Teresa Mendyk-Krajewska[1]

Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach

1. Wstęp

Biometria jest nauką zajmującą się identyfikacją i weryfikacją tożsamości osób na podstawie ich cech fizycznych, fizjologicznych lub behawioralnych, zwanych biometrykami. Metody biometryczne wykorzystują do tego celu osobnicze – unikatowe, trwałe i mierzalne cechy, które charakteryzują się akceptowalną odpornością na próby fałszerstwa. Takie biometryczne dane człowieka zaczęto wykorzystywać już w drugiej połowie XIX w., jednak przełom w tej dziedzinie nastąpił sto lat później wraz z rozwojem technologii informatycznych i możliwością szybkiego przetwarzania danych.

Od około dziesięciu lat techniki weryfikacji i identyfikacji biometrycznej są dynamicznie rozwijane i znajdują zastosowanie w coraz to nowszych obszarach. Równolegle prowadzone są intensywne prace normalizacyjne. Od wszystkich metod identyfikacji i poświadczania tożsamości wymaga się, by były wygodne i szybkie w użyciu, odporne na ataki i dawały stuprocentową poprawność wyniku.

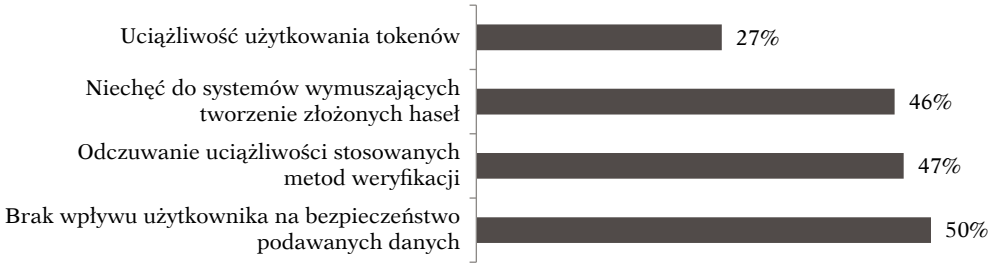
Celem artykułu jest ukazanie nowych obszarów zastosowań technik biometrycznych oraz związanych z tym wątpliwości i problemów, a także przedstawienie oceny biometrycznych metod weryfikacji tożsamości, wyrażonej przez objętych autorską ankietą użytkowników Internetu.

2. Weryfikacja tożsamości z wykorzystaniem biometrii

Barierą dla dalszego rozwoju usług realizowanych drogą elektroniczną mogą być powszechnie stosowane metody weryfikacji tożsamości użytkowników (na podstawie haseł i identyfikatorów materialnych). Z badań przeprowadzonych

[1] Politechnika Wrocławska, Wydział Informatyki i Zarządzania.

przez agencję TNS Polska w listopadzie 2014 r.[2] wynika bowiem, że użytkownicy odczuwają je jako uciążliwe, przy jednoczesnym braku możliwości wpływania na bezpieczeństwo uwierzytelniających danych. Udzielone przez ankietowanych odpowiedzi ujęto procentowo na rysunku 1.



Rysunek 1. Ocena tradycyjnych metod weryfikacji tożsamości

Źródło: opracowanie własne na podstawie danych raportu agencji TNS Polska, banking-magazine.pl/2015/01/15/nowy-raport-tns-pokazuje-ze-polacy-maja-dosc-hasel-dostepu-numerow-pin-tokenow--czas-na-haslo-glosowe/ (dostęp: 10.04.2018).

Niemal połowa pytanych odczuwa uciążliwość powszechnie stosowanych metod weryfikacji (47%) oraz sygnalizuje niechęć do systemów wymuszających tworzenie złożonych haseł (46%). Z badań wynika również, że co trzeci użytkownik chciałby posługiwać się podczas dostępu do wszystkich miejsc jednym hasłem. Prawie 40% użytkowników zmienia swoje hasło dostępowe tylko dlatego, że jest to wymuszane przez system, a jedynie co piąty zmienia je przynajmniej raz w roku[3].

Wygodnym i szybkim sposobem uwierzytelniania wydają się być rozwiązania biometryczne. Ich zaletą jest wysoka zdolność odróżniania uprawnionych użytkowników od osób, które się jedynie za takie podają – znając hasło lub posiadając odpowiedni identyfikator. Metody biometryczne umożliwiają też identyfikację (ustalenie tożsamości) oraz identyfikację negatywną (przesiewanie) w celu wykluczenia znajdowania się danej osoby na określonej liście[4]. Do mierzalnych cech zaliczamy: odciski palców, naczynia krwionośne dłoni i palca, geometrię

[2] Badaniem (na zlecenie firmy Nuance Communications) objęto reprezentatywną grupę tysiąca polskich internautów w wieku 18–65 lat, z podziałem na płeć, wiek i miejsce zamieszkania.

[3] https://bankomania.pkobp.pl/bankofinanse/nowe-technologie/jestesmy-zmeczeni-haslami-pin-ami-i-kodami/ (dostęp: 19.04.2018).

[4] M. Marucha-Jaworska, *Podpisy elektroniczne*, *biometria*, *identyfikacja elektroniczna*, Wolters Kluwer, Warszawa 2015, s. 176.

dłoni i twarzy, tęczówkę i siatkówkę oka, kod DNA, a także podpis odręczny, głos czy sposób chodzenia. W wielu zastosowaniach wskazuje się na potrzebę użycia więcej niż jednej cechy, celem uniknięcia błędów rozpoznania. Dodatkowo połączenie wielu biometryk zwiększa odporność na atak przez podszywanie się.

Dane biometryczne mają charakter danych wrażliwych[5]. Wszystkie techniki charakteryzuje cyfrowy zapis wzorca, który powinien być przechowywany w bazie danych w postaci zaszyfrowanej. To z nim porównywane są cechy uzyskane w wyniku pomiaru. W dniu 25 maja 2018 r. weszło w życie Unijne Rozporządzenie[6] w sprawie ochrony danych osobowych, w tym danych biometrycznych[7], m.in. regulujące zakres ich wykorzystywania. Przetwarzanie takich danych jest zabronione, jednak Rozporządzenie zawiera wyjątki (np. jest nim wyraźna i dobrowolna zgoda osoby, której te dane dotyczą).

Rozwiązania weryfikacji tożsamości na podstawie metod biometrycznych wykorzystywane są przede wszystkim jako sposób kontroli dostępu do zasobów (pomieszczeń, urządzeń, programów, danych), jednocześnie umożliwiają one blokadę nieautoryzowanych prób dostępu. Stosuje się je:

- w zakładach pracy (nadzór dostępu do obiektów, kontrola czasu pracy),
- przy kontroli dostępu do sprzętu (komputerów, telefonów komórkowych),
- w bankowości (oddziały, bankomaty, płatności elektroniczne),
- do ochrony porządku publicznego (m.in. w celu podniesienia bezpieczeństwa imprez masowych),
- w obiektach użyteczności publicznej (sklepach, kasynach, parkach rozrywki), w biurach obsługi klienta,
- w dokumentach (wizach, paszportach),
- do kontroli na przejściach granicznych,
- do zabezpieczania systemów alarmowych, zamków drzwiowych itp.

Wybór techniki biometrycznej dla konkretnej realizacji zależy od wygody pobierania próbki, szybkości jej weryfikacji, rozmiaru pamięci do przechowywania wzorca oraz od wymaganego poziomu bezpieczeństwa[8]. Na decyzję mają

---

[5] Nową definicję wprowadza Rozporządzenie – patrz przypis 6.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[7] Dane biometryczne oznaczają wszelkie przetworzone technicznie dane osobowe, odnoszące się do fizycznych, fizjologicznych i behawioralnych cech osoby fizycznej, które umożliwiają lub potwierdzają jej jednoznaczną identyfikację.

[8] Zob. R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, *Biometria*, WNT, Warszawa 2016.

wpływ warunki, w jakich system będzie użytkowany oraz jego przeznaczenie. Do oceny konkretnych rozwiązań oraz do wyboru metody i realizującego ją urządzenia służą między innymi następujące wskaźniki:

- FAR (ang. *False Acceptance Rate*) – niesłusznych akceptacji,
- FRR (ang. *False Rejection Rate*) – niesłusznych odrzuceń,
- EER (ang. *Equal Error Rate*) – równowagi między FAR a FRR,
- FTE (ang. *Failure To Enroll*) – niepowodzeń w rejestracji (z przyczyn technologicznych lub proceduralnych),
- FTA (ang. *Failure To Acquire*) – wskaźnik niepowodzeń w pobieraniu[9].

Niesłuszna akceptacja świadczy o luce w systemie zabezpieczeń, zaś niesłuszne odrzucenie jest kłopotliwe dla uprawnionego użytkownika. Z tego wynika potrzeba zachowania kompromisu pomiędzy FAR a FRR – kompromisu pomiędzy bezpieczeństwem a wygodą użytkowania. Wydajność jednego komparatora biometrycznego precyzyjnie i kompletnie opisuje krzywa ROC, która wyraża kompromis między wskaźnikiem niesłusznych zgodności (ang. *False Match Rate*, FMR) a wskaźnikiem niesłusznych niezgodności (ang. *False Non-Match Rate*, FNMR). Istnieje wiele rodzajów krzywych ROC, które mogą być użyte do wyrażenia tej samej informacji[10].

Od wielu lat techniki biometryczne są stosowane przy realizacji e-płatności. Celem dalszego usprawnienia weryfikacji tożsamości klientów jest powszechne wprowadzenie płatności w placówkach handlowych z wykorzystaniem biometrii palców. W Szwecji już kilka lat temu umożliwiono ich dokonywanie przez dotknięcie dłonią specjalnego czytnika (po uprzednim przypisaniu układu naczyń krwionośnych dłoni do karty płatniczej w specjalnym serwisie internetowym).

W ostatnim okresie obserwuje się duże zainteresowanie wykorzystaniem techniki rozpoznawania twarzy. Pobrane i odpowiednio przetworzone dane są porównywane z wzorcami uprzednio umieszczonymi w bazie, te zaś mogą być pogrupowane według określonych kategorii: osoby uprawnione, ważne, poszukiwane. Wynik weryfikacji – dopasowywanie wizerunku w czasie rzeczywistym do jednego z przechowywanych wzorców, umożliwia podjęcie odpowiedniego działania: zezwolenie na dostęp (aktywność), odmowę lub wszczęcie alarmu. Facebook kilka lat temu opracował aplikację DeepFace[11] do identyfikacji

[9] Pewien odsetek populacji nie dysponuje daną cechą biometryczną, tym samym nie ma możliwości pobrania próbki.

[10] Więcej o podstawowych błędach systemu w: R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, op. cit.

[11] Jest to zaawansowany system do rozpoznawania twarzy na cyfrowych obrazach, wykorzystujący dziewięciowarstwową sieć neuronową.

tej samej osoby na różnych porównywanych zdjęciach z dokładnością 97%, co wzbudziło obawy wielu instytucji[12] o prywatność danych użytkowników. Z kolei naukowcy z Instytutu Maxa Plancka w Saarbruecken zaprezentowali tzw. system rozpoznawania bez twarzy, który z wykorzystaniem sieci neuronowej umożliwia identyfikację twarzy częściowo zasłoniętych[13], przy czym skuteczność metody zależy od liczby analizowanych przez system zdjęć.

Przykładowymi technologiami biometrycznymi są: Touch ID firmy Apple Inc. (wykorzystuje linie papilarne, umożliwia tworzenie trójwymiarowego modelu), Palm Secure firmy Fujitsu (wykorzystuje naczynia krwionośne dłoni), NeoFace firmy NEC (rozpoznawanie twarzy nawet w tłumie i na obrazach o niskiej rozdzielczości w ciągu kilku sekund) czy VoicePrint firmy Fujitsu R&D Center Co., Ltd. (biometria głosowa stosująca kontrolę żywotności celem eliminacji robotów lub nagrań z playbacku).

3. Zastosowanie biometrii w nowych obszarach

Mnogość opracowanych metod uwierzytelniania i identyfikacji (jak np. automatyczne rozpoznawanie na podstawie analizy danych biometrycznych z wykorzystaniem siatek deformowalnych różnego typu[14]) pozwala wykorzystywać je w różnych celach. Na obszarze Unii Europejskiej od 2003 r. działa system identyfikacji odcisków palców azylantów i nielegalnych imigrantów Eurodac (European Dactiloscopie). Od 2006 r. wszystkie kraje UE (i wiele innych) wydają biometryczne paszporty.

Wraz z rozwojem technologii biometrycznych zyskuje się coraz większą trafność odpowiedzi i szybkość działania, czego efektem jest zwiększenie obszaru ich zastosowań. Opracowane z myślą o służbach bezpieczeństwa mogą być użyte do wykrywania niepożądanych osób na lotniskach, dworcach, stadionach czy w centrach handlowych. Od kilku lat w miejscach publicznych umieszczane są systemy rozpoznawania twarzy w celu zwiększenia skuteczności wykrywania poszukiwanych przestępców. Monitoring coraz powszechniej stosowany jest

[12] Przykładem National Telecommunications and Information Administration.

[13] https://tylkonauka.pl/wiadomosc/system-rozpoznawania-bez-twarzy-zidentyfikuje-cie-nawet-gdy-zaslonisz-swoja-twarz (dostęp: 21.03.2018).

[14] M.in. siatki z wielowymiarowymi deskryptami cech lokalnych czy dyskryminacyjne siatki deformowalne. Zob. K. Ślot, *Rozpoznawanie biometryczne. Nowe metody ilościowej reprezentacji obiektów*, WKiŁ, Warszawa 2010, s. 37–111.

na stacjach paliw, osiedlach mieszkaniowych, placach miejskich, w sklepach, a także prywatnych nieruchomościach. W połowie 2014 r. media donosiły o ujęciu w Chicago pierwszego przestępcy dzięki uruchomionemu systemowi kamer miejskich sprzężonych z technologią rozpoznawania twarzy NeoFace (jego zdjęcie znajdowało się w policyjnej bazie danych)[15].

Technologie te mogą być również stosowane np. do identyfikacji ważnych osób w miejscach publicznych, takich jak hotele, luksusowe sklepy, kasyna itd. Na niektórych lotniskach dla często podróżujących osób posiadających dokumenty z identyfikatorami biometrycznymi już dawno udostępniono specjalne przejścia przyspieszające odprawę. Od 2006 r. na londyńskim lotnisku Heathrow działa biometryczna odprawa pasażerów z wykorzystaniem skanowania tęczówki oka. Metoda stosowana jest też na niektórych lotniskach w Kanadzie, Holandii, Niemczech i Japonii. W 2015 r. na waszyngtońskim lotnisku Dulles przez kilka miesięcy testowano nowy system rozpoznawania twarzy dla sprawdzania tożsamości. Sporządzane fotografie wszystkich pasażerów były porównywane z ich zdjęciami umieszczonymi w paszportach[16]. W Stanach Zjednoczonych policyjna baza danych systemów rozpoznawania twarzy, do której dostęp mają różni przedstawiciele prawa, w 2016 r. zawierała dane już 117 mln osób[17]. W tym samym czasie pojawiła się informacja o wprowadzeniu podobnych rozwiązań w Niemczech. W 2017 r. kamery wyposażone w oprogramowanie do rozpoznawania twarzy zostały zainstalowane między innymi w Madrycie – w kasynie i na dworcu autobusowym na południu miasta (jednym z najbardziej ruchliwych w Europie) oraz w brazylijskim porcie lotniczym. Natomiast w Australii system rozpoznawania twarzy ma w niedługim czasie zastąpić paszporty. Kraj ten wprowadził taki system jako pierwszy, a automatyczna kontrola ma funkcjonować na wszystkich lotniskach do 2020 r. Technologia biometryczna pozwoli skanować i analizować dane podróżnych w czasie rzeczywistym; zastąpi wykorzystywany tam od 2007 r. system SmartGates. Już w 2015 r. zatwierdzono tam prawo pobierania danych (takich jak: odciski palców, zdjęcia twarzy, skany tęczówki oka, wzrost, waga) wszystkich pasażerów na lotniskach. Oczekuje się, iż śladem Australii pójdą też inne kraje. W Stanach Zjednoczonych również

[15] http://www.slashgear.com/facial-recognition-catches-its-first-criminal-in-chicago-10332851/ (dostęp: 12.09.2017).

[16] http://www.engadget.com/2015/03/21/dulles-airport-facial-recognition-trial/ (dostęp: 15.09.2017).

[17] Z raportu Centrum Prywatności i Technologii w Georgetown Law wynika, iż zdjęcia obywateli w bazie danych pochodzą z praw jazdy kierowców z 26 stanów, http://www.engadget.com/2016/10/19/cops-facial-recognition-database-half-us-adults/ (dostęp: 17.10.2017).

planuje się wprowadzenie skanerów biometrycznych na lotniskach, ale jedynie dla weryfikacji danych zawartych w paszportach podróżnych. System oparty na rozpoznawaniu twarzy rozwija już Francja, zaś Wielka Brytania – oparty na danych tęczówki oka.

W wielu stanach USA wprowadzono skanowanie układu krwionośnego dłoni dzieci w celu umożliwienia w razie potrzeby (np. wypadku drogowego) ich szybkiej identyfikacji. Z kolei w Indiach metody identyfikacji biometrycznej znalazły zastosowanie w systemach udzielania pomocy społecznej, a w Brazylii (2008 r.), Boliwii (2009 r.) i Ghanie (2012 r.) do weryfikacji osób biorących udział w wyborach (prezydenckich lub/i parlamentarnych). W Chinach technikę biometryczną rozpoznawania twarzy wykorzystano do monitorowania mniejszości etnicznych w muzułmańskim autonomicznym regionie Sinciang, graniczącym z Pakistanem i Afganistanem. Celem tych prowadzonych od 2017 r. testów jest zapobieganie terroryzmowi[18].

W związku ze stosowaniem monitoringu w miejscach publicznych powstają wyzwania dotyczące analizowania ogromnej ilości zarejestrowanego materiału, wyszukiwania w nim istotnych fragmentów (potencjalnych dowodów), a także sprawnego zarządzania materiałem video oraz raportowania wyników. Do tego celu powstają liczne, zaawansowane, wielofunkcyjne narzędzia, których przykładem może być system Kinesense LE[19] (w zakresie rozpoznawania twarzy wykorzystuje takie rozwiązania biometryczne jak NeoFace firmy NEC).

Stosunkowo nowy obszar zastosowań dla technik biometrycznych stanowi realizacja cyfrowych znaków wodnych w celu identyfikacji plików graficznych (obrazów, zdjęć, by potwierdzić ich autorstwo czy legalny zakup) – z wykorzystaniem cech biometrycznych ich autorów lub właścicieli.

4. Problemy dotyczące technologii biometrycznych

Ogólny model systemu biometrycznego uwierzytelniania i rejestracji składa się z kilku części: urządzenia wejściowego (czujnika), ekstraktora wzorca, komparatora, rejestratora, bazy wzorców i zastosowania. W takim modelu można

[18] http://www.businessinsider.com.pl/technologie/nowe-technologie/inwigilacja-mniejszosci-etnicznych-w-chinach-dzieki-technologii/gzq^{3}qvk (dostęp: 19.01.2018).

[19] Firma dostarcza oprogramowanie do szybkiego wyszukiwania przydatnych informacji z materiału wideo z CCTV (Closed-Circuit TeleVision – system przesyłu obrazu z kamer do zestawu rejestratorów w celu zwiększenia bezpieczeństwa obszaru objętego monitoringiem).

wskazać 11 podstawowych punktów ataku na system (są to m.in. ataki na identyfikatory biometryczne, na interfejsy wejściowe czy interfejsy wyjściowe)[20].

Problemów związanych z wykorzystywaniem cech biometrycznych jest wiele i można je rozpatrywać w różnych aspektach. Sporo wątpliwości wynika z obawy o zbyt niski poziom ochrony przechowywanych danych. Nie można bowiem wykluczyć możliwości włamania się do systemu bazodanowego, co może skutkować dopisaniem własnego wzorca do bazy uprawnionych osób lub przejęciem kontroli nad bazą. Nie można też wykluczyć możliwości oszukania urządzenia przez prezentację sztucznego wzorca – wprowadzenia go bezpośrednio z czytnika lub zmodyfikowania przesyłanych do bazy danych. Oczywiście różne techniki biometryczne cechuje różna odporność na ataki. Według danych firmy Kaspersky Lab, urządzenia umożliwiające nielegalne pozyskiwanie odcisków palców były dostępne już w 2016 r., zaś urządzenia do pobierania danych z systemów wykorzystujących naczynia krwionośne dłoni i analizujących tęczówkę oka – w fazie opracowywania[21].

Jednym z podstawowych warunków dla bezpieczeństwa rozwiązań biometrycznych było założenie, że uwierzytelnianie odbywa się lokalnie, bez przesyłania danych[22], jednak nie zawsze jest to możliwe. Ponadto, algorytmy realizujące procesy weryfikacji czy identyfikacji powinny być uruchamiane w chronionym środowisku niskopoziomowym, a nie na poziomie aplikacji.

Wdrażanie metod technologii biometrycznych napotyka duży opór społeczny, którego przyczyną jest sprzeciw wobec zbierania danych wrażliwych przez różne instytucje rządowe czy finansowe, takie jak urzędy wydające paszporty czy prawa jazdy oraz realizujące usługi drogą elektroniczną (np. banki). Naturalny sprzeciw, wynikający z potrzeby zachowania prywatności, budzi sama możliwość szybkiej identyfikacji osoby przez ukryte systemy pomiarowe instalowane w miejscach publicznych. W 2014 r. pojawiła się wiadomość o planowanej instalacji na ulicach Chicago zaawansowanych technologicznie latarni, których dodatkowym zadaniem miałoby być zbieranie informacji, m.in. o jakości powietrza i poziomie hałasu, ale także danych dotyczących codziennej aktywności mieszkańców – na podstawie używanych przez nich smartfonów (pomiar ruchu pieszych)[23]. Trudno nie dostrzec w tych działaniach możliwości dalszej

[20] R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, op. cit.

[21] http://www.kaspersky.pl/o-nas/informacje-prasowe/2671/oamanie-zabezpieczen-biometrycznych-kaspersky-lab-bada-zagrozenia-dla-bankomatow- (dostęp: 17.03.2018).

[22] Przetwarzanie danych powinno odbywać się jak najbliżej źródła (architektura *edge computing*).

[23] http://www.endaget.com/2014/06/22chicago-getting-smart-lamo-posts/ (dostęp: 5.07.2017).

inwigilacji ludności, choć wskazywanym celem przedsięwzięcia jest lepsze planowanie rozwoju miasta.

W 2013 r. została ogłoszona w Polsce nowelizacja wprowadzająca elektroniczne formularze potwierdzania odbioru pism sądowych[24]. Obecnie system EPO (Elektroniczne Potwierdzenie Odbioru), wykorzystujący tablet wyposażony w elektroniczne pióro, jest stosowany przy doręczaniu przesyłek poleconych, nie tylko sądowych. Złożony przez odbiorcę podpis odręczny przetwarzany jest na postać cyfrową i pozostaje w pamięci urządzenia, będąc dostępnym dla administratora tabletu. Może więc zostać skopiowany, upubliczniony, a jego nieuprawnione użycie byłoby bardzo trudne do udowodnienia. Jednym z warunków uznania podpisu elektronicznego za bezpieczny (powinno to również dotyczyć podpisu biometrycznego), jest jego sporządzenie z wykorzystaniem urządzenia pozostającego pod kontrolą osoby składającej podpis[25]. W przypadku elektronicznego potwierdzania odbioru przesyłek ten podstawowy warunek nie jest spełniony, zatem z uwagi na zagrożenie bezpieczeństwa podpis biometryczny nie powinien być stosowany m.in. w instytucjach publicznych, i nie powinno być przymusu jego sporządzania.

Jest dużo zastrzeżeń do wdrażania nowych technik w różnych obszarach. Na przykład stawiane jest pytanie, czy zabezpieczenia biometryczne powinna mieć broń. Nie wiadomo, jak unieważniać dane biometryczne w przypadku ich nielegalnego przejęcia, jak zorientować się, że dokonano nadużycia z ich wykorzystaniem, a wobec tego jak udowodnić, że nie przebywało się w miejscu zdarzenia, nie miało się dostępu do sprzętu itp.

Wiele aspektów związanych ze stosowaniem biometrii, w tym kwestie etyczne, społeczne i prawne porusza w swojej książce D. Jaroszewska-Choraś[26]. Ze stosowania danych biometrycznych (np. w paszportach i innych dowodach tożsamości) wynikają liczne zagrożenia etyczne, co zostało podkreślone w opinii Grupy Roboczej Art. 29 ds. Ochrony Danych[27]. Stosowanie biometrii może w konsekwencji prowadzić do ograniczenia prawa do prywatności[28], gdyż uzy-

---

[24] Dz.U. z 2013 r., poz. 600.

[25] Art. 3 pkt. 2 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. z 2001 r. Nr 130, poz. 1450.

[26] D. Jaroszewska-Choraś, *Biometria – aspekty prawne*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2016, s. 35–41, 75–114.

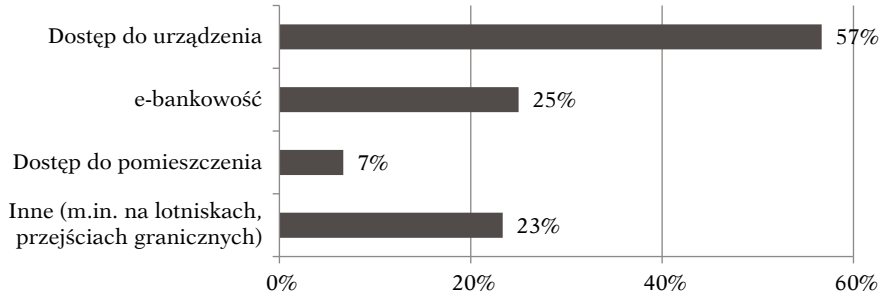
[27] Ibidem, s. 36.

[28] Ochronę prawa do prywatności przewiduje uchwalona w 1948 r. przez Zgromadzenie Ogólne ONZ Powszechna Deklaracja Praw Człowieka (Art. 12). Regulacje związane z pojęciem prawa do prywatności zostały też zawarte w Karcie praw podstawowych UE (Dz. Urz. C83 z 30 marca 2010 r.).

skane informacje, np. o braku posiadania mierzonych cech, niektórych chorobach lub przebytych zabiegach (plastycznych czy stomatologicznych), mogą być wykorzystane w sposób nieuprawniony.

5. Biometryczna kontrola tożsamości w ocenie użytkowników

W maju 2018 r. zostało przeprowadzone autorskie badanie ankietowe wśród studentów I i III roku informatyki Politechniki Wrocławskiej, którym objęto 120 osób. Z badań wynika, że różne usługi drogą elektroniczną (e-płatności, zakupy, rezerwacje itp.) systematycznie realizuje 83% ankietowanych. Większość z nich (77%) doświadczyła już weryfikacji biometrycznej, a najczęściej mierzonymi cechami były linie papilarne (71%), elektroniczny podpis odręczny (22%) oraz geometria twarzy (17%). W większości przypadków kontrola dotyczyła dostępu do urządzenia (57%), na drugim miejscu znalazła się e-bankowość (25%) (rysunek 2).

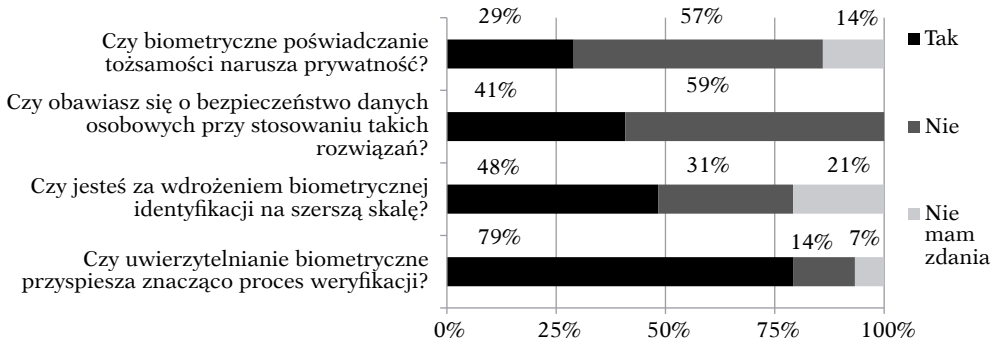


Rysunek 2. Deklarowane okoliczności biometrycznej kontroli tożsamości

Źródło: opracowanie własne.

Według zdecydowanej większości pytanych biometryczne metody sprawdzania tożsamości znacząco przyspieszają proces weryfikacji (79%) i nie ma powodów do obaw o bezpieczeństwo danych osobowych wykorzystywanych w tym procesie (59%) (rysunek 3). Jednak za wdrożeniem technik biometrycznych na szerszą skalę jest już mniej niż połowa ankietowanych (48%).

Większość objętych ankietą studentów na pytanie o akceptację stosowania technologii rozpoznawania twarzy w miejscach publicznych udzieliła odpowiedzi negatywnej (53%). Pozytywnie nastawionych było jedynie 35% ankietowanych, zaś 12% nie miało w tej kwestii zdania.



Rysunek 3. Ocena biometrycznych metod weryfikacji tożsamości

Źródło: opracowanie własne.

Zwraca uwagę fakt, że jedynie 29% objętych badaniem osób dostrzega przy stosowaniu biometrycznych metod poświadczania tożsamości problem naruszania prywatności. Większość (57%) na takie zapytanie odpowiada przecząco, zaś 14% nie ma w tej kwestii zdania.

Dzięki użyciu technik biometrycznych wzrasta wygoda i szybkość realizacji procesu weryfikacji użytkowników, jednak za cenę spadku poziomu ich anonimowości i prywatności. Obecnie biometria znajduje dużą akceptację społeczną – szczególnie wśród ludzi młodych, co potwierdzają przeprowadzone badania, i jest wdrażana w różnych obszarach, mimo że liczne problemy związane ze stosowaniem tej technologii dotąd nie zostały rozwiązane.

6. Podsumowanie

Jeszcze kilkanaście lat temu do technik weryfikacji biometrycznej podchodzono dość sceptycznie, mimo dostrzegania ich użyteczności w procesie sprawdzania tożsamości. Obecnie dane biometryczne wykorzystywane są do prowadzenia czynności prawnych czy finansowych, z tworzonych na te potrzeby baz danych korzystają także inne podmioty, a prace dotyczące zastosowania biometrii są intensywnie prowadzone na całym świecie. Inwestycje w nowe technologie identyfikacji tłumaczone są potrzebą wzrostu ochrony obywateli wobec nasilającego się zagrożenia terrorystycznego, jednak nie brak opinii, że zostały one rozwinięte, by stworzyć skuteczne narzędzie nadzoru.

Wysoko rozwinięte technologie, coraz bardziej akceptowalne, są wdrażane w różnych obszarach. Największe zainteresowanie budzi możliwość ich

wykorzystania do identyfikacji osób[29], czego nie da się zastąpić innymi rozwiązaniami. Istnieje plan utworzenia ujednoliconego, ogólnoświatowego systemu wykorzystującego dane biometryczne gromadzone w poszczególnych krajach do realizacji ich wspólnych celów.

W dobie powszechnego przechowywania i przetwarzania wszelkich możliwych danych na różne potrzeby, istnienie takiej bazy wydaje się oczywiste, jednak fakt, że rządy tych krajów będą w posiadaniu bardzo szczególnych informacji o każdej zidentyfikowanej osobie, może budzić uzasadniony niepokój.

Bibliografia

Bolle R.M., Connell J.H., Pankanti S., Ratha N.K., Senior A.W., *Biometria*, WNT, Warszawa 2016.

Jaroszewska-Choraś D., *Biometria – aspekty prawne*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2016.

Marucha Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna*, Wolters Kluwer, Warszawa 2015.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Ślot K., *Rozpoznawanie biometryczne. Nowe metody ilościowej reprezentacji obiektów*, WKiŁ, Warszawa 2010.

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. z 2001 r. nr 130, poz. 1450.

Źródła sieciowe

banking-magazine.pl/2015/01/15/nowy-raport-tns-pokazuje-ze-polacy-maja-dosc-hasel-dostepu-numerow-pin-tokenow-czas-na-haslo-glosowe/ (dostęp: 10.04.2018).

https://bankomania.pkobp.pl/bankofinanse/nowe-technologie/jestesmy-zmeczeni-haslami-pin-ami-i-kodami/ (dostęp: 19.04.2018).

https://www.businessinsider.com.pl/technologie/nowe-technologie/inwigilacja-mniejszosci-etnicznych-w-chinach-dzieki-technologii/gzq3qvk (dostęp: 19.01.2018).

http://www.endaget.com/2014/06/22chicago-getting-smart-lamo-posts/ (dostęp: 5.07.2017).

[29] Ustalenie tożsamości poprzez porównanie pobranej próbki z każdą zapisaną w bazie.

http://www.engadget.com/2015/03/21/dulles-airport-facial-recognition-trial/ (dostęp: 15.09.2017).

http://www.engadget.com/2016/10/19/cops-facial-recognition-database-half-us-adults/ (dostęp: 17.10.2017).

http://www.irisguard.com (dostęp: 15.03.2018).

http://www.kaspersky.pl/o-nas/informacje-prasowe/2671/oamanie-zabezpieczen-biometrycznych-kaspersky-lab-bada-zagrozenia-dla-bankomatow- (dostęp: 17.03.2018).

http://www.osnews.pl/system-rozpoznawania-twarzy-zastapi-paszporty-w-Australii/ (dostęp: 1.09.2017).

http://www.slashgear.com/facial-recognition-catches-its-first-criminal-in-chicago-10332851/ (dostęp: 12.09.2017).

https://tylkonauka.pl/wiadomosc/australia-chce-zastapic-paszporty-technologia-rozpoznawania-twarzy (dostęp: 12.09.2017).

https://tylkonauka.pl/wiadomosc/przelom-w-pracach-nad-technologia-rozpoznawania-twarzy (dostęp: 15.06.2017)

https://tylkonauka.pl/wiadomosc/system-rozpoznawania-bez-twarzy-zidentyfikuje-cie-nawet-gdy-zaslonisz-swoja-twarz (dostęp: 21.03.2018).

http://www.ubergizmo.com/2016/08/german-minister-facial-recognition-airports/ (dostęp: 24.09.2017).

http://www.zmianynaziemi.pl/wiadomosc/podpis-biometryczny-realne-zagrozenie (dostęp: 12.01.2018).

* * *

Biometric identity verification methods for new uses

Abstract

Widespread use of e-services using information systems and electronic devices requires ensuring a high level of their protection. One of the important mechanisms of the security system is users' identity control. Methods known and used for years are no longer enough protection and also are considered to be burdensome.

The advantage of biometric methods used for authentication and identification of individuals is the convenience of using them, with a guarantee of high efficiency. In the recent times, biometrics have been extensively developed. The multitude of available authentication methods allow them to be used for a variety of purposes. The greatest interest is aroused by the possibility of using them for automatic identification of people. The large-scale use of these techniques, however, raises many objections.

The aim of the article is to show new areas of application of biometric techniques and related problems.

Keywords: security, biometric, authentication, privacy