Nierówności Społeczne a Wzrost Gospodarczy, nr 58 (2/2019)
DOI: 10.15584/nsawg.2019.2.13 ISSN 1898-5084

dr inż. Teresa Mendyk-Krajewska[1]
Katedra Inżynierii Oprogramowania
Wydział Informatyki i Zarządzania
Politechnika Wrocławska

Kontrola tożsamości użytkowników e-usług wobec rozwoju informatyzacji sektora publicznego

Wprowadzenie

Powszechne wykorzystywanie systemów teleinformatycznych we wszystkich niemal dziedzinach oraz stosowanie urządzeń elektronicznych do realizacji usług (udostępnianych w coraz szerszym zakresie) – wymusza intensywne działania na rzecz ich ochrony. Jednym z istotnych mechanizmów bezpieczeństwa są systemy weryfikacji wiarygodności źródła i przesyłanych danych. Aby był możliwy dalszy rozwój ICT w administracji publicznej, by rosło zainteresowanie użytkowników wykorzystywaniem udostępnianych platform realizujących e-usługi (bankowe, finansowe, administracji, służby zdrowia i inne użyteczności publicznej) – musi być łatwy i szybki do nich dostęp, w tym wygodny i odporny na ataki proces uwierzytelniania użytkowników. Stosowane od lat metody, wymagające posiadania poświadczeń materialnych lub znajomości ustalonych haseł, stają się coraz mniej wystarczającym zabezpieczeniem. Korzystne rozwiązanie mogą nieść w tym zakresie systemy oparte o dane biometryczne.

Celem artykułu jest ukazanie zagadnień i problemów dotyczących kontroli tożsamości w systemach teleinformatycznych oraz przedstawienie opinii, objętych autorską ankietą użytkowników Internetu, na temat wykorzystania technologii biometrycznych.

Uwierzytelnianie w systemach teleinformatycznych sektora publicznego

Informatyzacja sektora publicznego w ostatnich latach przebiega bardzo intensywnie. Usługi realizowane drogą elektroniczną z wykorzystaniem wdrożo-

[1] Adres korespondencyjny: Politechnika Wrocławska, Wydział Informatyki i Zarządzania, Katedra Inżynierii Oprogramowania, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław; e-mail: teresa.mendyk-krajewska@pwr.edu.pl. ORCID: 0000-0001-8720-2366.

nych platform systemowych oferowane są w coraz szerszym zakresie, a użytkownicy zachęcani do takiej drogi kontaktu z urzędami administracji publicznej. Z najnowszego raportu o stanie cyfryzacji wynika, że w obszarze cyfrowych usług publicznych Polska zajmuje wśród państw Unii Europejskiej dopiero 24. miejsce (Kucharczyk, 2018). Problem tkwi w braku powszechnego dostępu do stałych łączy szerokopasmowych, dlatego Ministerstwo Cyfryzacji postanowiło doprowadzić je, do 2025 roku, do wszystkich gospodarstw domowych w Polsce.

Popularny sposób uwierzytelniania (autentykacji) użytkowników, oparty na kontroli podawanych przez nich nazwy i hasła, cechuje niski koszt wdrożenia, łatwość użycia oraz brak konieczności korzystania z dodatkowych wyspecjalizowanych urządzeń – jednak w praktyce stosowane hasła są zbyt krótkie i łatwe do zapamiętania (by były mocne), ponadto istnieje możliwość ich podglądnięcia. Metoda jest powszechnie stosowana przy dostępie do zasobów komputerowych, w poczcie elektronicznej i serwisach internetowych.

Inna metoda to uwierzytelnianie z wykorzystaniem identyfikatorów, takich jak tokeny i karty (elektroniczne, magnetyczne, zbliżeniowe czy SIM), będących nośnikami danych opisujących właściciela. Ten sposób weryfikacji użytkowników stosowany jest głównie przy realizacji e-płatności. Kontrola tożsamości może opierać się tylko na jednym czynniku (tzw. uwierzytelnianie jednoczynnikowe) lub kilku wybranych (np. haśle i identyfikatorze materialnym – uwierzytelnianie wieloczynnikowe).

Każda standardowa procedura dotycząca elektronicznej kontroli tożsamości obejmuje trzy procesy ujęte w międzynarodowej normie ISO/IEC 29115 (*Information Technology – Security Techniques – Entity Authentication Assurance Framework*):

- rejestrację – pozyskanie danych do procesu weryfikacji,
- zarządzanie wykorzystywanymi danymi (ich wydawanie, odnawianie, zawieszanie, unieważnianie),
- poświadczanie tożsamości.

W tej normie zdefiniowano też dopuszczalne poziomy wiarygodności wyniku poświadczania tożsamości dla każdej dostępnej e-usługi. Na określenie takiego poziomu wpływa wiele czynników technicznych i organizacyjnych, przy czym ostateczna klasyfikacja zależy od najniższego poziomu uzyskanego przy ocenie każdego z nich. I tak wyróżnia się cztery poziomy:

- LoA 1 (*Level of Assurance 1*) – minimalna wiarygodność (lub jej brak),
- LoA 2 – ograniczona wiarygodność; stosowane uwierzytelnianie jednoczynnikowe, wymagany bezpieczny protokół uwierzytelnienia (redukujący wpływ potencjalnych ataków), wymagana ochrona danych,
- LoA 3 – wysoka wiarygodność; poziom wymaga uwierzytelniania wieloczynnikowego oraz wykorzystania systemów kryptograficznych,
- LoA 4 – bardzo wysoka wiarygodność deklarowanej tożsamości; do wymagań dla poziomu LoA 3 dochodzi konieczność fizycznej obecności rejestrowanej osoby oraz użycie odpornych na manipulacje identyfikatorów sprzętowych przechowu-

jących tajne informacje, a stosowany w procesie protokół ma zapewnić (z użyciem metod kryptograficznych) poufność wykorzystywanych danych osobowych.

Weryfikacja tożsamości w teleinformatycznych systemach administracji publicznej jest możliwa poprzez użycie Profilu Zaufanego lub podpisu elektronicznego. Profil Zaufany pełni funkcję podpisu odręcznego. Każdy obywatel może posiadać tylko jeden Profil Zaufany, a jego ważność wynosi 3 lata. Dzięki niemu można wysyłać drogą elektroniczną do określonych urzędów różne dokumenty i wnioski (dot. wydania dowodu osobistego, złożenia deklaracji podatkowej, rejestracji działalności gospodarczej, zameldowania itd.). Profil Zaufany można założyć w wybranych serwisach bankowych (m.in. PKO BP, ING Bank Śląski, Bank Millennium, mBank czy BZWBK) lub poprzez serwis pz.gov.pl (w tym przypadku wymagane jest osobiste potwierdzenie tożsamości w wybranym punkcie potwierdzającym Profil Zaufany). Liczba użytkowników tego systemu wynosi już ponad 1,7 mln (Kucharczyk, 2018).

Systemy informatyczne oraz urządzenia przeprowadzające mocne uwierzytelnianie i autoryzację[2] wykorzystują algorytmy kryptograficzne. W realizacji podpisu elektronicznego stosuje się jednokierunkową funkcję skrótu (np. SHA-2, SHA-3), która dla dowolnej wiadomości wejściowej generuje ciąg bitów określonej długości umożliwiając weryfikację integralności danych, oraz asymetryczny algorytm szyfrowania (np. RSA). Użytkownik korzystający z mechanizmu podpisu elektronicznego jest w posiadaniu pary kluczy: swojego tajnego klucza prywatnego do wygenerowania podpisu (poprzez szyfrowanie skrótu otrzymanego z wiadomości) oraz publicznego, który udostępnia dla potrzeb realizacji procesu weryfikacji. Podpisy cyfrowe mogą być wykorzystywane do potwierdzenia dokumentów w postaci elektronicznej w bankowości, handlu, administracji publicznej i służbie zdrowia. Autentyczność klucza publicznego jest poświadczana stosownym certyfikatem wydanym przez urząd certyfikacji podległy głównemu urzędowi certyfikacji, którym w Polsce jest Narodowe Centrum Certyfikacji, utworzone przez Narodowy Bank Polski. Dla uniemożliwienia sfałszowania daty powstania e-dokumentu, sporządzany podpis elektroniczny może być znakowany czasem, dzięki usłudze kwalifikowanego znacznika czasu (DTS – *Digital Time Stamping*). Może mieć to istotne znaczenie w przypadku powszechnie wykorzystywanych e-dokumentów w działalności biznesowej. Znacznik czasu jest realizowany przez urząd znacznika czasu (TSA – *Time Stamping Authority*) w ramach infrastruktury klucza publicznego. Protokół znacznika czasu został zdefiniowany w standardzie RFC 3161 w 2001 r. przez ITEF (*Internet Engineering Task Force*). Skrót dokumentu zostaje oznaczony czasem, podpisany z użyciem klucza prywatnego podmiotu świadczącego tę usługę, i odesłany nadawcy (Marucha-Jaworska, 2015).

Z badań przeprowadzonych na zlecenie firmy Nuance Communications przez agencję TNS Polska w listopadzie 2014 roku wynika, że prawie połowa użytkow-

[2] Proces, w którym sprawdzane jest, czy dany podmiot (o ustalonej tożsamości) ma prawo dostępu do zasobów, do których stara się go uzyskać.

ników (47%) odczuwa uciążliwość stosowanych metod weryfikacji, a 46% czuje niechęć do systemów wymuszających tworzenie złożonych haseł. Wspomnianym badaniem objęto reprezentatywną grupę tysiąca polskich internautów w wieku 18–65 lat, z podziałem na płeć, wiek i miejsce zamieszkania. Połowa ankietowanych podkreśla brak wpływu użytkownika na bezpieczeństwo podawanych przez siebie danych (Balawender, 2015). Tylko co piąty użytkownik dla bezpieczeństwa zmienia swoje hasło czy PIN przynajmniej raz w roku, a prawie 40% czyni to w wyniku wymuszenia zmiany przez system (Morawiecka, 2015). Według badań firmy Telesign, aż 73% internautów w USA i Wielkiej Brytanii używa tylko jednego hasła do wszystkich kont w Internecie, a 47% wykorzystuje to samo hasło od pięciu lat (Ciesielski, 2016).

Wyniki analiz wskazują, iż powszechnie stosowane metody weryfikacji użytkowników mogą stanowić barierę w dostępie do e-usług i hamować dalszy ich rozwój. Z uwagi na wzrost przestępczości elektronicznej wprowadzenie silniejszych sposobów potwierdzania tożsamości staje się koniecznością. Dla podniesienia poziomu ochrony podejmowane są różne działania. Między innymi rozważany jest powrót do koncepcji dowodu osobistego z warstwą elektroniczną, które to rozwiązanie funkcjonuje już w kilkudziesięciu państwach europejskich. W dokumencie Ministerstwa Cyfryzacji z 2016 roku podkreśla się wagę przyjęcia jednolitego standardu cyfrowej identyfikacji obywateli w systemach e-usług administracji publicznej. Jednym z proponowanych rozwiązań jest usprawniony technicznie Profil Zaufany, który wymaga weryfikacji opartej na wytycznych unijnego rozporządzenia eIDAS (*electronic identification and trust services*). Ponieważ jakość i tempo rozpowszechniania podpisu elektronicznego i Profilu Zaufanego, który jest elementem systemu ePUAP (*Elektroniczna Platforma Usług Administracji Publicznej*) są dalece niewystarczające, podjęte zostały prace prowadzące do przyspieszenia upowszechniania elektronicznej identyfikacji obywateli.

Korzystne rozwiązanie mogą nieść w tym zakresie systemy oparte o dane biometryczne.

Biometryczne technologie poświadczania tożsamości

W ciągu ostatnich dziesięciu lat intensywnie rozwijane są techniki biometrycznej kontroli tożsamości dla różnych zastosowań.

Biometria to dziedzina wiedzy zajmująca się pomiarem i wykorzystaniem unikatowych fizycznych, fizjologicznych i behawioralnych cech człowieka (tzw. biometryk), m.in. w systemach identyfikacji (ustalania) i uwierzytelniania (potwierdzania tożsamości). Do mierzalnych cech fizycznych wykorzystywanych w biometrii zaliczamy: odciski palców, naczynia krwionośne palca, naczynia krwionośne dłoni, geometrię dłoni, geometrię twarzy, tęczówkę oka i siatkówkę oka. Wykorzystywanymi cechami behawioralnymi są np. podpis odręczny i głos.

Zalety metod biometrycznych to wygoda użytkowania oraz brak potrzeby posiadania dodatkowych przedmiotów czy pamiętania pomocniczych informacji.

Uwierzytelnianie w oparciu o geometrię dłoni wymaga wykonania pomiaru dłoni i palców oraz sprawdzenia wybranych punktów charakterystycznych. Czytniki wykonują trójwymiarowe zdjęcia rejestrując łącznie ponad 90 pomiarów różnych cech, w tym długość i szerokość dłoni oraz grubość palców i wielkość obszarów pomiędzy kostkami. Rozpoznawanie kształtu dłoni jest wygodne w użyciu, akceptowalne, ale podatne na oszustwa, zaś wykorzystywane urządzenia są duże i kosztowne. Metoda może być stosowana przy ograniczonej liczbie użytkowników z uwagi na duży współczynnik błędu. Można ją łączyć z technikami badającymi rozkład naczyń krwionośnych dłoni.

Metoda identyfikacji i weryfikacji w oparciu o linie papilarne jest szybka i tania – stąd jej duża popularność. Odcisk palca reprezentowany jest przez wektor o długości równej liczbie rejestrowanych cech, a precyzja pomiaru zależy od stawianych wymagań. Wartości liczbowe zawarte w wektorze opisują mierzone cechy linii papilarnych, m.in. rozwidlenia i zakończenia (tzw. minucje – najpowszechniej wykorzystywane) (Bolle, Connell, Pankanti, Ratha, Senior, 2008). Najnowsza technologia oparta na ultradźwiękach umożliwia tworzenie trójwymiarowego modelu układu linii papilarnych, z uwzględnieniem zagłębień i wypukłości. Przykładem jej realizacji jest Touch ID firmy Apple Inc.

Technika rozpoznawania układu naczyń krwionośnych (skanowanie bliską podczerwienią tkanki pod powierzchnią skóry – palca, dłoni) cechuje się bardzo dobrymi współczynnikami jakości weryfikacji oraz wysoką odpornością na próby fałszerstwa. Biometria naczyń krwionośnych dłoni wykorzystywana jest w technologii PalmSecure firmy Fujitsu.

Weryfikacja oparta o geometrię twarzy polega na wyznaczeniu owalu twarzy i jej elementów, tj. oczu, nosa i ust (punktów, linii). Nie wymaga bezpośredniego kontaktu osoby z urządzeniem pomiarowym. Przełomem było stworzenie samouczącego się algorytmu Deep Dense Face Detector, w którym zastosowano konwolucyjną sieć neuronową[3]. Dzięki tym wynikom pracy naukowców z Yahoo Labs i Stanford Uniwersity możliwe jest szybkie i precyzyjne rozpoznawanie twarzy nawet w przypadkach jej częściowego zakrycia lub obrócenia. Przykładem technologii rozpoznawania twarzy jest NeoFace japońskiej firmy NEC.

Metoda identyfikacji wykorzystująca tęczówkę oka jest bezdotykowa, szybka i cechuje się wysoką dokładnością. Na podstawie wykonanego zdjęcia tworzony jest opis punktów charakterystycznych, zgodny z przyjętym kodem. Systemy rozpoznawania tęczówki oka są odporne na ruchy głowy i mrugnięcie powieki. Przykładem realizacji jest rozwiązanie EyeBank firmy IrisGuard. Z kolei metoda wykorzystująca siatkówkę oka (układ naczyń krwionośnych znajdujących się z tyłu oka)

[3] *Convolutional Neural Network* składa się zwykle z kilku warstw konwolucyjnych, a każda jest zbiorem map filtrów; dzięki ich nakładaniu na fragmenty obrazu uzyskiwane są cechy.

jest inwazyjna (wymaga zbliżenia głowy do urządzenia pomiarowego używającego lasera) i charakteryzuje się zmiennością mierzonych cech (np. wskutek chorób).

Niedawno odkryto, że każdy człowiek ma charakterystyczny rozkład temperatury na twarzy. Można go rejestrować dzięki kamerze termowizyjnej pracującej w dalekiej podczerwieni. Metoda pomiaru nie jest inwazyjna i może być stosowana w ciemności – co jest jej dodatkową zaletą, natomiast metoda wykorzystująca stosunkowo łatwy do pobrania kod DNA nie może być stosowana na szerszą skalę, gdyż umożliwia pozyskanie wielu dodatkowych informacji o stanie zdrowia danej osoby.

Duże zainteresowanie budzi biometria głosowa, wykorzystująca zarówno cechy fizyczne związane m.in. z budową strun głosowych, jak i behawioralne (akcent, szybkość wypowiedzi, artykulację). Dla stworzenia fonoskopijnego wzorca – matematycznej reprezentacji charakterystyki głosu – gromadzone są setki parametrów. Technologie są tak zaawansowane, że obecnie możliwa jest precyzyjna weryfikacja zarejestrowanej w systemie osoby, nawet w przypadku modyfikacji głosu na skutek czynników środowiskowych czy fizycznych. Wyróżnia się biometrię głosową pasywną i aktywną. W przypadku biometrii pasywnej weryfikacja odbywa się na zasadzie swobodnej wypowiedzi, natomiast w drugim przypadku użytkownik jest uwierzytelniany na podstawie ustalonej frazy (np. numeru konta, hasła). Dla bezpieczeństwa, celem eliminacji robotów lub nagrania z playbacku, przeprowadzany jest test żywotności. Przykładem tej technologii jest VoicePrint firmy Fujitsu R&D Center Co., Ltd.

Elektroniczny podpis biometryczny (odręczny, składany na tablecie) jest łatwo dostępny, przy tym zależny od emocji i stanu zdrowia. Jednym z warunków uznania podpisu elektronicznego za bezpieczny jest jego sporządzanie z wykorzystaniem urządzenia będącego pod kontrolą osoby składającej podpis (Art. 3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym)[4], zatem nie powinien być on stosowany w instytucjach publicznych i nie powinno być przymusu takiego poświadczania. Odwzorowanie realnego podpisu jest trudno osiągalne i nie ma możliwości weryfikacji odbiorcy, a mimo to podpis biometryczny stał się powszechną praktyką przy potwierdzaniu odbioru przesyłki. Takie wykorzystywanie danych biometrycznych budzi szereg wątpliwości w związku z możliwością kopiowania podpisu i ryzykiem jego użycia w innych celach.

Dla wszystkich technik utworzony wzorzec, z którym porównywane są uzyskane podczas pomiaru cechy, jest przechowywany (w bazie danych lub w urządzeniu weryfikującym) w postaci cyfrowej, i dodatkowo powinien być on zaszyfrowany. Najważniejszymi cechami technik biometrycznych, które stanowią podstawę ich porównania, są: łatwość użycia, podatność na zakłócenia, czas pomiaru i weryfikacji, rozmiar wzorca, dokładność odpowiedzi, koszt wdrożenia i użytkowania systemu oraz wielkość urządzenia.

[4] Ustawa została uchylona i zastąpiona ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

Przy wyborze urządzenia w aspekcie wiarygodności wyników można posłużyć się takimi wskaźnikami jak:
- FAR (*False Acceptance Rate*) – wskaźnik niesłusznych akceptacji,
- FRR (*False Rejection Rate*) – odrzuceń prawidłowych próbek,
- EER (*Equal Error Rate*) – równowagi między FER i FRR
- FTE (*Failure To Enroll*) – niepowodzeń w rejestracji (z przyczyn technologicznych lub proceduralnych),
- FTA (*Failure To Acquire*) – wskaźnik niepowodzeń w pobieraniu; dolna granica FTA definiuje uniwersalność biometryki.

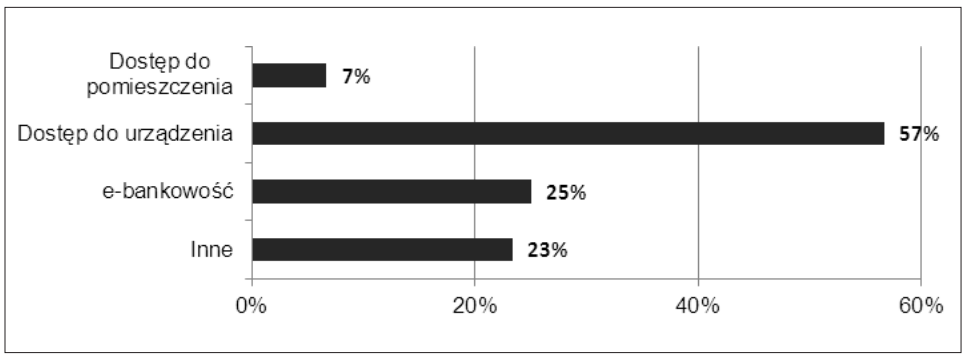
Błędy (niesłuszna akceptacja – stanowi lukę w systemie zabezpieczeń, niesłuszne odrzucenie – utrudnia dostęp) pociągają za sobą określone konsekwencje. Wzajemne ustawienie wartości wskaźników (kompromis pomiędzy wygodą użytkowania a bezpieczeństwem) zależy od zastosowań systemu wykorzystującego daną technikę biometryczną i związanych z tym wymagań. Wygoda konkretnego zastosowania definiowana jest jako łatwość, z jaką poprawnie zarejestrowana osoba jest uwierzytelniana, gdy próbuje uzyskać dostęp do zastosowania (co obejmuje m.in. proces weryfikacji, w tym obsługi wyjątków i niesłuszne odrzucenia) (Bolle, Connell, Pankanti, Ratha, Senior, 2008). Problemy użytkowania mogą wynikać z faktu, iż pewien odsetek populacji nie dysponuje daną cechą biometryczną (nie ma możliwości pobrania próbki) i prawie wszystkie cechy ulegają zmianom z upływem czasu (w procesie starzenia się), ale też na skutek urazów czy niektórych chorób. Trafność odpowiedzi i bezpieczeństwo systemów można zwiększyć dzięki łączeniu kilku technik biometrycznych. Dla osiągnięcia wysokiej skuteczności weryfikacji można też łączyć rozwiązania tradycyjne z technikami biometrycznymi.

Weryfikacja tożsamości w oparciu o metody biometryczne stosowana jest m.in. podczas kontroli dostępu do obiektów (w zakładach pracy) czy do sprzętu (komputerów, telefonów komórkowych), w bankowości, w celu zwiększenia ochrony porządku publicznego, do zabezpieczania systemów alarmowych, zamków drzwiowych itp. oraz dla przyspieszenia procesu sprawdzania tożsamości na lotniskach, przejściach granicznych itd.

W Polsce prace w zakresie stosowania technik biometrycznych w rozwiązaniach informatycznych są prowadzone m.in. przez MSWiA, pracowników naukowych Politechniki Śląskiej oraz gliwicką spółkę WASKO. Równolegle tworzone są dokumenty normalizacyjne; warto tu wymienić: normę ISO/IEC 19794, zawierającą znormalizowane formaty danych dla różnych technik biometrycznych (do przesyłania i przechowywania), normę ISO/IEC 19784-1:2006 zawierającą opracowanie wysokopoziomowego programistycznego modelu uwierzytelniania biometrycznego oraz 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). Rozporządzenie weszło w życie 25 maja 2018 r.

Nowe techniki weryfikacji w ocenie użytkowników

Zalety realizacji usług drogą elektroniczną to dostępność w każdym miejscu, oszczędność czasu, szybkość i wygoda. W pełni potwierdzają to wyniki autorskiego badania ankietowego, przeprowadzonego w maju 2018 roku wśród studentów I i III roku informatyki Politechniki Wrocławskiej, którym objęto 120 osób. Wszyscy ankietowani realizują e-usługi, z czego 83% czyni to systematycznie. Większość (65%) objętych badaniem studentów stosuje już identyfikację biometryczną w celu uzyskania szybkiego dostępu do swojego sprzętu (smartfona, tabletu itp.). Z badań wynika, że 77% ankietowanych było już poddanych uwierzytelnianiu metodami biometrycznymi w różnych okolicznościach. Uzyskane wyniki przedstawiono na rys. 1 i 2.

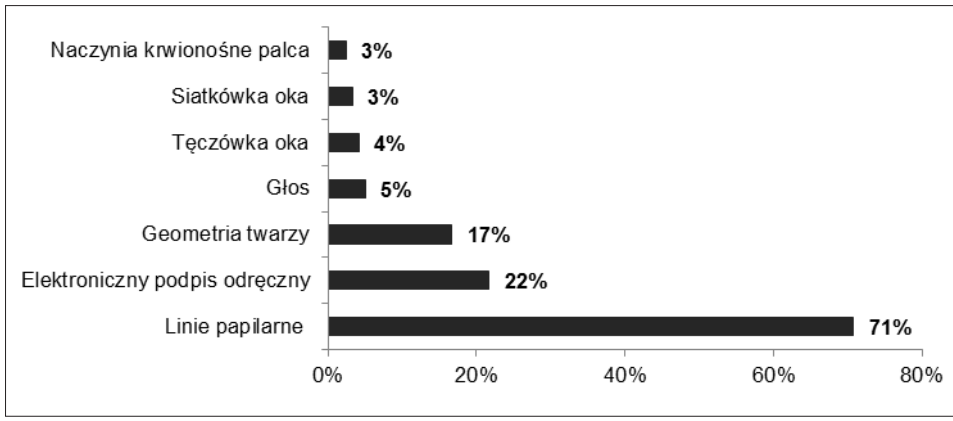


Rys. 1. Deklarowane okoliczności biometrycznej kontroli tożsamości

Źródło: opracowanie własne.

Znanym obszarem zastosowań technik biometrycznych jest bankowość (oddziały, bankomaty, płatność elektroniczna) – i dla tych potrzeb są one intensywnie rozwijane (Mendyk-Krajewska, 2018).

Bankowość biometryczna w Polsce rozwinęła się dzięki zaangażowaniu banków spółdzielczych. Biometryczne bankomaty jako pierwsze wdrożyły: Bank Polskiej Spółdzielczości i Podkarpacki Bank Spółdzielczy w 2010 roku. Pod koniec 2017 roku w Grupie BPS biometria była udostępniona w ponad 30 bankach (Pawęda, 2017). Przykładowo, do połowy 2017 roku odnotowano 1,2 mln aktywacji aplikacji mobilnej IKO przez klientów banku PKO BP (Bielecka, 2017). Opatrzoną certyfikatem aplikację można pobrać z zaufanego sklepu internetowego (Google Play, App Store, Windows Phone Store). Logowanie wymaga użycia PIN-u lub metody biometrycznej (odcisk palca). Udostępniona w 2013 roku aplikacja została rozbudowana o kolejne funkcje: doładowanie telefonu, realizacje płatności zbliżeniowych z wykorzystaniem technologii NFC (*Near Field Communications*), przelewów, zakładanie lokat, obsługę kart płatniczych itd.



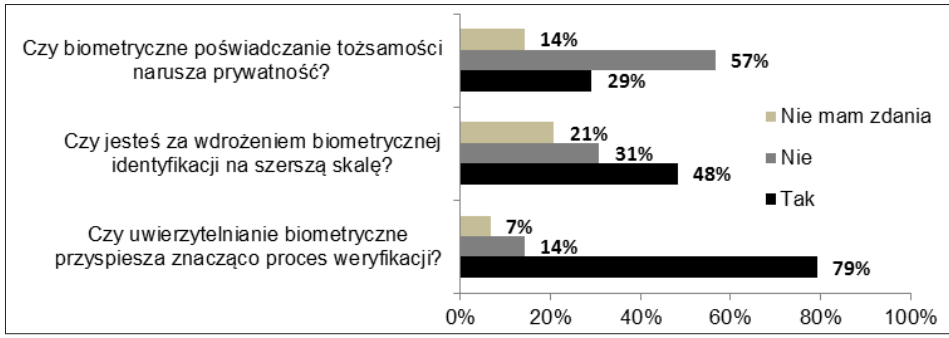
Rys. 2. Cecha mierzona podczas weryfikacji biometrycznej respondentów

Źródło: opracowanie własne.

Korzystanie z e-bankowości deklaruje 25% ankietowanych. Większość pytanych pozytywnie ocenia biometryczną kontrolę tożsamości (42% pozytywnie, a 49% raczej pozytywnie), jedynie 6% raczej negatywnie, a zdecydowanie negatywnie tylko 1% (2% nie miało w tej kwestii zdania). Jednocześnie 41% użytkowników obawia się o bezpieczeństwo swoich danych osobowych przy stosowaniu takich rozwiązań. Zdecydowana większość (79%) jest zdania, że nowe techniki znacząco przyspieszają proces uwierzytelniania. Na pytanie, czy biometryczne poświadczanie tożsamości narusza prywatność[5] – 57% ankietowanych odpowiada przecząco, a 14% nie ma zdania. Jednak dane biometryczne są szczególną kategorią danych osobowych. Biometria stanowi zagrożenie dla prywatności, gdyż niesie informacje np. o braku posiadania określonych cech (co może prowadzić do dyskryminacji), niektórych chorobach, przeprowadzonych operacjach plastycznych czy zabiegach stomatologicznych. Aspekty prawne dotyczące prywatności i ochrony danych osobowych, w tym odnoszące się do danych biometrycznych, w szerokim zakresie analizuje Jaroszewska-Choraś (2016). Stosunek ankietowanych do nowych technik identyfikacji i uwierzytelniania przedstawiono na rys. 3.

Otrzymane wyniki potwierdzają akceptację nowych metod uwierzytelniania przez młodych użytkowników e-usług i wskazują na zainteresowanie ich wdrożeniem. Najmniejsze obawy, z uwagi na powszechną obecność mikrofonów i kamer, budzą analiza głosu i rysów twarzy. Biometria głosowa jest jedną z najbardziej akceptowalnych metod – szczególnie do autoryzacji usług podczas zdalnej obsługi klienta. Wzorzec głosowy może być stosowany we wszystkich kanałach obsługi: w telefonicznym biurze obsługi, portalu, w aplikacjach mobilnych itd.

[5] Prawo człowieka do prywatności i ochrony danych osobowych jest objęte ochroną w sferze prawnomiędzynarodowej; prawo do prywatności pojawiło się w USA na przełomie XIX i XX w., a w Europie rozwinęło w XX wieku.



Rys. 3. Ocena biometrycznych metod weryfikacji tożsamości

Źródło: opracowanie własne.

Uzyskane przez agencję TNS Polska, we wspomnianym badaniu, wyniki wykazują, że 54% ankietowanych uważa weryfikację głosem za wygodną, szybką i bezpieczną, a jedynie 23% wyraziło wątpliwości (zmiana głosu, łatwość nagrania) (Balawender, 2015).

Jednym z pierwszych banków, który wdrożył biometrię głosową (Nuance FreeSpeech) jest komercyjny bank słowacki Tatra banka, założony w 1990 r. W ciągu roku z tej metody zaczęło korzystać ponad 70% klientów, a średni czas uwierzytelniania skrócił się o 66%. Przeprowadzone przez bank badanie wykazało, że 90% klientów uważa tę metodę za dobrą alternatywę dla klasycznego sposobu weryfikacji. Technologię Nuance FreeSpeech stosują też ING Bank w Holandii, brytyjski Barclays Wealth & Investment Management, Abu Dhabi Commercial Bank i wiele innych. W Polsce pierwszą instytucją finansową, która wprowadziła autoryzację głosem był Smart Bank (w 2015 r.).

Wykorzystanie biometrycznych metod poświadczania tożsamości użytkowników widziane z perspektywy instytucji sektora publicznego może być gwarancją wzrostu bezpieczeństwa realizowanych przez nią e-usług, a tym samym przyczynić się do poprawy jej wizerunku.

Podsumowanie

Polski obywatel, przedsiębiorca czy organizacja muszą mieć możliwość szybkiego i bezpiecznego załatwienia sprawy w urzędach administracji publicznej każdego szczebla. Do tego są potrzebne zarówno infrastruktura teleinformatyczna i rozwinięte usługi e-administracji, jak i mocny mechanizm identyfikacji i uwierzytelniania użytkowników.

Powszechnie stosowane sposoby weryfikacji nie umożliwiają sprawdzenia faktycznej tożsamości (a jedynie potwierdzają znajomość hasła i/lub posiadanie identyfikatora) – dlatego muszą być zastąpione mechanizmami pozbawionymi tej wady.

Postęp technologiczny sprawia, że metody biometrycznego poświadczania tożsamości stają się coraz bardziej akceptowalne i są wdrażane w coraz to nowych obszarach. Prace dotyczące zastosowania biometrii są intensywnie prowadzone przez środowiska naukowe, przedstawicieli rządów i sektorów bankowych. Istnieje nawet plan utworzenia ogólnoświatowego systemu wykorzystującego dane biometryczne zgromadzone w poszczególnych krajach dla realizacji ich wspólnych celów.

Niestety, ceną użycia technik biometrycznych jest spadek poziomu anonimowości i prywatności obywateli.

BIBLIOGRAFIA

Balawender, D. (2015). *Nowy raport TNS pokazuje, że Polacy mają dość haseł dostępu, numerów PIN, tokenów. Czas na hasło głosowe*. Pobrane z: http://banking-magazine.pl/2015/01/15/nowy-raport-tns-pokazuje-ze-polacy-maja-dosc-hasel-dostepu-numerow-pin-tokenow-czas-na-haslo-glosowe/ (2018.04.20).

Bielecka, Ż. (2017). *Nie bój się bankowania w telefonie*. Pobrane z: https://bankomania.pkobp.pl/bankofinanse/bankowosc-internetowa-i-mobilna/nie-boj-sie-bankowania-w-telefonie/ (2018.06.12).

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W. (2008). *Biometria*. Warszawa: Wydawnictwa Naukowo-Techniczne.

Ciesielski, M. (2016). *Biometria w bankach przyspieszy, bo mamy dość haseł*. Pobrane z: http://forsal.pl/artykuly/992697,biometria-w-bankach-przyspieszy-bo-mamy-dosc-hasel.html (2018.06.11).

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

Kucharczyk, K. (2018). *Cyfryzacja administracji w Polsce dopiero nabiera tempa*. Pobrane z: http://www.rp.pl/Biznes-IT/306119912-Cyfryzacja-administarcji-w-Polsce-dopiero-nabiera-tempa.html (2018.06.15).

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

Mendyk-Krajewska, T. (2018). Techniki uwierzytelniania biometrycznego dla realizacji usług drogą elektroniczną. *Ekonomiczne Problemy Usług, 2*(131/2), 117–126. DOI: 10.18276/epu.2018.131/2-11.

Ministerstwo Cyfryzacji, Kierunki Działań Strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych. Pobrane z: www.gov.pl/cyfryzacja/kierunki-dzialan-strategicznych-ministra-cyfryzacji-w-obszarze-informatyzacji-uslug-publicznych (2018.06.19).

Morawiecka, A. (2015). *Jesteśmy zmęczeni hasłami, PINami i kodami*. Pobrane z: https://bankomania.pkobp.pl/bankomania/nowe-technologie/jestesmy-zmeczeni-haslami-pin-ami-i-kodami/ (2018.05.18).

Pawęda, D. (2017). *„Przybij piątkę w bankomacie" – czyli o biometrii palm vein w bankowości spółdzielczej*. Pobrane z: https://bs.net.pl/przybij-piatke-w-bankomacie-czyli-o-biometrii-palm-vein-w-bankowosci-spoldzielczej-2/ (2018.06.17).

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 (Dz. Urz. UE L.119/1 z 2016 r.).

Streszczenie

Istotnym warunkiem dalszej informatyzacji administracji publicznej oraz bezpiecznej realizacji e-usług jest wygodny i bezpieczny proces weryfikacji tożsamości. Znane, stosowane od lat metody wymagające posiadania poświadczeń materialnych lub znajomości poufnych haseł nie są już wystarczającym zabezpieczeniem, ponadto są odczuwane jako uciążliwe. Korzystne rozwiązanie mogą nieść systemy oparte o mierzalne, unikatowe cechy fizyczne i behawioralne użytkowników. Intensywnie rozwijane techniki biometrycznej weryfikacji stają się coraz bardziej akceptowalne i znajdują zastosowanie w coraz to nowych obszarach.

Celem artykułu jest wskazanie dynamicznie rozwijanych technik uwierzytelniania biometrycznego oraz przedstawienie opinii użytkowników Internetu, objętych autorską ankietą, na temat wdrażania i wykorzystania nowych technologii sprawdzania tożsamości.

Słowa kluczowe: bezpieczeństwo e-usług, uwierzytelnianie, biometria.

The identity control of e-services and the development of computerization in the public sector

Summary

A convenient and secure process of identity verification is an important condition for further computerization of public administration and secure realization of e-services. . Methods known and used for years which require material credentials or knowledge of confidential passwords are no longer enough protection as well as they are considered to be burdensome. An advantageous solution may lie in systems based on measurable, unique physical and behavioral characteristics of users. Intensively developed biometric verification techniques are becoming more and more acceptable and are used in more and more new areas.

The aim of the paper is to indicate dynamically developed biometric authentication techniques and to present the opinions of Internet users covered by the author's questionnaire on the implementation and use of new identity verification technologies.

Keywords: e-services security, authentication, biometric.

JEL: O32, O39.