



Anna Nowacka

Państwowa Wyższa Szkoła Zawodowa w Płocku
Wydział Nauk Ekonomicznych i Informatyki
Zakład Finansów i Rachunkowości
prorektor@pwszplock.pl

Mariola Szewczyk-Jarocka

Państwowa Wyższa Szkoła Zawodowa w Płocku
Wydział Nauk Ekonomicznych i Informatyki
Zakład Finansów i Rachunkowości
m.szewczyk-jarocka@pwszplock.pl

BEZPIECZEŃSTWO USŁUG BANKOWOŚCI ELEKTRONICZNEJ W OPINII KLIENTÓW BANKÓW SPÓŁDZIELCZYCH

Streszczenie: Bankowość elektroniczna przyczyniła się do wprowadzenia zmian formy i zakresu świadczonych usług bankowych. Jest to nie tylko alternatywna możliwość oferowania tego typu usług, ale raczej konieczność, która wynika z realiów konkurencyjnych. Banki jako instytucje zaufania publicznego muszą zwracać szczególną uwagę na bezpieczeństwo swoich klientów. Choć skala działania banków spółdzielczych jest znacznie mniejsza niż w przypadku komercyjnych, to ich klienci są tak samo narażeni na możliwość ataku ze strony środowiska przestępczego, jak w dużych bankach komercyjnych. Dlatego ważna jest edukacja w zakresie korzystania z technologii informatycznych. Celem artykułu jest zaprezentowanie opinii klientów banków spółdzielczych na temat bezpieczeństwa usług bankowości elektronicznej.

Słowa kluczowe: bankowość elektroniczna, banki spółdzielcze, bezpieczeństwo, usługa bankowa.

Wprowadzenie

Banki spółdzielcze w Polsce stoją przed dużym wyzwaniem sprostania ciągle rosnącym wymaganiom współczesnych klientów oraz konkurencji ze strony banków komercyjnych oraz innych instytucji finansowych. Konsumenci coraz chętniej korzystają z usług bankowości elektronicznej i rzadziej odwiedzają placówki bankowe. To wymaga oferowania produktów, a także usług bankowych w rosnącej liczbie kanałów elektronicznych. Banki wręcz prześcigają się w oferowaniu coraz to nowszych usług i udogodnień w bankowości internetowej oraz mobilnej, a technologiczne nowinki stają się standardowymi usługami. Dzieje

się tak, ponieważ internet i nowoczesne technologie pozwalają na spore oszczędności czasu i środków, wynikające chociażby z odciążenia obsługi naziemnej.

Rozwój elektronicznych kanałów dystrybucji związany jest z inwestycjami w bezpieczeństwo transakcji bankowych.

1. Bankowość elektroniczna w bankach spółdzielczych

Bankowość elektroniczna polega na dostarczaniu usług i produktów bankowych za pomocą elektronicznych kanałów dystrybucji przy użyciu różnych urządzeń elektronicznych, np. komputerów, telefonów, terminali. Banki spółdzielcze oferują swoim klientom następujące usługi [Wojciechowska-Filipek, 2008, s. 75-76]:

- karty płatnicze,
- systemy *home/office banking* – zdalną obsługę przy wykorzystaniu specjalnej aplikacji informatycznej dostarczonej przez bank i zainstalowanej w zasobach komputerowych klienta,
- bankowość telefoniczną – dostęp do operacji przez telefon stacjonarny,
- bankowość mobilną – dostęp do operacji przy wykorzystaniu telefonu komórkowego,
- bankowość internetową – bazującą na zdalnej komunikacji z klientem poprzez wykorzystanie komputerów osobistych wyposażonych w przeglądarkę internetową lub dostęp do łącza internetowego.

Zatem przez pojęcie „bankowości elektronicznej” należy rozumieć formę usług świadczonych przez banki na rzecz klientów, polegającą na umożliwieniu dostępu do rachunku bankowego na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak: komputer, telefon, bankomat, terminal, odbiorniki telewizji cyfrowej [Górniewicz, Obczyński i Pstruś, 2014, s. 5].

Rozwój bankowości elektronicznej w Polsce przebiega niezależnie od zmian sytuacji gospodarczej kraju. Dynamiczny wzrost liczby klientów korzystających z usług swojego banku drogą elektroniczną potwierdza tę tendencję. Pod koniec drugiego kwartału 2015 r. dostęp do bankowości internetowej miało ponad 27 mln klientów indywidualnych i 2,1 mln firm. W porównaniu do drugiego kwartału 2014 r. nastąpił wzrost o 16,77% w przypadku klientów indywidualnych i 7,12% w odniesieniu do firm [www 1].

Usługa bankowości internetowej jest systemem elektronicznym, pozwalającym klientom na łączenie się z bankiem. Internet umożliwia dostęp do informacji i transakcji w dowolnym czasie i miejscu [Wiśniewska, 2012, s. 106]. Bankowość internetowa

towa jest jedną z innowacyjnych usług oferowanych przez banki spółdzielcze, która pozwala na dokonywanie operacji bankowych za pomocą wydawanego urządzenia zwanego „touken” lub hasła podanego w SMS-ie do rachunku rozliczeniowo-oszczędnościowego. Klient w taki sposób może wykonać następujące czynności: sprawdzenie salda rachunku, przeglądanie historii konta, zarządzanie szablonami płatności, zakładanie i likwidowanie lokat, wysyłanie przelewów, monitorowanie terminarza spłat kredytu itp. [Nowy system bankowości..., 2011, s. 33].

Bankowość internetowa wydaje się dobrym rozwiązaniem dla klientów banków spółdzielczych, ze względu na odległość i dostęp do placówek oraz:

- możliwość przeprowadzania transakcji bankowych poza czasem pracy,
- zmniejszenie czasochłonnych, bezpośrednich kontaktów z placówką banku,
- szybszy dostęp do informacji o ofercie banku,
- pełen wachlarz produktów i usług w zasięgu ręki.

Usługi bankowości telefonicznej z wykorzystaniem telefonu stacjonarnego, oferowane przez banki spółdzielcze, zaliczane są do najstarszych form zdalnej komunikacji klienta z bankiem. Na rynku oferowane są dwa rozwiązania w tym zakresie [KNF, 2010]:

1. Call center – to serwis telefoniczny banku, obsługiwany przez operatora danego banku z wykorzystaniem dwustronnej komunikacji głosowej, pozwalający na dokonywanie operacji bankowych za pośrednictwem telefonu stacjonarnego. Biorąc pod uwagę efektywność obsługi bankowej podczas rozmowy z klientem jest ona niska, ponieważ konsultant cały czas poświęca na rozmowę z jednym klientem. Zaś koszty transakcyjne w tym systemie są zbyt wysokie.
2. IVR – to automatyczny serwis telefoniczny banku z wykorzystaniem jednostronnej komunikacji głosowej. Klient otrzymuje komunikaty głosowe i dokonuje wyboru odpowiedniej sekwencji znaków na klawiaturze telefonu, w zależności od operacji bankowej, którą chce wykonać. Funkcjonalność tego kanału jest mniejsza niż kanału obsługiwanego przez operatora call center, gdyż nie jest możliwa obsługa operacji nietypowych lub takich, które nie zostały wcześniej zdefiniowane w automatycznym serwisie telefonicznym banku.

W ramach bankowości elektronicznej oprócz świadczenia usług bankowych przy wykorzystaniu telefonu stacjonarnego istnieje możliwość komunikacji klienta z bankiem za pomocą telefonu komórkowego lub innego urządzenia przenośnego. Taką formę usług nazywa się bankowością mobilną (*mobile banking*). Do niedawna najpowszechniej wykorzystywanymi formami świadczenia usług z zakresu bankowości mobilnej były:

- SMS Banking,
- WAP,
- System SIM Toolkit.

WAP (*Wireless Application Protocol*) jest technologią dostosowaną do potrzeb telefonów komórkowych i innych urządzeń przenośnych o niewielkim wyświetlaczu, która umożliwia korzystanie z internetu i wykonywanie operacji bankowych w podobny sposób, jak w przypadku bankowości internetowej [KNF, s. 41]. Z kolei SIM Toolkit (*Subscriber Identity Module Application Toolkit*) jest technologią, umożliwiającą wykonywanie operacji bankowych poprzez zainstalowanie na standardowej karcie SIM telefonu komórkowego specjalnie przygotowanej aplikacji bankowej przesyłanej drogą bezprzewodową [KNF, s. 41].

Te dwa rozwiązania były mało popularne i zostały wdrożone tylko przez kilka banków. Obecnie najczęściej oferowaną formą bankowości mobilnej są wersje light versus strony responsywne, a także aplikacje natywne. Często są to odrębne aplikacje na smartfony i tablety [Pawęda, 2015b, s. 46]. Banki spółdzielcze, posiadające w swojej ofercie bankowość mobilną, najczęściej oferują swoim klientom wersję light i strony responsywne, czyli budowanie serwisu internetowego, który będzie kompatybilny z różnymi wielkościami ekranów, w tym również na urządzeniach mobilnych. Kolejnym krokiem w tym zakresie mogą być płatności mobilne.

Inną formą bankowości elektronicznej jest bankowość terminalowa, która polega na dokonywaniu transakcji bankowych, z wykorzystaniem takich elektronicznych urządzeń jak bankomaty i terminale do akceptowania kart płatniczych. Choć bankomaty należą do urządzeń przestarzałych pod względem technologicznym to banki spółdzielcze wprowadzają coraz to nowsze udogodnienia, np. możliwość wpłacania gotówki (funkcja wpłatomatu) lub możliwość doładowania telefonu.

Nowoczesną usługą, zastosowaną w bankowości terminalowej, jest biometria, czyli skanowanie układu krwionośnego palca w bankomatach. Pionierami w tym zakresie były banki spółdzielcze. W 2010 r. Bank Polskiej Spółdzielczości i Podkarpacki Bank Spółdzielczy jako pierwsze uruchomiły biometryczne bankomaty. Banki spółdzielcze zaimplementowały dwa rozwiązania biometryczne: *finger vein* (biometria naczyń krwionośnych palca) i *palm vein* (biometria naczyń krwionośnych dłoni) [Pawęda, 2015a, s. 112]. Z punktu widzenia klienta jest to technologia prosta w obsłudze. Chroni przed problemem skimmingu kart, a dodatkowo może być alternatywą dla osób starszych, które ze względu na bezpieczeństwo nie chcą nosić przy sobie karty bankomatowej. Bankowość biometryczna została wdrożona w ponad 30 bankach spółdzielczych w grupie BPS i kilku z grupy SGB.

Popularność zakupów w internecie, również wśród klientów banków spółdzielczych zachęca te instytucje do udostępniania innowacyjnych rozwiązań w zakresie e-płatności, umożliwiających realizację płatności internetowych.

Płatności *pay-by-link* polegają na automatycznym przekierowaniu klienta sklepu internetowego do jego bankowości elektronicznej. Po zalogowaniu w serwisie swojego banku, klient widzi wypełniony przelew, którego realizację może zaakceptować. System uzupełnia bankowy formularz danymi do przelewu i przekazuje sprzedawcy informację o zleconej płatności [Czas na e-płatności..., 2015, s. 108].

Dzięki współpracy Zrzeszeń BPS i SGB z KIR uruchomiono usługę płatności internetowych *Paybynet*, która wykorzystywana jest zarówno na rynku handlu elektronicznego, jak i w cyfrowej administracji publicznej. Jest to jedyny system, w którym pieniądze przekazywane są bezpośrednio pomiędzy klientem a sklepem czy urzędem. Obecnie 109 banków spółdzielczych (stan na 1.12.2015 r.) oferuje tę usługę [www 2]. Banki spółdzielcze udostępniające *Paybynet* pojawiają się automatycznie w obsługiwanych przez system sklepach internetowych oraz w sklepach obsługiwanych przez współpracujące z KIR inne systemy płatności.

2. Zagrożenia i środki bezpieczeństwa w bankowości elektronicznej

Rozwój bankowości elektronicznej, w tym dynamicznie rozwijającej się bankowości internetowej, opartej na elektronicznym przetwarzaniu danych, pociąga za sobą wzrost liczby różnorodnych form przestępczej aktywności wymierzonej przeciwko bezpieczeństwu danych, zagrażających bezpieczeństwu finansowemu na rynku usług bankowych, w szczególności bezpieczeństwu środków zgromadzonych na rachunku bankowym, do których dostęp możliwy jest na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak komputer, telefon itp. [Górniewicz, Obczyński i Pstruś, 2014, s. 5].

Najczęściej bezpieczeństwu bankowości elektronicznej zagrażają [Górniewicz, Obczyński i Pstruś, 2014, s. 5]:

- wyłudzenia danych pozwalających na przeprowadzenie transakcji,
- kradzieże z wykorzystaniem złośliwego oprogramowania,
- kopiowanie kart płatniczych,
- kradzieże związane z kartami zbliżeniowymi,
- kradzieże przy użyciu danych karty płatniczej,
- zagrożenia dotyczące płatności mobilnych,
- kradzieże tożsamości,
- „oszustwa nigeryjskie”,
- kradzieże w sklepach internetowych.

Częstym sposobem stosowanym do wyłudzenia danych, pozwalających na przeprowadzenie transakcji, wykorzystywanym przez przestępców jest przesyłanie w wiadomości e-mail linków rzekomo prowadzących do serwisów bankowości internetowej. W praktyce są to strony internetowe na serwerach przestępców. Użytkownik wprowadzając na takiej stronie swoje dane logowania oraz dane autoryzacyjne płatności w praktyce przekazuje je przestępcom. Taki rodzaj przestępczej działalności często nazywany jest phishingiem [Górniewicz, Obczyński i Pstruś, 2014, s. 5].

Często zdarzają się kradzieże z wykorzystaniem złośliwego oprogramowania. Przestępcy zorientowali się, że środowiska teleinformatyczne instytucji finansowych są z reguły bardzo dobrze zabezpieczone. Dlatego też szukali innych rozwiązań tzn. komputerów (telefonów, tabletów), które często zabezpieczone są w ograniczonym zakresie lub wcale [Górniewicz, Obczyński i Pstruś, 2014, s. 5].

Jednym z kluczowych zadań związanych z bezpieczeństwem jest ochrona przed złośliwym oprogramowaniem. Zablokowanie dostępu złośliwego kodu do infrastruktury informatycznej jest niezbędne do ochrony danych banku oraz jego klientów [Dąbrowski, 2014, s. 50-51].

Inny sposobem jest kopiowanie kart płatniczych. Przestępcy w bankomatach umieszczają urządzenia, dzięki którym sczytują dane z kart płatniczych. Jest to tzw. skimming. Ponadto potrzebują jeszcze PIN-u, w czym pomagają przestępcom dwie technologie. Montują nad klawiaturą listwy z miniaturową kamerą albo używają fałszywej klawiatury, którą przyklejają na tę prawdziwą. Dzięki temu można wpisać PIN i wypłacić pieniądze, a przestępcy wiedzą, jakie klawisze zostały naciśnięte [Górniewicz, Obczyński i Pstruś, 2014].

Kolejne to kradzieże związane z kartami zbliżeniowymi. Działania przestępcze, nakierowane są na kradzież danych z kart (zwłaszcza kredytowych) – niezależnie od tego, czy są one zbliżeniowe czy nie – i dokonywanie nimi tzw. transakcje typu *card-not-present* (bez fizycznej obecności karty, np. przez internet) [Górniewicz, Obczyński i Pstruś, 2014].

Kolejne to kradzieże przy użyciu karty płatniczej. Osoby, które płacą kartami w polskich i europejskich sklepach wiedzą, że do przeprowadzenia transakcji trzeba podać „kod zabezpieczający”, znajdujący się na odwrocie karty. Niestety są kraje, w których kod CVC2/CVV2, trzycyfrowy kod wydrukowany z tyłu karty obok miejsca na podpis, nie jest wymagany i do skutecznego przeprowadzenia transakcji wystarczy numer karty, data ważności i dane personalne na niej wytłoczone [Górniewicz, Obczyński i Pstruś, 2014].

Następna kwestia to zagrożenia dotyczące płatności mobilnych. Aby uniknąć zagrożenia trzeba zastosować kilka wymienionych niżej zasad [Górnisiewicz, Obczyński i Pstruś, 2014]:

- telefon z zainstalowaną aplikacją do płatności mobilnych powinien mieć włączoną blokadę ekranu, której dezaktywacja powinna wymagać wprowadzenia hasła (lub w inny sposób była możliwa do dokonania jedynie dla prawowitego właściciela telefonu),
- nie należy zapisywać hasła do aplikacji płatności mobilnych na kartce (lub innym nośniku), zwłaszcza przechowywanej wraz z telefonem,
- hasło do telefonu powinno być inne niż do aplikacji płatności mobilnych, hasła te powinny również być trudne do odgadnięcia,
- telefon używany do dokonywania płatności mobilnych powinien zawsze być zabezpieczony przez aktualne oprogramowanie antywirusowe,
- na telefonie służącym do dokonywania płatności mobilnych należy zawsze instalować najnowsze aktualizacje bezpieczeństwa systemu operacyjnego,
- oddając telefon do serwisu warto odinstalować aplikację płatności mobilnych,
- niezwłocznie po utracie telefonu, na którym zainstalowana była aplikacja płatności mobilnych, należy zgłosić ten fakt w swoim banku.

Kolejnym elementem zagrażającym bezpieczeństwu bankowości elektronicznej są kradzieże tożsamości. Na przykład fałszywy pracodawca kontaktuje się w celu ustalenia terminu rozmowy kwalifikacyjnej i z prośbą o wypełnienie bardzo szczegółowego kwestionariusza osobowego na stronie internetowej lub o przesłanie odpowiednich danych w pliku na adres e-mail. Jeśli podamy numer naszego rachunku bankowego, wszystkie dane osobowe i numer telefonu komórkowego – przestępcy mogą wykorzystać te informacje do zakładania rachunków bankowych, które następnie są używane np. do przesyłania pieniędzy pochodzących z przestępstw. Wtedy stajemy się tzw. słupami, np. w procederze prania pieniędzy [Górnisiewicz, Obczyński i Pstruś, 2014].

Następnym zagrożeniem są „oszustwa nigeryjskie”. Przyjęcie pieniędzy niewiadomego pochodzenia na swój rachunek bankowy i przekazanie ich dalej może być udziałem w większym oszustwie – praniu pieniędzy czy nawet finansowaniu terroryzmu. Udział w przekazywaniu środków pieniężnych może skutkować podjęciem odpowiednich czynności przez prokuraturę oraz sąd, a następnie wymierzeniem kary [Górnisiewicz, Obczyński i Pstruś, 2014].

Ostatni wymieniony element to kradzieże w sklepach internetowych. Ofiarą takiego oszustwa może zostać każdy. Do tego typu przestępstw dochodzi również na portalach aukcyjnych. Sprawcy wykorzystują w tym przypadku przelewy na rachunki, płatności przy użyciu PayPal bądź podobnych rozwiązań [Górnisiewicz, Obczyński i Pstruś, 2014].

3. Bezpieczeństwo w bankowości elektronicznej w świetle badań własnych

Celem badania było określenie zakresu usług bankowości elektronicznej, z których korzystają klienci banków spółdzielczych oraz poznanie ich opinii na temat bezpieczeństwa tych usług.

Badanie ankietowe zostało przeprowadzone we wrześniu i październiku 2015 r. wśród klientów wybranych banków spółdzielczych, zlokalizowanych na terenie powiatu plockiego (województwo mazowieckie) i żywieckiego (województwo śląskie). Klienci objęci badaniem ankietowym zostali wybrani metodą doboru wygodnego [Hill i Aleksander, 2003, s. 126]. O wypełnienie ankiety poproszeni zostali klienci, którzy wychodzili z banku i wyrażali chęć udzielenia odpowiedzi na zawarte w kwestionariuszu pytania. Łącznie przebadanych zostało 99 osób z województwa mazowieckiego i 32 z województwa śląskiego. Próba miała charakter niereprezentatywny. Obliczenia wykonano w programie IBM SPSS 23.0. Jako poziom istotności statystycznej przyjęto $p < 0,05$.

W badaniu uczestniczyło 32 mężczyzn i 50 kobiet, będących członkami banków spółdzielczych, co stanowiło odpowiednio 56,1% i 67,6%. Pozostałe przebadane osoby, tj. 49 respondentów nie było członkami banków spółdzielczych. 13 osób uplasowało się w przedziale wiekowym 18-25 lat, 18 respondentów było z przedziału wiekowego 26-35 lat, 21 osób w przedziale 36-45 lat, 17 osób w przedziale wiekowym 46-55 lat, a 14 respondentów miało 56 lat i więcej. Większość osób będących członkami banków spółdzielczych zamieszkiwało wieś, tj. 30 osób, wieś-gminę – 39 osób. Najwięcej osób posiadało wykształcenie średnie zawodowe – 21 osób i wyższe zawodowe – 20 osób. 36 osób było zatrudnionych na stałe. Z reguły osoby te były rolnikami – 20 osób, a 17-osobowe grupy stanowili urzędnicy i pracownicy fizyczni. Najwięcej osób, tj. 26 deklarowało się, iż otrzymuje dochód miesięczny z przedziału 1001-1500 zł, a 1501-2000 zł – 13 respondentów.

Narodziny bankowości elektronicznej pozwoliły bankom przyciągnąć klientów swoją ofertą. To zmieniło również sytuację banków spółdzielczych. Tradycyjne produkty bankowe, oferowane w placówkach były często jedyną dostępną propozycją korzystania z usług finansowych dla mieszkańców małych miast oraz wsi. Z roku na rok sektor stanął wobec konkurencji banków, świadczących usługi elektroniczne. Banki spółdzielcze zostały zmuszone do przeprowadzenia procesów informatyzacji swojej działalności i zapewnienia tym samym dostępu do usług świadczonych za pośrednictwem elektronicznych kanałów dystrybucji. Usługi bankowości elektronicznej cieszą się coraz większą popularnością również wśród klientów banków spółdzielczych, o czym świadczą wyniki zaprezentowane w tab. 1.

Tabela 1. Korzystanie z usług bankowości elektronicznej oferowanych przez banki spółdzielcze?

Wyszczególnienie	Częstość	Procent	Procent ważnych	Procent skumulowany
Tak	59	44,7	45,7	45,7
Nie	66	50,0	51,2	96,9
Bank nie oferuje takich usług	4	3,0	3,1	100,0
Ogółem	129	97,7	100,0	0
Braki danych	3	2,3	0	0
Ogółem	132	100,0	0	0

Źródło: Na podstawie przeprowadzonych badań ankietowych.

59 osób zadeklarowało korzystanie z usług bankowości elektronicznej, prowadzonej przez banki spółdzielcze. Stanowi to ok. 45% udzielonych odpowiedzi. Dane te odzwierciedlają ogólnopolskie tendencje wzrostowe w zakresie korzystania z bankowości elektronicznej. Z danych Związku Banków Polskich wynika, że pod koniec 2015 r. ponad 30 mln Polaków podpisało umowy o rachunek bankowy z dostępem do bankowości internetowej, z czego ponad 14 mln było aktywnych [ZBP, 2015].

Poproszono klientów banków spółdzielczych o określenie częstotliwości korzystania z poszczególnych form bankowości elektronicznej (tab. 2).

Tabela 2. Popularność usług bankowości elektronicznej wśród klientów banków spółdzielczych

Kategoria usługi bankowej	Liczba wskazań	Średnia częstotliwość korzystania z usługi w miesiącu
Bankowość internetowa	59	9,07
Bankowość telefoniczna	55	1,02
Karty płatnicze	56	12,09
Karty kredytowe	56	0,52

Źródło: Na podstawie przeprowadzonych badań ankietowych.

Respondenci wskazywali bankowość internetową ze średnią częstotliwością korzystania w miesiącu na poziomie 9,07. Najczęściej korzystali jednak z kart płatniczych (średnia 12,09). Te wyniki potwierdzają, że prawie wszystkie osoby, które ogólnie zadeklarowały korzystanie z bankowości elektronicznej, korzystały z różnych jej form.

Ogólnopolskie badania przeprowadzone przez NBP w 2013 r. potwierdziły, że 62% Polaków, posiadających bankowość internetową, korzysta z niej często lub bardzo często, a 18% tej grupy nie korzysta w ogóle. Podobnie wyglądała

sytuacja z kartami płatniczymi – 63% badanych posiada je i korzysta, natomiast 1/3 Polaków nie uczestniczy w obrocie bezgotówkowym. Znacznie mniej Polaków ma i korzysta z karty kredytowej (13%). Przyczyn niekorzystania z tej formy usług należy upatrywać w braku technicznych możliwości (brak internetu i komputera), nieumiejętności korzystania z internetu i bankowości internetowej oraz obawach związanych z bezpieczeństwem tego typu transakcji [Kozłowski, 2013, s. 93].

Tabela 3. Zagrożenie bezpieczeństwa transakcji w bankowości terminalowej (bankomaty, karty bankomatowe) a przynależność do grupy społeczno-zawodowej

Wyszczególnienie		Przynależność do grupy społeczno-zawodowej							Ogółem
		urzędnik	wolny zawód	nauczyciel	rolnik	pracownik fizyczny	rzemieślnik	inny	
Nie	N	8	6	6	10	16	0	5	51
	%	15,7%	11,8%	11,8%	20 %	31,3%	0	9,4%	52%
Tak	N	10	6	1	12	8	6	4	47
	%	21,3%	12,8%	2,1%	25,5%	17%	12,8%	8,5%	48%
Ogółem	N	18	12	7	22	24	6	9	98
	%	18,4%	12,3%	7,1%	22,4%	24,5%	6,1%	9,2%	100%

N – liczba klientów

Źródło: Na podstawie przeprowadzonych badań ankietowych.

Tabela 4. Test Chi-kwadrat

Wyszczególnienie	Wartość	df	Istotność asymptotyczna (dwustronna)
Chi-kwadrat Pearsona	12,611	6	,050

$$\chi^2 = 12,611$$

$$df = 6$$

$$p = 0,050$$

test istotny przy $p < 0,05$

Pomiędzy zmiennymi wykazano istotną zależność, co oznacza że przynależność do grupy społeczno-zawodowej miała wpływ na opinię na temat bezpieczeństwa transakcji w bankowości terminalowej. Wśród osób uważających, że istnieje zagrożenie w bankowości terminalowej najliczniejszą grupę stanowili: rolnicy (25,5%) oraz pracownicy fizyczni (21,3%). Przeciwnego zdania byli najczęściej: pracownicy fizyczni (31,3%) oraz rolnicy (20%). Dostępnym zaskakujące, że w obydwu grupach znaleźli się rolnicy. Może to wynikać z faktu, że stanowią najliczniejszą grupę klientów banków spółdzielczych. Rozkład odpowiedzi wynika z częstotliwości przeprowadzanych transakcji i częściowo znajduje odzwierciedlenie w ogólnopolskich badaniach przeprowadzonych przez NBP, które wskazują że: największy udział płatności kartami, pod względem liczby płatno-

ści, występuje wśród specjalistów i techników (30%) oraz urzędników i pracowników instytucji publicznych (28%). Najmniej kartami płacą rolnicy (2%), renciści (3%), emeryci (4%), osoby zajmujące się domem (5%) i bezrobotni (6%) [Kozłiński, 2013, s. 93].

Istotną zależność można zauważyć pomiędzy wiekiem respondentów a zagrożeniem bezpieczeństwa transakcji w bankowości internetowej (tab. 5 i 6).

Tabela 5. Zagrożenie bezpieczeństwa transakcji w bankowości internetowej (konta internetowe) a wiek respondentów

Wyszczególnienie		Wiek respondentów					Ogółem
		18-25	26-35	36-45	46-55	56 i więcej	
Nie	N	3	11	13	8	1	36
	%	8,3%	30,6%	36,1%	22,2%	2,8%	33,3%
Tak	N	16	11	15	15	15	72
	%	22,3%	15,3%	20,8%	20,8%	20,8%	66,7%
Ogółem	N	19	22	28	23	16	108
	%	17,6%	20,4%	25,9%	21,3%	14,8%	100%

N – liczba klientów

Źródło: Na podstawie przeprowadzonych badań ankietowych.

Tabela 6. Test Chi-kwadrat

Wyszczególnienie	Wartość	df	Istotność asymptotyczna (dwustronna)
Chi-kwadrat Pearsona	12,845	4	,012

$$\chi^2 = 12,845$$

$$df = 46$$

$$p = 0,012$$

test istotny przy $p < 0,05$

Najmłodszy i najstarszy klienci najrzadziej uważali, że nie występuje zagrożenie bezpieczeństwa transakcji w bankowości internetowej. Grupa wiekowa 18-25 najczęściej korzysta z elektronicznego kanału dystrybucji usług i dlatego też najczęściej udzielała odpowiedzi twierdzącej (22,3%). Trzeba jednak zauważyć, że wśród klientów twierdzących, iż istnieje zagrożenie transakcji w bankowości internetowej nie ma zbyt istotnych różnic. Natomiast osoby te stanowią prawie 67% wszystkich ankietowanych, którzy odpowiedzieli na to pytanie.

Banki spółdzielcze coraz więcej inwestują w bankowość mobilną. Z badań opublikowanych w PRNews.pl wynika, że liczba aktywnych użytkowników bankowości mobilnej przekroczyła 5 mln użytkowników na koniec września 2015 r. [PRNews.pl, 2015].

Tabela 7. Zagrożenie bezpieczeństwa transakcji w bankowości mobilnej a przynależność do grupy społeczno-zawodowej

Wyszczególnienie		Przynależność do grupy społeczno-zawodowej							Ogółem
		urzędnik	Wolny zawód	nauczyciel	rolnik	Pracownik fizyczny	rzemieślnik	inny	
Nie	N	13	3	4	19	17	6	7	69
	%	18,8%	4,3%	5,8%	27,5%	24,6%	8,7%	10,1%	70,4%
Tak	N	5	9	3	3	7	0	2	29
	%	17,2%	31,0%	10,4%	10,4%	24,1%	0%	6,9%	29,6%
Ogółem	N	18	12	7	22	24	6	9	98
	%	18,4%	12,2%	7,1%	22,4%	24,5%	6,1%	9,3%	100%

N – liczba klientów

Źródło: Na podstawie przeprowadzonych badań ankietowych.

Tabela 8. Testy Chi-kwadrat

Wyszczególnienie	Wartość	df	Istotność asymptotyczna (dwustronna)
Chi-kwadrat Pearsona	17,942	6	,006

 $\chi^2 = 17,942$

df = 6

p = 0,006

test istotny przy $p < 0,05$

Pomiędzy zmiennymi wykazano istotną zależność, co oznacza że rolnicy (27,5%) najczęściej wskazywali brak zagrożenia bezpieczeństwa transakcji w bankowości mobilnej. Przeciwnego zdania były osoby wykonujące wolny zawód – 31%.

Podsumowanie

Bankowość elektroniczna pełni wiele funkcji – jest zarówno narzędziem marketingowym, jak i dystrybucyjnym. Z jednej strony ma na celu pozyskanie nowych klientów. Z drugiej jest ogromną szansą dla banków spółdzielczych poszukujących oszczędności. Stanowi nowoczesną formę komunikacji z klientem. Dzięki temu nowe produkty bankowe można oferować i wprowadzać również klasycznymi kanałami dystrybucji.

Nowoczesne technologie i rozwiązania niosą za sobą nowe rodzaje ryzyka bankowego oraz zagrożeń, ale są jednak nieodzownym elementem zapewniającym rozwój banków spółdzielczych. Badana zbiorowość nie jest reprezentatywna dla ogółu polskich banków spółdzielczych. Jednak pewne wnioski można odnieść do całej zbiorowości. Ankietowani klienci banków spółdzielczych

posiadają wiedzę na temat nowych rozwiązań technologicznych w bankowości, dlatego też ich oczekiwania i preferencje zmieniają się. Prawie połowa respondentów korzysta z różnych form bankowości elektronicznej. Najbardziej popularna pozostaje wciąż bankowość internetowa. Zaprezentowane wyniki badań wskazują, że klienci dosyć często korzystają z usług w zakresie bankowości elektronicznej i zdają sobie sprawę z zagrożeń związanych z korzystaniem z tej oferty. Najniższą świadomość dotyczącą zagrożenia bezpieczeństwa transakcji odnotowano w przypadku bankowości mobilnej. Wynika to z faktu, że są to nowe usługi i jeszcze niezbyt popularne wśród klientów banków spółdzielczych.

Banki spółdzielcze chcące sprostać rosnącej konkurencji muszą oferować produkty i usługi w różnych kanałach dystrybucji elektronicznej. To wiąże się z rosnącym ryzykiem w obszarze IT i wysokimi nakładami na zapewnienie bezpieczeństwa środków pieniężnych, zgromadzonych na kontach. Rozwiązaniem dla banków spółdzielczych może być budowa Centrum Usług Wspólnych (CUW) dla sektora bankowości spółdzielczej, wprowadzające wystandaryzowane usługi w obszarze IT dla całego sektora. Nakłady na informatyzację są na tyle znaczące dla pojedynczego banku, że CUW pozwoliłoby na współdzielenie kosztów utrzymania i rozwoju technologicznego.

Literatura

- Czas na e-płatności w bankach spółdzielczych* (2015), „Nowoczesny Bank Spółdzielczy”, nr 9, s. 108-109.
- Dąbrowski R. (2014), *Bezpieczeństwo IT z punktu widzenia Rekomendacji D [w:] Czy misja potrzebuje IT? Technologiczne aspekty rozwoju banków spółdzielczych*, VI Forum Technologii Bankowości Spółdzielczej, 20-21 maja, Warszawa.
- Górniewicz M., Obczyński R., Pstruś M. (2014), *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, Komisja Nadzoru Bankowego, CEDUR, Warszawa, https://www.knf.gov.pl/Images/Bezpiec_finansowe_tcm75-39005.pdf (dostęp: 15.12.2015).
- Hill N., Aleksander J. (2003), *Pomiar satysfakcji i lojalności klientów*, Oficyna Ekonomiczna, Kraków.
- Komisja Nadzoru Finansowego (2010), *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Warszawa.
- Koźliński T. (2013), *Zwyczajne płatnicze Polaków*, NBP, Warszawa, http://www.nbp.pl/system_platniczy/zwyczajne_platnicze/zwyczajne_platnicze_Polakow.pdf (dostęp: 3.01.2016).
- Nowy system bankowości internetowej* (2011), „Bank wspólnych sił. Magazyn Grupy BPS”, nr 2, s. 33.

- Pawęda D. (2015a), *Biometria – rewolucja czy ewolucja?* „Nowoczesny Bank Spółdzielczy”, nr 9, s. 110-115.
- Pawęda D. (2015b), *Rozwiązania mobilne w bankowości spółdzielczej*, publikacja podsumowująca VII Forum Technologii Bankowości Spółdzielczej, Warszawa, s. 45-48.
- PRNews.pl (2015), *Rynek bankowości mobilnej – III kw. 2015*, <http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-mobilnej-iii-kw-2015-6551613.html> (dostęp: 15.02.2016).
- Wiśniewska A. (2012), *Innowacyjne usługi bankowe dla klientów indywidualnych w bankach spółdzielczych* [w:] M. Stefański (red.), *Wybrane historyczne i współczesne aspekty rozwoju banków spółdzielczych w Polsce*, Wydawnictwo Wyższej Szkoły Humanistyczno-Społecznej we Włocławku, Włocławek.
- Wojciechowska-Filipek S. (2008), *Zastosowanie technologii informacyjnej w produktach i usługach banków spółdzielczych* [w:] M. Stefański (red.), *Perspektywy rozwoju bankowości spółdzielczej w Polsce*, Wydawnictwo Wyższej Szkoły Humanistyczno-Ekonomicznej we Włocławku, Włocławek.
- ZBP, *Bankowość internetowa i płatności bezgotówkowe III kwartał 2015 r.*, http://zbp.pl/public/repozytorium/wydarzenia/images/grudzien_2015/konf/Netbank_Q3_finalna.pdf (dostęp: 13.12.2015).
- [www 1] http://zbp.pl/public/repozytorium/wydarzenia/images/wrzesien_2015/konferencja_prasowa/Netbank_Q2_201523.09.2015.pdf (dostęp: 15.01.2016).
- [www 2] <http://www.paybynet.pl> (dostęp: 13.12.2015).

SECURITY OF ON-LINE BANKING SERVICES IN THE OPINION OF THE CLIENTS OF COOPERATIVE BANKS

Summary: Banks as institutions of public trust have to pay particular attention to the security of their clients. Even if cooperative banks function on a significantly smaller scale than commercial ones, their clients are equally vulnerable to the possibility of criminal attack as it is the case with big commercial banks. That is why education concerning the use of information technologies is of particular importance. The purpose of the article is to present the opinions of clients of cooperative banks on the security of online banking services.

Keywords: on-line banking, cooperative banks, security, banking services.