• F I N A N S E I P R A W O F I N A N S O W E •
• JOURNAL OF FINANCE AND FINANCIAL LAW •

Wrzesień/ September 20025 • vol. 3(47): 103–128

Funding information: Not applicable. **Conflicts of interests:** None. **Ethical considerations:** The Authors assure of no violations of publication ethics and take full responsibility for the content of the publication.

WYKORZYSTANIE BIOMETRII BEHAWIORALNEJ W KONTEKŚCIE CYBERBEZPIECZEŃSTWA POLSKIEGO SEKTORA BANKOWEGO (2019–2024)

Wiesław Macierzyński[*], **Michał Macierzyński**[**]

https://doi.org/10.18778/2391-6478.3.47.07

USING BEHAVIORAL BIOMETRICS IN THE CONTEXT OF CYBERSECURITY OF POLISH BANKING SECTOR (2019-2024)

ABSTRACT

The purpose of the article. The purpose of the article is verification of the hypothesis that behavioral biometrics may become a solution which will reduce the extent of financial fraud in Poland. The problem in question is notable due to the negative impact of changes on cybersecurity in the environment of banking sector, after the COVID-19 pandemic. Only over the years 2019–2024 there was a tenfold increase in the value of fraud. The risk of financial crime in cyberspace is becoming the major challenge faced by the financial sector. Such high dynamism, as well as the extent of the loss experienced by customers, made supervisory authorities interested in the problem, which resulted in issuing to banks a number of directives concerning educating customers and minimizing the risk of fraud at a system level. One of the directives recommended in this matter to payment service providers is using systems based on behavioural biometrics. This modern technological solution allows to verify in real time whether the person logging in to a bank account and performing financial operations is actually the owner of the account. This paper contains strategic diagnosis of this technology by means of a SWOT analysis. This method allowed to identify and assess key internal factors (strengths and weaknesses) and external ones (opportunities and threats), as well as determining the dominant strategy of development on the financial market in Poland. As a result, the authors formed strategic recommendations both for financial institutions and regulators, which may enhance the effectiveness of behavioural biometrics in reducing financial fraud.

Methodology. In the article the qualitative research approach was implemented. The main method of the analysis is the case study of Polish banking sector over the years 2019–2024. Descriptive analysis was used to present the evolution of cyber threats, the extent of financial frauds, as well as regulatory frameworks. The key tool in the research is the SWOT analysis, which allowed to identify strengths and weaknesses of behavioural biometrics, as well as market opportunities and threats. It led to formulating recommendations.

[*] Dr hab., prof. URad., Kierownik Katedry Polityki Ekonomicznej i Bankowości na Wydziale Ekonomii i Finansów Uniwersytetu Radomskiego im. Kazimierza Pułaskiego, https://orcid.org/0000-0003-4466-977X, E-mail: w.macierzynski@uthrad.pl

[**] Dr, Dyrektor Departamentu Usług Cyfrowych w PKO Banku Polskim, analityk w firmie Bankier.pl S.A., założyciel i wieloletni redaktor naczelny serwisu finansowego PRNews.pl i Przeglądu Finansowego Bankier.pl, https://orcid.org/0009-0008-2140-0894, E-mail: michal@macierzynski.pl

Complementarily, secondary data analysis was used. The data derived from reports, publications and statements by the market regulators.

The results of the research. From the perspective of financial institutions, behavioural verification may constitute the key factor in eliminating the most common financial frauds. The most effective approach adopted by banks should be proactive use of internal assets of behavioural biometrics to maximize the benefits from external market opportunities. The biggest challenge and the blocker of the development of this technology is a low level of customer acceptance, and the external threat in the form of restrictive legal and regulatory barriers. In this case, a solution should be changing the present process of obtaining a customer's consent. Connecting the consent with the benefits of convenient using e-banking may considerably increase the index of acceptance, and as a result, eliminate the biggest barrier in the development. It will enable to use the full potential of the solution supported by the development of the sector platform. Although behavioural biometrics plays a lesser role in preventing non-authorised transactions by customers manipulated by criminals, it is an important part of a proactive cybersecurity strategy, especially in the context of the principle of the refund D+1. It is essential in the context of the pressure by regulators which increases the responsibility of banks for fraud transactions.

Practical implications. Behavioural biometrics may become a key tool limiting the extent of financial frauds. If implemented, it increases the level of customer protection, and as a result, allows to reduce the extent of financial frauds, especially those related to taking over a bank account. The biggest benefit connected with this technology is constant, non-invasive verification of a customer's identity in the background. It is an excellent supplement to presently existing anti-fraud systems and solutions. Using sector platform may contribute to a better and faster acceptance, and increasing the efficiency of the security measures used. It will allow banks for a better reaction to incidents, and meeting the regulators' increasing demands concerning protecting customers. However, the success of implementing and using behavioural biometrics depends on solving the problem of legal barriers, market and customers education, without which the technology will remain only a niche solution**.**

Keywords: cybersecurity, financial fraud, behavioural biometrics, e-banking.

JEL Class: G21, G23, G29.

Wstęp

Rozwój współczesnej bankowości cyfrowej odbywa się w otoczeniu szybko rosnącego ryzyka cyberprzestępczości. Przestępstwa finansowe stały się zjawiskiem systemowym w skali globalnej i mają wpływ nie tylko na bezpieczeństwo pojedynczych użytkowników i firm, ale również na stabilność i zaufanie do całego sektora finansowego. Istnieje uzasadniona obawa, że w przyszłości cyberprzestępczość skierowana na usługi finansowe będzie zagrażała nawet rozwojowi państw, zwłaszcza rozwijających się, które nie mają tylu środków, żeby przeciwdziałać skutkom takich przestępstw. Zgodnie z danymi Narodowego Banku Polskiego w latach 2019–2024 wartość oszustw z wykorzystaniem polecenia przelewu w Polsce wzrosła aż dziesięciokrotnie. Wskazuje to na dynamikę tego problemu wynikającą ze skoncentrowania się przestępców na klientach indywidualnych, którzy powszechnie w łańcuchu bezpieczeństwa uznawani są za najsłabsze ogniwo.

W tym kontekście istotną rolę może odegrać biometria behawioralna. Rozwiązanie to umożliwia bieżącą analizę charakterystycznych wzorców zachowań użytkowników podczas korzystania z bankowości elektronicznej. Identyfikacja odstępstw od zarejestrowanego wcześniej profilu umożliwia wykrycie próby nieautoryzowanego dostępu i przejęcia konta. W ten sposób dostarcza bankom dodatkową warstwę zabezpieczeń, działającą równolegle do dotychczasowych metod uwierzytelnienia. Ciągłe monitorowanie sesji uniemożliwia jej przejęcie, a dodatkową i bardzo cenioną zaletą jest też jej nieinwazyjny charakter, który nie wpływa na doświadczenie klienta w korzystaniu z bankowości elektronicznej. Wdrożenie weryfikacji behawioralnej napotyka na istotne bariery prawne i społeczne. Kluczowym wyzwaniem jest konieczność uzyskania świadomej i dobrowolnej zgody klienta na przetwarzanie danych biometrycznych. Zgodnie z Rozporządzeniem o Ochronie Danych Osobowych (RODO) są to dane szczególnej kategorii (Unia Europejska, 2016). Stanowisko Urzędu Ochrony Danych Osobowych jednoznacznie ogranicza możliwość wykorzystania biometrii behawioralnej bez uprzedniej zgody klienta (Lidke, 2024b). Ma to negatywny wpływ na tempo upowszechnienia się tego rozwiązania w rodzimym sektorze bankowym.

Oszustwa finansowe jako systemowe zagrożenie sektora bankowego

Rozwój nowoczesnych usług bankowości elektronicznej w połączeniu z szybkim napływem mniej doświadczonych klientów, który miał miejsce w wyniku pandemii COVID-19, przyczynił się do zwiększenia liczby negatywnych zjawisk. Wśród nich największe znaczenie miał duży wzrost cyberprzestępczości. Większa liczba użytkowników i zdalnych transakcji doprowadziła do gwałtownego wzrostu liczby przestępstw i ataków na użytkowników bankowości cyfrowej. Działania te nasiliły się szczególnie w okresie pandemii COVID-19, czyli od początku 2020 r. Wpływ na to miała również łatwość transferu skradzionych pieniędzy poza granice Polski, wraz z ich wykorzystaniem. Z danych Komendy Głównej Policji wynika, że w 2021 r. stwierdzono 18,3 tys. przestępstw dotyczących kategorii e-bankowości i phishingu (art. 287 Kodeksu karnego). Dla porównania w 2020 r.

było ich 10 tys., czyli nastąpił wzrost o 80%. Jeszcze w 2019 r. policja notowała 9,1 tys. takich przestępstw, w 2018 r. 5,8 tys., a w 2017 r. 4,3 tys. Negatywny trend, który pojawił się w okresie pandemicznym utrwalił się i był widoczny w kolejnych latach. W 2022 r. liczba przestępstw wzrosła do 25,2 tys. I chociaż rok później liczba spadła do ponad 19 tys. (KGP, 2025), to spadek ten mógł jednak wynikać z braku chęci zgłaszania stosunkowo niewielkich strat finansowych oraz z obaw o to, że służby nie będą potrafiły rozwiązać problemu (Cyberdefence24.pl, 2024). Taką sytuację może potwierdzać liczba unikalnych incydentów cyberbezpieczeństwa, rejestrowanych przez CERT Polska. W 2021 r. zarejestrowano łącznie 29,5 tysiąca incydentów, co stanowiło wzrost o 182% w stosunku do roku poprzedniego, kiedy zanotowano ich 10,4 tys. (CERT.PL, 2022). Jeszcze w 2019 r. takich incydentów było niecałe 6,5 tys. Dynamika kolejnych lat wskazuje na narastający problem. W 2022 r. było ich 39,6 tys., w 2023 r. 80,2 tys., a w 2024 r. liczba ta przekroczyła 100 tys. (Bankier.pl, 2025; CERT.PL, 2025). Udostępnione przez policję dane dotyczą zaś jedynie informacji o przestępstwach stwierdzonych, bez uwzględnienia tych, które są jeszcze w toku. Nie wszystkie przypadki są też obligatoryjnie opisywane w katalogach w ramach kategorii e-bankowość czy phishing (Komenda Powiatowa Policji w Kołbucku, 2025). Na rosnącą liczbę przestępstw dotyczących kradzieży środków z rachunków bankowych w powiązaniu z pandemią COVID-19 wskazywał również Rzecznik Finansowy, podkreślając równocześnie, że jest to najczęstsza przyczyna skarg klientów podmiotów rynku finansowego z zakresu naruszeń Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Rzecznik Finansowy, 2021). Sam temat dotyczący nieautoryzowanych transakcji pojawiał się bardzo często w podejmowanych interwencjach Rzecznika w latach 2020–2022. Wskazywał on m.in. na nowe rodzaje ataku, w tym również problem okradzionych klientów z wykorzystaniem tzw. „kredytów na klik" (Rzecznik Finansowy, 2022). O ile do niedawna przestępcy koncentrowali się na atakowaniu klientów mających większe środki na rachunku, to coraz częściej, dzięki szybkiemu postępowi technologicznemu, okradani są również klienci, którzy posiadają zdolność kredytową. Przez internet lub aplikację mobilną w sposób w zasadzie automatyczny klient lub podszywający się pod niego złodziej w ciągu zaledwie kilku minut może zaciągnąć nawet kilkudziesięciotysięczny kredyt. Następnie pieniądze są szybko transferowane na zewnątrz banku. Liczba przestępstw – zarówno takich, jak i omawianych wcześniej – zaczęła rosnąć lawinowo w latach 2021–2022, na co wskazują również dane Narodowego Banku Polskiego z tego okresu. Wynika z nich również, że większość nie jest zgłaszana na policję czy do Rzecznika Finansowego. Ze statystyk NBP, opracowywanych na podstawie danych zbieranych z banków, wynika, że w czwartym kwartale 2019 r. miało miejsce 3007 operacji oszukańczego polecenia przelewu. Dwa lata później liczba takich operacji wzrosła aż czterokrotnie, do 12 069. Na koniec tego samego kwartału 2024 r. było ich blisko 17 tys. Podobnie, jak w przypadku liczby transakcji oszukańczych, NBP raportował również duży wzrost wartości takich operacji – porównując czwarty kwartał 2019 r. i ten sam okres 2024 r. wartość ta wzrosła z 12 aż do 135 mln zł. W latach 2019–2024 wartość oszustw z wykorzystaniem polecenia przelewu wzrosła zatem aż dziesięciokrotnie. Dane te nie uwzględniają transakcji oszukańczych kartami płatniczymi, których liczba jest znacznie wyższa – w 2024 r. średnio

90 tys. operacji kwartalnie (NBP, 2025). Co ciekawe w samej pandemii liczba oszukańczych operacji kartami spadła (NBP, 2022). Wszystkie te straty to efekt wzmożonego działania przestępców. Z raportu zespołu CSIRT działającego przy Komisji Nadzoru Finansowego wynika, że w latach 2019–2024 liczba notowanych incydentów wzrosła w tempie wykładniczym, aż 16-krotnie, z 6 484 do 103 449 (KNF, 2024). Tylko pomiędzy rokiem 2020 a 2021 nastąpił wzrost o ponad 180%. Podobnie było z liczbą blokowanych domen. O ile w 2019 r. zablokowano ich zaledwie 2600, w 2020 r. już 4300, to rok później liczba phishingowych domen wzrosła do 11,5 tys. W 2024 r. zgłoszono do blokady ponad 51 tys. domen. W tym czasie zmienił się również tzw. wektor ataków z podszywania się pod banki na oferowanie fałszywych inwestycji.

Zmiana paradygmatu cyberprzestępczości. Socjotechnika jako kluczowe narzędzie oszustw finansowych

Transformacja cyfrowa instytucji finansowych, która przyspieszyła po pandemii COVID-19, w połączeniu z regulacjami wzmacniającymi bezpieczeństwo systemowe banków spowodowała znaczące polepszenie rozwiązań operacyjnych i technologicznych po stronie banków i innych dostawców usług płatniczych. Ataki na banki są trudne do przeprowadzenia i wymagają ogromnego doświadczenia oraz środków finansowych.

Zwiększenie cyberbezpieczeństwa klientów, które miało miejsce po powszechnym wprowadzeniu dodatkowych metod autoryzacji i identyfikacji, było efektem zastosowania w 2015 r. dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego UE, powszechnie określaną jako PSD2 (Unia Europejska, 2015). Dyrektywa została stworzona między innymi w celu lepszego zabezpieczenia danych i pieniędzy klientów, tak żeby mogli bez obaw przeprowadzać transakcje w internecie. W bankowości i płatnościach elektronicznych wprowadzono wymóg stosowania silnego uwierzytelniania klientów, z nielicznymi i jasno wskazanymi wyjątkami od tej reguły. Ta najbardziej odczuwalna i początkowo krytykowana zmiana polegała na podwyższeniu poziomu weryfikacji tożsamości klienta. W praktyce znacząco wydłużało to proces logowania do serwisów bankowości internetowej oraz procesy płatności dokonywanych na przykład kartami płatniczymi (SEON, 2025; Clever Advice, 2019). Silne uwierzytelnianie klienta (SCA – *Strong Customer Authentication*) to kluczowy mechanizm bezpieczeństwa, który ma na celu redukcję ryzyka oszustw w transakcjach elektronicznych. Jest to proces uwierzytelniania klienta oparty na co najmniej dwóch niezależnych elementach z kategorii: wiedzy, posiadania i cech klienta. Mechanizmy te podlegają wymogom technicznym, które wprowadziły obowiązek dynamicznego powiązania kodu autoryzacyjnego z parametrami konkretnej transakcji. Mechanizm wprowadza wymagania co do tego, żeby klient otrzymał informację o kwocie i odbiorcy przed autoryzacją, a sam kod autoryzacyjny był unikalny dla danej transakcji oraz by jakakolwiek modyfikacja parametrów transakcji unieważniała kod (Unia

Europejska, 2018). Ogromną zmianą było wprowadzenie praktyki stosowania co najmniej dwóch elementów należących do wspomnianych wcześniej kategorii:

- wiedza – coś, co wie wyłącznie użytkownik (ciągi znaków używane jako ustalone hasło),
- posiadanie – coś, co posiada wyłącznie użytkownik (używane w połączeniu z hasłami jednorazowymi przekazywanymi za pośrednictwem telefonu lub aplikacji mobilnej, np. karta płatnicza, token, ale również komputer lub telefon),
- cechy klienta – coś, co jest charakterystyczne wyłącznie dla użytkownika (np. biometria, odcisk palca).

Celem stosowania się do tych wymogów przez wydawców instrumentów płatniczych oraz podmiotów świadczących usługi *acquiringu* było podwyższenie poziomu bezpieczeństwa w transakcjach elektronicznych (Tomczyk, 2023). Wzmocnienie zabezpieczeń skłoniło przestępców do rozwoju innych sposobów kradzieży i przeprowadzania oszustw. W konsekwencji na całym świecie można zaobserwować znaczący wzrost oszukańczych transakcji wykorzystujących manipulację i różnego rodzaju narzędzia socjotechniki skierowane w szczególności do osób fizycznych, określanych mianem najsłabszego ogniwa w łańcuchu bezpieczeństwa (Barrett, 2003). Na rozwój takich oszustw miała też wpływ pandemia COVID-19, w czasie której część osób, wcześniej wykluczonych z korzystania z bezgotówkowych instrumentów płatniczych, w szczególności starszych i mniej obeznanych z rozwiązaniami cyfrowymi, zaczęła masowo korzystać z zakupów online, bankowości elektronicznej i płatności cyfrowych. Osoby te, posiadając mniejszą wiedzę o ryzykach i zagrożeniach związanych ze stosowaniem instrumentów płatniczych, nie rozpoznają prawidłowo prób przestępczych. Tacy klienci korzystają często z komputerów i urządzeń słabiej zabezpieczonych przed atakami przestępców, którzy sugestywnie zachęcają ich do instalowania złośliwego oprogramowania (np. przez SMS lub e-mail) czy złośliwego pulpitu na komputerze posiadacza rachunku. Tego rodzaju ataki można podzielić na trzy podstawowe grupy oszustw:

1. Przestępstwa polegające na przejęciu dostępu do rachunku płatniczego. Może to mieć miejsce w wyniku kradzieży lub przywłaszczenia danych, na przykład w skutek pozyskania takich informacji w wyniku manipulacji i zastosowania technik socjotechnicznych lub też w wyniku wycieku wrażliwych informacji dotyczących konta. Przestępca wykorzystuje te informacje w celu wyprowadzenia środków finansowych z tak przejętego rachunku. Tego rodzaju ataki są dużo trudniejsze do przeprowadzenia od czasu wdrożenia zaleceń dyrektywy PSD2. Z tego też względu obecnie funkcjonują w połączeniu z innymi działaniami, mającymi na celu wyłudzenie narzędzia autoryzacyjnego lub skłonienie do akceptacji zmanipulowanego użytkownika.
2. Przestępstwa polegające na zmanipulowaniu użytkownika i zachęceniu go do zainstalowania oprogramowania umożliwiającego dostęp do rachunku płatniczego z wykorzystaniem tzw. zdalnego pulpitu na urządzeniu posiadacza rachunku oraz wyprowadzeniu środków

pieniężnych. Również w takim przypadku wymagana jest interakcja przestępcy z nieświadomym takiego działania klientem instytucji finansowej.

3. Przestępstwa polegające na zmanipulowaniu posiadacza rachunku przez przestępcę podszywającego się np. za pracownika instytucji finansowej lub policji i skłonieniu go do niekorzystnego rozporządzenia swoim majątkiem. W takim przypadku to sam klient dokonuje samodzielnie autoryzacji transakcji, np. przelewu środków pieniężnych na wskazany rachunek płatniczy, podaje kod BLIK i autoryzuje transakcję czy wpłaca we wpłatomacie pieniądze na rachunek przestępcy. W każdym takim przypadku zmanipulowany płatnik uważa, że przelew jest dokonywany na rachunek uprawnionego odbiorcy.

Oszustwa wykorzystujące socjotechnikę cały czas ewoluują. Po wstępnym zainteresowaniu ofiary, przestępcy kontaktują się bezpośrednio – czy to przez telefon, czy komunikator – nakłaniając do bardziej skomplikowanych działań, które ostatecznie mają na celu wyłudzenie i kradzież pieniędzy. Coraz częściej zmanipulowane ofiary same przelewają środki na wskazane konta i rachunki, do samego końca nie mając świadomości oszustwa. Skalę tego zjawiska potwierdzają dane publikowane przez NBP (NBP, 2025). Zmieniając od 2024 r. metodologię agregowanych danych, uwzględniono szerszy zakres rodzajów transakcji oszukańczych, w tym przede wszystkim oszustwa powstałe w wyniku zmanipulowania płatnika. W przypadku fraudów z wykorzystaniem polecenia przelewu w 2024 r. banki zaraportowały straty na poziomie 557,5 mln zł (140 mln USD). Jak się okazuje, oszustwa wynikające z manipulacji płatnikiem odpowiadały za zdecydowaną większość, bo średnio 70% wartości wszystkich zaraportowanych oszustw (62% w I, 67% w II, 75% w III i 77% w IV kwartale 2024 r.). Uwzględniając transakcje oszukańcze na kartach płatniczych, łączne straty w 2024 r. wynosiły w Polsce 654 mln zł, z czego 394 mln zł (60%) wynikały z manipulacji płatnikiem. Dla porównania w Wielkiej Brytanii w tym samym okresie było to ok. 38% (Harley-McKeown, 2025). Dane te wskazują jednoznacznie, że największym wyzwaniem sektora bankowego w Polsce są przede wszystkim oszustwa dokonywane przez samych klientów, zmanipulowanych i wprowadzonych w błąd przez przestępców.

Zalecenia nadzorcze jako odpowiedź na rosnące zagrożenia cyberprzestępczości

Rosnąca liczba przestępstw i wartość utraconych środków, które znacząco zwiększyły się wraz z wykorzystaniem przez przestępców nowych metod manipulacji socjotechnicznej użytkowników, wzbudziły duże zainteresowanie administracji państwowej, w tym przede wszystkim Urzędu Komisji Nadzoru Finansowego oraz Urzędu Ochrony Konkurencji i Konsumentów. W lutym 2021 r. przewodniczący KNF w liście skierowanym do sektora bankowego podkreślił, że dostawcy usług finansowych powinni konsekwentnie stosować paradygmat określany jako *security first*. W praktyce miało to oznaczać stawianie kwestii bezpieczeństwa na pierwszym miejscu. Wdrażając nowe usługi, banki i pozostałe instytucje finansowe powinny brać pod uwagę istniejące i nowe trendy ataków,

sposoby działania cyberprzestępców, a także ryzyka wynikające z planowanych przez dostawcę działań, nie tylko wobec swoich klientów, ale również w kontekście potencjalnego wpływu tych działań na cały sektor usług (Jastrzębski, 2021). Pismo przewodniczącego KNF jest przykładem tzw. miękkiej rekomendacji. Chociaż nie miało wiążącego charakteru dla banków, jak wydawane przez Urząd rekomendacje, to w praktyce ma podobne znaczenie. Sam ten fakt dowodzi, jak ogromne znaczenie Komisja kładzie na zagadnienie cyberbiezpieczeństwa i edukacji. Większość instytucji na bieżąco reaguje na nowe formy ataków, informując o tym swoich użytkowników poprzez zamieszczanie na swoich stronach internetowych odpowiednich komunikatów i alertów. W opinii KNF działania te są jednak niewystarczające i nie przynoszą spodziewanych efektów, o czym świadczy skala skutecznych ataków na użytkowników usług bankowych i związany z tym poziom fraudów. Według Urzędu banki nie powinny się też koncentrować wyłącznie na swoich klientach, ale prowadzić szeroką kampanię dotyczącą cyberbezpieczeństwa (Forsal.pl, 2021). Również w 2021 r. prezes Urzędu Ochrony Konkurencji i Konsumentów wszczął postępowanie wyjaśniające, w ramach którego Urząd miał sprawdzić, jak banki rozpatrują reklamacje konsumentów związane z kradzieżą pieniędzy z konta oraz jakie stosują mechanizmy uwierzytelniania transakcji. Wezwania do przedstawienia wyjaśnień i przekazania dokumentów w tych sprawach zostały wysłane do osiemnastu banków (UOKiK, 2021). Powodem takiego działania była rosnąca liczba skarg od konsumentów dotyczących kradzieży pieniędzy z konta lub zaciągnięcia zobowiązania na ich dane. Klienci zgłaszali do UOKiK problem utraty oszczędności oraz nieuznawania reklamacji przez banki. Same zgłoszenia dotyczyły między innymi podszywania się przez oszustów pod pracownika infolinii banku, wykorzystywania fałszywej strony internetowej banku czy oprogramowania szpiegującego w celu wyłudzenia danych. Postępowaniem wyjaśniającym objęto w zasadzie wszystkie największe banki komercyjne w Polsce. Zebrany w ciągu roku materiał dowodowy pozwolił postawić pierwszym bankom zarzuty naruszania zbiorowych interesów konsumentów. W toku postępowania wyjaśniającego, prezes UOKiK ustalił również, że banki mogły wprowadzać w błąd w odpowiedziach na reklamacje dotyczące nieautoryzowanych transakcji. Jest to o tyle istotne, ponieważ za naruszenie zbiorowych interesów konsumentów bankom grożą kary nawet do 10% obrotu (UOKiK, 2024). UOKiK nakazał również, by banki zwróciły klientom pieniądze z tytułu nieautoryzowanych transakcji w terminie D+1, czyli do końca następnego dnia roboczego po zgłoszeniu nieautoryzowanej transakcji. Urząd powołał się na art. 46 Ustawy o usługach płatniczych (Dziennik Ustaw, 2011) będącej implementacją przepisów unijnych. Obowiązek ten został potwierdzony w oficjalnych komunikatach UOKiK, m.in. w 2022 r. i 2024 r., kiedy zostały wszczęte postępowania wobec kilku banków za bezprawną odmowę zwrotu środków w wymaganym przez Urząd terminie (UOKiK, 2022b; UOKiK, 2024). Wyjątki od tej zasady dotyczą jedynie sytuacji, kiedy zgłoszenie nastąpiło później niż 13 miesięcy po transakcji lub istnieje uzasadnione podejrzenie oszustwa ze strony klienta. W takim przypadku, jeśli bank ma takie podejrzenie, musi obowiązkowo zawiadomić organy ścigania. Podobne podejście do zwrotu środków w terminie D+1 zaprezentował Rzecznik Finansowy (2023). Również UKNF co do zasady przychylił

się do takiego podejścia, zwracając jednak uwagę na konieczność walki z przestępczością w obszarze płatności elektronicznych. Komisja wskazała na potrzebę zrównoważenia ochrony konsumentów, z jednoczesnym rozwijaniem przez sektor bankowy mechanizmów prewencyjnych.

Celem szeregu zaleceń opracowanych dla banków przez UOKiK jest zwiększenie skuteczności walki ze zjawiskiem nieautoryzowanych transakcji płatniczych. Szczególne znaczenie ma przy tym wykorzystanie nowoczesnych technologii, w tym stosowanie systemów opartych na sztucznej inteligencji lub biometrii behawioralnej, która może być skutecznym narzędziem zwiększającym bezpieczeństwo transakcji oraz elementem wieloskładnikowego uwierzytelnienia klienta. Biometrię behawioralną, zdaniem Urzędu, można stosować nie tylko przy logowaniu, ale również przy skracaniu okresu tzw. funkcji *cooling period*, czyli opóźnienia wykonania transakcji od złożenia dyspozycji w systemie przez klienta do czasu jej wykonania przez dostawcę. Jest ona rekomendowana ze względu na maksymalne ograniczenie ryzyka ingerencji osoby trzeciej. Podobne zastosowanie biometrii behawioralnej zalecane jest przy okazji aktywacji w bankowości mobilnej lub internetowej funkcji uprzednio niedostępnej lub samodzielnie zablokowanej przez konsumenta.

Charakterystyka i zasada działania biometrii behawioralnej

W kontekście wymienionych zagrożeń rozwiązaniem, które pozwala na skuteczną, a przy tym nieinwazyjną ochronę klienta, jest biometria behawioralna. Biometria to nauka rozpoznawania jednostek na podstawie ich fizycznych lub behawioralnych cech (Jain i in., 2006). Wykorzystując technologię cyfrową można identyfikować i weryfikować osoby na podstawie ich cech fizycznych lub behawioralnych.

Przystępując do analizy zastosowania biometrii w systemach bankowych, należy doprecyzować pojęcie identyfikacji i uwierzytelnienia, ponieważ ich definicje różnią się w zależności od dziedziny. W obszarze bezpieczeństwa informatycznego proces identyfikacji polega na przedstawieniu przez użytkownika deklaracji swojej tożsamości. Najczęściej dzieje się to poprzez podanie unikalnego identyfikatora jakim jest na przykład login. Uwierzytelnienie jest w tym przypadku weryfikacją i potwierdzeniem, że użytkownik jest tym, za kogo się podaje. W literaturze przedmiotu dotyczącej biometrii behawioralnej pojęcia te funkcjonują w nieco innym znaczeniu. Identyfikacja biometryczna oznacza porównanie próbki z całą bazą danych wzorców w celu ustalenia tożsamości nieznanej osoby, a weryfikacja oznacza z kolei porównanie próbki z jednym, konkretnym wzorcem biometrycznym przypisanym do konkretnej tożsamości(Kałużny i Stolarski, 2019). Dla zachowania przejrzystości i spójności artykułu, przyjęto konwencję stosowaną praktyce cyberbezpieczeństwa systemów IT. W takim przypadku biometria behawioralna pełni funkcję narzędzia uwierzytelnienia. Oznacza to, że w procesie klient najpierw dokonuje identyfikacji w momencie podania loginu, a następnie przechodzi proces uwierzytelnienia podając hasło. Biometria jest w tym przypadku dodatkową, działającą w tle

warstwą zabezpieczeń, która w sposób ciągły weryfikuje użytkownika. Służy do potwierdzenia, że osoba zalogowana jest prawowitym właścicielem rachunku.

Tradycyjna biometria opiera się na niezmiennych cechach fizycznych użytkownika i jest stosowana głównie do jednorazowej identyfikacji lub weryfikacji. Biometria behawioralna analizuje i profiluje zachowania użytkowników, takie jak sposób korzystania z urządzeń np. telefonu, tempa pisania na klawiaturze czy charakterystycznych ruchów myszą (Karnan i in., 2011). Liczba indywidualnych cech jest znacznie szersza i wraz z rozwojem technologii oraz urządzeń cały czas rośnie. W ramach analizy behawioralnej może być badanych łącznie nawet kilkaset różnych czynników.

Istotną cechą zastosowania biometrii behawioralnej jest fakt, że ocena zgodności zebranych danych z przechowywanym wzorcem nie musi być zawsze taka sama i jednoznaczna. Dzieje się tak nie tylko zarówno w przypadku pojedynczego zalogowania, ale również w czasie trwania dłuższej sesji, w czasie której zgodność ta może ulegać zmianom. Dynamika korzystania z klawiatury komputera i ruchu myszki, czy korzystania ze smartfonu, może się różnić w zależności od pory dnia pomiędzy różnymi dniami w dłuższym okresie, a także może być uzależniona od wielu różnych czynników zewnętrznych. Przykładowo może to być korzystanie z telefonu w autobusie, złamana ręka, zmieniona myszka komputerowa etc. Pomimo takiej zmienności nowoczesne systemy biometryczne dostosowują się do nowych warunków, a także wykazują zgodność w sposób powtarzalny w większości badanych przypadków. Potencjalne zmiany zachowania, po przednim potwierdzeniu dodatkową autoryzacją, rozbudowują profil użytkownika, dając również wsad do ogólnego wzorca zmian.

Zastosowanie biometrii behawioralnej w przeciwdziałaniu fraudom i przejęciom kont

Stosując biometrię behawioralną, bank ma możliwość wykrycia różnic w zachowaniu użytkownika oraz odróżnić zachowania przestępcy od zachowania posiadacza rachunku, którego wzorzec dla celów porównawczych wcześniej pozyskał. Pozwala mu to na podjęcie odpowiedniej reakcji, czy to blokady dostępu do rachunku czy konkretnej transakcji, do czasu uzyskania dodatkowego uwierzytelnienia. Istotną zaletą takiego rozwiązania jest również działanie w tle, które nie wpływa na codzienne korzystanie z kanałów zdalnych, a także ochrona wszystkich klientów, również takich, którzy cechują się mniejszym poziomem świadomości zagrożeń i w konsekwencji utraty dostępu do rachunku. Biometria może być jednocześnie wykorzystywana równolegle razem z innymi rozwiązaniami zabezpieczającymi dostęp do bankowości elektronicznej, takimi jak silne uwierzytelnienie klienta, *device fingerpinting*, analiza ryzyka transakcji etc.

W stosunku do innych rodzajów zabezpieczeń biometria behawioralna z punktu widzenia sektora finansowego posiada niewątpliwe zalety. Należą do nich:

1. Ciągła weryfikacja tożsamości użytkownika. W przeciwieństwie do standardowych metod uwierzytelniania, w tym klasycznej biometrii, weryfikujących tożsamość w momencie logowania lub autoryzacji transakcji, biometria behawioralna umożliwia stałe

monitorowanie zachowania użytkownika podczas całej sesji (PingIdentity.com, n.d.), natychmiastowe wykrywanie ewentualnych anomalii wskazujących na nieautoryzowane przejęcie dostępu (Ghiciuc, 2024) oraz działanie w tle bez ingerencji w doświadczenie użytkownika. Znacząco zwiększa to bezpieczeństwo, eliminując lub ograniczając ataki polegające na przejęciu sesji, czy oszustwa zdalnego dostępu. W takim przypadku system wykryje nagłe anomalie, czego nie są w stanie tak dobrze zatrzymać czy wyśledzić inne stosowane przez banki metody, takie jak *device fingerpinting* czy silna identyfikacja klienta.

2. Skuteczność w wykrywaniu zaawansowanych oszustw. Biometria behawioralna jest szczególnie skuteczna w wykrywania ataku typu *Account Takeover Fraud*, w którym oszust przejmuje konto ofiary, posiadając prawidłowe dane do logowania (Mórawski, 2023). W połączeniu z innymi danymi analiza biometryczna może też przyczynić się do identyfikacji manipulacji socjotechnicznych. Ofiara ataku działa pod wpływem manipulacji, a jej zachowanie w stresie różni się od standardowego wzorca (Lidke, 2024a). Wykorzystując żyroskop aplikacji mobilnej banku, wymaganej do autoryzacji przelewu lub dzięki współpracy z telekomami, bank może sprawdzić, czy klient podczas korzystania z bankowości elektronicznej prowadzi równolegle rozmowę telefoniczną. Pomaga to wytypować podejrzane transakcje. Mimo licznych fałszywych sygnałów, tzw. *false positive*, klienci, którzy wyrazili zgodę na wykorzystanie analizy behawioralnej, padają wielokrotnie rzadziej ofiarą oszustów niż pozostali (Baglajewski, 2024).
3. Skuteczny i samouczący się mechanizm działania. Biometria behawioralna działa efektywnie ze względu na jej zaawansowane mechanizmy samo uczenia, oparte na uczeniu maszynowym. Systemy te tworzą indywidualny profil zachowania każdego, pojedynczego użytkownika. Pozwala to stworzyć charakterystyczne wzorce interakcji użytkownika z urządzeniem, a także analizy mikrozachowań, takich jak: dynamika korzystania z klawiatury, sposób trzymania telefonu, tempo pisania, etc. Wzory te dostosowują się do zmieniającego się wieku, miejsca korzystania z urządzenia, etc. W połączeniu z automatycznymi reakcjami na anomalie, takimi jak możliwość zablokowania lub spowolnienia wykonania podejrzanych transakcji, daje to czas na dodatkowe uwierzytelnienie użytkownika oraz ewentualną aktualizację jego profilu. Ten sposób pozwala lepiej zweryfikować klientów w sytuacji, w której mogą dobrze nie działać inne zabezpieczenia, takie jak *device fingerprinting*. Niezależnie czy klient loguje się na danym urządzeniu pierwszy raz, korzysta z VPN, czy czyści ciasteczka w przeglądarce, jego indywidualny profil behawioralny umożliwia bankowi łatwiejszą identyfikację użytkownika, a tym samym zwiększa skuteczność stosowanych zabezpieczeń.
4. Możliwość sektorowego współdzielenia informacji pomiędzy uczestnikami centralnej platformy technologicznej. Biometria behawioralna umożliwia szybką i skuteczną wymianę informacji pomiędzy bankami w celu wykrywania nieautoryzowanych transakcji. Model taki

pozwala na wymianę informacji o wzorcach zachowań pomiędzy wszystkimi użytkownikami oraz zwiększa skuteczność wykrywania fraudów. Oszust, przejmujący konto w jednym banku, jest łatwo i automatycznie identyfikowany w drugim – nie tylko w kontekście logowania danymi klienta, ale również w przypadku podszywania się pod niego, na przykład w celu wyłudzenia kredytu czy założenia rachunku bankowego (Uryniuk, 2024a).

Ważną cechą biometrii behawioralnej jest fakt, że ocena zgodności zebranych danych z przechowywanym wzorcem nie jest zawsze taka sama i jednoznaczna. System przy każdym logowaniu klienta porównuje zebraną próbkę z posiadanym uprzednio wzorcem. W ten sposób za każdym logowaniem, bazując na stopniu prawdopodobieństwa, wyliczany jest poziom zgodności. Może on za każdym razem nieco się różnić. Chcąc zwiększyć poziom bezpieczeństwa bank może wymagać wysokiego poziomu zgodności próbki z wzorcem. Występująca zmienność tego parametru może w takim przypadku prowadzić do zbyt częstego, niezamierzonego blokowania klientów (*False Rejection Rate*). Niższy wskaźnik akceptacji prowadzi z kolei do zwiększenia ryzyka nieautoryzowanego dostępu, czyli wpuszczenia do systemu bankowego oszusta (*False Acceptance Rate*). To znany od początku bankowości elektronicznej dylemat, jakim jest znalezienie odpowiedniego balansu pomiędzy skuteczną ochroną przed cyberprzestępcami, a wygodą klienta. Zbyt restrykcyjne podejście prowadzi do wymogu częstego, dodatkowego potwierdzania wykonywanych operacji lub wręcz do blokowania kanałów dostępu. Biometria behawioralna bardzo dobrze sprawdza się jako dodatkowy, ale nie jedyny element systemu zabezpieczeń. Stosowane w niej rozwiązania pozwalają procentowo określić, czy w danej chwili z systemu korzysta właściwy użytkownik, czy też ktoś, kogo wzorce zachowań znacząco różnią się od stworzonego wcześniej indywidulanego profilu behawioralnego. W przypadku rozwiązania sektorowego możliwe jest dodatkowo łatwiejsze wykrycie przestępcy, który przejąwszy tożsamość ofiary wykorzystuje jej dane do rozpoczęcia relacji, czyli założenia konta bankowego lub zaciągnięcia kredytu przez internet. Wykorzystanie biometrii behawioralnej pozwala bankom na elastyczność i znalezienie punktu przecięcia (*Equal Error Rate*) w zależności od zbieranych w sposób ciągły danych i kontekstu transakcji. Rozwiązanie to dostarcza cały czas procentowy wskaźnik zgodności, który w praktyce można interpretować w trzystopniowej skali: wysokiego, średniego i niskiego zaufania. Pozwala to na optymalizację procesu doświadczenia klienta, przy zachowaniu wysokiego poziomu cyberbezpieczeństwa. Systemy antyfraudowe mogą w ten sposób być bardziej restrykcyjne w przypadku przelewów wysokokwotowych lub odbiegających od reguły i odpowiednio mniej, jeśli klient dokonuje typowe operacje. Zwiększa to ergonomię korzystania z systemów bankowości elektronicznej, bez zmniejszania ochrony przed przestępcami.

Skuteczność zabezpieczania klienta rośnie wraz z połączeniem biometrii behawioralnej z innymi, równolegle funkcjonującymi rozwiązaniami. Dodatkowe i niezależne od innych reguł dane, zwiększają skuteczność systemów antyfraudowych. Przykładem takiego rozwiązania jest powszechnie stosowany od czasów wdrożenia PSD2 rozwiązanie *device fingerprintingu*, czyli tzw. zaufanego

urządzenia. Ta technologia identyfikacji i śledzenia urządzenia bazuje na kombinacji atrybutów urządzenia i przeglądarki, z której korzysta klient. W połączeniu z tradycyjnymi atrybutami, takimi jak pliki cookies czy adresacja IP, tworzy indywidualny cyfrowy identyfikator urządzenia. W ten sposób system może wykryć, czy logowanie następuje z tego samego komputera co zazwyczaj czy z innego lub zidentyfikować nietypowy wzorzec dostępu. Wszystko to, w połączeniu z zebranymi przez system biometrii behawioralnej informacjami, ułatwia wykrycie potencjalnego, nieautoryzowanego dostępu do rachunku. W takim przypadku może nastąpić zablokowanie dostępu do bankowości elektronicznej lub wymuszenie dodatkowej weryfikacji klienta. Dzięki utworzonemu w ten sposób miksowi technologicznemu bank chroni swoich klientów przed przejęciem konta, a tym samym przed transakcjami oszukańczymi. Tego typu mechanizm można implementować również w innych rozwiązaniach, na przykład do ochrony płatności kartą w internecie. Obecnie w Unii Europejskiej wymagana jest dodatkowa autoryzacja z wykorzystaniem standardu 3-D Secure, czyli dodatkowego narzędzia autoryzacji dostarczonego przez bank. Zaimplementowanie biometrii behawioralnej może stanowić ważny system zabezpieczeń, wskazujący na użycie karty przez osobę nieuprawnioną.

Bariery upowszechnienia biometrii behawioralnej i perspektywy rozwoju

Biometria behawioralna w sposób istotny jest w stanie zwiększyć bezpieczeństwo klienta i banku oraz skutecznie przeciwdziałać oszustwom, nie zakłócając przy tym doświadczenia użytkownika (UX). Pierwsze wdrożenie biometrii behawioralnej w formie testów w polskim sektorze bankowym miało miejsce na przełomie 2018 r. i 2019 r. Projekt został zrealizowany przez mBank we współpracy z Centrum Bezpieczeństwa Cyfrowego S.A., spółką z portfela funduszu mAkcelerator (mBank, 2018). Na początku 2020 r. z tego samego rozwiązania zaczął korzystać ING Bank Śląski (Ostrowska, 2020), nieco później, w 2023 r., takie rozwiązanie wdrożył BNP Paribas, rok później Velo Bank, PKO Bank Polski oraz SKOK Stefczyka, a w 2025 r. – Credit Agricol Polska. Poza ostatnim bankiem, wszystkie instytucje korzystają z rozwiązania firmy Digital Fingerprint, która w 2022 r. została przejęta przez Biuro Informacji Kredytowej (Mamstartup.pl, 2022; BANK.pl, 2022). Pierwsze wdrożenia biometrii behawioralnej w mBank i ING Bank Śląski były realizowane w formie pilotażowej. Korzystać z takiego rozwiązania mogli jedynie klienci, którzy wcześniej przystąpili do pilotażu. Taki model współpracy pozwalał na bezpieczne przetestowanie nowej technologii na środowisku produkcyjnym, przy większym obciążeniu. W kontrolowany sposób można było dostosować wszystkie systemy antyfraudowe i reguły bezpieczeństwa. W komunikacie informującym o wdrożeniu, mBank podkreślał etyczność wprowadzonego rozwiązania. Klienci zainteresowani usługą, przed przystąpieniem do korzystania, musieli wyrazić zgodę na udział w pilotażu. Bank nie obejmował nią osób, które tego nie chciały. Jak informowano, w ramach biometrii behawioralnej oferowanej przez Digital Fingerprints, system miał analizować wyłącznie sposób interakcji klientów z urządzeniami podczas korzystania z usług bankowości elektronicznej mBanku. Nie pobierano danych na temat

korzystania z innych stron czy narzędzi. W komunikacji podkreślano jednocześnie, że rozwiązanie sprawdza, jak użytkownik korzysta z serwisu banku, a nie to, co w nim robi, a także fakt, że dane zbierane na potrzeby budowy profili behawioralnych nie zawierają żadnych wrażliwych informacji. Same profile były przechowywane w formie modeli matematycznych, które uniemożliwiają przechowującej je spółce oraz innym podmiotom identyfikację konkretnej osoby. Samemu użytkownikowi usługi przysługiwało prawo do zapomnienia, czyli usunięcia jego danych (Palczewski, 2018). Tego typu podejście do oferowania biometrii behawioralnej jest typowe dla większości banków wprowadzających tę usługę. Klient jest zachęcany do aktywacji usługi, która wymaga wyrażenia jednoznacznej zgody, w tym akceptacji regulaminu.

Mimo niewątpliwych zalet wynikających z korzystania z biometrii behawioralnej, odsetek klientów objętych tym rozwiązaniem w bankach, które go wprowadziły, jest stosunkowo niski. W ING Banku Śląskim po 3 latach od wdrożenia wynosił on 27% (CCNews, 2024). mBank, który jako pierwszy wprowadził takie rozwiązanie nie informował publicznie o liczbie klientów objętych taką usługą, jednak z zagregowanych informacji o całym rynku, które były prezentowane na Konferencji Antyfraudowej BIK 2024 wynikało, że procent ten był znacznie niższy niż w ING Banku Śląskim (Wójciecki, 2024). Analiza danych wykazała również, że taką usługę włączały przede wszystkim osoby, które już wcześniej były bardziej świadome zagrożeń w sieci. Tacy klienci stanowili przy tym minimalny odsetek wśród wszystkich oszukanych klientów ING Banku Śląskiego – było to mniej niż 4%, a w niektórych miesiącach ich udział spadał poniżej %. W rezultacie takiej sytuacji użytkownicy, którzy nie korzystają z rozwiązania biometrii behawioralnej, to jednocześnie klienci, którzy ze względu na poziom wiedzy i doświadczenia w korzystaniu z usług cyfrowych są bardziej narażeni na działania przestępców. Na włączenie nowej usługi decydują się dopiero w momencie, kiedy zostaną oszukani (Uryniuk, 2023).

Wśród wyzwań związanych z wdrożeniem i funkcjonowaniem biometrii behawioralnej, za najważniejsze uważa się niechęć klientów do udzieleniem zgody na korzystanie z takiego rozwiązania. Innym wyzwaniem jest duża liczba sesji klienckich bez pozyskania danych, na przykład w sytuacji logowania się na konto z nowego telefonu. Budowa profilu biometrycznego klienta wymaga co najmniej kilku logowań. Dopiero wówczas pozyskane dane stanowią dobrą podstawę do prawidłowej weryfikacji tożsamości. Technologia zastosowana w bankowości mobilnej różni się dodatkowo od tej, która jest wykorzystywana na komputerze. Jest to o tyle duże wyzwanie, że coraz większa część klientów to tzw. klienci *mobile only*, którzy tylko w wyjątkowych sytuacjach korzystają z bankowości internetowej, a nawet jeśli już, to korzystają z niej na telefonie komórkowym, a nie na komputerze stacjonarnym. Systemy mają również problem w sytuacji współdzielenia loginu do rachunków, na przykład przez współmałżonków. Taka sytuacja powoduje, że generowana jest duża liczba fałszywych alarmów, kiedy prawowity użytkownik konta jest weryfikowany negatywnie. Wszystkie te elementy powodują, że pomimo teoretycznie wysokiej skuteczności biometrii behawioralnej, w praktyce jedynie ograniczona liczba klientów jest objęta taką ochroną – znacznie niższa niż sama liczba pozyskiwanych zgód. Wynika to z jednej strony z długotrwałego procesu budowania profilu, z drugiej strony z wielu sytuacji, które

wywołują fałszywe alarmy. W takim przypadku brak dodatkowego, skutecznego i taniego sposobu potwierdzania tożsamości klienta tworzy ogromne wyzwania przy zastosowaniu biometrii behawioralnej jako masowej, silnej metody weryfikacji. W konsekwencji rozwiązanie to staje się niszowe. Wymaga zgody klienta, a później stosunkowo długiego okresu budowania jego profilu. Okres ten może trwać nawet do kilku miesięcy i jest uzależniony od częstotliwości logowania się klientów do serwisu bankowości internetowej.

Biorąc pod uwagę wszystkie te elementy oraz koszty związane z wdrożeniem, utrzymaniem oraz promocją wśród klientów takiego rozwiązana, należy dojść do wniosku, że pomimo niewątpliwych zalet biometrii behawioralnej w codziennym jej zastosowaniu, wydaje się ona mało skuteczna i nieefektywna. Główną barierą w jej wykorzystaniu jest przede wszystkim wymóg pozyskania dobrowolnej i świadomej zgody od klienta. Wynika to z faktu, że korzystanie z takiej technologii stanowi głęboką ingerencję w prawo do prywatności osób fizycznych, które jest zagwarantowane w art. 8 ust. 1 Karty Praw Podstawowych Unii Europejskiej (Unia Europejska, 2012), art. 47 i art. 51 Konstytucji RP (Zgromadzenie Narodowe, 1997) oraz w Rozporządzeniu Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. (Unia Europejska, 2016). w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Dane biometryczne traktowane są jako dane szczególnej kategorii w rozumieniu art. 9 ust. 1 RODO w zw. z art. 6 RODO. Zgodnie z definicją danych biometrycznych, zawartą w art. 4 pkt 14 RODO, pojęcie „dane biometryczne" oznacza dane, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby. To zaś oznacza, że poza odstępstwem związanym z ważnym interesem publicznym, użytkownik musi być w pełni poinformowany i wyrazić zgodę na przetwarzanie takich danych. Taka zgoda musi wyraźnie odróżniać się od pozostałych kwestii poruszanych w umowie z klientem, a osoba, której dane dotyczą, musi wyraźnie ją zaakceptować. Nie może to być zatem zgoda domniemana, a odmowa nie powinna wpływać niekorzystnie na sytuację klienta. Takie stanowisko polskiego Urzędu Ochrony Danych Osobowych z marca 2024 r. w zasadzie zamyka drogę do upowszechnienia biometrii bez zgody klienta, tak jak chciały to banki, bazując na podstawie art. 10 Ustawy o usługach płatniczych (Uryniuk, 2024b). Wskazuje on, że dostawcy, organizacje płatnicze i podmioty prowadzące systemy płatności przetwarzają dane osobowe w zakresie niezbędnym do zapobiegania oszustwom związanym z wykonywanymi usługami płatniczymi, prowadzeniem schematu płatniczego lub prowadzeniem systemu płatności oraz dochodzenia i wykrywania tego rodzaju oszustw przez właściwe organy. UODO stwierdzając, że dane behawioralne to dane biometryczne potwierdził, że banki nie mogą ich wykorzystać bez zgody klienta (Lidke, 2024b).

Mając na uwadze jednoznaczne sformułowania RODO, banki oraz oferujące rozwiązanie Biuro Informacji Kredytowej zrezygnowały z korzystania z dotychczasowej i upowszechnionej nazwy biometria behawioralna, a zaczęły korzystać z alternatywnej – weryfikacja lub analiza behawioralna.

Jednym z argumentów był fakt, iż pojęcie biometrii budzi zastrzeżenia wśród klientów banków, dlatego warto posługiwać się precyzyjnymi pojęciami, biorąc pod uwagę istotne prawnie różnice pomiędzy metodami biometrycznymi, a analizą behawioralną (Mórawski, 2023). Ogromne znaczenie nabiera również edukacja klientów w zakresie bezpieczeństwa, zwłaszcza że większość użytkowników odczuwa obawy dotyczące przetwarzania ich danych. Wskazywaną alternatywą jest też zmiana sposobu pozyskiwania zgody klientów, czego przykładem może być PKO Bank Polski, który przełamał barierę braku wyrażania przez klientów zgody, łącząc ją z korzyściami UX i bezpieczeństwa. Bank zrezygnował przy logowaniu do bankowości internetowej z nowo wprowadzonej każdorazowej, dwuetapowej weryfikacji klientów, którzy wyrazili taką zgodę. Mogą oni również ustawić znacznie wyższy maksymalny dzienny limit przelewów przez internet. Klienci z mobilną autoryzacją, ale bez zgody na biometrię mogą przelać maksymalnie 200 tys. złotych, podczas gdy dla klientów ze zgodą maksymalny limit wynosi 300 tys. Działania te spowodowały, że bank w niecały rok od wdrożenia rozwiązania pozyskał ponad 60% zgód od aktywnych klientów bankowości internetowej (Lidke, 2025). Bank zdecydował się również na wejście w rozwiązanie sektorowe Biura Informacji Kredytowej, co zwiększy skuteczność całej platformy dla innych uczestników (Uryniuk, 2024a). Chociaż takie rozwiązanie okazało się skuteczne, to instytucja ta nie ustrzegła się od negatywnych opinii w mediach, w których zwracano uwagę na zastosowany schemat pozyskiwania zgód. Chociaż tego typu artykułów czy komentarzy nie było dużo, to wskazywały na negatywne podejście części klientów.

Analiza SWOT biometrii behawioralnej w bankowości

W celu znalezienia odpowiedzi na pytanie, czy biometria behawioralna może stanowić ważny element w redukcji najczęściej występujących oszustw finansowych w Polsce, przeprowadzono analizę SWOT. Zaproponowana metoda jest jedną z technik diagnozy strategicznej. W swojej istocie służy poszukiwaniu, gromadzeniu i porządkowaniu danych o czynnikach determinujących i wpływających na organizację, system lub rozwiązanie, przedstawionych w przejrzystej i czytelnej formie. Zaproponowana w badaniu analiza może pomóc określić najlepszy kierunek rozwoju biometrii behawioralnej w kontekście wpływu zarówno czynników zewnętrznych, jak i wewnętrznych. Analiza rozpoczyna się od identyfikacji mocnych i słabych stron biometrii behawioralnej stosowanej przez polskie banki, ale także rozpoznania pojawiających się szans i zagrożeń z otoczenia – podejście powszechnie znane jako analiza SWOT (Strengths, Weaknesses, Opportunities, Threats). Zidentyfikowane czynniki wpływające na skuteczność wykorzystania biometrii behawioralnej podzielono na zbiory i przypisano im wagi, tworząc macierz składającą się z czterech pól S/W/O/T. Poziomy wag zostały określone zgodnie z wiedzą autorów na temat potencjalnego wpływu poszczególnych czynników, co przedstawia Tabela 1.

Tabela 1

Czynniki analizy SWOT wykorzystania biometrii behawioralnej w bankowości

Czynniki wewnętrzne S-Strengths	Waga	Czynniki wewnętrzne W-Weaknesses	Waga
S1 - Ciągła i nieinwazyjna weryfikacja: biometria behawioralna działa w tle, monitorując użytkownika przez cały czas trwania sesji, wychwytując odstępstwa od profilu, bez wpływu na jego doświadczenie (UX).	0,3	**W1 – Niski poziom akceptacji wśród klientów:** wymóg uzyskania świadomej i dobrowolnej zgody klienta na przetwarzanie danych biometrycznych jest kluczową barierą umasowienia tej technologii	0,4
S2 – Wykrywanie zaawansowanych zagrożeń: technologia pozwala na identyfikację oszustw typu *Account Takeover Fraud* (przejęcie konta), nawet kiedy przestępca dysponuje danymi do logowania lub wykorzystuje oprogramowanie do zdalnego dostępu do komputera. Może wykrywać anomalie w zachowaniu wskazujące na manipulację socjotechniczną klienta.	0,4	**W2 – Długi proces budowania profilu:** system potrzebuje co najmniej kilku logowań do stworzenia profilu behawioralnego klienta. W przypadku rzadko logujących się klientów może to trwać kilka miesięcy.	0,15
S3 – Samouczący się mechanizm: system oparty na uczeniu maszynowym tworzy unikalne, dynamiczne profile dla każdego użytkownika, adaptując je do naturalnych zmian w zachowaniu klienta.	0,15	**W3 – Wysokie ryzyko fałszywych alarmów:** nietypowe, chociaż normalne działania klienta takie jak zmiana nawyków, czy inne urządzenie mogą być błędnie interpretowane przez system jako atak. Przy zbyt rygorystycznym podejściu może to powodować niepotrzebne blokady lub alerty, obniżając wygodę korzystania. Niższy poziom zgodności zwiększa prawdopodobieństwo nieautoryzowanego dostępu.	0,15
S4 – Wzmocnienie systemów antyfraudowych: Biometria behawioralna jest ważnym uzupełnieniem innych zabezpieczeń, takich jak zaufane urządzenie, czy silne uwierzytelnienie, wspierając wielowarstwowy system ochrony.	0,15	**W4 – Ograniczona skuteczność przy oszustwach opartych na socjotechnice**: biometria behawioralna nie jest dostateczni skuteczna przy transakcjach płatniczych dokonywanych przez klientów zmanipulowanych przez przestępców.	0,3
Czynniki zewnętrzne O-Opportunities		**Czynniki zewnętrzne T-Threats**	
O1 – Rosnąca skala fraudów: Wzrost wartości oszustw finansowych (blisko dziesięciokrotny w latach 2019–2024) tworzy pilną potrzebę wdrażania nowych, skutecznych sposobów zabezpieczenia bankowości elektronicznej.	0,3	**T1 – Bariery prawne i regulacyjne:** restrykcyjna interpretacja RODO przez Urząd Ochrony Danych Osobowych klasyfikuje dane behawioralne jako dane biometryczne szczególnej kategorii. Banki muszą pozyskiwać dobrowolną zgodę od klienta, co uniemożliwia szybkie objęcie ochroną większej grupy użytkowników.	0,4
O2 – Możliwość budowy rozwiązania sektorowego: współdzielenie informacji			

o wzorcach zachowań klientów pomiędzy bankami (np. w ramach platformy BIK) pozwala na szybszą identyfikację oszusta.	0,2	**T2** – **Obawy o prywatność:** klienci obawiają się o prywatność i niechętnie wyrażają zgody pozwalające analizować ich zachowanie w sieci, co utrudnia masowe wykorzystanie technologii.	0,2
O3 – Rozwój technologiczny: postęp w dziedzinie AI i uczenia maszynowego zwiększa skuteczność i szybkość weryfikacji behawioralnej. Sztuczna inteligencja może ułatwić wykrywanie subtelnych anomalii w czasie rzeczywistym i sprzyjać lepszemu dostosowaniu do nowych metod ataków.	0,1	**T3 – Rozwój nowych metod ataków**: masowe wykorzystanie *deepfake'ów* i narzędzi AI tworzy zupełnie nowe zagrożenia i może ułatwiać jeszcze lepszą manipulację większej grupy klientów. Nowe mechanizmy mogą również skuteczniej odtwarzać zachowania klienta lub omijać stosowane zabezpieczenia.	0,1
O4 – Zgodność z zaleceniami regulatorów: urzędy takie jak UKNF i UOKiK bezpośrednio wskazują biometrię behawioralną jako narzędzie do walki z fraudami.	0,25	**T4 – Ryzyko nadużyć mechanizmu zwrotu środków w D+1:** UOKiK interpretuje przepisy w taki sposób, że banki mają obowiązek zwracania klientom pieniądze z tytułu nieautoryzowanych transakcji w terminie D+1, czyli do końca następnego dnia roboczego po zgłoszeniu nieautoryzowanej transakcji. Tworzy to nowe ryzyko finansowe dla banków, ponieważ przestępcy mogą masowo składać fałszywe reklamacje i wykorzystywać asymetrię czasową do wyłudzania środków.	0,2
O5 – Nowe sposoby pozyskiwania zgód: banki mogą wykorzystać UX i stosować zachęty, takie jak uproszczone logowanie (bez konieczności każdorazowej autoryzacji dwuetapowej) czy wyższe limity transakcyjne do łatwiejszej aktywacji usługi. Zgoda na biometrię behawioralną może pojawiać się cyklicznie przy każdym logowaniu do serwisu.	0,15	**T5 – Zwiększenie praw klienta po wdrożeniu PSD3/PSR:** planowane przepisy poszerzają katalog sytuacji uprawniających do zwrotu środków (np. błędne transakcje), co oznacza, że banki będą musiały zwracać klientom znacznie więcej pieniędzy i w szerszym zakresie niż dzieje się to obecnie.	0,1

Źródło: opracowanie własne.

Kolejnym krokiem była identyfikacja interakcji pomiędzy czynnikami zaklasyfikowanymi do poszczególnych kategorii, co zostało przedstawione w Tabeli 2. Zaprezentowana jest tam macierz zidentyfikowanych interakcji. Wartość 1 oznacza istnienie merytorycznie uzasadnionego powiązania między czynnikiem wewnętrznym, a czynnikiem zewnętrznym. Wartość 0 oznacza brak takiego powiązania.

Tabela 2

Macierz Interakcji Strategicznych SWOT

	O1	O2	O3	O4	O5	T1	T2	T3	T4	T5
S1	1	1	1	1	1	0	0	1	1	1
S2	1	1	1	1	0	0	0	1	1	1
S3	1	1	1	0	0	0	0	1	0	0
S4	1	1	1	1	0	0	0	1	1	1
W1	1	1	0	1	0	0	0	1	1	1
W2	1	1	1	1	0	0	0	1	1	1
W3	1	1	0	0	1	0	1	0	0	0
W4	1	0	0	1	0	0	0	1	1	1

Źródło: opracowanie własne.

Analizę SWOT kończy podsumowanie wyników (w tym liczba i ważona liczba interakcji, będąca sumą powiązań) przedstawione w Tabeli 3. Zastosowano następujący zestaw pytań testowych:

1. Dla interakcji mocna strona – szansa (S–O): Czy dana mocna strona pozwala wykorzystać nadarzającą się okazję?
2. Dla interakcji mocna strona – zagrożenie (S–T): Czy dana mocna strona pomoże złagodzić dane zagrożenie?
3. Dla interakcji słaba strona – szansa (W–O): Czy konkretna słabość ogranicza możliwości wykorzystania danej okazji?
4. Dla interakcji słaba strona – zagrożenie (W–T): Czy określony słaby punkt zwiększa ryzyko związane z danym zagrożeniem?

Podsumowanie zawiera interpretację wyników, wskazującą jeden z czterech podstawowych typów strategii, która jest najbardziej odpowiednia dla biometrii behawioralnej w Polsce.

Tabela 3

Zbiorcze wyniki analizy SWOT

Strategia	Suma interakcji	Ważona suma interakcji
S/O (maxi–maxi) – agresywna	16	4,15
S/T (maxi–mini) – konserwatywna	10	2,7
W/O (mini–maxi) – konkurencyjna	12	2,85
W/T (mini–mini) – defensywna	10	2,7

Źródło: opracowanie własne.

Analiza kombinacji S/O wskazuje na duży potencjał wykorzystania biometrii behawioralnej przez polskie banki. Odpowiada to strategii silnej ekspansji i dynamicznego rozwoju. Jest to też strategia

o największym potencjale sukcesu. Strategia agresywna (maxi–maxi), z ważonym wynikiem 4,15, wskazuje na dominujący typ strategii. Znacząco przewyższa pozostałe opcje. Wskazuje to, że najbardziej efektywnym podejściem dla banków powinno być proaktywne wykorzystanie wewnętrznych atutów biometrii behawioralnej w celu maksymalizacji korzyści płynących z zewnętrznych szans rynkowych. Pozostałe wyniki należy interpretować w kontekście tej dominującej strategii. Strategia konkurencyjna na poziomie 2,85 wskazuje, że istnieje możliwość wykorzystania sprzyjających warunków rynkowych do przezwyciężenia wewnętrznych słabości technologii. Niższe wyniki strategii konserwatywnej i defensywnej na poziomie 2,7 wskazują, że chociaż zagrożenia i ich interakcje ze słabościami muszą być zarządzane, to należy je mitygować, koncentrując wysiłek na działaniach ekspansywnych.

Największym wyzwaniem i barierą w rozwoju biometrii behawioralnej jest niski poziom akceptacji wśród klientów oraz zewnętrzne zagrożenie w postaci restrykcyjnych barier prawnych i regulacyjnych. Bez skutecznego rozwiązania tych dwóch elementów nie będzie możliwe wykorzystanie mocnych stron technologii. Wydaje się, że najłatwiej dokonać tego poprzez zmianę procesu pozyskiwania zgody klienta. Z przeszkody prawnej, jaką jest wymóg uzyskania świadomej i dobrowolnej zgody klienta na przetwarzanie danych biometrycznych, banki powinny stworzyć propozycję wartości dodanej. Powiązanie zgody na analizę behawioralną z korzyściami wygodnego korzystania z serwisów bankowości elektronicznej może znacząco zwiększyć wskaźnik akceptacji, a tym samym wyeliminować główną barierę rozwoju. W ten sposób będzie można wykorzystać pełny potencjału rozwiązania, wspartego rozwojem platformy sektorowej. Presja ze strony regulatorów zwiększa odpowiedzialność banków w kontekście transakcji nieautoryzowanych. Biometria może stanowić w takim przypadku ważny element proaktywnej strategii cyberbezpieczeństwa, zwłaszcza w kontekście zasady zwrotu środków w terminie D+1.

Zakończenie

Biometria behawioralna stanowi skuteczne narzędzie zwiększające poziom bezpieczeństwa w bankowości elektronicznej, a także może się stać się rozwiązaniem, które umożliwi redukcję skali oszustw finansowych w Polsce. Ciągła i nieinwazyjna weryfikacja klienta pozwala na identyfikowanie nieautoryzowanych prób dostępu do rachunku, a także wykrycie anomalii w zachowaniu użytkownika umożliwia to natychmiastową reakcję, zablokowanie dostępu do rachunku lub zastosowanie dodatkowej weryfikacji użytkownika.

W toku badań zweryfikowano hipotezę „biometria behawioralna może stać się rozwiązaniem, które umożliwia redukcję skali oszustw finansowych w Polsce”. Wyniki przeprowadzonej analizy SWOT wskazują, że dominującą strategią polskich banków dla rozwoju tej technologii powinna być strategia agresywna (maxi–maxi). Polega ona na proaktywnym wykorzystaniu unikalnych mocnych stron w odpowiedzi na szybko rosnącą skalę oszustw. Takie podejście wsparte jest pozytywnymi

rekomendacjami nadzorców. Potencjał ten jest jednak mocno hamowany przez kluczowe bariery, którymi są restrykcyjna interpretacja przepisów RODO i wynikający z niej niski poziom akceptacji rozwiązania wśród klientów. Bez przezwyciężenia tych dwóch wyzwań, biometria behawioralna pozostanie rozwiązaniem niszowym, z ograniczonym wpływem na cyberbezpieczeństwo. Na podstawie przeprowadzonej w artykule diagnozy strategicznej, sformułowano rekomendacje dla kluczowych interesariuszy.

Sektor bankowy powinien skupić się na powiązaniu aktywacji analizy behawioralnej z korzyściami w zakresie doświadczenia użytkownika. Może to być łatwiejsze logowanie do konta i wyższe limity transakcyjne. Zbieranie zgody powinno być powtarzalnym elementem każdego logowania do serwisu. Jest to obecnie najskuteczniejszy sposób na przełamanie bariery niskiej akceptacji. Instytucje finansowe powinny również aktywnie uczestniczyć w rozwoju jednej sektorowej platformy wymiany informacji. Zwiększy to skuteczność wykrywania oszustw w całym systemie, a także skróci proces budowania profilu dla nowych klientów, o ile nie nastąpi fragmentaryzacja całego rynku, poprzez wdrażanie rozwiązań różnych dostawców. Takie podejście niweluje jedną z technicznych słabości technologii. Biometria behawioralna nie powinna być też traktowana jako samodzielne rozwiązanie, ale jako kluczowy element wielowarstwowej strategii cyberbezpieczeństwa. Dane pozyskiwane w ten sposób powinny wzmacniać istniejące systemy antyfraudowe, zwłaszcza w kontekście rosnącej odpowiedzialności finansowej banków wynikającej z zasady zwrotu środków w terminie D+1. Pozwoli to również na łatwiejsze znalezienie odpowiedniego balansu pomiędzy skuteczną ochroną przed cyberprzestępcami, a wygodą klienta. Pozwala to ograniczyć fałszywe alarmy, które powodują ryzyko zablokowania klienta i zmniejszają jego zadowolenie z korzystania z bankowości elektronicznej.

Opierając się o diagnozę strategiczną, sformułowano również rekomendacje dla nadzoru i administracji publicznej. Oszustwa finansowe są problemem społecznym, który nie dotyczy tylko sektora bankowego. Mimo, że ochrona danych osobowych jest priorytetem, to Urząd Ochrony Danych Osobowych powinien dążyć do znalezienia równowagi pomiędzy prywatnością, a bezpieczeństwem finansowym obywateli. W interesie wszystkich klientów banków jest stworzenie takich ram prawnych, które wspierałyby nowe technologie antyfraudowe. Nadzorcy powinni również wspierać ogólnopolskie kampanie edukacyjne na temat zagrożeń i sposobów ochrony w internecie. Powinno to obejmować zwłaszcza techniki socjotechniczne, w wyniku których przestępcy manipulują płatnikiem. Autorytet administracji państwowej może pomóc w przełamaniu barier mentalnych i obaw o prywatność przy wykorzystywaniu biometrii behawioralnej. Ważnym zadaniem administracji jest również ograniczenie zjawiska fałszywych reklam i linków, dzięki którym przestępcy łatwo nawiązują kontakt ze swoimi ofiarami.

Reasumując, chociaż biometria nie jest rozwiązaniem uniwersalnym i wolnym od ograniczeń, to posiada potencjał, żeby stać się jednym z kluczowych filarów cyberbezpieczeństwa w polskich bankach. W sytuacji szybko rosnącej liczby przestępstw, technologia ta powinna stać się ważnym

narzędziem ograniczającym skutki działania cyberprzestępców. Świadomość potencjału musi być powszechniejsza nie tylko w sektorze finansowym, ale również w administracji państwowej oraz wśród regulatorów. Skuteczność działania biometrii behawioralnej jest bowiem zdeterminowana nie tyle przez samą technologię, a przez synergię działań biznesowych, regulacyjnych i edukacyjnych.

Bibliografia

Baglajewski, Z. (2024). Biometria behawioralna w usługach finansowych – szansa czy zagrożenie? *Rzecznik Finansowy.* https://rf.gov.pl/wp-content/uploads/2024/12/RZECZNIK-FINANSOWY-artykul-Ziemowita-Baglajewskiego_4X4_10.12_PRAWNIK.pdf

BANK.pl. (2022). *Digital Fingerprints z Grupy BIK ma nowy zarząd*. https://bank.pl/digital-fingerprints-z-grupy-bik-ma-nowy-zarzad/

Bankier.pl. (2025). *Oszuści buszują w sieci. Podszywają się pod koncerny, udają inwestorów*. https://www.bankier.pl/wiadomosc/Oszusci-buszuja-w-sieci-Podszywaja-sie-pod-koncerny-udaja-inwestorow-8919553.html

Barrett N. (2003). Penetration testing and social engineering: Hacking the weakest link. *Information Security Technical Report*, Volume 8, Issue 4, s. 56–64.

CCNews. (2024). *PKO BP: 10% aktywnych klientów zdecydowało się na biometrię behawioralną w tydzień po wdrożeniu*, https://ccnews.pl/2024/05/29/pko-bp-10-aktywnych-klientow-zdecydowalo-sie-na-biometrie-behawioralna-w-tydzien-po-wdrozeniu/

CERT.PL. (2025). *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*. https://cert.pl/uploads/docs/Raport_CP_2024.pdf

CERT.PL. (2022). *Statystyki obsługi incydentów w 2021 r.* https://cert.pl/posts/2022/04/statystyki-obslugi-incydentow-2021/

Clever Advice. (2019). *Impact of implementing SCA on e-Commerce*. https://europeanpaymentadvisors.com/wp-content/uploads/2020/04/Impact-of-implementing-SCA-on-e-commerce-14jun2019.pdf

Cyberdefence24.pl. (2024). *Cyberprzestępczość w Polsce. Rośnie czy spada?* https://cyberdefence24.pl/cyberbezpieczenstwo/cyberprzestepczosc-w-polsce-rosnie-czy-spada

Dziennik Ustaw. (2011). *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych* (Dz.U. 2011 nr 199 poz. 1175, z późn. zm.).

Forsal.pl. (2021). *KNF: banki powinny lepiej edukować swoich klientów w kwestii cyberbezpieczeństwa*. https://forsal.pl/finanse/finanse-osobiste/artykuly/8096464,knf-banki-lepiej-edukowac-swoich-klientow-w-kwestii-cyberbezpieczenstwa.html

Ghiciuc, I. (2024). *Behavioral Analytics for Fraud Prevention in Banking Apps*. https://www.thinslices.com/insights/behavioral-analytics-for-fraud-prevention-in-banking-apps

Harley-McKeown, L. (2025). Fraud losses reach £1.2bn as financial crime and scams soar. *Yahoo Finance*, https://uk.finance.yahoo.com/news/fraud-losses-financial-crime-scam-050001482.html

Jain, A.K., Ross, A., Pankanti, S. (2006). Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics and Security*, Volume 1, Issue 2, s. 125–143.

Jastrzębski, J. (2021). *Cyberbezpieczeństwo elektronicznych kanałów dostępu do usług bankowych – list Przewodniczącego KNF do sektora bankowego*. https://www.knf.gov.pl/knf/pl/komponenty/img/Cyberbezpieczenstwo_elektronicznych_kanalow_dostepu_do_uslug_bankowych%E2%80%93list_Przewodniczacego_KNF_do_sektora_bankowego_72587.pdf

Karnan, M., Akila, M., Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, Volume 11, Issue 2, s. 1565–1573.

Kałużny, P., Stolarski, P. (2019). Biometria behawioralna i 'tradycyjna' w mobilnych usługach bankowych – stan oraz przyszłe możliwości zastosowania. *Bezpieczny Bank*, 1(74), s. 26–41.

KGP. (2025). *Oficjalne statystyki Komendy Głównej Policji przestępstw z art. 287 KK (oszustwa komputerowe, phishing) za lata 1999–2023.* https://statystyka.policja.pl/download/20/362027/Art287.xlsx

KNF. (2024). *Raport Roczny CSIRT KNF 2024*. https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf

Komenda Powiatowa Policji w Kołbucku. (2025). *Stan bezpieczeństwa*. https://klobuck.policja.gov.pl/k12/z-zycia-jednostki/stan-bezpieczenstwa/38918,Stan-bezpieczenstwa.html

Lidke, R. (2024a). *Jak biometria behawioralna wzmacnia bezpieczeństwo klientów banków?*. Jak biometria behawioralna wzmacnia bezpieczeństwo klientów banków?

Lidke R. (2024b). *Prezes UODO o stosowaniu przez banki analizy behawioralnej*. https://bank.pl/prezes-uodo-o-stosowaniu-przez-banki-analizy-behawioralnej/

Lidke R. (2025). *Skończyła się romantyczna era bankowości.* Skończyła się romantyczna era bankowości elektronicznej

Mamstartup.pl. (2022). *Biuro Informacji Kredytowej inwestuje w polski fintech Digital Fingerprints*. https://mamstartup.pl/masz-pomysl-na-startup-unicorn-hub-innovation-lab-pomoze-ci-go-zweryfikowac-rozwinac-i-stworzyc-mvp/

mBank. (2018). *mBank testuje rewolucyjną biometrię behawioralną*. https://pl.media.mbank.pl/46297-mbank-testuje-rewolucyjna-biometrie-behawioralna

Mórawski, K. (2023). *Forum Usług Płatniczych o analizie behawioralnej*. https://bank.pl/forum-uslug-platniczych-o-analizie-behawioralnej/

NBP. (2025). *Informacja o transakcjach oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych w IV kwartale 2024 r.* https://nbp.pl/wp-content/uploads/2025/04/2024-Q4-informacja-o-transakcjach-oszukanczych.pdf

NBP. (2022). *Informacja o transakcjach oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych w II kwartale 2022 r.* https://nbp.pl/wp-content/uploads/2022/11/Informacja-o-transakcjach-oszukanczych-w-Q2-2022.pdf

Ostrowska, M. (2020). *Weryfikacja behawioralna w ING*. https://media.ing.pl/informacje-prasowe/926/pr/480937/weryfikacja-behawioralna-w-ing

Palczewski, S. (2018). *mBank wprowadza biometrię behawioralną. Przełom w bankowości*. https://cyberdefence24.pl/biznes-i-finanse/mbank-wprowadza-biometrie-behawioralna-przelom-w-bankowosci

PingIdentity.com. (n.d.) *What Is Continuous Authentication?*. https://www.pingidentity.com/en/resources/identity-fundamentals/authentication/continuous-authentication.html

Rzecznik Finansowy. (2023). *Ogólnopolska kampania społeczna „Stracisz dane, stracisz pieniądze!”*. https://rf.gov.pl/ogolnopolska-kampania-spoleczna-stracisz-dane-stracisz-pieniadze/

Rzecznik Finansowy. (2022). *Rzecznik Finansowy zbada „kredyty na klik”*. https://archiwum.rf.gov.pl/2022/04/20/rzecznik-finansowy-zbada-kredyty-na-klik/

Rzecznik Finansowy. (2021). *Rzecznik Finansowy ponownie pyta banki o nieautoryzowane transakcje*. https://archiwum.rf.gov.pl/2021/07/29/rzecznik-finansowy-ponownie-pyta-banki-o-nieautoryzowane-transakcje/

SEON. (2025). *TRA Exemptions in PSD2 to Reduce Friction and Boost Your ROI*, https://seon.io/resources/tra-exemptions/

Tomczyk, K. (2023). Transakcje oszukańcze dokonywane przy użyciu bezgotówkowych instrumentów płatniczych jako przykład cyberprzestępczości. [w:] D. Dziembek, L. Ziora (red.). Przedsiębiorczość i konkurencyjność w dobie transformacji cyfrowej. *Wydawnictwo Politechniki Częstochowskiej.*

Unia Europejska. (2015). *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD2).* Dziennik Urzędowy Unii Europejskiej, L337, https://eur-lex.europa.eu/eli/dir/2015/2366/oj

Unia Europejska. (2012). *Karta Praw Podstawowych Unii Europejskiej* (2012/C 326/02). Dziennik Urzędowy Unii Europejskiej, C326. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:12012P/TXT

Unia Europejska. (2018). *Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę (UE) 2015/2366 Parlamentu Europejskiego i Rady w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta oraz wspólnych i bezpiecznych otwartych standardów komunikacji.* Dziennik Urzędowy Unii Europejskiej, L 69/23. https://eur-lex.europa.eu/eli/reg_del/2018/389/oj?locale=pl

Unia Europejska. (2016). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. – ogólne rozporządzenie o ochronie danych (RODO)*. Dziennik Urzędowy Unii Europejskiej, L 119, https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=PL

UOKiK. (2021). *Nieautoryzowane transakcje bankowe – postępowania*. https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/nieautoryzowane-transakcje-bankowe-postepowania/

UOKiK. (2024). *Nieautoryzowane transakcje – kolejne wszczęcia*. https://uokik.gov.pl/nieautoryzowane-transakcje-kolejne-wszczecia

UOKiK. (2022a). *Stanowisko Prezesa UOKiK w sprawie interpretacji przepisów Ustawy z 19 sierpnia 2011 r. o usługach płatniczych w zakresie dotyczącym nieautoryzowanych transakcji płatniczych*. https://finanse.uokik.gov.pl/produkcja/wp-content/uploads/Stanowisko-Prezesa-UOKiK-w-sprawie-transakcji-nieautoryzowanych.pdf

UOKiK. (2022b). *Transakcje nieautoryzowane – zarzuty wobec 5 banków*. https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/transakcje-nieautoryzowane-zarzuty-wobec-5-bankow/

Uryniuk, J. (2024a). *PKO BP wejdzie do sektorowego systemu weryfikacji behawioralnej. Relacja w wczorajszego Cashless Breakfast*. https://www.cashless.pl/16166-cashless-breakfast-weryfikacja-behawioralna-relacja

Uryniuk, J. (2023). *ING na temat biometrii behawioralnej: klienci korzystający z rozwiązania padają ofiarą fraudu osiem razy rzadziej niż pozostali*. https://www.cashless.pl/14353-ing-biometria-behawioralna-statystyki

Uryniuk, J. (2024b). *Raport NBP: weryfikacja behawioralna poprawi bezpieczeństwo, ale pod warunkiem, że będzie powszechna*. https://www.cashless.pl/16173-raport-nbp-weryfikacja-behawioralna

Wójciecki, B. (2024). *Product Owner BIK, „Weryfikacja behawioralna"* – Prezentacja, Łochów.

Zgromadzenie Narodowe. (1997). *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz. U. Nr 78, poz. 483). https://www.sejm.gov.pl/prawo/konst/polski/2.htm

WYKORZYSTANIE BIOMETRII BEHAWIORALNEJ W KONTEKŚCIE CYBERBEZPIECZEŃSTWA POLSKIEGO SEKTORA BANKOWEGO (2019-2024)

STRESZCZENIE

Cel artykułu. Celem artykułu jest weryfikacja hipotezy wskazującej, że biometria behawioralna może stać się rozwiązaniem, które umożliwia redukcję skali oszustw finansowych w Polsce. Zagadnienie to jest istotne ze względu na negatywny wpływ zmian na cyberbezpieczeństwo w otoczeniu sektora bankowego po pandemii COVID-19. Tylko w latach 2019–2024 nastąpił dziesięciokrotny wzrost wartości fraudów. Ryzyko przestępstw finansowych
w cyberprzestrzeni staje się głównym wyzwaniem stojącym przed sektorem finansowym. Tak duża dynamika i skala ponoszonych przez klientów strat spowodowała zainteresowanie urzędów nadzorczych, które skierowały do banków liczne zalecenia dotyczące edukacji klientów oraz minimalizacji ryzyka oszustw na poziomie systemowym. Jednym ze wskazywanych w tym kontekście zaleceń dla dostawców usług płatniczych jest stosowanie systemów opartych na biometrii behawioralnej. To nowoczesne rozwiązanie techniczne pozwala na bieżące weryfikowanie, czy osoba logująca się do konta bankowego i przeprowadzająca operacje finansowe jest właścicielem rachunku. W pracy przeprowadzono diagnozę strategiczną tej technologii przy użyciu analizy SWOT. Metodologia ta pozwoliła na identyfikację i ocenę kluczowych czynników wewnętrznych (mocnych i słabych stron) oraz zewnętrznych (szans i zagrożeń), a także na określenie dominującej strategii rozwoju na polskim rynku finansowym. W konsekwencji autorzy sformułowali rekomendacje strategiczne zarówno dla instytucji

finansowych, jak i regulatorów, które mogą pomóc w zwiększeniu skuteczności biometrii behawioralnej w redukcji oszustw finansowych.

Metodologia. W artykule zastosowano jakościowe podejście badawcze. Główną metodą analizy jest studium przypadku polskiego sektora bankowego w latach 2019–2024. Do przedstawienia ewolucji zagrożeń cybernetycznych, skali oszustw finansowych oraz ram regulacyjnych wykorzystano analizę deskryptywną. Kluczowym narzędziem badawczym jest analiza strategiczna SWOT, za pomocą której zostały zidentyfikowane mocne i słabe strony biometrii behawioralnej, a także szanse i zagrożenia rynkowe. Pozwoliło to na sformułowanie rekomendacji. Uzupełniająco zastosowano analizę danych wtórnych, pochodzących z raportów, publikacji i komunikatów regulatorów rynku.

Wyniki badania. Z punktu widzenia instytucji finansowych weryfikacja behawioralna może stanowić kluczowy element redukcji najczęściej występujących oszustw finansowych. Najbardziej efektywnym podejściem dla banków powinno być proaktywne wykorzystanie wewnętrznych atutów biometrii behawioralnej w celu maksymalizacji korzyści płynących z zewnętrznych szans rynkowych. Największym wyzwaniem i blokerem w rozwoju tej technologii jest niski poziom akceptacji wśród klientów oraz zewnętrzne zagrożenie w postaci restrykcyjnych barier prawnych i regulacyjnych. Rozwiązaniem w tym przypadku powinna być zmiana istniejącego procesu pozyskiwania zgody klienta. Powiązanie jej z korzyściami wygodnego korzystania z serwisów bankowości elektronicznej może znacząco zwiększyć wskaźnik akceptacji, a tym samym wyeliminować główną barierę rozwoju. Umożliwi to wykorzystanie pełnego potencjału rozwiązania, wspartego rozwojem platformy sektorowej. Chociaż biometria behawioralna ma mniejsze znaczenie przy zapobieganiu nieautoryzowanym transakcjom klientów zmanipulowanych przez przestępców, to stanowi ważny element proaktywnej strategii cyberbezpieczeństwa, zwłaszcza w kontekście zasady zwrotu środków w terminie D+1. Jest to istotne w kontekście presji ze strony regulatorów, która zwiększa odpowiedzialność banków za transakcje oszukańcze.

Praktyczne implikacje. Biometria behawioralna może stać się kluczowym narzędziem ograniczającym skalę oszustw finansowych. Wdrożenie jej zwiększa poziom ochrony klientów, a tym samym pozwala na ograniczenie skali oszustw finansowych, zwłaszcza związanych z przejęciem rachunku. Największą wartością tej technologii jest ciągła i nieinwazyjna weryfikacja tożsamości klienta w tle. Jest to bardzo dobre uzupełnienie istniejących rozwiązań i systemów antyfraudowych. Wykorzystanie platformy sektorowej może przyczynić się do szybszej akceptacji oraz zwiększenia skuteczności zastosowanych zabezpieczeń. Umożliwi to bankom lepszą reakcję na incydenty, przy spełnieniu rosnących wymagań regulatorów w zakresie ochrony klientów. Powodzenie wdrożenia i wykorzystania biometrii behawioralnej zależy jednak od rozwiązania barier prawnych oraz edukacji rynku i klientów, bez czego technologia ta pozostanie jedynie rozwiązaniem niszowym**.**

Słowa kluczowe: cyberbezpieczeństwo, oszustwa finansowe, biometria behawioralna, bankowość elektroniczna.

JEL Class: G21, G23, G29.

Received: 12.09.2025
Accepted: 26.09.2025
Available online: 30.09.2025