**mgr Julita Mlaskawa**
**Wyższa Szkoła Biznesu w Dąbrowie Górniczej**

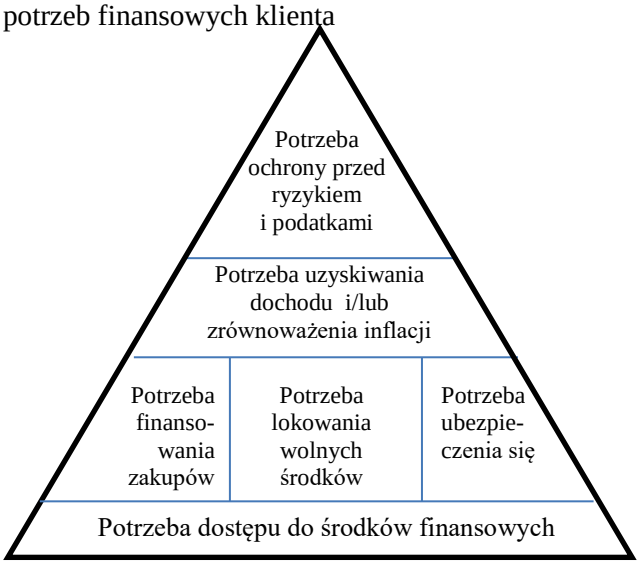
https://doi.org/10.26366/PTE.ZG.2015.32

# Biometria w bankowości - szanse i zagrożenia Banku przyszłości

## 1. Wstęp

Szybki rozwój nowoczesnych technologii wywiera coraz większe piętno na codziennym życiu współczesnych społeczności. Informacja jest dobrem powszechnie dostępnym, szybko dystrybuowanym za pośrednictwem kanałów elektronicznych oraz innych mass mediów. Pogoń za informacją i nowinkami technologicznymi nieustannie przyspiesza tempo życia człowieka. Czas staje się cennym zasobem, wartością wymierną wysoce pożądaną przez zabieganego konsumenta, który coraz częściej jest skłonny zrezygnować z poszukiwania miejsc i sposobów tańszych zakupów, na rzecz pozyskania dodatkowego czasu (Gawlik 2014, s. 24). Istotną wartością z punktu widzenia klienta jest uproszczenie przeprowadzanych transakcji handlowych, szczególnie w obszarach związanych z bankowością, z zarządzaniem finansami oraz wzrost poziomu bezpieczeństwa realizowanych transakcji bankowych. Hasła generowane przez systemy bankowe są skomplikowane i trudne do zapamiętania, co jest bezpośrednią przyczyną zapisywania i przechowywania tajnych danych w miejscach łatwo dostępnych, przykładowo w podręcznym notesie, telefonie lub po prostu w portfelu klienta. Niewłaściwe zabezpieczenie kodów bankowych może prowadzić do nieuprawnionego przejęcia informacji przez osoby niepożądane, a w konsekwencji do utraty środków pieniężnych lub oszczędności klienta. Współczesny konsument poszukuje rozwiązań prostych i intuicyjnych, umożliwiających wygodnie i bezpiecznie korzystanie z ogólnie dostępnych usług bankowych. Zgodnie z klasyfikacją przedstawioną przez S.Smyczka, potrzeba dostępu do środków finansowych stanowi podstawę piramidy potrzeb finansowych klienta (Rysunek 1.). Dopiero po zapewnieniu zadawalającego poziomu usługi podstawowej, klient będzie skłonny rozmawiać o usługach wyższego rzędu, związanych z finansowaniem zakupów, z lokowaniem wolnych środków finansowych lub z ubezpieczaniem swojego zdrowia i majątku (Smyczek 2007, s. 49).

**Rysunek 1.** Hierarchia potrzeb finansowych klienta




Źródło: Smyczek 2007, s.49.

Rozwiązaniem pozwalającym osiągnąć wymierny wzrost satysfakcji klienta związany z możliwością pozyskania deficytowego dobra jakim jest oszczędność czasu klienta, jak również z zwiększeniem poziomu bezpieczeństwa realizowanych transakcji bankowych jest zastosowanie innowacyjnych systemów biometrycznej weryfikacji tożsamości klienta.

## 2. Pojęcie i znaczenie biometrii

Termin „biometria" pochodzi od greckich słów *bios*–„życie" oraz *metron* – „pomiar". W ujęciu naukowym stosowany jest do określenia nauki zajmującej się mierzalnymi cechami biologicznymi człowieka (Marucha-Jaworska 2015, s. 169). Wykorzystanie cech biometrycznych w bankowości nie jest zjawiskiem nowym, nowością są metody pobierania i analizy danych biometrycznych. Dane biometryczne w bankowości mogą zastać wykorzystane między innymi do identyfikacji i uwierzytelnienia klienta, autoryzacji dostępu do wydzielonych pomieszczeń i skrytek depozytowych, lub rejestracji pracowników banku.

Weryfikacja tożsamości klienta może zostać przeprowadzona w oparciu o:

- mienie, czyli przedmioty fizyczne posiadane przez daną osobę (klucze, paszporty, inteligentne karty),
- wiedzę, czyli tajne informacje pozostające w wyłącznym posiadaniu danej osoby (hasła, kody, pin do karty),
- biometrię opisującą fizjologiczne i behawioralne cechy wyróżniające daną osobę na tle grupy (Bolle 2008, s.4-5).

Wskazane formy uwierzytelnienia mogą funkcjonować samodzielnie, lub w dowolnych kombinacjach. W bankowości stosuje się łączenie przynajmniej dwóch różnych form uwierzytelnienia, przykładowo wypłata gotówki z bankomatu wymaga, ażeby mienie w postaci karty płatniczej zostało potwierdzone wiedzą, w postaci unikalnego numeru PIN.

Mienie i wiedza mogą zostać skradzione a następnie skopiowane. Biometria jest niepowtarzalna i przynależy wyłącznie do wskazanej osoby, dodatkowo z technologicznego punktu widzenia, utworzenie atrapy umożliwiającej oszukanie czytnika biometrycznego, jest bardzo trudne a czasami wręcz niemożliwe (Marucha-Jaworska 2015, 179). Wdrożenie biometrii w procedurach bankowych jest możliwe jedynie w przypadku, gdy badana cecha spełnia łącznie pięć podstawowych warunków (Tabela 1.).

**Tabela 1.** Cechy biometrii w procedurach bankowych

| **Cecha** | **Identyfikacja cechy** |
|---|---|
| Uniwersalność | Każdy klient banku powinien posiadać daną cechę |
| Jednoznaczność | Dana biometryka powinna być niepowtarzalna i specyficzna dla każdego klienta |
| Trwałość | Jest to cecha, która powinna być stała w czasie |
| Ściągalność | Cecha powinna posiadać możliwość zmierzenia za pomocą dostępnych urządzeń pomiarowych |
| Akceptowalność | Sposób pomiaru cechy jest powszechnie akceptowalny w grupie klientów |

Źródło: opracowanie własne na podstawie Bolle 2008,s.4-6.

Biometria może dotyczyć pomiaru parametrów statycznych możliwych do odczytania w danej chwili lub charakterystyk behawioralnych mówiących o tym, w jaki sposób dana czynność jest wykonywana. Pomiar statyczny realizowany jest dla cech fizjologicznych zawartych w biometrykach odnoszących się do weryfikacji:

- odcisku palca,
- wzoru naczyń krwionośnych w palcu i dłoni
- obrazu twarzy,
- geometrii dłoni,
- obrazu tęczówki oka,
- siatkówki oka,
- DNA,
- kształtu ucha,

- zapachu,
- termogramu,
- połysku skóry.

Biometria behawioralna stosowana jest w przypadku rejestracji i analizy czynności określających:

- sposób wykonywania podpisu własnoręcznego,
- tempo pisania,
- sposób pisania na klawiaturze,
- ruch myszką,
- głos,
- ruch ust,
- sposób chodzenia,
- sposób reakcji mózgu (fala p300) (Marucha-Jaworska 2015, s.169-170).

Przed wyborem optymalnej metody biometrycznej należy określić usługę, w ramach której będzie stosowane projektowane rozwiązanie. Istotną kwestią jest także koszt czytnika biometrycznego oraz jego połączenia z urządzeniami pozostającymi w posiadaniu banku.

## 3. Charakterystyka wybranych metod biometrycznych

Najbardziej intuicyjną i powszechnie stosowaną biometryką jest wizerunek twarzy rozmówcy. W trakcie wizyty klienta w oddziale banku, przed rozpoczęciem czynności operacyjnych doradca weryfikuje zgodność twarzy interesanta z wzorem wizerunku zamieszczonym na przedkładanym dokumencie tożsamości. Metoda wizualnej oceny zgodności porównywanych obrazów jest subiektywna i uzależniona od poziomu zmęczenia osoby sprawdzającej tożsamość. Zastosowanie elektronicznego systemu analizy wizerunku klienta zwiększa wiarygodności i dokładności metody. Rejestrowanie obrazu twarzy jest czynnością dyskretną (Bolle 2008, s.162), dzięki czemu może być realizowane bezpośrednio przy stanowisku obsługi, lub w formie ogólnego zapisu pobieranego przez zintegrowany system kamer monitorujących grupę osób przebywających na terenie banku w danym momencie.

Biometria twarzy może być stosowana do realizacji procedury przesiewania, polegającej na przeszukiwaniu określonych baz pod względem występowania analizowanego wizerunku. Funkcjonalność przesiewania w przyszłości może zostać wykorzystana do szybkiej identyfikacji osób zaginionych i poszukiwanych (Marucha-

Jaworska 2015, s.176). Proponowane rozwiązanie wymaga dużych zmian informatycznych i proceduralnych w bankach oraz w instytucjach bezpośrednio powiązanych z organami ścigania. Ważną kwestią decydującą o skuteczności metody może okazać się konieczność utajnienia samego faktu jej stosowania.

Praktyczne stosowanie systemów bazujących na biometrii twarzy wymaga zapewnienia analogicznych warunków pobierania próbki obrazu (Bolle 2008, s.163). Procedura analizy wizerunku klienta może zostać uszczelniona weryfikacją biometrii określającej kształt i krawędzie ucha klienta (Bolle 2008, s.63).

Systemy umożliwiające weryfikacje głosu klienta dedykowane są w szczególności dla tworzenia procedur powiązanych z bankowością telefoniczną i internetową. Zastosowanie biometrii głosowej poprawia komfort i bezpieczeństwo telefonicznej obsługi klienta, dodatkowo minimalizuje ryzyko nieuprawnionego przekazania lub kradzieży tajnych kodów bankowych. Weryfikacja dźwiękowa w zależności od wyboru metody badania może być realizowana w oparciu o:

- systemy zależne od stałej i powtarzalnej treści hasła,
- systemy badania niezależnego od wypowiadanej treści, pozwalające na uwierzytelnienie głosu klienta w trakcie standardowej rozmowy telefonicznej,
- systemy konwersacyjne, oparte na metodach częściowo zależnych od treści.

Najpewniejszą metodą badania głosu klienta jest zastosowanie systemu badania niezależnego od wypowiadanej treści, ograniczającego ryzyko związane z próbami odtworzenia gotowych nagrań głosu klienta (Woszczyński 2013, s.14). Zagrożeniem powszechnego stosowania biometrii głosowej, jest możliwość tworzenia fałszywych tożsamości poprzez rejestrację wzorca głosu pochodzącego z syntezatora mowy. Barierą ograniczającą zakres stosowania metody, są kwestie techniczne związane z jakością połączeń telefonicznych oraz z zakłóceniami, które mogą wystąpić w trakcie połączenia. Produkcyjne wdrożenie elektronicznych systemów rozpoznawania głosu klienta, wymaga opracowania dodatkowych form uwierzytelnienia, dla osób, które na skutek urazu, choroby lub innego niespodziewanego zdarzenia chwilowo utraciły głos (Bolle 2008, s.164).

Jednym z deskryptorów elektronicznej analizy głosu jest ocena stanu emocjonalnego osoby mówiącej (Ślot 2010, s.15-16) Funkcjonalność umożliwiająca określenie emocji klienta, w przyszłości może posłużyć do identyfikacji klientów zdenerwowanych, mogących mieć złe intencje względem banku(oszustwo, wyłudzenie,

napad) oraz osób zastraszonych, pozostających pod presją osób postronnych (wczesne rozpoznawanie oszustwa na „wnuczka"). Wykrycie emocji powiązanych ze strachem powinno skutkować, uruchomieniem szczególnie drobiazgowej weryfikacji tożsamości klienta i sytuacji, w jakiej klient znajduje się w danym momencie. Jeżeli klientem jest osoba starsza, to warto zapytać, w jakim celu wypłacane są pieniądze, i czy klientowi towarzyszy ktoś bliski z rodziny. Wzmocnienie procedur dla tego typu klienta może zwiększyć wykrywalność prób wyłudzenia pieniędzy od osób samotnych i starszych zwanych potocznie oszustwem na wnuczka. W przypadku identyfikacji klienta zdenerwowanego, wskazane jest wdrożenie procedury indywidualnej obsługi w specjalnie wydzielonym pomieszczeniu, pozostającym pod stałym monitoringiem ochrony. Zdenerwowanie klienta może bowiem wynikać z przyczyn prozaicznych dotyczących niezadowolenia ze współpracy z bankiem, lecz może wynikać ze stresu związanego z zaplanowanym napadem, kradzieżą lub oszustwem. Jako czynnik łagodzący zdenerwowanie klienta warto rozważyć możliwość okresowej aromatyzacji pomieszczenia, specjalnie dobranym zapachem wpływającym pozytywnie na uspokojenie i wyciszenie negatywnych emocji interesanta (Skowronek 2011, s.9).

Podstawową metodą autoryzacji większości transakcji bankowych jest złożenie odręcznego podpisu klienta na papierowym dokumencie. Powstająca w ten sposób papierowa dokumentacja jest rejestrowana, skanowana a następnie przekazywana do archiwizacji, co generuje zbędne koszty i dodatkową pracochłonność po stronie banku. Fizyczny obieg dokumentu papierowego można zastąpić wirtualnym obiegiem dokumentu elektronicznego, zatwierdzanego odręcznym podpisem klienta, składanym na specjalnym urządzeniu typu „tablet". Weryfikacja zgodności podpisu z wzorem zdeponowanym w bazach bankowych może być realizowana w formie:

- analizy *off-line* polegającej na cyfrowej analizie podpisów już istniejących na dokumencie papierowym lub elektronicznym,
- analiza *on-line*, dotyczącej weryfikacji podpisu składanego przy użyciu urządzenia dostarczającego na bieżąco informacji na temat cech dynamicznych dotyczących nacisku, położenia pióra, czasu i płynność wykonywania podpisu.

Poziom błędów dla systemów *on-line* zawierają się w 2% podczas gdy dla systemów *off-line* są nawet dziesięciokrotnie większe (Marucha-Jaworska 2015, s.186). Wymierną korzyścią stosowania systemu *on-line* są oszczędności związane z wyeliminowaniem dokumentu papierowego oraz natychmiastowa dostępność dokumentu dla szerokiego grona użytkowników. Wadą biometrii podpisu odręcznego jest podatność na zmiany

wynikające zestarzenia się, przebytych chorób, lub emocji, które mogą powodować odrzucenie pobranych danych przez system pomiarowy.

Kolejnym kuszącym rozwiązaniem jest zastosowanie biometrii odcisku palca pobieranej przy użyciu specjalistycznych skanerów. Jakość pozyskanego materiału zależy od sposobu przyłożenia i siły nacisku palca na urządzenie pomiarowe. Wiek, urazy, lub zużycie skóry palców mogą być przyczyną dużego współczynnika błędnych odrzuceń. Obawy klienta mogą budzić względy higieniczne związane z wielokrotnym używaniem tego samego urządzenia przez różne osoby. Przykładowo, pierwszym kwartale 2015 roku zrealizowano 173,45 milionów wypłat z 20 936 bankomatów, co jest równoznaczne z tym, że z jednego bankomatu w ciągu dnia mogło średnio korzystać 92 osoby (*Raport bankowość* .... 2015, s.24). Czystość wielokrotnie dotykanego urządzenia mogłaby budzić zastrzeżenia, dyskusyjna byłaby także wiarygodność pobieranych danych biometrycznych (Bolle 2008, s.162). Zagrożeniem stosowania metody jest możliwość kopiowania i odtworzenia gumowej atrapy palca, która może zostać wykorzystana do nieuprawnionej autoryzacji transakcji bankomatowych (Bolle 2008, s.241). Wydajność badania odcisku palca może zostać wzmocniona badaniem połysku skóry klienta (Bolle 2008, s.64).

Biometria odcisku palca, podobnie jak biometria wizerunku twarzy jest metodą umożliwiającą realizację procedury przesiewania pozyskiwanych danych pod względem identyfikacji osób poszukiwanych przez organy ścigania.

Technologicznym rozwinięciem metody badania odcisku linii papilarnych jest biometria naczyń krwionośnych palca (z ang. *Finger Vein*). Wzór naczyń krwionośnych pobierany jest w sposób nie inwazyjny poprzez naświetlenie palca światłem bliskim podczerwieni, stosowanym na co dzień w medycynie. Metoda jest coraz częściej stosowana w bankomatach i w stacjonarnych oddziałach bankowych. Pionierami rozwiązania na polskim rynku finansowym były Banki Spółdzielcze. W marcu 2010 roku Bank Polskiej Spółdzielczości S.A. uruchomił pierwszy bankomat biometryczny w Polsce wykorzystujący metodę *Finger Vein*.

Biometria układu naczyń krwionośnych palca znajduje szerokie zastosowanie w pozostałych obszarach usług bankowych dotyczących w szczególności:

- obsługi klienta w oddziałach stacjonarnych,
- podpisu biometrycznego,
- kiosków informacyjnych i wirtualnych oddziałów bankowych,

- obszaru bankowości elektronicznej,
- terminali płatniczych,
- kontroli dostępu do wydzielonych pomieszczeń i skrytek depozytowych,
- bezpieczeństwa systemów IT (*Hitachi, Bankowość Biometryczna 2015*).

Zaletami stosowania technologii *Finger Vein* są przede wszystkim:

- wygoda dla użytkownika,
- wysoka akceptowalność społeczna,
- oszczędności banku związane z brakiem konieczności wydawania kart dla klientów oraz z redukcją obiegu papierowego dokumentu,
- ochrona prywatności użytkowników,
- bezpieczeństwo dla zdrowia klienta (Woszczyński 2013, s.13).

Biometryczna analiza wybranych cech organizmu ludzkiego, może dostarczyć cennych informacji na temat stanu zdrowia klienta. Badanie tęczówki jest najdokładniejszą biometryką charakteryzującą się bardzo małą liczbą niesłusznych akceptacji. Pobieranie obrazu tęczówki jest nieco kłopotliwe dla osób noszących okulary lub soczewki, ponieważ mogą one zostać poproszone zdjęcie okularów na czas pobierania próbki danych (Bolle 2008, s.164-165). Biometria tęczówki stosowana jest w celu uwierzytelnienia dostępu do wydzielonych pomieszczeń banku lub do skrytek depozytowych. Z medycznego punktu widzenia obraz tęczówki stanowi zbiór informacji umożliwiających irydologowi (specjalista zajmujący się badaniem tęczówki) ocenę aktualnego stanu zdrowia badanej osoby, określenie predyspozycji do niektórych chorób, zawartości toksyn w organizmie, rozpoznanie śladów przebytych chorób oraz prognoz na temat przyszłych zagrożeń zdrowotnych. Proponowane rozwiązanie wymaga nawiązania ścisłej współpracy pomiędzy bankami i placówkami medycznymi oraz wypracowania szczelnych przepisów i technologii, chroniących dane wrażliwe dotyczące stanu zdrowia klienta (Majewska, 2015). Istotnym ryzykiem związanym z pobieraniem i przesyłaniem danych dotyczących stanu zdrowotnego klienta, jest ryzyko przejęcia przez osoby lub instytucje niepożądane, które mogą wykorzystywać skradzione dane w celach handlowych a czasami nawet przestępczych. System wczesnej diagnostyki medycznej powinien zostać skonstruowany w taki sposób, ażeby dane biometryczne były szyfrowane zgodnie z kluczem pozostającym w wyłącznym posiadaniu współpracujących z bankiem jednostek medycznych.

Biometria dotycząca zapachu klienta może zostać w przyszłości wykorzystana do wczesnej diagnostyki raka płuc. Pobieranie zapachu do analizy mogłoby się odbywać stacjonarnie na stanowiskach obsługi w Oddziałach Banku lub na odległość z pomocą komputera. Zgodnie z informacją zamieszczoną w publikacji B. Hultena (s.64-65), trwają badania nad opracowaniem elektronicznego nosa, który umożliwi wykrywanie subtelnego zapachu charakterystycznego dla wczesnego stadium raka płuc. Połączenie usług bankowych z wczesną diagnostyką medyczną może okazać się rozwiązaniem zaskakująco praktycznym, zarówno z punktu widzenia klienta jak i placówek medycznych zajmujących się wczesna diagnostyką chorób płuc.

## 4. Podsumowanie i wnioski

Biometria jest innowacyjnym rozwiązaniem doskonale korespondującym z technologicznym rozwojem usług bankowych. W dobie chaosu informacyjnego bardzo ważne jest zabezpieczanie danych i informacji, które powinny pozostawać w wyłącznym posiadaniu klienta. Niestety zabezpieczenia, które zostały opracowane przez człowieka, mogą zostać przez niego złamane. Dane biometryczne zostały wytworzone w drodze ewolucji przez naturę, dzięki czemu stanowią jedyny w swoim rodzaju kod biologiczny przyporządkowany wyłącznie do danego człowieka. Współczesne technologie stale zmniejszają koszt wytworzenia i późniejszej eksploatacji czytników biometrycznych, dzięki czemu coraz częściej można odnaleźć przykłady ich stosowanie w bieżącej obsłudze klienta bankowego. Dane biometryczne zawierają ogromny potencjał informacji, które w przyszłości mogą zostać wykorzystane do budowania nietypowych połączeń pomiędzy branżami, których połączenie może zaskoczyć efektem synergii, przykładowo w przypadku łączenia usług bankowych z usługami wstępnej diagnostyki zdrowia klienta lub z kartotekami policyjnymi. Zaletą stosowania biometrycznych systemów uwierzytelnienia jest znaczne skrócenie czasu obsługi klienta przy równoczesnym zwiększeniu poziomu bezpieczeństwa realizowanych transakcji bankowych. Biometria umożliwia wyeliminowanie fizycznego obiegu dokumentacji co jest zjawiskiem wysoce pożądanym zarówno z ekologicznego punktu widzenia jak również w perspektywie uzyskania dodatkowych oszczędności dla banków.

Stosowanie nowoczesnych technologii biometrycznych jest inwestycją długoterminową związaną z koniecznością doposażenia wszystkich urządzeń bankowych dedykowanych do modyfikowanej usługi. Ciągły rozwój nowoczesnych

technologii skutkuje coraz mniejszą długością życia nowinek technologicznych. Innowacyjne na chwilę obecną, metody biometryczne za kilka lat mogą okazać się przestarzałe i niepraktyczne. Dlatego przy planowaniu wdrożenia wybranej biometrii należy brać pod uwagę, niezbyt wysoki kosz urządzenia pomiarowego oraz możliwość jego wymiany na aktualizowane wersje urządzenia w przyszłości. Dużym ryzykiem stosowania biometrii w bankowości, jest możliwość kradzieży elektronicznych baz danych zawierających biometryczne kartoteki klientów, stanowiących indywidualny miernik biologicznych cech ludzkich i w niepowołanych rękach mogą stanowić duże zagrożenie dla banku i klienta.

Pomimo ryzyka związanego z krótkim cyklem życia nowości technologicznych, oraz z ryzykiem kradzieży danych biometrycznych, elektroniczne systemy analizy biometrii ciała ludzkiego, są przełomową technologią stanowiącą szansę na dynamiczny rozwój nowoczesnych i bezpiecznych technologii determinujących kierunek zmian w sektorze bankowym. Biometria może stanowić pomost łączący różne, pozornie rozbieżne branże i dyscypliny naukowe. Przyszłość należy do biometrii, a to jak szybko i w jakich obszarach będzie wykorzystywana zależy wyłącznie od instytucji finansowej, która zdecyduje się na zastosowanie innowacyjnego rozwiązania w bankowości.

## Literatura


1. *Bankowość biometryczna*, dostęp: http://www.hitachi.pl/veinid/biometric_banking.html - aktywna na dzień 07.07.2015.
2. Bolle R.M., Connell J.H., Pankanti S., Ratha N. K., Senior A.W.(2008), *Biometria*, Wydawnictwa Naukowo – Techniczne, Warszawa.
3. Gawlik K., Kocianowski M., Wódkowski A. (2014), *Nowe nurty konsumenckie*, Harvard Business Review Polska, Październik.
4. Hulten B., Broweus N., M. van Dijk (2011), *Marketing sensoryczny*, Polskie Wydawnictwo Ekonomiczne, Warszawa.
5. Majewska M. *Irydologia - jakie choroby można wyczytać z oczu*?, dostęp: http://www.poradnikzdrowie.pl/sprawdz-sie/badania/irydologia-jakie-choroby-mozna-wyczytac-z-oczu_33493.html - aktywna na dzień 07.07.2015.
6. Marucha-Jaworska M. (2015), *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Wolters Kluwer, Warszawa.
7. *Raport bankowość internetowa i płatności bezgotówkowe* (I kwartał 2015), dostęp: http://zbp.pl/public/repozytorium/wydarzenia/images/czerwiec_2015/konferencja/Netbank_Q1_2015v4.pdf. - aktywna na dzień 07.07.2015.
8. Skowronek I. (2011), *Oddziaływanie zapachem jako forma marketingu sensorycznego*, „Marketing i Rynek", nr 1.
9. Smyczek S. (2007), *Modele zachowań konsumentów na rynku usług finansowych*, Wydawnictwo Akademii Ekonomicznej im. Karola Adamieckiego w Katowicach, Katowice.

10. Ślot K. (2010), *Rozpoznawanie biometryczne. Nowe metody ilościowej reprezentacji obiektów*, Wydawnictwa Komunikacji i Łączności, Warszawa.
11. Woszczyński T. (2013), *Raport biometryczny 2.0, Bankowość biometryczna*, Grupa FTB ds. Biometrii, Warszawa, dostęp: http://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Raport_Biometryczny_2.0_strona_FTB.pdf - aktywna na dzień 07.07.2015.

**Streszczenie**

**Biometria w bankowości - szanse i zagrożenia Banku przyszłości**

Biometria jest naturalnym znacznikiem tożsamości każdego człowieka, dzięki czemu coraz częściej jest wykorzystywana jako klucz dostępu do wydzielonych pomieszczeń, oraz systemów informatycznych. Zastosowanie metod biometrycznych w bankowości dotyczy w szczególności identyfikacji i weryfikacji klienta. Nowoczesne technologie umożliwiają wykorzystanie metody w obszarze bankowości stacjonarnej jak również w bankowości telefonicznej i internetowej. Ciało ludzkie posiada określony zbiór indywidualnych cech biologicznych na podstawie, których można przeprowadzić wstępną analizę zdrowia klienta lub rozpoznawać osoby poszukiwane i zaginione. Synergia usług bankowych z wczesną diagnostyką medyczną i ogólnie pojmowanym bezpieczeństwem, stanowi wyzwanie dla naukowców i praktyków. Podstawową korzyścią przemawiającą za wprowadzeniem biometrii w bankowości jest zwiększenie bezpieczeństwa transakcji bankowych, oraz wyeliminowanie fizycznego obiegu papierowych dokumentów wewnątrz organizacji.

**Słowa klucze**: biometria, bank, identyfikacja klienta, uwierzytelnienie klienta, bezpieczeństwo.

**Abstract**

**Biometrics in banking - opportunities and threats of the Bank of the future**

Biometrics is a natural marker of identity of every human being; thanks to this it is more and more often used as an access key to designated IT spaces and systems. The use of biometrics methods in banking concerns, in particular, customer identification and verification. Modern technologies enable the use of the method in the area of stationary banking, as well as in telephone and online banking. The human body has a specific set of individual biological characteristics based on which one may conduct a preliminary analysis of the client's health or identify lost or wanted persons. The synergy of banking services with early medical diagnostics and generally understood security is a challenge for researchers and practitioners. The main advantage in favour of the introduction of biometrics in banking is the increase of safety of bank transactions and eliminating the physical circulation of paper documents within the organisation.

**Key words:** biometrics, bank, customer identification, customer authentication, security.