Ekonomiczne Problemy Usług nr 2/2018 (131), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/2-11 | strony: 117–126

Teresa Mendyk-Krajewska
Politechnika Wrocławska
Wydział Informatyki i Zarządzania
Katedra Inżynierii Oprogramowania
teresa.mendyk-krajewska@pwr.edu.pl

Techniki uwierzytelniania biometrycznego dla realizacji usług drogą elektroniczną

Kody JEL: 0320, 0390
Słowa kluczowe: biometria, uwierzytelnianie, bezpieczeństwo e-usług
Streszczenie. Realizacja usług drogą elektroniczną wymaga szybkiej i wygodnej identyfikacji, autoryzacji i weryfikacji użytkowników. Wyróżnia się trzy podstawowe grupy sposobów poświadczania tożsamości: metody oparte na wiedzy, metody wykorzystujące identyfikatory materialne oraz mechanizmy stosujące biometrię. Techniki biometrycznego poświadczanie tożsamości są w ostatnich latach intensywnie rozwijane. Ich zaletą jest wygoda stosowania przy wysokiej skuteczności działania. Od kilku lat wykorzystywane są m.in. w bankowości, a mają być też wdrażane w administracji i szeroko rozumianej gospodarce – co budzi wiele wątpliwości.

Wprowadzenie

Wraz z rozwojem gospodarki elektronicznej coraz więcej usług świadczonych jest z wykorzystaniem internetu i urządzeń elektronicznych. Bezpieczna realizacja e-usług wymaga ochrony przechowywanych i przesyłanych danych oraz identyfikacji i weryfikacji tożsamości użytkowników. Systemy kontroli dostępu łączą wiele rozwiązań technicznych, których zadaniem jest udostępnianie obiektów i zasobów osobom upoważnionym (przy jednoczesnej blokadzie działań nieuprawnionych). Proces uwierzytelniania, zależnie od potrzeb, może przebiegać jednostronnie, dwustronnie lub z udziałem zaufanej trzeciej strony. Jest wiele metod umożliwiających sprawdzanie tożsamości.

Tradycyjne sposoby identyfikacji[1], weryfikacji (autentykacji)[2] i autoryzacji[3] w różnych zastosowaniach wymagają identyfikatorów materialnych (tj. tokenów[4], kart magnetycznych, elektronicznych, zbliżeniowych[5] czy SIM[6]) lub znajomości poufnych haseł (lub kluczy kryptograficznych). Słabościami tych zabezpieczeń są odpowiednio: konieczność posiadania wymaganych przedmiotów oraz możliwość stosowania prostych haseł i łatwość ich nielegalnego pozyskania. Tradycyjne metody pozwalają jedynie ustalić czy weryfikowana osoba jest w posiadaniu poświadczenia materialnego lub zna właściwe hasło (czy PIN).

Ze względu na rozwój e-usług oraz wzrost przestępczości elektronicznej dąży się do wprowadzenia silniejszych sposobów potwierdzania tożsamości. Coraz częściej stosowane są do tego metody biometryczne, wykorzystujące wybrane unikatowe cechy osobnicze (niezmienne, mierzalne i niepodrabialne).

Celem artykułu jest ukazanie obserwowanej w ostatnich latach dynamiki rozwoju biometrycznych metod potwierdzania tożsamości, które znajdują coraz szersze zastosowanie, a także wskazanie związanych z tym problemów.

1. Kryteria oceny technik uwierzytelniania biometrycznego

Biometria to dziedzina wiedzy zajmująca się technikami pomiaru i wykorzystaniem unikatowych cech człowieka, m.in. w systemach identyfikacji i kontroli dostępu. Biometryczne systemy kontroli mogą bazować na pomiarach cech fizycznych (genotypów), takich jak: linie papilarne, geometria twarzy, tęczówka i siatkówka oka, rozkład temperatury na twarzy, geometria dłoni, rozkład naczyń krwionośnych (na dłoni lub przegubie ręki) oraz cech behawioralnych – związanych z zachowaniem (fenotypów), takich jak: głos, chód, podpis odręczny czy sposób pisania na klawiaturze. Do najważniejszych cech technik biometrycznych, stanowiących podstawę ich porównania, należą:

- łatwość użycia,
- podatność na zakłócenia,
- czas rejestracji (pomiaru) i weryfikacji (podjęcia decyzji),
- rozmiar wzorca,

---

[1] Realizacja procesu wymaga porównania pobranej próbki z każdą zapisaną w bazie.

[2] Proces sprawdzania autentyczności użytkowników przez porównanie uzyskanej informacji z wcześniej zapisaną w bazie.

[3] Proces sprawdzania prawa dostępu do danych zasobów podmiotu o ustalonej tożsamości.

[4] Generator kodów jednorazowych biorących udział w uwierzytelnianiu (dodatkowym zabezpieczeniem jest czas ich ważności); z powodu wysokich kosztów urządzeń, jednorazowe kody są dostarczane w wiadomościach sms lub funkcję tokena pełni aplikacja.

[5] Rodzaj karty wykorzystującej technologię RFID (*Radio Frequency Identification*).

[6] Subscriber Identity Module.

- wiarygodność wyników (dokładność odpowiedzi),
- koszt wdrożenia i użytkowania systemu,
- wielkość urządzenia,
- akceptowalność społeczna.

Ważne jest, by technika biometryczna była właściwie dobrana – zależnie od warunków, w jakich będzie stosowana oraz od przeznaczenia wykorzystującego ją systemu. Na wybór metody mogą wpływać różne parametry. Jednym z nich jest czas weryfikacji tożsamości (pomiaru i odpowiedzi systemu). Czas rejestracji jest zwykle dłuższy i może wynosić nawet kilkadziesiąt sekund (w przypadku pomiaru tęczówki oka oraz naczyń krwionośnych palca i dłoni). Innym istotnym parametrem jest rozmiar wzorca cechy biometrycznej wpływający na wielkość pamięci wymaganej do jej przechowywania i na czas potwierdzania. Najmniejszy rozmiar wzorca cechuje metodę pomiaru kształtu dłoni, zaś duże wartości wzorce osiągają przy pomiarze naczyń krwionośnych dłoni i analizie głosu. Do porównania systemów biometrycznych wykorzystuje się takie wskaźniki jak:

- FAR (*False Acceptance Rate*) – wskaźnik niesłusznych akceptacji,
- FRR (*False Rejection Rate*) – wskaźnik niesłusznych odrzuceń,
- FTA (*Failure to Enroll*) – niepowodzeń w rejestracji,
- EER (*Equal Error Rate*) – określa poziom równowagi między FER i FRR.

Im współczynnik FAR jest lepszy, tym gorszy jest FRR (i odwrotnie). Ustawienie ich wartości zależy od zastosowań i związanych z tym wymagań. Niepowodzenia w rejestracji mogą wynikać z ograniczeń technologicznych lub problemów proceduralnych. Do najbardziej akceptowanych metod zalicza się kolejno: badanie głosu, analizę linii papilarnych i rozpoznawanie kształtu dłoni. Większa akceptowalność cechuje metody nieinterakcyjne, niewymagające kontaktu z urządzeniem pobierającym próbkę. Na akceptowalność społeczną wpływa również łatwość użycia danej techniki, dlatego najmniejsze obawy budzi analiza głosu i rysów twarzy (z uwagi na powszechną obecność mikrofonów i kamer), zaś największe – metoda skanowania siatkówki oka. Akceptowalność rozwiązań biometrycznych jest coraz większa, szczególnie wśród ludzi młodych.

2. Biometryczne systemy weryfikacji użytkowników e-usług

W konsekwencji rozwoju e-usług obserwowanego w ciągu ostatnich lat trudno sobie już wyobrazić organizację (instytucję, firmę), która nie umożliwiałaby ich realizacji drogą elektroniczną. Popularność e-usług w sektorze bankowym, administracji centralnej i samorządowej oraz w wielu innych obszarach stale rośnie z powodu korzyści ekonomicznych, elastyczności działania i oszczędności czasu. Niestety, systemy informatyczne i elektroniczne kanały komunikacyjne są podatne na różnego rodzaju zagrożenia, dlatego ważnym elementem bezpiecznej realizacji e-usług jest mechanizm uwierzytelniania uprawnionych użytkowników.

Biometryczny system kontroli składa się z czytnika biometrycznego lub urządzenia skanującego, oprogramowania przetwarzającego pobrane dane na postać cyfrową oraz bazy danych przechowującej wzorce do porównań w procesie weryfikacji. Podstawą działania systemu jest wcześniejsza rejestracja uprawnionych użytkowników. W tym celu pobierane są od nich wybrane cechy biometryczne w postaci próbek, które są przetwarzane z wykorzystaniem określonych algorytmów, i zapamiętywane w bazie danych w formie cyfrowego wzorca. Najważniejszym elementem systemu biometrycznego jest czytnik, a na jakość pobranego materiału mogą mieć wpływ czynniki zewnętrzne (np. sposób przyłożenia palca i siła jego nacisku w przypadku linii papilarnych). Działanie algorytmów przetwarzających dane polega na analizie zależności pomiędzy określonymi punktami charakterystycznymi w przetwarzanej próbce. Weryfikacja może być dokonywana w czytniku lub w połączonym z nim komputerze.

Zwykle systemy wykorzystujące cechy fizyczne są szybsze i wygodniejsze w użytkowaniu, niż te oparte na cechach behawioralnych. Przy masowym użytkowaniu systemu weryfikacji (wymagana łatwość użycia i niski koszt) korzystny jest wybór techniki rozpoznawania głosu lub rysów twarzy, natomiast przy wymogach wysokiego poziomu bezpieczeństwa – naczyń krwionośnych lub tęczówki czy siatkówki oka.

Każdy system ma określony próg akceptacji odpowiedzi. Jeśli wynik bieżącego pomiaru zbyt odbiega od przechowywanego w bazie wzorca, do uwierzytelnienia nie dochodzi. Zaufanie do systemów bazuje na zaufaniu do producentów urządzeń realizujących te usługi. Jest wiele firm oferujących gotowe narzędzia identyfikacji biometrycznej do różnych zastosowań. Wśród znanych producentów można wymienić takie firmy jak: Hitachi (pomiar naczyń krwionośnych palca), Fujtsu (pomiar naczyń krwionośnych dłoni), Iris Guard (pomiar tęczówki) czy Siemens (pomiar linii papilarnych).

Jako zalety nowych technik ustalania tożsamości wskazuje się wygodę użytkowania, brak potrzeby posiadania dodatkowych przedmiotów i pamiętania (przechowywania) pomocniczych informacji. Fizyczne karty dostępu mogą zostać ponadto zniszczone lub zgubione, a hasła odgadnięte lub podejrzane – co nie dotyczy nowych metod. Jedną z istotnych wad weryfikacji z wykorzystaniem danych biometrycznych jest jej zawodność w przypadku deformacji ciała wskutek urazów mechanicznych lub procesu starzenia się.

Dla osiągnięcia wysokiej skuteczności potwierdzania tożsamości, wskazuje się możliwość działania wieloetapowego – łączącego rozwiązania tradycyjne z technologią biometryczną, lub opartą na kilku cechach biometrycznych. Jedna z koncepcji rozwoju technik biometrycznego uwierzytelniania jest ukierunkowana na tworzenie uniwersalnych systemów bazujących na różnych technikach biometrycznych, co umożliwiałoby dokonywanie wyboru techniki weryfikacji tożsamości zależnie od potrzeb użytkowania. Takie rozwiązanie wymaga między innymi standaryzacji formatów danych.

3. Biometryczne techniki sprawdzania tożsamości w praktyce

Duży obszar dla zastosowań biometrycznych technik weryfikacji tożsamości stanowi bankowość elektroniczna. Urządzenia biometryczne można stosować w bankomatach, oddziałach banków, w płatnościach mobilnych i bankowości korporacyjnej. W Polsce w 2007 roku powstała Grupa ds. biometrii w ramach Forum Technologii Bankowych przy Związku Banków Polskich w celu popularyzacji zastosowania i edukacji w tym zakresie środowiska bankowego i administracji publicznej.

Początek działania bankomatów z czytnikami biometrycznymi to 2005 rok. Zastosowanie biometrii w e-bankowości najszybciej rozwijało się w Azji. Do wiodących krajów należą Indie i Japonia, druga w kolejności jest Ameryka Południowa, gdzie przoduje Brazylia. Na koniec 2012 roku 7% bankomatów na świecie wyposażonych było w rozwiązania biometryczne, głównie w pięciu krajach Azji. W tym samym czasie w Europie Zachodniej jedynie 3% tych urządzeń wyposażonych było w odpowiednie czytniki (Automatyka, 2013).

Banki najczęściej stosują weryfikację linii papilarnych (*Finger Print*), naczyń krwionośnych palca (*Finger Vein*) oraz naczyń krwionośnych dłoni (*Palm Vein*). Około 80% z nich wykorzystuje technologię *Finger Vein*, której dokładność zbliżona jest do metody wykorzystującej skanowanie tęczówki oka. Pionierami w bankowości biometrycznej w Europie są polskie banki spółdzielcze – Bank Polskiej Spółdzielczości (2010 r.) i Podkarpacki Bank Spółdzielczy – co miało je promować na rynku. W obu przypadkach zastosowano technologię *Finger Vein* firmy Hitachi. Stopniowo technologie biometryczne zaczęły wprowadzać banki komercyjne – początkowo do weryfikacji klientów w oddziałach (BPH, Getin Bank, Eurobank), a następnie w bankomatach i innych urządzeniach samoobsługowych (Automatyka, 2013). Od stycznia 2013 roku z technologii *Finger Vein* korzystają już wszystkie oddziały banku BPH w Polsce. Obecnie z technologii tej korzysta np. Krakowski Bank Spółdzielczy, ale są banki, które stosują technologię *Palm Vein*, np. Kaszubski Bank Spółdzielczy.

Na potrzeby rządów i organizacji sektora prywatnego firma Fujitsu opracowała system *Palm Secure*, wykorzystujący naczynia krwionośne dłoni. Systemy oparte na odczycie układu naczyń krwionośnych dłoni lub palców znalazły zastosowanie w japońskim sektorze finansowym (ponad 80% instytucji), w bankach tureckich (Turkiye IS Bankasi) (Plucińska, Wójtowicz, 2014) oraz w brytyjskim Barclays Bank (Automatyka, 2015). Stosunkowo późno wdrażaniem technik biometrycznych w sektorze bankowym zainteresowały się Stany Zjednoczone. Pierwszy amerykański pilotażowy program płatności z ich wykorzystaniem rozpoczął się na początku 2015 roku (testy dotyczyły biometrii siatkówki oka).

Bankomaty reagują głównie na odcisk palca użytkownika, natomiast w Chinach w 2015 roku wprowadzono pierwszy system dokonujący potwierdzenia tożsamości na podstawie twarzy (Westlake, 2015). Ten sposób uwierzytelniania wdrożył np. chiński Merchants Bank w bankomatach (kamera skanuje twarz klienta w momencie podcho-

dzenia do urządzenia), planując wprowadzenie go też przy obsłudze klientów w placówkach banku (Automatyka, 2015).

Biometryczny system rozpoznawania głosu przez wychwytywanie i rejestrowanie jego unikatowych cech, a następnie ich porównanie z próbką zapisaną w bazie to wygodna metoda autoryzacji przy próbie dostępu do aplikacji, usług online albo obsługi urządzeń IoT[7] (Nosowski, 2017). BZ WBK już w 2015 roku wdrożył biometrię głosu na infolinii, co wymagało wcześniejszej rejestracji próbek głosu klientów w bazie danych (Boczoń, 2017). Obecnie technika uwierzytelniania Voiceprint, polskiej firmy VoicePIN, wykorzystywana jest m.in. przez Bank ING i Ministerstwo Finansów. System VoicePIN ma mechanizm zabezpieczający przed playbackiem i użyciem syntezatora mowy (Business, 2017)[8]. Metoda jest łatwa w realizacji, bo czytnik (mikrofon) jest zwykle dostępny w każdym urządzeniu i gwarantuje bezpieczeństwo na akceptowalnym poziomie.

Szerokie zastosowanie biometria znalazła w bankowości mobilnej. Już od początku 2016 roku czytnikami Touch ID[9] zaczęli posługiwać się klienci banków Millenium, ING Banku Śląskiego, Eurobanku, Citi Handlowego oraz mBanku, jeśli dysponowali urządzeniami ją obsługującymi (Bień-Chudarek, 2016). Obecnie w Polsce wiele banków umożliwia logowanie odciskiem palca do aplikacji iOS – np. Alior Bank, BZ WBK, mBank, a dla klientów korporacyjnych także ING Bank Śląski. W przypadku aplikacji iOS i Androida są to banki: Citi Handlowy, Eurobank, Getin Bank, Millennium, Plus Bank, a dla klientów detalicznych też ING Bank Śląski (Boczoń, 2017). Nowe rozwiązanie realizujące e-płatności w sposób bezdotykowy zaproponowała w 2016 roku firma Google udostępniając w aplikacji Android Pay opcję HandsFree. Weryfikacja tożsamości odbywała się na podstawie zdjęcia klienta przesłanego do terminalu, jednak przewidywano wprowadzenie kamery umożliwiającej automatyczną identyfikację (Bień-Chudarek, 2016). Interesujący projekt badawczy nad wprowadzeniem kompleksowego rozwiązania stosującego kilka metod (skanowanie twarzy, naczyń krwionośnych dłoni, analizę głosu oraz podpisu odręcznego) prowadzi PKO BP.

Ostatnio pojawiły się doniesienia o rezygnacji przez niektóre banki (Bank Polskiej Spółdzielczości, Getin Bank, Alior Bank) z rozwoju bądź udostępniania usług biometrycznej autoryzacji (Boczoń, 2017) – co może być zaskakujące. Jak dotąd, rozwiązania biometryczne sprawdzają się lokalnie, gdyż problemem jest stworzenie wspólnej dla wszystkich zainteresowanych instytucji (np. banków, urzędów miast) bazy wzorców oraz powstanie podmiotu, który by nią administrował.

Problem weryfikacji tożsamości nabiera szczególnego znaczenia w przypadku osób wykorzystujących do realizacji usług (także bankowych) urządzenia mobilne,

---

[7] *Internet of Thinks* – Internet Rzeczy.

[8] Istniała możliwość przeprowadzenia zaawansowanego technicznie ataku polegającego na konwersji głosu użytkownika przez system przetwarzania mowy.

[9] Technologia wykorzystująca do weryfikacji użytkownika linie papilarne.

w których przyjęta koncepcja bezpieczeństwa oparta jest głównie na ochronie dostępu do samych urządzeń.

Smartfony z czytnikami linii papilarnych zostały spopularyzowane przez firmę Apple (począwszy od iPhone 5S)[10], choć technologia została po raz pierwszy wprowadzona przez jedną z chińskich firm. Odpowiedni czujnik wokół przycisku rejestruje dotyk i aktywuje skanowanie powierzchni palca. Pobrany obraz w wysokiej rozdzielczości jest szczegółowo analizowany, po czym odcisk zostaje przypisany do jednego z trzech podstawowych typów (łuku, pętli lub wiru). Czytnik Touch ID umożliwia skanowanie wielu odcisków palców pod dowolnym kątem. Po stwierdzeniu podobieństwa pobranych danych z przechowywanym zaszyfrowanym wzorcem, urządzenie zostaje odblokowane. Wykorzystywana jest tu zaawansowana architektura zabezpieczeń Secure Enclave, w którą wyposażony jest układ procesorowy urządzenia. Technika służąca do odblokowywania smartfonów stosowana jest też do weryfikacji płatności przez sklepy internetowe iTunes Store i App Store, w usłudze Apple Pay[11] oraz do uwierzytelniania konta w aplikacjach mobilnych banków i płatności PayPal.

Urządzenia biometryczne wykorzystywane kilkanaście lat temu nie zapewniały pożądanego poziomu bezpieczeństwa. Można było je dość łatwo oszukać m.in. używając fotografii twarzy, pobierając odciski lub stosując sztuczny palec. Powszechna dostępność wybranych cech, a tym samym łatwość ich pozyskania, nadal może stwarzać zagrożenie.

W 2014 roku informowano o kilku możliwościach przeprowadzenia ataku na smartfony, pracujące pod systemem Android i wyposażone w czytniki linii papilarnych, a problem dotyczył urządzeń wielu producentów. Przykładowo, w Samsungu Galaxy S5 zewnętrzne aplikacje mogą uzyskać dostęp do API (*Application Programming Interface*) czytnika linii papilarnych, czego konsekwencją może być użycie aplikacji realizującej usługi bankowe (Niebezpiecznik, 2015). W iPhone 5S czytnik Touch ID również można oszukać, jednak fałszywe odciski palców muszą być sporządzone bardziej precyzyjnie z powodu jego dużej rozdzielczości.

W urządzeniach mobilnych wykorzystuje się również inne techniki biometryczne. Na przykład firma Fujitsu wprowadziła skanowanie dłoni w laptopach Lifebook E741/s (od 2011 r.) i Celsius H730 (od 2013 r.) (Wolna, 2014). W nowej wersji smartfona firmy Samsung – Galaxy S8 (z marca 2017 r., z Androidem 7.0), oprócz skanera linii papilarnych udostępniono, dający większe bezpieczeństwo, skaner tęczówki oka. Technologia Face ID dostępna w iPhone X[12] firmy Apple tworząca trójwymiarowy model twarzy, działająca szybko i sprawnie nawet przy złym oświetleniu, uznawana jest nato-

[10] Apple wyposażyła w te czytniki także iPhone 6S i inne modele oraz iPad 5. generacji, iPad Pro, iPad Air2 oraz iPad mini 3 i nowszy, jednak jesienią 2017 r. pojawiła się informacja, że iPhone 8 i iPhone 8 Plus będą ostatnimi smartfonami je wykorzystującymi.

[11] Metoda płatności wykorzystująca technologię NFC (*Near Field Communications*).

[12] W urządzeniu brakuje przycisku Home i skanera linii papilarnych.

miast za wysoce bezpieczną. Szansa odblokowania urządzenia przez osobę nieupoważnioną jest jedna na milion (istnieje taka możliwość w przypadku osoby blisko spokrewnionej).

4. Bezpieczeństwo danych biometrycznych

Umieszczone w bazach danych oryginalne wzorce wykorzystywane w biometrycznych metodach uwierzytelniania wymagają silnego zabezpieczenia. Mierzone cechy osobnicze użytkowników systemów są odpowiednio kodowane i dodatkowo chronione metodami kryptograficznymi. Przykładowo, systemy biometryczne wykorzystujące geometrię dłoni przekształcają wyniki pomiaru do postaci 9-bajtowego wzorca, który zostaje zaszyfrowany, i są przechowywane w takiej postaci. Na pobranej w procesie uwierzytelniania próbce są wykonywane te same przekształcenia, a weryfikacja polega na porównaniu nowo utworzonego wzorca z przechowywanym w bazie. Tak zapisanych danych nie da się łatwo pobrać czy podrobić, i nielegalnie wykorzystać – jednak nie jest to niemożliwe.

Istnieje też możliwość oszukania czytnika w trakcie dokonywania pomiaru. Na przykład metoda rozpoznawania kształtu dłoni nie jest odporna na wysoki stopień podobieństwa dłoni bliźniaków lub bliskich krewnych. Również weryfikacja tożsamości z wykorzystaniem linii papilarnych palców stosowana w smartfonach, zamkach do drzwi i w bankomatach, okazała się nie być tak skutecznym zabezpieczeniem, jak tego oczekiwano. Skuteczne próby udowodnienia jej zawodności z wykorzystaniem danych uzyskanych, np. ze zdjęć czy odcisków pobranych z przedmiotów podejmowano już dawno. Jesienią 2016 roku naukowcom amerykańskim udało się stworzyć replikę dłoni przy pomocy drukarki 3D, pozwalającą oszukać skaner linii papilarnych. Trójwymiarowa replika została stworzona dla opracowania standardu kalibracji czytników, a okazało się, że może zostać wykorzystana do obchodzenia tego typu zabezpieczeń. Dla podniesienia poziomu bezpieczeństwa wprowadzono różne testy żywotności, takie jak rejestracja mimiki twarzy czy badanie pulsu w opuszku palca (Kubanek, 2013).

Zagrożeniem dla użytkowników bankomatów wykorzystujących karty są urządzenia odczytujące dane z paska lub czipa (tzw. skimmery). Istnieje też możliwość zdalnego skopiowania danych z karty zbliżeniowej. Technologie biometryczne także nie są odporne na ten rodzaj ataków, jednak w przypadku „przejęcia" osobniczych cech użytkownika, nie ma możliwości ich unieważnienia. W 2016 roku urządzenia umożliwiające nielegalne pozyskiwanie odcisków palców były już dostępne, zaś urządzenia do pobierania danych z systemów wykorzysujących naczynia krwionośne dłoni i analizujących tęczówkę oka – w fazie opracowywania (Kaspersky, 2016).

Podsumowanie

Tradycyjne metody uwierzytelniania są coraz mniej wystarczającym zabezpieczeniem. Użytkownicy systemów, mimo świadomości realnych zagrożeń, nierzadko używają słabych, łatwych do zapamiętania (i złamania) haseł, a popełnianie błędów logowania może zniechęcać do realizacji usług drogą elektroniczną. Powszechne zastosowanie wygodnych, coraz tańszych i bardziej niezawodnych biometrycznych technik identyfikacji może ten problem rozwiązać. Ich stosowanie, niezwykle ważne w aspekcie szeroko rozumianego bezpieczeństwa, budzi jednak wiele zastrzeżeń, m.in. ze względu na ograniczanie prywatności i obawy o odpowiedni nadzór nad wykorzystywaniem gromadzonych danych, dlatego jest wielu przeciwników wdrażania ich na szeroką skalę.

Mimo licznych wątpliwości, technologie biometryczne są intensywnie rozwijane, zakres ich użyteczności zwiększa się, a liczba banków oferujących poświadczanie tożsamości z ich wykorzystaniem rośnie.

Bibliografia

Automatyka (2013). Pobrane z: automatykabankowa.pl/biometria-w-bankomatach-coraz-bardziej-popularna-na-swiecie-ale-2/ (10.09.2017).

Automatyka (2015). Pobrane z: automatykabankowa.pl/w-bankowosci-biometria-rosnie-w-sile/ (20.11.2017).

Bień-Chudarek, S. (2016). Pobrane z: gomobi.pl/blogi/technologia-biometrii-i-inne-nowosci-na-rynku-platnosci-mobilnych/ (15.06.2017).

Boczoń, W. (2017). *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?* Pobrane z: bankier.pl/wiadomość/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html (15.11.2017).

Business (2017). Pobrane z: businessinsider.com.pl/technologie/nowe-technologie/voicepin-zabezpieczenia-biometryczne-thing-big-upc/l20w4f3 (15.10.2017).

Kaspersky (2016). Pobrane z: kaspersky.pl/o-nas/informacje-prasowe/2671/oamanie-zabezpieczen-biometrycznych-kaspersky-lab-bada-zagrozenia-dla-bankomatow-ktore-pojawia-sie-w-nieodleglej-przyszlosci (10.11.2017).

Kubanek, M. (2013). *Wybrane metody i systemy biometryczne bazujące na ukrytych Modelach Markowa*. Warszawa: Akademicka Oficyna Wydawnicza EXIT.

Niebezpiecznik (2015). Pobrane z: niebezpiecznik.pl/post/powazna-dziura-w-androidzie-umozliwia-wykradanie-odciskow-palcow/ (15.09.2017).

Nosowski, M. (2017). *Biometria a bezpieczeństwo*. Pobrane z: alfatronik.com.pl/info/biometria-a-bezpieczenstwo (12.09.2017).

Plucińska, M., Wójtowicz, J. (2014). *Analiza technik biometrycznych do uwierzytelniania osób.* Pobrane z: imm.org.pl/imm/plik/pliki-do-pobrania-plucinska42014_nn292.pdf (15.11.2017).

Westlake, A. (2015). *China debuts world's first ATM with facial recognition tech*. Pobrane z: slashgear.com/china-debuts-worlds-first-atm-with-facial-recognition-tech-01386122/ (15.09.2017).

Wolna (2014). *Technologia biometryczna w smartfonach: nowy kierunek*. Pobrane z: wolna-polska.pl/wiadomosci/ technologia-biometryczna-w-smartfonach-nowy-kierunek-2014-03 (9.09.2017).

BIOMETRIC AUTHENTIC TECHNIQUES FOR THE IMPLEMENTATION OF E-SERVICES

Keywords: biometric, authorization, e-services security

Summary. The implementation of e-services requires fast and convenient identification, authorization and verification of users. There are three basic types of identity verification methods: knowledge-based methods, methods that use material identifiers, and biometric mechanisms. Biometric authentication techniques have been intensively developed in recent years. Their advantage is the convenience of using it with high efficiency. For several years, they have been used, among others in banking, and they will also be implemented in administration and the broadly understood economy.

Translated by Teresa Mendyk-Krajewska

Cytowanie

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.