Zeszyty Naukowe Wydziału Ekonomii i Finansów
Uniwersytetu Radomskiego im. Kazimierza Pułaskiego
Studia Ekonomiczne, Prawne i Administracyjne
Zeszyt 4 (2025)
DOI https://doi.org/10.24136/sepia.2025.019

Julia Pękala[1], Katarzyna Tkacz[2], Aleksandra Ziomka[3]

ROZWÓJ BANKOWOŚCI MOBILNEJ A BEZPIECZEŃSTWO DANYCH KLIENTÓW

Streszczenie

W artykule omówiono rozwój bankowości mobilnej w Polsce oraz związane z nim wyzwania w zakresie bezpieczeństwa danych klientów. Przedstawiono główne zagrożenia oraz rozwiązania stosowane przez banki. Na przykładach wybranych instytucji finansowych wskazano, że skuteczna ochrona wymaga połączenia nowoczesnych technologii z edukacją użytkowników. Podkreślono, że dalszy rozwój bankowości mobilnej powinien opierać się na innowacyjnych zabezpieczeniach i świadomym korzystaniu z usług cyfrowych.

Słowa kluczowe: bank, bankowość mobilna, bezpieczeństwo danych.

WSTĘP

Dynamiczny rozwój technologii informacyjno-komunikacyjnych w ostatnich latach znacząco wpłynął na sposób funkcjonowania sektora finansowego. Jednym z najważniejszych przejawów tej transformacji jest bankowość mobilna, która umożliwia klientom dostęp do usług bankowych z dowolnego miejsca i o dowolnym czasie. Użytkownicy mogą realizować operacje finansowe, zarządzać kontem czy inwestycjami za pośrednictwem smartfona lub tabletu, co czyni bankowość mobilną niezwykle wygodnym i popularnym kanałem kontaktu z bankiem.

[1] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 119676@student.uthrad.pl.
[2] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 119679@student.uthrad.pl.
[3] Uniwersytet Radomski im. Kazimierza Pułaskiego, Wydział Ekonomii i Finansów, e-mail: 119681@student.uthrad.pl.

Upowszechnienie rozwiązań mobilnych przyniosło jednak również nowe wyzwania w zakresie bezpieczeństwa danych klientów. Wraz ze wzrostem liczby użytkowników rośnie liczba zagrożeń – od ataków phishingowych i malware, po wyłudzenia z wykorzystaniem socjotechniki. Dlatego współczesne instytucje finansowe stają przed koniecznością nieustannego doskonalenia systemów ochrony informacji, a także podnoszenia świadomości użytkowników w zakresie bezpiecznego korzystania z usług online.

Celem niniejszego artykułu jest analiza rozwoju bankowości mobilnej oraz ocena stosowanych przez banki mechanizmów zabezpieczających dane klientów. W pracy przedstawiono ewolucję usług mobilnych w Polsce, omówiono podstawowe zagrożenia towarzyszące korzystaniu z aplikacji bankowych, a także zaprezentowano konkretne przykłady rozwiązań stosowanych przez wybrane instytucje finansowe. Artykuł ma na celu ukazanie, że bezpieczeństwo bankowości mobilnej stanowi złożone zagadnienie technologiczno-organizacyjne, wymagające współdziałania banku i klienta w ramach wspólnego systemu ochrony.

1. Istota i rozwój bankowości mobilnej

Bankowość mobilna (ang. *mobile banking*, m-banking) stanowi jeden z kluczowych obszarów cyfrowej transformacji sektora finansowego. W najszerszym rozumieniu odnosi się do możliwości dokonywania operacji bankowych za pomocą telefonu komórkowego[4]. Bardziej szczegółowo definiowana jest jako usługa oferowana przez instytucje finansowe umożliwiająca dostęp do rachunku bankowego poprzez urządzenia mobilne posiadające dostęp do Internetu, w szczególności smartfonów i tabletów, z wykorzystaniem dedykowanych aplikacji, przeglądarek internetowych w wersji mobilnej lub komunikatów SMS/USSD[5]. Podsumowując przytoczone definicje, bankowość mobilna rozumiana jest jako platforma, która umożliwia dostęp do usług lub produktów bankowych za pośrednictwem urządzeń mobilnych[6]. Na podstawie definicji można wyróżnić jej kilka cech. Po pierwsze komunikacja na linii bank – klient realizowana jest za pośrednictwem Internetu mobilnego. Drugą cechą bankowości mobilnej jest interaktywność oraz dostęp w dowolnym czasie i miejscu. Bankowość mobilna może być realizowana za pośrednictwem różnych technologii – SMS, WAP, „lekkich" stron internetowych oraz aplikacji mobilnych. Wyróżniane są dwa rodzaje dostępu do usług lub produktów bankowych: pasywny i aktywny. W ramach dostępu aktywnego klient może realizować transakcje, np. zlecać przelewy, zakładać lokaty czy spłacać karty kredytowe. W dostępie pasywnym

[4] Z. Dobosiewicz, *Bankowość*, PWE, Warszawa 2011, s. 271-272.

[5] A. Janc, G. Kotliński, *Nowe technologie we współczesnym banku*, Akademia Ekonomiczna w Poznaniu, Poznań 2004.

[6] G. Uytterhoeven, *Financial services through mobile devices*, „Efma journal", nr 228, kwiecień-czerwiec 2011, s. 56.

klient nie ma możliwości realizacji transakcji, a jedynie posiada dostęp do informacji takich jak saldo, informacje o posiadanych kartach, historia transakcji itd.[7]

Pierwsze próby wykorzystania bankowości mobilnej miały miejsce w ubiegłym stuleciu, zasadniczo tuż przed rozwojem bankowości internetowej. Pod koniec lat 90. bankowość mobilna była nazywana bankowością SMS, ponieważ obsługiwana była głównie za pośrednictwem wiadomości SMS. Pierwsze usługi były bardzo ograniczone, był to np. SMS z zapytaniem o saldo konta. W 1999 roku wraz z wprowadzeniem protokołu WAP (Wireless Application Protocol) banki zaczęły oferować swoim klientom pierwsze platformy bankowości mobilnej. Pierwsza bankowość WAP pojawiła się w Norwegii w 1999 roku.

Do 2010 roku usługi bankowości mobilnej były oferowane za pośrednictwem SMS-ów i WAP. W 2007 roku Bank of Scotland ogłosił pierwszą na świecie aplikację bankowości mobilnej na smartfony. Co więcej, już w 2009 roku firma udostępniła swoim klientom darmową, pierwszą aplikację mobilną na iPhone'a oraz funkcję szybkich wyciągów tekstowych (SMS) na żądanie. Klienci mogli również sprawdzać aktualne saldo i ostatnie transakcje w czasie rzeczywistym.

W 2011 roku szkocki bank uruchomił pierwszą na świecie darmową, w pełni funkcjonalną aplikację bankową, dostępną na iPhone'y, Androida i Blackberry. Odbiór w społeczeństwie był pozytywny i w ciągu pierwszych sześciu miesięcy usługa przyciągnęła ponad milion użytkowników, którzy przelali za jej pośrednictwem ponad miliard funtów[8].

Bankowość mobilna w Polsce rozwijała się stopniowo, jedynie z lekkim opóźnieniem do państw Europy Zachodniej i początkowo związana była z dostępem do konta z wykorzystaniem krótkich wiadomości tekstowych SMS oraz technologii WAP. W 2000 r. Bank Zachodni WBK jako pierwszy uruchomił serwis w standardzie WAP, który umożliwiał aktywny dostęp do rachunku[9]. W tym samym czasie mBank uruchomił serwis aktywny w technologii SMS. Dużym krokiem w rozwoju bankowości mobilnej w Polsce był rok 2002, wówczas Raiffeisen Bank Polska – jako pierwszy bank na polskim rynku – udostępnił mobilną aplikację (SIM Application Toolkit). Na przestrzeni lat kolejne banki korzystały z tych rozwiązań. W 2005 r. powiadomienia SMS uruchomił Bank Millennium. Rok później mBank, MultiBank, Citi Handlowy oraz ING Bank Śląski wykorzystały także SMS do przesyłania haseł jednorazowych w celu autoryzacji transakcji w kanale internetowym (np. przelewów). W następnych latach w wyniku generowania wysokich kosztów i słabej funkcjonalności stopniowo wycofywano się z rozwiązań protokołu WAP[10]. W 2010 r. już tylko nieliczne banki

---

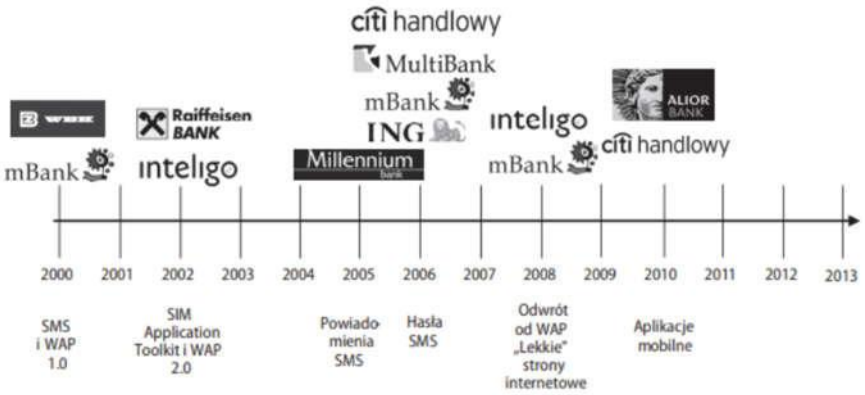
7 T. Hassa, *Stan i perspektywy rozwoju bankowości mobilnej dla klientów indywidualnych w Polsce*, Szkoła Główna Handlowa w Warszawie, s. 41.

8 M. Kochańska, *Historia bankowości mobilnej*, https://whitehats.pwr.edu.pl/research/history-of-mobile-banking/ [dostęp: 30.09.2025].

9 Instytut Badań nad Gospodarką Rynkową, *Prognoza rozwoju rynku bankowego do 2016 r.* Gdańsk, kwiecień 2012, s. 231.

10 M. Kochańska, *Historia...*, op. cit.

posiadały serwisy WAP. Kamieniem milowym, który spowodował stworzenie rynku trwającego do dziś, było uruchomienie przez banki tzw. „lekkich" stron internetowych. W 2008 roku Inteligo, jako pierwsze w Polsce, uruchomiło taki serwis. Krótko potem kolejne banki korzystały z tego rozwiązania. W latach 2010/2011 można było się już spotkać z bankowością mobilną w wersji aplikacyjnej. Na przestrzeni dwóch lat już 12 banków na polskim rynku dawało możliwość korzystania z aplikacji bankowej. Obecnie serwis SMS (powiadomienia, autoryzacja lub zlecanie transakcji) oraz „lekkie" strony internetowe są codziennością na rynku. Należy zaznaczyć, że praktycznie wszystkie banki zapewniają przez wspomniane usługi aktywny dostęp do konta. Najważniejsze etapy rozwoju bankowości mobilnej w Polsce przedstawiono na rys. 1.



Rys. 1. Historia bankowości mobilnej w Polsce
Źródło: T. Hassa, *Stan i perspektywy rozwoju bankowości mobilnej dla klientów indywidualnych w Polsce*, Szkoła Główna Handlowa w Warszawie, 2013, s. 43

Wraz z dynamicznym rozwojem bankowości mobilnej kluczowego znaczenia nabiera zagadnienie cyberbezpieczeństwa, które odnosi się do stanu zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają samej cyberprzestrzeni, jak i funkcjonowania w niej, a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji[11]. Bankowość mobilna, jako kanał w pełni cyfrowy, jest narażona na szerokie spektrum zagrożeń, takich jak ataki typu *phishing* i *smishing* czy złośliwe oprogramowanie. Zapewnienie odpowiedniego poziomu bezpieczeństwa wymaga wielowarstwowego podejścia. Banki stosują obecnie zaawansowane mechanizmy kryptograficzne, uwierzytelnianie wieloskładnikowe, ale również prowadzą działalność edukacyjną i uświadamiającą w tym zakresie.

[11] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne, Akademia Sztuki wojennej, 2019,* s. 12-13.

W kontekście dalszych rozważań szczególnego znaczenia nabierają kwestie bezpieczeństwa danych klientów, architektury aplikacji oraz zgodności z regulacjami prawnymi, co stanowi kluczowy obszar analizy w kolejnych częściach niniejszej pracy.

2. Zagrożenia dla klientów związane z bankowością mobilną

W literaturze przedmiotu wskazuje się, że bankowość mobilna podlega szerokiemu spektrum zagrożeń, które można klasyfikować w różny sposób – od ataków technicznych i luk programistycznych, po błędy ludzkie i niebezpieczne zachowania klientów. Celem niniejszego rozdziału jest przedstawienie i omówienie kluczowych zagrożeń związanych z korzystaniem z bankowości mobilnej.

Zjawisko *phishingu* jest jednym z najpowszechniejszych zagrożeń. Polega na otrzymywaniu wiadomości mailowych, SMS lub poprzez komunikatory internetowe, które wydają się autentyczne. Ich celem jest pozyskanie danych osobowych odbiorcy. Sprawcy podszywają się pod znane instytucje lub zaufane osoby w celu pozyskania haseł bankowych i loginów. *Phishing* określany jest jako „łowienie haseł" (ang. *Password harvesting phishing*)[12]. W Polsce rozpoznano również pokrewne zagrożenie, tzw. „na BLIKa". Przestępcy wykradają dane logowania swoich ofiar do kont na komunikatorach społecznościowych, a następnie podszywając się, piszą wiadomość do potencjalnej ofiary, która znajduje się w grupie znajomych i proszą o szybką pożyczkę. Przykładowo informują, że stoją w sklepie przy kasie i zapomnieli portfela, a terminal obsługuje płatności Blikiem. W rzeczywistości oszust może stać przed bankomatem i czekać na podanie kodu, który umożliwi mu wypłatę pieniędzy bez użycia karty debetowej. W temacie bankowości popularne są również połączenia telefoniczne od rzekomych pracowników banku, którzy informują o konieczności zweryfikowania danych do logowania. Sprawcy *phishingu* często wysyłają wiadomości SMS informujące o konieczności uiszczenia dodatkowej opłaty za przesyłkę zamówioną np. na portalu Allegro.pl lub za paczkę, która nie istnieje. Celem sprawców *phishingu* jest wykorzystanie błędów ludzkich, a nie sprzęt czy jego oprogramowanie[13].

Kolejne zagrożenie to Man-in-theMiddle (MITM). Ataki MITM polegają na manipulowaniu istniejącymi sieciami lub tworzeniu złośliwych sieci kontrolowanych przez cyberprzestępcę. Cyberprzestępcy działają jako „pośrednicy" między osobą wysyłającą i odbierającą informację, wyłudzając informacje, stąd nazwa „atak man-in-the-middle". Ataki te są powszechne zwłaszcza w publicznych sieciach Wi-Fi,

---

[12] K.Oleś, *Phishing, skimming jako przestępstwa bankowe. Charakterystyka i metody działania sprawców*, s. 220, https://www.researchgate.net/profile/Dawid-Pytel/publication/380519519_Model_kompetencji_menedzerskich_w_kontekscie_nowych_wyzwan_zarzadzania_zasobami_ludzkimi_w_branzy_kinowej/links/6640989a7091b94e93217248/Model-kompetencji-menedzerskich-w-kontekscie-nowych-wyzwan-zarzadzania-zasobami-ludzkimi-w-branzy-kinowej.pdf#page=220, [dostęp: 30.09.2025].

[13] Ibidem, s. 222-225.

które często są niezabezpieczone, więc nie można wiedzieć, kto monitoruje lub przechwytuje ruch internetowy.

Skimming jest zagrożeniem, którego celem są karty płatnicze. Skimming wywodzi się z angielskiego słowa *skim* oznaczającego „zbierać", zatem definiowany jest jako „bezprawne skopiowanie informacji zapisanych na pasku magnetycznym umieszczonym na karcie płatniczej oraz przechwycenie zabezpieczającego kodu PIN bez wiedzy i zgody posiadacza lub użytkownika w celu wykonania duplikatu karty, służącego do obciążenia rachunku bankowego posiadacza"[14]. Najgroźniejszą odmianą *skimmingu* jest tzw. *skimming* bankomatowy, którego celem są bankomaty, a dokładniej modyfikacja (nielegalna) tych urządzeń w celu pozyskania danych. Na bankomatach montowane są urządzenia skanujące/skimmer, które kopiują dane znajdujące się na drugiej ścieżce paska magnetycznego. Informacje od razu są wysyłane do przestępcy znajdującego się w okolicy. Innych sposobem na modyfikację bankomatu jest instalacja bardzo małej kamerki lub nakładki na klawiaturę, które mają na celu wyłudzenie numeru PIN[15].

Niebezpieczeństwa w cyberprzestrzeni wynikają nie tylko z ataków technicznych. Zagrożenia stanowią również luki w oprogramowaniu w aplikacjach bankowych. Zaliczane są tutaj m.in. niewłaściwe projektowanie systemów lub niedostateczne testowanie aplikacji. Typowe przykłady obejmują brak odpowiedniego szyfrowania danych przesyłanych lub przechowywanych na urządzeniu mobilnym, podatności w interfejsach API umożliwiających komunikację aplikacji z serwerami bankowymi, a także zapisywanie wrażliwych informacji w pamięci urządzenia w sposób niezabezpieczony (np. w postaci jawnej). Błędy i słabości związane z oprogramowaniem stanowią „pokusę" dla przestępców do przejęcia danych uwierzytelniających lub manipulacji komunikacją między aplikacją a bankiem, co bezpośrednio zagraża poufności i integralności danych klientów.

Ostatnim ogniwem powodującym wyłudzenia są sami klienci i użytkownicy bankowości mobilnej. Nieostrożność lub brak świadomości zwiększa prawdopodobieństwo wystąpienia przestępstwa. Takie zachowania to m.in. instalowanie aplikacji z niepewnych źródeł, korzystanie z niezabezpieczonych sieci publicznych, stosowanie słabych lub powtarzalnych haseł, a także ignorowanie komunikatów i ostrzeżeń dotyczących bezpieczeństwa.

Zagrożenia związane z bankowością mobilną mają charakter wielowymiarowy i obejmują zarówno kwestie techniczne, wynikające z luk w oprogramowaniu czy zaawansowanych metod ataków cybernetycznych, jak i czynniki behawioralne związane z zachowaniami użytkowników. Analiza literatury wskazuje, że to właśnie połączenie niedoskonałości technologicznych z niskim poziomem świadomości klientów tworzy środowisko sprzyjające działalności cyberprzestępców. Z tego względu skuteczne przeciwdziałanie ryzyku w obszarze bankowości mobilnej wymaga podejścia

[14] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming,* Przegląd Bezpieczeństwa Wewnętrznego 2014, nr 10(6), s. 104.

[15] K. Oleś, Phishing..., s. 224-226.

kompleksowego – obejmującego zarówno rozwój i wdrażanie nowoczesnych zabezpieczeń technicznych, jak i systematyczne działania edukacyjne skierowane do użytkowników końcowych. Tylko równoczesne wzmocnienie obu tych obszarów może zagwarantować stabilny i bezpieczny rozwój usług bankowości mobilnej w perspektywie długoterminowej.

3. Zabezpieczenia stosowane przez bank

Rozwój bankowości internetowej i mobilnej sprawił, że korzystanie z konta stało się niezwykle wygodne i szybkie, jednak równocześnie pojawiły się nowe zagrożenia związane z bezpieczeństwem danych i środków finansowych. Aby chronić klientów przed ryzykiem, banki wdrażają rozbudowane mechanizmy ochronne. Ich zadaniem jest nie tylko zabezpieczenie infrastruktury technicznej, ale również wsparcie użytkownika w codziennym korzystaniu z usług online.

Jednym z najważniejszych elementów ochrony jest szyfrowanie komunikacji pomiędzy klientem a serwerem banku. W tym celu stosuje się protokoły SSL/TLS, które zapewniają poufność i nienaruszalność przesyłanych informacji. Dzięki nim dane logowania, numery rachunków czy szczegóły przelewów nie mogą zostać przechwycone i wykorzystane przez osoby niepowołane. Każdy klient powinien upewniać się, że adres strony banku rozpoczyna się od „https://" oraz że w pasku przeglądarki widoczna jest ikona kłódki.

Kolejną warstwą zabezpieczeń jest wieloskładnikowa autoryzacja (MFA). Oznacza ona, że logowanie czy zatwierdzanie transakcji nie opiera się wyłącznie na haśle. Do uwierzytelnienia wykorzystuje się zazwyczaj co najmniej dwa elementy: coś, co klient wie (np. hasło, PIN); coś, co posiada (np. token, aplikację mobilną z kodami jednorazowymi, SMS-kod) oraz biometrie (np. odcisk palca, rozpoznanie twarzy czy głosu). Dzięki temu samo przejęcie hasła nie pozwoli przestępcy na dostęp do konta.

Popularnym rozwiązaniem są wciąż kody jednorazowe – wysyłane SMS-em, generowane przez tokeny sprzętowe lub aplikacje bankowe. Każdy z nich jest ważny tylko raz i przez krótki czas, co uniemożliwia ponowne użycie. Coraz częściej banki odchodzą od SMS-ów na rzecz aplikacji mobilnych, które oferują wyższy poziom ochrony.

Znaczącą rolę odgrywają również metody biometryczne. Dzięki nim klient może logować się do aplikacji lub zatwierdzać przelewy przy użyciu odcisku palca, skanu twarzy czy głosu. Biometria jest nie tylko bezpieczna, ale i wygodna, ponieważ eliminuje konieczność pamiętania skomplikowanych haseł.

Banki wdrażają także monitoring aktywności. Systemy analizują charakterystyczne wzorce działań – godziny logowania, zwyczajowe kwoty przelewów, miejsca dostępu. Jeśli wykryją nietypowe zdarzenia, np. przelew na wysoką kwotę wysłany za granicę czy logowanie z nieznanej lokalizacji, mogą automatycznie zablokować transakcję, ograniczyć dostęp do konta lub skontaktować się z klientem. W tym celu stosuje się również limity transakcyjne, które ograniczają maksymalne kwoty przelewów w określonym czasie.

Oprócz tego banki inwestują w systemy ochrony przed *phishingiem*. Weryfikują autentyczność witryn poprzez certyfikaty EV SSL, korzystają z filtrów blokujących fałszywe wiadomości i współpracują z dostawcami oprogramowania antywirusowego. Celem tych działań jest maksymalne utrudnienie oszustw polegających na podszywaniu się pod bank.

Nie bez znaczenia są również działania organizacyjne – banki regularnie prowadzą kampanie edukacyjne, które przypominają o konieczności ostrożności w sieci i aktualizowania oprogramowania. W sytuacjach zagrożenia uruchamiane są procedury kryzysowe, takie jak blokowanie kont, zatrzymywanie przelewów i bezpośredni kontakt z klientem.

Wszystkie te mechanizmy tworzą wielowarstwowy system bezpieczeństwa, którego zadaniem jest zminimalizowanie ryzyka kradzieży danych i pieniędzy. Na ochronę składają się zarówno rozwiązania techniczne – szyfrowanie, biometryka, analiza ryzyka – jak i inicjatywy edukacyjne. Warto jednak pamiętać, że skuteczność tych zabezpieczeń zależy nie tylko od banku, lecz także od samych klientów. Nawet najbardziej zaawansowane narzędzia nie ochronią użytkownika, który lekkomyślnie udostępni swoje dane lub zignoruje podstawowe zasady bezpieczeństwa.

4. Przykłady banków i stosowanych rozwiązań zabezpieczających

Wraz z dynamicznym rozwojem bankowości mobilnej w Polsce (ponad 23 mln aktywnych użytkowników w 2024 r.[16]) rośnie znaczenie ochrony danych klientów. Banki wdrażają zróżnicowane rozwiązania – zarówno technologiczne, jak i edukacyjne – które mają minimalizować ryzyko utraty środków i poufnych informacji.

4.1. PKO Bank Polski

PKO BP, lider rynku mobilnego, w aplikacji IKO i serwisie iPKO stosuje m.in. uwierzytelnianie dwuetapowe, autoryzację mobilną zamiast kodów SMS, logowanie biometryczne oraz możliwość ustawiania limitów transakcji[17]. Dane użytkownika są szyfrowane, a aplikacja wymaga każdorazowej autoryzacji przy operacjach finansowych[18].

4.2. BNP Paribas Bank Polska

BNP Paribas koncentruje się na wykorzystaniu analizy behawioralnej – system monitoruje sposób korzystania z telefonu (np. tempo pisania, ruchy dłoni) i w razie wykrycia anomalii blokuje transakcję[19]. Dodatkowo stosowane są zabezpieczenia

[16] Związek Banków Polskich, *Raport: Bankowość Mobilna 2024*, bnpparibas.pl [dostęp: 30.09.2025].
[17] PKO Bank Polski, *Bezpieczne logowanie do banku online,* pkobp.pl [dostęp: 30.09.2025].
[18] PKO Bank Polski, *Mobilna autoryzacja IKO*, iko.pkobp.pl [dostęp: 30.09.2025].
[19] PRNews, *BNP Paribas rozpozna oszusta po tym, jak trzyma smartfon*, prnews.pl [dostęp: 30.09.2025 r.].

biometryczne oraz natychmiastowe powiadomienia o operacjach[20]. Rozwiązania te łączą klasyczne mechanizmy (PIN, limity) z nowoczesnymi metodami analizy zachowań.

4.3. Santander Bank Polska

Santander promuje model bezpieczeństwa oparty na edukacji użytkownika. W poradniku *5 zasad bezpiecznego bankowania* bank wskazuje m.in. na konieczność unikania podejrzanych linków, stosowania silnych haseł, instalacji aplikacji wyłącznie z oficjalnych źródeł oraz aktualizacji systemu[21]. Wyróżnia się również szybka reakcja na zgłoszenia klientów i zachęta do samodzielnego monitorowania konta.

Wnioski

Polskie banki konsekwentnie integrują zaawansowane technologie (biometrię, autoryzację mobilną, szyfrowanie) z działaniami edukacyjnymi. Badania wskazują, że „postrzegane ryzyko" ma istotny wpływ na akceptację bankowości mobilnej[22], dlatego kluczowe jest nie tylko wdrażanie zabezpieczeń, lecz także budowanie świadomości użytkowników. Przykłady PKO BP, BNP Paribas i Santandera dowodzą, że skuteczna ochrona danych wymaga współdziałania banku i klienta w ramach wielopoziomowego systemu bezpieczeństwa.

Zakończenie

Bankowość mobilna stała się integralną częścią współczesnego systemu finansowego, a jej znaczenie rośnie wraz z postępującą cyfryzacją usług i potrzebą natychmiastowego dostępu do informacji finansowych. Analiza rozwoju tego sektora pokazuje, że polskie banki z powodzeniem wdrożyły nowoczesne rozwiązania technologiczne, które zapewniają klientom wygodę, szybkość i elastyczność w zarządzaniu finansami. Jednocześnie rozwój ten wiąże się z koniecznością stałego wzmacniania ochrony danych osobowych i finansowych.

Przedstawione w artykule przykłady działań PKO Banku Polskiego, BNP Paribas oraz Santander Bank Polska dowodzą, że skuteczne bezpieczeństwo w bankowości mobilnej wymaga wielopoziomowego podejścia – łączącego technologię, procedury organizacyjne i edukację użytkowników. Zastosowanie rozwiązań takich jak uwierzytelnianie wieloskładnikowe, biometria, szyfrowanie danych czy analiza behawioralna znacząco ogranicza ryzyko utraty środków i nieuprawnionego dostępu do informacji.

---

[20] BNP Paribas, *7 zasad bezpieczeństwa bankowości mobilnej*, bnpparibas.pl [dostęp: 30.09.2025].

[21] Santander Bank Polska, *5 zasad bezpiecznego bankowania*, santander.pl [dostęp: 30.09.2025 r.].

[22] P. Sikorski, *The usage of mobile banking applications in Poland – empirical results*, *ResearchGate*, 2019.

Wnioski płynące z opracowania wskazują, że dalszy rozwój bankowości mobilnej powinien opierać się na dwóch filarach: innowacyjnych technologiach bezpieczeństwa oraz świadomym, odpowiedzialnym użytkowniku. Tylko synergia tych elementów pozwoli utrzymać wysoki poziom zaufania klientów i zapewnić stabilny rozwój cyfrowych usług finansowych w przyszłości.

Bibliografia

1. Ataki typu „man-in-the-middle" (MITM), [online] https://www.keepersecurity.com/pl_PL/threats/man-in-the-middle-attacks-mitm.html [dostęp: 30.09.2025].
2. BNP Paribas, *7 zasad bezpieczeństwa bankowości mobilnej*, bnpparibas.pl [dostęp: 30.09.2025].
3. Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne,* Akademia Sztuki Wojennej, Warszawa, 2019.
4. Dobosiewicz Z., *Bankowość*, PWE, Warszawa, 2011.
5. Hassa T., *Stan i perspektywy rozwoju bankowości mobilnej dla klientów indywidualnych w Polsce,* Szkoła Główna Handlowa w Warszawie, 2013.
6. *Historia bankowości mobilnej*, http://komorkomania.pl/2010/04/02/historia-mobilnej-bankowosci [dostęp: 30.09.2025].
7. *Historia bankowości mobilnej – jak to się wszystko zaczęło?,* [online] https://finanteq.com/blog/fintech-trends/history-of-mobile-banking-how-it-all-started/#:~:text=The%20Bank%20of%20Scotland%20is,ATMs%20as%20early%20as%202004 [dostęp: 30.09.2025].
8. Instytut Badań nad Gospodarką Rynkową, *Prognoza rozwoju rynku bankowego do 2016 r.,* Gdańsk, kwiecień 2012.
9. Janc A., Kotliński G., *Nowe technologie we współczesnym banku*, Akademia Ekonomiczna w Poznaniu, Poznań, 2004.
10. Kochańska M., *Historia bankowości mobilnej*, https://whitehats.pwr.edu.pl/research/history-of-mobile-banking/ [dostęp: 30.09.2025].
11. Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming,* Przegląd Bezpieczeństwa Wewnętrznego 2014, nr 10(6).
12. Oleś K., *Phishing, skimming jako przestępstwa bankowe. Charakterystyka i metody działania sprawców*, Dąbrowa Górnicza 2023, [online] https://www.researchgate.net/profile/Dawid-Pytel/publication/380519519_Model_kompetencji_menedzerskich_w_kontekscie_nowych_wyzwan_zarzadzania_zasobami_ludzkimi_w_branzy_kinowej/links/6640989a7091b94e93217248/Model-kompetencji-menedzerskich-w-kontekscie-nowych-wyzwan-zarzadzania-zasobami-ludzkimi-w-branzy-kinowej.pdf#page=220 [dostęp: 30.09.2025].
13. PKO Bank Polski, *Bezpieczne logowanie do banku online,* pkobp.pl [dostęp: 30.09.2025].
14. PKO Bank Polski, *Mobilna autoryzacja IKO*, iko.pkobp.pl [dostęp: 30.09.2025].
15. PRNews, *BNP Paribas rozpozna oszusta po tym, jak trzyma smartfon*, prnews.pl [dostęp: 30.09.2025].

16. Santander Bank Polska, *5 zasad bezpiecznego bankowania*, santander.pl [dostęp: 30.09.2025].
17. Sikorski P., *The usage of mobile banking applications in Poland – empirical results*, ResearchGate, 2019.
18. Uytterhoeven G., *Financial services through mobile devices*, „Efma Journal", nr 228, kwiecień–czerwiec 2011.
19. Związek Banków Polskich, *Raport: Bankowość Mobilna 2024*, bnpparibas.pl [dostęp: 30.09.2025].

THE DEVELOPMENT OF MOBILE BANKING AND CUSTOMER DATA SECURITY

Abstract

Paper discussed the development of mobile banking in Poland and the related challenges concerning customer data security. It presents the main threats and the solutions implemented by banks. Based on examples from selected financial institutions, it is shown that effective protection requires combining modern technologies with user education. The article emphasizes that the further development of mobile banking should be based on innovative security measures and responsible use of digital services.

Keywords: bank, mobile banking, security of information.