



Tom 25/2017, ss. 203–214
ISSN 1644-888X
e-ISSN 2449-7975
DOI: 10.19251/ne/2017.25(13)
www.ne.pwspzlock.pl

Mariola Szewczyk-Jarocka

Państwowa Wyższa Szkoła Zawodowa w Płocku

**BANKOWOŚĆ MOBILNA I TERMINALOWA
JAKO PRZYKŁAD USŁUG BANKOWOŚCI
ELEKTRONICZNEJ ZAGROŻONEJ
BEZPIECZEŃSTWEM W OPINII KLIENTÓW BANKÓW
SPÓŁDZIELCZYCH – BADANIA WŁASNE**

MOBILE AND TERMINAL BANKING AS AN EXAMPLE OF ELECTRONIC
BANKING SERVICES WITH A SECURITY RISK IN THE OPINION OF
COOPERATIVE BANKS CUSTOMERS – BASED ON OWN RESEARCH

Streszczenie

Obecnie możemy o każdej porze dnia i z dowolnego miejsca korzystać ze zdobyczy technologii, zwłaszcza informatycznych. Bez czasochłonnej wizyty w banku możemy się ubezpieczyć, założyć lokatę lub dokonać comiesięcznych opłat za rachunki.

Produkty i usługi bankowe dostarczane są przy wykorzystaniu najróżniejszych kanałów przepływu informacji z zastosowaniem urządzeń elektronicznych.

Summary

Nowadays, we can use technological achievements, especially in information technology, at any time and anywhere. We can insure ourselves, open a deposit or make monthly payments without a time-consuming visit to the bank.

Banking products and services use various channels of information flow delivered via electronic devices. Modern services provided by cooperative banks include:

- internet banking,

Nowoczesne usługi świadczone w bankach spółdzielczych obejmują:

- bankowość internetową,
- bankowość mobilną,
- bankowość terminalowa,
- bankowość telefoniczną,
- karty płatnicze i bankomaty,
- usługi biometryczne stosowane w bankomatach,
- przekazy Western Union.

Celem artykułu jest odpowiedź na pytanie czy występuje czy raczej nie występuje zależność pomiędzy bankowością mobilną oraz bankowością terminalową jako usługą bankowości elektronicznej zagrożenie bezpieczeństwa w opinii klientów banków spółdzielczych. Autorka stara się odpowiedzieć na pytanie czy faktycznie w ocenie klientów występuje zagrożenie bezpieczeństwa przy korzystaniu z bankowości mobilnej i bankowości terminalowej, czy raczej w ocenie większości ankietowanych nie ma takiej tendencji tzn. transakcje nie są zagrożone w większości przypadków, ponieważ banki oferują nowoczesne, bezpieczne rozwiązania informatyczne.

Słowa kluczowe: bankowość mobilna, bankowość terminalowa, usługi bankowości elektronicznej, banki spółdzielcze, badania własne, opinii klientów

Wprowadzenie

Obecnie możemy o każdej porze dnia i z dowolnego miejsca korzystać ze zdobyczy technologii, zwłaszcza informatycznych. Bez czasochłonnej wizyty w banku możemy się ubezpieczyć, założyć lokatę lub dokonać comiesięcznych opłat za rachunki.

M-banking lub mobile banking umożliwia dostęp do rachunku bankowego przy pomocy urządzeń, które posiadają dostęp do Internetu tj. telefon

- mobile banking,
- terminal banking,
- phone banking,
- pay cards and ATMs,
- biometric services used in ATMs,
- Western Union money transfers.

The author of this thesis aims to answer the question whether there is, or rather there is no relationship between mobile banking and terminal banking as electronic banking services as far as security threat is concerned in the opinion of cooperative banks customers. The author attempts to answer the question whether, in the opinion of customers, the security threat actually exists when using mobile banking and terminal banking, or rather the majority of respondents think that there is no such tendency, i.e. transactions are not at risk in most cases, since banks offer modern and secure IT solutions.

Keywords: mobile banking, terminal banking, electronic banking services, cooperative banks, own research, customers opinions.

komórkowy, smartfon, tablet. Bankowość mobilna jest elementem bankowości internetowej. Poważanym wyzwaniem dla banków oferujących bankowość mobilną jest zapewnienie bezpieczeństwa. Zapewnienie bezpieczeństwa musi być skoordynowane przez twórców aplikacji komórkowych, przez dział IT banku oraz operatorów sieci bezprzewodowych. Transakcje można uznać za bezpieczne jeśli spełniają określone warunki, do których m.in. należą szyfrowanie danych, uwierzytelnienie nazwy i hasła użytkownika banku, ochrona sprzętu przenośnego itp.

Nowoczesną usługą zastosowaną w bankowości terminalowej jest biometria czyli skanowanie układu krwionośnego palca w bankomatach. Pionierami w tym zakresie były banki spółdzielcze. W 2010 roku Bank Polskiej Spółdzielczości i Podkarpacki Bank Spółdzielczy jako pierwsi uruchomili biometryczne bankomaty. Banki spółdzielcze zaimplementowały dwa rozwiązania biometryczne: finger vein (biometria naczyń krwionośnych palca) i palm vein (biometria naczyń krwionośnych dłoni) [Pawęda, 2015, 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.

Celem autorki artykułu jest odpowiedź na pytanie czy występuje czy raczej nie występuje zależność pomiędzy bankowością mobilną oraz bankowością terminalową jako usługami bankowości elektronicznej, a zagrożeniem bezpieczeństwa w opinii klientów banków spółdzielczych. Autorka stara się odpowiedzieć na pytanie czy faktycznie w ocenie klientów występuje zagrożenie bezpieczeństwa przy korzystaniu z bankowości mobilnej i bankowości terminalowej, czy raczej w ocenie większości ankietowanych nie ma takiej tendencji tzn. transakcje nie są zagrożone w większości przypadków, ponieważ banki oferują nowoczesne, bezpieczne rozwiązania informatyczne.

1. Nowoczesne usługi w bankach spółdzielczych

W wyniku dynamicznych zmian zachodzących na rynku usług bankowych oraz ciągłego pojawiania się kolejnych generacji klientów, banki zmuszone są do stałego poszukiwania nowych rozwiązań w zakresie obsługi klienta. Ich oferta oraz sposób jej udostępnienia muszą być dostosowane do oczekiwań poszczególnych, obsługiwanych segmentów klientów. Takie możliwości

dają technologie informacyjne stosowane w różnych dziedzinach gospodarki, w tym również w bankowości. Produkty i usługi bankowe dostarczane są przy wykorzystaniu najróżniejszych kanałów przepływu informacji z zastosowaniem urządzeń elektronicznych. Nowoczesne usługi świadczone w bankach spółdzielczych obejmują:

- bankowość internetową,
- bankowość mobilną,
- bankowość telefoniczną,
- karty płatnicze i bankomaty,
- usługi biometryczne stosowane w bankomatach,
- przekazy Western Union.

Usługi bankowości elektronicznej cieszą się coraz większą popularnością również wśród ankietowanych klientów banków spółdzielczych, o czym świadczą wyniki zaprezentowane w tabeli 1.

Tabela 1. Korzystanie z usług bankowości elektronicznej w bankach spółdzielczych

| Wyszczególnienie | Liczba | Procent |
|-------------------------------|--------|---------|
| Tak | 59 | 44,7 |
| Nie | 66 | 50,0 |
| Bank nie oferuje takich usług | 4 | 3,0 |
| Ogółem | 129 | 97,7 |
| Braki danych | 3 | 2,3 |
| Ogółem | 132 | 100,0 |

Źródło: Opracowanie własne w oparciu o przeprowadzone badania ankietowe.

59 osób zadeklarowało korzystanie z usług bankowości elektronicznej prowadzonej przez banki spółdzielcze. Stanowi to około 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 roku ponad 30 mln Polaków podpisało umowy o rachunek bankowy z dostępem do bankowości internetowej, z czego ponad 14 mln było aktywnych [www1].

2. Bankowość mobilna i terminalowa jako usługa bankowości elektronicznej

Bankowość mobilna zawiera się w bankowości elektronicznej, jak i internetowej, nazywana bywa m-banking. Bankowość mobilna jest to korzystanie z systemu bankowego przez Internet, jednak wyłącznie przy użyciu telefonu komórkowego, najczęściej tzw. smartfona. To więc wyłącznie urządzenie, z jakiego korzystamy łącząc się z systemem, wskazuje na to, czy mamy do czynienia z bankowością internetową, czy w węższym znaczeniu - bankowością mobilną [www2].

Bankowość mobilna to dostęp do usług bankowych przez aplikację mobilną zainstalowaną w telefonie lub na tablecie. Tak jak bankowość internetową oferują ją wszystkie banki uniwersalne, tak i aplikacje bankowości mobilnej posiada już większość liczących się banków na rynku. Aplikacje bankowe wykorzystują nowoczesne funkcje dostępne w urządzeniach mobilnych (GPS, kamera, czujniki położenia), aby zaoferować klientowi unikalne możliwości podczas korzystania z bankowości. Zasadnicza różnica między aplikacjami polega na zakresie dostępnych operacji oraz na rodzaju / ilości funkcji dodatkowych, specyficznych i niekoniecznie finansowych [www3].

Bankowość terminalowa, inaczej bankowość samoobsługowa lub self-banking, stanowi najstarszą i najbardziej powszechną formę bankowości elektronicznej. Polega ona na samoobsługowym korzystaniu przez użytkownika z terminala udostępnionego przez bank (zazwyczaj w miejscu publicznym). Bankomaty to najprostszy rodzaj terminali wykorzystywanych w bankowości terminalowej. Są to samoobsługowe urządzenia wyposażone w czytniki paska magnetycznego lub mikroprocesora, umożliwiające dokonywanie operacji bankowych przy użyciu kart płatniczych.

Pierwszy bankomat na świecie został uruchomiony w 1964 roku przez First Pennsylvania Bank w Stanach Zjednoczonych, natomiast do użytku publicznego pierwszy bankomat wprowadzono w 1969 roku w Wielkiej Brytanii. Jeśli chodzi o Polskę to pierwszy bankomat pojawił się w drugiej połowie lat osiemdziesiątych ubiegłego wieku w III Oddziale Banku Polska Kasa Opieki w Warszawie (obecnie PKO S.A.).

3. Bezpieczeństwo elektronicznych usług bankowych

Odwiecznym problemem banków, a także banków spółdzielczych jest zapewnienie bezpieczeństwa w bankach na odpowiednim poziomie. Według J.

Grzywacza: *Doświadczenia z praktyki bankowej potwierdzają, że rozwój nowoczesnych usług bankowych zależy w istotnym stopniu od skuteczności przekonania klientów o wysokim poziomie bezpieczeństwa stosowanych technologii. Przedsiębiorstwa i osoby fizyczne często pytają o bezpieczeństwo przy podejmowaniu decyzji o korzystaniu z łączności elektronicznych w kontaktach z bankiem i składaniu tą drogą różnych zleceń. Z drugiej strony media informują o nadużyciach dokonywanych przy pomocy technologii informatycznych, co wywołuje opory przy korzystaniu z usług bankowości elektronicznej, a co z tym idzie i bankowości mobilnej.* [Grzywacz, 2016, s. 118]

Klient, któremu bank, a także bank spółdzielczy zapewni bezpieczeństwo będzie korzystał z nowoczesnych technologii i rozwiązań obsługi finansowej oferowanej przez banki. Opinie na temat bezpieczeństwa usług oferowanych przez banki są bardzo zróżnicowane i zależą od wieku, wykształcenia, płci, stanu cywilnego, miejsca zamieszkania, przynależności do grupy społeczno-zawodowej, dochodów itp.

Według A. Gospodarowicza określających bankowość elektroniczną, a co z tym idzie bankowość mobilną jako *zbiór atrybutów* [Gospodarowicz, 2005, s. 55]:

- *poufność*, czyli gwarancja o dostępie do danych jedynie osób uprawnionych,
- *integralność*, czyli gwarancja, że sposób przesyłania danych jest prawidłowy i nie mogą one być zmienione,
- *autentyczność*, czyli gwarancja, że osoba, która dokonuje transakcji jest ta, za którą się podaje,
- *niezaprzeczalność*, czyli brak możliwości zanegowania faktu, że wiadomość elektroniczna została nadana bądź odebrana,
- *niezawodność*, czyli gwarancja, że system działa we właściwy sposób oraz zgodnie z jego przeznaczeniem.

Według J. Grzywacza wydaje się, że najważniejszą kwestią zwłaszcza w przypadku bankowości internetowej, a co z tym idzie i mobilnej jest zapewnienie przez bank [Grzywacz, 2016, s. 119]:

- natychmiastowego potwierdzenia tożsamości osób realizujących transakcję,
- stosowanie skutecznego systemu szyfrowania transmisji informacji i zapewnienia jej całkowitej poufności,

- odpowiedniego zabezpieczenia serwera instytucji, będącej dostawcą internetowych usług finansowych, przed nielegalnym dostępem,
- zabezpieczenie serwera przed celowymi atakami przeprowadzanymi zarówno z zewnątrz (Internet), jak i od środka (sieć lokalna).

Z drugiej strony według J. Grzywacza bezpieczeństwo operacji elektronicznych zależy od klienta, który powinien przestrzegać następujących zasad [Grzywacz, 2016, s. 120]:

- posiadane hasła umożliwiające dostęp do rachunku powinny być starannie chronione (dotyczy to także tokenów generujących jednorazowe hasło),
- każdorazowe połączenie z bankiem wymaga sprawdzenia, czy przesyłane informacje są szyfrowane,

4. Regulacje prawne dotyczące bezpieczeństwa informatycznego

Przepisy prawne są bardzo istotnym elementem dla osób korzystających z technologii informacyjnych, ponieważ regulują bezpieczny przepływ informacji. Duże znaczenie odgrywają tu m.in.:

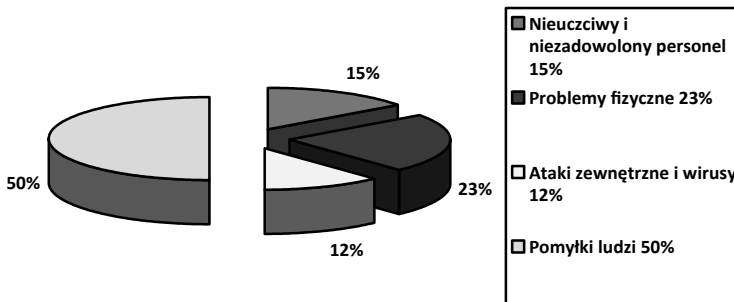
- ustawa o ochronie danych osobowych,
- ustawa o ochronie informacji niejawnych,
- ustawa Prawo bankowe,
- kodeks karny,
- ustawa o podpisie elektronicznym,
- kodeks cywilny,
- ustawa o elektronicznych instrumentach płatniczych.

Szybki rozwój nowoczesnych sieci informatycznych całkowicie uzasadnia konieczność dostosowania istniejących regulacji prawnych do nowych zmian i uwarunkowań.

5. Wybrane rodzaje zagrożeń systemów informatycznych

Rozwój współczesnej technologii jest z jednej strony olbrzymim ułatwieniem, a z drugiej strony niesie za sobą szereg zagrożeń wynikających z następujących kwestii [Grzywacz, 2016, s. 122]:

- większość dokumentacji i informacji, które znajdowały się wcześniej w różnych miejscach przechowywana jest na komputerze, co oznacza ułatwienie ich znalezienia,
- dane gromadzone są w systemach informatycznych i znajdują się pod opieką osoby odpowiednio przygotowanej – administratora systemu,
- wysoki koszt zabezpieczeń danych, problem bezpieczeństwa zostaje zaniedbany przez użytkowników systemów informatycznych,
- firmy oferujące zabezpieczenia do systemów informatycznych nie są certyfikowane, co świadczy o niskiej jakości usług,
- proponowane przez firmy systemy informatyczne są wadliwe lub zawierają błędy,
- nowe zagrożenia niesie Internet,
- informacja jest jednym z poszukiwanych towarów n rynku,
- banki, dla których zaufanie jest kwestią kluczową, nie dopuszczają często do przekazywania opinii publicznej informacji o przypadkach naruszenia ochrony danych, utrudnia to pracę organom ścigania, które w trakcie prowadzonych działań mają ograniczony dostęp do informacji.



Wykres 1. Podstawowe źródła zagrożeń dla systemów informatycznych

Źródło: Opracowanie własne na podstawie: J. Grzywacz, *Bankowość elektroniczna w przedsiębiorstwie*, SGH, Warszawa 2016. Dane Komendy Głównej Policji.

Okazuje się, iż podstawowym źródłem zagrożeń systemów informatycznych w 50% są pomyłki ludzi. Szczegółowe informacje przedstawiono na wykresie nr 1.

6. Zabezpieczenia systemów informatycznych

Według J. Grzywacza właściwie eksploatowany system zabezpieczeń spełnia m.in. następujące zadania:

- zabezpieczenie przed naruszeniem tajności danych,
- uniemożliwia dokonywanie transakcji na rachunkach przez osoby niepowołane,
- ochrania składane zlecenia przed zniekształceniem w trakcie transakcji, gwarantuje integralność danych przesyłanych przez sieć,
- uniemożliwia wyparcie się przez klienta dokonanych transakcji, a także zapewnia autentyczność podmiotów, co oznacza możliwość weryfikacji uprawnień klienta do korzystania z konta,
- gwarantuje dostępność autoryzowanych podmiotów biorących bezpośredni lub pośredni udział w transakcji elektronicznej w danym czasie,
- umożliwia kontrolę działań w systemie przez użytkowników,
- zabezpiecza przed zablokowaniem usługi, polegającym na zaburzeniu toku pracy użytkownika, np. przez wirusy komputerowe.

7. Bankowość mobilna i bankowość terminalowa jako przykład usługi zagrożonej elektronicznie bezpieczeństwem w opinii klientów banków spółdzielczych – badania własne

Rozwój bankowości elektronicznej 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. [Górnisiewicz, Obczyński, Pstruś, 2014, s.5].

Podczas badania ankietowego respondenci wypowiedzieli się na temat zagrożenia bezpieczeństwa przeprowadzanych transakcji w bankowości mobilnej (tabela 2).

Tabela 2. Zagrożenie bezpieczeństwa transakcji w bankowości mobilnej a przynależność do grupy społeczno – zawodowej

| Wyszczególnienie | | Grupa społeczno – zawodowa | | | | | | | Ogółem |
|------------------|---|----------------------------|-------------|------------|--------|--------------------|-------------|-------|--------|
| | | urzędnik | wolny zawód | nauczyciel | rolnik | pracownik fizyczny | rzemieślnik | inny | |
| Nie | N | 13 | 3 | 4 | 19 | 17 | 6 | 7 | 69 |
| | % | 72,2% | 25% | 57,1% | 86,4% | 70,8% | 100% | 77,8% | 70,4% |
| Tak | N | 5 | 9 | 3 | 3 | 7 | 0 | 2 | 29 |
| | % | 27,8% | 75% | 42,9% | 13,6% | 29,2% | 0,0% | 22,2% | 29,6% |
| Ogółem | N | 18 | 12 | 7 | 22 | 24 | 6 | 9 | 98 |
| | % | 18,37% | 12,24% | 7,14% | 22,45% | 24,49% | 6,12% | 9,18% | 100% |

Źródło: Opracowanie własne w oparciu o przeprowadzone badania ankietowe.

Tabela 2a. Test 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 $p < 0,05$

Źródło: Opracowanie własne.

Pomiędzy zmiennymi wykazano istotną zależność, co oznacza, że pomiędzy przynależnością do grupy społeczno- zawodowej, a zagrożeniem bezpieczeństwa transakcji w bankowości mobilnej występuje istotna zależność. Najczęściej rolnicy - 86,4% oraz rzemieślnicy 100% wskazywali brak zagrożenia bezpieczeństwa transakcji w bankowości mobilnej. Przeciwnego zdania były osoby wykonujące wolny zawód – 75%.

Ponadto respondenci wypowiedzieli się na temat zagrożenia bezpieczeństwa przeprowadzanych transakcji w bankowości terminalowej (tabela 3).

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% |

| Wyszczególnienie | Przynależność do grupy społeczno-zawodowej | | | | | | | Ogółem | |
|------------------|--|-------------|------------|--------|--------------------|-------------|------|--------|------|
| | urzędnik | Wolny zawód | nauczyciel | rolnik | Pracownik fizyczny | rzemieślnik | inny | | |
| 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% |

Źródło: Opracowanie własne w oparciu o przeprowadzone badania ankietowe.

Tabela 3a. 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 $p < 0,05$

Źródło: Opracowanie własne.

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 urzędnicy (21,3%). Przeciwnego zdania byli najczęściej: pracownicy fizyczni (31,3%) oraz rolnicy (20%). Dosyć 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 płatności, jest wśród specjalistów i techników (30% to płatności kartami) 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].

Zakończenie

Z uwagi na ograniczone zasoby finansowe banki spółdzielcze ponoszą niższe nakłady na obszar IT niż banki komercyjne. Banki spółdzielcze muszą sprostać wymaganiom określonym w rekomendacjach dotyczących bezpieczeństwa transakcji przeprowadzanych przy pomocy elektronicznych kanałów dostępu. Powoduje to racjonalizację wyboru między bezpieczeństwem, a sprawnością działania oraz wygodą w korzystaniu z bankowości elektronicznej przez

klientów. Należy jednak pamiętać, że najważniejszym elementem systemu bezpieczeństwa jest człowiek. Okazuje się, iż podstawowym źródłem zagrożeń systemów informatycznych w 50% są pomyłki ludzi.

Rozwój bankowości elektronicznej 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.

Przeprowadzone badania pokazały, że przynależność do grupy społeczno-zawodowej miała wpływ na opinię na temat bezpieczeństwa transakcji w bankowości mobilnej, a także terminalowej. Najczęściej rolnicy - 86,4% oraz rzemieślnicy 100% wskazywali brak zagrożenia bezpieczeństwa transakcji w bankowości mobilnej. Przeciwnego zdania były osoby wykonujące wolny zawód – 75%. Wśród osób uważających, że istnieje zagrożenie w bankowości terminalowej najliczniejszą grupę stanowili: rolnicy (25,5%) oraz urzędnicy (21,3%). Przeciwnego zdania byli najczęściej: pracownicy fizyczni (31,3%) oraz rolnicy (20%).

Literatura

Gospodarowicz Andrzej. 2005. *Bankowość elektroniczna*. Warszawa: Polskie Wydawnictwo Ekonomiczne.

Grzywacz Jacek. 2016. *Bankowość elektroniczna w przedsiębiorstwie*. Warszawa: Oficyna Wydawnicza SGH.

Górnisiewicz Mateusz, Obczyński Radosław, Pstruś Mariusz. 2014. *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*. Komisja Nadzoru Bankowego. Warszawa: CEDUR.

Koźliński Tomasz. 2013. *Zwyczaj płac Polaków*. Raport NBP. Warszawa, dostęp online: http://www.nbp.pl/systemplatniczy/zwyczaj_platnicze/zwyczaj_platnicze_Polakow.pdf

[www 1] Raport ZBP, *Bankowość internetowa i płatności bezgotówkowe III kwartał 2015 r.*, dostęp online: http://zbp.pl/public/repozytorium/wydarzenia/images/grudzien_2015/konf/Netbank_Q3_finalna.pdf, dostęp: 06.11.2016.

[www 2] <http://www.czasnafinanse.pl/produkty-finansowe/konta/artykuly/bankowosc-mobilna>, dostęp: 2.02.2017

[www 3] <http://www.wieczestem.us.edu.pl/bankowosc-elektroniczna-bankowosc-mobilna>, dostęp: 27.02.2017