вопроса о дополнении уголовных кодексов как России, так и Украины нормами об уголовной ответственности именно за международный терроризм.

Возможные возражения на такую постановку проблемы, связанные с отсутствием общепризнанного определения этого понятия, вряд ли могут считаться серьезным доводом против криминализации международного терроризма в национальном уголовном законодательстве. Ибо, как учит история борьбы с терроризмом, первые национальные законы об уголовной ответственности за него появились в мире задолго до признаваемой большинством государств дефиниции (первым специальным актом в этой области стал Указ Временного государственного совета Государства Израиль о пресечении терроризма 1948 г.[1]) и, по крайней мере, за 15 лет до рождения первой антитеррористической конвенции ООН – Конвенции о преступлениях и некоторых других актах, совершаемых на борту воздушных судов 1963 года.

К тому же, наличие в национальном уголовном законодательстве широкого круга стран норм об ответственности именно за международный терроризм видится необходимым предварительным условием универсального признания будущей Всеобъемлющей конвенции о международном терроризме.

УДК 65.012.8:343.982.34

В.П. Захаров

ТЕНДЕНЦІЇ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ, ЯКІ НЕ ВХОДЯТЬ ДО "ТРЬОХ ВЕЛИКИХ БІОМЕТРИК", У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

У статті розглянуті сучасні тенденції використання в системах захисту інформації біометричних технологій, які не входять до "трьох великих біометрик", а саме: ідентифікації за ДНК, за зображенням кисті руки, малюнком вен долоні або пальця руки, термограмою обличчя, формами вушних раковин, запахом, голосом, підписом, клавіатурним почерком, шляхом аналізу біоелектричної активності мозку й даються пропозиції щодо їх використання в правоохоронних органах України.

Ключові слова: *біометрія, методи біометричної автентифікації, ідентифікація за ДНК, ідентифікація за зображенням кисті руки, ідентифікація за малюнком вен долоні або пальця руки, ідентифікація за термограмою обличчя, ідентифікація за формами вушних раковин, ідентифікація за запахом, ідентифікація за голосом, ідентифікація за підписом, ідентифікація за клавіатурним почерком, ідентифікація*

[1] Prevention of Terrorism Ordinance № 33 of 5708-1948Official Gazette, No. 24 of the 25th Elul, 5708 (29th September, 1948).

шляхом аналізу біоелектричної активності мозку, системи контролю та управління доступом.

В статье рассмотрены современные тенденции использования в системах защиты информации биометрических технологий, которые не входят в "три большие биометрики", а именно: идентификация по ДНК, по изображению кисти руки, рисунку вен ладони или пальца руки, термограмме лица, форме ушных раковин, запаху, голосу, подписи, клавиатурному почерку, путём анализа биоэлектрической активности мозга и даются предложения по их использованию в правоохранительных органах Украины.

Ключевые слова: *биометрия, методы биометрической аутентификации, идентификация по ДНК, идентификация по изображению кисти руки, идентификация по рисунку вен ладони или пальца руки, идентификация по термограмме лица, идентификация по форме ушных раковин, идентификация по запаху, идентификация по голосу, идентификация по подписи, идентификация по клавиатурному почерку, идентификация путём анализа биоэлектрической активности мозга, системы контроля и управления доступом.*

We considered the modern trend of using in the systems of information protection of biometric technologies, that are not part of the "three big biometrics", namely the identification of DNA, by the image of the hand, with vein pattern palm or fingers, by facial thermogram, by type ears, by the smell, by the voice, by signature, by handwriting keyboard, by analyzing the bioelectrical activity of the brain, and given suggestions for their use in law enforcement bodies of the Ukraine.

Key words: *biometrics, biometric methods of authentication, the identification of DNA, the identification by the image of the hand, the identification with vein pattern palm or fingers, the identification by facial thermogram, the identification by type ears, the identification by the smell, the identification by the voice, the identification by signature, the identification by handwriting keyboard, the identification by analyzing the bioelectrical activity of the brain, checking and access control systems.*

Постановка проблеми. Розробки в галузі захисту інформації є надзвичайно актуальними на сьогоднішній день, коли злочинці намагаються заволодіти інформацією за допомогою сучасних високих технологій. Адже всі знають, що той, хто володіє інформацією, той володіє світом. А якщо злочинці заволодіють інформацією, яка використовується в діяльності правоохоронних органів, то вони зможуть значно ефективніше здійснювати протиправну діяльність. Також актуальними є розробки в галузі систем управління доступом, які використовуються в комплексних системах захисту інформації як важлива складова.

Найбільш сучасним напрямом розробок у вище названих галузях є використання біометричних технологій. Біометричні технології мають низку переваг порівняно з традиційними методами ідентифікації осіб для надання їм права доступу до інформації. Є біометричні методики, які

використовуються вже традиційно, а є такі, які досі вважаються екзотичними. Але не слід забувати, що до недавнього минулого взагалі будь-які біометричні технології вважалися екзотикою.

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 осіб 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 подальший розвиток. 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]. Тому запровадження в практичну діяльність новітніх біометричних технологій, навіть таких, які зараз є незвичними та перебувають в зародковому стані, є справою недалекого майбутнього.

Але розробки в галузі використання таких методик потрібно проводити вже сьогодні. Необхідно визначити, які з цих технологій є найбільш придатними для застосування в правоохоронних органах як з точки зору надійності, так і з точки зору економічної доступності.

Стан дослідження. Проблемам використання біометричних технологій для захисту інформації присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах, зокрема, таких учених: 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., Брюхомицький Ю.А., Казарин М.Н., Іванов А.І., Урсуленко І.В., Полєнніков М.О., Попов М., Воронина Н., Прохоров А., Семко Ю., Пономаренко Л. В.

Важливість наукового здобутку та внеску в теорію і практику інформаційної безпеки згаданих учених важко переоцінити. Аналіз літературних джерел дає підстави стверджувати, що в процесі проектування, створення й 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 статті є розгляд сучасних тенденцій використання біометричних технологій, зокрема, у системах захисту інформації правоохоронних органів України.

Виклад основних положень.

Біометрія використовується для визначення права доступу осіб до інформації на основі їх ідентифікації за допомогою індивідуальних особливостей тіла цих осіб.

З точки зору поширеності біометричних методик виділяють "три великі біометрики": ідентифікація за відбитками пальців, за геометрією обличчя та за райдужною оболонкою ока. Як вважають деякі автори, системи ідентифікації за відбитками пальців займають більше половини ринку біометричних технологій, системи на основі технології розпізнавання за геометрією обличчя – 13-18 %, а системи на основі ідентифікації за райдужною оболонкою ока – 6-9 % [3]. І в значно меншій мірі в системах захисту інформації використовуються такі методики, як ідентифікація за сітківкою ока, за ДНК, за зображенням кисті руки, за малюнком вен долоні або пальця руки, за термограмою обличчя, за формами вушних раковин, за запахом, за голосом, за підписом, за клавіатурним почерком та шляхом аналізу біоелектричної активності мозку.

Найбільш надійним з практично реалізованих методів вважається метод сканування сітківки ока. Тому він використовується в системах контролю доступу на особливо секретні об'єкти. Із-за низького рівня поширення таких систем малою є вірогідність реалізації спроб зламу. Але недоліком є висока вартість систем із використанням цього методу.

Сполучення нуклеотидів у ланцюжок ДНК (дезоксирибонуклеїнова кислота) складає генетичний код будь-якої живої істоти [1]. Ідентифікація за ДНК здійснюється шляхом порівняння ДНК особи з ДНК контрольних зразків. Але на сьогодні ця методика використовується лише для ідентифікації особи в криміналістиці, а в системах захисту інформації вона наразі не знайшла використання внаслідок високої вартості та складності обладнання.

Ідентифікація за формою долоні або за геометрією кисті базується на побудові трьохвимірного зображення кисті руки. Для здійснення ідентифікації знімаються такі характеристики пальців чи долоні, як довжина, ширина, товщина та параметри поверхні шкіри. Загалом оцінюється понад 90 різних характеристик. Недоліком методу є зміни кисті руки протягом життя, що спричиняє низьку надійність. Тому цей метод розглядається лише як доповнення до інших біометричних технологій [1]. Хоча є приклади його успішного використання в практичній діяльності. Одним з пристроїв, що використовує цю методику, є Handkey компанії Escape (США), який сканує внутрішню та бокову сторони долоні за допомогою вбудованої відеокамери із застосуванням алгоритмів стискання. Також є пристрій ID3D-R Handkey компанії Recognition Systems (США) [2]. Декілька компаній, зокрема, BioMet Partners, Palmetrics и BTG розробляють пристрої, які можуть сканувати також інші параметри руки [4].

Розпізнавання за венами руки базується на використанні знімків зовнішньої та внутрішньої сторін руки. Оскільки гемоглобін крові поглинає інфрачервоне випромінювання, ступінь відбиття променів зменшується і вени стають видимими у вигляді чорних ліній. А рисунок вен у кожної людини є індивідуальним. Сканування можна робити безконтактно. Ця технологія за надійністю є порівняною з ідентифікацією за райдужною оболонкою ока. Недоліком є вплив деяких хвороб, зокрема, артриту. А перевагою є менш дороге обладнання при високій точності. Наприклад, обладнання є дешевшим, ніж для методів розпізнавання за геометрією обличчя чи за райдужною оболонкою. Розробками обладнання та програмного забезпечення займаються компанії Fujitsu, Veid Pte. Ltd., Hitachi VeinID [3].

Компанія "Hitachi" виготовляє систему "Finger Vein", яка використовує зображення малюнка вен будь-якого пальця особи, оскільки малюнок вен на пальці, як і на долоні, неможливо підробити. FRR цієї системи становить 0.01%, а FAR – 0.0001% [1].

Термографічна картина обличчя, отримана за допомогою інфрачервоної камери, залежить від густини кісток, жиру та кровоносних судин і є суто індивідуальною ознакою. Точність цього методу є дуже високою і дозволяє розрізняти навіть близнюків. Цей метод не залежить від застосування косметики, макіяжу, пластичної хірургії та дозволяє проводити розпізнання негласно [5].

Оскільки форми вушних раковин є індивідуальними, то вони теж дозволяють ідентифікувати особу. Навіть недорога Web-камера дає змогу з високою надійністю здійснювати ідентифікацію [5]. Але відомостей про виробництво приладів для такої ідентифікації немає.

Давно відомою є здатність собак розпізнавати людей за запахом. На сьогодні вже здійснюються розробки "електронного носа", який містить системи відбору проб запахів та їх підготовки, матриці сенсорів, які сприйматимуть запахи та процесору для обробки сигналів матриці сенсорів. Але ці розробки ще далекі від практичної реалізації [5].

Вищеперераховані методи належать до статичних, які використовують фізіологічні параметри людини, що не змінюються в часі. Крім них є динамічні методи, які базуються на індивідуальних поведінкових особливостях людини. До них належать голосова ідентифікація, ідентифікація за підписом, за клавіатурним почерком, за біоелектричною активністю мозку. Але ці технології не забезпечують високої точності та надійності ідентифікації.

Одним із методів, які дозволяють розпізнавати особу на відстані та негласно, є голосова ідентифікація. Перевагами є дешевизна цього методу, оскільки потрібні лише мікрофон та звукова карта, яка є тепер в кожному комп'ютері, та відсутність психологічного дискомфорту під час іде-

нтифікації [6]. Під час ідентифікації за голосом аналізуються висота тону, модуляція, інтонація тощо. Але надійність і точність цього методу не є високими, оскільки голос може залежати від стану здоров'я та поведінкових факторів [7]. Одним із розробників технологій розпізнавання особи за голосом є російське товариство з обмеженою відповідальністю "Центр мовних технологій" [1].

Одним з найбільш звичних для нас методів ідентифікації особи є її підпис. Якщо підпис як графічне зображення можна підробити, то поведінку руки особи під час підпису скопіювати неможливо. Біометричний метод ідентифікації людини за підписом базується на аналізі швидкості руху руки, сили тиску та тривалості виконання етапів підпису. Людина імітує свій звичний підпис, а прилад знімає параметри руху та звіряє з наявними в базі даних. Але цей метод не можна використовувати в системах контролю доступу, він має перспективи в тих галузях, де підписуються важливі документи, наприклад, у банківській сфері [7]. У галузі розпізнавання підпису було видано сотні патентів фірмам "IBM", "NCR", "VISA", "Adapteck" [1].

Метод ідентифікації за клавіатурним почерком схожий на ідентифікацію за підписом, але тут використовується введення кодового слова на стандартній клавіатурі комп'ютера. Основною характеристикою є динаміка набору кодового слова [7]. Перевагою є використання звичайного комп'ютера. Такий метод наразі не є поширеним, але розробки в цій галузі здійснюються. Наприклад, компанія "BioPassword Inc." розробила програму перевірки особистості користувача комп'ютера за ритмічними характеристиками набору тексту [1].

Ідентифікація шляхом аналізу біоелектричної активності мозку базується на електроенцефалографії. За допомогою шапочки з електродами система здійснює моніторинг електричної активності мозку, передає дані на комп'ютер і формує цифровий портрет електричної активності мозку особи. Під час ідентифікації знята енцефалограма порівнюється з еталонною. Але ряд фахівців вважає, що така ідентифікація не набуде практичного використання через свою непрактичність[1].

Найбільша ефективність захисту інформації досягається шляхом комбінації різних методів ідентифікації. Наприклад, НПФ "Кристал" (Росія) виготовляє систему захисту інформації "Рубіж", де комбіновано використовуються голосова ідентифікація, ідентифікація за динамікою підпису та за персональним кодом ключа "Touch memory" [2].

Висновки.

На сьогоднішній день в системах захисту інформації правоохоронних органів України не використовуються вищезазначені методи ідентифікації особи. Розглянувши переваги та недоліки, а також існуючі практичні реалізації цих методів, можна дійти висновку, що для практичного

використання в правоохоронних органах України сьогодні можна рекомендувати ідентифікацію за геометрією кисті, за венами руки та пальців і за голосом. Ці методи не вимагають дорогого обладнання й програмного забезпечення, які до того ж є у продажу. Також доцільною є розробка такого обладнання і програмного забезпечення в Україні, оскільки науковий та промисловий потенціал нашої держави це дозволяє.

Використана література:

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. Современные биометрические методы идентификации. Хабрахабр від 11.08.2011 // http:// habrahabr.ru/post/126144.

4. Попов М. Биометрические системы безопасности. БДИ №1(41), 2002 // http://www.bre.ru/security/12571.html

5. Воронина Н., Прохоров А., Семко Ю. Биометрические пароли. КомпьютерПресс №3'2002. // http://www.compress.ru/article.aspx?id=10058 &iid=419

6. Пономаренко Л. В. Система захисту від несанкціонованого доступу на основі голосової автентифікації: Дисертація канд. наук: 05.13.21 – 2009 // http://www.lib.ua-ru.net/diss/cont/355488.html

7. Шаров В. Биометрические методы компьютерной безопасности. ByteРоссия №4 (80), апрель 2005 // http://www.bytemag.ru/articles/detail.php?ID=6719

УДК 343.163:351.746.2(477)

Д.О. Бабічев
В.Л. Соколкін

ДОКТРИНАЛЬНІ ЗАСАДИ ТА ПРАКТИКА ПРОКУРОРСЬКОГО НАГЛЯДУ ЗА ЗАКОННІСТЮ РІШЕНЬ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Використовуючи результати змістовного дослідження чинного законодавства України, літературних джерел, прокурорської та оперативно-розшукової практики в статті обґрунтовується авторська позиція щодо особливостей прокурорського нагляду за законністю рішень в оперативно-розшуковій діяльності.

Ключові слова: *прокурорський нагляд, оперативно-розшукова діяльність, законність, рішення в оперативно-розшуковій діяльності, оперативно-розшукова справа.*

Используя результаты исследования действующего законодательства Украины, литературных источников, прокурорской и оперативно-розыскной практики в статье обосновывается авторская позиция относительно особенно-