

6. Левицький К. Історія політичної думки галицьких українців. 1848-1914. – Львів: З друкарні о.Василян, 1926. С. 492.
7. Мельник В. Діяльність Теофіла та Ярослава Окуневських у віденській «Січі» // Схід, № 9 (100), грудень 2009, с. 50-54.
8. Окуневський Т. Станиславів у 1880-их роках / Теофіл Окуневський / Альманах Станиславівської землі. Наукове Товариство ім. Шевченка. Український Архів. Т. XXVIII. – Нью-Йорк; Торонто; Мюнхен, 1975. – С.103.
9. Переписка Михайла Драгоманова з д-ром Теофілом Окуневським (1883, 1885-1891, 1893-1895) / Драгоманов М., Окуневський Т.; Зладив М.Павлик. – Львів : З «Народової Друк.» Манецьких, 1905. – С.47-48.
10. Про суд над нашим студентством//Діло 1907 14 вересня
11. Якимович Б. „Гей, „Січ” іде, красен мак цвіте...”. Львів, 2000. С.31-32.
12. Яшан В. Д-р Теофіл Окуневський/ Городеничина. Історико-мемуарний збірник. – Нью-Йорк – Торонто – Вінніпег. 1978. С.580
13. Яшан В. Паціфікація в Городенці і Городенківському повіті / Городеничина. Історико-мемуарний збірник. – Нью-Йорк – Торонто – Вінніпег. 1978. С.225
14. Яшан В. Судівництво та адвокатура й адміністрація / Городеничина. Історико-мемуарний збірник. – Нью-Йорк – Торонто – Вінніпег. 1978. С.94

УДК 65.012.8

**В.П. Захаров**

*Львівський державний університет внутрішніх справ*

**О.І. Зачек**

*Львівський державний університет внутрішніх справ*

## **ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ**

**В статті розглянуті сучасні тенденції використання біометричних технологій в системах захисту інформації та даються пропозиції щодо їх використання в правоохоронних органах України.**

**Ключові слова:** *біометрія, методи біометричної автентифікації, дактилоскопія, автоматизовані дактилоскопічні ідентифікаційні системи, системи контролю та управління доступом.*

**В статье рассмотрены современные тенденции использования биометрических технологий в системах защиты информации и даются предложения по их использованию в правоохранительных органах Украины.**

**Ключевые слова:** *биометрия, методы биометрической аутентификации, дактилоскопия, автоматизированные дактилоскопические идентификационные системы, системы контроля и управления доступом.*

**We considered the modern trend of using biometric technologies in the systems of information protection and given suggestions for their use in law enforcement bodies of the Ukraine.**

**Key words:** *biometrics, biometric methods of authentication, fingerprinting, automatic fingerprint identification systems, access control.*

**Постановка проблеми.** Такі виклики сьогодення, як кібертероризм та кіберзлочинність, спричиняють необхідність подальшого розвитку систем захисту інформації у всіх галузях суспільної практики і, зокрема, в діяльності правоохоронних органів. Одним з перспективних напрямів розвитку систем захисту інформації є використання біометричних технологій.

До 11 вересня 2001 року біометричні системи доступу використовувалися в основному тільки для захисту військових секретів та найважливішої комерційної інформації [1]. Але після теракту в Нью-Йорку ситуація різко змінилася. Так наприклад, серед громадян США всього 10 % підтримувало ідею біометричної паспортизації до 11 вересня 2001 року і вже понад 75 % – після теракту, коли відстеження потенційно небезпечних особистостей стало першорядним завданням [2]. На даний час попит на системи, які використовують біометричні технології, значно зріс, зросла кількість галузей їх використання та вдосконалилися технології. Відбулося зниження вартості елементів таких систем, що позитивно впливає на зростання розвитку. Наприклад, до недавнього часу вартість дактилоскопічних систем становила \$ 2000-5000 США, а після створення мініатюрного мікроелектронного дактилосканера вартість біометричного захисту комп'ютерів знижена до \$ 50 – 100 США [2].

Злочинці використовують найсучасніші методи здобуття інформації, особливо їх цікавить інформація, яка використовується правоохоронними органами в процесі боротьби зі злочинністю. Тому нагальною є потреба

використання найбільш сучасних методів захисту інформації та проведення наукових розробок в цьому напрямі. Використання біометричних технологій і є найбільш актуальним напрямом в галузі захисту інформації.

**Стан дослідження.** Проблемам використання біометричних технологій для захисту інформації присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах, зокрема, таких вчених: Захаров В.П., Рудешко В.І., Барсуков В.С., Двоєносова Г., Двоєносова М., Козирев С.П., Корченко А.О., Мацьків Н.С., Гречишкіна О.М., Кухарев Г. А., Дубчак О.В., Підгайна К.І., Брюхомицкий Ю.А., Казарин М.Н., Іванов А.І., Урсуленко І.В., Полєнніков М.О.

Важливість наукового здобутку та внеску у теорію і практику інформаційної безпеки згаданих вчених важко переоцінити. Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування біометричних систем захисту інформації є певні недоліки, які знижують ефективність їх функціонування.

**Мета дослідження.** Біометричні технології захисту інформації використовують різні параметри особи з метою її автентифікації. Метою даної статті є розгляд сучасних тенденцій використання біометричних технологій, зокрема, в системах захисту інформації правоохоронних органів України.

**Виклад основних положень.** Згідно визначення Двоєносової, біометрія – це наукова дисципліна, що вивчає способи вимірювання різних параметрів людини з метою встановлення подібності або різниці між людьми та виділення однієї конкретної людини з множини інших людей. Слово "біометрія" перекладається з грецької мови як "вимірювання життя" [3].

Методи біометричної автентифікації поділяються на статичні та динамічні. Статичні методи використовують наступні фізіологічні характеристики людини: відбитки пальців, форма долоні, малюнок вен на долоні чи пальцях руки, малюнок райдужної оболонки ока, малюнок кровоносних судин сітківки ока, двовимірне або тривимірне зображення форми обличчя, термографія обличчя, руки або пальця, ДНК та інші методи. Динамічні ж методи використовують поведінкові характеристики людини при виконанні різних рухів. До цих методів належить автентифікація за рукописним почерком (за підписом), за клавіатурним почерком, за голосом та інші методики.

Не всі з перелічених методів є в однаковій мірі зручними. Дубчак О.В. вважає [4], що системи розпізнавання за сітківкою або райдужною оболонкою ока або за відбитками пальців незручні на практиці через жорсткі вимоги до порядку сканування відповідних біометричних характеристик людини. Крім того, на його думку, користувачі дактилоскопічних систем розпізнавання стурбовані гігієнічністю циклу, а систем розпізнавання за радужною оболонкою – твердими вимогами до рухів і ступеня видимості деяких значимих частин ока. Цей автор вважає, що способи розпізнавання за обличчям особи та її голосом мають відчутну перевагу: відеозапис і аудіозапис не вимагають фізичного контакту користувача із системою й ретельного позиціонування перед реєструючим сенсором [4].

Але найбільш широко вживаним на даний час є використання систем розпізнавання за відбитками пальців. Ця біометрична технологія на сьогодні має найбільшу кількість напрямків використання та застосувань з усіх біометричних технологій. Це обумовлено невисокою вартістю порівняно з іншими методами біометричної ідентифікації, а також високою точністю у зв'язку з незмінністю біометричної ознаки. На думку деяких авторів (Anil K. Jain, Michigan State University, Jianjiang Feng, Tsinghua University, Beijing, Karthik Nandakumar, Institute for Infocomm Research, Singapore) [5] основними причинами популярності методів розпізнавання за відбитками пальців є:

- успішність їх використання в різних криміналістичних, урядових та цивільних додатках;
- той факт, що злочинці часто залишають відбитки пальців на місці злочину;
- наявність великих спадкових баз даних;
- доступність компактних та недорогих пристроїв для зняття відбитків пальців.

Дактилоскопія ("пальцездивляння": від грецького "daktylos – палець" та "skopeo – дивлюся") – це розділ криміналістики, що вивчає будову візерунків шкіри внутрішніх поверхонь нігтьових фаланг пальців та долонь для ідентифікації особистості, кримінальної реєстрації та розшуку злочинця [1].

Наприкінці ХХ століття розпочалася експлуатація автоматизованих дактилоскопічних ідентифікаційних систем (АДІС). Піонерами у створенні єдиних масивів дактилоскопічної інформації є Німеччина, Ізраїль, Швейцарія, Франція, Угорщина та інші країни. В Україні перші автоматизовані системи запроваджуються з 1992 року в Луганській, Київській, Миколаївській областях, м. Києві та в Криму. Сьогодні вони функціонують у всіх підрозділах експертної служби МВС України. Сьогодні в експертній службі МВС України використовується цілий ряд автоматизованих систем, представлених автоматизованими дактилоскопічними комплексами, ідентифікаційними системами, програмно-апаратними комплексами, інформаційно-пошуковими системами, які відрізняються як апаратною реалізацією, так і організаційною структурою, що пояснюється часом створення, комплексом виконуваних завдань, різноманітністю використаного програмного забезпечення, рівнем взаємодії з іншими базами даних. У 2002 р. комісією МВС України у складі працівників експертної служби, ДІТ МВС України, НДІ "Спецтехніка" проведено тестування АДІС зарубіжних та вітчизняних виробників. За результатами тестування тільки дві АДІС – "Дакто 2000" та "Сонда" – були визнані такими, що можуть застосовуватися на всіх рівнях (центральному, обласному та місцевому) дактилоскопічних обліків МВС України. Тому для ведення дактилоскопічних обліків та досліджень МВС України використовує саме ці АДІС [6].

В процесі проведення криміналістичних досліджень та під час зіставлення за допомогою АДІС відбувається ідентифікація особи за наявними відбитками пальців, а під час застосування біометричних технологій для створення систем безпеки здійснюють верифікацію особи.

Використання біометричних технологій на основі дактилоскопії є дуже популярним для забезпечення контролю доступу до комп'ютера та комп'ютерних мереж, внаслідок чого користувачу не потрібно запам'ятовувати пароль, досить зісканувати відбиток пальця. Дуже перспективним є використання вищезазначених технологій в системах контролю та управління доступом, що дозволяє підвищити рівень безпеки.

Але біометричні технології, які базуються на використанні відбитків пальців мають і недоліки. Неодноразово в засобах масової інформації з'являлися повідомлення про успішні спроби фальсифікації відбитків пальців для зламу систем захисту на основі дактилоскопії. Найбільш свіжим є повідомлення від 23 вересня цього року [7] про те, що команда біометричних хакерів Chaos Computer Club (CCC) успішно обійшла механізм біометричного захисту Apple Touch ID в iPhone 5S, який позиціонувався як такий, що неможливо зламати. Для зламу був використаний відбиток пальця власника, що був залишений на гладкій поверхні. Відбиток був сфотографований з мінімальною роздільною здатністю 2400dpi, зображення оброблене у програмі Photoshop, інвертоване та роздруковане на лазерному принтері з мінімальною роздільною здатністю 1200dpi поверх прозорого листа таким чином, щоб надрукований шар мав відчутну товщину. Потім візерунок змащується столярним клеєм, плівка якого після висихання віддирається, трохи зволожується диханням з рота і потім поміщається на читувач відбитків. Ця технологія зламу була перевірена на більшості інших систем захисту, які є на ринку [7].

**Висновки.** Використання біометричних технологій є перспективним і найчастіше вони використовуються в біометричних методиках на основі дактилоскопії, в той же час мають невисоку стійкість до зламу зловмисниками. Найкращим способом подолання цього є використання мультибіометричних систем, тобто таких, де здійснюється ідентифікація за двома та більше біометричними параметрами.

Правоохоронні органи України на даний час використовують лише ідентифікацію особи на основі АДІС. Для забезпечення достатнього рівня захисту інформації доцільним є застосування біометричних технологій для контролю доступу до комп'ютерів, комп'ютерних мереж та в приміщення, але з врахуванням вищезгаданих недоліків.

#### Список використаної літератури

1. Захаров В.П., Рудешко В.І. Використання біометричних технологій правоохоронними органами у XXI столітті: науково-практичний посібник / В.П. Захаров, В.І. Рудешко. – Львів: ЛьвДУВС, 2009. – 440 с.
2. Барсуков В.С. Біоключ – шлях до безпеки // <http://kvartir-remont.com.ua/biokljuch-shljah-do-bezpeki>.
3. Двоеносова Г. , Двоеносова М. Биометрия как наука, метод и способ документирования. // Журнал "Управление персоналом" № 11, 2009 г.
4. Дубчак О. В., Урсуленко І.В. Оцінювання ефективності біометричних методів // [http://www.rusnauka.com/27\\_NNM\\_2011/Informatica/4\\_93650.doc.htm](http://www.rusnauka.com/27_NNM_2011/Informatica/4_93650.doc.htm)
5. Кузнецов С. Биометрия на службе охраны правопорядка и безопасности. Обзор февральского 2010 г. номера журнала Computer (IEEE Computer Society, V. 43, No 2, февраль, 2010) // <http://citforum.ru/computer/2010-02>.
6. Автоматизована дактилоскопічна ідентифікаційна система "Сонда": Методичні рекомендації для виконання лабораторних робіт з дисципліни "Інформаційно-пошукові системи ОВС" // І.С. Керницький, О.І.Зачек, В.М. Фірман, А.О. Полтавський. – Львів: Львівський державний університет внутрішніх справ, 2009. – 111 с., з іл. і табл.
7. Соя О. Chaos Computer Club зламують Touch ID. Гаджети українською від 23.09.2013р. // <http://vinsee.com.ua/chaos-computer-club-zlamuyut-touch-id>