Miscellanea

*Mateusz Staszczyk**

OCHRONA KONSUMENTÓW KORZYSTAJĄCYCH Z USŁUG BANKOWOŚCI ELEKTRONICZNEJ – NA PRZYKŁADZIE ANKIETY PRZEPROWADZONEJ WŚRÓD OSÓB PRACUJĄCYCH I/LUB STUDIUJĄCYCH W ŁODZI

WSTĘP

W Polsce rośnie zainteresowanie konsumentów usługami bankowymi. Jak jednak wynika z analizy Urzędu Ochrony Konkurencji i Konsumentów, wciąż są obszary, w których dochodzi do łamania praw słabszych uczestników rynku. Z roku na rok coraz chętniej zakładane są rachunki oszczędnościowo-rozliczeniowe. Wzrasta także tempo rozwoju bankowości elektronicznej – ponad 10 mln klientów korzysta z dostępu do rachunku bankowego przez Internet. Konsumenci spotykają się na rynku usług finansowych z licznymi problemami. Wynikają one głównie ze stosowanych przez przedsiębiorców postanowień umownych, które kształtują prawa i obowiązki słabszych uczestników rynku w sposób sprzeczny z dobrymi obyczajami, rażąco naruszając ich interesy.

* Mateusz Staszczyk jest doktorantem w Instytucie Finansów na Wydziale Ekonomiczno-Socjologicznym Uniwersytetu Łódzkiego.

O bezpieczeństwie bankowości elektronicznej nierzadko mówi się w ujęciu ogólnym, sprowadzającym zagadnienie do najpopularniejszych problemów z nim związanych, takich jak podpisy cyfrowe czy hasła dostępu. Tymczasem sprawa bezpieczeństwa bankowości elektronicznej to niezwykle złożone zagadnienie. Obejmujące nie tylko terminy z płaszczyzny technologicznej, ale również ekonomicznej i prawnej. O bezpieczeństwie bankowości elektronicznej w największym stopniu decyduje zachowanie się, a w zasadzie ogół zachowań, jej użytkowników. Praktyczna skuteczność stosowanych obecnie mechanizmów bezpieczeństwa zależy przede wszystkim od sposobu korzystania z nich przez użytkowników e-bankowości.

Rozwój kart płatniczych oraz zwiększona dostępność tych usług m.in. dzięki rozwojowi elektronicznych kanałów dystrybucji usług bankowych może przyczynić się do zwiększenia zagrożenia bankructwem klientów indywidualnych. Źródłem tego jest lekkomyślność konsumentów, którzy ulegają reklamie, nabywając drogie dobra, czasem świadomie lekceważąc kwestie planowania swoich budżetów domowych. W momencie gdy dochody nie są wystarczające, gospodarstwa domowe zaciągają kolejne kredyty, aby spłacić wcześniejsze, i w rezultacie popadają w spiralę zadłużenia.

Możliwość pobierania opłat za czynności bankowe nie oznacza przyzwolenia na ustanowienie każdej opłaty w dowolnej wysokości – granice swobody umów w zakresie obrotu z konsumentami stanowią bowiem przepisy regulujące instytucję niedozwolonych postanowień umownych.

Z pobieraniem przez banki opłat za świadczone usługi związanych jest wiele kontrowersji. Analiza tabeli opłat i prowizji może prowadzić do wniosku, że praktycznie każda czynność podlega określonej opłacie. Zastrzeżenia powoduje nie tylko ich liczba czy też wysokość, ale także możliwość ich kumulacji w związku z jednym zdarzeniem.

Tematem niniejszego opracowania jest problematyka ochrony najsłabszych uczestników e-bankowości, tj. konsumentów. W tym obszarze dochodzi często do konfliktu interesów między uczestnikami, tj. użytkownikami, wydawcami i akceptantami instrumentów elektronicznych. Artykuł powstał w wyniku analizy ankiety przeprowadzonej w 2013 r. Ma na celu ukazanie na podstawie badania ankietowego poziomu ochrony oraz świadomości konsumenta bankowości elektronicznej. Weryfikuje również hipotezę, że typ grupy społecznej ma wpływ na bezpieczeństwo e-bankowości.

1. OPIS PROCESU BADAWCZEGO

Proces badawczy składał się z dwóch głównych części – skompletowania i porównania ze sobą materiałów wtórnych oraz zebrania i analizy materiałów pierwotnych. Analiza materiałów wtórnych miała przede wszystkim pomóc w ustale-

niu aktualnego stanu i zakresu ochrony konsumenta bankowości elektronicznej. Posłużyła również do opracowania kwestionariusza ankiety wykorzystywanego do zbierania materiałów źródłowych. Materiały te dostarczyły informacji, na podstawie których można było określić stopień bezpieczeństwa elektronicznych kanałów dystrybucji banków. Pozwoliły także wykazać ewentualne braki w ochronie konsumentów.

W części pierwszej, polegającej na skompletowaniu i analizie literatury, wykorzystano dostępne materiały bankowe i przeprowadzone przez innych autorów badania społeczne.

Ankieta właściwa została zredagowana na podstawie informacji uzyskanych po przeprowadzeniu analizy literatury przedmiotu i badań społecznych. Składała się z pięciu części. Pierwsza część dotyczyła ogólnych spraw związanych z bezpieczeństwem konsumenta bankowości elektronicznej (8 pytań). Druga część pozwoliła na zbadanie opinii konsumentów na temat ochrony prawnej (4 pytania dotyczące instytucji konsumenckich). W trzeciej części pytania dotyczyły problemów technicznych (5 pytań). W części czwartej pytano o aspekty ekonomiczne – m.in. nadmierne zadłużenie i ubezpieczenie kart kredytowych (7 pytań). Ankietę zamykała tak zwana metryczka, która zawierała pytania o bank konsumenta, płeć, wiek, wykształcenie, miejsce zamieszkania, zatrudnienie, wielkość gospodarstwa domowego i ocenę sytuacji materialnej (11 pytań).

Do analizy zebranych danych wykorzystano nominalną skalę pomiaru Likerta, czyli pięciostopniową skalę porządkową; jest ona często wykorzystywana do badania postaw wobec różnych opinii. Szczególna przydatność tego formatu zasadza się na jednoznacznym uporządkowaniu kategorii odpowiedzi[1].

Do zbierania danych zastosowano celowy dobór próby według następujących kryteriów:

- ❖ osoby pracujące i/lub studiujące w Łodzi,
- ❖ zgoda na wzięcie udziału w wywiadzie.

W ankiecie głównej uczestniczyło 1000 osób. Reprezentowały one sześć grup:

- ❖ studenci Wydziału Ekonomiczno-Socjologicznego Uniwersytetu Łódzkiego – 48,3%,
- ❖ słuchacze Łódzkiego Uniwersytetu Trzeciego Wieku – 17,8%,
- ❖ pracownicy Urzędu Skarbowego Łódź-Widzew – 13,2%,
- ❖ pracownicy MPK-Łódź sp. z o.o. – 9,7%,
- ❖ pracownicy Urzędu Skarbowego Łódź-Śródmieście – 7,5%,
- ❖ pracownicy Sądu Rejonowego dla Łodzi-Widzewa w Łodzi – 3,5%.

[1] E. Babbie, *Podstawy badań społecznych*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 197.

2. ANALIZA PYTAŃ OGÓLNYCH

Pierwsze pytanie ankiety było filtrujące i dotyczyło korzystania z usług bankowości elektronicznej. 88% respondentów korzystało z tego typu bankowości. Osoby te odpowiadały na kolejne pytania ankiety, natomiast osoby niekorzystające z tych usług przechodziły bezpośrednio do metryczki. Wśród nich 81,2% stanowiły kobiety, 45,4% osoby w wieku 55 lat i więcej, 54,2% osoby ze średnim wykształceniem, 79% osoby z miast powyżej 100 tysięcy mieszkańców, 59,5% osoby nie pracujące, 44,4% osoby z gospodarstw jednoosobowych i 59,7% osoby o przeciętnej sytuacji gospodarczej.

Wśród osób korzystających z usług bankowości elektronicznej 72,5% stanowiły kobiety, 48,4% osoby w wieku 15–24 lat, 53,1% osoby ze średnim wykształceniem, 61,5% osoby z miast powyżej 100 tysięcy mieszkańców, 48,7% osoby nie pracujące, 39,2% osoby z gospodarstw jednoosobowych i 57,6% osoby o przeciętnej sytuacji gospodarczej.

Najwięcej konsumentów korzystało z usług: PKO BP (29,3%), mBanku (18,5%) i Banku Pekao SA (15,8%).

3. OCHRONA PRAWNA KONSUMENTA BANKOWOŚCI ELEKTRONICZNEJ

Ryzyko prawne e-bankingu powiązane jest ściśle z pozostałymi pokrewnymi ryzykami, występuje przede wszystkim wówczas, gdy przepisy pierwotnie skonstruowane w odniesieniu do bankowości tradycyjnej nie przystają do świata wirtualnego. W takich sytuacjach bank musi brać pod uwagę regulacje mogące narazić bank lub jego klientów na niedogodności czy nawet straty finansowe. Istnieją sytuacje, gdy co prawda nie ma bezpośredniego zagrożenia kondycji banku, ale funkcjonuje on w swego rodzaju próżni prawnej[2].

Klienci banku na skutek niepełnych lub mylących instrukcji i informacji zamieszczonych na stronach internetowych banków oraz w regulaminach mogą błędnie pojmować swoje obowiązki lub nie są świadomi środków ostrożności, które należy zachować przy korzystaniu z elektronicznego kanału dostępu. To niebezpieczeństwo potęguje się, kiedy bank zaczyna świadczyć usługi transgraniczne. Klienci mogą w sytuacjach gdy ponieśli straty wnosić oskarżenia przeciw bankowi[3].

Wśród 8 instytucji czuwających nad bezpieczeństwem konsumenta wymienionych respondentom najczęściej wskazywane w ankiecie były: Rzecznik Praw Obywatelskich (23,3%), Komisja Nadzoru Finansowego (22,4%) oraz Urząd Ochrony Konkurencji i Konsumentów (20,9%).

---

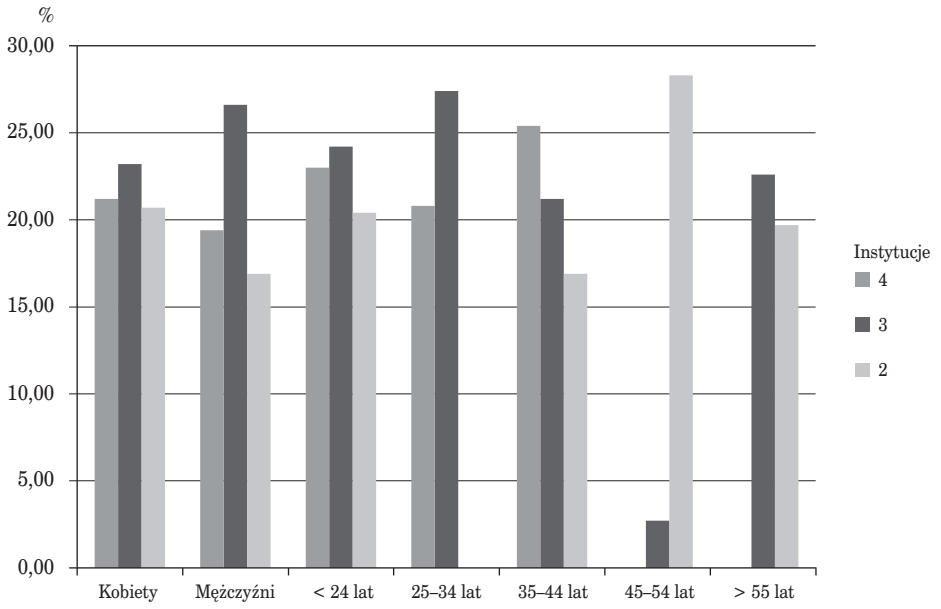
2 J. Górka, *Specyfika ryzyka bankowości elektronicznej*, „Materiały i Studia", Zeszyt nr 205, NBP, Warszawa 2006, s. 35.

3 *Ibidem*.

Kobiet znających 3 instytucje było 23,2%, 4 – 21,2%, 2 – 20,7% (por. rysunek 1). Mężczyzn wskazujących 3 instytucje było 26,6%, 4 – 19,4%, 2 – 16,9%. W przedziale wiekowym do 24 lat 3 instytucje znało 24,2%, 4 – 23%, 2 – 20,4%; w wieku 25–34 lata 3 instytucje wymieniło 27,4%, 4 – 20,8% i 1 – 15%; w wieku 35–44 lata 4 instytucje znało 25,4%, 3 – 21,2%, 2 – 16,9%; w wieku 45–54 lata 2 instytucje wskazało 28,3%, 3 – 2,7%, 1 – 18,3%; powyżej 55 lat 1 instytucję wymieniło 27%, 3 – 22,6% i 2 – 19,7%. Wśród badanych osób ze średnim wykształceniem 3 instytucje znało 25%, 2 – 23,5%, 4 – 20,1%; osób z wyższym wykształceniem 3 instytucje wskazało 23,5%, 4 – 21,7%, 2 – 16,4%).

W podziale na sytuację materialną, wśród osób oceniających ją jako złą 3 instytucje znało 44%; jako raczej złą – 3 instytucje wymieniło 30%; jako przeciętną – 3 instytucje – 23,6%; jako dobrą – 3 instytucje –23,2%; jako bardzo dobrą 4 instytucje znało 33,3% badanych.

Rysunek 1. Znajomość instytucji konsumenckich przez ankietowanych



Źródło: opracowanie własne na podstawie przeprowadzonej ankiety.

Aż 84,4% ankietowanych nie zwracało się nigdy do instytucji konsumenckiej, bo nie mieli takiej potrzeby. Wśród kobiet było to 86,3%, a wśród mężczyzn 80,5%. Wśród osób do 24 lat było to 85,1%, w przedziale wiekowym 25–34 lata – 88,8%, 35–44 lata – 84,6%, 45–54 lata – 86,4% i wśród osób powyżej 55 roku życia – 78,5%. 85,2% osób z wykształceniem średnim nie zwracało się nigdy do instytucji konsu-

menckiej gdyż nie mieli takiej potrzeby, a osób z wykształceniem wyższym było 84,2%. 66,7% osób oceniających swoją sytuację materialną jako złą nie zwracało się do instytucji konsumenckiej, oceniających jako raczej złą było 75,5%, jako przeciętną – 84%, jako dobrą – 86,9% i jako bardzo dobrą – 88%.

Wyłączenie odpowiedzialności banku było głównym naruszeniem przez banki wzorców umów o karty płatnicze – 33,2% odpowiedzi. Na drugim miejscu znalazły się klauzule niedozwolone dotyczące reklamacji (26,5%), a na trzecim brak obowiązkowych elementów umowy (17,4%).

W badaniu „Konsumenci na rynku usług bankowych" wskazywano najczęściej: UOKIK (60,3% odpowiedzi), KNF (26,7%) i Powiatowego/Miejskiego Rzecznika Konsumentów (21,3%). 96,6% ankietowanych nigdy nie zwracało się do instytucji zajmującej się ochroną praw konsumenta[4].

4. OCHRONA TECHNICZNA KONSUMENTA BANKOWOŚCI ELEKTRONICZNEJ

Wśród najczęściej spotykanych działań przestępczych w e-bankingu można wymienić[5]:

- posługiwanie się skradzionymi lub zagubionymi kartami płatniczymi,
- kopiowanie kart płatniczych przez nieuczciwych sprzedawców, za pomocą nielegalnego skanera,
- podrabianie i fałszowanie kart płatniczych przez organizacje przestępcze,
- wyłudzanie od posiadaczy kart płatności za towary rzekomo wysłane,
- włamywanie się do systemów telekomunikacyjnych w celu przechwycenia danych o numerach kart, przyporządkowanym im hasłach PIN,
- napady na bankomaty lub na osoby z nich korzystające.

Niewiele ponad połowa ankietowanych (56,1%) przed dokonaniem transakcji zawsze zwracała uwagę na wygląd bankomatu, 29,5% robiło to, ale bardzo rzadko, a 14,4% nigdy nie zwracało na to uwagi. 55,8% kobiet zwracało zawsze uwagę na bankomat, a mężczyzn 56,4% (por. rysunek 2). W przedziale wiekowym do 24 lat było to 47,7%, w przedziale 25–34 lat – 56,6%, w przedziale 35–44 lat – 65%, w przedziale 45–54 lat – 62,7% i przedziale ponad 55 lat – 67,3%. Osób z wykształceniem średnim sprawdzających bankomat było 52,4%, z wykształceniem wyższym było 58,8%. Osób oceniających swą sytuację materialną jako raczej złą, bankomat

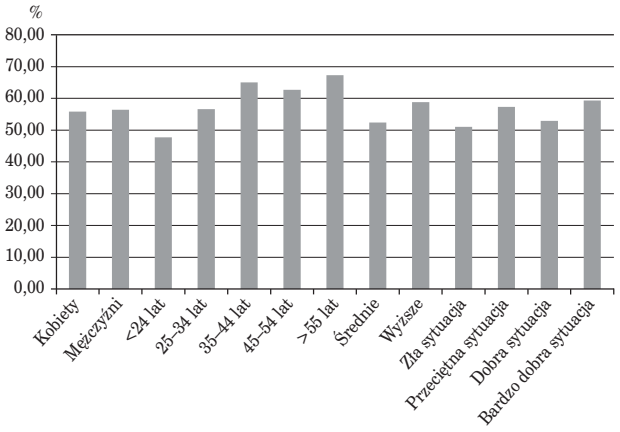
[4] UOKIK, Konsumenci na rynku usług bankowych – raport z badań, Warszawa lipiec 2009, https://uokik.gov.pl/download.php?plik=9332, s. 41–43 (dostęp: 5.03.2016).

[5] J. Sosnowski, *Zagrożenia i systemy zabezpieczeń pieniądza elektronicznego*, [w:] *Wyzwania w systemie bankowym w XXI wieku*, red. A. Piotrowska-Piątek, Kieleckie Towarzystwo Edukacji Ekonomicznej, Kielce 2009, s. 336.

sprawdzało 51%, oceniających sytuację jako przeciętną – 57,3%, jako dobrą – 52,9% i jako bardzo dobrą – 59,3%.

Certyfikat bezpieczeństwa konta internetowego sprawdzało: przy każdym logowaniu – 14,7%, czasami – 21,6%, natomiast bardzo rzadko, nigdy lub tylko przy pierwszym logowaniu aż 63,5%. Kobiet sprawdzających przy każdym logowaniu było 12%, mężczyzn – 20,6% (zob. rysunek 3).

Rysunek 2. Zwracanie uwagi na wygląd bankomatu przez ankietowanych



Źródło: opracowanie własne na podstawie przeprowadzonej ankiety.

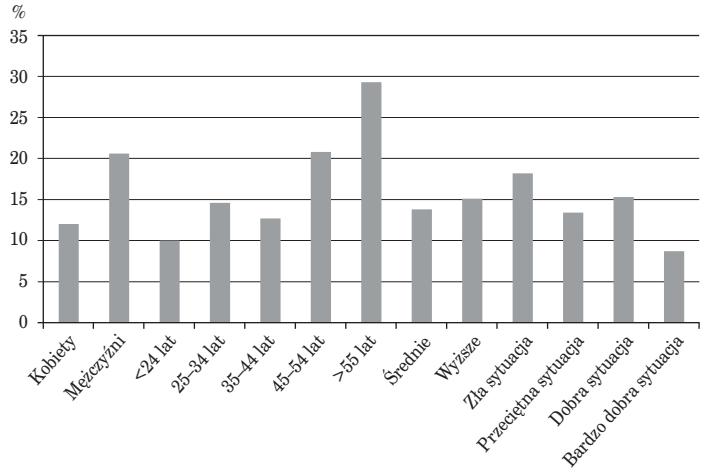
Jeśli chodzi o wiek, to certyfikat bezpieczeństwa sprawdzały osoby w wieku: do 24 lat – 10%, 25–34 lat – 14,6%, 35–44 lat – 12,7%, 45–54 lat – 20,8% i ponad 55 lat – 29,3%. Osoby z wykształceniem średnim w 13,8%, z wyższym w 15,1%. Osoby o raczej złej sytuacji materialnej w 18,2%, przeciętnej w 13,4%, dobrej w 15,3% i bardzo dobrej w 8,7% sprawdzały certyfikat.

Na pytanie, jaka forma kontroli dostępu do bankomatu byłaby satysfakcjonująca, 37,5% ankietowanych wskazało kartę bankomatową i PIN, 33,3% odcisk palca, a 16,5% kartę inteligentną ze wzorcem biometrycznym.

W raporcie przygotowanym przez TNS Polska i jestem.mobi na zlecenie Getin Banku respondenci zostali zapytani, jakich czynności nigdy nie zrealizują za pomocą telefonu. Najczęściej wskazywano: złożenie wniosku o kredyt (47%), przelewy przez Facebook zamiast na nr konta bankowego (46%) oraz założenie lokaty (38%). Najrzadziej natomiast: sprawdzanie salda konta (4%), wyszukanie najbliższego oddziału/placówki (4%) i sprawdzanie historii ostatnich transakcji (3%)[6].

[6] *Rola mobilnych finansów w życiu Polaków, Raport przygotowany przez TNS Polska i jestem.mobi na zlecenie Getin Banku*, http://jestem.mobi/2013/10/raport-rola-mobilnych-finansow-w-zyciu-polakow/, 15.10.2013, s. 14 (dostęp: 5.03.2016).

Rysunek 3. Sprawdzanie certyfikatu bezpieczeństwa konta internetowego przez ankietowanych



Źródło: opracowanie własne na podstawie przeprowadzonej ankiety.

Kobiety wykazują się większym poziomem nieufności wobec rozwiązań mobilnych. Szczególnie obawiają się braku pomocy (odpowiedź „Nikt mi nie pomoże, jeśli coś pójdzie nie tak", wskazywało tak 16% kobiet i tylko 3% mężczyzn). Najczęściej jednak boją się utraty telefonu, w konsekwencji czego ich finanse mogą być zagrożone (tak odpowiedziało 34% kobiet i 29% mężczyzn)[7].

Badanie „Kradzież tożsamości – Raport z badań" zaczęło się 22 października 2013 r. i trwało do 4 października 2014 r. W ciągu roku ankietę wypełniło 1107 badanych. Raport został wykonany przez Fellowes przy współpracy z BIK. Uczestnicy programu stosunkowo dobrze zabezpieczają kody PIN do posiadanych kart płatniczych, choć jedynie 2% wykorzystuje specjalne programy do przetrzymywania haseł. Większość badanych (72%) niszczy je zaraz po zapamiętaniu. Aż 19% trzyma je w domu, w miejscu uważanym za bezpieczne. Jednak aż 7% respondentów naraża się na duże zagrożenie zapisując swoje kody PIN na kartkach noszonych w portfelu razem z kartami płatniczymi albo w telefonie. Takie zachowania narażają te osoby na kradzież tożsamości i utratę środków pieniężnych znajdujących się na koncie[8].

[7] *Ibidem*, s. 32.
[8] A. Wilk, *Kradzież tożsamości. Raport z badań*, http://www.giodo.gov.pl/plik/id_p/6594/j/pl/, s. 7 (dostęp: 5.03.2016).

Tabela 1. Bezpieczeństwo korzystania z mobilnej przeglądarki dla bankowości mobilnej

Ocena	2011 r.	2012 r.
Bardzo bezpieczne	5,6	9,8
Nieco bezpieczne	36	27,8
Nieco niebezpieczne	18,8	15,1
Bardzo niebezpieczne	7,6	9,6
Nie wiem	30,2	36,4
Odmówiło odpowiedzi	2	1,4
Liczba respondentów	2002	2291

Źródło: *Board of Governors of the Federal Reserve System, Consumers and Mobile Financial Services 2013*, march 2013, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf, s. 16 (dostęp: 5.03.2016).

Ankietowani w badaniu przeprowadzonym przez Rezerwę Federalną ocenili jako bezpieczne korzystanie z mobilnej przeglądarki i aplikacji banku w telefonie komórkowym. Suma odpowiedzi „bardzo bezpieczne" i „nieco bezpieczne" była jednak w 2012 r. niższa w porównaniu do 2011 r. (por. tabele 1 i 2).

Tabela 2. Bezpieczeństwo korzystania z aplikacji banku w bankowości mobilnej

Ocena	2011 r.	2012 r.
Bardzo bezpieczne	7,4	9,4
Nieco bezpieczne	32,9	25,3
Nieco niebezpieczne	15,1	13,2
Bardzo niebezpieczne	6,8	9,4
Nie wiem	36,1	41
Odmówiło odpowiedzi	1,8	1,8
Liczba respondentów	2002	2291

Źródło: *Board of Governors of the Federal Reserve System…*, *op. cit*.

Praktyki stosowane powszechnie w celu ustalenia i stosowania podziału obowiązków dotyczących bankowości elektronicznej obejmują[9]:

[9] K. Bobyk, *Bezpieczeństwo systemów informatycznych w bankowości*, „Studia i Prace Kolegium Zarządzania i Finansów", Zeszyt naukowy 80, Szkoła Główna Handlowa w Warszawie, Warszawa 2007, s. 32–33.

- ❖ procesy i systemy transakcyjne powinny być tak zaprojektowane, aby uniemożliwiały każdemu pracownikowi lub wynajętemu usługodawcy zainicjowanie, autoryzację i realizację transakcji,
- ❖ należy zachować podział na osoby inicjujące dane statyczne (w tym treść strony internetowej) oraz osoby odpowiedzialne za weryfikację rzetelności tych danych,
- ❖ należy testować systemy bankowości elektronicznej w celu upewnienia się, że nie można obejść podziału obowiązków,
- ❖ należy zachować podział na osoby opracowujące oraz osoby administrujące systemami bankowości elektronicznej.

Dla rozwoju bankowości elektronicznej ważne są wady i zalety metod kontroli dostępu również z punktu widzenia klienta (zob. tabela 3).

Tabela 3. Porównanie metod kontroli dostępu z punktu widzenia klienta

Metoda uwierzytelniania	Bezpieczeństwo	Wady	Zalety
Własnoręczny podpis (transakcje kartami)	Praktycznie nie zabezpiecza wcale	Łatwość podrobienia	Nie wymaga żadnego wysiłku od klienta, podpis składa się mechanicznie
PIN	Bezpieczniejszy niż podpis odręczny, ale przestępcy instalują specjalistyczne urządzenia (zarówno na bankomatach, jak i w ich wnętrzu), służące do pozyskiwania kodów PIN	Konieczność zapamiętania niekiedy dużej liczby różnych PIN-ów (do kilku kart, do logowania)	Często istnieje możliwość ustalania PIN przez klienta
Hasło (statyczne, maskowane)	Metoda nieodporna na phishing i większość ataków, stanowi jedynie utrudnienie (hasła z reguły są bardzo proste, by nie stwarzały problemów w zapamiętaniu)	Konieczność zapamiętania hasła; dodatkowo często wymuszane przez systemy okresowe zmiany haseł	Hasło ustala klient
Karta zdrapka	Narażone na phishing i nieodporne na ataki typu *man-in-the-middle* i *man-in-the-browser*	Konieczność posiadania karty podczas wykonywania transakcji, konieczność zabezpieczenia karty przed zgubieniem czy kradzieżą	Nie trzeba nic zapamiętywać, wystarczy posiadać kartę

Metoda uwierzytelniania	Bezpieczeństwo	Wady	Zalety
SMS z hasłem jednorazowym	Zabezpiecza przed popularnymi atakami phishingowymi, nie zabezpiecza jednak przed atakami *man-in-the-middle* i *man-in-the-browser*	Metoda zależna jest nie tylko od samego banku, ale również od operatora GSM	Nie trzeba nic zapamiętywać, telefon każdy nosi przy sobie
SMS z opisem transakcji	Do niedawna najbezpieczniejsza metoda na rynku. Odporna na phishing, ataki *man-in-the-middle* i *man in-the-browser* – o ile użytkownik czyta skrupulatnie dane transakcji	jw.	jw.
Token generujący hasła na bazie czasu	Zabezpiecza przed popularnymi atakami mającymi na celu wyłudzenie haseł do logowania/potwierdzania transakcji, ale nie zabezpiecza przed *man-in-the-middle* i *man-in-the-browser*	Konieczność noszenia tokenu i posiadania go w momencie przeprowadzania transakcji	Klient nie musi niczego zapamiętywać, kody do akceptowania transakcji przepisuje się z ekranu
Token generujący hasła na bazie licznika	Jest mniej bezpieczny niż urządzenie generujące hasła ograniczone czasowo. Klient korzystający z tej metody narażony jest na wszystkie popularne ataki włącznie z phishingiem	jw.	jw.
Token generujący hasła w trybie Challenge Response	Poziom bezpieczeństwa większy niż w przypadku tokenów generujących hasła jednorazowe. Nie można przeprowadzić ataku phishingowego polegającego na wcześniejszym zdobyciu hasła. Metoda nie chroni jednak przed atakami typu *man-in-the-middle* i *man-in-the-browser*	jw.	jw.

Metoda uwierzytelniania	Bezpieczeństwo	Wady	Zalety
Podpis elektroniczny	Zabezpieczają one tylko przed phishingiem i atakami *man-in-the-middle*. Są całkowicie bezbronne wobec zagrożeń typu *man-in the-browser*	Należy posiadać nośnik kluczy do podpisu	Duża funkcjonalność podpisu elektronicznego – można go wykorzystywać do innych celów – Podpisywanie dokumentów, umów itp.
Metody biometryczne	Jest to jedyna metoda, która udowadnia tożsamość osoby przeprowadzającej transakcję	Osoby mogą poczuć się dyskryminowane jeśli nie przejdą weryfikacji; obawy o bezpieczeństwo przechowywania wzorców biometrycznych	Wystarczy być, nie trzeba niczego zapamiętywać i niczego nosić

Źródło: S. Wojciechowska-Filipek, *Metody kontroli dostępu w bankowości elektronicznej*, Konferencja Innowacje w Zarządzaniu i Inżynierii Produkcji, Zakopane 2011, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/115.pdf, s. 566–567 (dostęp: 5.03.2016).

Doświadczenia wskazują, że regulacje dotyczące zachowania użytkowników systemów bezpieczeństwa muszą być skorelowane z możliwościami dostosowania się do tych zaleceń. Fundamentalną zasadą budowy skutecznego systemu bezpieczeństwa jest wykorzystanie analogii z innych dziedzin życia: nie można zakładać, że użytkownik takiego systemu będzie przestrzegał założonych reguł, o ile reguły te nie będą jasne, zrozumiałe i oparte na analogiach z życia codziennego. Drugą fundamentalną zasadą jest takie konstruowanie systemu bezpieczeństwa, aby brał on pod uwagę możliwość dokonywania błędów przez użytkownika[10].

5. OCHRONA EKONOMICZNA KONSUMENTA BANKOWOŚCI ELEKTRONICZNEJ

Ochrona posiadacza karty płatniczej, oprócz przepisów ustawy o usługach płatniczych, realizowana jest również w przepisach ustawy o nadmiernym oprocentowaniu. Zgodnie z nimi odsetki pobierane w stosunku do kart płatniczych nie mogą przewyższać wysokości odsetek maksymalnych określonych przez ustawę[11].

[10] M. Kutyłowski, *Koncepcje uregulowań prawnych dotyczących bezpieczeństwa technicznego banków elektronicznych a polski stan prawny*, e-Biuletyn 3/2004, http://www.bibliotekacyfrowa.pl/Content/24750/Koncepcje_uregulowan_prawnych.pdf, s. 3 (dostęp: 5.03.2016).

[11] R. Kaszubski, *Ochrona posiadacza karty płatniczej*, e-Biuletyn 2/2008, http://www.bibliotekacyfrowa.pl/Content/23654/Ochrona_posiadacza.pdf, s. 4 (dostęp: 5.03.2016).

Potrącenie kwoty zadłużenia z tytułu karty kredytowej z innych rachunków bankowych powoduje uzasadnione wątpliwości. Co więcej, konsument nie zawsze jest wprost informowany o takiej możliwości, a tymczasem w świetle prawa jego wyraźna zgoda jest niezbędna[12].

Oprocentowanie jest podstawowym składnikiem ceny kredytu kartowego, bezpośrednio związanym z jego udzieleniem. Cena kredytu kartowego (jako kategoria marketingowa) obejmuje jednak także inne elementy, bezpośrednio bądź pośrednio związane z udzieleniem i obsługą kredytu kartowego. Chodzi tu w szczególności o[13]:

- opłaty za wydanie i (lub) używanie karty (opłaty te zazwyczaj są pobierane od posiadaczy kart jednorazowo w cyklu rocznym i często określane jako opłaty roczne), oraz
- składki z tytułu obowiązkowych i (lub) fakultatywnych ubezpieczeń dodawanych do kart kredytowych.

Badania dowiodły, że w Polsce istnieje wysoka dysproporcja w kosztach pomiędzy gotówką a kartą płatniczą, na niekorzyść tej drugiej. Koszt związany z opłatami gotówkowymi z punktu widzenia akceptanta waha się od niecałych 3 do 6 groszy na transakcję w średniej kwocie 28 zł (0,1–0,21% wartości obrotu gotówką), natomiast koszt związany z opłatami związanymi z kartą płatniczą – od 1,79 do 2,64 zł na transakcję w średniej kwocie 83 zł (2,15–3,16% wartości obrotu kartą)[14].

Dla 31% ankietowanych oszczędność pieniędzy z racji niższych opłat w bankowości elektronicznej nie rekompensuje poziomu ryzyka tego kanału. 29,8% miało odmienne zdanie. 4,8% dla poprawy bezpieczeństwa płaciłoby więcej za obsługę konta, a 2,3% za operacje finansowe. Według 31,6% respondentów bankowość elektroniczna w porównaniu z bankowością tradycyjną sprzyja nadmiernemu zadłużeniu, a według 37,9% badanych nie sprzyja.

Koncepcja „odpowiedzialnego kredytowania" powinna zmierzać do wyjaśnienia dwóch kwestii[15]:

- Jak zwiększyć przejrzystość działalności kredytowej, aby w porę zapobiegać nadmiernemu zadłużeniu oraz poprawnie oceniać zdolność kredytową,
- Jakie powinny być miary zadłużenia, które pozwolą również na orientację konsumenta, który będzie mógł realistycznie oceniać dopuszczalne pole manewru w zaciąganiu długów.

---

12 UOKiK, Raport w sprawie przestrzegania praw konsumentów w umowach o korzystanie z kart płatniczych, Warszawa lipiec 2005, https://uokik.gov.pl/download.php?id=580, s. 26 (dostęp: 5.03.2016).

13 A. Kowalczyk, *Wybrane aspekty kształtowania oprocentowania kredytów związanych z funkcjonowaniem kart kredytowych na rynku bankowym w Polsce*, „Bank i Kredyt", 2006, nr 4, s. 43–44.

14 J. Górka, *Aspekty ekonomiczne obrotu bezgotówkowego*, [w:] *Obrót bezgotówkowy*, red. H. Żukowska, M. Żukowski, Wydawnictwo KUL, Lublin 2013, s. 147–148.

15 W. Szpringer, *Społeczna odpowiedzialność banków. Między ochroną konsumenta a osłoną socjalną*, Wolter Kluwer, Warszawa 2009, s. 80.

PODSUMOWANIE

Istotnym wnioskiem płynącym z przeprowadzonego badania jest to, że typ grupy społecznej ma wpływ na bezpieczeństwo e-bankowości. Mężczyźni częściej od kobiet sprawdzają certyfikat bezpieczeństwa konta internetowego. Osoby starsze zwracają większą uwagę na wygląd bankomatu i certyfikat konta internetowego. Wyższy poziom wykształcenia konsumenta zwiększa bezpieczeństwo bankowości elektronicznej. Należy jednak zaznaczyć, że przynależność do określonej grupy społecznej nie jest jedynym czynnikiem wpływającym na bezpieczeństwo e-bankowości. Poziom ochrony konsumentów jest również uzależniony od elementów, na które nie mają wpływu.

Spośród 8 instytucji czuwających nad bezpieczeństwem konsumenta wymienionych respondentom, ankietowani najczęściej wskazywali: Rzecznika Praw Obywatelskich (23,3%), Komisję Nadzoru Finansowego (22,4%) oraz Urząd Ochrony Konkurencji i Konsumentów (20,9%).

Aż 84,4% ankietowanych nie zwracało się nigdy do instytucji konsumenckiej, bo nie mieli takiej potrzeby. Częściej zwracali się z prośbą mężczyźni, badani w wieku powyżej 55 roku, osoby z wyższym wykształceniem oraz osoby oceniające swoją sytuację materialną jako złą.

Dla 31% respondentów oszczędności z racji niższych opłat w bankowości elektronicznej nie rekompensują poziomu ryzyka tego kanału. 29,8% było innego zdanie. 4,8% dla poprawy bezpieczeństwa ponosiłoby większe koszty za obsługę konta, a 2,3% za operacje finansowe. Według 31,6% ankietowanych bankowość elektroniczna w porównaniu z bankowością tradycyjną sprzyja spirali zadłużeniu, a według 37,9% nie sprzyja.

Mimo rozwoju technologii, korzystanie z bankowości elektronicznej jest nadal związane z pewnym ryzykiem i potencjalnymi działaniami przestępczymi, które nie mogą być całkowicie wyeliminowane.

Obraz bezpieczeństwa transakcji e-bankingu jest zakłócony przez częste doniesienia mediów (np. gangi kopiujące karty i wypłacające pieniądze). Utrata karty kredytowej daje nieporównanie większe prawdopodobieństwo zwrotu pieniędzy w porównaniu do gotówki. Nieuprawnione użycie karty jest mniej ryzykowne również dlatego, że transakcje z kart są monitorowane przez banki.

Podstawowym dylematem banków jest taki rozwój zabezpieczeń w celu ochrony konsumentów, aby nie obniżać łatwości i szybkości obsługi rachunków e-bankingu.

Streszczenie

Przedmiotem niniejszego opracowania jest przedstawienie kwestii ochrony najsłabszych uczestników e-bankowości – konsumentów. W tej dziedzinie często

istnieje konflikt interesów między uczestnikami, tj. użytkownikami, wydawcami i akceptantami instrumentów elektronicznych. Artykuł powstał w wyniku analizy ankiety przeprowadzonej w 2013 r. Ma na celu ukazanie na podstawie badania ankietowego poziomu ochrony oraz świadomości konsumenta bankowości elektronicznej. Weryfikuje również hipotezę, że rodzaj grupy społecznej ma wpływ na bezpieczeństwo e-bankowości.

Słowa kluczowe: bankowość elektroniczna, ochrona konsumentów

Abstract

The subject of this paper is to present the issue of the protection of the weakest participants in e-banking – consumers. In this area, there is often a conflict of interest between participants, i.e. users, publishers, merchants and electronic instruments. The work is the result of an analysis of a survey conducted in 2013. The work aims to show, on the basis of a survey, the level of protection and consumer awareness of electronic banking. The work also reviews the hypothesis that the type of social group has an impact on the security of e-banking.

Key words: electronic banking, consumer protection

Bibliografia

Babbie E., *Podstawy badań społecznych*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Bobyk K., *Bezpieczeństwo systemów informatycznych w bankowości*, „Studia i Prace Kolegium Zarządzania i Finansów", Zeszyt naukowy 80, Szkoła Główna Handlowa w Warszawie, Warszawa 2007.

Górka J., *Aspekty ekonomiczne obrotu bezgotówkowego*, [w:] *Obrót bezgotówkowy*, red. H. Żukowska, M. Żukowski, Wydawnictwo KUL, Lublin 2013.

Górka J., *Specyfika ryzyka bankowości elektronicznej*, „Materiały i Studia", Zeszyt nr 205, NBP, Warszawa 2006.

Kowalczyk A., *Wybrane aspekty kształtowania oprocentowania kredytów związanych z funkcjonowaniem kart kredytowych na rynku bankowym w Polsce*, „Bank i Kredyt", 2006, nr 4.

Sosnowski J., *Zagrożenia i systemy zabezpieczeń pieniądza elektronicznego*, [w:] *Wyzwania w systemie bankowym w XXI wieku*, red. A. Piotrowska-Piątek, Kieleckie Towarzystwo Edukacji Ekonomicznej, Kielce 2009.

Szpringer W., *Społeczna odpowiedzialność banków. Między ochroną konsumenta a osłoną socjalną*, Wolter Kluwer, Warszawa 2009.

Materiały internetowe

Board of Governors of the Federal Reserve System, Consumers and Mobile Financial Services 2013, march 2013, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf (dostęp: 5.03.2016).

Kaszubski R., *Ochrona posiadacza karty płatniczej*, e-Biuletyn 2/2008, http://www.bibliotekacyfrowa.pl/Content/23654/Ochrona_posiadacza.pdf (dostęp: 5.03.2016).

Kutyłowski M., *Koncepcje uregulowań prawnych dotyczących bezpieczeństwa technicznego banków elektronicznych a polski stan prawny*, e-Biuletyn 3/2004, http://www.bibliotekacyfrowa.pl/Content/24750/Koncepcje_uregulowan_prawnych.pdf (dostęp: 5.03.2016).

Rola mobilnych finansów w życiu Polaków, Raport przygotowany przez TNS Polska i jestem.mobi na zlecenie Getin Banku, http://jestem.mobi/2013/10/raport-rola-mobilnych-finansow-w-zyciu-polakow/ (dostęp: 5.03.2016).

UOKIK, Konsumenci na rynku usług bankowych – raport z badań, Warszawa lipiec 2009, https://uokik.gov.pl/download.php?plik=9332 (dostęp: 5.03.2016).

UOKiK, Raport w sprawie przestrzegania praw konsumentów w umowach o korzystanie z kart płatniczych, Warszawa lipiec 2005, https://uokik.gov.pl/download.php?id=580, s. 26 (dostęp: 5.03.2016).

Wilk A., *Kradzież tożsamości. Raport z badań*, http://www.giodo.gov.pl/plik/id_p/ 6594/j/pl/ (dostęp: 5.03.2016).

Wojciechowska-Filipek S., *Metody kontroli dostępu w bankowości elektronicznej*, Konferencja Innowacje w Zarządzaniu i Inżynierii Produkcji, Zakopane 2011, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/115.pdf (dostęp: 5.03.2016).