ROCZNIKI EKONOMII I ZARZĄDZANIA
Tom 6(42), numer 2 – 2014

PIOTR BOLIBOK
ANNA MATRAS-BOLIBOK

BANKOWOŚĆ MOBILNA JAKO INNOWACYJNY KANAŁ DOSTĘPU DO USŁUG BANKOWYCH

WSTĘP

Dynamiczny rozwój technologii teleinformatycznych w ostatnich kilkunastu latach doprowadził do wyodrębnienia nowego rodzaju bankowości elektronicznej, jaką jest bankowość mobilna. Istotą bankowości mobilnej jest umożliwienie użytkownikom zdalnego korzystania z usług bankowych za pośrednictwem różnego rodzaju urządzeń przenośnych przy zastosowaniu metod komunikacji niegłosowej (np. SMS, przeglądarki internetowe, aplikacje mobilne). Tym samym, głosowa komunikacja z bankiem poprzez *call center* lub IVR (ang. *interactive voice response*), nawet jeżeli jest realizowana za pomocą urządzeń przenośnych, nie powinna być uznawana za bankowość mobilną[1].

Początki bankowości mobilnej sięgają połowy lat dziewięćdziesiątych XX wieku, jednak jej ekspansja rynkowa przebiegała znacznie wolniej w porównaniu do bankowości internetowej, która pojawiła się w tym samym okresie. Główną przyczyną tego zjawiska była ograniczona funkcjonalność i ergonomia wcześniejszych generacji telefonów komórkowych oraz relatywnie wysokie koszty transferu danych, które wpływały na postrzeganie bankowości mobilnej jedynie w kategoriach uzupełniającego kanału dostępu, służącego wyłącznie realizacji najprostszych form komunikacji z bankiem.

DR PIOTR BOLIBOK – adiunkt Katedry Bankowości i Finansów, Instytut Ekonomii i Zarządzania na Wydziale Nauk Społecznych Katolickiego Uniwersytetu Lubelskiego Jana Pawła II; adres do korespondencji: Al. Racławickie 14, 20-950 Lublin; e-mail: piotr.bolibok@kul. pl

DR ANNA MATRAS-BOLIBOK – adiunkt Katedry Ekonomii i Agrobiznesu, Wydział Agrobioinżynierii Uniwersytetu Przyrodniczego w Lublinie; adres do korespondencji: ul. Akademicka 13, 20-950 Lublin; e-mail: anna.matras@up.lublin.pl.

[1] M. POLASIK, *Bankowość elektroniczna. Istota – stan – perspektywy*, CeDeWu, Warszawa 2012, s. 25.

Impulsem, który stopniowo zmienia ten wizerunek i dynamizuje rozwój bankowości mobilnej w ostatnich latach, stała się znacząca poprawa wydajności i funkcjonalności urządzeń przenośnych, zwłaszcza w obszarze połączeń internetowych. Nowoczesne generacje smartfonów i tabletów umożliwiają komfortową, wielokanałową komunikację klienta z bankiem, w tym pełnienie funkcji kart płatniczych, pozwalając na realizację transakcji w punktach handlowo-usługowych, czy wypłatę gotówki w bankomatach. Postęp ten sprawił, że bankowość mobilna zaczyna być obecnie traktowana jako najważniejsza wiązka innowacji w bankowości detalicznej[2].

Perspektywa komfortowego korzystania z dostępu do usług bankowych w dowolnym miejscu i czasie w połączeniu z systematycznym spadkiem cen zaawansowanych urządzeń przenośnych oraz kosztów komunikacji niegłosowej sprawia, że bankowość mobilna może się stać w najbliższym czasie realną alternatywą dla pozostałych form kontaktu klientów z bankiem. Z punktu widzenia banków stanowi ona kolejną metodę zwiększenia samoobsługi klientów w zakresie realizacji czynności bankowych, co w dłuższej perspektywie powinno przyczyniać się do redukcji kosztów ich działalności i poprawy rentowności. Z kolei osobisty charakter i multimedialne funkcjonalności nowoczesnych urządzeń mobilnych pozwalają na bardziej trwałe związanie klienta z bankiem oraz adresowanie do niego spersonalizowanych ofert produktowych i informacji marketingowych[3].

Celem artykułu jest przedstawienie ewolucji innowacyjnych rozwiązań w bankowości mobilnej ze szczególnym uwzględnieniem kwestii bezpieczeństwa tego kanału dostępu do usług bankowych. Pozostała część artykułu składa się z pięciu sekcji. W sekcji pierwszej omówione zostały wykorzystane w opracowaniu źródła danych i metody badawcze. Sekcja druga poświęcona została przedstawieniu genezy oraz dotychczasowych i przewidywanych kierunków rozwoju bankowości mobilnej. W sekcji trzeciej scharakteryzowano najważniejsze współczesne i prognozowane funkcjonalności tego kanału dostępu do usług bankowych, natomiast sekcja czwarta prezentuje zagadnienia związane z jego bezpieczeństwem. Artykuł zamyka podsumowanie zawarte w sekcji piątej.

[2] B. ENSOR [i in.], *The state of mobile banking 2012*, Forrester Research Inc., Cambridge 2012, s. 2.

[3] *World retail banking report 2013,* Capgemini, Efma 2013, s. 5, 20, http://www.capgemini.com/resource-file-access/resource/pdf/wrbr_2013.pdf [dostęp: 24.03.2014].

1. ŹRÓDŁA DANYCH I METODY BADAWCZE

Przedstawione w artykule rozważania i analizy oparte zostały na dostępnych wynikach aktualnych badań przeprowadzonych przez wiodące instytucje, zajmujące się problematyką rozwoju rynku bankowości mobilnej: TNS Global, TNS Polska, Ipsos, Capgemini, Efma, Forrester Inc., Mobile Marketing Association oraz Zarząd Rezerwy Federalnej Stanów Zjednoczonych. Wykorzystano również informacje dotyczące najbardziej zaawansowanych obecnie aplikacji mobilnych na rynku polskim pochodzące ze stron internetowych banków PKO BP SA i Pekao SA. Dodatkowym źródłem informacji były także publikacje Komisji Nadzoru Finansowego.

W opracowaniu zastosowano metody przeglądu oraz analizy krytycznej, opisowej i porównawczej treści zawartych w dostępnych krajowych i zagranicznych źródłach literatury przedmiotu oraz raportach poświęconych problematyce bankowości mobilnej. Wybrane zagadnienia zaprezentowano w postaci tabelarycznej i graficznej.

2. ROZWÓJ RYNKU BANKOWOŚCI MOBILNEJ

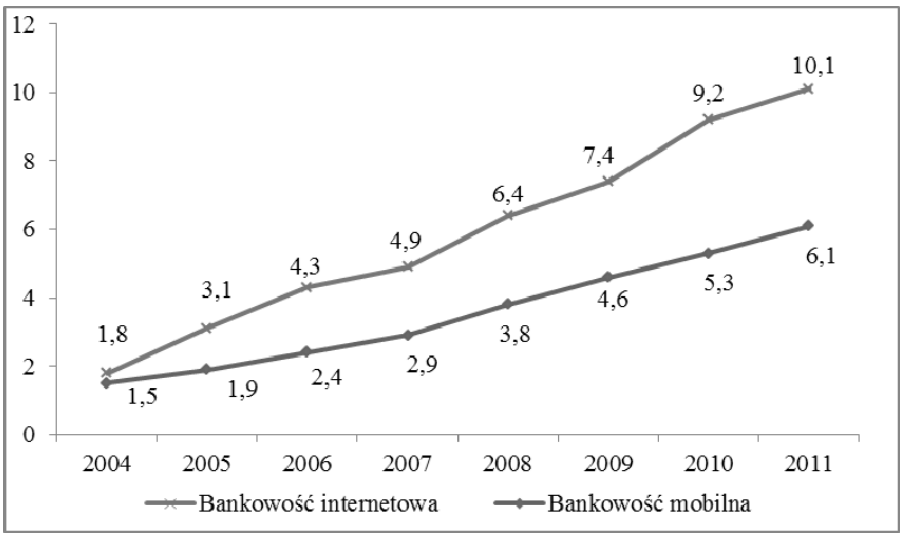
Początki bankowości mobilnej na świecie związane były z wprowadzeniem w 1996 r. przez fiński OKO Bank usług opartych na komunikacji SMS. W 1999 r. ten sam bank stał się prekursorem w zakresie umożliwienia klientom dostępu do usług poprzez mobilną stronę internetową opartą na protokole WAP. Dwa lata później usługę WAP uruchomił natomiast amerykański gigant (i jeden z pionierów bankowości internetowej) – Wells Fargo[4].

W Polsce bankowość mobilna zaczęła rozwijać się w 2000 r., kiedy to kanał informacyjny SMS oraz mobilną stronę internetową opartą na protokole WAP uruchomił Bank Zachodni WBK. W tym samym roku usługi te wdrożył również mBank. Dwa lata później Inteligo i Raiffeisen Bank zaoferowały usługi oparte o SIM ToolKit oraz protokół WAP 2.0. W 2005 r. Bank Millennium wprowadził powiadomienia SMS, a w kolejnym roku ING Bank Śląski, Citi Handlowy, Multibank i mBank rozpoczęły wykorzystanie kanału SMS do autoryzacji transakcji (hasła). Najbardziej zaawansowane rozwiązania, jak *mobile web* i aplikacje

[4] T. KOŹLIŃSKI, *Bankowość internetowa. Część II – rozwój na świecie i w Polsce*, „Bank i Kredyt" 36 (2005), nr 6, s. 33-34.

klienckie zaczęły być uruchamiane od 2009 r. – pionierami w tym obszarze były Citi Handlowy, Alior Bank i Inteligo[5].

W początkowej fazie rozwoju bankowości mobilnej niewygodny interfejs i ograniczona funkcjonalność starszych generacji telefonów komórkowych w połączeniu z wysokimi kosztami transferu danych utrudniały komfortową komunikację z bankiem, osłabiając tym samym dynamikę ekspansji rynkowej tego kanału dostępu, zwłaszcza w porównaniu z dynamicznie rozwijającą się bankowością internetową (rys. 1).



Rys. 1. Liczba rachunków bankowych klientów indywidualnych w Polsce z aktywnym dostępem internetowym oraz aktywnymi usługami mobilnymi w latach 2004-2011 [w mln]

Źródło: Opracowanie własne na podstawie: M. POLASIK, *Wykorzystanie elektronicznych kanałów dystrybucji usług bankowych w Polsce,* „Copernican Journal of Finance & Accounting" 2 (2013) 1, s. 144.

W ostatnich latach dynamika rozwoju rynku bankowości mobilnej uległa wyraźnemu przyspieszeniu, głównie za sprawą upowszechnienia i poprawy funkcjonalności przenośnych urządzeń komunikacyjnych, takich jak smartfony czy tablety, oraz relatywnego spadku kosztów transferu danych w sieciach komórkowych.

W świetle badań przeprowadzonych w 2013 r. przez TNS Global w 43 krajach świata na grupie 38 tys. konsumentów, z bankowości mobilnej korzystało już

[5] A. JADCZAK, *Bankowość mobilna – najnowsze rozwiązania i przykłady techniczne,* Evangelist 2011, s. 3, http://www.rewolucjawfinansach.pl/download/gfx/rewolucjawfinansach/ pl/ default aktualnosci/ 12/7/1/08062011_rwf_evangelist_arek_jadczak.pdf [dostęp: 24.03.2014].

średnio 22% użytkowników telefonów komórkowych[6]. W Stanach Zjednoczonych odsetek ten jest nieco wyższy i wynosi 28% (48% dla posiadaczy smartfonów), co odpowiada blisko 24% populacji dorosłych[7]. W Europie odsetek klientów bankowości mobilnej szacowany jest obecnie również na ok. 25% populacji[8]. W Polsce natomiast udział użytkowników bankowości mobilnej wśród posiadaczy telefonów komórkowych jest wyraźnie niższy – w 2013 r. szacowany był on na 12% (29% dla posiadaczy smartfonów)[9].

Publikowane prognozy przewidują kontynuację tendencji wzrostowej rynku bankowości mobilnej na całym świecie, głównie za sprawą upowszechniania się smartfonów. Co ciekawe, szczególnie dynamiczny wzrost oczekiwany jest w krajach rozwijających się, w których jest ona często jedynym możliwym kanałem zdalnego dostępu do usług bankowych, a tym samym istotnym narzędziem ubankowienia społeczeństwa[10]. Uzyskane dzięki niej zmniejszenie zależności od infrastruktury bankowej powinno zatem przyczynić się do ograniczenia istniejących dysproporcji regionalnych w korzystaniu z usług banków w skali świata.

3. FUNKCJONALNOŚCI BANKOWOŚCI MOBILNEJ

Podstawową technologią wykorzystywaną w bankowości mobilnej są usługi SMS (ang. *short message service*), polegające na komunikacji za pomocą krótkich wiadomości tekstowych w sieciach telefonii komórkowej. Wiadomości te mogą dotyczyć informacji o saldach na rachunkach bankowych, historii operacji, potwierdzeń zrealizowanych operacji lub ostrzeżeń (tzw. *alerting*[11]). Powszechnym zastosowaniem SMS we współczesnej bankowości jest również autoryzacja operacji zlecanych kanałem internetowym, w ramach której bank przesyła kod

[6] *Mobile Life 2013*, TNS Global 2013, http://www.tnsglobal.pl/obszary-dzialania/mobile/ [dostęp: 09.03.2014].

[7] *Consumers and Mobile Financial Services 2013,* Washington: Board of Governors of the Federal Reserve System 2013, s. 4, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf [dostęp: 25.03.2014].

[8] *Financial empowerment in the digital age*. *Mobile banking, social media and financial behaviour*, ING 2013, s. 7-8, https://www.ing-diba.at/uploads/media/ING_International_Survey_-_Financial_Empowerment_in_the_Digital_Age_-Jul..._01.pdf [dostęp: 24.03.2014].

[9] *Mobile Life…, Rola mobilnych finansów w życiu Polaków*. *Raport przygotowany przez TNS Polska i jestem.mobi na zlecenie Getin Banku*, Getin Bank 2013, s. 30, https://getinup.pl/raport/pdf/rola_mobilnych_finansow_w_zyciu_polakow_raport_z_badania.pdf [dostęp: 09.03.2014].

[10] ENSOR [i in.], *The state*, s. 23.

[11] *Innowacyjne usługi banku*, red. D. Korenik, Wydawnictwo Naukowe PWN, Warszawa 2006, s. 248.

autoryzacyjny na numer telefonu komórkowego klienta w celu wprowadzenia go w formularzu składanego zlecenia internetowego, jako substytutu podpisu potwierdzającego autentyczność dyspozycji.

Wśród technologii wykorzystywanych w bankowości mobilnej wskazać można również komunikację w ramach protokołu WAP (ang. *wireless application protocol*), stanowiącego odpowiednik protokołu HTTP (ang. *hypertext transfer protocol*), ale dostosowanego do ograniczeń technicznych i komunikacyjnych urządzeń mobilnych starszej generacji. Realizacja operacji bankowych za pomocą WAP odbywa się analogicznie jak w tradycyjnej bankowości internetowej (logowanie do serwisu, wybór operacji bankowej do zrealizowania, ustalenie jej parametrów, a następnie autoryzacja)[12]. Technologia WAP nie zdobyła jednak szerszej akceptacji ze strony klientów banków z uwagi na niewygodną i skomplikowaną obsługę oraz powolność działania, co zdecydowanie ograniczało jej atrakcyjność[13].

Kolejnym rozwiązaniem możliwym do stosowania w bankowości mobilnej jest przesyłanie klientowi przez bank informacji (zwykle o charakterze marketingowym) w ramach usługi MMS (ang. *multimedia messaging service*). Usługa ta umożliwia dostarczanie poprzez sieć komórkową wiadomości graficznych, animacji czy sekwencji wideo wraz z dźwiękiem.

W zakresie możliwości wykorzystania w kontaktach pomiędzy klientem a bankiem zaawansowanych możliwości współczesnych telefonów komórkowych, wspomnieć należy również o koncepcji bankowości multimedialnej, obejmującej m.in. możliwość realizacji połączeń wideo z konsultantami banku w ramach technologii UMTS[14]. Jak dotąd, rozwiązanie to nie znalazło jednak szerszego zastosowania na rynku, gdyż w praktyce trudno jest wskazać merytoryczne przesłanki dla istotnej przewagi tego typu komunikacji nad komunikacją wyłącznie głosową. Biorąc ponadto pod uwagę fakt, iż komunikacja głosowa warunkuje możliwość komunikacji wideo, należałoby uznać to rozwiązanie po prostu za bardziej zaawansowaną formę usługi *call center* i zaliczyć ją raczej do bardziej zaawansowanej bankowości telefonicznej niż mobilnej.

Kolejną technologią wykorzystywaną w bankowości mobilnej są zapisywane na karcie SIM telefonu aplikacje SAT (ang. SIM Application Toolkit). Dzięki temu rozwiązaniu możliwe jest realizowanie usług bankowych bezpośrednio z menu telefonu. Opracowanie i instalacja takich aplikacji wymaga jednak współpracy pomiędzy bankiem a operatorami poszczególnych sieci telefonii komórko-

[12] POLASIK, *Bankowość*, s. 25.
[13] *Innowacyjne usługi*, s. 246.
[14] POLASIK, *Bankowość*, s. 25.

wej, co w przypadku braku uzgodnienia stanowisk, może skutkować ograniczeniem zasięgu odbiorców usługi do klientów konkretnych sieci komórkowych. Taka sytuacja może stwarzać dodatkowe niedogodności dla klientów banku, gdyż chcąc skorzystać z oferowanej przez bank usługi musieliby być jednocześnie klientami sieci komórkowej, z którą bank współpracuje[15].

Stale wzrastająca moc obliczeniowa urządzeń przenośnych oraz malejące koszty transmisji danych w sieciach komórkowych sprawiają, że we współczesnej bankowości mobilnej coraz bardziej powszechnie wykorzystywane są aplikacje mobilne oferowane przez banki. Aplikacje te po zainstalowaniu na urządzeniu przenośnym klienta umożliwiają realizację typowych operacji bankowości internetowej, wykorzystując do tego celu komunikację w ramach sieci GSM lub poprzez łącze WiFi. Kluczową przewagą aplikacji mobilnych nad dostępem do usług bankowych poprzez przeglądarkę internetową jest czytelny interfejs dostosowany do niewielkich rozmiarów ekranów urządzeń przenośnych, znacznie podnoszący komfort pracy. Istotna jest także redukcja wolumenu przesyłanych danych (nawet tysiąckrotnie), służąca przyspieszeniu komunikacji i ograniczeniu jej kosztów[16]. Rozwiązanie to podnosi jednak koszty ponoszone przez banki w związku z koniecznością opracowania i aktualizacji aplikacji dla zróżnicowanych platform sprzętowych i systemów operacyjnych, a także zapewnienia jej bezpiecznego i niezawodnego funkcjonowania[17].

Oprócz standardowych operacji bankowych, jak sprawdzenie sald i historii rachunku, obsługa kart płatniczych, lokat, kredytów, czy realizacja przelewów, operacje na lokatach, współczesne aplikacje bankowości mobilnej oferują również cały szereg dodatkowych funkcjonalności, jak wyszukiwanie bankomatów i placówek banku (poprzez GPS), informacje o kursach walut, kanał szybkiego kontaktu z bankiem, doładowywanie telefonu, wyszukiwarki rabatów czy skaner kodów QR[18].

Konkurencyjną w stosunku do aplikacji mobilnych technologią komunikacji klienta z bankiem jest tworzenie uproszczonych stron internetowych serwisów transakcyjnych banków, przystosowanych do przeglądania na urządzeniach przenośnych (tzw. wersje *light* lub *mobile web*). Rozwiązanie to pozwala bankom na

[15] *Innowacyjne usługi*, s. 246.

[16] P. SKRZYŃSKI, *Mobilna bankowość – potrzeba czy moda?*, Mobiltek 2011, s. 13, http://www.mobiltek.pl/wp-content/uploads/2011/10/mobilna-bankowosc-potrzeba-czy-moda.pdf [dostęp: 24.03.2013].

[17] POLASIK, *Wykorzystanie elektronicznych kanałów*, s. 147.

[18] *Kieszonkowe aplikacje bankowe 2013*, Symetria.pl 2013, s. 4, http://symetria.pl/blog/wp-content/uploads/2013/11/Raport_Symetrii_Kieszonkowe_Aplikacje_Bankowe_2013.pdf [dostęp: 14.03. 2014].

zmniejszenie kosztów wdrażania usług mobilnych, ale nie rozwiązuje problemu ograniczonej ergonomii korzystania z przeglądarek internetowych na urządzeniach przenośnych niewielkich rozmiarów[19]. Ponadto, nowoczesne smartfony zazwyczaj bezproblemowo obsługują zwykłe strony internetowe.

Urządzenia mobilne mogą być również wykorzystane w bankowości jako instrumenty płatnicze. Współczesne technologie teleinformatyczne umożliwiają rozmaite sposoby realizacji płatności. Wśród najczęściej stosowanych wymienić można wbudowane w urządzenia przenośne karty płatnicze w technologii zbliżeniowej RFID (ang. *radio frequency identification*), w szczególności smartfony z chipem NFC (ang. *near field communication*) umożliwiającym komunikację bezstykową za pomocą dedykowanej aplikacji oraz danych karty płatniczej umieszczonych na karcie SIM-NFC[20] lub SD-NFC[21]. Telefony obsługujące NFC mogą nie tylko emulować działanie zbliżeniowych kart płatniczych, ale również pełniąc jednocześnie funkcje karty i czytnika, oferują użytkownikom zdecydowanie szersze spektrum możliwości komunikacyjnych i płatniczych[22].

Aktualnie najbardziej zaawansowane mobilne aplikacje płatnicze na rynku polskim to IKO Banku PKO BP SA oraz PeoPay Banku Pekao SA. Umożliwiają one w szczególności dokonywanie za pomocą telefonu płatności w wybranych punktach handlowo-usługowych oraz sklepach internetowych, wypłatę gotówki z przystosowanych do ich obsługi bankomatów oraz realizację przelewów pomiędzy użytkownikami aplikacji[23].

Wyniki badań przeprowadzonych przez Forrester Inc. na 59 bankach z 13 krajów rozwiniętych wykazały, że niemal wszystkie duże banki i wiele mniejszych oferuje wielokanałowe usługi bankowości mobilnej. Niemal ¾ z nich umożliwia klientom dostęp do serwisu transakcyjnego zarówno przez mobilne strony internetowe, jak i aplikacje, a blisko 90% oferuje powiadomienia SMS[24].

---

[19] POLASIK, *Wykorzystanie elektronicznych kanałów*, s. 145-146.

[20] Przykładami takiej integracji na rynku polskim mogą być usługi oparte na technologii MasterCard *paypass*^{TM} : *Orange Cash* oferowana przez operatora sieci Orange we współpracy z mBankiem oraz *MyWallet* oferowana przez T-Mobile we współpracy z Raiffeisen-Polbankiem, mBankiem, Getin Bankiem i Noble Bankiem i Alior Bankiem.

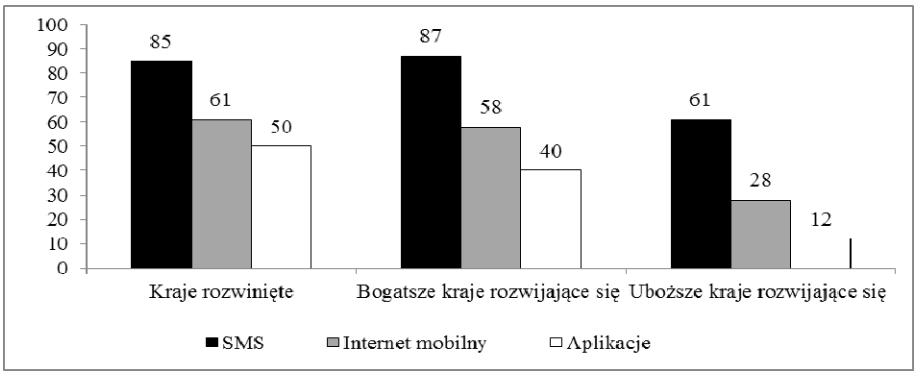
[21] *Mobilne płatności zbliżeniowe – o czym warto wiedzieć*, KNF, Warszawa 2012, s. 1, http:// www.knf.gov.pl/ Images/ mobline_platnosci_tcm75-32797.pdf [dostęp: 09.03.2014].

[22] M. POLASIK, K. MACIEJEWSKI, *Innowacyjne usługi płatnicze w Polsce i na świecie*, „Materiały i Studia" Narodowy Bank Polski 241, Warszawa 2009, s. 40.

[23] http://www.peopay.pl/ [dostęp: 14.03.2014]; http://www.pkobp.pl/iko-platnosci-mobilne/ [dostęp: 14.03.2014].

[24] ENSOR [i in.], *The state*, s. 3-4.

Według TNS Global najbardziej powszechną funkcjonalnością telefonów komórkowych wykorzystywaną w realizacji mobilnych usług finansowych wciąż pozostają SMS-y. Kolejne miejsce zajmują, odpowiednio, mobilny internet i aplikacje, przy czym w krajach rozwiniętych i bogatszych krajach rozwijających się udział tych ostatnich staje się już porównywalny (rysunek 2).



Rys. 2. Funkcjonalności telefonów komórkowych wykorzystywane w mobilnych usługach finansowych według grup krajów [w %]

Źródło: Opracowanie własne na podstawie *Mobile Life 2013*, TNS Global 2013 http://www.tnsglobal.pl/obszary-dzialania/mobile/ [dostęp: 09.03.2014].

Wachlarz usług oferowanych w bankowości mobilnej nieustannie się poszerza. Nowoczesne smartfony stają się stopniowo narzędziami powszechnego użytku, wspomagającymi całą gamę codziennych czynności, w tym zarządzanie osobistymi finansami i kontakt klienta z bankiem[25]. Przewiduje się, że w przyszłości kompleksowa bankowość mobilna obejmować będzie cztery główne komponenty[26]:

1) zarządzanie finansami osobistymi przez wyspecjalizowane aplikacje dedykowane kontroli domowych budżetów,

2) zintegrowaną platformę płatności mobilnych – od zbliżeniowych, przez serwisy płatnicze, aż do płatności na portalach społecznościowych,

3) cyfrowy portfel – zintegrowanie technologii QR i NFC pozwoli zamienić smartfon w wielofunkcyjne urządzenie wspomagające realizację zakupów (płatności, informacja o produktach, otrzymywanie paragonów, upustów, punktów lojalnościowych),

[25] M. ZŁOCH, *Smartfon: klucz do bankowości*, „Miesięcznik Finansowy BANK" 240 (2009), nr 1, s. 50-53.

[26] Ibidem, s. 22-23.

4) kanał marketingu kontekstowego – dostarczanie klientom spersonalizowanych ofert, materiałów reklamowych i promocyjnych, w tym w ramach cross-sellingu.

Istotna poprawa funkcjonalności i kosztów eksploatacji urządzeń przenośnych w połączeniu z brakiem ograniczeń czasowych i przestrzennych mogą zatem sprawić, że bankowość mobilna będzie stopniowo zmniejszać dystans do innych kanałów dostępu.

4. BEZPIECZEŃSTWO USŁUG BANKOWOŚCI MOBILNEJ

Kluczową cechą bankowości mobilnej jest wykorzystywanie urządzeń przenośnych komunikujących się z systemami teleinformatycznymi banku za pośrednictwem łączności bezprzewodowej. Z tego powodu źródeł potencjalnych zagrożeń dla klientów upatrywać należy w możliwości nielegalnego przechwycenia wrażliwych danych zarówno wprost z urządzenia ofiary ataku, jak i w trakcie komunikacji nawiązywanej pomiędzy nim a infrastrukturą sieci bezprzewodowej. Użytkownicy bankowości mobilnej są zatem narażeni na rozmaite zagrożenia typowe dla innych form zdalnego dostępu do usług (tabela 1.).

Tabela 1. Zagrożenia w bankowości mobilnej

Lp.	**Rodzaj zagrożenia**	**Opis**
1	Klonowanie (ang. *cloning*)	Kopiowanie tożsamości jednego urządzenia przenośnego na inne, umożliwiające sprawcy podszycie się pod klienta w celu uzyskania dostępu do jego rachunków bankowych.
2	Przejęcie kontroli (ang. *hijacking*)	Przejęcie przez sprawcę kontroli nad komunikacją pomiędzy bankiem a klientem, poprzez podszycie się pod jedną ze stron w celu uzyskania dostępu do rachunków bankowych klienta.
3	Szkodliwe oprogramowanie (ang. *malware*)	Oprogramowanie wprowadzone do systemu informatycznego, zazwyczaj niejawnie, na urządzeniu przenośnym ofiary, bramce SMS lub serwerze banku dostarczającego usług mobilnych, z zamiarem naruszenia poufności, integralności lub dostępności informacji lub transakcji finansowych.
4	Atak typu „człowiek pośrodku” (ang. *man-in-the-middle attack*)	Atak skierowany na wymianę danych w ramach protokołu uwierzytelniającego, w trakcie którego sprawca zajmuje pozycję pomiędzy klientem i weryfikatorem z zamiarem przechwycenia i modyfikacji przesyłanych danych.
5	Wyłudzanie (ang. *phishing*)	Podszywanie się przez sprawcę pod bank w celu skłonienia ofiary do ujawnienia wrażliwych informacji osobistych (np. danych niezbędnych do

		logowania w systemie) lub instalacji szkodliwego oprogramowania. Odmianami wyłudzania często występującymi w bankowości mobilnej są: • *vishing* (*voice and phishing*) – nakłanianie ofiary do ujawnienia infroamcji wrażliwych w trakcie rozmowy telefonicznej, • SMiShing – wykorzystanie kanału SMS do fałszywych żądań ujawnienia informacji osobistych.
6	Przekierowanie (ang. *redirecting*)	Przechwycenie komunikacji między klientem a bankiem przez zastosowanie fałszywego adresu lub tożsamości elektronicznej, potencjalnie dzięki skutecznemu przeprowadzeniu ataku typu „człowiek pośrodku".
7	Podszywanie się (ang. *spoofing*)	Wysyłanie sieciowych pakietów danych pozorujących pochodzenie z uprawnionego źródła.

Źródło: Opracowanie własne na podstawie *Mobile Banking Overview (NA)*, Mobile Marketing Association 2009, s. 10, http://www.mmaglobal.com/files/mbankingoverview.pdf [dostęp: 09.03.2014].

Transmisje w sieciach GSM są szyfrowane specjalnymi algorytmami i odpowiednio zabezpieczane sprzętowo. Skuteczność potencjalnego ataku wymagałaby nielegalnego transmitowania przez przestępcę drogą bezprzewodową specyficznych danych imitujących stację bazową GSM oraz fizycznej obecności pomiędzy klientem a rzeczywistą stacją bazową. Znacznie trudniejsze byłoby przechwycenie danych transmitowanych w sieciach CDMA, wykorzystujących rozpraszanie sygnałów połączeń w całej szerokości pasma komunikacyjnego, przez co nabierają one charakterystyki szumów dla innych urządzeń komunikacyjnych lub detektorów. Taka architektura sieci wymagałaby od przestępcy próbującego przechwycić dane użycia równocześnie wielu połączonych urządzeń w celu synchronizacji z docelowym sygnałem[27].

Wśród głównych zagrożeń związanych z realizacją transakcji zbliżeniowych za pomocą urządzeń mobilnych wskazać można natomiast[28]:

1) fizyczną utratę urządzenia przenośnego,
2) nieuprawniony odczyt danych,
3) atak typu przekaźnikowego,
4) logiczne klonowanie karty.

Fizyczna utrata urządzenia mobilnego umożliwiającego realizację płatności zbliżeniowych wiąże się z zagrożeniem realizacji nieuprawnionych transakcji mieszczących się w jednostkowym limicie 50 PLN. Czynnikami ograniczającymi

[27] *Mobile Banking Overview (NA)*, Mobile Marketing Association 2009, s. 10, http:// www.mmaglobal.com/ files/ mbankingoverview.pdf [dostęp: 09.03.2014].

[28] *Analiza poziomu bezpieczeństwa kart zbliżeniowych z punktu widzenia ich posiadaczy*, Urząd Komisji Nadzoru Finansowego, Warszawa 2013, s. 16-20, http://www.knf.gov.pl/Images/14 06 2013_karty%20zblizeniowe_tcm75-34934.pdf [dostęp: 14.03.2014].

ryzyko w tym zakresie są możliwe do zdefiniowania przez klienta ilościowe i kwotowe limity takich transakcji, stosowane w terminalach POS wymuszanie autoryzacji losowo wybranych transakcji zbliżeniowych kodem PIN oraz ustawowe ograniczenie odpowiedzialności posiadacza skradzionej karty za transakcje zrealizowane przed zastrzeżeniem karty do równowartości 150 EUR[29].

Dane wymieniane w technologii NFC są szyfrowane przez specjalny układ kryptograficzny (tzw. *secure element*)[30]. Terminal płatniczy obsługujący połączenia w trybie NFC inicjuje połączenie i odbiera numeryczny identyfikator telefonu, a następnie przesyła na wyświetlacz nazwę punktu handlowego i kwotę transakcji, żądając potwierdzenia. Terminal potrafi rozpoznać kolizję emitowanego sygnału z innymi sygnałami radiowymi, w tym również podsłuchującymi realizowaną transakcję[31]. Zagrożenie dotyczące nieuprawnionego odczytu danych z karty płatniczej dotyczy możliwości wykorzystania tych danych w płatnościach niewymagających fizycznej obecności karty (ang. *card-not-present transaction*), np. dla dokonania zakupów w internecie. Interfejs zbliżeniowy umożliwia jednak odczytanie tylko części danych karty płatniczej wbudowanej w urządzenia przenośne, takich jak numer i data ważności, natomiast dane identyfikacyjne posiadacza karty ani kody autoryzacyjne CVV2/CVC2 nie są w ten sposób udostępniane. W związku z powyższym wykorzystanie przechwyconych danych mogłoby teoretycznie pozwolić wyłącznie na realizację transakcji u sprzedawców, którzy wbrew standardom organizacji płatniczych nie wymagają kompletu danych.

Atak typu przekaźnikowego wiąże się z teoretyczną możliwością realizacji nieuprawnionych transakcji przy wykorzystaniu przez przestępców dwóch pośredniczących urządzeń mobilnych – jednego odczytującego dane karty z urządzenia ofiary ataku i przesyłającego je równocześnie przez sieć internet na drugie wykorzystywane w tym samym czasie do realizacji transakcji zbliżeniowej w terminalu POS. Ryzyko tego typu przestępstwa ogranicza konieczność pobrania danych z urządzenia ofiary dokładnie w momencie, w którym drugie urządzenie pośredniczące zbliżane jest do terminala. Ponadto, czas potrzebny na przesłanie danych pomiędzy urządzeniami pośredniczącymi może przekroczyć maksymalny limit opóźnienia komunikacji pomiędzy kartą a terminalem (ang. *time-out*).

Logiczne klonowanie karty polega na zbliżeniowym pozyskaniu z karty urządzenia przenośnego ofiary ataku danych, wykorzystywanych następnie do trans-

[29] *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych*, Dz. U. 2011, Nr 199, poz. 1175 ze zm., art. 46, ust. 2.

[30] A. BORCUCH, *Bankowość elektroniczna w* Polsce, CeDeWu, Warszawa 2011, s. 95-96.

[31] G. SZUSTAK, *Innowacje rynku kart płatniczych w Polsce – charakter, tempo i zasadność wprowadzanych zmian,* „Annales UMCS", Sec. H, 47 (2013), nr 3, s. 535.

akcji zbliżeniowych przy użyciu urządzenia mobilnego z funkcją NFC. Realizacja nieuprawnionych transakcji mogłaby być możliwa jedynie przy założeniu niewykorzystywania przez kartę ofiary połączonego uwierzytelniania danych dynamicznych i generowania kryptogramu aplikacji i jedynie do momentu dokonania przez ofiarę kolejnej transakcji, prowadzącej do wygenerowania kolejnego dynamicznego kodu CVV3/CVC3.

W zakresie mobilnych płatności zbliżeniowych KNF zaleca[32]:

1) zapoznanie się z regulaminem oraz przestrzeganie warunków umowy o świadczenie usługi NFC;
2) weryfikację i dostosowanie do własnych potrzeb wysokości limitu transakcyjnego dla sumy wielokrotnych płatności zbliżeniowych, jakie można wykonać bez podania kodu PIN;
3) uaktywnienie lub niewyłączanie dostępnych w smartfonie zabezpieczeń, w tym blokad uruchomienia aparatu, inicjalizacji karty SIM-NFC oraz wprowadzenie hasła do aplikacji płatniczej;
4) zainstalowanie w smartfonie oprogramowania zabezpieczającego (skanera antywirusowego, zapory sieciowej) oraz jego regularną aktualizację;
5) niestosowanie łatwych do odgadnięcia numerów PIN, niezapisywanie kodów w sposób jawny (np. w pamięci telefonu) oraz niezwłoczną zmianę kodu w przypadku podejrzenia ujawnienia nieuprawnionym osobom;
6) szyfrowanie wrażliwych danych zamieszczonych w pamięci urządzenia przenośnego;
7) korzystanie z funkcji bieżącego informowania o wykonanej transakcji komunikatem SMS, okresowe kontrolowanie zgodności wyciągu z rachunku bankowego z wykonanymi transakcjami oraz niezwłoczne formalne zgłaszanie bankowi nieuprawnionych transakcji;
8) unikanie instalowania w smartfonie oprogramowania pochodzącego z nieautoryzowanych źródeł oraz weryfikację aplikacji przez oprogramowanie antywirusowe przed ich instalacją;
9) wyłączanie telefonu przed oddaniem do depozytu, szatni itp. oraz wyłączanie funkcjonalności bezprzewodowych (Bluetooth, IRDA, Wi-Fi, WirelessHD), gdy nie są one wykorzystywane;
10) nieoddawanie telefonu do serwisu wraz z kartą SIM-NFC, SD-NFC, jeżeli limit płatności zbliżeniowych nie został wcześniej zablokowany;

[32] *Mobilne płatności zbliżeniowe – o czym warto wiedzieć*, KNF, Warszawa 2012, s. 1-2, 43-47, http://www.knf.gov.pl/Images/mobline_platnosci_tcm75-32797.pdf [dostęp: 09.03.2014].

11) w przypadku utraty lub kradzieży telefonu z funkcją NFC niezwłoczne blokowanie karty SIM-NFC u operatora telekomunikacyjnego oraz w banku;
12) zapisanie w łatwo dostępnym miejscu numerów telefonów centrum rozliczeniowego operatora karty i banku, pod którymi można zgłaszać zastrzeżenie karty płatniczej;
13) dezaktywację usługi NFC (lub karty SIM, która w usłudze NFC stanowi nośnik danych) przed przekazaniem telefonu do użytkowania innej osobie usługą płatności zbliżeniowych.

Stosowane obecnie rozwiązania techniczne w zakresie form komunikacji wykorzystywanych w bankowości mobilnej pozwalają na pozytywną ocenę poziomu oferowanego przez nią bezpieczeństwa. Należy jednak podkreślić, że podobnie jak w przypadku innych kanałów zdalnego dostępu do usług bankowych, kluczowe znaczenie w tej kwestii ma przestrzeganie przez użytkowników elementarnych zasad bezpieczeństwa związanych z wykorzystywaniem komunikacji elektronicznej.

PODSUMOWANIE

Znaczący postęp w dziedzinie technologii teleinformatycznych, jaki nastąpił w ostatnich latach, a zwłaszcza istotna poprawa funkcjonalności i upowszechnienie się smartfonów i tabletów w połączeniu z relatywnym spadkiem kosztów transferu danych w sieciach telefonii komórkowej, sprawił, że bankowość mobilna na nowo znalazła się w centrum uwagi zarówno banków, jak i ich klientów.

Wydaje się, że wiązka innowacji produktowych i procesowych, jaką stanowi obecnie bankowość mobilna, ma potencjał, aby na zawsze zmienić charakter i zakres relacji bank–klient. Dotyczy to zarówno wielorakich możliwości realizacji operacji bankowych, w zasadzie bez ograniczeń czasowych i przestrzennych (bankowość internetowa, aplikacje mobilne, płatności w punktach handlowo-usługowych), jak i wykorzystania przez banki osobistego charakteru urządzeń przenośnych do realizacji nowoczesnych strategii marketingowych, zorientowanych na dostarczanie klientom dalece spersonalizowanych informacji handlowych i ofert produktowych.

Podobnie jak w przypadku innych kanałów zdalnego dostępu do usług bankowych, korzystanie z bankowości mobilnej wiąże się z ryzykiem wynikającym z zagrożeń utraty wrażliwych danych lub uzyskania przez osoby nieuprawnione dostępu do zasobów finansowych klienta. W świetle przedstawionych w artykule argumentów wydaje się jednak, że przy przestrzeganiu przez użytkowników elementarnych zasad bezpieczeństwa, stosowane współcześnie rozwiązania techniczne skutecznie ograniczają to ryzyko.

BIBLIOGRAFIA

Analiza poziomu bezpieczeństwa kart zbliżeniowych z punktu widzenia ich posiadaczy, Urząd Komisji Nadzoru Finansowego, Warszawa 2013, http://www.knf.gov.pl/Images/14_06_2013_ karty% 20zblizeniowe_tcm75-34934.pdf [dostęp: 14.03.2014].

BORCUCH A., Bankowość elektroniczna w Polsce, CeDeWu, Warszawa 2011.

Consumers and Mobile Financial Services 2013, Washington: Board of Governors of the Federal Reserve System 2013, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf [dostęp: 25.03.2014].

ENSOR B., MONTEZ T., WANNEMACHER P., The state of mobile banking 2012, Forrester Research Inc., Cambridge 2012.

Financial empowerment in the digital age. Mobile banking, social media and financial behaviour, ING 2013, https://www.ing-diba.at/uploads/media/ING_International_Survey_-_Financial_Empowerment_in_the_ Digital_Age_- Jul..._01.pdf [dostęp: 24.03.2014].

http://www.peopay.pl/ [dostęp: 14.03.2014].

http://www.pkobp.pl/iko-platnosci-mobilne/ [dostęp: 14.03.2014].

Innowacyjne usługi banku, red. D. Korenik, Wydawnictwo Naukowe PWN, Warszawa 2006.

JADCZAK A., Bankowość mobilna – najnowsze rozwiązania i przykłady techniczne, Evangelist 2011, http://www.rewolucjawfinansach.pl/download/gfx/rewolucjawfinansach/pl/defaultaktualnosci/12/7 /1/08062011_rwf_evangelist_arek_jadczak.pdf [dostęp: 24.03.2014].

Kieszonkowe aplikacje bankowe 2013, Symetria.pl 2013, http://symetria.pl/blog/wp-content/uploads/ 2013/11/Raport_Symetrii_Kieszonkowe_Aplikacje_Bankowe_2013.pdf [dostęp: 14.03. 2014].

KOŹLIŃSKI T., Bankowość internetowa. Część II – rozwój na świecie i w Polsce, „Bank i Kredyt" 36 (2005), nr 6.

Mobile Banking Overview (NA), Mobile Marketing Association 2009, www.mmaglobal.com/files/ mbankingoverview.pdf [dostęp: 09.03.2014].

Mobile Life 2013, TNS Global 2013, http://www.tnsglobal.pl/obszary-dzialania/mobile/ [dostęp: 09.03.2014].

Mobilne płatności zbliżeniowe – o czym warto wiedzieć, KNF, Warszawa 2012, http://www.knf.gov.pl/ Images/ mobline_platnosci_tcm75-32797.pdf [dostęp: 09.03.2014].

POLASIK M., Bankowość elektroniczna. Istota – stan – perspektywy, CeDeWu, Warszawa 2012.

POLASIK M., Wykorzystanie elektronicznych kanałów dystrybucji usług bankowych w Polsce, „Copernican Journal of Finance & Accounting" 2 (2013), 1.

POLASIK M., MACIEJEWSKI K., Innowacyjne usługi płatnicze w Polsce i na świecie, „Materiały i Studia" – Narodowy Bank Polski, Warszawa 2009.

Rola mobilnych finansów w życiu Polaków. Raport przygotowany przez TNS Polska jestem.mobi na zlecenie Getin Banku, Getin Bank 2013, https:// getinup.pl/ raport/ pdf/ rola_mobilnych_finansow_w _zyciu_polakow _raport_z_badania.pdf [dostęp: 09.03.2014].

SKRZYŃSKI P., Mobilna bankowość – potrzeba czy moda?, Mobiltek 2011, http://www.mobiltek.pl/wp-content/uploads/2011/10/mobilna-bankowosc-potrzeba-czy-moda.pdf [dostęp: 24.03.2013].

SZUSTAK G., Innowacje rynku kart płatniczych w Polsce – charakter, tempo i zasadność wprowadzanych zmian, „Annales UMCS", Sec. H, 48 (2013), nr 3.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz. U. 2011, Nr 199, poz. 1175 ze zm.

World retail banking report 2013, Capgemini, Efma 2013, http://www.capgemini.com/resource-file-access/resource/pdf/wrbr_2013.pdf [dostęp: 24.03.2014].

ZŁOCH M., Smartfon: klucz do bankowości, „Miesięcznik Finansowy BANK" 240 (2013), nr 1.

BANKOWOŚĆ MOBILNA JAKO INNOWACYJNY KANAŁ DOSTĘPU DO USŁUG BANKOWYCH

Streszczenie

Celem artykułu jest przedstawienie ewolucji innowacyjnych rozwiązań w bankowości mobilnej, ze szczególnym uwzględnieniem kwestii bezpieczeństwa tego kanału dostępu do usług bankowych. Rozważania oparto na krajowych i zagranicznych raportach poświęconych problematyce rynku bankowości mobilnej. Przeprowadzone analizy wskazują, że wiązka innowacji produktowych i procesowych stanowiąca współczesną bankowość mobilną ma potencjał, aby na zawsze zmienić relacje pomiędzy bankami a klientami. Zmiany te dotyczą zarówno likwidacji czasowych i przestrzennych ograniczeń operacji bankowych, jak i wykorzystania przez banki osobistego charakteru urządzeń przenośnych do realizacji strategii marketingowych. Dzięki tym rozwiązaniom bankowość mobilna ma możliwość istotnego zmniejszenia dystansu dzielącego ją od innych kanałów dostępu do usług bankowych. Ryzyko wynikające z licznych zagrożeń, na jakie narażeni są użytkownicy bankowości mobilnej, może być natomiast skutecznie ograniczane dzięki stosowanym współcześnie rozwiązaniom technicznym oraz przestrzeganiu elementarnych zasad bezpieczeństwa.

Słowa kluczowe: bankowość mobilna, innowacje, technologie teleinformatyczne

MOBILE BANKING AS AN INNOVATIVE CHANNEL OF ACCESS TO BANKING SERVICES

Summary

The aim of the paper is to present the evolution of innovations in mobile banking with a particular regard to the issue of security of this channel of access to banking services. The discussion was based on domestic and foreign reports on mobile banking market. The conducted analyses indicate that cluster of innovations forming the modern mobile banking has a potential to change the relations between banks and their clients forever. These changes regard not only elimination of time and space barriers of banking operations, but also the use of personal character of mobile devices for realisation of banks' marketing strategies. Though these solutions mobile banking has an ability to decrease significantly its distance from the other channels of access to banking services. The risk resulting from numerous threats to the users of mobile banking can be effectively mitigated by modern technical solutions and obeying the elementary security rules.

Key words: mobile banking, innovations, ICT.

Translated by Piotr Bolibok, Anna Matras-Bolibok