Nr 3(72) 2018

ISSN 2544-7068

BEZPIECZNY BANK

BANKOWY FUNDUSZ GWARANCYJNY

Nr 3(72) 2018

ISSN 2544-7068

BEZPIECZNY BANK

BFG
BANKOWY
FUNDUSZ
GWARANCYJNY

BEZPIECZNY BANK jest czasopismem wydawanym przez Bankowy Fundusz Gwarancyjny od 1997 roku, poświęconym zagadnieniom stabilności systemu finansowego, ze szczególnym uwzględnieniem systemu bankowego.

Artykuły publikowane w BEZPIECZNYM BANKU są recenzowane.
Za publikację naukową w BEZPIECZNYM BANKU Minister Nauki i Szkolnictwa Wyższego przyznał trzynaście punktów.
BEZPIECZNY BANK (online) ISSN 2544-7068
Wcześniejsze wydania BEZPIECZNEGO BANKU miały numer ISSN 1429-2939

REDAKCJA

Krystyna Kawerska

WYDAWCA

Bankowy Fundusz Gwarancyjny
ul. Ks. Ignacego Jana Skorupki 4
00-546 Warszawa

SEKRETARIAT REDAKCJI

Ewa Teleżyńska
Telefon: 22 583 08 78
e-mail: ewa.telezynska@bfg.pl

Informacje dotyczące wymogów formalnych i edytorskich dla autorów publikacji znajdują się na stronie: **www.bfg.pl**

DOI: 10.26354/bb.8.3.72.2018

Miscellanea

Szymon Cegiełko*

Kultura użytkowa zabezpieczeń biometrycznych klientów banków w Polsce na podstawie sondażu internetowego**

Streszczenie

Artykuł podejmuje tematykę związaną z zabezpieczeniami biometrycznymi oraz ich wykorzystaniem przez klientów instytucji finansowych. Jego celem jest zapoznanie Czytelnika z wynikami przeprowadzonego badania sondażowego (zrealizowanego metodą CAWI na próbie 505 osób). Przedstawione w publikacji rozważania podkreślają, że społeczeństwo polskie jest świadome przestępstw elektronicznych, natomiast zautomatyzowane zabezpieczenia oparte na biometrykach, zwiększające poziom bezpieczeństwa, mogą być przyszłością dla wielu organizacji – także finansowych. Badanie przedstawia wzrost popularności w użytkowaniu biometryk oraz eksponuje charakterystykę zachowań przeciętnego użytkownika usług bankowych w XXI w. Artykuł opisuje również aspekty prawne zabezpieczeń biometrycznych oraz, na podstawie wyników ankietowych, wskazuje kierunek rozwoju dla instytucji finansowych.

Słowa kluczowe: bankowość, bezpieczeństwo, biometria, zabezpieczenia biometryczne

* Absolwent Uniwersytetu Łódzkiego.

** Opracowanie jest fragmentem pracy dyplomowej napisanej pod kierunkiem naukowym prof. Moniki Marcinkowskiej.

The Usable Culture of Biometric Security of Banks Clients in Poland

Abstract

The article deals with the issues related to biometric security and their use in the financial institutions. Its purpose is to present and evaluate contemporarily used biometrics and depict conclusions got from the study exploring the usable culture of biometric security. The considerations presented in this article show that society is aware of electronic crimes, and that the automated security systems based on biometrics that increase the level of security, may be the future for many organizations – including the financial ones. The article presents the increase in popularity in the use of biometrics and exposes the behavior of the average user of banking services in the 21st century. The article also describes the legal aspects of biometric security and, basing on the survey results, indicates the direction of development for financial institutions.

Key words: banking, security, biometrics, biometric security

Wstęp

Rozwój gospodarek wolnorynkowych pozytywnie wpływa nie tylko na poszerzanie wiedzy społeczeństwa, lecz i na rozwój technologiczny niemal wszystkich aspektów życia człowieka. Ekspansja nowoczesnych technologii ułatwiających funkcjonowanie we współczesnym świecie dotarła także do środowiska bankowego, gdzie trafiła na bardzo podatny grunt w zakresie udoskonalania standardów obsługi klienta i wychodzenia naprzeciw jego nieprzerwanie zmieniających się potrzeb. Jednocześnie pozwoliła instytucjom finansowym na podniesienie jakości świadczonych usług oraz stworzenie nowego źródła dochodów. Obecnie w społeczeństwie zauważalny jest trend wzrastającej szybkości obsługi klienta, także jej dostępności – tak, by można było skorzystać z usługi w każdym miejscu i o każdej porze.

W grudniu 1994 roku niewielki bank kalifornijski LA Jolla Bank FSB umożliwił swoim klientom dokonywanie transakcji przez Internet[1]. Narodziła się bankowość elektroniczna – odpowiedź na potrzeby ludzi, umożliwiająca obsługę konta bankowego bez wychodzenia z domu oraz na łatwy i szybki kontakt z instytucją finansową. Niestety, razem z przeniesieniem bankowości do Internetu, mimo – z punktu widzenia instytucji finansowej – ograniczeń kosztów związanych ze zmniejszeniem opłat za budynki oraz wykwalifikowane kadry, pojawiły się liczne problemy związane z bezpieczeństwem transakcji i zdeponowanymi w bankach środkami finansowymi. Podpis, login, hasło, kod PIN – okazały się zabezpieczeniami niewystarczającymi. Częste ataki hakerskie, nierozważne udostępnianie swoich danych osobowych oraz ujawnianie przez klientów banków PIN-ów wpłynęło na to, że bankowość elektroniczna przestała być tak bezpieczna, jak tego oczekiwano. Szukano sposobów zapewniających bezpieczeństwo transakcji klientów banków, i pojawił się pomysł wykorzystania w tym celu metod biometrycznych. Termin „biometria" pochodzi z greki. Powstał w wyniku złożenia dwóch słów – *bios* – oznaczającego

[1] M. Polasik, *Bankowość elektroniczna: istota – stan – perspektywy*, Wydawnictwo CeDeWu, Warszawa 2006, s. 38.

życie oraz *metron* – czyli pomiar. Początkowo odnosił się wyłącznie do wyznaczania właściwości istot żywych, bez wskazania celu i metodyki wykonywanego badania[2].

Współczesne osiągnięcia umożliwiły wykorzystanie wcześniejszych wyników analiz, uważanych przez długi czas za bezwartościowe. Okazało się, że dzięki nowoczesnym metodom możliwe jest zwiększenie bezpieczeństwa posiadacza tradycyjnych kart bankomatowych, łącząc je z odciskiem palca. Podjęte działania umożliwiły również podniesienie obniżonego wcześniej przez nierozwagę ludzi i ataki hakerskie bezpieczeństwa. Społeczeństwo natomiast zyskało kolejne udogodnienia – zbędne okazało się zapamiętywanie długich haseł oraz troska o to, by wpisywany PIN nie został przez nikogo zauważony. Nastąpiło udoskonalenie procesu identyfikacji podmiotu uprawnionego do korzystania z bankowości elektronicznej oraz powstały nowe zabezpieczenia zwiększające ochronę klientów i ich rachunków bankowych, zmniejszające przy tym liczbę pojawiających się ataków hakerskich.

Celem opracowania jest charakterystyka wyników badań kultury użytkowej zabezpieczeń biometrycznych przejawianej przez 505 klientów banków w Polsce.

1. Biometria – zagadnienia podstawowe

Nauka o zabezpieczeniach biometrycznych, kryptografii oraz biometrykach nie ma ugruntowanej definicji biometrii. Jest to pojęcie rozumiane przez naukowców w niejednolity sposób. W szeroko pojętej literaturze występuje wiele definicji koncentrujących się na różnych elementach tej kategorii. Zgodnie z definicją słownikową biometria to: „nauka zajmująca się badaniem prawidłowości kierujących zmiennością cech populacji organizmów żywych posługująca się metodami statystyki matematycznej”[3]. A jedną z najbardziej popularnych definicji biometrii podaje Ruud M. Bolle, który traktuje ją jako: „naukę zajmującą się identyfikowaniem lub weryfikacją tożsamości osoby na podstawie jej cech fizjologicznych lub behawioralnych”[4]. Termin biometria jest też często utożsamiany z techniką wykonywania pomiarów wszelkich istot żywych. Rezultaty owych badań mogą znajdować swoje zastosowanie w nowoczesnych technologiach[5]. Zaś w ujęciu społecznym – według M. Maruchy-Jaworskiej: „biometria to nauka zajmująca się mierzalnymi cechami biologicznymi człowieka”[6].

[2] R.W. Kaszubski, *Społeczne i prawne aspekty biometrii. Człowiek i dokument*, Forum Technologii Bankowych, 2011, podaję za: M. Marucha-Jaworska, *Podpisy elektroniczne, biometria, identyfikacja elektroniczna*, Wydawnictwo Wolters Kluwer, Warszawa 2015, s. 169.

[3] J. Bralczyk (red.), *Słownik 100 tysięcy potrzebnych słów*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 57.

[4] M. Ruud Bolle, J.H. Connel, S. Pankanti, *Biometria*, Wydawnictwo Naukowo-Techniczne, Warszawa 2008, s. 4.

[5] W. Boczoń, *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?*, 13.09.2017, strona internetowa Bankier.pl, https://www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html (dostęp: 28.11.2017).

[6] R.W. Kaszubski, *Społeczne i prawne aspekty biometrii. Człowiek i dokument*, Forum Technologii Bankowych, Warszawa 2011, podaję za: M. Marucha-Jaworska, *Podpisy elektroniczne...*, *op. cit.*, s. 169.

Technologie biometryczne wykorzystują różnorodne metody, by potwierdzić tożsamość człowieka. Zastosowanie nowoczesnych technik umożliwia ograniczenie ryzyka związanego z oszustwami, zapewnia autoryzację osób uprawnionych do wykonywania określonych czynności, a także pomaga przy identyfikacji sprawców przestępstw[7]. MIT Technology Review określił biometrię jako: „jedną z najważniejszych [...] innowacji technologicznych, która zmieni świat" [8].

Biometria to dziedzina, która wciąż się rozwija. Udoskonalenia techniczne oraz wzrost rozumienia sposobów wykorzystania wyników badań wpłynęły na obserwowany w ostatnich latach jej rozkwit. Mnogość perspektyw rozwojowych ma istotny wpływ na definiowanie terminu biometrii. Większość naukowców eksponuje związek z dokonywaniem pomiarów na istotach żywych, które mają cechy pozwalające w łatwy sposób zidentyfikować tożsamość. Najpopularniejsze biometryki podzielić można na biometryki fizyczne (np. dłoń człowieka, odcisk palca, ukrwienie i kontury twarzy, naczynia krwionośne, siatkówka oraz tęczówka oka, kształt ucha, a także pomiar ciała) i behawioralne (np. głos, podpis)[9].

2. Wymogi prawne dotyczące zabezpieczeń biometrycznych w bankowości

Zabezpieczenia biometryczne wykorzystywane w sposób automatyczny w społeczeństwie są technikami nowymi, dlatego też ich użytkowanie nie zostało ściśle określone przez przepisy prawa. Każdy kolejny rok jednak może być przełomowy, wpływając przy tym na rozpowszechnianie biometryk i sytuację, w której ludzie będą korzystać wyłącznie z danych biometrycznych do płacenia lub chociażby potwierdzania tożsamości w relacjach z instytucjami finansowymi.

Kluczową kwestią w działalności banków jest zapewnienie bezpieczeństwa powierzonych środków i realizowanych transakcji. Problem identyfikacji użytkownika oraz autoryzacji transakcji, także z wykorzystaniem zabezpieczeń biometrycznych, jest ściśle związany z kwestiami odpowiedzialności za wykonywane operacje i czynności bankowe[10]. Ustawa o usługach płatniczych zobowiązuje banki do

[7] A. Bodnar, J. Michalski, *Dokument biometryczny a prawa człowieka*, http://www.prawaczlowieka.pl/precedens/images/stories/dokument_biometryczny_a_prawa_czowieka.pdf (dostęp: 05.12.2017).

[8] J. Pugliese, *Biometrics: bodies, technologies, biopolitics*, Routledge, Londyn 2010, s. 1.

[9] I. Kuchciak, *Bankowość biometryczna – nowe wyzwanie dla polskiego sektora bankowego*, „Annales Universitatis Mariae Curie-Skłodowska" 2011, Vol. XLV, 2, s. 226.
Więcej na temat biometryk znaleźć można w: T. Woszczyński (red.), *Biometria w bankowości – kluczowe aspekty*, Warszawa 2015, https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/bankowosc_elektroczniczna/FTB/biometria_raport_09_2015_A4_e_light.pdf; R.W. Kaszubski (red.), *Biometria w bankowości i administracji publicznej*, Forum Technologii Bankowych, Warszawa 2009, https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Forum_Technologii_Bankowych_-_Biometria_dla_bankowosci_i_administracji.pdf

[10] B. Bajor, *Bankowość elektroniczna. Studium prawne*, Wydawnictwo Naukowe Scholar, Warszawa 2011, s. 295.

zapewnienia użytkownikom instytucji jak najwyższego możliwego poziomu bezpieczeństwa poprzez wykorzystywanie odpowiednich rozwiązań technicznych. Nie narzuca im jednak metod do przeprowadzania identyfikacji[11]. Usługi bankowe zabezpieczone biometrykami mają głównie formę internetową i co za tym idzie, podlegają ustawie o świadczeniu usług drogą elektroniczną. Wykorzystywanie w bankowości zabezpieczeń biometrycznych odpowiada za świadczenie klientom usług elektronicznych, przy jednoczesnym uniemożliwianiu dostępu do treści osobom nieuprawnionym[12]. Bank jest zobowiązany zapoznać klientów z formami identyfikacji użytkowników usług bankowych, a w przypadku usług elektronicznych przydzielić niepowtarzalny identyfikator[13]. Ponadto prawo bankowe nakłada na bank i podmioty z nim związane obowiązek ścisłej ochrony danych klienta.

Kolejnym elementem regulacji, mającym wpływ na posługiwanie się zabezpieczeniami biometrycznymi, może być prawo bankowe. We fragmentach opisujących zachowanie tajemnicy bankowej można się dowiedzieć, że wszelakie informacje opisujące dane klienta muszą być ściśle chronione[14]. Także Kodeks Karny w art. 267 traktuje o sankcjach w stosunku do osób, które nielegalnie uzyskują dostęp do informacji dla nich nieprzeznaczonych (tzw. hakerstwo)[15].

Zabezpieczenia biometryczne są ściśle powiązane z ustawą o ochronie danych osobowych. W świetle tejże ustawy wszystko, co pozwala na zidentyfikowanie osoby, uważa się za dane osobowe[16]. Ustawa zawiera także definicje ściśle związane z bankowymi systemami informatycznymi, a dotyczące utrwalania, zbierania, przetwarzania, udostępniania i administrowania danymi[17]. Dane biometryczne można uznać za szczególną kategorię danych osobowych. Jednak ich wykorzystanie nie jest aktualnie określane przez polskie prawo[18]. Reguluje je natomiast Rozporządzenie Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Uznaje ono biometryki za dane wrażliwe, które mogą być przetwarzane wyłącznie za zgodą użytkownika[19].

Przemiany technologiczne wymuszają zmiany regulacyjne, jednak często ich wprowadzanie jest pracochłonne i długotrwałe – przykładem może być prawo pracy.

[11] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, t.j.: Dz.U. 2017 poz. 2003, ze zm., art. 60.
[12] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, t.j.: Dz.U. 2017 poz. 1219 ze zm., art. 7.
[13] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych..., *op. cit.*, art. 4.
[14] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, t.j.: Dz.U. 2017 poz. 1876 ze zm., art. 10.
[15] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j.: Dz.U. 2017 poz. 2204 ze zm., art. 267.
[16] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j.: Dz.U. 2016 poz. 922 ze zm., art. 6.
[17] S. Wojciechowska-Filipek, *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, s. 81.
[18] Polska Agencja Prasowa, *UE: przetwarzanie danych biometrycznych tylko za zgodą,* 13.06.2016 strona internetowa Lex.pl, http://www.lex.pl/czytaj/-/artykul/ue-przetwarzanie-danych-biometrycznych-tylko-za-zgoda (dostęp: 27.12.2017).
[19] Rozporządzenie Parlamentu Europejskiego i Rady UE 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 2016/679, punkt 51.

W artykule 22 Kodeksu Pracy znajduje się lista danych osobowych, których może żądać pracodawca od pracownika. Jednak nie zostały tam wymienione dane biometryczne jako obowiązkowe informacje o aplikujących do pracy osobach[20].

3. Przedmiot, cel i organizacja badania

Celem poznania kultury użytkowej klientów banków w zakresie biometrii wykorzystano metodę sondażu diagnostycznego. Badanie zostało przeprowadzone metodą CAWI (*Computer-Assisted Web Interview*) w języku polskim, w sposób anonimowy. Kwestionariusz elektroniczny ankiety wraz z uzasadnieniem znajdował się na stronie https://docs.google.com/forms/d/e/1FAIpQLSdvvd6JXNXy-k6EDln7tA_tPYr-PjzI7n3mFHwQgDNsFC8Ai9w/viewform?usp=sf_link. Zainteresowani respondenci odpowiadali na pytania zredagowane w formie zamkniętej – jedno- i wielokrotnego wyboru oraz w formie półotwartej. Na podstawie uzyskanych odpowiedzi stworzono wizerunek współczesnego klienta usług bankowych w Polsce w zakresie korzystania z zabezpieczeń biometrycznych oraz ich kultury użytkowej.

Badanie przeprowadzono w okresie od 9 marca do 16 kwietnia 2018 roku. By dotrzeć do szerokiego grona odbiorców wykorzystano portal społecznościowy Facebook i wybrane fora internetowe. Prośbę o wypełnienie kwestionariusza rozsyłano również mailowo na bazę adresową Autora. Badaniem objęto osoby, które ukończyły 16. rok życia, bez względu na płeć, miejsce zamieszkania oraz wykształcenie.

Kwestionariusz zawierał 14 pytań w porządku sekwencyjnym i dedukcyjnym (od ogółu do szczegółu). Elektronicznie wypełnione kwestionariusze nie zawierały błędów, a ostateczna liczba respondentów wyniosła 505.

4. Charakterystyka próby badawczej

W przeprowadzonym badaniu udział wzięło 505 osób, z czego niemal 70% stanowiły kobiety, natomiast 30% mężczyźni (por. tabela 1).

Tabela 1. Liczba i struktura respondentów według płci

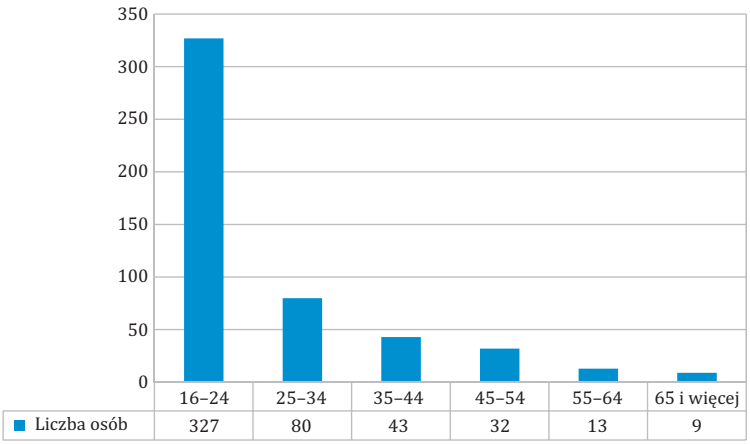
Płeć respondentów	Liczba wypełnionych ankiet	Struktura procentowa (w %)
Kobiety	351	69,5
Mężczyźni	153	30,3
Brak odpowiedzi	1	0,2
Razem	505	100

Źródło: opracowanie własne.

[20] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, t.j.: Dz.U. 2016 poz. 1666 ze zm., art. 22.

Przewaga kobiet nad mężczyznami w przeprowadzonym badaniu jest znacząca; struktura próby jest odmienna od struktury całej populacji.

Rysunek 1. Liczba respondentów według wieku



Źródło: opracowanie własne.

Niemal 65% respondentów stanowiły osoby w wieku 16–24 lata, co w pewnym stopniu odzwierciedla aktywność informatyczną polskiego społeczeństwa, z dominacją pokolenia Z (zob. rysunek 1)[21]. Jednocześnie wskazuje na historyczne dziedzictwo w sferze posługiwania się społeczną komunikacją z wykorzystaniem Internetu. Tylko jeden respondent nie udzielił odpowiedzi na pytanie o wiek.

Struktura demograficzna respondentów, a także forma, sposób i miejsce realizacji badania pozwalają założyć, że w badaniu udało się dotrzeć do kluczowej grupy potencjalnych użytkowników nowoczesnych zabezpieczeń w bankowości – osób zaznajomionych z technikami cyfrowymi, otwartymi na innowacje.

W pewnym stopniu potwierdzeniem segmentacji informacyjnej społeczeństwa polskiego jest struktura respondentów ze względu na wykształcenie (por. tabela 2). Niemal 98% ogółu respondentów stanowią osoby z wykształceniem średnim oraz wyższym, wśród których dominują prawdopodobnie studenci i absolwenci uczelni.

[21] M. Haponiuk, *X,Y,Z: sztafeta pokoleń na rynku pracy*, 19.07.2013, strona internetowa: Instytutobywatelski.pl, http://www.instytutobywatelski.pl/16154/blogi/co-z-ta-praca/xyz-sztafeta-pokolen-na-rynku-pracy (dostęp: 16.04.2018).

Tabela 2. Liczba i struktura respondentów według wykształcenia

Wykształcenie respondentów	Liczba wypełnionych ankiet	Struktura procentowa
Podstawowe	2	0,4
Gimnazjalne	5	1,0
Zawodowe/Zasadnicze	6	1,2
Średnie	251	49,7
Wyższe	237	46,9
Brak odpowiedzi	4	0,8
Razem	505	100,0

Źródło: opracowanie własne.

Tabela 3. Liczba i struktura respondentów według miejsca zamieszkania

Miejsce zamieszkania respondentów	Liczba wypełnionych ankiet	Struktura procentowa
Wieś	155	30,7
Miasto do 50 tys. mieszkańców	78	15,4
Miasto do 100 tys. mieszkańców	48	9,5
Miasto do 250 tys. mieszkańców	21	4,2
Miasto powyżej 250 tys. mieszkańców	200	39,6
Brak odpowiedzi	3	0,6
Razem	505	100,0

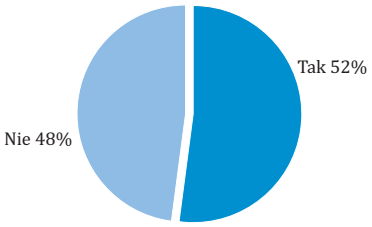
Źródło: opracowanie własne.

Krytrium podziału respondentów na mieszkańców wsi i miast daje proporcję 3 do 7 (zob. tabela 3). Przy czym liczba respondentów – mieszkańców wsi wynosi ok. 31%, zaś miast powyżej 250 tys. mieszkańców ok. 40%.

5. Wyniki badania kwestionariuszowego

Pierwsze pytanie dotyczyło znajomości terminu „zabezpieczenie biometryczne" (por. rysunek 2).

Rysunek 2. Struktura odpowiedzi dotyczących znajomości terminologii związanej z zabezpieczeniami biometrycznymi



Źródło: opracowanie własne.

Wśród badanych 52% zadeklarowało znajomość znaczenia terminu „zabezpieczenie biometryczne". Pozostali przyznali, że nigdy wcześniej nie spotkali się z pojęciem biometrii. Dokonując analizy odpowiedzi respondentów (według ich płci), można zauważyć, że to większy odsetek mężczyzn ma wiedzę związaną z terminologią zabezpieczeń opartych na biometrykach. Twierdząco na zapytanie odpowiedziało 102 panów (66,7%) i 160 pań (45,6%). Odpowiedzi negatywnych udzieliło tylko 51 mężczyzn (33,3%) oraz 191 kobiet (54,4%). Efektem pytania filtrującego były dwie ścieżki pytań – pierwsza dla osób znających termin biometrii, natomiast druga – umożliwiająca osobom nie mającym wiedzy na zapoznanie się z wyjaśnieniem pojęcia.

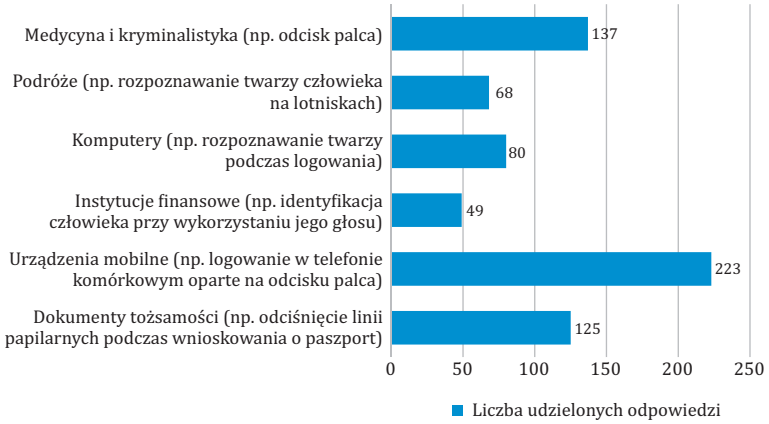
Zagadnienie dotyczące doświadczeń z wykorzystaniem zabezpieczeń biometrycznych było pytaniem wielokrotnego wyboru. Kafeteria odpowiedzi składała się z 6 propozycji (zob. rysunek 3), jednak ankietowani mieli możliwość udzielenia własnych odpowiedzi.

Respondenci najczęściej spotykali się z terminologią zabezpieczeń biometrycznych w sytuacjach związanych z wykorzystaniem urządzeń mobilnych – taką odpowiedź zaznaczyło ok. 88% badanych deklarujących znajomość pojęcia biometrii (263 osoby udzielały odpowiedzi na powyższe pytanie). Próg 100 odpowiedzi przekroczyły skojarzenia z zastosowań medycznych i kryminalistycznych oraz proces wyrobienia dokumentów tożsamości (tj. paszport). Pozostałe odpowiedzi wiążące biometrię z podróżami oraz komputerami zaakcentował co czwarty z ankietowanych. Połączenie biometrii z instytucjami finansowymi kojarzy się tylko co piątemu respondentowi. 19 ankietowanych postanowiło dodać swoje własne doświadczenia z biometrią – wśród odpowiedzi pojawiły się:

- Filmy akcji i *science fiction* – 5 odpowiedzi,
- Skanowanie odcisku palca w punkcie rejestracji na siłowniach oraz basenach z wykorzystaniem OK System – 4 odpowiedzi,

- Możliwość dostania się do pomieszczeń/biura – 3 odpowiedzi,
- Doświadczenia własne, rozmowy ze znajomymi – 3 odpowiedzi,
- Praca nad projektami technicznymi – 2 odpowiedzi,
- Uczelniane zajęcia z trendów w bankowości – 2 odpowiedzi.

Rysunek 3. Struktura odpowiedzi na pytanie, w jakich sytuacjach respondenci zetknęli się z pojęciem zabezpieczeń biometrycznych



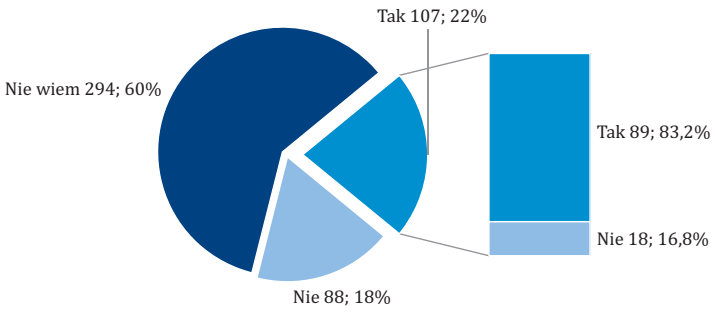
Źródło: opracowanie własne.

Kolejne pytanie pozwoliło wyselekcjonować podpróbę respondentów posiadających rachunek bankowy. Wśród 505 respondentów znalazło się 16 osób, które nie mają rachunku bankowego. Odpowiedzi tej udzieliło 12 osób z grupy wiekowej 16–24 lata, jedna z grupy 25–34 lata oraz trzy z grupy 45–55 lat; dokładnie połowa z tych osób była mieszkańcami miast, a połowa – wsi.

Posiadacze rachunku bankowego odpowiadali na pytanie, czy ich bank posiada w swojej ofercie różne formy zabezpieczeń biometrycznych (zob. rysunek 4). Odpowiedzi na to pytanie udzielić mogło 489 osób. Tylko 107 ankietowanych (prawie 22% podpróby) jest świadomych tego, że instytucja finansowa, w której mają rachunek, oferuje swoim klientom zabezpieczenia biometryczne. 88 respondentów odpowiedziało, że ich bank nie zawiera w swoich propozycjach biometrii. 60% badanych nie było w stanie udzielić odpowiedzi na to pytanie – w wynikach sondażu diagnostycznego aż 294 razy pojawiła się odpowiedź, że respondent nie wie, czy instytucja finansowa, w której ma konto bankowe, oferuje różne rodzaje form biometryk w celu zwiększenia bezpieczeństwa transakcji finansowych klientów.

Respondenci deklarujący wiedzę o oferowaniu przez banki różnych form zabezpieczeń biometrycznych zostali zapytani, czy korzystają z możliwości zwiększających bezpieczeństwo. Spośród 107 respondentów, którzy wiedzą, że ich bank oferuje zabezpieczenia biometryczne, aż 83,2% odpowiedziało, że z nich korzysta, natomiast 16,8% – mimo wiedzy o ofercie instytucji finansowej – nie skorzystało dotąd z zabezpieczeń biometrycznych.

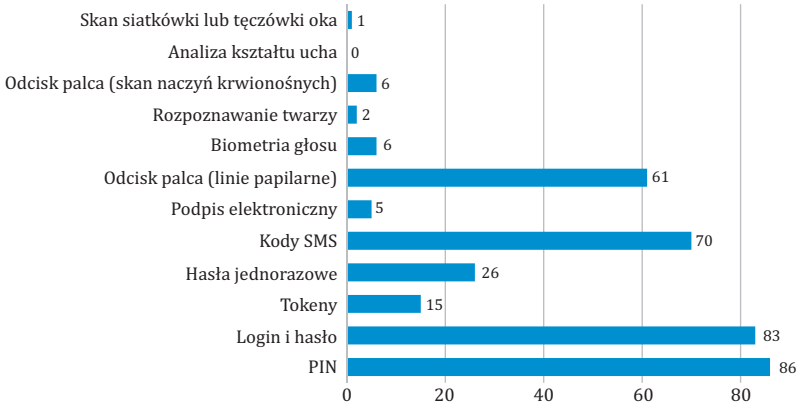
Rysunek 4. Liczba i struktura odpowiedzi na pytanie, czy banki respondentów oferują formy zabezpieczeń biometrycznych (wykres kołowy) oraz czy ankietowani świadomi tych ofert z nich korzystają (wykres słupkowy)



Źródło: opracowanie własne.

Z kolei 89 respondentów korzystających z oferty zabezpieczeń zapytano, jakie formy zwiększające bezpieczeństwo sami użytkują (rysunek 5)[22].

Rysunek 5. Liczba odpowiedzi dotyczących wykorzystywanych przez respondentów form zabezpieczeń w bankach



Źródło: opracowanie własne.

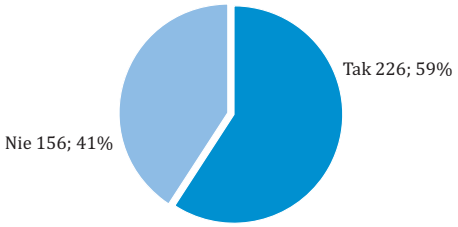
Odpowiedzi respondentów dowodzą, że zdecydowanie dominują klasyczne zabezpieczenia (PIN, login i hasło, kody SMS). Relatywnie niewielu klientów korzysta z hasła jednorazowego, tokenu, a marginalnie z podpisu elektronicznego. Natomiast aż 69% deklaruje korzystanie z zabezpieczenia w formie odcisku palca (linii papilarnych). Śladową popularność uzyskały pozostałe formy zabezpieczeń biometrycznych. Tylko 2 osoby z 89 wykorzystują rozpoznawanie twarzy, a 1 osoba

[22] Respondenci mogli wskazać więcej niż jedną odpowiedź, nie występowało ograniczenie w liczbie możliwych do zaznaczenia odpowiedzi.

skanowanie siatkówki lub tęczówki oka. Nikt z badanych w celu identyfikacji nie korzystał z analizy kształtu ucha. Interpretując odpowiedzi, można przypuszczać, że biometryczne sposoby zabezpieczeń związane są z wykorzystywaniem mobilnych aplikacji bankowych oraz popularnością nowoczesnych urządzeń telefonii komórkowej.

Na pytanie o oferowanie przez banki zabezpieczeń biometrycznych 382 ankietowanych, którzy odpowiedzieli „nie" lub „nie wiem", zostali poproszeni o określenie szans na przekonanie ich do rezygnacji z tradycyjnych form zabezpieczeń i zastąpienia ich biometrią (rysunek 6). Niemal 60% osób byłoby skłonnych zainteresować się zwiększeniem bezpieczeństwa poprzez wykorzystanie biometryk. Bardziej otwarci na taką zmianę są mężczyźni (65%) niż kobiety (57%).

Rysunek 6. Struktura odpowiedzi dotyczących skłonności zmian tradycyjnych form zabezpieczeń na biometrię



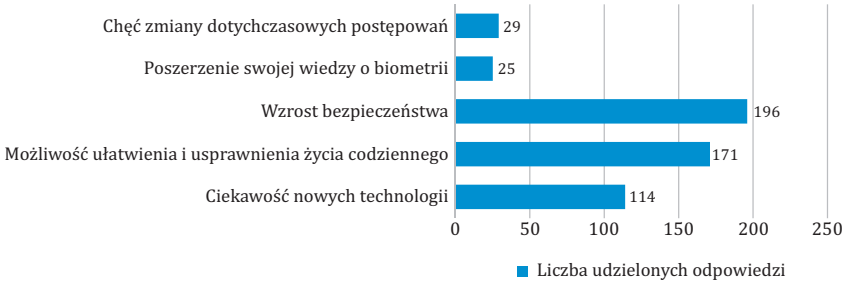
Źródło: opracowanie własne.

Kolejne dwa pytania zostały skierowane do osób, które nie miały rachunku bankowego, jak również klientów banków, którzy nie korzystali z biometrycznych form zabezpieczeń oraz pozytywnie wypowiedzieli się w kwestii potencjalnej zmiany w korzystaniu z tradycyjnych PIN-ów, loginów, haseł itd. na rzecz biometryk. Na pierwsze pytanie – wielokrotnego wyboru – odpowiedziało 260 osób, które z kafeterii 5 wariantów wybierały najważniejsze przyczyny mogące skłonić je do skorzystania w przyszłości z zabezpieczeń biometrycznych (rysunek 7).

Najważniejszym powodem potencjalnej zmiany zachowań było bezpieczeństwo. Co drugi respondent zaznaczył, że duży wpływ na możliwe skorzystanie z zabezpieczeń biometrycznych miałaby ciekawość nowych technologii. Co dziesiąty ankietowany chciałby skorzystać z „biometryk", by poszerzyć swoją wiedzę na ich temat oraz zmienić dotychczasowe postępowania. Dla respondentów w wieku 16–24 lata najważniejsze było ułatwienie życia codziennego oraz wzrost bezpieczeństwa. Te powody zostały wybrane przez 47 ankietowanych, co stanowi niemal 30% najmłodszych respondentów (do lat 24). Spośród odpowiedzi wielokrotnego wyboru także to połączenie było najpopularniejsze dla osób z wykształceniem wyższym oraz średnim (ponad 30% respondentów).

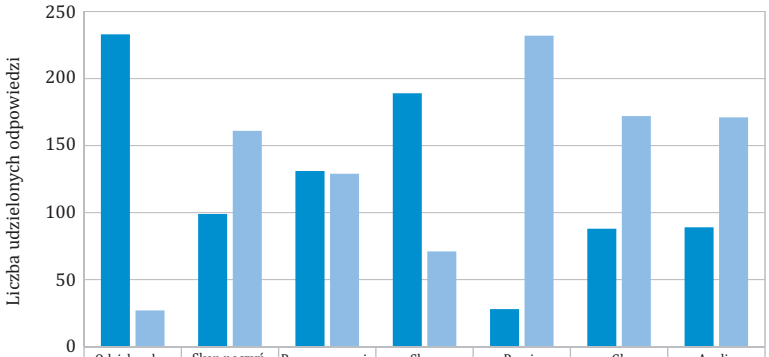
Drugie pytanie w tej grupie dotyczyło skłonności respondentów do skorzystania z danego rodzaju zabezpieczenia biometrycznego (rysunek 8).

Rysunek 7. Powody, dla których respondenci byliby skłonni skorzystać z zabezpieczeń biometrycznych



Źródło: opracowanie własne.

Rysunek 8. Skłonność respondentów do skorzystania z danego rodzaju zabezpieczenia biometrycznego



	Odcisk palca	Skan naczyń krwionośnych dłoni	Rozpoznawanie twarzy	Skan siatkówki lub tęczówki oka	Pomiar kształtu ucha	Głos	Analiza podpisu odręcznego
Tak	233	99	131	189	28	88	89
Nie	27	161	129	71	232	172	171

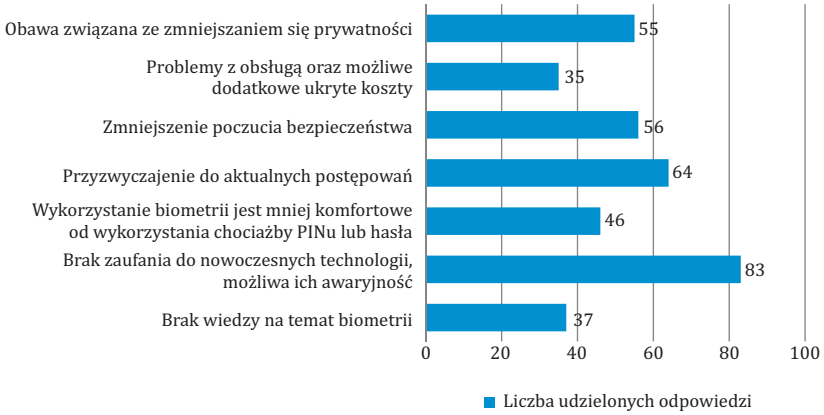
Źródło: opracowanie własne.

Największą skłonność do wykorzystania – jako formy zabezpieczenia w bankowości – ankietowani wyrazili dla odcisku palca oraz skanu siatkówki lub tęczówki oka. Te dwie biometryki znacząco przeważyły pozytywnymi odpowiedziami nad negatywnymi. Odpowiedzi respondentów były zrównoważone w przypadku identyfikowania człowieka z wykorzystaniem rozpoznawania twarzy. Zdecydowana większość spośród 260 badanych odpowiadających na to pytanie nie wyraziła skłonności do wykorzystania pozostałych biometryk, tj. skanu naczyń krwionośnych dłoni, głosu oraz analizy podpisu odręcznego. Najgorszy wynik uzyskała biometria oparta na analizie i pomiarze kształtu ucha człowieka. Uwzględniając opinie wyników niniejszego sondażu należałoby także rozważyć wprowadzenie rozwiązań wykorzystujących skan siatkówki lub tęczówki oka. Tym bardziej, że uzyskane wyniki

są m.in. konsekwencją doświadczeń zdobytych przez klientów posługujących się nowoczesnymi telefonami komórkowymi, w zakresie przeprowadzania transakcji finansowych[23].

Respondenci niechętni do stosowania biometrycznych zabezpieczeń byli proszeni o uzasadnienie swych odpowiedzi poprzez wybór przynajmniej jednego z 7 wariantów powodów (rysunek 9).

Rysunek 9. Powody, dla których respondenci nie chcieliby skorzystać z zabezpieczeń biometrycznych



Źródło: opracowanie własne.

Prawie 53% respondentów jako przyczynę niechęci do wykorzystywania zabezpieczeń biometrycznych wskazało brak zaufania do nowoczesnych technologii i potencjalną ich awaryjność. Zresztą, co typowe, respondenci w szerszym zakresie eksponowali postawę zachowawczą – obok braku zaufania były to: relatywnie często przyzwyczajenia, zmniejszenie poczucia bezpieczeństwa czy obawa przed utratą prywatności. W interpretacji wyników trzeba wziąć pod uwagę, że respondenci wybierali odpowiedzi spośród wyszczególnionych w kwestionariuszu wariantów. Natomiast 12 ankietowanych udzieliło własnej odpowiedzi na powyższe pytanie, wyjaśniając niechęć do wykorzystywania biometryk:

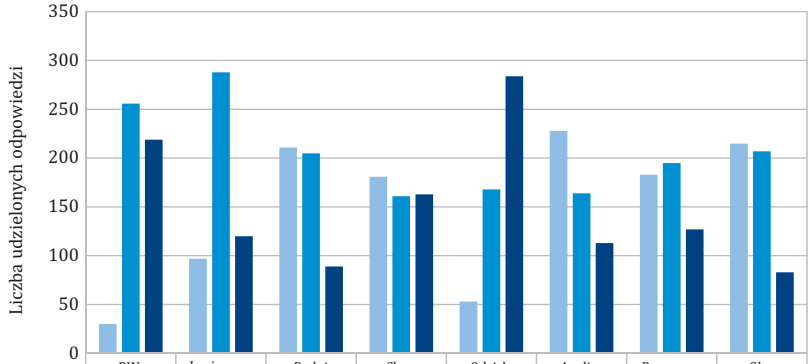
- możliwą utratą palca/oka oraz zmianami spowodowanymi starzeniem się organizmu człowieka – 4 odpowiedzi,
- brakiem możliwości zlecenia komuś innemu wykonanie usługi na ich rachunku (np. wypłata gotówki z bankomatu) – 3 odpowiedzi,
- wysokimi kosztami wprowadzenia urządzeń opartych na biometrii – 2 odpowiedzi,
- obowiązkiem kontroli, by nikt nie zdobył ich odcisku palca – 2 odpowiedzi,
- niebezpieczeństwem kradzieży danych z baz elektronicznych – 1 odpowiedź.

[23] Otrzymane wyniki badania zgodne są z rezultatami prezentowanymi przez M. Siekierską, *Europejczycy chcą korzystać z biometrii w płatnościach*, 29.01.2017, https://www.payu.pl/blog/europejczycy-chca-korzystac-z-biometrii-w-platnosciach (dostęp: 24.07.2018).

Odpowiedzi samodzielnie wygenerowane przez respondentów, z wyjątkiem przyzwolonego korzystania z rachunku oraz kosztów wdrożenia nowości, w kontekście obecnego stanu wiedzy można uznać za nieracjonalne. Ogólnie kwestia niechęci znacznej części klientów banków do zastosowań zabezpieczeń biometrycznych wymaga szerokiej akcji edukacyjnej i uświadamiającej, gdyż stosunkowo silnie na ich postawy wpływają stereotypy lub po prostu brak wiedzy.

Pozostałe pytania były kierowane do wszystkich ankietowanych, bez względu na udzielane odpowiedzi w poprzednich etapach badania. Respondenci zostali poproszeni o ocenę poziomu komfortu korzystania z wyszczególnionych form zabezpieczeń w bankowości oraz określenie poziomu bezpieczeństwa związanego z ich użytkowaniem (rysunek 10).

Rysunek 10. Charakterystyka odpowiedzi 505 respondentów na pytanie o komfort korzystania z zabezpieczeń w bankowości



	PIN	Login oraz hasło	Podpis odręczny	Skan siatkówki lub tęczówki oka	Odcisk palca	Analiza naczyń krwionośnych dłoni	Rozpoznawanie twarzy człowieka	Głos
Niekomfortowy	30	97	211	181	53	228	183	215
Akceptowalny	256	288	205	161	168	164	195	207
Komfortowy	219	120	89	163	284	113	127	83

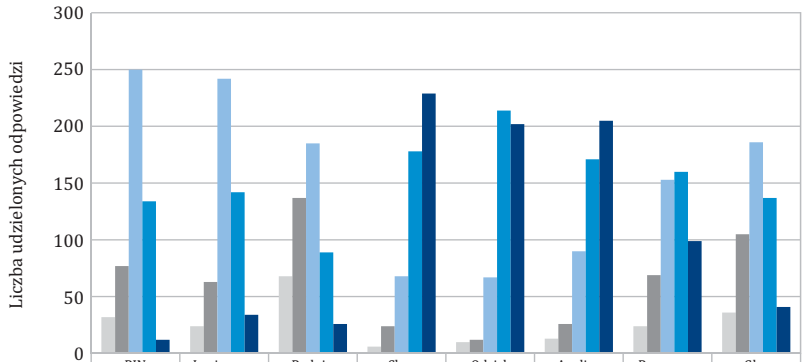
Źródło: opracowanie własne.

Największe zainteresowanie wśród respondentów wzbudziła biometryka oparta na odcisku palca. 284 badanych (56%) uznało to zabezpieczenie za najbardziej komfortowe. Wynika z tego, że respondenci są świadomi unikalności linii papilarnych człowieka. Wyróżniającą liczbę pozytywnych opinii uzyskały także PIN (219 osób – 43% – oceniło tę formę ochrony jako komfortową) oraz analiza siatkówki lub tęczówki oka człowieka (163 osoby – 32% badanych). W tych przypadkach komfort użycia może być wiązany z łatwością zastosowania zabezpieczenia oraz ogólnie przyjętymi przyzwyczajeniami. Najczęściej spotykane zabezpieczenia, czyli PIN, login oraz hasło zostały ocenione jako akceptowalne w użytkowaniu – odpowiedzi takich udzieliło odpowiednio 51% i 57% badanych, co może wskazywać na fakt

osobistych zastosowań tych form zabezpieczeń przez respondentów i nawyków. Największy odsetek odpowiedzi „niekomfortowy" pojawił się przy zabezpieczeniach opartych na podpisie odręcznym oraz analizie naczyń krwionośnych dłoni. Niemal co drugi z respondentów (odpowiednio: 211 i 228 osób) uważa, że wykorzystanie tych form ochrony nie byłoby wygodne (w przypadku analizy naczyń krwionośnych dłoni wynik ten mógłby być związany z wykorzystaniem w nazwie terminologii „naczyń krwionośnych", które często budzą lęk w społeczeństwie, spowodowany prawdopodobnie pobieraniem krwi, operacjami, pobytem w szpitalu). Najmniejszy odsetek odpowiedzi negatywnych odnosił się do zabezpieczeń opartych na PIN-ie (zabezpieczenie to zostało określone jako niekomfortowe przez co 20 respondenta) oraz odcisku palca człowieka (tylko 10% badanych).

Tradycyjne formy zabezpieczeń zostały określone jako akceptowalne w użyciu, co może być powodowane powszechnością ich zastosowań i przyzwyczajeniami społeczeństwa. Biometryki wzbudzają wśród ankietowanych różne odczucia, ponieważ badani nie są świadomi tego, jak korzysta się z danej formy zabezpieczenia, lub też nie potrafią sobie tego wyobrazić. Konfrontacja bezpośrednia, kiedy klient będzie mógł doświadczyć nowoczesnych rozwiązań w rzeczywistości, może spowodować zmiany w ich opiniowaniu.

Rysunek 11. Ocena klientów poziomu bezpieczeństwa użytkowania zabezpieczeń



	PIN	Login oraz hasło	Podpis odręczny	Skan siatkówki lub tęczówki oka	Odcisk palca	Analiza naczyń krwionośnych dłoni	Rozpoznawanie twarzy człowieka	Głos
Bardzo niski	32	24	68	6	10	13	24	36
Niski	77	63	137	24	12	26	69	105
Przeciętny	250	242	185	68	67	90	153	186
Wysoki	134	142	89	178	214	171	160	137
Bardzo wysoki	12	34	26	229	202	205	99	41

Źródło: opracowanie własne.

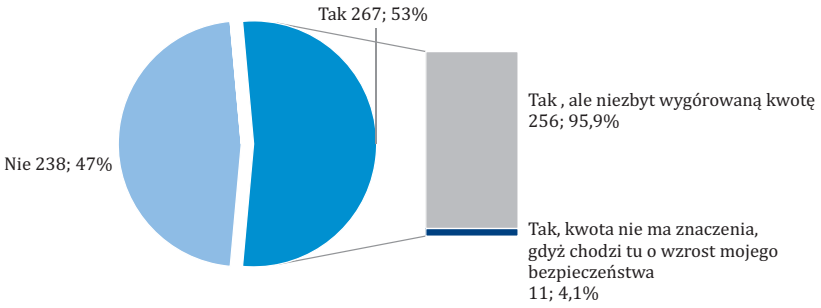
Do oceny poziomu bezpieczeństwa wśród zabezpieczeń w bankowości wykorzystano pięciostopniową skalę (rysunek 11). Najbardziej korzystnie (wysoko lub bardzo wysoko) określono bezpieczeństwo przy zastosowaniu odcisku palca (82%

badanych), skanu siatkówki lub tęczówki oka człowieka (81%) oraz analizy naczyń krwionośnych dłoni (74%)[24]. To właśnie te formy powinny być wykorzystywane chociażby przez instytucje finansowe do zabezpieczania rachunków klientów. Ochronę poprzez wykorzystanie PIN-u, loginu oraz hasła respondenci uznali jako przeciętną (w obu przypadkach takiej odpowiedzi udzielił co drugi z badanych). Może to być spowodowane doświadczeniami ankietowanych, szczególnie sytuacjami wynikającymi z niewystarczającego poziomu ochrony. W przeprowadzonym badaniu najmniejsze zaufanie wśród ankietowanych uzyskał podpis odręczny i głos. Odpowiednio 41% oraz 28% badanych udzieliło odpowiedzi, że te formy ochrony charakteryzują się niskim lub bardzo niskim poziomem bezpieczeństwa.

Wyniki prezentujące poziom bezpieczeństwa poszczególnych biometryk, podobnie jak w przypadku oceny komfortu stosowalności, wskazują na przeciętny poziom ocen odnoszących się do tradycyjnych form zabezpieczeń. Respondenci są świadomi niepowtarzalności cech biometrycznych człowieka, a tym samym zabezpieczenia na nich oparte oceniają jako bezpieczniejsze.

Znając opinię ankietowanych o zabezpieczeniach tradycyjnych oraz biometrykach, zapytano o gotowość poniesienia dodatkowych kosztów związanych z wdrożeniem nowych technologii zwiększających ich bezpieczeństwo jako klienta banków (rysunek 12).

Rysunek 12. Struktura odpowiedzi dotyczących poniesienia dodatkowych kosztów związanych z użytkowaniem zabezpieczeń biometrycznych



Źródło: opracowanie własne.

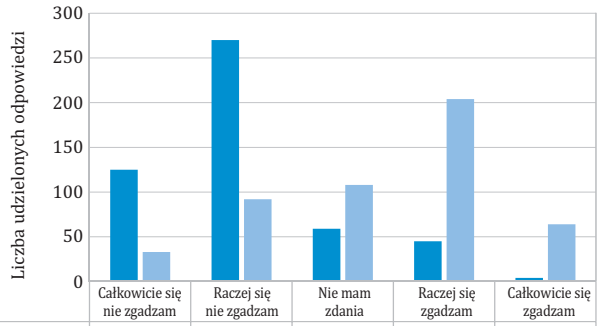
53% respondentów byłoby gotowych ponieść dodatkowe koszty związane z użytkowaniem zabezpieczeń biometrycznych, przy czym aż 96% spośród nich uwarunkowuje to „niezbyt wygórowaną kwotą". Kwestia rzeczywistego kosztu akceptowanego przez klientów wymaga dalszych badań, tym bardziej że 47% respondentów deklaruje niechęć ponoszenia kosztów wdrożenia takich zabezpieczeń. Instytucje finansowe rozpoczynające wdrażanie biometryk muszą więc być świadome

[24] Potwierdza to wyniki uzyskane z badania przeprowadzonego na próbie międzynarodowej: IBM Security, Future of identity study, https://hollandfintech.com/wp-content/uploads/2018/03/security-ibm-security-solutions-wg-research-report-22012422usen-20180124.pdf

oczekiwań klientów w kwestii ponoszenia kosztów wykorzystywania biometrii, a nadto muszą zbadać tzw. elastyczność cenową nowych usług, przynajmniej w wariancie występowania konkurencyjnych rozwiązań w danym okresie.

Ankietowani zostali poproszeni także o ocenienie dwóch stwierdzeń dotyczących kwestii biometrii we współczesnym świecie (rysunek 13). Respondenci do udzielenia odpowiedzi wykorzystywali pięciostopniową skalę Likerta.

Rysunek 13. Odpowiedzi respondentów dotyczące zabezpieczeń biometrycznych w Polsce



	Całkowicie się nie zgadzam	Raczej się nie zgadzam	Nie mam zdania	Raczej się zgadzam	Całkowicie się zgadzam
Polacy mają wiedzę na temat zabezpieczeń biometrycznych	125	270	59	45	3
Polska to dobre miejsce na wprowadzanie innowacyjnych form zabezpieczeń	33	92	108	204	64

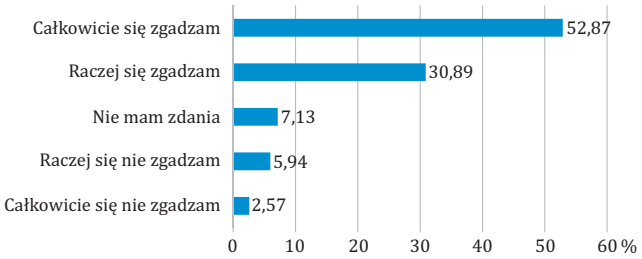
Źródło: opracowanie własne.

Respondenci, określając poziom wiedzy o zabezpieczeniach biometrycznych wśród Polaków oraz oceniając, czy Polska to dobry kraj do wprowadzenia innowacyjnych form zwiększających bezpieczeństwo, stworzyli interesujący profil społeczeństwa. W odpowiedzi na te dwa pytania została ujawniona asymetria charakteryzująca społeczeństwo polskie jako nie mające znaczącej wiedzy na temat biometrii, ale zdecydowane na uzyskanie możliwości korzystania z nowych form zabezpieczeń. Zdecydowana większość respondentów stwierdziła, że Polacy nie znają zabezpieczeń biometrycznych; jednocześnie większość badanych określiło Polskę jako dobre miejsce na rozwój innowacyjnych zabezpieczeń[25]. Odpowiedzi na te pytania mogą być potwierdzeniem, że Polacy przychylni są innowacjom technologicznym i chętnie adaptują nowe rozwiązania. Jednocześnie jest to ważna informacja dla banków (i innych podmiotów zainteresowanych wykorzystaniem zabezpieczeń biometrycznych), że niezbędne są szeroko zakrojone działania edukacyjne w tym zakresie.

[25] Rozszerzeniem badania mogą być wnioski zaprezentowane przez Łukasza Majchrzyka, redaktora mobiRANK.pl z artykułu *Polscy konsumenci oczekują więcej cyfrowych usług*, 27.09.2016, https://mobirank.pl/2016/09/27/polscy-konsumenci-oczekuja-wiecej-cyfrowych-uslug (dostęp: 24.07.2018).

Struktura odpowiedzi dotycząca zagrożenia wynikającego z cyberprzestępstw pośrednio wskazuje, że respondenci są świadomi zagrożeń związanych z korzystaniem z Internetu, a jednocześnie wierzą, że zabezpieczenia biometryczne mogą ograniczyć cyberzagrożenia – ataki hakerskie czy kradzieże danych dostępowych (rysunek 14).

Rysunek 14. Struktura odpowiedzi na pytanie, czy zabezpieczenia biometryczne mogą ograniczać cyberzagrożenia



Źródło: opracowanie własne.

Podsumowanie

Metody i technologia zabezpieczeń biometrycznych nie są jeszcze w pełni zbadane ani eksperymentalnie, ani w praktyce zastosowań w bankowości. Wiele jednak wskazuje na duży potencjał zastosowań praktycznych w sposób zintegrowany, i to nie tylko w bankowości i finansach. Uzyskane wyniki badań mogą stanowić przyczynek do dyskusji na temat rozwoju zabezpieczeń biometrycznych i ich wykorzystania w instytucjach finansowych. Warunkiem *sine qua non* wpowadzenia zabezpieczeń biometrycznych jest z jednej strony zwiększenie poziomu bezpieczeństwa usług i korzystania z nich przez klientów, a z drugiej akceptowalne dla banków nakłady, zaś dla klientów – koszty. Wykorzystując doświadczenia z wdrażania bankowości elektronicznej i internetowej, można przypuszczać, że proces zastępowania dotychczasowych metod zabezpieczeń, które dość paradoksalnie nazywane są tradycyjnymi, będzie postępował. Podobnie jak proces „wypychania" klientów z tradycyjnych oddziałów banków, może następować on sukcesywnie lub – w przypadku eskalacji zagrożeń, w tym zwłaszcza hakerskich – być znacząco przyspieszony.

W świetle wyników przeprowadzonego badania warto eksponować potrzebę szerokiej akcji edukacyjnej społeczeństwa, tym bardziej, że odpowiednie zabezpieczenia biometryczne stanowią czynnik integracji elektronicznych usług bankowych z innymi sferami aktywności człowieka i usług publicznych. Analiza literatury i wyniki przeprowadzonego sondażu wskazują, że biometria nie jest aktualnie kojarzona głównie z instytucjami finansowymi. By to zmienić, banki powinny zadbać o szeroką akcję edukacyjną, i to prowadzoną nie tylko w zakresie usług bankowych czy finansowych. Ważne znaczenie może mieć wprowadzenie problematyki biometrii do programów szkolnych, a także popularyzowanie jej w środkach masowego przekazu.

Bibliografia

Bajor B., *Bankowość elektroniczna. Studium prawne*, Wydawnictwo Naukowe Scholar, Warszawa 2011.

Boczoń W., *Biometria w bankowości. Co za jej pomocą załatwimy dziś w banku?*, 13.09.2017, strona internetowa Bankier.pl, https://www.bankier.pl/wiadomosc/Biometria-w-bankowosci-Co-za-jej-pomoca-zalatwimy-dzis-w-banku-7542743.html (dostęp: 28.11.2017).

Bodnar A., Michalski J., *Dokument biometryczny a prawa człowieka*, http://www.prawaczlowieka.pl/precedens/images/stories/dokument_biometryczny_a_prawa_czowieka.pdf (dostęp: 05.12.2017).

Bralczyk J. (red.), *Słownik 100 tysięcy potrzebnych słów*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Haponiuk M., *X,Y,Z: sztafeta pokoleń na rynku pracy*, 19.07.2013, strona internetowa: Instytut obywatelski.pl, http://www.instytutobywatelski.pl/16154/blogi/co-z-ta-praca/xyz-sztafeta-pokolen-na-rynku-pracy (dostęp: 16.04.2018).

IBMSecurity,Futureofidentitystudy,https://hollandfintech.com/wp-content/uploads/2018/03/security-ibm-security-solutions-wg-research-report-22012422usen-20180124.pdf

Kaszubski R.W. (red.), *Biometria w bankowości i administracji publicznej*, Forum Technologii Bankowych, Warszawa 2009, https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/technologie_bankowe/publikacje/Forum_Technologii_Bankowych_-_Biometria_dla_bankowosci_i_administracji.pdf

Kaszubski R.W., *Społeczne i prawne aspekty biometrii. Człowiek i dokument*, Forum Technologii Bankowych, 2011.

Kuchciak I., *Bankowość biometryczna – nowe wyzwanie dla polskiego sektora bankowego*, „Annales Universitatis Mariae Curie-Skłodowska" 2011, Vol. XLV, 2.

Majchrzyk Ł., *Polscy konsumenci oczekują więcej cyfrowych usług*, 27.09.2016, https://mobirank.pl/2016/09/27/polscy-konsumenci-oczekuja-wiecej-cyfrowych-uslug (dostęp: 24.07.2018).

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

Polasik M., *Bankowość elektroniczna: istota – stan – perspektywy*, Wydawnictwo CeDeWu, Warszawa 2006, s. 38.

Polska Agencja Prasowa, *UE: przetwarzanie danych biometrycznych tylko za zgodą,* 13.06.2016 strona internetowa Lex.pl, http://www.lex.pl/czytaj/-/artykul/ue-przetwarzanie-danych-biometrycznych-tylko-za-zgoda (dostęp: 27.12.2017).

Pugliese J., *Biometrics: bodies, technologies, biopolitics*, Routledge, Londyn 2010.

Rozporządzenie Parlamentu Europejskiego i Rady UE 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 2016/679, punkt 51.

Ruud Bolle M., Connel J.H., Pankanti S., *Biometria*, Wydawnictwo Naukowo-Techniczne, Warszawa 2008.

Siekierska M., *Europejczycy chcą korzystać z biometrii w płatnościach*, 29.01.2017, https://www.payu.pl/blog/europejczycy-chca-korzystac-z-biometrii-w-platnosciach (dostęp: 24.07.2018).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, t.j.: Dz.U. 2016 poz. 1666 ze zm., art. 22.

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j.: Dz.U. 2017 poz. 2204 ze zm., art. 267.

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, t.j.: Dz.U. 2017 poz. 1876 ze zm., art. 10.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j.: Dz.U. 2016 poz. 922 ze zm., art. 6.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, t.j.: Dz.U. 2017 poz. 1219 ze zm., art. 7.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, t.j.: Dz.U. 2017 poz. 2003, ze zm., art. 60.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych..., *op. cit.*, art. 4.

Wojciechowska-Filipek S., *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010.

Woszczyński T. (red.), *Biometria w bankowości – kluczowe aspekty*, Warszawa 2015, https://zbp.pl/public/repozytorium/dla_bankow/rady_i_komitety/bankowosc_elektroczniczna/FTB/biometria_raport_09_2015_A4_e_light.pdf