

– кореляція на основі групування подій інформаційній безпеки без чітко визначеного критерію на основі помилок відновлення за допомогою нейронних мереж;

– кореляція на основі навчання моделі і побудови шаблонів помилкових і істинних подій, заснованих на помічених системним оператором даних.

Список бібліографічних посилань

1. Узлов Д. Ю. Використання методів і моделей інтелектуальної обробки неструктурованої криміналістичної інформації // Інтелектуальні системи та прикладна лінгвістика : матеріали III Всеукраїнської науково-практичної конференції. Харків : НТУ «ХПІ», 2014. С. 13-15.

2. Manning C. D., Raghavan P., Schütze H. Introduction to Information Retrieval. Cambridge : Cambridge University Press, 2008. 544 p.

3. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologies. New York : CRC Press Taylor & Francis Group, 2009. 440 p.

Одержано 02.11.2018

УДК 343.98

Станіслав Олександрович ФІЛІПОВ,

кандидат психологічних наук, доцент, докторант

Національної академії Державної прикордонної служби України;

ORCID: <https://orcid.org/0000-0001-6700-4194>

ЗНАЧЕННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ДЛЯ ПРОТИДІЇ ТРАНСКОРДОННІЙ ЗЛОЧИННОСТІ

Своєчасна та повна необхідна інформація про осіб, що перетинають державний кордон, забезпечує функціонування системи протидії транскордонній злочинності саме у той спосіб, що відповідає характеристикам оптимальності та ефективності. Беззаперечним чинником, що детермінує дієвість системи прикордонної безпеки, є наявність умов, за яких застосування персональних даних і документів для вчинення транскордонних кримінальних правопорушень або взагалі є неможливим, або створює можливість для їх подальшого припинення. На посилення цієї дієвості працює впровадження біометричних технологій у виготовлення документів для виїзду за кордон (далі – проїзних документів). Це дозволяє не тільки підняти рівень їх захисту, а також забезпечує можливість ідентифікації за таким набором персональних даних, що виключає помилку. У свою чергу, це значно посилює можливість як запобігання злочинності, так і припинення окремих злочинів.

I. Підроблені документи під час перетину державного кордону використовуються у вчиненні таких кримінальних правопорушень як торгівля людьми або інша незаконна угода щодо передачі людини; контрабанда; виготовлення, зберігання, придбання, перевезення,

пересилання, ввезення в Україну з метою збуту або збут підроблених грошей, державних цінних паперів чи білетів державної лотереї, шахрайство; зловживання службовим становищем тощо. У ст. 358 Кримінального кодексу України передбачена відповідальність за підроблення документів, печаток, штампів та бланків, їх збут, а також використання підроблених документів [1]. Серед умов ефективності інформаційного забезпечення протидії транскордонній злочинності на найближчі роки слід вважати тенденцію до міжнародного обміну даними та застосування баз даних, що працюють з інформацією, отриманою засобами біометричної ідентифікації [2, с. 111]. Кардинально зменшує ризики, пов'язані з використанням підроблених документів, застосування біометричних технологій, тобто автоматичних або автоматизованих методів розпізнавання особи людини за її біологічними параметрами.

Стратегією державної міграційної політики України на період до 2025 року визначено, що з метою підвищення рівня безпеки документів Україна повинна забезпечити: «видачу біометричних проїзних документів, які відповідають стандартам Міжнародної організації цивільної авіації (ICAO), у тому числі в консульських установах України за кордоном». Передбачається, що це «розширить можливості для скорочення неврегульованої міграції, боротьби з транснаціональною злочинністю і тероризмом» [3].

Біометричні дані – це будь-які дані, що характеризують певний біометричний параметр. При всьому різноманітті цих параметрів, у сфері виготовлення документів, що посвідчують особу при перетині державного кордону (та деяких інших документів), а також для біометричної ідентифікації та верифікації у світі застосовується технологія, що враховує три параметри: розпізнавання рис обличчя (обов'язкове); розпізнавання відбитку пальця; розпізнавання райдужної оболонки ока. З них в Україні застосовуються перші два. У 2018 р. в Україні створено національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Суб'єктами національної системи є ДМС, Адміністрація Держприкордонслужби, Національна поліція, МВС, МЗС, закордонні дипломатичні установи, Мінінфраструктури, СБУ, Служба зовнішньої розвідки та Міноборони. Розпорядником системи є ДМС [4]. Така система, очевидно, дає значні переваги в ідентифікації як правопорушників, так і потенційних потерпілих від транскордонної торгівлі людьми. При цьому:

- біометрична ідентифікація – це здійснення пошуку за принципом “один до багатьох” шляхом розпізнавання і зіставлення одного або двох біометричних даних (параметрів) особи з біометричними даними (параметрами) осіб у відомчих інформаційних системах суб'єктів національної системи;

- біометрична верифікація – здійснення пошуку за принципом “один до одного” між біометричними даними (параметрами),

отриманими від особи в даний момент, і біометричними даними (параметрами), наявними у відомчих інформаційних системах суб'єктів національної системи [4].

II. У контексті протидії злочинності, О. Г. Волеводзом запропоновано такий погляд на переваги застосування документів з персональними біометричними даними:

- більш високий ступінь захисту від підробки;
- можливість автоматичної перевірки приналежності власнику документа, що скорочує час на ідентифікацію особистості, збільшує швидкість даної процедури і виключає суб'єктивізм при оцінці її результатів;
- значний технологічний потенціал даного документа, тобто на чіп, крім ідентифікаційних даних, можуть записуватися інші різноманітні персональні дані;
- втрачає сенс підроблення та незаконне використання електронних документів з біометричними даними,
- біометричні персональні дані, що збираються при оформленні електронних паспортів можуть застосовуватися в діяльності з розслідування кримінальних правопорушень [5, с. 108].

III. Ураховуючи глобальний характер уніфікації машинозчитувальних документів, що засвідчують особу, та підвищені вимоги до авіабезпеки, розробку регламентів і стандартів в цій галузі покладено на Міжнародну організацію цивільної авіації (ICAO), яка з 1968 р. здійснює цю діяльність.

У 2005 р. 188 державами – членами ICAO затверджено стандарт Doc 9303, відповідно до якого документами, що засвідчують особу є:

- машинозчитуваний проїзний документ (паспорт, віза);
- машинозчитуваний паспорт (паспорт, що відповідає специфікаціям, визначеним Doc 9303);
- електронний паспорт – ePassport, біометричний паспорт (машинозчитуваний паспорт, що містить чіп безконтактної інтегральної схеми, на якому зберігаються дані, у тому числі біометричні характеристики власника паспорту і елемент захисту даних) [6].

На сьогодні понад 100 держав і міжнародних організацій видають ePassport, всього їх видано більш як 490 мільйонів. Наприклад, з 2012 р. строком на п'ять років їх (e-UNLP) видає ООН [7].

IV. Будь-який автоматизований метод ідентифікації заснований на зіставленні даних ідентифікованого об'єкта і біометричного еталона. Підрозділи прикордонного контролю для цього обладнуються програмно-технічними комплексами з функціями оброблення інформації про осіб, які перетинають державний кордон, їх паспортних документів з використанням електронних носіїв інформації, у тому числі з функцією біометричного контролю. Прогрес не стоїть на місці і з середини 2000-х років в різних аеропортах світу встановлюються

автоматизовані системи прикордонного контролю (Automated Border Control systems).

Важливим є обмін даними між найбільшими інформаційними системами EUROPOL та FRONTEX. У жовтні 2018 року між цими міжнародними організаціями підписано «Заяву про принципи співробітництва», з метою спільної протидії транскордонній злочинності, у тому числі торгівлі людьми.

Відповідно до документу FRONTEX надає інформацію, зібрану на зовнішніх кордонах ЄС, інформаційному центру EUROPOL, та, у свою чергу, отримує необхідні дані. Також діяльність обох міжнародних організацій буде координуватися у питанні впровадження Європейської системи авторизації та інформування про поїздки (ETIAS) [8].

У цьому зв'язку наведемо приклад припинення у 2018 р. діяльності організованої злочинної групи, що спеціалізувалася на торгівлі людьми, жертвами якої були громадяни Словаччини, переміщені до Великобританії з метою сексуальної експлуатації. Зокрема, залучалися жінки з найбільш уразливої в економічному відношенні соціальної сфери, яких шляхом обману, з обіцянкою привабливих і добре оплачуваних робочих місць у Великобританії, переправляли в Сполучене королівство. Потім організовувалося їх фіктивне одруження (для легалізації їхнього перебування на території Великобританії) з подальшим залученням до проституції (кінцева мета всієї схеми). Показово, що правоохоронними органами Словаччини та Сполученого Королівства, які побудували доказову базу на виявлених проїзних документах (паспортах) вдалося притягнути до відповідальності п'ять громадян різних держав і виявити шістнадцять жінок - потенційних жертв торгівлі людьми [9].

V. Застосування біометричних технологій є надзвичайно важливими у боротьбі з тероризмом. Це стало очевидно з поширенням авіатероризму. На питанні застосування біометричних технологій у боротьбі з тероризмом зосереджено основні акценти Резолюції 2396 (2017) Ради безпеки ООН [10]. Зокрема, ст. 15 цього документу передбачено, що «держави-члени повинні розробляти і впроваджувати системи збору біометричних даних, які можуть включати ідентифікаційні біометричні дані, для відповідального і належного виявлення терористів, включаючи іноземних бойовиків-терористів, РБ ООН закликає держави-члени, міжнародні, регіональні і субрегіональні організації надавати державам-членам технічну допомогу, ресурси і підтримку в нарощуванні потенціалу для застосування таких систем і рекомендує державам-членам ділитися цими даними, згідно з обставинами, з відповідними державами-членами, а також з Інтерполом та іншими відповідними міжнародними органами» [10]. В даний час Інтерпол має біометричні дані більш як 41 000 іноземних бойовиків – терористів (FTF).

Актуальними на наш погляд, є такі **висновки**, що мають практичну новизну:

1. Останнім часом значного поширення в світі набувають інформаційно-пошукові системи біометричної ідентифікації особистості по зображенню обличчя за оперативними даними від камер, розміщених у громадських місцях. Ураховуючи це, слід дослідити можливості удосконалення систем автоматизованих інформаційних систем та інформаційно-пошукових систем, що стоять на озброєнні правоохоронних органів України.

2. У деяких випадках законослухняний власник ePassport не зацікавлений у тому, щоб на кордоні була виявлена історія його подорожей. Наприклад, деякі арабські країни відмовляють у дозволі на в'їзд громадянам третіх держав, що мають ізраїльські візи. В окремих випадках, громадянин, в'їжджаючи в Сполучені Штати через Канаду, може бути не зацікавлений у виявленні факту візиту у країну, яка в США внесена у перелік країн, що сприяють тероризму. Отже, окремі особи маючи обґрунтовані побоювання щодо заборони на в'їзд, зацікавлені у частковій підробці паспорту шляхом заміни сторінки з небажаною візою або відміткою про в'їзд. Ці приклади демонструють аргумент на користь впровадження електронної візи, що записується на чіп ePassport. При цьому потребує вдосконалення система збору біометричної інформації від заявників на отримання візи для унікальної ідентифікації та подальшого використання таких даних під час здійснення прикордонного контролю.

3. Оскільки впровадження електронного носія інформації, що містить біометричні дані його власника, дозволяє виключити можливість використання зазначених документів іншою особою, це не тільки критично важливо за умов спрощеного візового (або безвізового) режиму переміщення через державний кордон, а й відкриває нові можливості для запобігання транскордонній злочинності. При цьому вразливим місцем у застосуванні біометричних технологій в Україні є процедури подання та обробки заяв для видачі проїзних документів та первинних документів. Інше вразливе місце – можливість дистанційного зняття даних з електронного чіпа, що обумовлює потенційний ризик несанкціонованого стеження за людьми, що, у свою чергу, створює загрозу порушення прав людини.

Перспективними, на наш погляд, є дослідження, якими буде встановлено шляхи мінімізації названих ризиків від застосування біометричних технологій.

Список бібліографічних посилань

1. Тальянчук Л. С. Криміналістичне дослідження документів, що посвідчують особу при перетині державного кордону України : дис...канд. юрид. наук. 12.00.09. К., 2016. 249 с.

2. Філіппов С. О. Інформаційне забезпечення протидії транскордонній злочинності. *Visegrad Journal on Human Rights*. 2018. № 4. Ч. 2. С. 107-112.

3. Стратегія державної міграційної політики України на період до 2025 р. Схвалено розпор. КМУ від 12.07.2017 р. № 482-р. // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/482-2017-%D1%80#n10/> (дата звернення: 09.10.2018).

4. Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Затверджено постановою КМУ від 27.12.2017 р. № 1073. // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/1073-2017-п> (дата звернення: 09.10.2018).

5. Волеводз А. Г. Удостоверяющие личность документы с биометрическими персональными данными: международные стандарты, иностранный опыт, отечественное правовое регулирование и его проблемы. *Ученые записки СПб филиала РТА*. 2015. № 1 (53). С. 87-117.

6. Doc 9303. Машиносчитываемые проездные документы Часть 3. Спецификации, общие для всех МСПД / ИКАО. URL: https://www.icao.int/publications/Documents/9303_p3_cons_ru.pdf (дата звернення: 09.10.2018).

7. ICAO. Security and Facilitation. Facilitation Programme. PKD. ePassport.Basics. URL: <https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx> (дата звернення: 10.10.2018).

8. EUROPOL and FRONTEX strengthen cooperation to tackle cross border crime / EUROPOL. 05 October 2018. URL: <https://www.europol.europa.eu/newsroom/news/europol-and-fronTEX-strengthen-cooperation-to-tackle-cross-border-crime> (дата звернення: 10.10.2018).

9. EUROPOL supports joint investigation into international human trafficking / EUROPOL. 15 February 2017. URL: <https://www.europol.europa.eu/newsroom/news/europol-supports-joint-investigation-international-human-trafficking> (дата звернення: 10.10.2018).

10. Resolution 2396 (2017) / adopted by the Security Council at its 8148th meeting, on 21 December 2017/ United Nations. Digital Library. URL: https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf (дата звернення: 09.10.2018).

Одержано 10.10.2018

УДК 004.93

Артем Олександрович ФРОЛОВ,

*аспірант кафедри твердотільної електроніки та інформаційної безпеки
фізичного факультету*

Ужгородського національного університету

ШИФРУВАННЯ КОЛЬОРОВИХ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ МАТРИЦЬ АДАМАРА

Сучасні поліграфічні і комп'ютерні технології стали загальнодоступними і дозволяють легко відтворювати зовнішній вигляд практично будь-якого документу. Навіть сама найскладніша поліграфія не в змозі самотійно забезпечити належний рівень захисту