте зон уязвимости от внешних электромагнитных полей).

Компактные антенны АИФ-1, в отличие от распространенных антенн с диаметром рамки более 250 мм, могут быть скрытно расположены на защищаемом объекте и, при работе совместно анализаторами спектра, сканирующими приемниками или другими средствами измерительной техники, оперативно сигнализировать об изменении электромагнитной обстановки (НМП) как внутри, так и по периметру защищаемого объекта, т. е. осуществлять радиомониторинг и пеленгацию.

Литература: ***1.*** *Закон Украины «О борьбе с терроризмом» от 20. 03. 2003 г.* ***2.*** *Вишняков Я. Д., Бондаренко Г. А., Васин С. Г., Грацианский Е. В.. Основы противодействия терроризму.; под ред. Я. Д. Вишнякова. — М.: Издательский центр «Академия», 2006. — 240 с.* ***3.*** *Шолохов С. Н. Информационное оружие. www.alltoday.ru/seo_articles/articles5779.html.* ***4.*** *www.ahsystems.com.* ***5.*** *www.electro-metrics.com.* ***6.*** *www.loniir.ru/ emc/equip/izm_anten/index.html.* ***7.*** *В. Галанский, А. Лаврентьев, М. Прокофьев. Точечные активные измерительные антенны в диапазоне 5 Гц – 30 МГц . Сборник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", № 11, 2005, стр. 180.* ***8.*** *Vladislav Galansky, Alexander Lavrent`ev, Vladimir Mats, Mikhail Prokof`ev. Dot active measuring loop-aerials. 2005 5th International Conference on antenna Theory and Techniques, 24-27 May, Kyiv, Ukraine, pp. 379 – 381.*

УДК 004:681.3

СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Петро Бідюк, Володимир Бондарчук

Інститут прикладного системного аналізу Національного технічного університету «Київський політехнічний інститут»

Анотація: **Розглянуто сучасні методи біометричної ідентифікації користувачів комп'ютерних систем, призначені для забезпечення захисту конфіденційної інформації. Встановлено недоліки і переваги кожного методу, наведені показники якості ідентифікації та визначені перспективні напрями досліджень.**

Summary: **The modern methods of biometric identification of users of computer systems that are designed to protect confidential information. Advantages and disadvantages of each method are given, the indicators of identification quality are defined as well as the future research directions are determined.**

Ключові слова: **Захист інформації, біометрична ідентифікація, статистичні дані, показники якості.**

I Вступ

Однією з актуальних задач розвитку інформаційних технологій на сучасному етапі є забезпечення надійного захисту інформації. Існуючі сьогодні методи захисту інформації поділяють на: апаратні, програмні, змішані; останні поєднують у собі як апаратні, так і програмні засоби.

Задача захисту інформації є особливо актуальною в умовах активного розвитку систем електронної торгівлі та банківських операцій, систем дистанційного навчання та великих корпоративних мереж, де циркулює конфіденційна інформація.

Важливою та ще не вирішеною проблемою захисту інформації є ефективна ідентифікація користувача, який отримує доступ до конфіденційної інформації [1]. Традиційний парольний захист має ряд очевидних недоліків. Наприклад, у разі порушення конфіденційності пароля, це часто може залишитися непоміченим його власником, відразу порушується захист всієї інформації, до якої він (власник) має доступ.

Як альтернатива парольній системі або її доповнення може розглядатися ідентифікація користувачів за біометричними характеристиками. Біометричні технології ідентифікації, автентифікації мають низку переваг перед традиційними і знаходять все більше застосування в комп'ютерних системах [2]. Біометричне підтвердження, а не проста перевірка пароля, який може бути вкрадений, перехоплений або вгаданий, є ключовим при розширенні Інтернет-торгівлі, створенні нових систем безпеки інформації в корпоративних мережах та системах дистанційного навчання та тестування.

Задача біометричної ідентифікації і методи її реалізації розглянуті в багатьох роботах різних вчених. Наприклад, роботи Іванова А. І., Сорокіна І. А., Рибчинко Д. Є. присвячені дослідженню динамічних методів біометричної ідентифікації, зокрема, динаміці рукописного почерку та клавіатурного почерку [1, 3 – 9]. У роботах Юркова П. Ю., Бабенко Л. К., Федорова В. М., Каткова О. Н., Дворянкина С. В. розглянуті методи динамічної біометричної ідентифікації за голосовим сигналом [1, 3, 10]. Роботи Диденко С. М., Шапцева В. А. присвячені дослідженню динамічних методів ідентифікації користувачів за почерком миші, зокрема за допомогою математичного апарату нейронних мереж [1, 2, 11]. Темі розробки методів статичної біометричної ідентифікації і зокрема ідентифікації за портретом обличчя присвячені роботи Старовойтова В. В., Муриніна А. Б., Цуркова В. І. [1, 2].

Інші статичні методи і алгоритми біометричної ідентифікації тримаються в таємниці виробниками.

Метою даної роботи є критичний огляд існуючих методів біометричної ідентифікації та обґрунтований вибір методів для подальшого дослідження та практичного застосування. Ці методи мають забезпечувати надійну ідентифікацію користувачів з високою ймовірністю, а також унеможливлювати надання доступу нелегальним користувачам.

II Огляд сучасних методів біометричної ідентифікації

Ідентифікувати людину можливо за ознаками, пов'язаними з її фізіологічними особливостями, які однозначно ідентифікують особу. До таких ознак можна віднести: геометричну будову руки, відбитки пальців, особливості малюнка сітківки ока, райдужну оболонку ока, портрет (наприклад, інфрачервону карту людини), характеристики і особливості мови, рукописний почерк, клавіатурний та комп'ютерний почерк, інші фізіологічні особливості людини, що робить її «особливою».

Особливість ідентифікації за біометричними параметрами базується на їх винятковості. Ймовірність того, що знайдуться дві людини з однаковими ознаками, дуже мала (наприклад, ймовірність того, що в двох різних людей на однакових пальцях однієї руки збігатимуться відбитки пальців, рівна 1/24 млн, тобто практично є нульовою). Основні характеристики перерахованих вище методів біометричної ідентифікації наведені в таблиці 1 [10].

Таблиця 1 – Основні характеристики методів біометричної ідентифікації

Метод отримання біометричних параметрів	**Ймовірність відмови у доступі %**	**Ймовірність помилкової ідентифікації «чужого» (без використання муляжу) %**	**Ймовірність помилкової ідентифікації «чужого» (з використанням муляжу) %**	**Збереження таємниці образу у процесі ідентифікації абонента**	**Вартість технічної реалізації в грошовому еквіваленті, у.о.**
Геометрична будова руки	0,2…4	0,2….1	10…75	неможливо приховати	Від 600 до 3000
Відбитки пальців	2...6	0,0001	10...70	неможливо приховати	Від 60 до 600
Особливості малюнка сітківки ока	0,4	6...10	_____	неможливо приховати	приблизно 4000
Райдужна оболонка ока	0,2…2	0,0001	_____	неможливо приховати	Від 500 до 6000
Портрет обличчя	1…9	_____	_____	неможливо приховати	55000
Рукописний почерк	0,5…5	0,5…5	0,5...5	8-10…10-40	_____
Клавіатурний та комп'ютерний почерк	3…9	3...9	_____	6-10…10-12	_____
Характеристики і особливості мови	0,5...5	0,5...5	25...90 (запис)	10-16…10-30	1...60

Методи біометричної ідентифікації діляться на дві великі групи:

– статичні методи, які ґрунтуються на фізіологічних характеристиках людини;

– динамічні методи, які ґрунтуються на особливостях поведінки людини - підсвідомих рухах в процесі виконання якої-небудь дії.

Статичні та динамічні методи біометричної ідентифікації – це два взаємопов'язані та взаємодоповнюючі напрями. Основною перевагою статичних методів біометричної ідентифікації є їх відносна незалежність від психологічного стану користувача, малих затрат зусиль користувача, і, як наслідок, можливість організації біометричної ідентифікації великих потоків людей [2].

Біометрична ідентифікація на основі динамічних характеристик, як правило, простіша в реалізації, оскільки, як правило, не вимагає дорогого устаткування і може обмежуватися тільки програмним забезпеченням, яке вимагає мінімальну підтримку фахівця в процесі експлуатації [1].

III Статичні біометричні характеристики

Основні статичні біометричні характеристики, а також види їх реалізації наведені в табл. 2.

Таблиця 2 – Реалізація фізіологічних біометричних характеристик

Біометрична характеристика	**Реєструючий пристрій**	**Зразок**	**Досліджувані риси**
Геометрична будова руки	Запатентований настінний пристрій	Тривимірне зображення зверху і боків кисті	Висота і ширина кісток і суглобів кисті і пальців
Відбиток пальця	Периферійний пристрій настільного комп'ютера, карта стандарту PC card, миша, мікросхема або зчитувальний пристрій, вбудований в клавіатуру	Зображення відбитку пальців (оптичне, на кремнієвому фотоприймачі, ультразвукове, або безконтактне)	Розташування і напрям гребінчастих виступів і розгалужень на відбитку пальців, дрібні деталі
Особливості малюнка сітківки ока	Запатентований настільний або настінний пристрій	Зображення сітківки	Розташування кровоносних судин на сітківці
Райдужна оболонка ока	Відеокамера, здатна працювати в інфрачервоному діапазоні, камера для ПК	Чорно-біле зображення райдужної оболонки ока	Смужки і борозенки на райдужній оболонці ока
Портрет обличчя	Відеокамера, камера для ПК, фотоапарат	Зображення особи (оптичне або теплове)	Відносне розташування і форма носа, розташування скул

У стадії розробки знаходяться нові біометричні технології, пов'язані з іншими фізіологічними характеристиками.

– Порівняння ДНК — це найдосконаліша на сьогодні біометрична технологія, що дає прямий доказ ідентичності особи, — окрім однояйцевих близнят, в яких однаковий генотип. Цей метод інколи називається дактилоскопією ДНК, що збиває з пантелику і вводить в оману, оскільки відбитки пальців не «проникають до рівня генома». Біометричні системи, засновані на порівнянні ДНК, можуть бути введені в дію лише згодом.

– Відбиток долоні — в цій системі використовується розташування ліній на долоні людини, повністю аналогічно біометричній технології, що використовує відбитки пальців.

– Судинні рисунки — розташування вен в різних частинах тіла людини, включаючи зап'ястя і тильну сторону долоні.

– Сигнали, що виробляються серцем (мозком, легенями), — в цій системі користувач торкається датчика «біодинамічного підпису» («Biodynamic signature» sensor) і залишається з ним в контакті деякий час (залежно від точності вимірів — до 8 секунд). За цей час датчик ідентифікує індивідуальні параметри людини.

Розпізнання за формою кисті руки

Даний статичний метод побудовано на розпізнаванні геометрії кисті руки (яка також є унікальною біометричною характеристикою людини) за допомогою спеціальних пристроїв, що дозволяють отримувати тривимірний образ кисті руки (деякі виробники сканують форму декількох пальців). Отримані дані використовують для отримання унікальної згортки, що однозначно ідентифікує людину. Існує два основних підходи до використання геометричних характеристик кисті руки. Перший з них ґрунтується на геометричних характеристиках руки. Другий вводить ще і образні характеристики руки (образи на стиках між фалангами пальців і візерунки кровоносних судин).

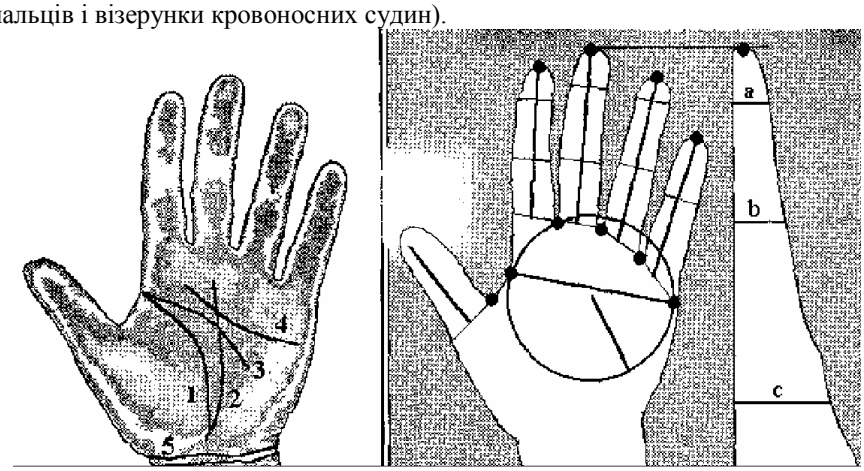

Рисунок 1 – Рисунок долоні

На рис. 1 показано візерунок на долоні, що складається з п'яти основних ліній (зліва) та контрольних точок і 17 геометричних ознак руки (справа). Основними геометричними ознаками є такі: ширина долоні, радіус вписаного в долоню кола, довжина пальців, ширина пальців, висота кисті руки в трьох місцях. Всі ці ознаки об’єднуються в єдиний вектор значень. Метод ідентифікації по вектору значень досить простий. Спочатку з користувача знімають декілька проекцій його руки. Для кожної з цих проекцій формується свій вектор значень. На основі декількох векторів значень створюється спеціальний клас. Далі всі ознаки в класі усереднюються, і формуються ознаки еталонного образу (знаходиться центр класу). В процесі роботи вихідні образи можуть модифікуватися. У разі успіху порівняння нового образу з еталоном, він може бути включений до класу вихідних ознак. Порівнювати ж між собою два образи можна за декількома критеріями. Найбільш очевидний з них – найменша відстань від досліджуваного образу до еталону. Складніший метод передбачає аналіз знімання чотирьох характеристик, три з яких – характерні розміри, а четверта півтонове зображення складок шкіри на згині між фалангами. Такий метод фактично унеможливлює обдурення приладу.

Розпізнавання за відбитком пальців

На отриманому зі сканера зображенні відбитків пальців (залежно від якості) можна виділити деякі характерні ознаки, які надалі можна використовувати в цілях ідентифікації.

На найпростішому технічному рівні, наприклад, якщо роздільна здатність отриманого зі сканеру зображення складає 300 – 500 dpi, на поверхні зображення пальця можна виділити досить велику кількість дрібних деталей, за допомогою яких можна їх класифікувати, але, як правило, в системах ідентифікації використовують всього два типи деталей візерунку (особливих точок):

– кінцеві точки – точки, в яких "виразно" закінчуються папілярні лінії;

– точки розгалуження – точки в яких папілярні лінії роздвоюються.

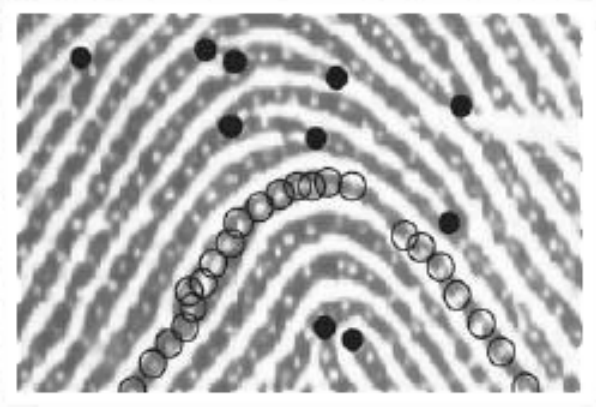

Рисунок 2 – Зображення відбитків пальців з відміченими порами, точками розгалуження і кінцевими точками

На зображенні поверхні пальця з роздільною здатністю близько 1000 dpi можна виявити деталі внутрішньої будови самих папілярних ліній, зокрема, пори потових залоз (рис. 2, порожніми колами відмічені пори, чорними колами відмічені кінцеві точки і точки розгалуження). Їх розташування можна використовувати для ідентифікації. Проте цей метод мало поширений внаслідок складності здобуття в не лабораторних умовах зображень такої якості.

При автоматизованому розпізнаванні відбитків пальців, на відміну від традиційної дактилоскопії, виникає значно менше проблем, пов'язаних із різними зовнішніми чинниками, що впливають на процес розпізнавання. При отриманні відбитків пальців за фарбовим методом неможливо виключити або, принаймні максимально зменшити, зсув або поворот пальця, зміну тиску, зміну якості поверхні шкіри і так далі. Електронні безфарбові сканери дозволяють отримати зображення відбитку пальця з достатньою для обробки якістю. Якість отриманого зі сканера зображення папілярного візерунку пальця є одним із основних критеріїв, від якого залежить вибір алгоритму формування згортки відбитку пальця і, зрештою, ідентифікації людини.

Розпізнавання за сітківкою ока

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Ймовірність пропуску незареєстрованого користувача (ймовірність помилки першого роду) при скануванні сітківки ока складає 0,0001%. При цьому ймовірність помилки другого роду досить висока — порядка 0,1%. Це пояснюється тим, що спочатку дані системи були розроблені на замовлення військових, де до помилок першого роду пред'являють найжорсткіші обмеження. При цьому передбачається, що користувачі можуть повторити процедуру автентифікації кілька разів.

Розпізнавання за райдужною оболонкою ока

Методи ідентифікації особи за райдужною оболонкою ока побудовані за одним і тим же принципом – виділення частотної або будь-якої іншої інформації про текстуру райдужної оболонки із зображенням і збереженням цієї інформації у вигляді спеціальних кодів (для системи Дагмана (Daugman) цей код отримав спеціальну назву райдужний код (Iriscode)). Можна порівнювати коди райдужних оболонок і зберігати в базі даних. Побудова коду здійснюється в три етапи:

– виділення зображення райдужної оболонки із загального зображення;

– обробка отриманого зображення, наприклад, усунення шуму (denoising), поліпшення зображення (enhansing), у тому числі вирівнювання гістограми, усунення відблиску; деякі методи "розгортають" круглу зіницю в прямокутне зображення – відбувається перехід від полярних координат в декартові; інколи після такої "розгортки" частина зображення відсікається, щоб накопичена на даному етапі помилка не вплинула на якість розпізнавання;

– складання коду; перетворене зображення фільтрується способом, залежним від конкретного методу; за результатами фільтрації складається представлення у вигляді коду.

Для кодів необхідно вибрати критерій порівняння. Часто код записується у вигляді послідовності бітів і критерієм порівняння є код Хеммінга. Як приклад, код Хеммінга використовується в системах Дагмана,

Ticce (Tisse) [12]. Більшість методів працюють із зображеннями в градаціях сірого або картами яскравості зображень, тобто кольорова складова є надлишковою.

Розпізнавання за портретом

У даному статичному методі ідентифікації будується двовимірний або тривимірний образ обличчя людини. За допомогою камери і спеціалізованого програмного забезпечення на зображенні або наборі зображень особи виділяються контури брів, очей, носа, губ і т. д., обчислюються відстані між ними й інші параметри, залежно від алгоритму, що використовується. За цими даними будується образ, що перетворюється в цифрову форму для порівняння. Причому кількість, якість і різноманітність образів (різні кути повороту голови, зміни нижньої частини обличчя при вимові ключового слова і т. д.) може варіюватися залежно від алгоритмів і функцій системи, що реалізує даний метод.

IV Динамічні біометричні характеристики

Основні динамічні біометричні характеристики, а також види їх реалізації наведено в табл. 3.

Таблиця 3 – Реалізація динамічних біометричних характеристик

Біометрична характеристика	**Реєструючий пристрій**	**Зразок**	**Досліджувані риси**
Голос	мікрофон, телефон	запис голосу	частота, модуляція і тривалість голосового образу
Підпис	планшет для підпису, перо для введення даних	зображення підпису і значення відповідних динамічних вимірів	швидкість, порядок ліній, тиск і зовнішній вигляд підпису
Динаміка натискання клавіш	клавіатура	ритм машинопису	час затримки (проміжок часу, протягом якого користувач утримує конкретну клавішу) час «польоту» (проміжок часу, який потрібний користувачеві для переходу з однієї клавіші на іншу)
Динаміка роботи з маніпулятором «миша»	маніпулятор «миша»	Образ характерної траєкторії	характерні точки траєкторії Та інші параметри траєкторії

Ідентифікація особи за особливостями голосу

Ідентифікація особи за особливостями голосу має ряд привабливих сторін. По-перше, існує високорозвинена телефонна мережа; по-друге, звукові карти стали стандартним устаткуванням сучасних персональних комп'ютерів. Як недолік біометричних систем ідентифікації особи за голосом необхідно відзначати, перш за все, те, що парольну фразу важко зберегти в таємниці.

Сучасні засоби акустичного прослуховування дозволяють досить успішно здійснювати несанкційоване копіювання парольної фрази. Очікується, що виключення небезпеки використання злочинцями прослуховування відбудеться при переході до ідентифікації особи за довільними фразами. Як потенційна протидія прослуховуванню використовується комбінування з іншими методами біометричної автентифікації. Ймовірність помилки для голосових систем складає від 1% до 2%.

Для того, щоб ідентифікувати абонента за голосом, необхідно мати мовний шаблон, з яким порівнюватиметься голосовий ключ, що вводиться в систему. Порівняння ключа і шаблону може проводитися в цілому або за декількома характеристиками мовного сигналу (тут, ми говоримо про цифровий мовний сигнал, що пройшов обробку і адаптований до поставленого завдання): амплітуда і потужність (гучність), часові, частотні (тембр), енергетичні, фазові характеристики [13].

Для забезпечення простоти аналізу мовний сигнал, його попередньо піддають дискретизації з використанням частотного або Вейвлет перетворення. Ідентифікація абонента може виконуватися за такими показниками:

- короткочасна енергія сигналу (визначається функцією короткочасної енергії з використанням вікон Хеммінга [13]);
- автокореляційна функція (дозволяє визначити енергію і періодичні властивості сигналу);

– число переходів сигналу через нуль (оскільки високі частоти приводять до великого числа переходів через нуль, а низькі – до малого, то існує жорсткий зв'язок між числом нульових переходів і розподілом енергії по частотах [13]);
– спектр сигналу;
– коефіцієнти лінійного передбачення [5];
– кепстральні коефіцієнти;
– кепстральні коефіцієнти, обчислені на основі лінійного передбачення.

Ідентифікація за динамікою рукописного підпису

Проблему ідентифікації користувача за його факсимільним підписом [3, 4] доцільно розглядати як дві незалежні задачі:

– ідентифікацію користувача лише за слідом пера автографа або за "мертвим" статичним підписом, вже наявним на документі, що перевіряється;

– ідентифікація автора за динамікою відтворення користувачем "живого" підпису, що вводиться ним у комп'ютер у момент ідентифікації, і спостереження індивідуальних особливостей звичних для автора підсвідомих рухів.

Відмічені вище дві постановки задачі мають суттєві відмінності, але можуть вирішуватися паралельно і незалежно. В першій постановці задачі мова йде про порівняння зображень, відтворених раніше в невідомій послідовності. В другій постановці – аналізуються дані про параметри коливань пера автора при відтворенні ним підпису в тривимірному просторі. Якщо це користувач декартової системи координат (X, Y, Z), то дані про динаміку відтворення підпису отримують у вигляді двох функцій часу коливань пера в площині графічного планшету X(t), Y(t) і ще одну функцію – варіації тиску пера на графічний планшет Z(t).

Необхідно відмітити, що першу постановку задачі важко реалізувати при сучасному рівні розвитку технологій. Як правило, такі системи напівавтоматичні, вони спрощують роботу експерта, надаючи йому можливість порівнювати відповідні чисельні характеристики подібності фрагментів "мертвого" підпису з оригіналом, але остаточне рішення приймає людина. Саме тому фірми-виробники не дають статистичних даних про помилки першого і другого роду для ідентифікації користувача тільки за допомогою "мертвого" статичного образу підпису.

У другій постановці задачі вирішальну роль відіграє обчислювальна машина, яка має істотно більше інформації порівняно з експертом. Як результат, системи ідентифікації особи, що аналізують динаміку відтворення автографа, за своїми статистичними характеристиками істотно кращі експертів.

Слід зазначити, що деякі з систем біометричної ідентифікації за підписом використовують не самі функції X(t), Y(t), Z(t), а їх першу або другу похідну. Останнє обумовлене лише типом використовуваного датчика, чутливого до похідної, і практично не впливає на якість і об'єм вихідної інформації. Слід зазначити, що помилка першого роду або помилкова відмова справжньому авторові з ймовірністю 0,01 — це прийнятна характеристика для вимог сьогоднішнього дня.

Ідентифікація за клавіатурним почерком

У традиційних системах захисту інформації доступ здійснюється за допомогою паролів. Якщо пароль збільшити, то при введенні пароля з'являється можливість спостерігати характерний для користувача клавіатурний почерк. Наприклад, як пароль використовується наступна фраза: "Пароль — це спосіб захисту інформації". При введенні подібної парольної фрази біометрична система фіксує час натиснення кожної клавіші і інтервал часу між натисненням чергової клавіші і відпуском попередньої клавіші. Графік співвідношення інтервалів часу натискання і відпуску клавіш для слова "Пароль" наведено на рис. 3.

З рис. 3 видно, що часи натискань клавіш t_1, t_2, t_3 ...., t_N різні і, відповідно, значення цих параметрів можуть бути використані для виявлення характерних особливостей індивідуального клавіатурного почерку користувача. Крім того, можуть бути використані як контрольовані параметри інтервали часу між натисненням сусідніх клавіш τ_1, τ_2, τ_3 ...., τ_{N-1}. Контрольовані параметри істотно залежать від того, скільки пальців використовує при наборі користувач, від характерних для користувача поєднань рухів різних пальців руки і від характерних рухів рук при наборі. Зокрема, якщо змусити користувачів працювати одним пальцем однієї руки, то клавіатурний почерк практично повністю втрачає індивідуальність. В цьому випадку час натиснення клавіш для різних людей перестає відображати їх індивідуальність. Інтервали між натисканнями стають пропорційні відстані між клавішами, а перекриття натиснень сусідніх клавіш стає неможливим. З іншого боку, в міру збільшення навиків роботи з клавіатурою і переходу до сліпого набору всіма пальцями обох рук істотно зростає індивідуальність клавіатурного почерку будь-якого з користувачів.

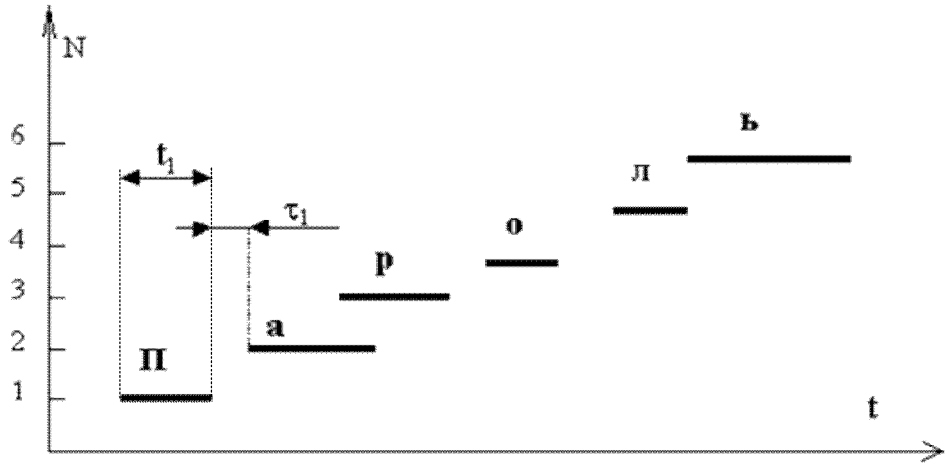

Рисунок 3 – Часова діаграма введення слова “Пароль”

Важливою характеристикою цієї технології біометричної ідентифікації є довжина парольної фрази. Практика показує, що парольна фраза має бути такою, що легко запам'ятовується і містити від 21 до 42 натискань на клавіші. При синтезі парольної фрази допустиме використання слів з сенсом з деякого словника. На відміну від класичних паролів, при наборі довгої парольної фрази допустимі помилки в один або два символи, що дещо погіршує стійкість парольної фрази до статичного підбору, але значно знижує ймовірність помилок першого роду [8].

Біометричний еталон введення парольної фрази отримують обчисленням математичних сподівань та дисперсій параметрів, що контролюються. При обчисленнях дуже важливим є виключення з історичної вибірки поганих прикладів або аномальних викидів [6]. Добрі результати отримані при використанні апарату нечіткої логіки для зменшення невизначеності вихідних даних [14]. Мабуть, найбільш складним для цієї технології біометричної ідентифікації є питання про присутність у користувача індивідуального клавіатурного почерку. Розробляються спеціальні обчислювальні процедури, що дозволяють відповісти на це питання і виміряти міру стабільності і індивідуальності клавіатурного почерку конкретного користувача [7].

Ідентифікація за почерком миші

Існуючі дослідження моніторингу маніпулятора миша при роботі користувача в системі показують надійність розпізнавання 0,8 – 0,9 [5]. При цьому екран розбивається на зони, в яких курсор миші знаходиться найчастіше і кожні дві хвилини аналізуються характеристики руху миші між зонами. Пропонується моніторинг всього процесу еволюції системи «користувач-миша» впродовж тривалого (потенційно необмеженого) інтервалу часу спостереження за користувачем [11].

При використанні ідентифікації за динамічними характеристиками насамперед необхідно визначити спосіб представлення набору числових значень. При аналізі підпису можна виділити координати характерних точок (екстремуми точки розриву підписів і так далі) та інші параметри траєкторії. Після вибору ключових значень можна розпочати накопичення бази зразків характеристик користувачів, на підставі порівняння з якими здійснюватиметься ідентифікація (еталонні зразки).

Також необхідно зробити важливе обмеження: всі траєкторії будемо вважати осмисленими, тобто користувач їх продукує в процесі повсякденної діяльності і з певною метою – маніпулювання певними елементами управління програмного забезпечення. В такому випадку генеровані траєкторії зумовлені такими факторами: антропологічними, фізіологічними, психологічними.

Насправді, це очевидно. Антропологічні дані людини (довжина ліктьового суглоба і розміри зап’ястя) впливають на таку характеристику, як радіус кривизни траєкторії. Фізіологічні дані людини, такі як структура м’язів ліктьового і плечового суглобів, впливають на швидкість і прискорення руху курсору, тобто динаміку руху. З іншого боку, психологічні фактори також впливають на зазначені характеристики, вводячи додатково елементи звички при виконанні робочих операцій. Таким чином, наведені фактори вступають у взаємозв’язок між собою і постійно впливають на процес генерування траєкторії. Загалом, задача аналізу вказаних траєкторій має аналоги із задачею аналізу рукописного тексту або рукописних підписів. Проте комп’ютерна система дає змогу розглянути цей процес в динаміці і скористатися додатковою інформацією про динаміку руху курсору.

Для аналізу отриманих на попередньому етапі характеристик нині вироблено декілька підходів:

– статистичний аналіз: обчислюється середнє кожного з ключових значень, його середньоквадратичне відхилення і здійснюється перевірка належності ключових значень зразка, що пред'являється, довірчим інтервалам, отриманим з аналізу еталонних зразків;
– застосування нейронних мереж;
– застосування байєсівських мереж;
– застосування прихованих моделей Маркова.

Аналіз почерку миші може здійснюватись повністю, або виконується попередня сегментація почерку з подальшим аналізом сегментів. У випадку аналізу почерку як цілісного об'єкту може застосовуватись спектральний аналіз [8].

У табл. 4 наведено порівняльний аналіз кожного з існуючих підходів до ідентифікації користувача за почерком миші [9]. В ході виконаної роботи були розглянуті біометричні методи ідентифікації користувачів.

Таблиця 4 – Порівняльний аналіз існуючих підходів до ідентифікації користувача за динамікою рухів маніпулятора «миші»

Метод	**Порівнювані характеристики / алгоритм ухвалення рішення**	**Розмір бази даних, ймовірність помилок**
Порівняння рядків	– глобальні характеристики – сполучні штрихи	20 – 103 користувачів, 10 – 30 підписів від кожного. Ймовірність помилки 3 – 5%
Приховані моделі Маркова	– алгоритм Баума – Велха – алгоритм Вітербі	14 – 15 користувачів, 20 – 30 підписів від кожного. Ймовірність помилки 1 – 4%
Нейронні мережі	– багатошаровий персептрон	27 користувачів, 30 підписів від кожного. Ймовірність помилки 4%
Байєсівські мережі	– метод головних компонент	27 користувачів, 30 підписів від кожного. Ймовірність помилки 0,5 4%

V Висновки

У результаті критичного огляду біометричних методів ідентифікації встановлено, що найменш вивченими та найбільш перспективними для подальшого дослідження виявились динамічні методи біометричної ідентифікації, побудовані на основі аналізу особливостей підсвідомих рухів. Зокрема, методи, що аналізують особливості інформаційного (комп'ютерного) почерку. Це особливо актуально в умовах, коли майже кожне робоче місце неможливо уявити без персональних комп'ютерів.

Однією з важливих переваг динамічних біометричних методів ідентифікації і, зокрема, ідентифікації за динамікою інформаційного почерку, є дешевизна і простота реалізації, оскільки в даному випадку не потрібне додаткове дороге устаткування, наприклад, для сканування сітківки ока. Реалізація такої системи дозволить здійснювати постійний контроль за доступом до конфіденційної інформації та ефективно протидіяти інформаційному шпигунству і витоку інформації. Проте, виграючи в дешевизні і простоті, ідентифікація за інформаційним підписом програє в точності розпізнавання.

Необхідно відзначити, що найбільшу ефективність захисту забезпечують системи, в яких біометричні методи поєднуються з іншими апаратними засобами автентифікації або декількома різними типами біометричної ідентифікації. Комбінуючи різні способи біометричної і апаратної автентифікації, можна отримати надійну систему захисту (що підтверджується великою зацікавленістю, яку проявляють до цих технологій провідні виробники програмного забезпечення).

Таким чином, в подальших дослідженнях доцільно сконцентрувати увагу на підвищенні якості ідентифікації за допомогою динамічних методів біометричної ідентифікації з використанням сучасних методів статистичного і ймовірнісного моделювання.

*Література: **1**. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений – Пенза: Издательство Пензенского государственного университета, 2000, С. 188. **2**. Голубев Г. А., Габриелян Б. А. Современное состояние и перспективы развития биометрических*

технологий // Нейрокомпьютеры. Разработка. Применение. № 10, 2004, – С. 39 – 46. ***3****. Беленков В. Д. Электронные системы идентификации подписей // Защита информации. Конфидент. 1997, № 6, – С.39 – 42.* ***4.*** *Plomondon R., Lorette G. Automatic signature verification and writer identification – the state of the art // Pattern Recognition 1999 – Vol. – 22, № 2, p. 107 – 131.* ***5****. Диденко С. М. Автореферат дисертации: «Разработка и исследование компьютерной модели динамики системы «пользователь-мышь»». Тюмень 2007. – 25 с.* ***6****. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.:"Яхтсмен", 1993. – 150 с.* ***7****. Рыбченко Д. Е. Критерии устойчивости и индивидуальности клавиатурного почерка при вводе ключевых фраз // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. Пенза, ПНИЭИ, 1997, Выпуск № 2. – С.104 –107.* ***8.*** *Колядин Д. В., Савин А. А. О проблеме верификации подписи в системах контроля доступа.* http://cs.mitp.ru/docs.research/signature.html ***9.*** *Griess F. D., Jain A. F. Project Report: Online signature verification /* http://www.cse.msu.edu/cgi-user/web/tech/document?ID=449 ***10.*** *Дворянкин С. В. Речевая подпись / Под ред. заслуженного деятеля науки РФ, д.т.н. проф. А. В. Петракова. – М.: РИО МТУСИ, 2003 – С. 183 – 184.* ***11.*** *Широчин В. П., Кулик А. В., Марченко В. В. Динамическая аутентификация на основе анализа клавиатурного почерка. - http://www.masters.donntu.edu.ua/2002/fvti/aslamov/files/bio_autentification.htm* ***12.*** *Resources Related to Biometrics and People with Disabilities. The International Center for Disability Resources on the Internet.* http://www.icdri.org/biometrics/biometrics.htm. ***13.*** *Рабинер Л. Р., Шафер Р. В. Цифровая обработка речевых сигналов: Пер. с англ./Под ред. М. В. Назарова, Ю. Н. Прохорова.– М.: Радио и связь, 1981.– 495 с.* ***14.*** *Рыбченко Д. Е., Иванов А. И. Анализ клавиатурного почерка аппаратом нечетких множеств для целей ограничения доступа и аудита // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. Пенза, ПНИЭИ, 1996, Выпуск №1., – С.116 – 119.*