Стандарти безпеки біометричних документів: реалізація в Україні та ЄС

Литовченко Віктор Петрович[1], Сезонов Віктор Станіславович[2], Диська Дар'я Григорівна[3]

Опубліковано	Секція	УДК
05.12.2022	Право	349

DOI: http://dx.doi.org/10.5281/zenodo.7513527

Annotation. Стаття надає характеристику реалізації стандартів безпеки біометричних документів в Україні та ЄС. Наводяться основні особливості та визначення біометричних документів. Наведено підходи до становлення використання біометричних документів. Зазначається про роль додержання стандартів безпеки біометричних документів як засобу забезпечення протидії міжнародній злочинності та тероризму. Зроблено висновок, що в разі відсутності належної системи безпеки біометричних даних в країні є загроза витоку даних, порушення основних прав людини, поширення тероризму. Охарактеризовано систему реалізації стандартів біометричних документів в Україні, як таку, що відповідає встановленим вимогам. Наголошено про використання в Україні застосунку «Дія», що містить дані про особу. Здійснено характеристику реалізації стандартів безпеки біометричних документів в країнах ЄС. Та зроблено висновок, що європейський рівень забезпечення додержання стандартів біометричних документів знаходиться на високому рівні, впроваджуються системи захисту і обробки даних. Постійно проводяться розробки з удосконалення стандартів та програмного забезпечення біометричних документів. Окрема увага наголошується на додержанні стандартів обробки даних для розпізнавання обличчя та поведінки особи. Зазначено про нову систему «розумні кордони» в країнах ЄС. Наводяться новітні розробки щодо використання і обробки біометричних документів, такі як BioCryptosystem, технології блокчейн. Залишається актуальним питання додержання стандартів безпеки для забезпечення захисту персональних даних та недопущення порушень прав людини під час використання біометричних документів.

[1] кандидат філософських наук, доцент кафедри соціально-гуманітарних дисциплін, Відокремлений підрозділ національного університету біоресурсів і природокористування України «Ніжинський агротехнічний інститут», 16600, Чернігівська обл., м. Ніжин, вул. Шевченка, 10, Україна, viktorpl08@gmail.com, https://orcid.org/0000-0003-0532-0188

[2] кандидат юридичних наук, доцент, завідувач сектору, Харківський НДЕКЦ МВС України, м. Харків, вул. Ковтуна, 34, Україна, SV26031985@UKR.NET, https://orcid.org/0000-0002-2580-2953

[3] кандидат юридичних наук, заступник декана факультету з навчально-методичної роботи, Харківський національний університет внутрішніх справ, м. Харків, проспект Льва Ландау, 27, Україна, disskaya@ukr.net, https://orcid.org/0000-0002-7593-1980

Keywords: біометрія, розпізнавання обличчя, захист персональних даних, стандарти ICAO, розумні кордони.

Security standards for biometric documents: implementation in Ukraine and the EU

Annotation. With the development of scientific and technical progress, the development of new technologies, the issue of using biometric documents is urgent. In the conditions of the modern world, where cases of international terrorism, crime, illegal migration are possible, special attention should be paid to the characteristics of the implementation of security standards of biometric documents in Ukraine and the EU. The article describes the implementation of security standards for biometric documents in Ukraine and the EU. The main features and definitions of biometric documents are given. Approaches to the formation of the use of biometric documents are given. The role of compliance with the security standards of biometric documents as a means of combating international crime and terrorism is noted. It is concluded that in the absence of a proper biometric data security system in the country there is a threat of data leakage, violation of fundamental human rights, and the spread of terrorism. The system of implementation of biometric document standards in Ukraine is characterized as meeting the established requirements. The use of the application "Diia" in Ukraine, which contains data about a person, is emphasized. The implementation of biometric document security standards in the EU countries is characterized. And it was concluded that the European level of ensuring compliance with biometric document standards is at a high level, data protection and processing systems are being implemented. Developments to improve the standards and software of biometric documents are constantly being carried out. Particular attention is paid to the observance of data processing standards for face recognition and behavior. The new system of "smart borders" in the EU countries is mentioned. The latest developments in the use and processing of biometric documents, such as BioCryptosystem, blockchain technology, are presented. The issue of compliance with security standards to ensure the protection of personal data and prevent human rights violations when using biometric documents remains relevant.

Keywords: biometrics, face recognition, personal data protection, ICAO standards, smart borders.

Вступ

З розвитком науково-технічного прогресу, розробкою нових технологій є актуальним питання використання біометричних документів. В умовах сучасного світу, де можливі випадки міжнародного тероризму, злочинності, незаконної міграції особливу увагу слід приділити характеристиці реалізації стандартів безпеки біометричних документів в Україні та ЄС.

Сучасна українська та зарубіжна наука містить значну кількість напрацювань 2021-2022 років щодо питання додержання стандартів безпеки біометричних документів в Україні та ЄС. Так, цю проблематику вивчали: Білоус І.В. [1], Ivan A. Tot, Jovan B. Bajčetić, Boriša Ž. Jovanović, Mladen B. Trikoš, Dušan Lj. Bogićević, Tamara M. Gajić [2], Thenuwara S. S., Premachandra C., Kawanaka H. [5], Чулінда Л., Бем Н. [11], Calderoni L., Magnani A. [13] та інші. Вчені наголошують на важливості додержання стандартів безпеки.

Мета даної статті – розкрити особливості додержання основних міжнародних стандартів використання біометричних документів в Україні та в країнах ЄС.

Результати

Питання забезпечення міжнародної та національної безпеки на сьогодні залишається актуальним з огляду на ситуацію у світі. Застосування біометричних документів сприяє запобіганню поширенню міжнародного тероризму, незаконній міграції, злочинності. Останні технологічні напрацювання дозволили розробити внесення біометричної інформації про власника документа, захистити ці дані [1, с. 263]. З огляду не це, системи ідентифікації людей становлять особливий інтерес в забезпеченні безпеки. Складні вимоги безпеки змусили експертів дослідити способи використання біометричних даних для ідентифікації користувачів. Біометричні стандарти і методи можна використовувати для ідентифікації користувачів у біометричних системах і для захисту інформаційних і комунікаційних систем [2, с. 963].

Біометричні технології набули стрімкого розвитку в останні два десятиліття. Термін «біометричний» складається з двох компонентів «біо» та «метрика», що передбачає вимірювання біологічних даних. Згідно з Оксфордським словником англійської мови, «біометрія» визначається як «позначення або відношення до фізичні характеристики, які є унікальними ідентифікаторами осіб (відбитки пальців, малюнок райдужної оболонки ока тощо)». Загалом, біометрія – це вимірювання біологічних сигналів людини [3]. Тож, фіксація та розрізнення біологічних даних становить сучасний інтерес як один із актуальних засобів забезпечення миру. Вчені розглядають біометрію як широку та різноманітну наукову галузь, де стикаються техніка, медицина, фізика, психологія тощо. Класифікації основних біометричних технологій потенційно можуть знайти застосування в операційних сферах, що представляють інтерес для спільноти. Ефективністю відрізняються біометричні технології (наприклад, розпізнавання відбитків пальців і розпізнавання обличчя) і технологічні системи з підтримкою біометрії (наприклад, електронні ворота та автономні роботизовані системи) [4]. Біометрію визначають як показники «біологічних моделей, що належать індивідам, таких як відбитки пальців, рисунок райдужної оболонки ока , голос і обличчя. Біометрія обличчя та відбиток пальця можна визначити як економічно ефективні та легкі ознаки доступу в біометричній сфері [5]. Інший підхід визначає біометрію як інструмент, який можна використовувати для доповнення або навіть заміни існуючих систем ідентифікації користувачів на основі того, що користувач знає або чим володіє, та є одним із ключових методів розпізнавання користувачів, оскільки вона забезпечує надійний захист і має велику практичність. Біометричні системи використовують біологічні та поведінкові характеристики людини, які можна розрізнити з метою біометричного розпізнавання. Існує кілька біометричних технологій, які використовувалися досі: відбитки пальців, обличчя, райдужна оболонка ока чи вени рук, електроенцефалограми, електрокардіограми і мультиспектральну фотометрію шкіри [2, с. 964]. Біометрія включає фізичні або поведінкові характеристики людини, такі як відбитки пальців, візерунки обличчя, голос або підпис, які є унікальними для окремих людей. Їх можна використовувати в цифровому вигляді для ідентифікації та надання людям доступу до країн, будівель, систем і пристроїв. Біометричні документи пропонують рішення, що допомагають зупинити поширення COVID-19 [6]. Таким чином, можна зробити висновок, що біометричний документ – це документ, що розроблений за допомогою високотехнологічних розробок, на якому зафіксована підтверджена інформація про сукупність біометричних характеристик людини, таких як відбитки пальців, візерунки обличчя, голос, підпис, райдужна оболонка ока чи вени рук, електроенцефалограма, електрокардіограма і мультиспектральна фотометрія шкіри тощо.

Внутрішній механізм біометричної автентифікації базується на технології, він надзвичайно простий і швидкий з точки зору користувача. Легше покласти палець на сканер, ніж ввести довгий пароль із кількома спеціальними символами, щоб миттєво

розблокувати обліковий запис. Більшість біометричних методів автентифікації використовуються лише з фізичними програмами; ви не можете передавати або повідомляти біологічні показники онлайн. Такі біометричні дані, як відбитки пальців, сканування райдужної оболонки ока, візерунки обличчя та інші, важко реконструювати за допомогою сучасних технологій. Імовірність того, що відбиток пальця зійдеться з відбитком пальця іншої людини, становить один до 64 мільярдів [7].

Не дивлячись на існуючі технологічні досягнення у використанні біометричних документів, все ж існують проблеми з безпекою систем, які їх використовують, зокрема їх незахищеність від зламу. Наприклад, якщо хтось прагне зламати пристрій, не потрібно знати внутрішню операційну систему, а використовуючи фальшивий відбиток пальця чи обличчя, можна видати себе за когось іншого чи приховати власну особу [6]. Засоби несанкціонованого доступу до біометричної системи не є вичерпними, до названих відносять також і підробку голосу тощо. Спроби підробки біометричних засобів називають «атаками», здатність виявляти такі атаки - виявлення біометричних атак, а предмет, який використовується для проведення атаки називають інструментом презентаційної атаки. Фальшивими або штучними атаками називають випадки навмисного пошкодження своїх біометричних даних людиною [6]. Серед наступних проблем із безпекою біометричних документів зазначають відсутність належних методів авторизації на кордоні, та внаслідок цього у світі відбувається зростання кількості злочинців та нелегальних мігрантів на кордоні [5]. З огляду на стрімкий та постійний розвиток біометричних технологій, виникають нові виклики, які спричиняють поширення негативних явищ серед країн.

Українські вчені наголошують на глобальному характері уніфікації біометричних документів міжнародними організаціями, зокрема, Міжнародною організацією цивільної авіації (ІКАО), якою з 1968 року проводиться робота з удосконалення машинозчитувальних проїзних документів, розробка стандартів та рекомендацій щодо оптичного зчитування знаків [1]. 1980 року цією організацією було розпочато розробку біометричної автоматичної верифікації особистості людини [8]. Переосмислення підходів до міжнародної безпеки та верифікації документів, що посвідчують особу, відбулось після трагічних подій у США 11 вересня 2001 року. Було проголошено процедуру запобігання міжнародному тероризму завдяки прикордонному контролю, проїзним документам, та розробкою заходів запобігання фальсифікації документів. Крім того, значна увага повинна бути приділена контролю реалізації стандартів ІКАО державами світу [1, с. 261].

В Україні становлення використання біометричних документів пов’язують із початком розвитку електронного уряду більше 15 років тому, з яких стрімкий розвиток ця сфера набула останні 10 років. Серед інструментів електронного урядування зазначають впровадження біометричних документів, розвиток інформаційного суспільства, відкритість та доступність публічного управління, які діють і під час війни 2022 року [9, с. 243].

В Україні перехід на біометричні паспорти почався з прийняття Указу Президента України «Про Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України» [10], що передбачено пунктом 1 цього Указу. Біометричні паспорти повинні виготовлятись згідно з найвищими стандартами ІСАО, маючи при цьому належний захист персональних даних.

Біометричні документи, які виготовляються в Україні виготовляються на спеціальних захищених бланках, зі спеціальних матеріалів, за допомогою високоякісного друку, містять комплекс високоякісних поліграфічних технологій друку, спеціальні елементи поліграфічного захисту (кольорові і флуоресцентні волокна, водяні знаки, захисні голографічні елементи, мікродрук,) елементи

наносяться спеціальними фарбами, застосовано технології персоналізації документа. «У документах, що посвідчують особу забезпечених безконтактною інтегральною схемою імплантовано безконтактний електронний носій, який відповідає вимогам стандарту ISO/IEC 14443 щодо запису і зчитування даних, а також вимогам нормативних документів України у сфері технічного та криптографічного захисту інформації.» Відповідно до цього, Україною було впроваджено всі стандарти ICAO щодо безпеки біометричних документів [1, с. 266]. На сьогодні до нових позитивних нововведень у сфері біометричних документів є можливість їх збереження та зчитування в застосунку «Дія» [9, с. 243].

Біометричний паспорт свідчить про роль стандартизації в авіаційному секторі. Пандемія Covid-19 викликала необхідність впровадження додаткових заходів запобігання порушенню захисту даних, та як авіакомпанії застосовують нові онлайн технології, а співробітники змушені працювати віддалено, що потребує постійного удосконалення заходів захисту персональних даних в авіаційній галузі. Хоча безпрецедентні масштаби COVID-19 призвели до суперечливих повноважень між агентствами та, як наслідок, до менш узгодженого підходу до обробки персональних даних пасажирів. ICAO визначила використання безконтактних процесів, включаючи біометрію обличчя, як пріоритет для захисту від передачі COVID-19. ICAO рекомендує ширше використовувати стандартизовані рішення для керування цифровими ідентифікаційними даними. Однак, щоб авіаційна промисловість використовувала біометричні дані та платформи для керування ідентифікаційними даними, записи про стан здоров'я та вакцинацію мають бути біометрично прив'язані до надійного документа, що засвідчує особу, наприклад електронного паспорта [11, с. 71]. Таким чином, можна зробити висновок, що в Україні впроваджено стандарти захисту біометричних документів, вони діють в умовах військового стану, допомагають для використання під час заходів з протидії пандемії COVID-19.

Для забезпечення лібералізації безвізового режиму було проведено низку заходів зі спрощення перетину кордону та забезпечення безпеки біометричних документів. Прибори для зчитування біометричних даних з паспортів було встановлено на 254 пунктах пропуску. Що робить миттєвий в'їзд для власників біометричних паспортів. Частина цих пунктів пропуску вже підключена до бази даних Інтерполу, а на деяких пунктах пропуску з Польщею та Молдавією здійснюється спільний контроль та проводиться робота з іншими державами-сусідами [12, с. 182].

В Європі стандарти автоматичного зчитування документів було запроваджено з 2003 року, та спрощено системи зчитування документів в аеропорту. З 2004 року в Бельгії, та інших країнах Європи почали виготовляти електронні паспорти за стандартами ICAO та вже у 2021 році це здійснюють більше 150 країн. Такі документи на чіпі містять цифрову біометричну та біографічну інформацію і дозволяють здійснювати автоматизований прикордонний контроль [11, с. 70]. Біометричні документи набули поширення у світі, найбільш захищені від підробок. Забезпечення безпеки біометричних даних і є основною задачею таких документів, з метою захисту суспільства від злочинності і тероризму [1, с. 264]. Для порівняння слід навести досвід Індонезії, у біометричних документах якої містяться електронний підпис, сканування райдужної оболонки ока, сканування відбитків пальців десяти пальців і паспорт високої роздільної здатності з 2012 року. Більше мільярда громадян було залучено до схеми, на яку наразі було витрачено близько 130 мільярдів індійських рупій. Це найбільша у світі система біометричної ідентифікації, яка має на меті забезпечити ідентифікацію кожного такого мешканця, який не має індивідуальної ідентифікації [7]. Тому бачимо, що в Європі впровадження та застосування біометричних документів

відбувається активно, але є країни на інших континентах, які впровадили більш розвинені технології .

Впровадження системи зчитування біометричних документів на кордоні є однією з основних критично важливих реальних програм у біометричній сфері за останні роки. А деякі біометричні ознаки можуть бути використані для автоматизованого прикордонного контролю в прикордонних місцях, визначених Міжнародною організацією цивільної авіації [5].

Одночасно з автоматизованими системами зчитування біометричних документів, порівнюють дані людини в документах із її зовнішнім виглядом на кордоні здійснюють паспортисти. Це висококваліфіковані люди, які можуть порівняти посвідчення особи з фотографією та зовнішній вигляд на кордоні. Науковці прийшли до висновку, що паспортисти погано працюють на кожному рівні. У деяких випадках вони визначили точні результати, не пов'язані з тривалістю досвіду або навчання. На сьогодні доведено, що паспортний персонал пропускає кожне сьоме підроблене посвідчення особи. Це означає, що існує величезний попит в галузі розпізнавання обличь. Розпізнавання обличчя є найуспішнішим способом аналізу зображень та привертає все більше уваги. Усі підходи машинного навчання для розпізнавання обличчя, такі як штучна нейронна мережа, звичайна нейронна мережа, застосовні для великого набору навчальних даних, але, на жаль, ці підходи є неточними [5]. Обличчя вважається основною біометричною ознакою машинозчитуваних паспортів. У цьому контексті стандарт ISO/IEC 19794-5 визначає набір вимог до фотографії для забезпечення якості зображення та спрощення процесу розпізнавання обличчя. Однак оцінка відповідності зображення обличчя стандартам ISO/ICAO сьогодні все ще виконується переважно людьми через відсутність автоматичних систем оцінки для виконання цього завдання [8].

Вчені пропонують до застосування контролю пасажиропотоку з використанням мультимодальної біометрії з удосконаленням парадигми на основі інтелектуального агента. Стратегія переговорів є основною концепцією запропонованого методу, і вона відносно схожа на спосіб прийняття рішень людиною. Індивідуальний агент, відповідальний за завдання розпізнавання, є новою концепцією домену автоматизованої біометричної авторизації. Система на основі агентів покращує якість процесу прийняття рішень порівняно з іншими методами синтезу, як показано в результатах. Експериментальний результат запропонованого методу показав, що загальна точність, продуктивність і час обчислення кращі, ніж інші мультимодальні системи авторизації. Запропонований метод використовує стандартні біометричні дані ICAO (обличчя та відбитки пальців), які є відносно економічно ефективними, ніж інші. Для майбутніх досліджень варто розглянути вдосконалення запропонованої системи контролю пасажиропотоку за допомогою робототехнічної операційної системи [5]. Дотримуючись вказівок ICAO, Міжнародна організація зі стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC) запропонували стандарт для фотографії обличчя для використання в електронних паспортах. Стандарт ISO/IEC 19794-5 визначає правила та формат запису для кодування, запису та передачі інформації про зображення обличчя. Він також визначає набір умов навколишнього середовища, фотографічних властивостей, функцій зйомки та атрибутів цифрового зображення зображень обличчя. Наприклад, зображення обличчя може мати однорідний фон з відсутністю тіней у будь-якій області зображення для внесення в електронний паспорт [8].

Науковці наголошують на погіршенні стану біометричних даних внаслідок їх стиснення. Внаслідок проведеного дослідження з використанням різних наборів даних, кожен з яких відображав конкретні параметри реєстрації, як запропоновано вхідними

правилами ISO та ICAO, результати виявились суперечливі, після стиснення зображення відомий інструмент із відкритим кодом показав значне погіршення. Розмір зображення, обмежений поточними специфікаціями, може втратити переваги, отримані від удосконалень у процесі реєстрації щодо оригінального розміру фотографії та якості сканування/отримання. Тому було запропоновано оновити правила реєстрації, вказавши збільшення місця, зарезервованого для зображення обличчя [13]. Глибокі нейронні мережі завоювали помітне місце завдяки своїй високій схильності розпізнавати складні шаблони. Однією з головних переваг цієї техніки є здатність отримувати інформацію з необроблених даних, іноді з невеликою попередньою обробкою або навіть без неї [8]. Серед останніх наукових розробок пропонується застосування технології безпечної системи розпізнавання обличчя з використанням нових схем захисту шаблонів Bio-Cryptographic. Впровадження запропонованої системи було розділено на три компоненти. Ділянки обличчя виявляються із вхідних зображень у першому компоненті. Потім застосовуються деякі методи виділення дискримінантних і відмінних ознак, щоб виділити риси з області обличчя. У другому компоненті риси проходять класифікацію, щоб перевірити або ідентифікувати особу на основі біометричних даних її обличчя. Така техніка була включена в біометричну функцію обличчя як BioCryptosystem для схеми захисту шаблону в третьому компоненті. Запропонована BioCryptosystem працює на рівні функцій у два етапи: підходи до шифрування на основі словника та ключа користувача з наступними процесами дешифрування . Крім того, було проведено деякі порівняння для аналізу безпеки використовуваної BioCryptosystem, який показує, що запропонована система потребує менше часу для автентифікаціїі, генерує довші та надійніші ключі, ніж інші існуючі біокриптографічні методи [14]. О. Денисенко, здійснюючи дослідження застосування нейронних мереж для розпізнавання тексту зазначає про точність розпізнавання моделі згорткової нейронної мережі. Пропонує до застосування гібридний метод бінаризації для покращення якості сегментації. На думку автора, впровадження запропонованої системи буде трудомістким, але ефективним процесом [15]. Зазначені пропозиції варті уваги та потребують подальших наукових досліджень

Наступною пропозицією з удосконалення систем захисту та використання біометричних документів пропонують застосувати технології блокчейну, за допомогою якого традиційні будівельні блоки будь-якої моделі глибокого навчання можна перетворити на безпечну систему. Це архітектура біометричного розпізнавання, яка використовує технологію блокчейн для забезпечення стійкого доступу в розподіленому середовищі. Він захищає як модель так і біометричний шаблон і попереджає всю систему, коли певний компонент змінюється. Це також полегшує виявлення потенційних збоїв. Біометричні системи ідентифікації, які поєднують біометрику та технологію блокчейн, можна використовувати для покращення безпеки, досягнення консенсусу в нестабільному середовищі та прийняття рішень, які можна перевірити. За допомогою персонального пристрою, такого як смартфон, користувачі можуть поділитися своїм цифровим ідентифікатором з постачальником послуг, навіть якщо вони фізично відсутні, і все одно мати доступ до основних послуг без шкоди для своєї конфіденційності [7].

Серед актуальних питань впровадження стандартів безпеки біометричних документів у країнах ЄС, та України, залишається питання додержання законодавства у сфері захисту персональних даних та недопущення порушень прав людини. У контексті чинного законодавства ЄС, що регулює біометричні методи, права на повагу до приватного життя та захист персональних даних особливо помітні. Значну роль в етичних дискусіях щодо використання біометричних методів відіграють положення про те, що людська гідність є недоторканною і повинна поважатися та захищатися.

Людська гідність забезпечується разом із свободою, демократією, верховенством права, вона розуміється як заборона інструменталізації або об'єктивація людських істот. Проте поняття гідності надзвичайно широке, що з одного боку, дає йому дуже широку та гнучку сферу застосування, але з іншого боку робить його вразливим. Заборонено будь-яку дискримінацію, таку як стать, раса, колір шкіри, етнічне чи соціальне походження, генетичні особливості, мова, релігія чи переконання, політичні або будь-які інші погляди, приналежність до національної меншини, майно, народження, інвалідність тощо [3]. Застосування технологій з використанням біометричних документів має негативні наслідки у вигляді витоку біометричних даних людини, що є грубим порушенням всіх нормативних актів у сфері забезпечення прав людини. Тому важливо не допускати витоку даних, проникнення до баз даних сторонніх осіб та забезпечення надійного зберігання. Впровадження новітніх технологій у сфері застосування біометричних документів потребує розробки технологій у сфері захисту біометричних даних.

Підвищення безпеки своїх кордонів за допомогою сучасних технологій, є постійним пунктом порядку денного ЄС. Впроваджено створення «Системи в'їзду/виїзду», що дозволяє записати та зберегти дату, час, місце в'їзд і виїзд, а також біометричні дані громадян третіх країн. Держави-члени із 2022 року запроваджують системи ідентифікації осіб за зовнішнім виглядом, обробкою відбитків пальців та біометрії обличчя. Для цього країни ЄС повинні встановити на пунктах пропуску камери з високою роздільною здатністю, які можуть ідентифікувати мандрівників за допомогою розпізнавання обличчя та потім створіть профіль цієї особи. Такий підхід має назву «розумні кордони», який використовує не тільки біометричні технології, але і системи виявлення емоцій. Ці автоматизовані засоби виявлення обману проаналізувати біометричні дані другого покоління, які пов'язані зі стресом, тривогою та брехнею співробітникам прикордонного контролю. Хоча в ЄС наразі не працюють системи виявлення емоцій кордонів, проект «Інтелектуальна портативна система керування» (iBorderCtrl), був спрямований на розробку інструментів виявлення обману та інструментів оцінки ризиків для безпеки кордону. Системи iBorderCtrl спрямовані на ідентифікацію осіб, які збрехали щодо своєї особистості, багажу, місця призначення або інших планів подорожей і класифікує осіб на «сумлінних» і «несумлінних» мандрівників. Якщо людина підпадає під останню категорію, проводиться співбесіда та спеціальне розслідування [3].

Висновки

За підсумками проведеного дослідження можна зробити висновки, що на сьогодні існує система міжнародних стандартів із додержання безпеки біометричних документів у ЄС. Біометричні документи не так давно застосовуються у європейській практиці, але доведено їх ефективність та безпечність порівняно зі звичайними. Біометричний документ – це документ, що розроблений за допомогою високотехнологічних розробок, на якому зафіксована підтверджена інформація про сукупність біометричних характеристик людини, таких як відбитки пальців, візерунки обличчя, голос, підпис, райдужна оболонка ока чи вени рук, електроенцефалограма, електрокардіограма і мультиспектральна фотометрія шкіри тощо. Україна також застосовує та впроваджує дані стандарти. Україною впроваджено використання біометричних документів, що виготовляється відповідно до стандартів, збережено всі вимоги до матеріалу та розпізнавальних знаків. На пунктах пропуску державного кордону також встановлено відповідне обладнання для забезпечення безпеки біометричних документів. Не дивлячись на існуючі технологічні досягнення у використанні біометричних документів, все ж існують проблеми з безпекою систем, які

їх використовують. Тому в Європейських країнах постійно проводиться робота з удосконалення існуючих систем безпеки.

Варто зазначити, що піднята нами тематика з додержання стандартів безпеки біометричних даних потребує подальших наукових досліджень для надання практичних висновків та рекомендацій для використання їх на практиці.

Список використаних джерел

1. Білоус І.В. Загальні відомості про сучасні вимоги до безпеки документів, що посвідчують особу та реалізація їх в Україні. *Криміналістика і судова експертиза*. 2018. № 62. С. 260-269. URL: https://digest.kndise.gov.ua/?download=1&kccpid=283&kcccount=https://digest.kndise.gov.ua/wp-content/uploads/2019/03/a2fc25cb69-260-269.pdf (29.10.2022).
2. Biometric standards and methods / I. Tot et al. *Vojnotehnicki glasnik*. 2021. Vol. 69, no. 4. P. 963–977. URL: https://doi.org/10.5937/vojtehg69-32296 (date of access: 29.12.2022).
3. Wendehorst, C., Duller, Y.. Biometric recognition and behavioural detection : assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. *European Parliament, Directorate-General for Internal Policies of the Union*. 2021. URL: https://data.europa.eu/doi/10.2861/982599 (date of access: 29.12.2022).
4. Frontex, Технологічне прогнозування біометрії для майбутнього подорожей - додаток II: систематика біометричних технологій і технологічних систем з підтримкою біометрії, Офіс публікацій Європейського Союзу. 2022. URL: https://data.europa.eu/doi/10.2819/181163 (date of access: 29.12.2022).
5. Thenuwara S. S., Premachandra C., Kawanaka H. A multi-agent based enhancement for multimodal biometric system at border control. *Array.* 2022. P. 100171. URL: https://doi.org/10.1016/j.array.2022.100171 (date of access: 28.12.2022).
6. Price A. Standards for secure biometrics systems. URL: https://www.biometricupdate.com/202103/standards-for-secure-biometrics-systems (date of access: 28.12.2022).
7. Garg Rishabh. Blockchain for Real World Applications. 2022. URL: https://www.researchgate.net/publication/366394066_Blokcejn_Neminuca_Revolucia?enrichId=rgreq-9dded36882c6192c8f82c99d1908cafa-XXX&enrichSource=Y292ZXJQYWdlOzM2NjM5NDA2NjtBUzoxMTQzMTI4MTEwODE4NzU4NUAxNjcxMzcxODQyNTIz&el=1_x_2&_esc=publicationCoverPdf (date of access: 28.12.2022).
8. de Andrade e Silva A. G., Gomes H. M., Batista L. V. A collaborative deep multitask learning network for face image compliance to ISO/IEC 19794-5 standard. Expert Systems with Applications, 2022, 198, 116756. https://doi.org/10.1016/j.eswa.2022.116756
9. Бєлікова М.І. Вплив воєнного стану на розвиток електронного урядування в Україні. *Наукові перспективи*. 2022. № 8(26). С. 243-251. URL: https://doi.org/10.52058/2708-7530-2022-8(26)- (дата звернення: 28.12.2022).
10. Про Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України. Указ Президента України від 22 квітня 2011 року N 494/2011. *Офіц. вісник Президента України*. 2011. № 13. С. 21. Ст. 657. https://zakon.rada.gov.ua/laws/show/494/2011#Text
11. Чулінда Л., Бем Н. Використання персональних даних відповідно до міжнародних стандартів ICAO. *International Science Journal of Jurisprudence & Philosophy*. 2022. № 1(2). С. 64-73. URL: https://doi.org/10.46299/j.isjjp.20220102.6 (дата звернення: 28.12.2022).
12. Перегняк І. В. Євроінтеграційний вектор оптимізації професійної підготовки військовослужбовців державної прикордонної служби України. *Педагогічний*

альманах. 2018. №37. С. 180-185. URL: http://nbuv.gov.ua/UJRN/pedalm_2018_37_31(дата звернення: 28.12.2022).

13. Calderoni L., Magnani A. The impact of face image compression in future generation electronic identity documents. *Forensic Science International: Digital Investigation*. 2022. Vol. 40. P. 301345. URL: https://doi.org/10.1016/j.fsidi.2022.301345 (дата звернення: 28.12.2022).
14. Sardar A., Umer S. Implementation of face recognition system using BioCryptosystem as template protection scheme. *Journal of Information Security and Applications*. 2022. Vol. 70. P. 103317. URL: https://doi.org/10.1016/j.jisa.2022.103317 (date of access: 29.12.2022).
15. Denysenko O. Research and development of text recognition system. *ΛΌΓΟΣ МИСТЕЦТВО НАУКОВОЇ ДУМКИ*. 2020. URL: https://doi.org/10.36074/2663-4139.11.04 (date of access: 29.12.2022).