

BANKOWOŚĆ ELEKTRONICZNA W POLSCE – KORZYŚCI ORAZ ZAGROŻENIA

Mateusz Banaszek, Aleksandra Żak*

Abstrakt *E-banking* to powszechna forma korzystania z bankowości przez Polaków. Jej rozwój w Polsce następuje szybko oraz znajduje się na coraz wyższym poziomie. Niestety mimo korzyści wynikających z bankowości elektronicznej, występuje również wiele zagrożeń, które możemy napotkać podczas korzystania z tych usług. Warto się z nimi zapoznać, aby uniknąć w przyszłości rozczarowań wynikających z niewiedzy na temat e-bankingu.

Słowa kluczowe bankowość elektroniczna, korzyści oraz zagrożenia związane z bankowością elektroniczną.

JEL Code G20; G21; G29.

ACCEPTED: 30th March 2017

PUBLISHED: 30th June 2017

WSTĘP

Bankowość elektroniczna jest najszybciej rozwijającym się obszarem bankowości. Bardzo duża konkurencja zobowiązuje banki do ciągłego wprowadzania innowacji i szukania nowych rozwiązań technologicznych. Aby sprostać wymaganiom klientów oraz zwiększyć przewagę wśród konkurentów, elektroniczne kanały dystrybucji usług bankowych są stale rozwijane. Z upływem czasu sposób postrzegania usług bankowości elektronicznej uległ znaczącym zmianom – klienci banków coraz chętniej korzystają z tego typu usług.

W niniejszym artykule zaprezentowano cechy bankowości elektronicznej w Polsce, kanały dystrybucji oraz szanse i zagrożenia jej rozwoju. Na podstawie badania przeprowadzonego na grupie 30 studentów pokazano poziom zainteresowania bankowością elektroniczną wśród młodych osób oraz sprawdzono ich wiedzę na temat zagrożeń z nią związanych.

* Wydział Ekonomiczno-Socjologiczny, Uniwersytet Łódzki.

Celem niniejszej pracy jest zbadanie zainteresowania usługami bankowości elektronicznej wśród młodych osób oraz świadomości zagrożeń z nią związanych. Wstępna analiza problemu pozwoliła na postawienie głównej hipotezy badawczej, która zakłada, że młode osoby chętnie korzystają z usług bankowości elektronicznej i są świadome zagrożeń dotyczących tego rodzaju bankowości.

1. BANKOWOŚĆ ELEKTRONICZNA W POLSCE

W literaturze przedmiotu istnieje wiele różnych definicji bankowości elektronicznej. W najszerszym znaczeniu, terminem tym określa się usługi świadczone przez wykorzystanie dowolnych elektronicznych kanałów dystrybucji produktów bankowych [Adamiec 2009, s. 174].

W Polsce bankowość elektroniczna pojawiła się w 1990 roku – jej pierwszą formą były wówczas bankomaty zainstalowane przez Bank Pekao SA. Od 1993 roku klienci mogą korzystać także z kart płatniczych oraz z usług *home banking*, umożliwiających klientowi komunikację z bankiem za pomocą komputera [Zalewska-Bochenko 2014, s. 187]. W 1998 roku Powszechny Bank Gospodarczy w Łodzi jako pierwszy w Polsce umożliwił klientom dostęp do rachunku bankowego za pomocą Internetu. Dwa lata później powstał pierwszy bank wirtualny – mBank. Od 2000 roku większość banków w Polsce wprowadziła do swojej działalności kanały bankowości elektronicznej [Adamiec 2009].

Obecnie na rynku bankowości elektronicznej dominuje bankowość internetowa oraz rynek kart płatniczych. Z roku na rok można zaobserwować wzrost liczby klientów korzystających z bankowości przez Internet oraz wzrost ich aktywności. Według raportu NetB@nk *Bankowość internetowa i płatności bezgotówkowe* wynika, że liczba klientów indywidualnych, którzy posiadają dostęp do bankowości internetowej, na koniec IV kwartału 2015 roku wynosiła ponad 30 milionów. W porównaniu z IV kwartałem 2014 roku nastąpił wzrost o ponad 5,2 miliona (20,83%). Liczba aktywnych klientów indywidualnych korzystających z bankowości internetowej (logujących się co najmniej raz na miesiąc) na koniec IV kwartału 2015 roku wynosiła 14 milionów i w porównaniu z IV kwartałem 2014 roku wzrosła o 1,5 miliona (11,31%). Jeśli chodzi o karty płatnicze można zaobserwować tendencję spadkową. W IV kwartale 2015 roku liczba kart płatniczych w Polsce wynosiła 35 milionów i w stosunku do roku 2014 spadła o 860 tysięcy (2,38%) [*Bankowość internetowa i płatności bezgotówkowe IV kwartał 2014 r.*, 2014].

Bankowość elektroniczna w Polsce stale się rozwija i obecnie znajduje się na bardzo wysokim poziomie [Borcuch 2014]. W przyszłości banki będą starały się stawiać na bankowość internetową i mobilną. Oprócz możliwości jakie daje postęp technologiczny, niesie on ze sobą również różne zagrożenia, dlatego banki będą musiały także udoskonalić bezpieczeństwo świadczonych usług.

2. KANAŁY DYSTRYBUCJI BANKOWOŚCI ELEKTRONICZNEJ

Postęp technologiczny sprawił, że bankowość tradycyjna stałą się mniej popularna a w jej miejscu pojawiła się bankowość elektroniczna. Można ją podzielić według następujących kanałów dystrybucji [Górka 2006]:

- Bankowość terminalowa – najstarsza i najbardziej powszechna forma bankowości elektronicznej. Zaliczają się do niej bankomaty oraz terminale do akceptowania płatności kartami płatniczymi (POS).

- *Home banking* – forma bankowości polegająca na komunikacji klienta z bankiem przez zainstalowane na komputerze oprogramowanie. Obecnie mniej popularna forma ze względu na upowszechnienie bankowości internetowej.

- Bankowość telefoniczna – usługi bankowe dostępne za pomocą telefonu komórkowego lub stacjonarnego. Obecnie bankowość telefoniczna jest kojarzona jako rozmowa z konsultantem, natomiast usługi bankowe dostępne na telefon komórkowy określane są mianem bankowości mobilnej.

- Elektroniczne instrumenty płatnicze – karty płatnicze i pieniądz elektroniczny.

- Bankowość internetowa – obecnie jedna z najpopularniejszych form bankowości elektronicznej. Pozwala na dokonywanie operacji bankowych przez Internet.

Bardzo szybki rozwój technologii telekomunikacyjnych i informatycznych oraz wzrost liczby użytkowników tych technologii sprawił, że bankowość mobilna i internetowa są najbardziej perspektywnymi kanałami dystrybucji usług bankowych. Dzięki nim klienci mogą szybko i sprawnie dokonywać płatności w każdym miejscu i czasie. Rosnąca popularność telefonów komórkowych sprawia, że klienci coraz chętniej korzystają z bankowych aplikacji mobilnych [Garczyński 2015]. Przedstawiciele sektora bankowego zakładają, że rosnąca liczba smartfonów znacznie wpłynie na rozwój m-bankingu (bankowości mobilnej) w Polsce [Kuchciak 2012].

3. KORZYŚCI ZWIĄZANE Z BANKOWOŚCIĄ ELEKTRONICZNĄ

Charakterystyczną cechą *e-bankingu* jest możliwość obsługi klienta danego banku zarówno w dowolnym czasie jak i miejscu, w którym można połączyć się z siecią oraz na dowolnym urządzeniu posiadającym opcję korzystania z Internetu [*E-banking*, 2000].

Zarówno bank jak i jego klienci korzystający z bankowości elektronicznej mogą liczyć na szereg korzyści wynikających z używania tej formy usług bankowych¹.

Patrząc na zalety korzystania z bankowości elektronicznej od strony klienta, wyróżnić można przede wszystkim: ułatwienie dostępu do usług bankowych za pomocą np. telefonu komórkowego bądź poczty elektronicznej, wygodę – możliwość sprawdzenia np. stanu rachunku w dowolnym miejscu oraz czasie (dostęp 24 godziny 7 dni w tygodniu) oraz wykluczenie zagrożeń związanych z korzystaniem z bankowości tradycyjnej: np. kradzież gotówki.

Inne korzyści dla klientów banku to także: niższe koszty prowadzenia rachunku (np. opłata za wykonywanie przelewów jest kilkukrotnie niższa, jeśli jest wykonana przez Internet niż w banku), szybsza realizacja zadań, zniwelowanie ilości wypełnianych dokumentów, atrakcyjne oprocentowanie, dostęp do aktualnej oferty banku.

Podstawowe zalety bankowości elektronicznej dla banku to: zniwelowanie zagrożeń powstających podczas korzystania z bankowości tradycyjnej, np. fałszerstwo dokumentów; rozszerzenie obszaru, na którym działa bank – bez konieczności tworzenia placówek fizycznych oraz skrócenie czasu potrzebnego do obsługi klienta – wiele operacji wykonywanych jest w trybie samoobsługowym [Janczyk-Strzała 2011].

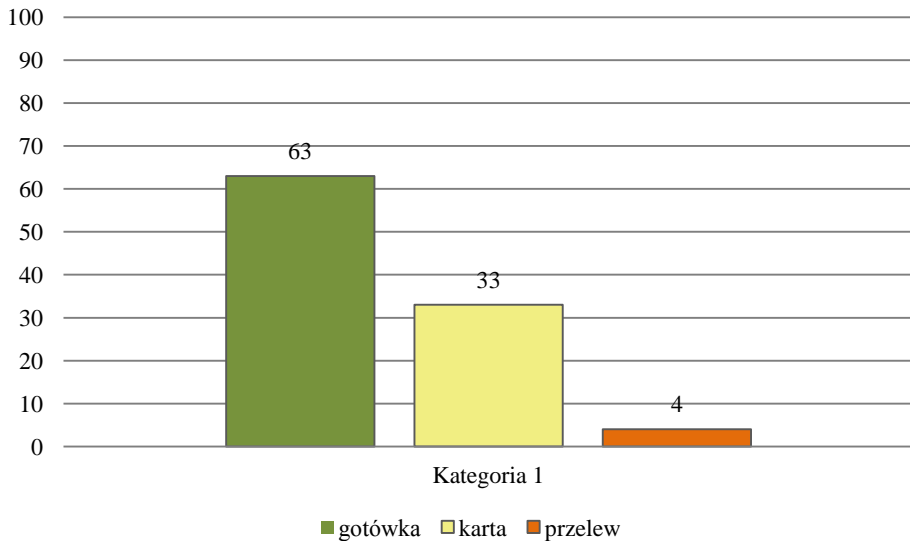
Ważną kwestią, którą należy rozpatrzyć podczas analizy korzyści dla banku to – koszty. Zaletą bankowości elektronicznej są mniejsze koszty utrzymania serwisu transakcyjnego banku niż tworzenia oraz utrzymania placówek a także niski poziom kosztów zmiennych ze względu na niewielką ilość zatrudnionych pracowników.

Niestety mimo wielu korzyści, istnieją również wady korzystania z usług bankowości elektronicznej.

4. ZAGROŻENIA ZWIĄZANE Z KORZYSTANIEM Z BANKOWOŚCI ELEKTRONICZNEJ ORAZ METODY ICH ZAPOBIEGANIA

Polska to jeden z krajów najlepiej rozwiniętych w sektorze bankowym, pomimo tego Polacy płacąc w sklepach posługują się głównie gotówką – a nie kartą czy też innymi aplikacjami umożliwiającymi zapłatę za zakupione produkty [Badanie Polaków nt. korzystania z usług bankowych i płatności 2016, 2017]. Badania przeprowadzone na 970 osobach dorosłych pokazały, że w 2016 r., 63% respondentów płaciło gotówką, 33% – kartą a 4% – przelewem (rys. 1).

¹ Opracowanie własne na podstawie korzystania z usług bankowości elektronicznej.



Rys. 1 Sposoby płatności Polaków za produkty w sklepach

Źródło: opracowanie własne na podstawie: *Wybrane wyniki badania Polaków nt. korzystania z usług bankowych i płatności 2016*.

Wyniki te mogą świadczyć o tym, że Polacy boją się zagrożeń płynących z korzystania z usług bankowości elektronicznej.

Bankowość elektroniczna posiada zarówno zalety – korzyści, jak i wady – zagrożenia. Jednym z najgroźniejszych jest ryzyko związane z korzystaniem z w/w usług. Podstawowe rodzaje ryzyka dla banku związane z bankowością elektroniczną to: ryzyko operacyjne, ryzyko prawne oraz ryzyko utraty reputacji banku [Górka 2006].

Ryzyko operacyjne w postaci wirusów, koni trojańskich a także jako czynnik ludzki: pracownicy banku, administratorzy sieci czy też dostawcy technologii.

Ryzyko prawne występuje zwłaszcza wtedy, gdy przepisy prawne, które były skonstruowane w odniesieniu do tradycyjnej bankowości, różnią się od regulacji dotyczących bankowości elektronicznej. Dotyczy również postawy banku, który również powinien zachować poufny charakter danych o jego klientach.

Ryzyko utraty reputacji może występować np. na skutek awarii systemu lub też nieodpowiedniego traktowania klienta (udostępnianie nieodpowiednich dokumentów, regulaminów, nieistotnych informacji).

Kolejne ryzyka o których warto wspomnieć podczas rozważań na temat e-bankingu to: ryzyko manipulacji polegające na tym, że hakerzy łamią zabezpieczenia posługując się np. *snifferami* czyli przechwytyują oni różnego typu dane, m.in. hasła, kody dostępu dzięki czemu przejmują kontrolę nad danymi

klientów; ryzyko prania brudnych pieniędzy; ryzyko słabej wydajności systemu oraz włamań do systemu z zewnątrz.

Istnieje wiele metod zapobiegających ryzykom związanym z korzystaniem z bankowości elektronicznej. Podstawowymi są: instalowanie różnego rodzaju zabezpieczeń, ochrona elektromagnetyczna, szyfrowanie haseł, wydzielanie stref bezpieczeństwa oraz kontrolowanie dostępu użytkowników do urządzeń systemowych. Bardzo często spotykaną metodą jest uwierzytelnianie dostępu poprzez hasła PIN klientów oraz ich identyfikatory, TAN kody a także tokeny. Wraz z rozwojem *e-bankingu* powstaje wiele innowacyjnych sposobów na zabezpieczenie się przed cyberprzestępcami. Jednym z takich rozwiązań jest biometryczna identyfikacja klienta poprzez: linie papilarne, podpis, fotografię, skan dłoni, rozpoznawanie głosu czy też skan oka [Zalewska-Bochenko 2013].

Na ryzyko w bankowości elektronicznej narażeni są także klienci. Zagrożenia związane z korzystaniem z *e-bankingu* przedstawiła Komisja Nadzoru Finansowego (KNF) w *Poradniku klienta usług finansowych [Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną, 2014]*. Są to przede wszystkim: wyłudzenie danych, które pozwala na przeprowadzanie transakcji; kradzież z wykorzystaniem złośliwego oprogramowania; kopiowanie karty płatniczej; kradzież z wykorzystaniem karty z możliwością płatności zbliżeniowych; kradzież z użyciem danych karty płatniczej klienta; niebezpieczeństwa związane z korzystaniem z aplikacji mobilnych; kradzież tożsamości klienta; tzw. „oszustwa nigeryjskie”; kradzież w sklepie internetowym.

KNF wymienia również przestępstwa związane z *e-bankingiem*, które mają swoje uregulowania w polskim prawie:

1. *Hacking* – nieuprawnione uzyskiwanie dostępu do wszelakich danych w wyniku przełamania systemów zabezpieczających.

2. *Spoofing* – przejęcie kontroli nad komputerami innych użytkowników bankowości elektronicznej w celu wykorzystania go do działań wykraczających poza poprawne normy prawne.

3. *Sniffing* – przechwycenie informacji przekazywanych w sieciach lokalnych oraz sieciach *WiFi* w celu uzyskiwania danych klientów banków do późniejszego bezprawnego ich wykorzystywania.

4. Zakładanie na bankomatach urządzeń, które mają na celu zebranie danych z karty płatniczej – część *skimmingu*.

5. Wirus komputerowy – program umieszczony w innym programie, który sam się replikuje. W wyniku zadziałania wirusa można np. utracić ważne dane z komputera czy też mieć utrudnioną pracę.

6. Bomba logiczna – rodzaj wirusa. Jego aktywacja występuje w określonym dniu oraz czasie lub też w wyniku wykonania określonej czynności przez użytkownika danego urządzenia.

7. Robak komputerowy – nie niszczy danych, ale może doprowadzić do obciążenia działania niektórych programów komputerowych.

8. Konie trojańskie – tzw. „trojany”. Mogą przechwycić np. hasła dostępowe użytkownika komputera. Uruchamiają się w momencie rozpoczęcia pracy na danym programie komputerowym.

9. *Phishing* – polega na przesłaniu wiadomości pocztą elektroniczną od osób, które podszywają się pod dany bank np. z prośbą o logowanie się na stronie banku w celu wyłudzenia danych o kliencie (np. haseł).

10. *Pharming* – forma *phishingu*. Polega na przekierowaniu użytkownika *e-bankingu* z prawidłowej strony banku na tę utworzoną w celu wyłudzenia danych klienta.

Aby ograniczyć możliwość zaistnienia danego ryzyka/zagrożenia/przestępstwa należy stosować kilka podstawowych zasad [Faroughian 2012]. Jedną z najważniejszych reguł jest to, aby nie podawać swoich danych osobowych ludziom niepowołanym do tej wiedzy a także zachować ostrożność miejsca, w którym to następuje. Ważne jest również, żeby zabezpieczyć swój komputer oraz telefon. Obecnie istnieje wiele programów zabezpieczających, które można użyć do polepszenia bezpieczeństwa urządzeń, z których się korzysta.

Aby nie paść ofiarą cyberprzestępczości powinno się również pamiętać o tym, aby nie otwierać *e-maili* oraz załączników niewiadomego pochodzenia. Nie można także zapomnieć o korzystaniu z sieci *WiFi*, które są odpowiednio zabezpieczone. Logowanie się w sieciach w galeriach handlowych często prowadzi do wyłudzenia od klientów danych osobowych. Utworzenie silnego hasła do konta, które będzie niepowtarzalne również pomoże w ograniczeniu ryzyka dostępu niepowołanych osób do kont bankowych.

Ważne jest również to, aby pamiętać o ustawieniu limitów transakcyjnych na swoich kartach płatniczych. Zniweluje to ewentualne straty pieniężne w razie wystąpienia np. kradzieży karty. Jeśli klient straci kartę płatniczą – powinien ją natychmiast zastrzec. Również korzystając z bankomatu powinno się pamiętać o tym, aby sprawdzić, czy nie zawiera on w sobie dziwnie wyglądających elementów, np. odstających części czy też urządzeń przypominających kamery.

Należy także pamiętać o zachowaniu zdrowego rozsądku oraz kierowaniu się wiedzą na temat finansów. Najważniejsze to przestrzeganie podstawowych zasad bezpieczeństwa w sieci. Należy pamiętać o tym, że jeśli korzysta się z jakiegoś produktu to powinno się najpierw z nim zapoznać. Wiedza na temat jego działania, korzyści oraz zagrożeń z nim związanych to podstawa racjonalnego korzystania z usług nowoczesnej bankowości.

5. BADANIE DOTYCZĄCE WIEDZY STUDENTÓW NA TEMAT ZAGROZEŃ BANKOWOŚCI ELEKTRONICZNEJ

Aby zbadać wiedzę klientów bankowości elektronicznej na temat zagrożeń płynących z korzystania z tego rodzaju usług, przeprowadzono badanie na grupie 30 studentów z różnych kierunków i uczelni. W badaniu, które polegało na wypełnieniu kwestionariusza zawierającego 17 pytań, wzięło udział 23 kobiety i 7 mężczyzn korzystających z bankowości elektronicznej. Poniższe zestawienie przedstawia wyniki badania:

1. Czy jest Pan/Pani studentem/studentką?
Tak: 30
Nie: 0
2. Płeć:
Kobieta: 23
Mężczyzna: 7
3. Nazwa uczelni, na której Pan/Pani studiuje:
Uniwersytet Łódzki: 19
Politechnika Częstochowska: 2
Uniwersytet Przyrodniczy w Poznaniu: 1
Uniwersytet Ekonomiczny w Poznaniu: 1
Politechnika Wrocławska: 2
Uniwersytet Jagielloński: 2
Uniwersytet Warszawski: 3
4. Kierunek jaki Pan/Pani studiuje:
Finanse i rachunkowość: 14
Automatyka i robotyka: 1
Architektura: 1
Medycyna: 1
Inżynieria środowiska: 1
Analiza i zarządzanie w biznesie: 1
Pedagogika: 3
Ekonomia: 1
Bezpieczeństwo narodowe: 1
Prawo podatkowe: 3
Elektrotechnika: 1
Mechanika i budowa maszyn: 1
Studia bliskowschodnie: 1

5. Rok studiów:
Pierwszy: 5
Drugi: 1
Trzeci: 4
Czwarty: 19
Piąty: 1
6. Miejsce stałego zamieszkania:
Wieś: 12
Miasto<10 tys: 0
Miasto 10 tys. – 100 tys: 7
Miasto 100 tys. – 500 tys.: 3
Miasto>500 tys.: 8
7. Czy korzysta Pan/Pani z bankowości elektronicznej?
Tak: 30
Nie: 0
8. Z jakich kanałów dystrybucji bankowości elektronicznej Pan/Pani korzysta i jak często?
Bankowość telefoniczna (telefon stacjonarny – infolinia/IVR)
Kilka razy w tygodniu: 1
Rzadziej niż raz w tygodniu: 2
Nie korzystam: 27
Bankowość mobilna (telefon komórkowy – aplikacje, SMS banking, WAP/SIM Toolkit)
codziennie: 5
kilka razy w tygodniu: 11
raz w tygodniu: 2
raz w miesiącu: 5
rzadziej niż raz w miesiącu: 2
nie korzystam: 5
Komputer z dostępem do Internetu
codziennie: 7
kilka razy w tygodniu: 8
raz w tygodniu: 8
raz w miesiącu: 5
rzadziej niż raz w miesiącu: 1
nie korzystam: 1
Home banking (komputer z oprogramowaniem bankowym bez użycia Internetu)
Nie korzystam: 30
Bankomat/wpłatomat
Kilka razy w tygodniu: 7

Raz w tygodniu: 8
Raz w miesiącu: 7
Rzadziej niż raz w miesiącu: 7
Nie korzystam: 1
Płatności kartą
codziennie: 9
kilka razy w tygodniu: 19
raz w tygodniu: 2
9. Czego boi się Pan/Pani podczas korzystania z bankowości elektronicznej?
Włamania na konto: 17
Kradzieży danych osobowych: 13
Kradzieży loginu i hasła: 12
Wirusów: 11
Fałszywych stron banku: 16
Niczego: 5
Innych zagrożeń (jakich?): 0
10 Jak ocenia Pan/Pani swoją wiedzę na temat zagrożeń bankowości elektronicznej?
Bardzo dobra: 2
Dobra: 14
Przeciętna: 11
Słaba: 3
Bardzo słaba: 0
11. Proszę zaznaczyć znane Panu/Pani zagrożenia bankowości elektronicznej
Konie trojańskie: 26
Robaki komputerowe: 15
Bomby logiczne: 6
Wirusy komputerowe: 26
Phishing: 16
Pharming: 5
Skimming: 12
Sniffing: 7
Spoofing: 6
Hacking: 24
Nie znam żadnego z wymienionych: 0
12. Czy kiedykolwiek miał Pan/Pani osobiście styczność z którymś z tych zagrożeń?
Nie: 27
Tak: 3

13. Czy uważa Pan/Pani, że bankowość tradycyjna jest bezpieczniejsza od bankowości elektronicznej?
Zdecydowanie tak: 1
Raczej tak: 8
Nie mam zdania: 13
Raczej nie: 7
Zdecydowanie nie: 1
14. Z jakimi formami zabezpieczeń bankowości elektronicznej Pan/Pani się spotkał/spotkała?
Token: 13
Kod TAN: 5
Login/hasło: 30
Powiadomienie SMS: 30
Podpis elektroniczny: 15
Autoryzacja liniami papilarnymi, skanem oka lub dłoni: 5
Żadne z wymienionych: 0
Inne (jakie?): 0
15. Jak ocenia Pan/Pani cechy bankowości elektronicznej w skali od 1 do 5 (1 – najslabiej, 5 – najlepiej)?
Wygoda: 1 (0 os.), 2 (0 os.), 3 (1 os.), 4 (1 os.), 5 (28 os.)
Bezpieczeństwo: 1 (1 os.), 2 (1 os.), 3 (14 os.), 4 (14 os.), 5 (0 os.)
Koszty usług: 1 (0 os.), 2 (2 os.), 3 (6 os.), 4 (9 os.), 5 (13 os.)
Oszczędność czasu: 1 (0 os.), 2 (0 os.), 3 (0 os.), 4 (5 os.), 5 (25 os.)
Całodobowy dostęp do usług bankowych: 1 (0 os.), 2 (0 os.), 3 (1 os.), 4 (4 os.), 5 (25 os.)
16. Jakie wady zalicza Pan/Pani do bankowości elektronicznej?
Brak osobistego kontaktu z pracownikiem banku: 10
Brak bezpieczeństwa: 11
Skomplikowana obsługa: 1
Wysokie koszty: 1
Uważam, że bankowość elektroniczna nie ma wad: 10
Inne (jakie?): 1
17. Czy w przyszłości zamierza Pan/Pani korzystać z bankowości elektronicznej?
Tak: 30
Nie: 0
Nie wiem: 0

Wyniki badania pokazały, że respondenci najczęściej korzystali z usług bankowości elektronicznej polegającej na: płatności kartą, bankowości internetowej oraz mobilnej. Tylko 5 osób z trzydziestoosobowej grupy na pytanie „czy boją się podczas korzystania z usług e-bankingu” odpowiedziało, że nie boją się niczego. Pozostałe najczęściej wskazywane obawy użytkowników to włama-

nia na konto (56,67%), fałszywe strony banku (53,33%) oraz kradzież danych osobowych (43,33%).

Zaledwie 2 osoby opowiedziały, że ich wiedza na temat zagrożeń bankowości elektronicznej jest bardzo dobra, 14 osób twierdzi, że ich wiedza jest dobra, 11 osób ma przeciętny poziom wiedzy na ten temat a 3 osoby mają słabą wiedzę w tym zakresie.

Na pytanie o znane respondentom zagrożenia, najczęściej wskazywanymi z wymienionych były: konie trojańskie i wirusy komputerowe (86,67%), *hacking* (80%) oraz *skimming* (40%). Aż 90% studentów nigdy nie miało styczności z żadnym z tych zagrożeń, natomiast 3 osoby padły ofiarą wirusów komputerowych oraz *phishingu*.

Na pytanie czy bankowość tradycyjna jest bezpieczniejsza od bankowości elektronicznej odpowiedzi rozłożyły się równomiernie. Prawie połowa (43,33%) z odpowiadających nie ma zdania na ten temat, a pozostała część jest podzielona pomiędzy odpowiedziami za bezpieczeństwem bankowości tradycyjnej oraz przeciw niej.

Jeśli chodzi o zabezpieczenia używane w *e-bankingu* wszyscy z odpowiadających potwierdzili znajomość powiadomienia SMS oraz stosowanie login/hasła. Połowa z nich słyszała również o podpisie elektronicznym, 43,33% o *tokenach* a 16,67% o kodach TAN i autoryzacji linii papilarnych.

Użytkownicy *e-bankingu* najbardziej cenią sobie wygodę (93,33%), oszczędność czasu (83,33%) oraz całodobowy dostęp do usług bankowych (83,33%). Wskazywane przez nich wady tej bankowości to brak bezpieczeństwa (36,67%) oraz brak osobistego kontaktu z pracownikiem banku (33,33). Aż jedna trzecia z ankietowanych twierdzi, że bankowość elektroniczna nie ma żadnych wad. Wszyscy respondenci wskazali, że w przyszłości zamierzają korzystać z usług bankowości elektronicznej.

Z badania wynika, że każdy ze studentów znał co najmniej kilka zagrożeń dotyczących *e-bankingu*. Mimo, że 10% z nich miało styczność z zagrożeniami, to oceniają oni bankowość elektroniczną pozytywnie i zamierzają nadal z niej korzystać.

ZAKOŃCZENIE

Bankowość elektroniczna w obecnych czasach cieszy się bardzo dużą popularnością [Szpringer 2002]. Ludzie coraz częściej odchodzą od usług bankowości tradycyjnej na rzecz usług *e-bankingu*. W świecie stale rozwijającej się technologii, banki muszą także pracować nad coraz bardziej innowacyjnymi rozwiązaniami obsługi klientów, ponieważ są oni coraz bardziej wymagający, jeśli chodzi o jakość usług. Jednocześnie cenią sobie wygodę oraz łatwość korzysta-

nia z nowych produktów. Obecnie większość osób posiada komputer lub telefon z dostępem do Internetu, co sprzyja rozwojowi bankowości internetowej i mobilnej. Niestety wraz z postępem technologicznym powstają nowe zagrożenia. Banki wprowadzając coraz nowsze rozwiązania, będą musiały także pamiętać o zapewnieniu swoim klientom bezpieczeństwa. Jeśli tego nie zrobią, konsumenci mogą przestać korzystać z ich usług [Chu 2012].

Wprowadzenie usług bankowości elektronicznej przyczyni się w przyszłości do zmniejszenia kosztów działalności banku, ale wiąże się to także z redukcją zatrudnienia. W wyniku postępu technologicznego, rola oddziałów bankowych zmieni się. Miejsca, w których można było dokonywać transakcji, staną się oddziałami doradczymi. Będą one niewielkie a ich liczba ulegnie zmniejszeniu, ale nadal będą pełnić istotną rolę jako punkty bezpośredniego kontaktu klienta z bankiem [Świtecka 2001]. Mimo wielu zwolenników *e-bankingu* nadal wiele osób uważa, że to bankowość tradycyjna jest bezpieczniejszą formą gospodarowania swoimi zasobami pieniężnymi, dlatego też oddziały bankowe mimo mniejszej liczebności, nadal będą funkcjonowały w sektorze finansowym.

Reasumując, bankowość elektroniczna posiada zarówno wiele zalet jak i zagrożeń wiążących się z jej korzystaniem. Opierając się na badaniach przeprowadzonych na potrzeby opracowania niniejszego artykułu można wywnioskować, że usługi bankowości elektronicznej nadal będą się rozwijały oraz zyskiwały coraz więcej zwolenników. Podstawą do osiągnięcia dobrych wyników z dziedziny *e-bankingu* jest kontrola tych usług przez bank. Jeśli bank będzie skrupulatnie przykładał uwagę do niwelowania ryzyka związanego z korzystaniem z owych usług to bankowość elektroniczna będzie zajmowała coraz ważniejszą rolę w funkcjonowaniu banków.

BIBLIOGRAFIA

Książki:

- Borcuch A., 2014, *Bankowość elektroniczna w Polsce*, CeDeWu.
Szpringer W., 2002, *E-commerce, e-banking: wyzwania globalizacji*, Difin.

Artykuły:

- Adamiec J., 2009, *Bankowość elektroniczna*, [w:] D. Grodzka (red.), *Spółeczeństwo informacyjne*, „Studia BAS”, nr 3(19).
Chu, 2012, *Service quality, customer satisfaction, customer trust, and loyalty in an e-banking context*, „Social Behavior and Personality” [0301-2212], vol. 40.
E-banking, 2000, „Financial Executive” [0895-4186] Anonymous, vol. 16.
Faroughian F., 2012, *Value and risk in business – to – business e-banking*, „Industrial Marketing Management” [0019-8501], vol. 41.
Garczyński D., 2015, *Technologiczne aspekty ryzyka operacyjnego w bankach*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace”, nr 3, t. 2, „Bankowość. Bankowość komercyjna i spółdzielcza”.

- Górka J. H., 2006, *Specyfika ryzyka bankowości elektronicznej*, Materiały i Studia – Zeszyt nr 205, Warszawa, kwiecień.
- Janczyk-Strzała E., 2011, *Rozwój i przyszłość bankowości elektronicznej w Polsce*, Zeszyt Naukowy nr 25, Wyższa Szkoła Bankowa we Wrocławiu.
- Kuchciak I., 2012, *Mobilna bankowość jako nowoczesny kanał dystrybucji usług bankowych*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio H”, Oeconomia 46/4.
- Świtecka B., 2001, *Bankowość elektroniczna – implikacje dla rozwoju sektora bankowego w Polsce*, [w:] G. W. Kołodko, „Nowa gospodarka” i jej implikacje dla długookresowego wzrostu w krajach posocjalistycznych, Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. Leona Koźmińskiego, Warszawa.
- Zalewska-Bochenko A., 2014, *Rozwój bankowości elektronicznej w Polsce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego”, nr 798.
- Zalewska-Bochenko A., 2013, *Zabezpieczenie bankowych usług internetowych w Polsce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego”, nr 797.

Raporty:

Badanie Polaków nt. korzystania z usług bankowych i płatności 2016, 2017, NBP, Styczeń.

Bankowość internetowa i płatności bezgotówkowe IV kwartał 2014 r., 2014, NetB@nk.

Bezpieczeństwo Finansowe w Bankowości Elektronicznej – Przestępstwa Finansowe Związane z Bankowością Elektroniczną – Poradnik Klienta Usług Finansowych, 2014, KNF, Warszawa.

Wybrane wyniki badania Polaków nt. korzystania z usług bankowych i płatności 2016, NBP.

E-BANKING IN POLAND – BENEFITS AND THREATS

Abstract E-banking is a common form of using banking by Poles. Its development in Poland is fast and now it is at an ever higher level. Unfortunately, despite the benefits of electronic banking, there are also many risks that we may encounter when during using these services. It is worth getting acquainted with them in order to avoid future disappointments resulting from ignorance about e-banking.

Keywords e-banking, benefits and threats related to e-banking.