

**USŁUGI BANKOWOŚCI ELEKTRONICZNEJ
DLA KLIENTÓW DETALICZNYCH
CHARAKTERYSTYKA I ZAGROŻENIA**

AUTORZY:

Grażyna Szwajkowska

Piotr Kwaśniewski

Kamil Leżoń

Filip Woźniczka

WSTĘP

Raport przeznaczony jest dla szerokiego grona odbiorców, korzystających lub planujących korzystać z usług bankowości elektronicznej. W materiale zebrano informacje charakteryzujące poszczególne rodzaje usług bankowości elektronicznej, standardy bezpieczeństwa tych usług oraz związane z nimi potencjalne zagrożenia dla klientów.

Dynamiczny rozwój bankowości elektronicznej rozpoczął się w Polsce po 2000 roku. W przypadku tego rodzaju usług bezpośredni kontakt klienta z pracownikiem banku może być w znacznym stopniu ograniczony, a klientowi, który nie jest specjalistą w dziedzinie systemów informatycznych, może brakować informacji, pozwalających na sprawne poruszanie się w tym obszarze.

Raport o bankowości elektronicznej stara się wypełnić tę lukę informacyjną, wzmacniając tym samym pozycję klientów detalicznych banków, korzystających z nowych technik dostępu do swoich pieniędzy na rachunkach bankowych.

Na potrzeby Raportu przyjęto podział usług bankowości elektronicznej na 3 rodzaje: bankowość terminalową (karty płatnicze), bankowość internetową i bankowość telefoniczną. W pierwszej części Raportu przedstawiono przepisy prawa dotyczące usług bankowości elektronicznej, opisano poszczególne rodzaje usług i związane z nimi zagrożenia. W drugiej części Raportu przedstawiono stan usług bankowości elektronicznej w Polsce.

Dołączony do Raportu *Przewodnik klienta usług bankowości elektronicznej* zawiera podane w przystępnej formie informacje, wskazówki i podstawowe zasady zachowania bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Raport przedstawia stan prawny na dzień 30 września 2010 r.

SPIS TREŚCI

1. Wprowadzenie do bankowości elektronicznej.....	5
1.1 Definicja i klasyfikacja bankowości elektronicznej.....	5
1.2 Przepisy prawne dotyczące bankowości elektronicznej.....	6
2. Bankowość terminalowa	16
2.1 Charakterystyka bankowości terminalowej	16
2.2 Bezpieczeństwo w bankowości terminalowej.....	19
3. Bankowość internetowa	24
3.1. Charakterystyka bankowości internetowej.....	24
3.2. Charakterystyka usług bankowości internetowej.....	27
3.3. Bezpieczeństwo w bankowości internetowej.....	29
4. Bankowość telefoniczna.....	38
4.1 Charakterystyka bankowości telefonicznej.....	38
4.2 Charakterystyka usług bankowości telefonicznej	39
4.3 Charakterystyka usług bankowości mobilnej.....	40
4.4 Bezpieczeństwo w bankowości telefonicznej	43
4.5 Bezpieczeństwo w bankowości mobilnej.....	44
5. Obecny stan świadczenia usług bankowości elektronicznej w Polsce.....	48
5.1 Bankowość terminalowa	48
5.2 Bankowość internetowa	62
5.3 Bankowość telefoniczna.....	72
PODSUMOWANIE	78

1. Wprowadzenie do bankowości elektronicznej

1.1 Definicja i klasyfikacja bankowości elektronicznej

Świadczenie usługi drogą elektroniczną¹ jest definiowane jako wykonanie usługi bez jednoczesnej obecności stron (czyli na odległość) poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej².

Z kolei termin *bankowość elektroniczna* (ang. e-banking) oznacza usługi świadczone drogą elektroniczną przez banki dla klientów detalicznych.

Bankowość elektroniczna (e-banking) jest formą usług, polegającą na umożliwieniu uprawnionego dostępu do rachunku bankowego za pomocą urządzenia elektronicznego: komputera, bankomatu, telefonu, terminalu i linii telekomunikacyjnych³.

W zależności od umowy zawartej przez klienta z bankiem bankowość elektroniczna umożliwia wykonywanie operacji pasywnych (tylko pozyskiwanie informacji np. sprawdzanie salda i historii rachunku, itp.) lub też aktywnych (wykonywanie operacji, np. dokonanie płatności czy też polecenia przelewu, założenie lokaty terminowej, itp.).

Podstawowymi elementami zapewniającymi funkcjonowanie systemu bankowości elektronicznej są:

- sprzęt (hardware),
- oprogramowanie (software),
- systemy transmisji/przekazu,
- użytkownicy.

Podstawową cechą bankowości elektronicznej jest wykorzystywanie sieci telekomunikacyjnej w celu świadczenia usług bankowych. Do powszechnie dostępnych kanałów komunikacji klienta z bankiem należą sieci „zamknięte” i „otwarte”. Sieci zamknięte ograniczają dostęp uczestników (instytucje finansowe, klienci, sprzedawcy i inni dostawcy usług), który wyznaczony jest zakresem umowy członkowskiej. W przypadku sieci otwartych (Internet) takie ograniczenia nie występują.

¹ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

² W rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.

³ W opracowaniu tym pominięto dostęp do rachunku bankowego z wykorzystaniem telewizyjnej platformy cyfrowej.

Usługi bankowości elektronicznej można podzielić na 3 rodzaje:

- bankowość terminalową (operacje dokonywane za pomocą kart płatniczych),
- bankowość internetową (operacje wykonywane za pomocą sieci Internet),
- bankowość telefoniczną (operacje wykonywane przy użyciu telefonów stacjonarnych oraz komórkowych).

1.2 Przepisy prawne dotyczące bankowości elektronicznej

Ogólne przepisy prawa

Działalność banków reguluje przede wszystkim *ustawa Prawo bankowe z dnia 29 sierpnia 1997 r.* (Dz. U. z 2002 r. Nr 72 poz. 665 z późn. zm.). Banki w Polsce działają w formie spółek akcyjnych - zgodnie z *ustawą z dnia 15 września 2000 Kodeks spółek handlowych* (Dz. U. z 2000 r. Nr 94 poz. 1037 z późn. zm.) lub w formie spółdzielni - zgodnie z *ustawą z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających* (Dz. U. z 2000 r. Nr 119 poz. 1252 z późn. zm.). Banki mogą też być tworzone jako banki państwowe. Poza bankami, usługi bankowe dla klientów mogą świadczyć również oddziały instytucji kredytowych funkcjonujące w strukturach organizacyjnych banków UE oraz oddziały banków zagranicznych (banki spoza UE). Banki i oddziały prowadzą rachunki bankowe klientów i mają obowiązek dochowania szczególnej staranności w zakresie zapewnienia bezpieczeństwa środków pieniężnych przechowywanych na rachunkach pieniężnych. Rozliczenia pieniężne przeprowadza się gotówkowo lub bezgotówkowo za pomocą papierowych lub informatycznych nośników danych. Rozliczenia bezgotówkowe przeprowadza się w szczególności kartami płatniczymi.

Relacje pomiędzy klientem banku i bankiem w zakresie usług bankowości elektronicznej reguluje *ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych*⁴ (Dz. U. z 2002 r. Nr 169 poz. 1385 z późn. zm.), *ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz. U. z 2002 r. Nr 144 poz. 1204 z późn. zm.), jednak podstawowym dokumentem jest umowa o prowadzenie rachunku i umowa o usługi bankowości elektronicznej/ umowa o kartę płatniczą, zawarte między klientem a bankiem, które określają sposób dostępu klienta do jego środków na rachunku bankowym. Informacje ogólne dla klientów – czyli te, które nie wymagają zgody klienta potwierdzonej podpisem - zwykle zawarte są w regulaminach banku. Z ustawy o eip wynikają określone obowiązki dla banków oraz dla ich klientów.

⁴ Dalej nazywana w skrócie ustawą o eip.

Obowiązki i odpowiedzialność banku

Elektronicznym instrumentem płatniczym (eip) jest każdy instrument płatniczy, w tym z dostępem do środków pieniężnych na odległość, umożliwiający danej osobie – na podstawie zawartej umowy – dokonywanie operacji przy użyciu informatycznych nośników danych lub elektroniczną identyfikację tej osoby. Najpowszechniejszym eip są karty płatnicze.

Przez zawarcie umowy o usługi bankowości elektronicznej bank zobowiązuje się do zapewnienia klientowi - za pośrednictwem urządzeń łączności przewodowej lub bezprzewodowej (bankomat, POS, komputer, telefon) - dostępu do jego środków na rachunku (lub udostępnionego kredytu w przypadku kart kredytowych) i do wykonywania operacji (lub innych czynności zleconych) na rachunku. Umowa nie może zawierać mniej korzystnych zapisów dla klienta, w porównaniu z przepisami ustawy o eip.

Umowa zawarta w formie pisemnej powinna określać (art. 3 oraz art. 30 ustawy o eip):

1. strony umowy (tj. bank i klient),
2. rodzaj udostępnianego elektronicznego instrumentu płatniczego i urządzeń, z których może korzystać posiadacz, dokonując operacji przy użyciu tego instrumentu (np. karta płatnicza, Internet, telefon),
3. rodzaje operacji, których można dokonywać przy użyciu elektronicznego instrumentu płatniczego,
4. terminy wykonywania przez wydawcę zleceń posiadacza,
5. określenie ograniczeń w dokonywaniu operacji, jeżeli umowa je przewiduje,
6. terminy wykonywania przez posiadacza zobowiązań z tytułu operacji dokonanych przy użyciu elektronicznego instrumentu płatniczego oraz z tytułu należnych wydawcy opłat i prowizji lub spłaty należności,
7. rodzaj i wysokość opłat i prowizji oraz warunki ich zmian,
8. zasady rozliczeń z tytułu operacji w walutach obcych oraz wskazanie stosowanych kursów walut,
9. zasady obliczania odsetek,
10. zasady, tryb i terminy składania oraz rozpatrywania reklamacji,
11. okres, na jaki została zawarta umowa, i warunki jej przedłużania,
12. sposób, termin i ważne powody wypowiedzenia warunków umowy przez wydawcę (nie może być krótszy niż miesiąc),

13. sposób postępowania w przypadku utraty elektronicznego instrumentu płatniczego,
14. zasady elektronicznej identyfikacji klienta,
15. zasady postępowania klienta w związku ze zleceniem dokonywania operacji oraz korzystania z innych usług określonych w umowie.

Do umowy dołącza się wzór podpisu klienta, jeżeli posługiwanie się instrumentem płatniczym (np. kartą płatniczą) wymaga użycia podpisu klienta.

Wydawca elektronicznego instrumentu płatniczego (bank) obowiązany jest ogłaszać w miejscu prowadzenia działalności lub przy użyciu innych środków publicznego komunikowania, w sposób ogólnie dostępny:

- stosowane stawki oprocentowania,
- wysokość pobieranych opłat i prowizji.

Klient banku powinien bezwzględnie przeczytać umowę i sprawdzić, czy zawiera wszystkie wymienione powyżej elementy. Można poprosić pracownika banku, aby wskazał, w którym miejscu umowy znajdują się odpowiednie informacje. Zapisy umowy są szczególnie ważne w sytuacji, gdyby klient składał reklamację i występował z roszczeniami wobec banku (należy pamiętać, że roszczenia te przedawniają się z upływem 2 lat).

Ustawa o eip określa też zasady wydawania i używania kart płatniczych.

Zgodnie z art. 3 ust. 1 ustawy o eip umowa o kartę płatniczą zawierana jest w formie pisemnej, natomiast art. 78 § 2 Kodeksu cywilnego dopuszcza zawarcie takiej umowy w formie elektronicznej, jeżeli umowa opatrzona jest bezpiecznym podpisem elektronicznym, weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu.

Wydanie karty następuje po zawarciu umowy o kartę płatniczą. Do chwili jej wydania wydawca ponosi odpowiedzialność za szkodę wynikającą z użycia karty przez osobę nieuprawnioną. Bank nie ma prawa wydawać klientowi karty, jeżeli klient nie zawarł z bankiem umowy o kartę płatniczą, a tym bardziej obciążać klienta jakimikolwiek kosztami.

Bank wydający kartę płatniczą zobowiązuje się wobec jej posiadacza (klienta banku) do rozliczania operacji, dokonanych przy użyciu karty, a posiadacz zobowiązuje się do zapłaty kwot operacji wraz z należnymi wydawcy kwotami opłat i prowizji lub do spłaty swoich zobowiązań na rachunek wskazany przez wydawcę. Należy pamiętać, że właścicielem karty jest jej wydawca czyli bank.

Klient banku może odstąpić od umowy o kartę płatniczą w terminie 14 dni od dnia otrzymania pierwszej karty płatniczej, o ile nie dokonał żadnej operacji przy użyciu tej karty. W takim przypadku wydawca zwraca posiadaczowi kwotę poniesionych opłat - ale w zakresie przewidzianym w umowie może obciążyć posiadacza kosztami związanymi z wydaniem karty płatniczej. Klient powinien więc zwrócić uwagę, jak sprawę tę reguluje zawierana z bankiem umowa.

Bank może sobie zastrzec w umowie prawo do zmiany, bez zgody posiadacza, limitów i ograniczeń dotyczących kwot dokonywanych operacji określonych w umowie w przypadku nieterminowej spłaty należności przez posiadacza lub stwierdzenia zagrożenia ich terminowej spłaty. Jeżeli takie zmiany nastąpią, bank musi o tym niezwłocznie poinformować klienta.

Do obowiązków banku należy także:

- poinformowanie klienta o sposobie oznaczenia akceptantów oraz bankomatów i innych miejsc, w których może dokonywać operacji przy użyciu karty płatniczej,
- przyjmowanie przez całą dobę zgłoszeń posiadaczy lub użytkowników kart płatniczych o utracie lub zniszczeniu karty płatniczej (przy wykorzystaniu dostępnych środków komunikowania),
- potwierdzenie przyjęcia zgłoszenia w sposób określony w umowie o kartę płatniczą,
- prowadzenie rejestru zgłoszeń utraty lub zniszczenia karty, zawierającego dane o numerze karty, osobie zgłaszającej, okolicznościach, wraz ze wskazaniem daty, godziny i minuty przyjęcia zgłoszenia,
- udostępnianie posiadaczowi - nie rzadziej niż raz w miesiącu - zestawienia operacji, w sposób i w terminach określonych w umowie o kartę płatniczą,
- wprowadzenie procedury tworzenia i udostępniania kodu identyfikacyjnego, uniemożliwiającej poznanie kodu przez osoby nieuprawnione.

Oferując usługi bankowości elektronicznej bank musi przestrzegać jednej z podstawowych zasad bankowości: obowiązku zapewnienia bezpieczeństwa środków pieniężnych gromadzonych na rachunkach bankowych jego klientów. Obsługa operacji dokonywanych przy wykorzystaniu różnorodnych kart płatniczych, w tym operacji wykonywanych przez Internet, podlega przepisom wynikającym z ustawy o eip. Art. 31 ust. 1 tej ustawy mówi, że „bank, świadcząc usługi na podstawie umowy o usługi bankowości elektronicznej, obowiązany jest do zapewnienia posiadaczowi bezpieczeństwa dokonywania operacji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych”. Przepis ten ma charakter bardzo ogólny i nie określa, jakie rozwiązania

techniczne są właściwe dla zapewnienia bezpieczeństwa operacji dokonywanych m.in. za pomocą kart służących pobieraniu gotówki z bankomatów.

Należy jednakże zaznaczyć, że klient banku za nieuprawnione transakcje dokonane jego kartą płatniczą ponosi przed zastrzeżeniem karty odpowiedzialność do kwoty 150 euro a po jej zastrzeżeniu całkowita odpowiedzialność spoczywa na banku, pod warunkiem, że klient nie zaniedbał swoich obowiązków - ochrony karty i kodów dostępu.

Ustawa o świadczeniu usług drogą elektroniczną również nakłada na usługodawcę – w tym przypadku bank, określone wymogi. Do najważniejszych obowiązków banku należy:

1. zapewnienie klientowi (art. 6) dostępu do aktualnej informacji o:
 - a. szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną,
 - b. funkcji i celu oprogramowania lub danych nie będących składnikiem treści usługi, wprowadzanych przez usługodawcę do systemu teleinformatycznego, którym posługuje się usługobiorca;
2. zapewnienie działania systemu teleinformatycznego, którym się posługuje (art. 7), umożliwiając nieodpłatnie usługobiorcy (gdy wymaga tego właściwość usługi):
 - a. korzystanie przez usługobiorcę z usługi świadczonej drogą elektroniczną, w sposób uniemożliwiający dostęp osób nieuprawnionych do treści przekazu składającego się na tę usługę, w szczególności przy wykorzystaniu technik kryptograficznych odpowiednich dla właściwości świadczonej usługi,
 - b. jednoznaczną identyfikację stron usługi świadczonej drogą elektroniczną oraz potwierdzenie faktu złożenia oświadczeń woli i ich treści, niezbędnych do zawarcia drogą elektroniczną umowy o świadczenie tej usługi, w szczególności przy wykorzystaniu bezpiecznego podpisu elektronicznego w rozumieniu *ustawy z dnia 18 września 2001 r. o podpisie elektronicznym* (Dz. U. Nr 130, poz. 1450 z późn. zm.);
3. zakończenie w każdej chwili, korzystania z usługi świadczonej drogą elektroniczną;
4. określenie regulaminu świadczenia usług drogą elektroniczną i nieodpłatne udostępnienie go klientowi przed zawarciem umowy o świadczenie takich usług. Regulamin ten określa w szczególności:
 - a. rodzaje i zakres usług świadczonych drogą elektroniczną,
 - b. warunki świadczenia usług drogą elektroniczną, w tym:
 - wymagania techniczne niezbędne do współpracy z systemem teleinformatycznym, którym posługuje się usługodawca,

- zakaz dostarczania przez usługobiorcę treści o charakterze bezprawnym,
- c. warunki zawierania i rozwiązywania umów o świadczenie usług drogą elektroniczną,
 - d. tryb postępowania reklamacyjnego.

Banki muszą się też stosować do wymogów technicznych, dotyczących szczególnych zasad postępowania przy przetwarzaniu danych osobowych (w tym kwestie zabezpieczania danych), wynikających z *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz. U. z 2002 r. Nr 101 poz. 926) i *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.09.2004 r. w sprawie sposobu prowadzenia dokumentacji i warunków, jakie powinny spełniać systemy informatyczne wykorzystywane do przetwarzania danych*. Rozporządzenie to nie określa jednak szczegółowych wymogów technicznych dla kart płatniczych.

Bezpieczeństwo operacyjne każdego banku zależy od jakości zastosowanej technologii informatycznej i przyjętych rozwiązań organizacyjnych, a w przypadku styku z otwartymi sieciami zewnętrznymi, jak Internet, jest głównie uwarunkowane poziomem zabezpieczeń technicznych i prawidłowym funkcjonowaniem wewnętrznych mechanizmów kontrolnych. Szczególnie niezawodne środki muszą być stosowane w przypadku zaangażowania się banku w transakcyjną bankowość internetową, gdyż wówczas osoby spoza banku otrzymują dostęp do systemu wewnętrznego banku, co rodzi dodatkowe ryzyko i może stanowić zagrożenie dla bezpieczeństwa działalności i środków pieniężnych gromadzonych na rachunkach bankowych. Z uwagi na fakt, że zagrożenia związane z Internetem podlegają nieustannej „ewolucji”, banki muszą na bieżąco monitorować bezpieczeństwo swojej sieci wewnętrznej i zapobiegać zagrożeniom, wynikającym ze stosowania coraz bardziej zaawansowanych technik o charakterze przestępczym. Ryzyko związane z systemami i sieciami teleinformatycznymi ma zasadniczy wpływ na bezpieczeństwo banku i realizowanych operacji. Zarządzanie tym ryzykiem jest o tyle trudne, że musi być dostosowane do indywidualnej architektury sieci teleinformatycznej i struktury organizacyjnej banku.

Obowiązki i odpowiedzialność klienta banku

Jakość usług bankowości elektronicznej, w tym bankowości internetowej ma bardzo duży wpływ na reputację banku, dlatego banki na bieżąco usprawniają stosowane systemy bezpieczeństwa. Niemniej jednak nie da się w pełni uchronić klienta przed niebezpieczeństwem kradzieży środków pieniężnych z jego konta, jeśli on sam nie będzie stosował się do wszystkich wymaganych w tym zakresie zaleceń.

Klucz do zapewnienia bezpieczeństwa leży nie tylko w technicznych zabezpieczeniach stosowanych przez banki, ale przede wszystkim w odpowiednim podejściu klientów. Klienci mogą w znacznym stopniu ograniczyć wpływ różnego rodzaju zagrożeń pochodzących z sieci Internet, zachowując ostrożność w działaniu, a także aktualizując swoje przeglądarki internetowe oraz instalując odpowiednie zabezpieczenia sprzętowe i programowe (wskazówki dla klientów zawarte są w *Przewodniku klienta usług bankowości elektronicznej*).

Podstawowym obowiązkiem klienta korzystającego z bankowości elektronicznej jest nieujawnianie informacji o działaniu elektronicznego instrumentu płatniczego udostępnionego w ramach umowy o usługi bankowości elektronicznej, gdyż może to spowodować brak skuteczności mechanizmów, zapewniających bezpieczeństwo zlecanych operacji.

Karta płatnicza może być używana wyłącznie przez osobę, której dane identyfikacyjne zostały umieszczone na karcie. Istnieje jednak możliwość określenia w umowie o kartę płatniczą, że karta będzie też używana przez innego użytkownika. Umowa taka musi wówczas określać sposób korzystania z karty przez tego użytkownika.

Na posiadaczu karty ciąży także inne obowiązki, zapewniające bezpieczne korzystanie z tego typu instrumentu płatniczego. Są to (art. 16 ustawy o eip):

- przechowywanie karty płatniczej i ochrona kodu identyfikacyjnego, z zachowaniem należytej staranności,
- nieprzechowywanie karty płatniczej razem z kodem identyfikacyjnym,
- niezwłoczne zgłoszenie wydawcy (bankowi) utraty lub zniszczenia karty płatniczej,
- nieudostępnianie karty płatniczej i kodu identyfikacyjnego osobom nieuprawnionym.

Postanowienia te stosuje się także do użytkownika karty płatniczej.

Dla dokonania zapłaty konieczne jest podanie przez posiadacza karty niezbędnych danych:

- nazwa karty,
- numer karty,
- data ważności karty.

Podanie tych danych może rodzić niebezpieczeństwo wykorzystania przekazanych informacji w sposób nieuprawniony (oczywiście jako przestępstwo wiąże się to z odpowiedzialnością karną) – ale jest oczywistym, że bez ich przekazania nie można przeprowadzić transakcji.

W przypadku podejrzenia o dokonaniu nieuprawnionych transakcji klient/posiadacz karty jest obowiązany zgłosić bankowi - w terminie określonym w umowie o kartę płatniczą (który nie może być krótszy niż 14 dni od dnia otrzymania zestawienia) - niezgodność w zestawieniu operacji, dotyczącą w szczególności:

- a. kwestionowanych operacji ujętych w zestawieniu,
- b. błędu lub innych nieprawidłowości w przeprowadzeniu rozliczenia.

Zgłoszenie powinno nastąpić także w razie nieotrzymania zestawienia operacji w ustalonym w umowie terminie.

Generalną zasadą jest nieobciążanie klienta operacjami dokonanymi przy użyciu elektronicznego instrumentu płatniczego, których zlecenia nie potwierdził. Od tej reguły są jednak wyjątki, wskazane w art. 28 i art. 32 ustawy o eip. Zgodnie z nimi klienta obciążają operacje w przypadku:

- ujawniania przez klienta informacji o działaniu elektronicznego instrumentu płatniczego, udostępnionego w ramach umowy o usługi bankowości elektronicznej, których ujawnienie może spowodować brak skuteczności mechanizmów zapewniających bezpieczeństwo zleczonych operacji, jak również operacje dokonane przez osoby, którym udostępnił te informacje (art. 28 ustawy o eip),
- operacje dokonane przez osoby, którym udostępnił kartę płatniczą lub ujawnił kod identyfikacyjny (art. 32 ustawy o eip).

W przypadku utraty karty do czasu zgłoszenia bankowi utraty karty, klienta obciążają operacje dokonane z użyciem utraconej karty płatniczej, do kwoty stanowiącej równowartość w złotych 150 euro według średniego kursu euro ogłaszanego przez NBP, obowiązującego w dniu dokonania zgłoszenia – chyba, że umowa przewiduje inaczej (kwota ta może być niższa, ale nie wyższa). Ograniczenie to nie dotyczy operacji, do których doszło z winy posiadacza lub użytkownika, a w szczególności gdy nie dopełnił on wymienionych powyżej obowiązków określonych w art. 16 ust. 1 lub w art. 27 ust. 1 ustawy o eip. Dodatkowo należy pamiętać, że klient nie może dokonywać modyfikacji karty płatniczej – np. poprzez zamazanie / zdrapanie kodu CVV/CVC.

Klienta obciążają operacje dokonane po zgłoszeniu utraty karty bankowi, jeżeli doszło do nich z winy umyślnej jego lub użytkownika.

Użycie kodu identyfikacyjnego nie wystarcza do obciążenia posiadacza zakwestionowaną przez niego operacją (chyba że został złożony bezpieczny podpis elektroniczny zgodnie z art. 5 ust. 1 *ustawy o podpisie elektronicznym*). Oznacza to, że klienta nie obciążają operacje, jeżeli karta płatnicza została wykorzystana bez fizycznego przedstawienia i elektronicznej identyfikacji posiadacza lub bez złożenia przez niego własnoręcznego podpisu na dokumencie obciążeniowym. Wyjątkiem jest sytuacja, w której umowa o kartę płatniczą przewiduje możliwość dokonywania operacji na odległość.

Posiadacza karty bankowej nie obciążają także operacje dokonane z użyciem utraconej karty płatniczej, jeżeli ich dokonanie nastąpiło wskutek nienależytego wykonania zobowiązania przez wydawcę lub akceptanta.

Postanowienia umowne mniej korzystne dla posiadacza bankowej karty płatniczej są nieważne.

Zgodnie z Art. 14 ustawy o ochronie praw konsumentów konsument (którym jest także klient banku) może żądać unieważnienia, na koszt przedsiębiorcy, zapłaty dokonanej kartą płatniczą w razie niewłaściwego wykorzystania tej karty w wykonaniu umowy zawartej na odległość. Nie uchyla to obowiązku naprawienia konsumentowi poniesionej przez niego szkody.

Zalety płynące z korzystania z kart płatniczych są oczywiste dla banków oraz ich klientów, jednak z ich użyciem wiążą się również niebezpieczeństwa. Mogą one wynikać z niedoskonałości obowiązującego prawa, braku pełnej skuteczności stosowanych zabezpieczeń, ale też z niefrasobliwości klientów banków, którzy często nie czytają umów oraz regulaminów i nie stosują się w pełni do wymogów bezpieczeństwa wskazanych przez bank. Wydawcy i użytkownicy kart oraz Internetu muszą być świadomi zagrożeń i potencjalnych działań przestępczych, związanych z kartami. Takie przestępstwa jak np. tzw. *skimming*, czyli pozyskanie danych zawartych na pasku magnetycznym karty wykorzystywanej w bankomacie oraz numeru PIN w celu stworzenia duplikatu karty, są szczególnie uciążliwe dla klientów banków, ale - tak jak większość przestępstw - trudne do wyeliminowania. Dokonanie tego typu przestępstwa jest znacznie trudniejsze w przypadku kart wyposażonych w mikroprocesor, dlatego bardziej powszechne wprowadzenie kart z mikroprocesorem powinno zwiększyć bezpieczeństwo klientów i banków. Z deklaracji Związku Banków Polskich wynika, że banki w Polsce - podobnie jak w innych krajach europejskich (zgodnie z samoregulacją SEPA tj. Jednolity Obszar Płatności w Euro) - zobowiązały się do wprowadzenia kart z mikroprocesorem do 1 stycznia 2011 roku.

Odpowiedzialność nadzoru bankowego

Komisja Nadzoru Finansowego nadzoruje działalność banków przede wszystkim na podstawie *ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym* (Dz.U. z 2006 r., nr 157 poz. 1119, z późn. zm.) i *ustawy Prawo bankowe*, natomiast zapewnienie bezpieczeństwa użytkownikom Internetu i zwalczanie przestępczości nie mieszczą się w kompetencjach nadzoru bankowego.

Aby zwiększyć bezpieczeństwo operacyjne banków i ich klientów Komisja wydała rekomendacje ostrożnościowe dla banków w zakresie zarządzania ryzykiem operacyjnym⁵ oraz ryzykiem systemów informatycznych⁶ (dostępne na stronie internetowej www.knf.gov.pl).

Nadzór bankowy w trakcie wykonywania czynności kontrolnych w bankach bada m.in. jakość systemu zarządzania bankiem, w tym ocenia system zarządzania ryzykiem i system kontroli wewnętrznej. Kwestie związane z bankowością elektroniczną (w tym internetową) są analizowane podczas badania i oceny zarządzania przez bank ryzykiem operacyjnym.

W ramach szczegółowych badań sprawdzane jest m.in. jak bank zarządza uprawnieniami dostępu, jakie są zabezpieczenia i czy wdrożony został system wykrywania nieuprawnionych wejść do sieci wewnętrznej banku lub ich prób (tzw. Intrusion Detection System). Ponadto kontroluje się, czy bank przeprowadza testy bezpieczeństwa sieci wewnętrznej i czy kwestia ta jest badana przez audyt wewnętrzny banku lub jego departament bezpieczeństwa.

W razie zidentyfikowania w wyniku czynności kontrolnych istotnych nieprawidłowości, KNF może zalecić bankowi przeprowadzenie audytu bezpieczeństwa. Jednak za jakość zabezpieczeń stosowanych przez klientów odpowiedzialni są oni sami i bank, z którym zawarli umowę o prowadzenie rachunku.

⁵ Rekomendacja **M** dotycząca zarządzania ryzykiem operacyjnym w bankach

⁶ Rekomendacja **D** dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki

2. Bankowość terminalowa

2.1 Charakterystyka bankowości terminalowej

Bankowość terminalowa polega na dokonywaniu transakcji bankowych z wykorzystaniem takich elektronicznych urządzeń jak bankomaty i terminale do akceptowania kart płatniczych (POS)⁷.

Jest to najczęściej wykorzystywana forma bankowości elektronicznej. Rozwój technologii elektronicznej i teleinformatycznej sprawił, że karty płatnicze wykorzystywane w bankowości terminalowej znajdują coraz szersze zastosowanie w rozliczeniach pieniężnych, głównie w płatnościach osób fizycznych.

Karta płatnicza⁸ jest instrumentem płatniczym, który identyfikuje wydawcę i upoważnionego posiadacza, uprawniając do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu - także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu.

Ze względu na sposób rozliczenia transakcji karty płatnicze można podzielić na⁹:

- **karty debetowe** - muszą posiadać pokrycie w środkach zgromadzonych na rachunku bankowym posiadacza karty; umożliwiają dokonywanie płatności tylko do wysokości salda konta posiadacza karty; są ściśle powiązane z rachunkiem bankowym i pełnią także funkcję bankomatową,
- **karty kredytowe** - pozwalają na korzystanie ze środków w ramach przyznanego przez bank kredytu, do wysokości limitu odnawialnego, ustalonego w umowie z bankiem wydającym kartę; w danym okresie rozliczeniowym, i na warunkach określonych w umowie, posiadacz karty jest zobowiązany do uzupełnienia spłaty limitu karty kredytowej,
- **karty obciążeniowe** (zwane także „charge”) - umożliwiają dokonywanie płatności za towary i usługi oraz wypłatę gotówki w ramach odnawialnego miesięcznego limitu rachunku, czyli salda rachunku powiększonego o kwotę dopuszczalnego zadłużenia.

Na rynku funkcjonują także **karty przedpłacone**. Dokonanie zapłaty kartą tego typu wymaga wcześniejszego zasilenia karty kwotą, do wysokości której następnie autoryzowane są transakcje. Karta taka może być wydana „na okaziciela”.

⁷ B. Swiecka: Bankowość elektroniczna. Wydanie I. Warszawa: CeDeWu 2004, s.24.

⁸ Definicja karty płatniczej znajduje się w ustawie Prawo bankowe

⁹ Iwańczuk Anna, Kotliński Grzegorz: Bankowe rozliczenia pieniężne. Poznań: AE w Poznaniu 2008

Krajowi wydawcy kart płatniczych umożliwiają również korzystanie z tzw. kart wirtualnych. Taka karta występuje tylko jako zarejestrowany w systemie rozliczeniowym numer (nie jest wydawana w fizycznej formie). Nie jest możliwe użycie jej do transakcji w terminalach POS i bankomatach. Można nią realizować tylko transakcje na odległość, czyli głównie w Internecie. Pod względem sposobu rozliczenia transakcji jest podobna do karty przedpłaconej.

Z punktu widzenia budowy można spotkać na rynku karty wypukłe (informacje o karcie takie jak nazwa posiadacza, numer karty, data ważności są wytłoczone na karcie) oraz karty płaskie (dane są nadrukowane na karcie).

Wg zapisu danych na karcie i sposobu ich odczytywania przez terminal rozróżniamy¹⁰:

- **karty z paskiem magnetycznym** - nośnikiem informacji jest pasek magnetyczny, na którym zapisane są informacje pozwalające na dokonanie transakcji (numer karty, data ważności itd.); na karcie tego typu nie jest zapisywany numer PIN, służący do uwierzytelnienia transakcji,
- **karty z układem elektronicznym** (karty chipowe, mikroprocesorowe) – dane niezbędne do autoryzacji transakcji są zapisane w mikroprocesorze umieszczonym w karcie; standard obsługi takich transakcji jest opracowany przez organizację zrzeszającą największych wydawców kart płatniczych: Europay, Mastercard i Visa (EMV), stąd o kartach chipowych mówi się, że są zgodne ze standardem EMV,
- **karty zbliżeniowe** (bezstykowe) - z układem elektronicznym, pozwalające na bezkontaktowe przeprowadzanie transakcji; na rynku polskim znajdują się obecnie dwie konkurujące ze sobą karty bezstykowe: VISA paywave i Mastercard paypass.

Realizowanie **płatności bezgotówkowej** za pomocą kart płatniczych odbywa się głównie poprzez płatność kartą za usługi lub towary u kontrahenta, posiadającego terminal POS (ang. *point of sale*). Terminal POS, czyli punkt sprzedaży, jest urządzeniem, które odczytuje karty płatnicze i za pomocą sieci teleinformatycznej łączy się z centrum autoryzacyjnym. Jeżeli transakcja jest realizowana w trybie on-line (zależy to od rodzaju karty, kwoty transakcji, centrum rozliczeniowego) terminal POS wysyła zapytanie do centrum autoryzacyjnego, czy posiadacz karty posiada środki płatnicze niezbędne do przeprowadzenia transakcji - jeśli tak, to transakcja zostaje zrealizowana, a płatność za zakupione usługi lub towary uregulowana. Centrum autoryzacyjne przekazuje następnie informację do centrum

¹⁰ Witryna NBP

rozliczeniowego banku i pobiera środki z rachunku posiadacza karty. Jednostka dokonująca sprzedaż otrzymuje należne jej środki w określonym terminie (najczęściej w okresach miesięcznych), pomniejszone o prowizję dla centrum rozliczeniowego.

Za pomocą kart płatniczych przeprowadza się też **transakcje gotówkowe**. Transakcja taka polega na wypłacie środków pieniężnych z bankomatu. Uczestnikami rozliczenia pieniężnego realizowanego przy użyciu karty płatniczej są zazwyczaj¹¹:

- posiadacz karty,
- akceptant,
- agent rozliczeniowy,
- bank akceptanta,
- bank, który wydał kartę.

Akceptantem jest przedsiębiorca, który zawarł z agentem rozliczeniowym umowę o przyjmowanie zapłaty przy użyciu elektronicznych instrumentów płatniczych czyli np. punkt handlowy akceptujący transakcje dokonane przy użyciu karty płatniczej. **Agent rozliczeniowy** (centrum akceptacyjne) zawiera z akceptantem umowę o przyjmowanie zapłaty przy użyciu elektronicznych instrumentów płatniczych, dokonuje autoryzacji (potwierdza, że osoba posługująca się daną kartą jest uprawniona do dokonania płatności), a także rozlicza i przetwarza transakcje.

¹¹ Iwańczuk Anna, Kotliński Grzegorz: Bankowe rozliczenia pieniężne. Poznań: AE w Poznaniu 2008

2.2 Bezpieczeństwo w bankowości terminalowej

Bezpieczeństwo kart płatniczych

Mimo postępu technicznego użytkowanie kart wciąż wiąże się z pewnymi zagrożeniami i potencjalnymi działaniami przestępczymi, których nie da się całkowicie wyeliminować. Poniżej przedstawiono najważniejsze zagrożenia oraz zasady postępowania, które powinny zwiększać bezpieczeństwo transakcji kartowych.

Obraz bezpieczeństwa transakcji dokonywanych kartami płatniczymi jest jednak zniekształcony przez częste medialne doniesienia (np. o gangach kopiujących karty i wypłacających pieniądze). Utrata karty płatniczej daje nieporównywalnie większe prawdopodobieństwo odzyskania pieniędzy niż utrata gotówki. Nieuprawnione użycie karty jest mniej ryzykowne także dlatego, że transakcje z użyciem kart są monitorowane przez banki.

SKIMMING

Największym zagrożeniem dla użytkowników kart z paskiem magnetycznym jest *skimming*. Jest to przestępstwo polegające na nielegalnym skopiowaniu zawartości paska magnetycznego karty płatniczej bez wiedzy jej posiadacza, w celu wykonywania nieuprawnionych płatności za towary i usługi.

Bezpieczeństwo posługiwania się kartami magnetycznymi zapewnia przede wszystkim kod PIN. Umożliwia on uwierzytelnienie osoby posługującej się kartą. Urządzenie, za pomocą którego przeprowadzana jest transakcja odczytuje z paska magnetycznego na karcie zawarte w niej informacje dotyczące banku (wydawcy karty), numeru karty oraz daty ważności. Numer karty wraz z kodem PIN są szyfrowane (za pomocą algorytmu DES lub 3DES) i wysyłane do wydawcy karty w celu ich weryfikacji. Wydawca sprawdza, czy podany PIN jest zgodny z PIN zapisanym w bazie danych wydawcy dla danej karty, i w przypadku pozytywnej weryfikacji zwraca/podaje numer rachunku bankowego, z którym związana jest dana karta. Następnie wysyłane jest zapytanie do systemu bankowego, w celu sprawdzenia czy na rachunku klienta znajdują się środki odpowiadające wartości transakcji. W przypadku pozytywnej odpowiedzi transakcja jest realizowana.

Skopiowana poprzez zeskanowanie danych karta zachowuje się w systemach banków tak jak karta oryginalna i trudno rozróżnić czy dana transakcja jest uprawnioną czy przestępczą. W celu zapobiegania tego typu przestępstwom, banki monitorują transakcje dokonywane przez swoich klientów. Analizowane są zachowania klienta dotyczące dokonywania płatności.

Nietypowe transakcje są weryfikowane za pomocą zdefiniowanych w systemie warunków logicznych w celu zidentyfikowania transakcji nieuprawnionych (oszukańczych). Następnie wygenerowany alert jest weryfikowany przez operatora, który może podjąć określone działania, np. kontaktuje się z posiadaczem karty.

Skimming może mieć miejsce w punktach sprzedaży. Nieuczciwy sprzedawca po użyciu karty w POS, w sposób niewidoczny dla klienta przeciąga kartę przez specjalne urządzenie, które kopiuje zawartość paska. Częściej jednak karty są kopiowane poprzez specjalne czytniki umieszczone przez przestępców na bankomatach, a numery PIN są wykradane za pomocą kamery umieszczonej na bankomacie lub z wykorzystaniem specjalnych nakładek na klawiaturę. Skimming bankomatowy staje się coraz bardziej wyrafinowany – zainstalowane urządzenia są zazwyczaj trudne do rozpoznania. Zdarza się także, że urządzenie kopiujące zawartość paska magnetycznego jest zainstalowane w samoobsługowych terminalach płatniczych np. na stacjach benzynowych.

Transakcje dokonywane kartami z paskiem magnetycznym są mniej bezpieczne od transakcji wykonywanych za pomocą kart wyposażonych w mikroprocesor (pod warunkiem, że jest on wykorzystywany do odczytywania danych z karty). Te ostatnie umożliwiają bezpieczną kontrolę dostępu, możliwość szyfrowania i deszyfrowania informacji, a także możliwość generowania i weryfikowania podpisów cyfrowych.

Jednak skimming jest możliwy również w przypadku kart z mikroprocesorem, jeśli karty te są wyposażone także w pasek magnetyczny (za pomocą którego można również autoryzować transakcje np. w bankomatach nie obsługujących standardu EMV).

Wyposażanie kart zarówno w pasek magnetyczny jak i mikroprocesor wynika głównie z braku pełnej dostępności POS i bankomatów obsługujących karty z mikroprocesorami. Według szacunków KNF na koniec 2009 r. ponad 25% bankomatów w Polsce nie było zgodnych z EMV (tzn. że odczytywały one dane jedynie z paska magnetycznego).

Stosunkowo duża liczba bankomatów niezgodnych z EMV była „zachętą” dla międzynarodowych gangów do wykorzystywania bankomatów do wybierania gotówki za pomocą skopiowanych kart. Dane skopiowane (najczęściej zagranicą) z paska magnetycznego karty chipowej służą do wypłacania pieniędzy z bankomatów niezgodnych z EMV. Za takie nadużycie odpowiada strona, która nie była dostosowana do EMV, czyli bank jako właściciel bankomatu odczytującego dane jedynie z paska magnetycznego.

Złodzieje rzadziej decydują się na płacenie skopiowanymi kartami w urządzeniach POS. Można zauważyć jednak wzrost wykorzystania skopiowanych kart do dokonywania płatności bez fizycznego użycia karty (w Internecie).

SKOPIOWANIE DANYCH KARTY WYPUKŁEJ

Kartami płatniczymi wypukłymi można także płacić bez fizycznego użycia karty płatniczej (tzw. transakcje na odległość, „card not present” czyli przez Internet). Zgodnie z zapisami art. 28 ust. 6 ustawy o eip, operacje takie są dopuszczalne tylko wtedy, jeżeli umowa zawarta między wydawcą karty (bankiem) a jej posiadaczem przewiduje taką możliwość. Tego typu transakcje obarczone są stosunkowo wyższym ryzykiem użycia karty przez osobę nieuprawnioną, gdyż do obciążenia karty dochodzi zwykle poprzez podanie jej numeru, daty ważności oraz dodatkowego kodu CVV2/CVC2 - nie jest przy tym niezbędne potwierdzenie czynności kodem PIN.

CVV2/CVC2 (Card Verification Value/Card Verification Code) jest to kod służący do weryfikacji transakcji zdalnych, umieszczony najczęściej na odwrocie karty tuż przy pasku do podpisu.

Niektórzy wydawcy wprowadzają dodatkowe mechanizmy potwierdzania operacji np. za pomocą kodów wysyłanych na telefony komórkowe.

W związku z możliwością dokonywania płatności na odległość, które w znacznej większości autoryzowane są jedynie poprzez dane zawarte na samej karcie, pojawia się zagrożenie polegające na sfotografowaniu karty płatniczej (np. telefonem komórkowym) i wykorzystaniu środków do płatności nieuprawnionych. Należy pamiętać, że w przypadku takiego nadużycia, ograniczenie odpowiedzialności klienta do kwoty 150 € o którym mowa w art. 28 ust. 2 ustawy o eip nie obowiązuje, gdyż odnosi się ono jedynie do operacji dokonanych z użyciem utraconej (zgubionej, skradzionej) karty płatniczej.

Ryzyko związane z płatnościami kartami w Internecie jest więc wyższe, ale jeżeli nieuczciwy sprzedawca wyłudził od nas zapłatę za towar, którego nie dostarczył lub za towar wadliwy, to klient może skorzystać z procedury reklamacyjnej, za pomocą której bank (wydawca karty) potrąca kwotę transakcji lub jej część agentowi rozliczeniowemu, kwestionując zasadność takiego obciążenia w oparciu o regulacje danego systemu kartowego (VISA, MasterCard, American Express, Diners, JCB)¹². Jest to tzw. *chargeback*.

¹² www.kartyonline.pl

Stosowanie *chargeback* jest ściśle sformalizowane i ograniczone do konkretnie wymienionych przypadków. Podobne procedury stosują w tym względzie zarówno Visa jak i MasterCard, a także inne organizacje płatnicze. Procedura rozpoczyna się, gdy klient złoży reklamację wykonanej transakcji kartowej (*chargeback* może być także zainicjowany z własnej woli przez bank, który wydał kartę płatniczą). Musi on w tej sytuacji podać powód reklamacji, który określa poprzez wskazanie kodu *chargeback*. Jednak możliwość złożenia reklamacji nie jest zależna od wystąpienia jednej ze sklasyfikowanych przyczyn, bowiem klient zawsze może zareklamować dowolną transakcję. Efektem tej procedury może być zarówno zwrot pieniędzy klientowi zgłaszającemu reklamację, jak i ostateczne odrzucenie *chargeback* i potwierdzenie prawidłowości wykonanej transakcji. W wyjątkowych przypadkach procedura może zostać powtórzona, a jeśli to nie przyniesie rezultatu, sprawa zostaje skierowana do organizacji płatniczej celem rozstrzygnięcia w drodze arbitrażu.

Finansowa odpowiedzialność z tytułu reklamacji transakcji jest określona w umowach zawieranych przez agenta rozliczeniowego¹³.

W przypadku płacenia kartami przez Internet należy zachować szczególną ostrożność i zwracać uwagę na zabezpieczenia komputera (oprogramowanie antywirusowe, firewall¹⁴, aktualizacje – patrz: *Przewodnik klienta usług bankowości elektronicznej*) oraz na to, czy transmisja ze stroną, poprzez którą dokonujemy płatności jest szyfrowana. Jeżeli tak nie jest, to ewentualne podsłuchanie transmisji i dostęp do danych o karcie umożliwi przestępcy dokonanie nieautoryzowanych transakcji.

W przypadku stwierdzenia dokonania nieuprawnionych transakcji na odległość kartą niezatrzeżoną konsument ma prawo do żądania unieważnienia transakcji (art. 14 *ustawy z 2002 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny*).

PHISHING

Należy też pamiętać o tzw. inżynierii społecznej, której celem jest wydobycie informacji o karcie płatniczej klienta. Zjawisko to nosi nazwę *phishing* tj. wyłudzenie poufnych informacji osobistych (np. haseł lub szczegółów dot. karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. W ten

¹³ M. Grabowski, *Reklamacja transakcji dokonywanych kartami płatniczymi – stosunek prawny między posiadaczem a wydawcą*, Prawo Bankowe nr 7-8/2007

¹⁴ Firewall (z ang. zaporą sieciową) – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami.

sposób nieświadomi klienci podają przestępcom dane niezbędne do dokonania transakcji „na odległość”.

Poziom bezpieczeństwa transakcji internetowych (a także innych bez fizycznego przedstawienia karty) podnosi **Standard 3-D Secure**. Jest to dodatkowe zabezpieczenie polegające na konieczności podania poza numerem karty, daty jej ważności i kodu CVV2/CVC2 jeszcze dodatkowego hasła. Hasło to nie jest używane w żadnych transakcjach, które wymagają fizycznej obecności karty, dlatego nie istnieje niebezpieczeństwo podejrzenia go przy zakupach w sklepie lub w innym punkcie sprzedaży. Czasami zamiast stałego hasła, dla każdej transakcji generowane jest hasło dynamiczne (SMSkod, wartość cyfrowa z tokena).

Aby skorzystać z technologii dodatkowego zabezpieczenia w postaci 3-D Secure, klient musi posiadać kartę płatniczą, która obsługuje ten standard, a sklep internetowy musi umożliwiać identyfikację poprzez 3-D Secure.

UTRATA KARTY BEZSTYKOWEJ

Technologia bezstykowa polega na dokonaniu płatności poprzez zbliżenie karty do terminala, bez konieczności dodatkowego potwierdzania transakcji podpisem czy kodem PIN. Aby transakcja taka mogła zostać przeprowadzona, konieczne jest zbliżenie karty do terminala na odległość kilku centymetrów. Wcześniej w terminalu przyjmującym płatność musi zostać wpisana kwota płatności. Takie karty są dostępne na polskim rynku od 2009 r.

Karta bezstykowa daje wygodę użytkownika, jednak brak konieczności potwierdzania transakcji do kwoty 50 zł sprawia, że w przypadku jej zgubienia, znalazca będzie mógł nią zapłacić do kwoty wyznaczonego limitu.

Dane przekazane do UKNF dotyczące wartości transakcji oszukańczych dokonanych kartami bezstykowymi nie są znaczące – na koniec 2009 wartość transakcji oszukańczych stanowiła 0,0002% obrotu kartami, które umożliwiały płatności bezstykowe. Niemniej jednak w Internecie pojawiły się już informacje o przenośnych czytnikach kart, które pozwalały pozyskać nielegalnie dane z kart zbliżeniowych¹⁵.

¹⁵ Dotyczy to USA.

3. Bankowość internetowa

3.1. Charakterystyka bankowości internetowej

Bankowość internetowa – forma świadczenia usług bankowych za pośrednictwem ogólnodostępnej sieci Internet, z wykorzystaniem standardowego oprogramowania (przeglądarka www) lub oprogramowania dedykowanego do komunikacji z bankiem (systemy home/corporate banking).

Począwszy od lat 90 XX wieku, serwisy bankowości internetowej podlegały intensywnemu rozwojowi pod kątem bezpieczeństwa transakcji i ich funkcjonalności.

Umownie przyjmuje się, że rozwój serwisów bankowości internetowej przebiegał w etapach:

- informacyjny - prezentacja oferty usług, informacje o banku,
- interaktywny (pasywny) - przeglądanie sald na rachunkach i kontakt z bankiem,
- transakcyjny - wykonywanie w sposób zdalny standardowych operacji finansowych,
- strategiczny - interaktywne zarządzanie finansami osobistymi i firmowymi, w tym między innymi: szeroki dostęp do oferty produktów bankowych, ubezpieczeniowych, usług maklerskich i doradztwo.

Większość funkcjonujących w Polsce systemów bankowości internetowej zostało uruchomionych lub zmodernizowanych w latach 2005 - 2009. Dostępne obecnie na polskim rynku systemy bankowości internetowej zaliczyć można niemal w 100 % do transakcyjnych i strategicznych.

Cechy charakterystyczne bankowości internetowej to między innymi:

- brak konieczności bezpośredniego kontaktu klienta z bankiem i wynikająca stąd oszczędność czasu,
- wysoka funkcjonalność serwisów bankowych, w tym dostępność wszystkich standardowych usług świadczonych w oddziałach banku (w przeciwieństwie do innych form bankowości elektronicznej, oferujących głównie usługi płatnicze),
- całodobowy dostęp do usług bankowych,
- zadowalający poziom bezpieczeństwa transakcji i środków na rachunku, przy założeniu przestrzegania przez klienta podstawowych zasad bezpieczeństwa,
- możliwość jednoczesnej i automatycznej obsługi dużej liczby klientów w czasie rzeczywistym,
- ograniczenie do minimum obiegu dokumentów papierowych,

- brak ograniczeń terytorialnych - dostęp do rachunku internetowego można uzyskiwać z dowolnego miejsca na świecie,
- niższe koszty realizacji transakcji w porównaniu z obsługą klientów w oddziałach banku oraz niższe koszty obsługi dla banku.

W odróżnieniu od innych form korzystania z usług bankowych, bankowość internetowa wymaga od klientów przygotowania w zakresie podstawowej znajomości obsługi komputera, świadomości potencjalnego ryzyka związanego z korzystaniem z Internetu oraz przestrzegania podstawowych zasad bezpieczeństwa w tym zakresie.

Dostępne obecnie na rynku systemy bankowości internetowej (zdalnej), ze względu na ich przeznaczenie, podzielić można na:

- bankowość internetową (detaliczna i dla podmiotów gospodarczych) – usługi dedykowane dla osób prywatnych i sektora MSP, których charakterystyczną cechą jest dostęp do usług bankowych z wykorzystaniem standardowego oprogramowania, tj. przeglądarki internetowej, przy użyciu zabezpieczonego kryptograficznie protokołu transmisyjnego (SSL) oraz pozwalające na realizację transakcji w czasie rzeczywistym,
- home banking – usługa dedykowana dla osób prywatnych i małych firm, wymagająca instalowania na komputerze klienta dedykowanego oprogramowania, często korzystająca z telefonicznego połączenia z serwisem banku bez konieczności dostępu do sieci Internet. Ze względu między innymi na ograniczoną funkcjonalność (często są to systemy funkcjonujące w trybie off line) i koszty funkcjonowania oraz rosnącą dostępność Internetu, home banking traci popularność.
- corporate banking – rozwiązania przeznaczone głównie dla dużych podmiotów gospodarczych i instytucji, charakteryzujące się rozbudowaną funkcjonalnością, pozwalające na integrację i automatyczną wymianę danych z systemem księgowym klienta oraz wielopoziomowy dostęp i rozbudowany system akceptowania transakcji. Usługi te wymagają instalacji na komputerze klienta dedykowanego oprogramowania do komunikacji z serwisem bankowym.

Ze względu na przyjęty model działalności operacyjnej banku, kanał internetowy może funkcjonować jako uzupełnienie lub ekwiwalent standardowej formy świadczenia usług w placówkach bankowych, bądź jako jedyny (obok innych form bankowości elektronicznej) kanał dystrybucji usług (tzw. bank wirtualny). Możliwość osobistego kontaktu z bankiem (dostępność placówki bankowej w niewielkiej odległości od miejsca zamieszkania), pomimo korzystania z kanału internetowego, jest wciąż istotnym kryterium wyboru oferty bankowej, dokonywanego przez klientów w Polsce.

Bankowość internetowa i systemy home/corporate banking, charakteryzują się rozbudowaną funkcjonalnością w porównaniu z innymi rodzajami bankowości elektronicznej (karty bankowe i systemy telefoniczne, które stanowią alternatywę głównie dla płatności gotówkowych).

Początkowo rozwój rynku bankowości internetowej w Polsce opóźniały stosunkowo wysokie koszty sprzętu komputerowego i dostępu do Internetu oraz niedostateczna jakość infrastruktury sieciowej. W latach 2005 – 2009 dostępność techniczna i ekonomiczna Internetu uległa znaczącej poprawie, spadły również koszty zakupu sprzętu niezbędnego do korzystania z bankowości internetowej.

Ocenia się, że w okresie 2005 - 2009 wzrost skali wykorzystania internetowego kanału dostępu do usług bankowych determinowały następujące czynniki:

zależne od banków:

- polityka cenowa i marketingowa w zakresie świadczonych usług¹⁶, zakładająca promowanie elektronicznych kanałów obsługi. W większości detalicznych banków standardowe transakcje realizowane za pośrednictwem kanału obsługi internetowej realizowane są w ramach miesięcznej, ryczałtowej opłaty za prowadzenie rachunku lub bezpłatnie,
- silna konkurencja na rynku usług bankowych, ograniczająca możliwość podnoszenia opłat za wykonanie standardowych operacji za pośrednictwem systemów bankowości internetowej,

niezależne od banków:

- spadek realnych kosztów korzystania z Internetu w latach 2005 – 2009, o czym świadczy między innymi malejący odsetek respondentów, wskazujących koszty jako barierę w dostępie do Internetu (z 35% do 29%)¹⁷,
- poprawa jakości infrastruktury sieciowej i dostępności szerokopasmowego Internetu w latach 2005 – 2009¹⁸,
- obowiązek wykonywania rozliczeń z wykorzystaniem rachunków bankowych¹⁹ oraz wymóg wpłat na rachunki (UE, ZUS, KRUS i US) w formie przelewu,

¹⁶ Wg monitoringu prowadzonego przez NBP w ramach „Programu obrotu bezgotówkowego w Polsce w latach 2009 – 2013”, w 2009 roku największa skala podwyżek cen usług dotyczyła wpłat gotówkowych i poleceń przelewu składanych w oddziałach banków.

¹⁷ <http://www.internetstats.pl/index.php/2009/03/powody-nieposiadania-internetu-w-domu-gus/>

¹⁸ Realizowany w latach 2007 – 2013 program „innowacyjna gospodarka” w zakresie budowy infrastruktury dostępowej do Internetu został objęty wsparciem UE w wysokości ok. 1 mld euro. W latach 2007 - 2009 odsetek gospodarstw domowych z szerokopasmowym dostępem do Internetu w Polsce wzrósł z 30 do 51 %, natomiast w UE z 42 do 56 %. Analiza SWOT dotycząca rozwoju Internetu szerokopasmowego: http://www.mswia.gov.pl/portal/SZS/494/6269/Analiza_SWOT.html.

- ulgi podatkowe w podatku dochodowym (PIT) z tytułu ponoszonych kosztów dostępu do Internetu.

Alternatywy dla systemów bankowości internetowej upatruje się w rozwiązaniach mobilnych, korzystających z technologii GSM – WAP, jednak pomimo dobrego nasycenia rynku telefonii komórkowej (liczba aktywnych kart SIM jest zbliżona do liczby ludności), usługi transakcyjne świadczone w ten sposób wolniej zyskują popularność. Przyczyną tego są głównie ograniczenia urządzeń mobilnych: mały ekran, niewygodna w użyciu klawiatura oraz dyskomfort związany z nawigacją w aplikacjach mobilnych. Ten kanał obsługi realizuje głównie funkcje informacyjne i autoryzacyjne a jego wykorzystanie w realizacji czynności transakcyjnych ma charakter perspektywiczny.

3.2. Charakterystyka usług bankowości internetowej

Rozwój funkcjonalności portali internetowych utrzymywanych przez banki w ostatnim okresie oraz realizowana polityka biznesowa i cenowa prowadzą do systematycznego wzrostu znaczenia internetowego kanału świadczenia usług bankowych.

Przejawia się to między innymi wzrostem liczby rachunków obsługiwanych przez Internet oraz rosnącą liczbą i wartością transakcji elektronicznych. Kanały obsługi internetowej zapewniają możliwość realizacji standardowych, powtarzalnych czynności bankowych.

Jednocześnie stopniowej zmianie ulega charakter czynności wykonywanych w oddziałach banków, które w miejsce czynności dysponenckich i kasowych, w większym stopniu pełnią rolę sprzedażową i doradczą.

Internetowe serwisy bankowe składają się zazwyczaj z dwóch części. Pierwsza z nich (informacyjna) dostępna jest dla wszystkich użytkowników Internetu i nie wymaga zawierania umowy z bankiem. Druga część (transakcyjna) jest udostępniana przez bank po zawarciu umowy o prowadzenie rachunku bankowego.

Usługi internetowe świadczone przez największe banki detaliczne na rzecz klientów oferowane są w pakietach, różniących się ceną. Na różnice cenowe poszczególnych pakietów wpływają głównie koszty wykonywania transakcji w oddziałach (przez dysponenta), dostępność bezprowizyjnych bankomatów i wysokość opłat pobieranych za płatności wykonywane kartami bankowymi. Najniższe ceny usług dotyczą pakietów, w których niemal wszystkie czynności wykonywane są przez klienta samodzielnie przez Internet lub za pomocą innych, elektronicznych kanałów obsługi.

¹⁹ Wymóg posiadania konta bankowego - ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej.

Podstawą korzystania z bankowości internetowej jest posiadanie rachunku w banku. Podpisanie umowy rachunku bieżącego (ROR), wraz z opcją obsługi przez Internet, stanowi zwykle jedyną czynność, którą klient wykonuje w placówce banku. Wraz z umową o prowadzenie rachunku klient otrzymuje identyfikator (login) oraz tzw. hasło startowe, umożliwiające pierwsze logowanie do systemu bankowości internetowej.

W większości przypadków, pozostałe produkty są aktywowane za pośrednictwem serwisu internetowego, w zależności od potrzeb klienta. Umożliwia to elastyczne dostosowanie uruchomionych opcji i produktów do indywidualnych wymagań. Uruchomienie dostępu do dodatkowych produktów, wykonywane jest przez klienta samodzielnie i z reguły nie wymaga osobistego kontaktu z bankiem (za wyjątkiem tych produktów bankowych, które wiążą się z koniecznością oceny zdolności kredytowej klienta i dostarczeniem przez klienta dodatkowej dokumentacji).

Zakres usług dostępnych poprzez większość bankowych portali internetowych pozwala na wykonanie niemal wszystkich standardowych czynności bankowych bez konieczności osobistego kontaktu z bankiem.

Udostępnione przez banki działające na polskim rynku systemy bankowości internetowej, pozwalają na wykonywanie wszystkich podstawowych operacji na rachunkach takich jak:

- przeglądanie operacji na rachunkach,
- realizacja przelewów,
- definiowanie list odbiorców płatności i przelewów predefiniowanych,
- spłata kredytu w rachunku kredytowym i karcie kredytowej,
- zakładanie i zrywanie lokat terminowych,
- obsługa rachunków oszczędnościowych,
- komunikacja z bankiem w formie bezpiecznej poczty elektronicznej, w tym otrzymywanie wyciągów, wnioskowanie o kredyt lub wydanie kart bankowych.

Ponadto, w bankach prowadzących taką działalność, możliwe jest nabywanie jednostek funduszy inwestycyjnych i papierów wartościowych (rachunki inwestycyjne/maklerskie), doładowanie telefonów komórkowych pre-paid oraz dostęp do serwisów informacyjnych.

Usługi home banking największą popularnością cieszyły się w początkowym okresie rozwoju bankowości elektronicznej. Systemy te komunikowały się najczęściej z serwisem bankowym bezpośrednio (bez korzystania z sieci Internet) i zazwyczaj funkcjonowały w tzw. trybie off line. Sporządzenie listy płatności i jej zatwierdzenie następowało na komputerze klienta, natomiast połączenie z serwisem bankowym nawiązywane było jedynie w celu wysłania do

banku (i odbioru) przygotowanych wcześniej przesyłek/pakietów, co do minimum skracало czas transmisji. Podstawową funkcją tych systemów było wykonywanie przelewów oraz otrzymywanie informacji o historii zapisów na rachunku bieżącym.

Oferty udostępnione w ramach usług corporate banking, poza wymienionymi wyżej czynnościami, uwzględniają specyficzne wymagania przedsiębiorstw i instytucji, między innymi dotyczące umożliwienia pracy wielu użytkowników (w tym hierarchiczne zatwierdzanie transakcji), automatyzacji czynności księgowych i wymiany danych z systemem ewidencyjnym przedsiębiorstwa, rozliczeń z kontrahentami (również zagranicznymi), obsługi przedsiębiorstw prowadzących działalność w strukturze wielooddziałowej a także korzystających z usług więcej niż jednego banku.

3.3. Bezpieczeństwo w bankowości internetowej

Podstawą funkcjonowania bankowości internetowej jest **niezaprzeczalność transakcji**, która jest autoryzowana kodem znanym jedynie posiadaczowi rachunku bankowego.

Charakterystyczną cechą transakcji internetowych jest proces ich autoryzacji. W przeciwieństwie do operacji wykonywanych w oddziałach banku, w tym przypadku nie identyfikuje się tożsamości klienta zlecającego transakcję, lecz zgodność wprowadzonych do systemu bankowości internetowej kodów autoryzacyjnych. Ze względu na charakter funkcjonowania systemów bankowości internetowej (dostęp uzyskiwany z komputera osobistego należącego do klienta), systemy autoryzacji wykorzystujące cechy biometryczne (np. odcisk palca, obraz tęczówki oka itp.) prawdopodobnie w najbliższym czasie nie znajdą zastosowania. Poufność haseł dostępu i bezpieczeństwo narzędzi służących do ich generowania będą zatem w dalszym ciągu głównym elementem bezpieczeństwa transakcji internetowych.

Główne metody zapewniające bezpieczeństwo transakcji internetowych to:

- szyfrowana transmisja danych - realizowana z wykorzystaniem protokołu SSL,
- proste uwierzytelnianie (identyfikator, hasło, PIN),
- silne uwierzytelnianie (np. token, certyfikat użytkownika, klucz prywatny),
- kwalifikowany podpis elektroniczny.

Podstawą współcześnie funkcjonujących zabezpieczeń bankowości internetowej jest protokół SSL wykorzystywany do ochrony transmisji realizowanej protokołem HTTP, korzystający

z metody tzw. klucza publicznego oraz szyfrowania symetrycznego. Główne funkcje protokołu SSL to:

- uwierzytelnienie – możliwość zweryfikowania tożsamości klienta i banku,
- poufność – możliwość szyfrowania przesyłanych informacji, które są czytelne jedynie dla komunikujących się stron,
- integralność – zabezpieczenie przed zmianą zawartości przesyłanego komunikatu.

Dostępność i skuteczność standardu SSL sprawiła, że jest on obsługiwany przez wszystkie przeglądarki www oraz pozwoliła na jego upowszechnienie niemal we wszystkich systemach bankowości internetowej.

W przeglądarkach internetowych nawiązanie bezpiecznego połączenia (SSL) sygnalizowane jest pojawieniem się ikony zamkniętej kłódki oraz pojawieniem się w adresie internetowym widocznym w oknie przeglądarki litery „s” (adres internetowy musi zaczynać się od „https://www. ...”). Powrót z trybu wymiany danych chronionego protokołem SSL do sesji nie szyfrowanej poprzedzany jest stosownym komunikatem (w zależności od konfiguracji przeglądarki). Protokół SSL korzysta z tzw. certyfikatów autentyczności wystawianych bankom przez powołane do tego podmioty certyfikujące (ang. *certificate authority*). Certyfikat jest to zbiór danych jednoznacznie identyfikujących jednostkę (bank) oraz pozwalający stwierdzić czy osoba, która się nim legitymuje, jest rzeczywiście tą, za którą się podaje. Certyfikat zawiera: nazwę certyfikowanego podmiotu (banku), identyfikator, klucz publiczny banku, czas ważności, nazwę wystawcy certyfikatu, identyfikator wystawcy, podpis wystawcy i skrót certyfikatu zaszyfrowany przy pomocy klucza prywatnego wystawcy. Kliknięcie w polu ikony zamkniętej kłódki pozwala na identyfikację tożsamości banku, z którym nawiązaliśmy połączenie. Stosowana standardowo długość klucza kryptograficznego (128 bitów) uniemożliwia w praktyce zdekodowanie tak zabezpieczonej transmisji i odszyfrowanie przesyłanych informacji w celu kradzieży środków z rachunku bankowego.

W zależności od systemu bankowości internetowej i rodzaju wykonywanej operacji, rozróżniamy następujące metody uwierzytelniania (w połączeniu z identyfikatorem przypisanym klientowi):

- hasło stałe,
- hasło jednorazowe,
- certyfikaty cyfrowe skojarzone z numerem PIN lub hasłem.

Hasła jednorazowe w zależności od przyjętego rozwiązania mogą być przekazywane klientowi w formie:

- listy haseł jednorazowych,
- karty TAN (Transaction Authorisation Number),
- tokena sprzętowego,
- tokena działającego w formie aplikacji np. w telefonie komórkowym,
- wiadomości SMS.

W systemach bankowości internetowej stosowanych przez banki działające w Polsce, autoryzacja transakcji przebiega minimum dwuetapowo:

1. Uzyskanie dostępu do opcji przeglądania rachunków - wymaga najczęściej podania identyfikatora i całego lub części (losowo wybranych znaków hasła statycznego). Część z banków w procesie autoryzacji dostępu wykorzystuje silniejsze metody ochrony w formie haseł jednorazowych generowanych przez token sprzętowy lub token działający w formie aplikacji w telefonie komórkowym. Hasło dostępu składa się z części stanowiącej wskazanie tokena oraz części ustalonej przez użytkownika (na wypadek kradzieży tokena), co w połączeniu z krótkim czasem ważności wygenerowanego hasła jednorazowego stanowi obecnie najbezpieczniejsze rozwiązanie. W systemach bankowości korporacyjnej najczęściej stosuje się kombinację hasła stałego i wskazania tokena lub certyfikatu cyfrowego umieszczonego na zewnętrznym nośniku (karta mikroprocesorowa) i odpowiednio zabezpieczonego przed skopiowaniem.
2. Wykonanie transakcji (zwłaszcza przelewów wychodzących) - wymaga dodatkowej autoryzacji, zazwyczaj w postaci podania kodu jednorazowego. W zależności od stosowanego rozwiązania są to kody przesyłane techniką SMS, generowane przez token sprzętowy lub token GSM (np. aplikacja w telefonie komórkowym), drukowane na papierowej liście (w formie „zdrapki”) lub odczytywane z karty TAN.

Brak wystarczających danych o zdarzeniach i stratach operacyjnych nie daje podstaw do stwierdzenia jednoznacznej korelacji pomiędzy stosowaną techniką generowania haseł a skalą nieuprawnionych transakcji.

Szczególnego nadzoru ze strony użytkownika wymagają systemy wykorzystujące drukowane listy haseł i karty TAN (ze względu na łatwe kopiowanie i możliwość późniejszego ich wykorzystania). Cechy tej pozbawione są rozwiązania oparte o system haseł jednorazowych generowanych przez tokeny sprzętowe i tokeny GSM oraz kody SMS.

Siła kryptograficzna (złożoność) stałych haseł dostępu (ustalanych przez klienta) jest zazwyczaj częściowo wymuszona przez system autoryzacyjny banku i uzależniona od minimalnej liczby znaków, zawartości małych i dużych liter oraz cyfr. Uwzględniając ograniczenie liczby błędnych logowań skutkujących blokadą konta oraz liczbę możliwych kombinacji znaków w haśle, prawdopodobieństwo udanego ataku słownikowego²⁰ jest znikome pod warunkiem ustalenia przez klienta hasła charakteryzującego się dobrą siłą kryptograficzną. Hasło nie powinno kojarzyć się np. z imieniem, nazwiskiem, nr telefonu, nr rejestracyjnym samochodu, sekwencją kolejnych znaków na klawiaturze „qwerty” itp., ale z kolei powinno być możliwe do zapamiętania.

Ochrona tajemnicy haseł i kodów autoryzacyjnych, w tym urządzeń generujących kody jednorazowe oraz ustalenie silnych haseł dostępu jest podstawą bezpieczeństwa transakcji internetowych i głównym obowiązkiem posiadacza rachunku bankowego.

Większość systemów bankowości internetowej pozwala na skonfigurowanie przez klienta mechanizmów bezpieczeństwa, między innymi poprzez:

- możliwość ustalenia maksymalnego dziennego limitu operacji i limitu operacji jednorazowej,
- możliwość ustalenia zakresu powiadamiania komunikatem SMS o logowaniu do rachunku, zmianie salda rachunku i innych czynnościach (usługa jest zwykle płatna w zależności od liczby wysłanych komunikatów),
- wykorzystanie informacji o udanych i nieudanych logowaniach do rachunku.

Parametry te powinien skonfigurować sam klient w oparciu o własne doświadczenia, liczbę i wartość realizowanych transakcji internetowych. Pozwoli to na ograniczenie skali strat w wyniku ewentualnej utraty haseł i kodów autoryzacyjnych.

Zagrożenia związane z funkcjonowaniem bankowości internetowej można podzielić na dwie grupy: bezpośrednie i zdalne.

Poniżej, w kolejności największego prawdopodobieństwa wystąpienia i potencjalnych skutków finansowych, opisano główne zagrożenia, na jakie narażony jest klient bankowości internetowej oraz sposoby ochrony przed tymi zagrożeniami:

KRADZIEŻ DOKUMENTÓW TOŻSAMOŚCI KLIENTA – działanie przestępcze polegające na podszyciu się pod właściciela rachunku za pomocą skradzionego lub sfalszowanego dokumentu tożsamości i wyłudzeniu od pracownika banku narzędzi

²⁰ Atak polegający na próbie odgadnięcia hasła.

autoryzacyjnych (nowy token, pakiet startowy), pozwalających na wprowadzenie pełnomocnictwa do rachunku, własnego hasła, zmianę nr telefonu do otrzymywania kodów SMS i innych parametrów konta użytkownika, umożliwiających kradzież środków z rachunku bankowego.

Zabezpieczeniem przed tego typu zagrożeniem jest ochrona dokumentów tożsamości, a w przypadku ich utraty, niezwłoczne ich zastrzeżenie za pośrednictwem infolinii lub w najbliższej placówce bankowej. Ze względu na znaczenie czasu reakcji w tym wypadku, zaleca się zapisanie w kilku łatwo dostępnych miejscach numeru telefonu pod którym można taką czynność wykonać (niestety łupem złodzieja może też paść telefon w którym ww. numer jest zapisany). Rozmowy telefoniczne w infolinii bankowej podlegają nagrywaniu, jednak należy dążyć do otrzymania pisemnego potwierdzenia faktu zastrzeżenia dokumentu tożsamości - z określeniem daty i godziny wykonania tej czynności.

Utrata dokumentu tożsamości musi być niezwłocznie zgłoszona bankowi prowadzącemu rachunek.

BEZPOŚREDNIA KRADZIEŻ HASEŁ I NARZĘDZI (token, karta TAN, telefon komórkowy itp.), służących do autoryzacji dostępu do rachunku i przeprowadzania transakcji internetowych. Przestępca wykorzystuje fakt zapisywania przez klientów loginów i haseł dostępu do systemów bankowości internetowej w formie jawnej.

Zabezpieczeniem przed tego typu zagrożeniem jest przestrzeganie zasady, by hasła dostępu nie były zapisywane w formie jawnej oraz bezpieczne przechowywanie narzędzi autoryzacyjnych. W przypadku jakichkolwiek wątpliwości co do poufności hasła dostępu należy dokonać jego zmiany w serwisie internetowym. Każdy przypadek utraty narzędzia autoryzującego transakcję należy jak najszybciej zgłosić do banku i uzyskać potwierdzenie tego faktu. W przypadku kradzieży lub zgubienia telefonu komórkowego (karty SIM), wykorzystywanego do autoryzacji transakcji, zaleca się zablokowanie (za pośrednictwem Internetu) dostępu do rachunku bankowego do czasu dezaktywowania utraconej karty SIM i otrzymania od operatora telefonicznego nowej karty. Z tego samego względu nie należy w pamięci telefonu zapisywać loginów i haseł dostępu do systemu bankowości internetowej.

PHISHING - działanie przestępcze polegające na zdalnym wyłudzeniu informacji autoryzacyjnych, które może przybierać formę:

- listu elektronicznego, wysłanego rzekomo w imieniu banku, zawierającego prośbę o podanie loginu i haseł dostępu,

- przekierowania do spreparowanej strony www kontrolowanej przez przestępcę, przypominającej graficznie stronę banku, .
- telefonu do klienta (rzekomo w imieniu banku) z prośbą o podanie loginu i hasła.

Zabezpieczeniem przed tego typu zagrożeniami jest stosowanie zasady, by w żadnym wypadku nie odpowiadać na podobne wiadomości i zapytania, a wszelkie tego typu zdarzenia zgłaszać niezwłocznie bankowi. W przypadku korzystania z infolinii, jeżeli bank udostępnia taką opcję, należy wprowadzić tzw. hasło identyfikacji zwrotnej, pozwalające na zidentyfikowanie czy telefonującym jest faktycznie pracownik banku.

Wszelką korespondencję elektroniczną z bankiem należy prowadzić jedynie poprzez portal bankowy (po zalogowaniu).

POMYŁKI W ZLECENIACH PŁATNICZYCH (wychodzących) wprowadzonych przez klienta bankowości internetowej. W przypadku stwierdzenia błędnie wprowadzonego numeru rachunku docelowego, należy niezwłocznie skontaktować się z bankiem w celu anulowania transakcji. Jest to możliwe pod warunkiem, że transakcja nie została jeszcze przez bank zrealizowana.

Zabezpieczeniem przed tego typu pomyłkami (poza algorytmem liczby kontrolnej NRB) jest zdefiniowanie kontrahentów, do których najczęściej wysyłane są przelewy - umożliwia to większość systemów bankowości internetowej. Odzyskanie błędnie wysłanych środków może być długotrwałe i nie zawsze skuteczne.

Realizując transakcje wychodzące należy szczególnie uważnie wpisywać numer rachunku bankowego kontrahenta.

ZDALNA KRADZIEŻ HASEŁ I KODÓW JEDNORAZOWYCH – przestępstwo to jest możliwe w przypadku zapisania danych do autoryzacji na dysku komputera klienta. W tym procederze wykorzystywane jest specjalne oprogramowanie (popularnie określane jako „koń trojański”, wirus komputerowy, spyware itp.) lub luki w systemie zabezpieczeń komputera klienta. Działanie polega na skopiowaniu zbiorów znajdujących się na dysku komputera lub rejestracji sekwencji znaków wpisywanych z klawiatury - w celu przejęcia informacji autoryzacyjnych.

Zabezpieczeniem przed tego typu zagrożeniami jest przestrzeganie zasady nie zapisywania na dysku komputera informacji autoryzacyjnych oraz:

- zgodna z zaleceniami banku konfiguracja przeglądarki internetowej,

- korzystanie z systemu haseł jednorazowych generowanych przez token lub otrzymywanych za pośrednictwem komunikatu SMS,
- właściwa konfiguracja stacji roboczej (wyłączenie zbędnych usług i procesów, stosowanie haseł użytkownika komputera, szyfrowanie partycji dyskowych lub wrażliwych danych),
- zainstalowanie oprogramowania antywirusowego z licencjonowanego źródła i jego właściwe skonfigurowanie oraz aktualizowanie,
- zainstalowanie oprogramowania kontrolującego ruch sieciowy przychodzący i wychodzący ze stacji roboczej klienta, popularnie nazywanego ścianą ogniową „firewall” oraz jego właściwe skonfigurowanie oraz aktualizowanie.

METODA „MAN-IN-THE-MIDDLE” (stanowiąca odmianę phishingu) - potencjalnie niebezpieczna metoda oszustwa, wymagająca ze strony atakującego dobrej znajomości techniki internetowej oraz wykorzystania braku ostrożności klienta. Polega na interaktywnej komunikacji przestępcy z klientem i wykorzystaniu wyłudzonych informacji (zazwyczaj w czasie rzeczywistym) przy pomocy sfałszowanej strony internetowej. Systemy bankowości internetowej są zabezpieczane przed ww. zagrożeniami, między innymi poprzez zastosowanie opisanego wyżej protokołu SSL i systemu haseł jednorazowych o krótkim czasie ważności.

Zabezpieczeniem przed tego typu zagrożeniem jest stosowanie zasad jak w przypadku phishingu oraz kontrola ważności certyfikatu banku w sposób opisany powyżej.

Wszelkie próby wyłudzenia danych autoryzacyjnych powinny zostać jak najszybciej zgłoszone bankowi prowadzącemu rachunek.

Potencjalne zagrożenie dla bezpieczeństwa transakcji internetowych stanowią mogą komputery, do których dostęp fizyczny posiada wielu użytkowników (np. kawiarenki internetowe, biblioteki itp.), ponieważ umożliwia to łatwe instalowanie oprogramowania szpiegującego, przeznaczonego między innymi do przechwytywania sekwencji znaków, wprowadzonych z klawiatury lub wykonania tzw. zrzutów obrazu ekranu. Z powyższego względu nie zaleca się korzystania z bankowości internetowej komputerów takich miejscach. Podobny typ zagrożeń związany jest z korzystaniem z ogólnodostępnych, radiowych sieci internetowych, w których ruch internetowy nie został zabezpieczony kryptograficznie.

W przypadku systemów corporate banking, poza opisanymi wcześniej zasadami, należy zwrócić szczególną uwagę na ich konfigurację i zakres nadanych uprawnień do wprowadzania i akceptowania transakcji (ze względu na większą liczbę użytkowników). Nadane pracownikom uprawnienia powinny wynikać z regulacji wewnętrznych firmy

i zakresów obowiązków poszczególnych pracowników. Niedopuszczalne jest przypisanie tego samego identyfikatora i hasła więcej jak jednej osobie. Należy również weryfikować i aktualizować listę pełnomocników posiadających możliwość dokonywania zmian parametrów rachunku bankowego.

METODA „MAN IN THE BROWSER” – jest to atak skierowany przeciwko przeglądarce www klienta. Polega na modyfikowaniu danych wpisywanych w formularzach, w trakcie pracy w systemie bankowości internetowej. Złośliwy kod dokonujący modyfikacji zapisuje się zazwyczaj na dysku komputera klienta i musi być profilowany pod kątem konkretnego systemu bankowości internetowej. Z tego między innymi względu, główny ciężar ochrony i przeciwdziałania przed tym zagrożeniem spoczywa na bankach.

Ochrona przed zagrożeniem ze strony klienta polega na aktualizacji oprogramowania przeglądarki internetowej, jej konfiguracji zgodnie z zaleceniami banku, aktualizacji oprogramowania antywirusowego oraz okresowej kontroli wyciągów bankowych. W przypadku dokonywania transakcji wychodzących o wysokiej wartości, zaleca się sprawdzenie w opcji historii rachunku lub opcjach pozwalających przeglądać przelewy oczekujące na realizację, kwoty przelewu i numeru rachunku docelowego. W przypadku wykrycia nieprawidłowości należy niezwłocznie anulować transakcję w systemie bankowości internetowej, lub gdy transakcja już została wykonana na rachunku klienta, niezwłocznie zgłosić ją bankowi w celu jej zablokowania na dalszym etapie rozliczenia.

NIEDOSTĘPNOŚĆ USŁUG BANKOWOŚCI INTERNETOWEJ - możliwość korzystania z usług bankowości internetowej przez klienta, uwarunkowana jest (w dużym uproszczeniu) jednoczesnym i właściwym funkcjonowaniem takich elementów jak:

- system internetowy banku,
- system ewidencyjny banku,
- połączenie banku z Internetem,
- sieć internetowa,
- połączenie z Internetem posiadane przez klienta,
- stacja robocza klienta w tym system operacyjny komputera wraz z jego komponentami i przeglądarką internetową.

Niesprawność któregośkolwiek z ww. elementów uniemożliwia wykonanie transakcji. Banki działające w Polsce podejmują działania zmierzające do zapewnienia niezawodności działania serwisów bankowych, jakkolwiek ze względu na dużą złożoność systemu i występujące współzależności, zdarzały się i prawdopodobnie w przyszłości również będą miały miejsce

przerwy w dostępie do usług świadczonych przez Internet. Głównym zadaniem banków jest zatem zapewnienie możliwości szybkiego wznowienia działania na wypadek awarii lub innych negatywnych zdarzeń.

Współpraca ze strony klientów, w tym niezwłoczne sygnalizowanie bankowi wszelkich nieprawidłowości w działaniu systemu lub prób uzyskania nieuprawnionego dostępu do rachunku, stanowią jeden z ważniejszych elementów pozwalających na wzrost poziomu bezpieczeństwa i jakości usług bankowości internetowej.

4. Bankowość telefoniczna

4.1 Charakterystyka bankowości telefonicznej

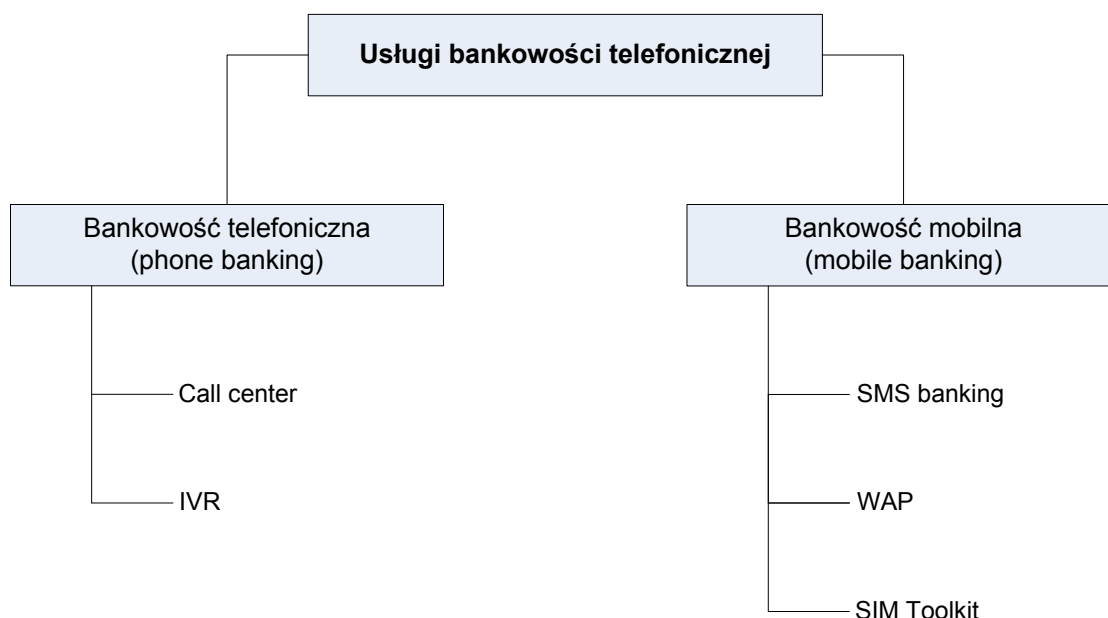
Bankowość telefoniczna jest to usługa polegająca na wykorzystaniu telefonu do obustronnej komunikacji klienta z bankiem.

Wyróżnia się dwa rodzaje bankowości telefonicznej:

- **bankowość telefoniczna (phone banking)**, która wykorzystuje telefony stacjonarne,
- **bankowość mobilna (mobile banking)**, wykorzystująca telefony komórkowe oraz inne urządzenia przenośne.

Usługi te umożliwiają klientom banków dostęp do rachunków bankowych oraz dokonywanie na nich operacji, jak również uzyskiwanie informacji na temat oferowanych produktów bankowych.

W ramach bankowości telefonicznej wykorzystującej telefony stacjonarne banki oferują usługi call center oraz IVR, natomiast do usług z zakresu bankowości mobilnej, w której narzędziem są głównie telefony komórkowe, zalicza się usługi SMS banking, WAP oraz SIM Toolkit.



Rys. 1 Klasyfikacja usług bankowości telefonicznej

4.2 Charakterystyka usług bankowości telefonicznej

Usługi bankowości telefonicznej z wykorzystaniem telefonu stacjonarnego zaliczane są do najstarszych form zdalnej komunikacji klienta z bankiem. Obecnie na polskim rynku oferowane są dwa rozwiązania:

- call center,
- IVR.

Call center jest to serwis telefoniczny banku, obsługiwany przez operatora danego banku z wykorzystaniem dwustronnej komunikacji głosowej, pozwalający na dokonywanie operacji bankowych za pośrednictwem telefonu stacjonarnego.

Zakres oferowanych usług bankowych za pośrednictwem serwisu call center jest zróżnicowany i zależy od oferty poszczególnych banków, niemniej jednak w większości banków istnieje możliwość przeprowadzenia następujących operacji:

- wykonanie przelewu na wcześniej zdefiniowane rachunki odbiorców,
- uzyskanie informacji o saldzie rachunku i historii wykonywanych zleceń,
- zakładanie lokaty,
- obsługa karty kredytowej,
- uzyskanie informacji o ofercie banku.

Klient może oczekiwać ze strony operatora danego banku porady w zakresie możliwych do przeprowadzania w ramach usług bankowości telefonicznej operacji, jak również uzyskać informacje na temat oferowanych produktów bankowych.

Drugim rozwiązaniem świadczenia usług bankowych w ramach bankowości telefonicznej jest wykorzystanie systemów IVR, dostępne dla klientów posiadających telefony stacjonarne pracujące w systemie tonowym.

IVR (Interactive Voice Response) jest 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.

Z punktu widzenia zastosowanych technologii systemy IVR mogą pracować jako²¹:

- systemy reagujące na głos (voice response),
- systemy rozpoznawania głosu (voice recognition).

Systemy reagujące na głos analizują wysokość dźwięków, które wydają klawisze telefonu z wybieraniem tonowym, i w zależności od wybranej sekwencji wykonywane są odpowiednie operacje bankowe.

System rozpoznawania głosu jest bardziej zaawansowany technologicznie od systemu reagującego na głos. Analizuje on wydane głosem polecenia i stara się wykonać żądane operacje, a także automatycznie generuje odpowiedzi w postaci syntezy mowy.

W zakresie obsługi realizowanej za pośrednictwem systemu IVR klient ma możliwość:

- uzyskania informacji o saldzie i kwocie dostępnych środków pieniężnych na rachunku,
- zlecenie otwarcia lub zamknięcia rachunku terminowej lokaty oszczędnościowej,
- zlecenie wykonania przelewu na wcześniej zdefiniowane rachunki odbiorców.

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.

4.3 Charakterystyka usług bankowości mobilnej

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)**.

Bankowość mobilna stała się w ostatnich latach bardzo popularna, dlatego niemal wszystkie znaczące banki posiadają ją w swojej ofercie. Najpowszechniej wykorzystywanymi formami świadczenia usług z zakresu bankowości mobilnej są:

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

²¹ Bankowość elektroniczna, pod red. Andrzeja Gospodarowicza, PWE, Warszawa 2005, s. 107

SMS Banking (Short Messaging Service Banking) polega na wykorzystywaniu krótkich informacji tekstowych SMS zarówno w formie otrzymywania przez klienta powiadomień z banku (usługa push), jak i samodzielnego zlecenia przez klienta określonych operacji bankowych (usługa pull).

Usługi typu push umożliwiają otrzymywanie wiadomości SMS, informujących o zdarzeniach, jakie wystąpiły na rachunku bankowym danego klienta. Wiadomości są wygenerowane i wysyłane automatycznie przez system bankowy i mogą powiadamiać klienta o następujących zdarzeniach:

- zrealizowanie przelewu,
- odrzucenie przelewu,
- zmiana salda,
- wystąpienie debetu.

Usługi typu pull umożliwiają wysyłanie do banku wiadomości SMS w odpowiedniej postaci, w celu wykonania określonych operacji, jakimi mogą być:

- uzyskanie informacji o saldzie rachunku,
- wykonanie przelewu (na wcześniej zdefiniowane rachunki odbiorców),
- uzyskanie informacji o predefiniowanym rachunku klienta,
- otrzymanie wykazu ostatnio przeprowadzonych operacji.

Inną formą świadczenia usług z zakresu bankowości mobilnej jest **usługa WAP**, która pozwala na wykonywanie operacji bankowych za pomocą telefonu komórkowego przy wykorzystaniu Internetu. Funkcjonalność tej usługi jest bardzo zbliżona do bankowości internetowej.

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.

Warunkiem korzystania z tej formy dostępu do rachunku bankowego jest posiadanie telefonu komórkowego wyposażonego w protokół WAP, który pozwala na korzystanie z sieci Internet. Do swojego konta klient loguje się najczęściej tak samo, jak do serwisu internetowego danego

banku za pomocą loginu i hasła maskowanego²². Wystarczy uruchomić przeglądarkę internetową w telefonie komórkowym i wpisać odpowiedni adres strony internetowej banku, żeby móc przejść do procesu logowania.

Technologia WAP umożliwia klientom banku sprawowanie stałej kontroli nad rachunkiem i zdalne zarządzania własnymi środkami finansowymi. W ramach usługi WAP możliwe są następujące operacje bankowe:

- dostęp do informacji o saldzie i obrotach na rachunku,
- wykonanie przelewu na wcześniej zdefiniowane rachunki,
- definiowanie zlecenia stałego,
- dyspozycja przelewu z przyszłą datą realizacji,
- zakładanie lokat terminowych,
- zmiana hasła dostępu.

Podobnym funkcjonalnie do usługi WAP rozwiązaniem, umożliwiającym zdalne wykonywanie operacji bankowych za pośrednictwem telefonu komórkowego jest usługa **SIM Toolkit**, która polega na korzystaniu ze specjalnie zaprojektowanej aplikacji bankowej.

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.

Rozwiązanie bazuje na współpracy banków z operatorami sieci komórkowych, zaś dostarczona przez bank aplikacja umożliwia łatwe przeglądanie danych w telefonie komórkowym i bezpośrednio składanie różnych zleceń bankowych. Warunkiem korzystania z tego typu usługi jest posiadanie odpowiedniego telefonu komórkowego dostosowanego do wymagań aplikacji oferowanej przez bank. Większość tzw. inteligentnych telefonów (smartfonów), w tym urządzenia działające pod kontrolą systemów Symbian, Windows CE, Android i iPhone OS, dostępnych obecnie na rynku spełnia minimalne wymagania takich aplikacji. W praktyce oznacza to, że po zainstalowaniu dostarczonej aplikacji bankowej w menu telefonu pojawia się dodatkowa ikona, poprzez którą właściciel telefonu uzyskuje

²² Hasło maskowane różni się od zwyczajnego hasła tym, że nie podaje się go w całości, ale wpisuje się tylko wybrane przez system znaki. System może poprosić o wpisanie np. pierwszego, czwartego i ósmego znaku i na tej podstawie zweryfikuje klienta.

dostęp do usług danego banku, a następnie może realizować operacje bankowe. Usługa pozwala na zarządzanie posiadanym poprzez klienta rachunkiem bankowym oraz kartami kredytowymi. Klient może dokonywać w ten sposób różnych czynności, w tym sprawdzać saldo rachunku i wykonywać przelewy na wcześniej zdefiniowane rachunki. W przypadku kart kredytowych klient może sprawdzać dostępny limit, historię operacji, dokonywać spłaty zadłużenia na karcie ze swojego rachunku bankowego, jak również zastrzec kartę.

4.4 Bezpieczeństwo w bankowości telefonicznej

Korzystając z usług bankowości telefonicznej możemy być narażeni na działania przestępców podszywających się pod bank. Należy zatem pamiętać o kilku podstawowych zasadach bezpieczeństwa, kontaktując się drogą telefoniczną z daną instytucją finansową.

Główną zasadą bezpieczeństwa w bankowości telefonicznej jest korzystanie tylko z oficjalnych numerów telefonów dostępnych na stronach internetowych banków, w oficjalnych materiałach reklamowych (np. ulotkach otrzymanych w placówkach banków), jak także oficjalnych wizytówkach oraz wyciągach bankowych. przesyłanych na wskazany przez klienta adres.

Szczególnie trzeba zwrócić uwagę na nową formę oszustwa, stosowaną wobec użytkowników bankowości telefonicznej, jaką jest tzw. **VISHING** (została ujawniona w Stanach Zjednoczonych już w 2006 r.)²³. Do klienta banku dzwonił telefon, a po jego odebraniu odzywał się lektor, który informował o problemie z autoryzacją transakcji, blokadą karty lub dostępem do rachunku. Nagrany głos prosił klienta o natychmiastowy kontakt z bankiem, celem wyjaśnienia zaistniałej sytuacji, podając fałszywy numer infolinii, podszywającej się pod instytucję finansową. Po wybraniu tego numeru, klient był proszony o potwierdzenie (tonowo albo w rozmowie z doradcą) numeru swojej karty, kodu PIN do karty albo numeru swojego rachunku oraz loginu i hasła do usług bankowości elektronicznej. Dane takie umożliwiały przestępcy nieograniczony dostęp do środków oszukanego klienta.

Nie należy podawać osobom trzecim ustanowionego hasła (np. do logowania się do usług bankowości elektronicznej, PIN-u do karty kredytowej) - żaden automatyczny serwis telefoniczny lub doradca banku nie może żądać od klienta takich informacji. Wyjątkiem są hasła, które klient ustanowił w obecności pracownika banku, przeznaczone bezpośrednio do kontaktu telefonicznego z bankiem.

²³ Opinie klientów w Stanach Zjednoczonych, którzy doświadczyli tej formy oszustwa dostępne są na stronie serwisu BBC: <http://news.bbc.co.uk/2/hi/technology/5187518.stm>

W razie wątpliwości, dotyczących tożsamości osoby, podającej się za przedstawiciela lub doradcę banku warto poprosić dzwoniącego o jego nazwisko oraz ogólnodostępny numer telefonu (np. taki, który można znaleźć w materiałach reklamowych czy na stronie internetowej banku), pod którym można się z nim zwrotnie skontaktować. Weryfikacja prawdziwości numeru, który otrzymaliśmy od doradcy (np. na stronach internetowych banku) może uchronić nas przed oszustwem.

Nawiązywanie połączenia z bankiem w miejscach publicznych, pomieszczeniach, gdzie przebywa dużo osób, zatłoczonych środkach komunikacji itp. może być obciążone ryzykiem. Podczas komunikacji z bankiem należy zapewnić sobie odpowiednie warunki do rozmowy telefonicznej, ze względu na poufność przekazywania danych.

4.5 Bezpieczeństwo w bankowości mobilnej

Wraz z postępem technologicznym telefon komórkowy w coraz większym stopniu upodabnia się do klasycznego urządzenia komputerowego, co oznacza, że obok licznych korzyści, takich jak np. większa funkcjonalność urządzenia, uniwersalność jego zastosowań i przyjazna interakcja z użytkownikiem, mogą się także pojawić dodatkowe ryzyka. Rośnie bowiem liczba zagrożeń dla bezpiecznego korzystania z telefonu komórkowego jako uniwersalnego urządzenia komunikacji bezprzewodowej, umożliwiającego dostęp do rachunku bankowego.

Krytycznym czynnikiem decydującym o bezpieczeństwie korzystania z usług bankowości mobilnej jest spełnienie minimalnych wymagań dotyczących zabezpieczenia wykorzystywanego telefonu komórkowego oraz praktyki jego stosowania²⁴.

Coraz większym zagrożeniem dla użytkowników tzw. inteligentnych telefonów komórkowych (smartfonów) staje się **OPROGRAMOWANIE ZŁOŚLIWE**, takie jak wirusy, robaki internetowe, oprogramowanie szpiegujące, wytrychy czy „konie trojańskie”. Już teraz pod pojęciem bezpiecznego smartfona rozumie się takie urządzenie, które obowiązkowo posiada zainstalowane dobre oprogramowanie antymalware.

Tworzenie i propagowanie oprogramowania złośliwego przeznaczonego do infekowania telefonów komórkowych nie jest jeszcze tak powszechne, jak w przypadku komputerów, ale wykazuje stałą tendencję wzrostową. Zagrożenie, wynikające z infekcji telefonu oprogramowaniem złośliwym ma taki sam charakter jak w przypadku klasycznych

²⁴ Źródło : <http://www.mobilnybank.pl>

komputerów. Zainfekowanie telefonu oznacza ryzyko kradzieży poświadczeń tożsamości (loginów i haseł) nie tylko w bankowości mobilnej, lecz również ryzyko ujawnienia numerów kart kredytowych, PIN-ów i innych wrażliwych danych. W pewnych przypadkach wiąże się także z poważnym ryzykiem podmiany danych transakcyjnych np. kont beneficjentów zlecanych przelewów.

Telefon komórkowy, wyposażony w interfejsy sieciowe w postaci wbudowanego modemu GSM lub bezprzewodowej karty sieciowej (WiFi) od chwili nawiązania połączenia z Internetem staje się, podobnie jak komputer, potencjalnym celem ataków ze strony hackerów lub oprogramowania złośliwego, dlatego powinien być wyposażony w skuteczną osobistą zaporę sieciową.

Brak ochrony przed atakami z sieci może skutkować infekcją telefonu oprogramowaniem złośliwym ze wszystkimi szkodliwymi skutkami, opisanymi wcześniej, lub wyprowadzeniem poufnych danych. Środkiem zaradczym jest instalacja na smartfonie zintegrowanego pakietu zabezpieczeń, obejmującego jako minimum skaner antywirusowy i osobistą zaporę sieciową. Dostępne na rynku produkty tego rodzaju na ogół oferują dodatkowo ochronę w zakresie kontroli procesów, przeciwdziałania atakom z Internetu i czasem także szyfrowania plików.

Aplikacje instalowane na telefonie komórkowym powinny być podpisane cyfrowo przez dostawcę. Pozwala to na zweryfikowanie wiarygodnego pochodzenia aplikacji, jak również jej integralności, czyli sprawdzenie, czy nikt nie ingerował w jej kod od momentu skompilowania aplikacji przez zaufanego dostawcę.

Na telefonie komórkowym nie należy instalować oprogramowania pochodzącego **Z NIEZAUFANYCH ŹRÓDEŁ** (np. nielegalnego oprogramowania poddanego przeróbkom w celu złamania zabezpieczeń praw autorskich i licencyjnych). Pamiętajmy, że takie oprogramowanie nierzadko posiada wbudowane w kod funkcje tylnych wejść (ang: *backdoors*), które mogą być wykorzystane przez agresorów do złamania zabezpieczeń telefonu, wygenerowania wysokich rachunków za transfer danych, zainstalowania oprogramowania złośliwego albo wyprowadzenia wrażliwych danych z pamięci telefonu.

Jednym z najpoważniejszych źródeł podatności i luk w bezpieczeństwie każdego rodzaju oprogramowania są jego usterki i wady. Przeważnie są to wady istniejące na poziomie kodu aplikacji. Producenci oprogramowania usuwają ujawnione w nim błędy i usterki poprzez przygotowywanie dla użytkowników odpowiednich poprawek oraz aktualizacji, czyli tzw. łatek (ang. *patches*).

System operacyjny telefonu komórkowego wraz z oprogramowaniem standardowym także może wymagać okresowych aktualizacji, w celu usuwania błędów i luk w zabezpieczeniach. Dotyczy to zwłaszcza otwartych platform takich jak Windows Mobile, Symbian itp. Aktualizacja nie zawsze jest czynnością łatwą do wykonania dla właściciela telefonu. W niektórych modelach telefonów taką operację można bezpiecznie przeprowadzić jedynie w odpowiednich, specjalistycznych punktach usługowych, nierzadko z autoryzacją producenta. Niewłaściwie przeprowadzona aktualizacja systemowego oprogramowania telefonu może doprowadzić do nieodwracalnej utraty cennych danych, a nawet awarii telefonu.

Użytkownik telefonu komórkowego przed podjęciem ewentualnej decyzji o aktualizacji oprogramowania systemowego powinien zrobić zapasową kopię danych, które zapisane są w pamięci telefonu.

Aktualizację oprogramowania systemowego można przeprowadzić we własnym zakresie jedynie wówczas, gdy jest to operacja bezpieczna, użytkownik wie, jak ją wykonać oraz ma do dyspozycji oprogramowanie narzędziowe udostępnione przez producenta telefonu i inne niezbędne akcesoria. Oprogramowanie aktualizujące musi pochodzić z wiarygodnego źródła i nie może naruszać warunków gwarancji. To, czy należy przeprowadzać aktualizację oprogramowania systemowego i jak często ją robić, zależy od konkretnej platformy programowej smartfona. Zalecane jest śledzenie doniesień o bezpieczeństwie wykorzystywanego przez siebie rodzaju smartfona oraz instalowanie aktualizacji i łatek rekomendowanych przez producentów.

O bezpieczeństwie telefonu komórkowego oraz zapisanych w jego pamięci danych decyduje także jego ochrona przed zagubieniem i kradzieżą.

Wrażliwe dane (na przykład hasła, numery kart kredytowych, numery PIN itp.) zapisane w pamięci telefonu lub na karcie pamięci muszą być zabezpieczone przed ujawnieniem i nieuprawnionym wykorzystaniem. W praktyce zabezpieczenia takie sprowadzają się do ich zaszyfrowania. Na rynku dostępnych jest wiele produktów, umożliwiających szyfrowanie wrażliwych danych w telefonie komórkowym.

W razie potrzeby przechowywania w pamięci telefonu danych niezbędnych do korzystania z bankowości mobilnej oraz innych wrażliwych danych (na przykład haseł czy poufnych notatek) należy stosować oprogramowanie szyfrujące do szyfrowania baz haseł lub plików czy też pamięci telefonu. Oferta tego typu oprogramowania jest dość bogata dla wszystkich

popularnych platform smartfonów. Obejmuje ona również oprogramowanie dostępne bezpłatnie.

Spośród usług z zakresu bankowości mobilnej najbardziej bezpiecznym rozwiązaniem komunikacji klienta z bankiem wydaje się być zastosowanie technologii SIM Toolkit. Dostęp do aplikacji bankowej w menu telefonu komórkowego można uzyskać tylko po wpisaniu poufnego kodu PIN, a kilkakrotne wprowadzenie złego kodu powoduje blokadę aplikacji, którą zdalnie może usunąć tylko bank. W przypadku dokonywania przelewów każda transakcja potwierdzana jest poprzez podanie dodatkowego kodu. Komunikacja z bankiem szyfrowana jest algorytmem symetrycznym 3 DES, co oznacza, że w żadnym przypadku operator sieci komórkowej nie ma możliwości ingerencji w transmisję danych. Ponadto, w razie pojawienia się niebezpieczeństwa korzystanie z usługi może być też w każdej chwili zablokowane przez operatora lub bank.

5. Obecny stan świadczenia usług bankowości elektronicznej w Polsce²⁵

W Polsce jest kilka instytucji monitorujących rynek bankowości elektronicznej. Dane, dotyczące kart płatniczych zbiera²⁶ Narodowy Bank Polski (NBP), a z kolei dane dot. usług bankowości elektronicznej - ale tylko w odniesieniu do bankowości internetowej i home/corporate banking oraz bankowości mobilnej - Związek Banków Polskich (ZBP). Badania statystyczne w tym zakresie prowadzone są przez GUS i ośrodki badania opinii społecznej. Analizy rynku usług bankowości elektronicznej wskazują na wzrost popularności usług elektronicznych oraz skali ich wykorzystania. Tego typu badania rzadko są jednak upowszechniane a przekazy medialne koncentrują się głównie na przypadkach dużych awarii lub nadużyć wykonywanych z wykorzystaniem systemów bankowości elektronicznej. W znacznie mniejszym stopniu akcentowane są niewątpliwe korzyści wynikające ze stosowania elektronicznych form rozliczeń. Należy wymienić tu m.in. czas, którego nie tracimy stojąc w kolejkach do kas bankowych np. w celu zapłaty rachunku czy spłaty raty kredytu.

Według danych ZBP na koniec 2009 roku liczba indywidualnych klientów banków, którzy zawarli umowy o usługi bankowości internetowej wynosiła 13,3 mln a klientów aktywnych, czyli takich, którzy wykonali w miesiącu przynajmniej jedną operację za pośrednictwem Internetu było 7,4 mln²⁷ (należy zwrócić przy tym uwagę, że jedna osoba może być klientem kilku banków). ZBP prognozuje, że na koniec 2010 r. liczba aktywnych klientów indywidualnych oraz małych firm korzystających z usług bankowości internetowej wyniesie ok. 10 mln.

²⁵ Przedstawiony w Raporcie ogólny opis stanu świadczenia usług bankowości elektronicznej w Polsce przygotowany został głównie na podstawie danych NBP, EBC oraz badania ankietowego przeprowadzonego przez UKNF wśród krajowych banków komercyjnych. Z powodu braku dostępności danych część banków nie udzieliła odpowiedzi na wszystkie pytania zawarte w ankiecie, toteż w Raporcie dla potrzeb analizy danych nie można było przyjąć stałej wielkości próby.

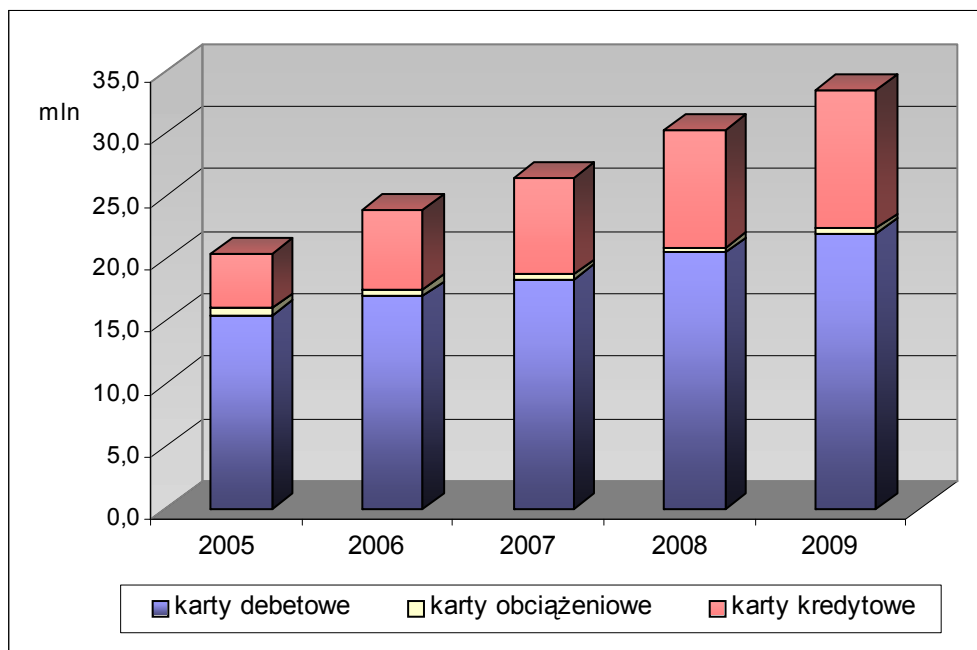
²⁶ Na podstawie Rozporządzeń Ministerstwa Finansów.

²⁷ Na podstawie danych zbieranych przez ZBP z 25 banków komercyjnych oraz 11 banków spółdzielczych, stanowiących łącznie 95% sektora.

5.1 Bankowość terminalowa

Rynek kart płatniczych należy do najbardziej dynamicznie rozwijających się usług bankowych w kraju. Liczba wyemitowanych kart płatniczych w latach 2005-2009, z podziałem na poszczególne rodzaje kart, przedstawiona została na wykresie nr 1.

Wykres 1. Liczba wyemitowanych kart płatniczych w Polsce w latach 2005 - 2009



Źródło: Opracowanie własne na podstawie danych NBP

W 2009 roku wyemitowano w Polsce 33,4 mln kart płatniczych (wzrost o 10,3 % w stosunku do 2008 roku). Największy udział w emisji kart stanowiły karty debetowe (65,8 %) i karty kredytowe (33,1 %). Liczba wyemitowanych kart obciążeniowych była niewielka (1,1 %). Można zauważyć, że procentowy udział kart debetowych w ogólnej liczbie kart systematycznie spada (w 2009 roku udział ten zmniejszył się o 1,7 %). Zwiększa się za to udział kart kredytowych (w 2009 wzrost o 1,9 %). Większa liczba kart kredytowych automatycznie wpływa na wzrost liczby płatności bezgotówkowych (karty tego typu są rzadziej wykorzystywane do dokonywania wypłat z bankomatów).

Liczba wyemitowanych kart płatniczych wg technologii zapisu w latach 2005-2009 przedstawiona została w tabeli nr 1.

Tabela nr 1. Liczba kart płatniczych wyemitowanych wg technologii zapisu danych w latach 2005 – 2009

Podział kart		2005	2006	2007	2008	2009
Karty wyposażone tylko w pasek magnetyczny	Liczba w tys. szt.	19 737,96	22 483,68	24 455,99	25 311,84	25 277,36
	Udział w %	96,90%	94,28%	92,18%	83,61%	75,73%
Karty wyposażone w pasek magnetyczny i mikroprocesor	Liczba w tys. szt.	584,36	1 308,82	1 977,88	4 879,90	8 019,86
	Udział w %	2,90%	5,49%	7,58%	16,12%	24,01%
Karty wyposażone tylko w mikroprocesor	Liczba w tys. szt.	15,8	16,7	12,6	15,4	17,3
	Udział w %	0,10%	0,07%	0,05%	0,05%	0,00%
Karty wirtualne	Liczba w tys. szt.	32,2	38,9	49,7	68,3	86,6
	Udział w %	0,20%	0,16%	0,19%	0,23%	0,26%

Źródło: Opracowanie własne na podstawie danych NBP

W Polsce ciągle dominują karty z paskiem magnetycznym, których udział w ogólnej liczbie wyemitowanych kart płatniczych w 2009 roku wyniósł 75,7 %. Systematycznie rośnie liczba kart, które oprócz paska magnetycznego wyposażone są w mikroprocesor. Na koniec 2009 r. stanowiły one 24 % liczby wszystkich wyemitowanych w tym roku kart a ich liczba szybko się zwiększa (w 2009 roku nastąpił przyrost o 64,3 %). Wciąż niewiele jest kart zaopatrzonych tylko w mikroprocesor (w 2009 roku wyemitowano ich tylko 17,3 tys., co stanowiło znikomy udział w całkowitej liczbie wyemitowanych w tym roku kart płatniczych). Fakt ten wynika z braku pełnej zgodności infrastruktury bankomatów i terminali POS ze standardem EMV (nie można wówczas zapłacić kartą wyposażoną tylko w mikroprocesor).

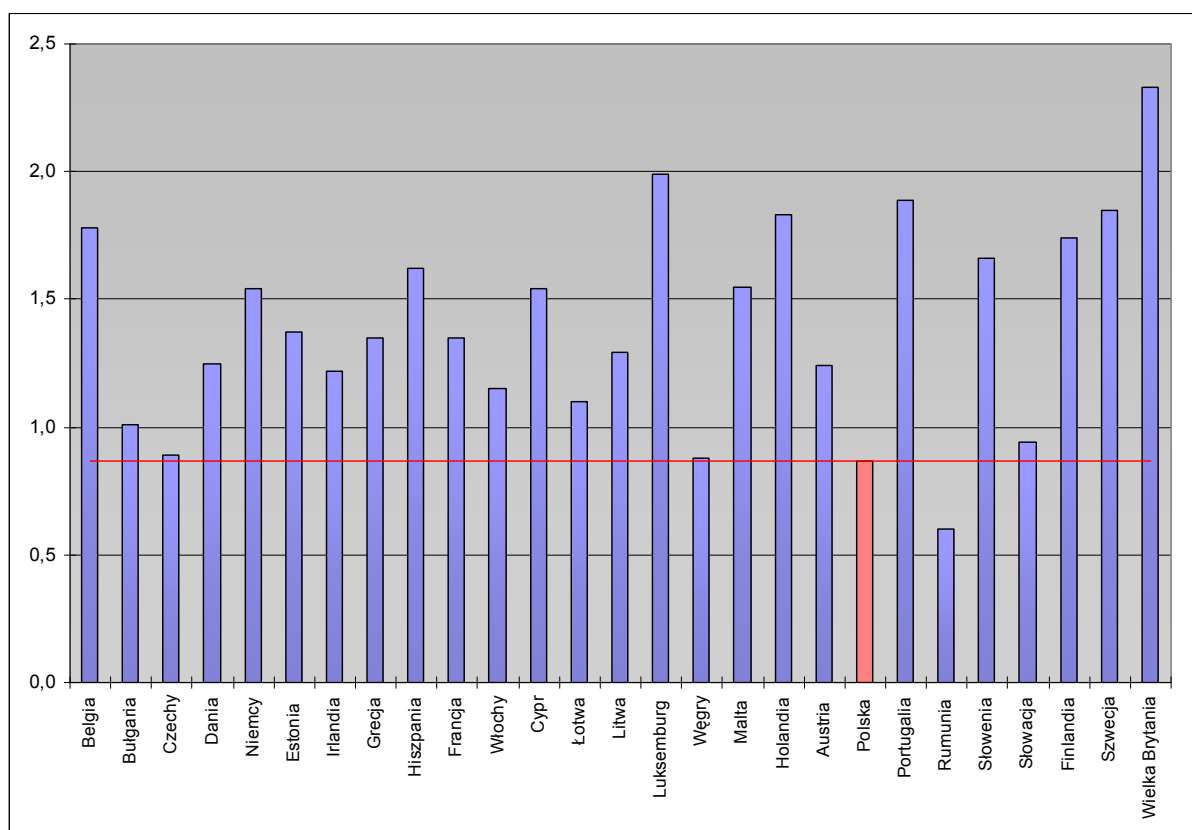
Zgodnie z wymogami SEPA (Single Euro Payments Area - Jednolity Obszar Płatności w Euro) wszystkie europejskie banki powinny dostosować się do standardów EMV do końca 2010 co oznacza, że od 1 stycznia 2011 r. wszystkie karty płatnicze wydane przez banki powinny być wyposażone w mikroprocesor.

Od 2004 roku na rynku polskim funkcjonują również tzw. karty wirtualne, przeznaczone przede wszystkim do dokonywania płatności w Internecie lub innych płatności dokonywanych bez fizycznego przedstawienia karty. W 2009 r. wyemitowano 86,6 tys. kart wirtualnych, co stanowiło zaledwie 0,3 % wszystkich wyemitowanych w tym roku kart płatniczych.

Bardzo szybko rozwija się w Polsce rynek kart bezstykowych (zbliżeniowych). Szacuje się, że do końca 2010 roku znajdzie się na rynku 2 mln kart zbliżeniowych pozwalających na dokonywanie płatności do 50 zł bez podawania PIN-u²⁸.

Pomimo wzrostu liczby emitowanych w naszym kraju kart płatniczych, pod względem liczby kart płatniczych na jednego mieszkańca Polska plasuje się na końcu statystyk w porównaniu z innymi krajami UE (wykres nr 2). Na jednego mieszkańca Polski przypadało w 2009 r. 0,87 wyemitowanych kart, podczas gdy przykładowo w Wielkiej Brytanii wskaźnik ten wynosił 2,33.

Wykres 2. Liczba wyemitowanych kart płatniczych w przeliczeniu na jednego mieszkańca w poszczególnych krajach UE w 2009 roku

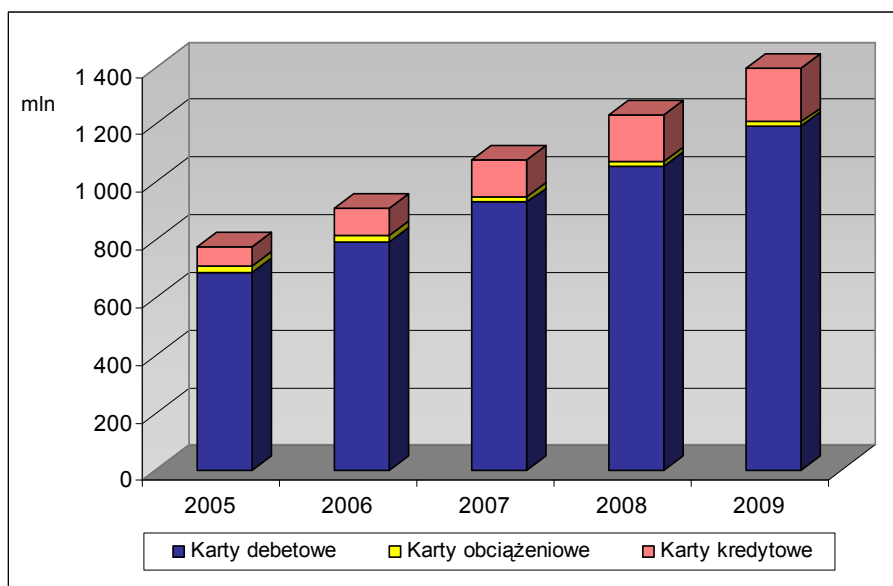


Źródło: Opracowanie własne na podstawie danych ECB

Podobne wnioski nasuwają się po analizie danych dotyczących korzystania z kart płatniczych. W 2009 roku za pomocą kart płatniczych zrealizowanych zostało łącznie 1 394 mln transakcji (wzrost o 13,1 % w stosunku do 2008 r.), z czego najwięcej dokonanych zostało za pomocą kart debetowych (85,5 %), następnie kredytowych (13,4 %) a najmniej za pomocą kart obciążeniowych (1,1%). Liczba transakcji dokonanych za pomocą kart płatniczych w Polsce w latach 2005-2009 przedstawiona została na wykresie nr 3.

²⁸ Źródło: <http://www.idg.pl/news/359724/Rewolucja.w.bankach.coraz.wiecej.kart.zblizeniowych.html>

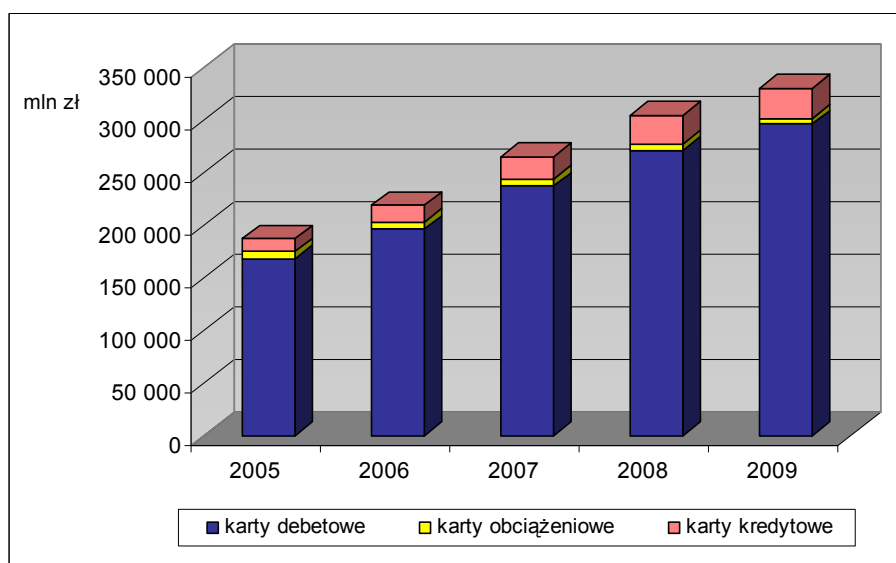
Wykres 3. Liczba transakcji dokonanych za pomocą kart płatniczych w Polsce w latach 2005-2009



Źródło: Opracowanie własne na podstawie danych NBP

Wartość transakcji dokonanych za pomocą kart płatniczych w Polsce w latach 2005-2009 (wykres nr 4), podobnie jak liczba transakcji, ma tendencję wzrostową. Wartość wszystkich transakcji dokonanych kartami bankowymi w 2009 roku wyniosła 330,4 mld zł (wzrost o 8,6 % w stosunku do 2008 r.), przy czym udział transakcji przy wykorzystaniu kart debetowych stanowił 89,6%, kart kredytowych 8,8 % a kart obciążeniowych 1,6 %. Średnia wartość jednej transakcji dokonanej w 2009 roku za pomocą karty płatniczej wyniosła 237 zł.

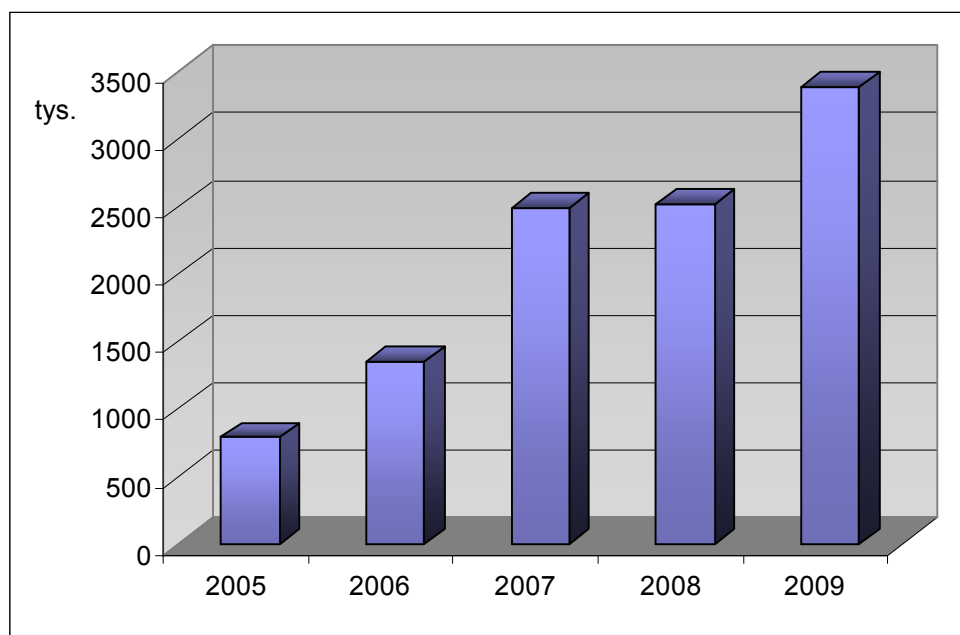
Wykres 4. Wartość transakcji dokonanych za pomocą kart płatniczych w Polsce w latach 2005-2009



Źródło: Opracowanie własne na podstawie danych NBP

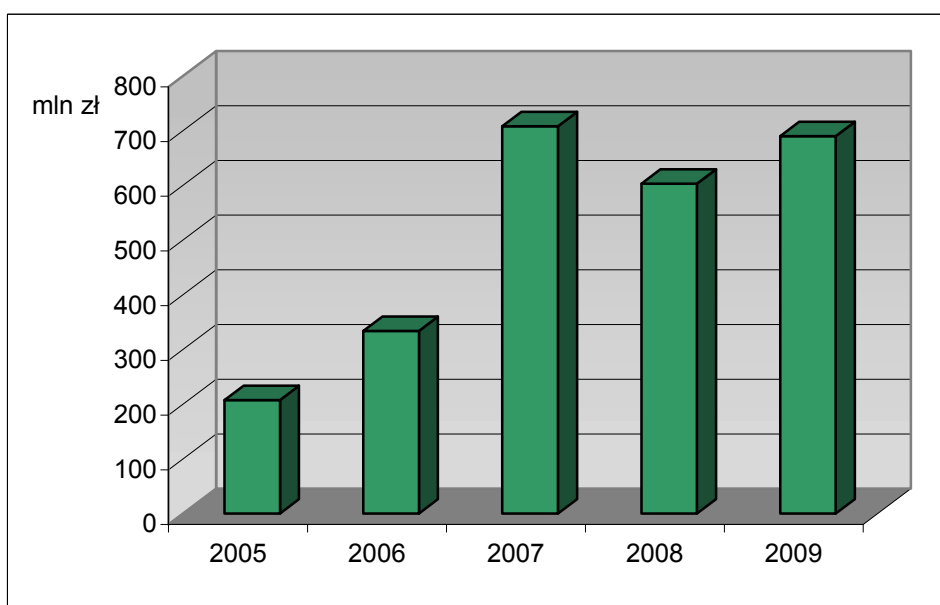
Liczba i wartość transakcji kartowych w Polsce przy sprzedaży towarów i usług w Internecie w latach 2005-2009 przedstawiona została na wykresach nr 5 i 6. W 2009 roku liczba dokonanych transakcji w Internecie wyniosła 3,39 mln (wzrost o 34,7 % w stosunku do 2008 roku) a ich wartość 690,6 mln zł (wzrost o 14,9 % w stosunku do roku poprzedniego).

Wykres 5. Liczba transakcji dokonanych w Internecie za pomocą kart płatniczych w Polsce w latach 2005-2009



Źródło: Opracowanie własne na podstawie danych NBP

Wykres 6. Wartość transakcji dokonanych w Internecie za pomocą kart płatniczych w Polsce w latach 2005-2009

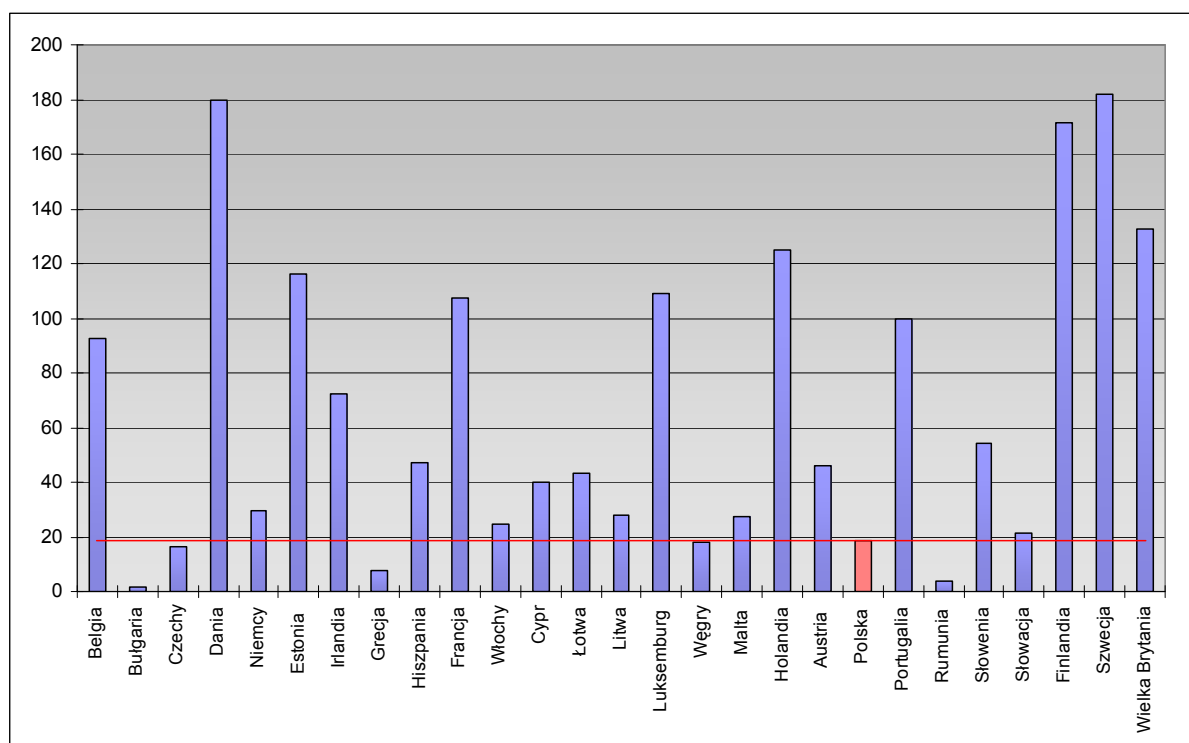


Źródło: Opracowanie własne na podstawie danych NBP

Na podstawie danych NBP można stwierdzić, że posiadacze kart płatniczych coraz częściej wykorzystują je do dokonywania płatności bezgotówkowych. Według statystyk NBP w II półroczu 2009 r. po udział transakcji bezgotówkowych w ogólnej liczbie transakcji dokonanych kartami płatniczymi raz pierwszy przekroczył połowę i wynosił 51,9 %.

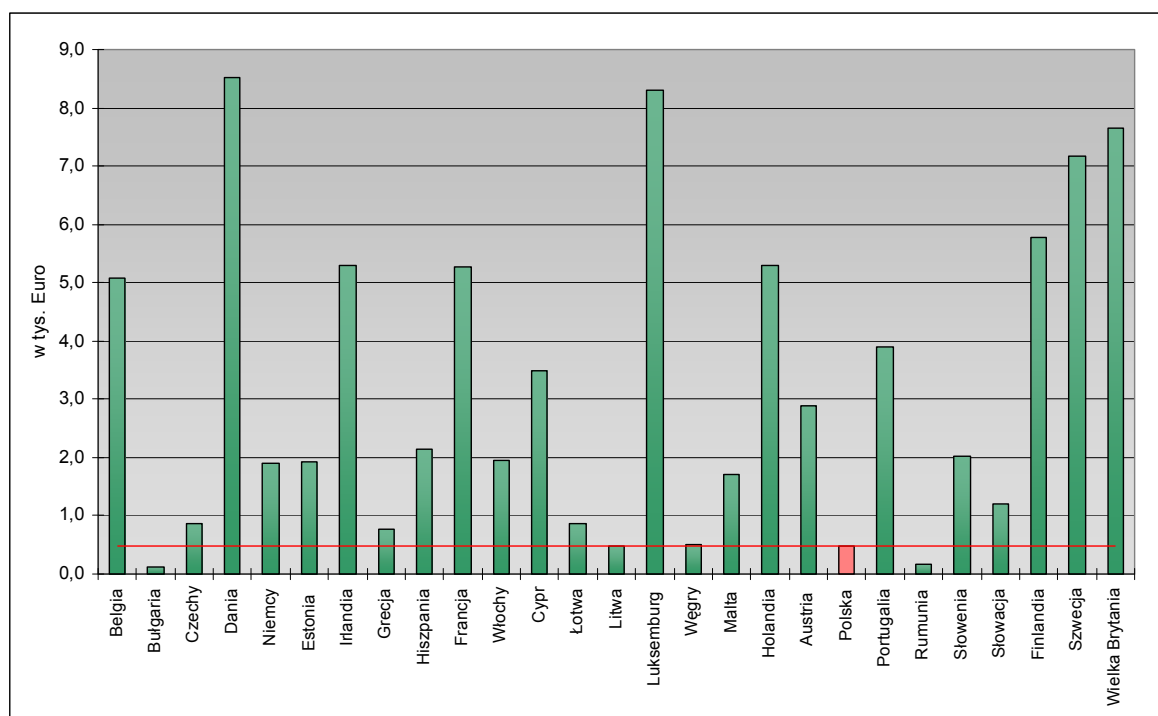
Interesująco wygląda wykorzystanie kart płatniczych w Polsce na tle innych krajów UE. Na wykresach nr 7 i 8 przedstawiona została liczba oraz wartość transakcji dokonanych kartami bankowymi w przeliczeniu na jednego mieszkańca. Wykres pokazuje, że stopień wykorzystania kart płatniczych w Polsce jest stosunkowo niski w porównaniu z innymi krajami UE. W 2009 roku statystyczny Polak przeprowadził 18 transakcji za pomocą kart płatniczych, a np. w Finlandii na jednego mieszkańca przypadało 171 takich transakcji. Podobnie wyglądała sytuacja Polski pod względem wartości transakcji dokonywanych za pomocą kart. Wartość transakcji dokonanych w 2009 roku w przeliczeniu na jednego mieszkańca Polski wynosiła 0,47 tys. euro, a przykładowo w Dani wartość takich transakcji wyniosła 8,5 tys. euro.

Wykres 7. Liczba transakcji dokonanych za pomocą kart płatniczych w przeliczeniu na jednego mieszkańca w poszczególnych krajach UE w 2009 roku



Źródło: Opracowanie własne na podstawie danych ECB

Wykres 8. Wartość transakcji dokonanych za pomocą kart płatniczych w przeliczeniu na jednego mieszkańca w poszczególnych krajach UE w 2009 roku



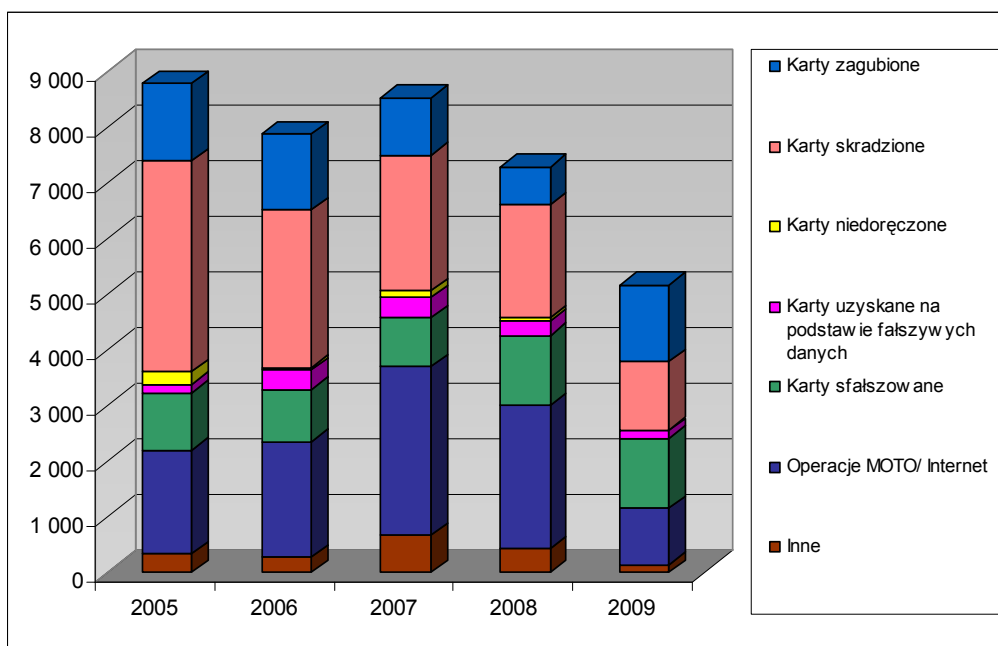
Źródło: Opracowanie własne na podstawie danych ECB

Mimo coraz większej popularności kart płatniczych liczba oszustw kartowych w Polsce maleje od 2007 roku (wykres nr 9). W 2009 roku dokonano 5167 takich przestępstw (spadek o 29% w stosunku do 2008 roku). Największą liczbę oszustw (1371) stanowiły te, które były skutkiem zagubienia kart przez ich posiadaczy - w stosunku do roku poprzedniego wzrosły o 98,9 %. Na drugim miejscu najczęstszych oszustw są oszustwa dokonane za pośrednictwem sfalszowanych kart (1251), których liczba w 2009 r. spadła o 1,3 % w porównaniu do roku poprzedniego. Trzecią co do wielkości liczbę oszustw kartowych stanowiły oszustwa w wyniku kradzieży kart (1234), ale w stosunku do 2008 roku nastąpił ich znaczący spadek o 39,1 %. Istotny udział w oszustwach kartowych (1021) miały także oszustwa w wyniku przeprowadzanych operacji MOTO (Internet), choć ich liczba również spadła o 60 % w stosunku do 2008 roku.

Wraz ze spadkiem liczby oszustw kartowych zmniejszyła się również ich wartość – zarówno średnia jak i ogółem. W 2009 roku spadła o 32,3 %, do 4,73 mln zł. Największą wartość oszustw stanowiły operacje dokonane za pośrednictwem kart sfalszowanych (2,06 mln zł; spadek o 22,6 % w stosunku do roku poprzedniego). Drugą znaczną wartość oszustw kartowych (1,09 mln zł) stanowiły w 2009 r. oszustwa dokonane za pośrednictwem kart skradzionych, niemniej jednak w porównaniu do 2008 r. nastąpił ich znaczny spadek o 35,5 %. Istotną pozycję w 2009 r. stanowiły także oszustwa w wyniku przeprowadzanych

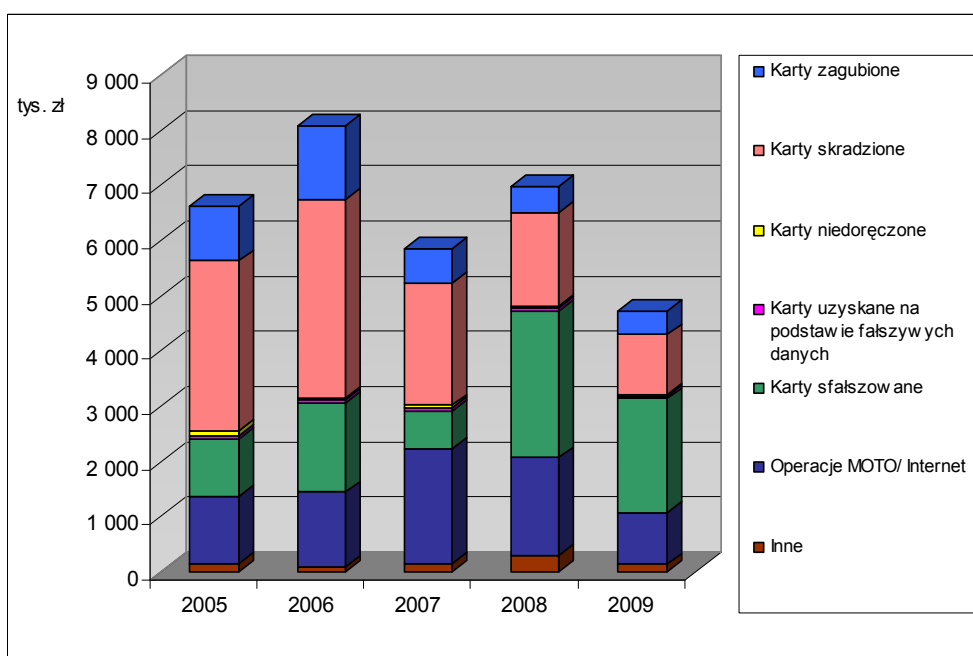
operacji MOTO (Internet), których wartość wyniosła 938,5 tys. zł. Obniżyła się średnia nominalna wartość oszustw kartowych - z 953,9 zł 2008 r. do 915,5 zł w 2009 r.

Wykres 9. Liczba oszustw kartowych w Polsce w latach 2005-2009



Źródło: Opracowanie własne na podstawie danych NBP przekazywanych przez agentów rozliczeniowych

Wykres 10. Wartość oszustw kartowych w Polsce w latach 2005-2009



Źródło: Opracowanie własne na podstawie danych NBP przekazywanych przez agentów rozliczeniowych

Bankomaty i terminale POS

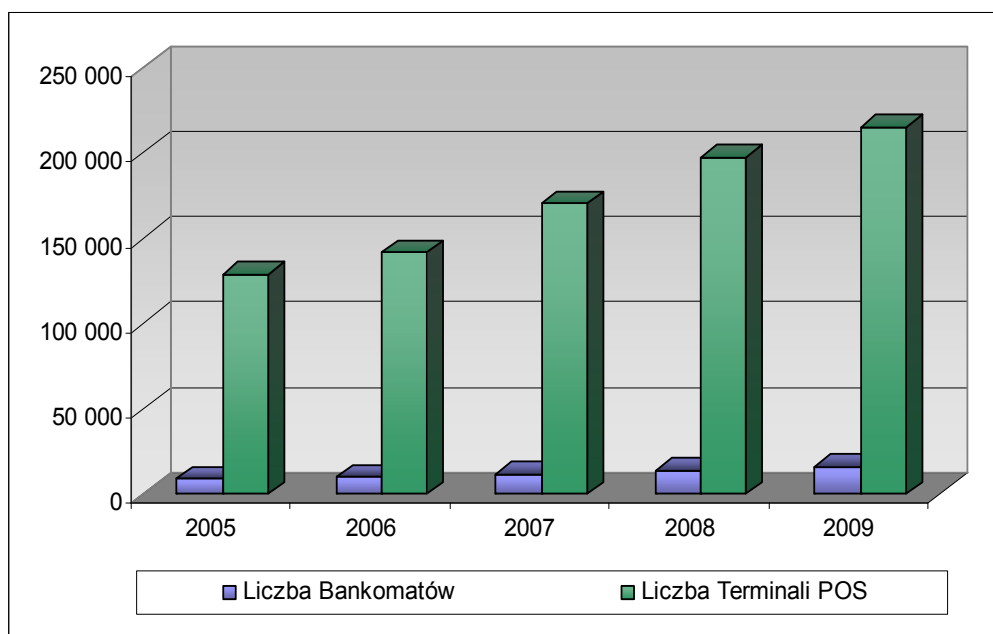
W 2009 roku na terenie Polski funkcjonowało 15 883 bankomatów (wzrost o 17% w stosunku do 2008 roku). Wraz z pojawieniem się bankomatów pracujących w trybie on-line znacznie rozszerzył się zakres ich funkcjonalności, gdyż możliwe stało się np. uzyskiwanie informacji o stanie rachunku, zakładanie lokat, dokonywanie przelewów, zasilenia konta telefonu komórkowego. Pojawiły się także urządzenia przyjmujące wpłaty gotówki tzw. wpłatomaty.

Wg szacunków UKNF na koniec 2009 r. ponad 25% bankomatów nie było zgodnych ze standardem EMV (bankomaty odczytywały dane tylko z paska magnetycznego karty).

Na koniec 2009 roku zarejestrowano 215 509 terminali POS, które umożliwiały płatności bezgotówkowe w punktach handlowych i usługowych (wzrost o 3,2% w stosunku do poprzedniego roku). Coraz rzadziej wykorzystywane są tzw. imprintery – urządzenia, przy pomocy których sprzedawca robi „odcisk” karty na specjalnym blankiecie, a transakcję autoryzuje telefonicznie podając centrum rozliczeniowemu wymagane dane.

Liczbę bankomatów oraz terminali POS funkcjonujących w Polsce w latach 2005-2009 przedstawiono na wykresie nr 11.

Wykres 11. Liczba bankomatów i terminali POS w Polsce w latach 2005 - 2009



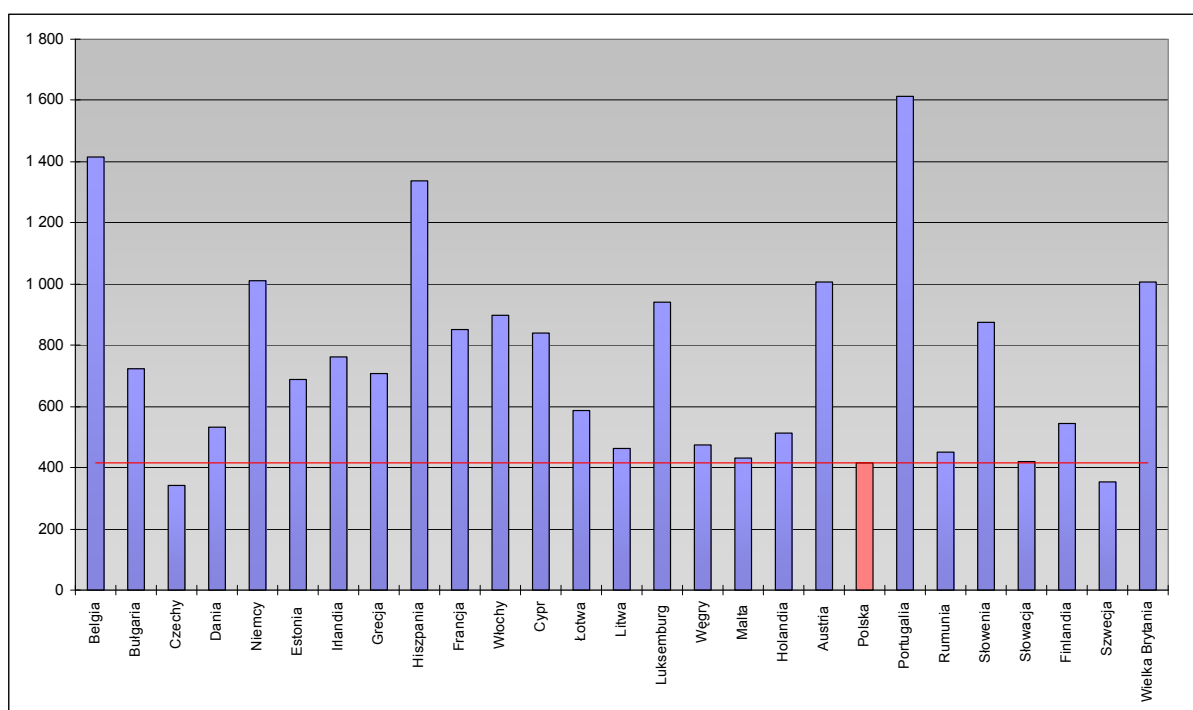
Źródło: Opracowanie własne na podstawie danych NBP przekazanych przez agentów rozliczeniowych.

Pomimo rosnącej liczby bankomatów oraz terminali POS Polska należy do krajów o najmniejszej liczbie tych urządzeń na mieszkańca w UE. Liczba bankomatów oraz terminali

POS przypadających na milion mieszkańców w poszczególnych krajach UE na koniec 2009 roku przedstawiona została na wykresach nr 12 i 13. W Polsce na milion mieszkańców przypadało 416 bankomatów, znacznie mniej niż przykładowo w Niemczech (1010) lub Portugalii (1614). Podobnie jest w przypadku terminali POS. W 2009 roku na milion mieszkańców naszego kraju przypadało 6 043 terminali, zaś dla porównania w Hiszpanii było ich 30 324, a w Grecji – 45 164..

Polska jest natomiast pierwszym krajem w Europie, który wprowadza bankomaty z identyfikacją biometryczną. Właściciel konta będzie mógł wypłacić pieniądze po tym, jak czytnik w bankomacie zeskanuje i rozpozna układ naczyń krwionośnych w palcu wypłacającego²⁹. W Polsce rozpoczęto też instalowanie bankomatów przystosowanych do potrzeb osób niepełnosprawnych. Urządzenia te mają specjalne oprogramowanie i wejście słuchawkowe.

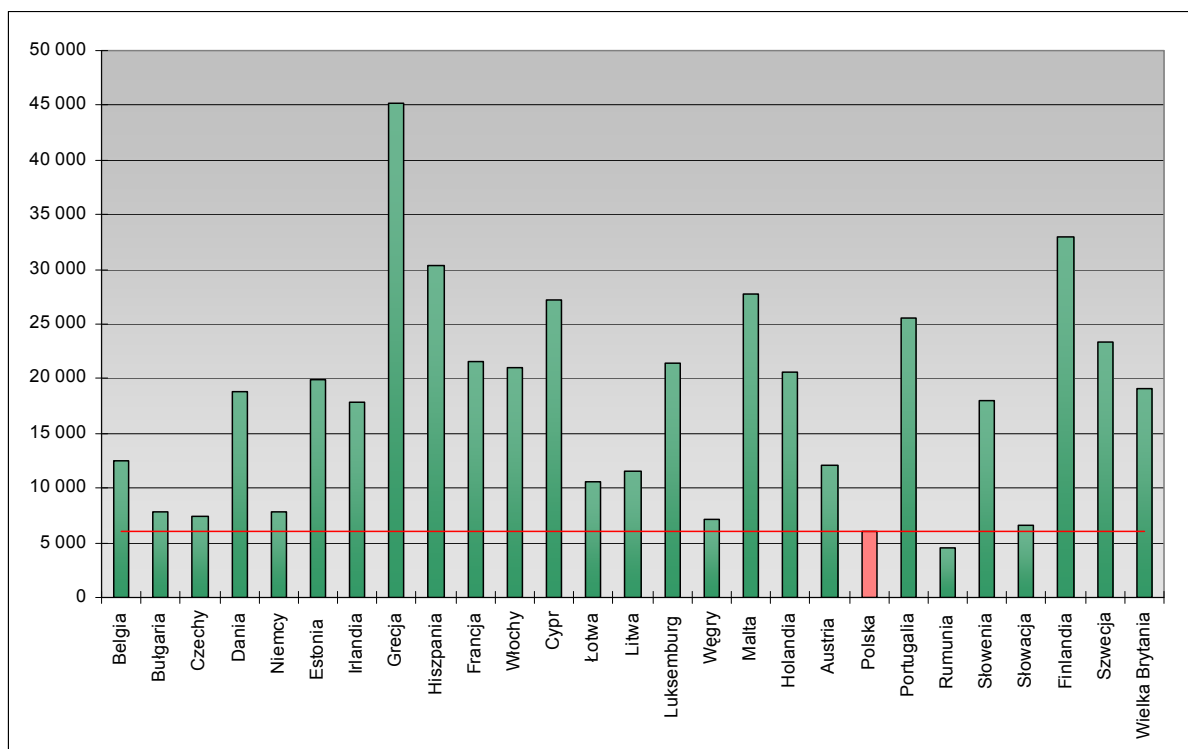
Wykres 12. Liczba bankomatów przypadających na milion mieszkańców w poszczególnych krajach UE na koniec 2009 roku



Źródło: Opracowanie własne na podstawie danych ECB

²⁹ Źródło: <http://biznes.gazetaprawna.pl>

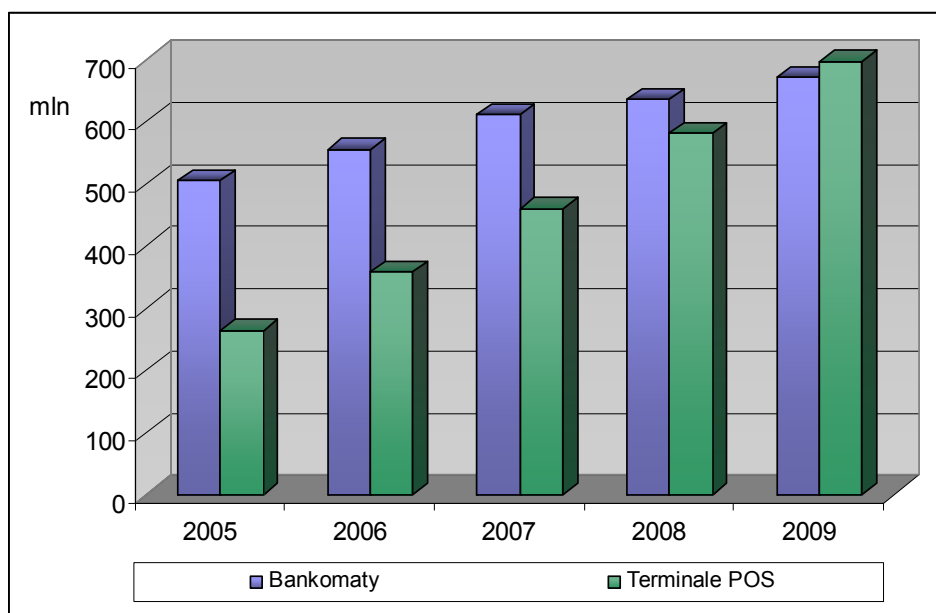
Wykres 13. Liczba terminali POS przypadających na milion mieszkańców w poszczególnych krajach UE na koniec 2009 roku



Źródło: Opracowanie własne na podstawie danych ECB

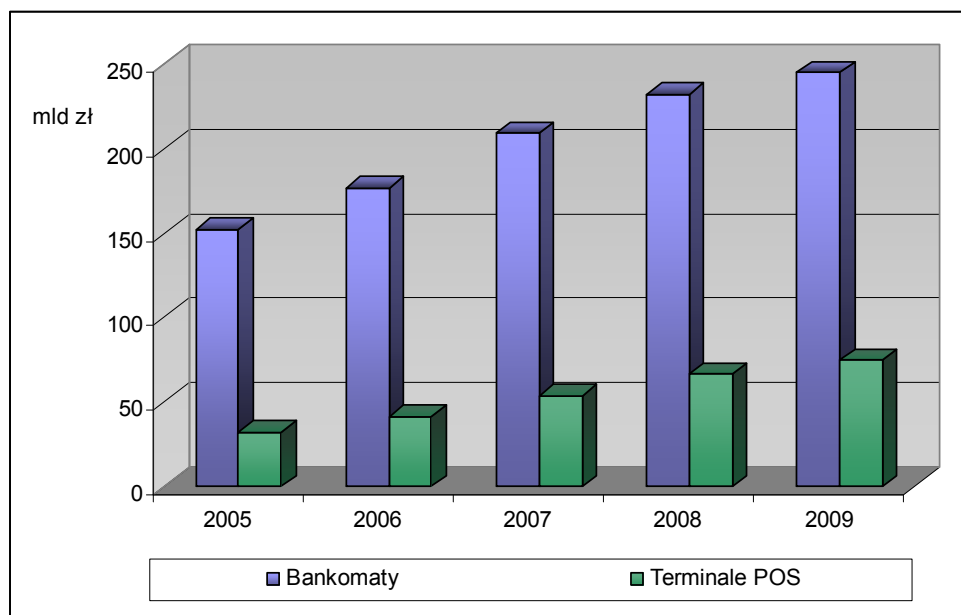
Liczbę oraz wartość operacji przeprowadzonych w Polsce za pośrednictwem bankomatów oraz terminali POS przedstawiono na wykresach nr 14 i 15.

Wykres 14. Liczba operacji przeprowadzonych w Polsce za pośrednictwem bankomatów i terminali POS w latach 2005 – 2009



Źródło: Opracowanie własne na podstawie danych NBP od agentów rozliczeniowych.

Wykres 15. Wartość operacji przeprowadzonych w Polsce za pośrednictwem bankomatów i terminali POS w latach 2005 – 2009



Źródło: Opracowanie własne na podstawie danych NBP od agentów rozliczeniowych.

W 2009 roku za pośrednictwem bankomatów dokonano 671,27 mln operacji (wzrost o 5,5 % w stosunku do roku 2008). Po raz pierwszy liczba ta była niższa od liczby transakcji dokonanych za pośrednictwem terminali POS, których w 2009 roku było 697,7 mln (wzrost o 20,1 % w stosunku do roku poprzedniego). W niektórych krajach UE sytuacja taka miała miejsce kilka lat temu (np. w Niemczech w 2006 roku a w Wielkiej Brytanii już w 2004 roku liczba transakcji POS była dwukrotnie większa niż transakcji bankomatowych).

Wartość nominalna operacji przeprowadzonych za pośrednictwem bankomatów w 2009 roku wyniosła 245,14 mld zł (wzrost o 5,7 % w porównaniu do 2008 roku). Średnia nominalna wartość operacji bankomatowych w 2009 roku wyniosła 365,19 zł i była porównywalna do 2008 roku (średnia 364,72 zł). Wartość nominalna operacji przeprowadzonych za pośrednictwem terminali POS w 2009 roku wyniosła 75,07 mld zł (wzrost o 12,7% w stosunku do 2008 roku). Systematycznie zmniejsza się średnia wartość transakcji w terminalach POS (na koniec 2009 wynosiła 107,6 zł a w latach 2007, 2008 było to odpowiednio 116,4 zł i 114,6 zł). Karty płatnicze wykorzystywane są coraz częściej - i do mniejszych kwotowo płatności.

Wzrasta w Polsce zainteresowanie usługą *cash back*, która umożliwia posiadaczom kart wypłatę gotówki w punktach handlowych przy okazji płacenia za zakupy kartą. Transakcja może być przeprowadzona jedynie łącznie z płatnością kartą za towar. Przy zakupie klient musi zgłosić chęć wypłacenia dodatkowej kwoty. Usługa ta jest dostępna dla posiadaczy kart debetowych systemów Visa i Mastercard tych banków, które uruchomiły funkcjonalność *cash back*. Wypłata gotówki w punkcie akceptującym karty zwykle jest wolna od opłat, lub opłata ta jest niższa od tej stosowanej dla wypłat gotówki z bankomatów nie należących do banku wydającego kartę. Z usługi tej można korzystać już w ok. 17 tys. placówkach. W samym 2009 r. dokonano 714 tys. transakcji *cash back* o łącznej wartości 77 mln zł (średnia wartość usługi – 107 zł).

5.2 Bankowość internetowa

Polski sektor bankowy w latach 2005 – 2009 charakteryzował się intensywnym wzrostem skali wykorzystania Internetu w procesie świadczenia usług. Świadczą o tym m.in.: rosnąca liczba rachunków bankowych, do których aktywowano dostęp za pośrednictwem serwisów internetowych oraz dynamika liczby wykonanych transakcji i szybko rosnąca ich wartość. Było to możliwe przede wszystkim dzięki przeprowadzonym przez wszystkie znaczące systemowo banki procesom centralizacji zasobów teleinformatycznych (głównie systemów ewidencji księgowej), co pozwoliło na odmiejscowienie³⁰ rachunków prowadzonych na rzecz klientów i wprowadzenie jednolitych standardów ich obsługi.

Większość funkcjonujących obecnie rozwiązań technicznych systemów bankowości internetowej została w latach 2005 – 2009 wdrożona lub unowocześniona pod kątem funkcjonalności i bezpieczeństwa usług. Dzięki temu bankowość internetowa stanowi dziś w pełni ekwiwalentną formę świadczenia usług w porównaniu z tradycyjną obsługą prowadzoną w oddziałach banków. Niskie jednostkowe koszty wykonania operacji bankowych sprawiły, że ten kanał dystrybucji usług traktowany jest jako jeden z najważniejszych czynników zdobywania pozycji rynkowej. Wzrost skali działalności i liczby obsługiwanych klientów za pośrednictwem bankowości internetowej nie pociąga za sobą bowiem konieczności rozbudowy sieci placówek operacyjnych ani wzrostu kosztów zatrudnienia. Potwierdza to zestawienie rosnącej liczby prowadzonych rachunków i transakcji ze stabilnym poziomem zatrudnienia w placówkach operacyjnych. Otwarcie rachunku bankowego z dostępem przez Internet stanowi często początek nawiązania trwalszych relacji banku z klientem, co ułatwia sprzedaż innych produktów. Doceniając aspekt marketingowy bankowości internetowej, część banków prowadzi konta internetowe nieodpłatnie lub w ramach miesięcznej, ryczałtowej opłaty, niezależnej od liczby wykonanych transakcji.

Przedstawiając w Raporcie dane liczbowe dotyczące usług bankowości internetowej dążono do zapewnienia reprezentatywności tych danych. Ze względu jednak na zróżnicowane możliwości techniczne banków w zakresie pozyskiwania danych o przeprowadzonych transakcjach (w wymaganych przekrojach), liczba banków przyjętych do próby (N) przedstawiana na poszczególnych wykresach jest zróżnicowana.

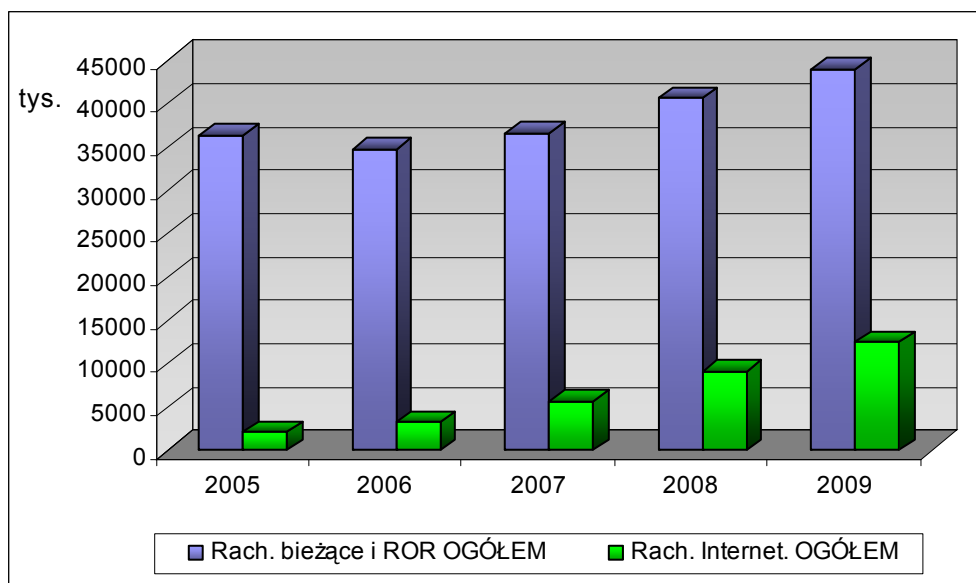
Liczba aktywnych rachunków bankowych³¹ z dostępem za pośrednictwem bankowości internetowej na tle liczby wszystkich aktywnych rachunków bankowych ogółem

³⁰ Odmiejscowienie rachunku – możliwość pełnej obsługi w dowolnej placówce banku.

³¹ Aktywne rachunki bankowe – rachunki bieżące oraz rachunki ROR, na których w ciągu danego roku klient przeprowadził przynajmniej jedną operację.

przedstawiona została na wykresie nr 16. Z wykresu tego wynika, że wzrost ogólnej liczby aktywnych rachunków bankowych (w 2009 r. wzrost o ok. 9% stosunku do roku poprzedniego) jest spowodowany w dużej mierze wzrostem liczby rachunków bankowych z dostępem za pośrednictwem bankowości internetowej (w 2009 roku liczba rachunków bankowych z dostępem przez Internet wzrosła o 36% w stosunku do roku poprzedniego).

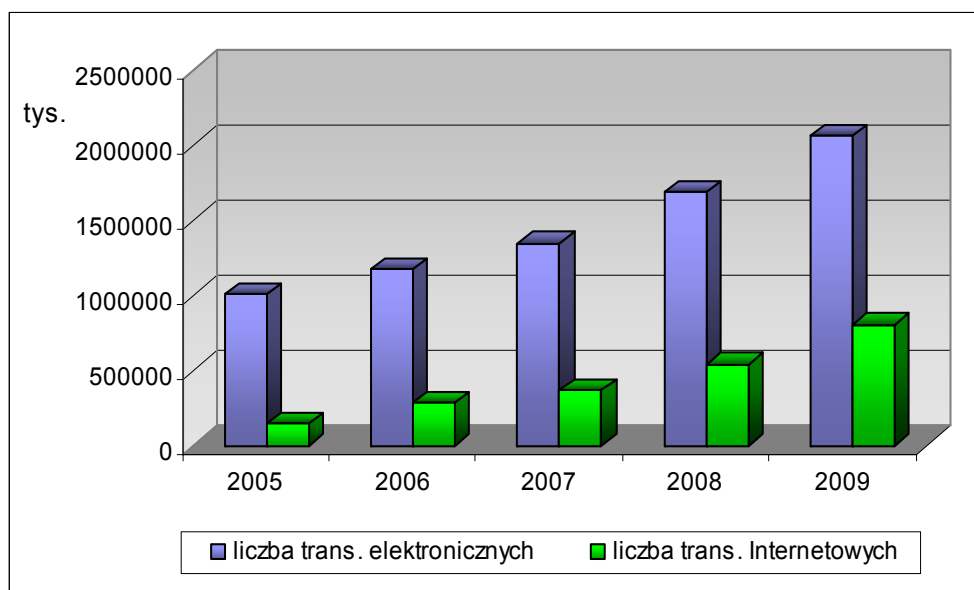
Wykres 16. Liczba aktywnych rachunków bankowych z dostępem przez Internet na tle liczby wszystkich aktywnych rachunków bankowych ogółem



Źródło: Wyniki badań UKNF przeprowadzonej wśród krajowych banków komercyjnych, N = 23.

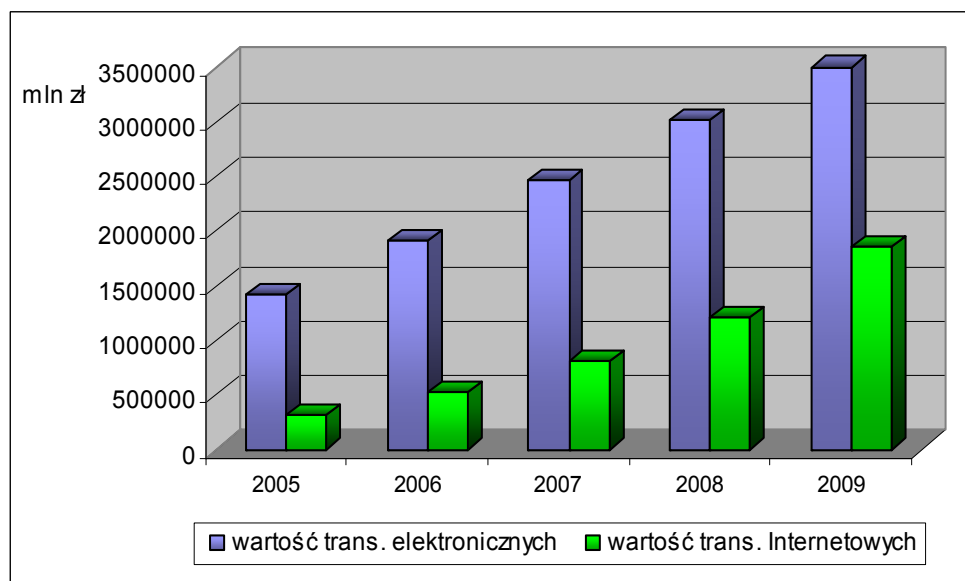
Liczba oraz wartość nominalna transakcji dokonanych przez klientów za pośrednictwem bankowości internetowej na tle liczby transakcji dokonanych za pośrednictwem wszystkich kanałów bankowości elektronicznej przedstawiona została na wykresach nr 17 i 18. Zarówno liczba jak i wartość transakcji dokonanych w ciągu kilku ostatnich lat za pośrednictwem wszystkich kanałów bankowości elektronicznej, a także za pośrednictwem samej bankowości internetowej ma wyraźną tendencję wzrostową. Liczba transakcji dokonanych przez Internet w 2009 roku w stosunku do roku poprzedniego wzrosła o 49%, a liczba wszystkich transakcji elektronicznych wzrosła o 22%. Wartość samych transakcji internetowych w 2009 roku w stosunku do roku poprzedniego wzrosła o ok. 55%, a wartość wszystkich transakcji elektronicznych wzrosła o 16%. Można zatem stwierdzić, że transakcje dokonywane za pośrednictwem Internetu odgrywają coraz bardziej znaczącą rolę.

Wykres 17. Liczba transakcji dokonanych za pomocą bankowości internetowej na tle transakcji dokonanych za pośrednictwem wszystkich kanałów bankowości elektronicznej



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N = 31.

Wykres 18. Wartość transakcji dokonanych za pomocą bankowości internetowej na tle transakcji dokonanych za pośrednictwem wszystkich kanałów bankowości elektronicznej



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N = 24.

W bankach komercyjnych, które były przedmiotem analizy, występują znaczne różnice pod względem udziału liczby rachunków, do których uruchomiono dostęp za pośrednictwem Internetu w ogólnej liczbie rachunków bankowych. Różnice te wynikają głównie z profilu obsługiwanych klientów (skłonności do korzystania z bankowości internetowej), w mniejszym stopniu natomiast z uwarunkowań technicznych i funkcjonalności systemów

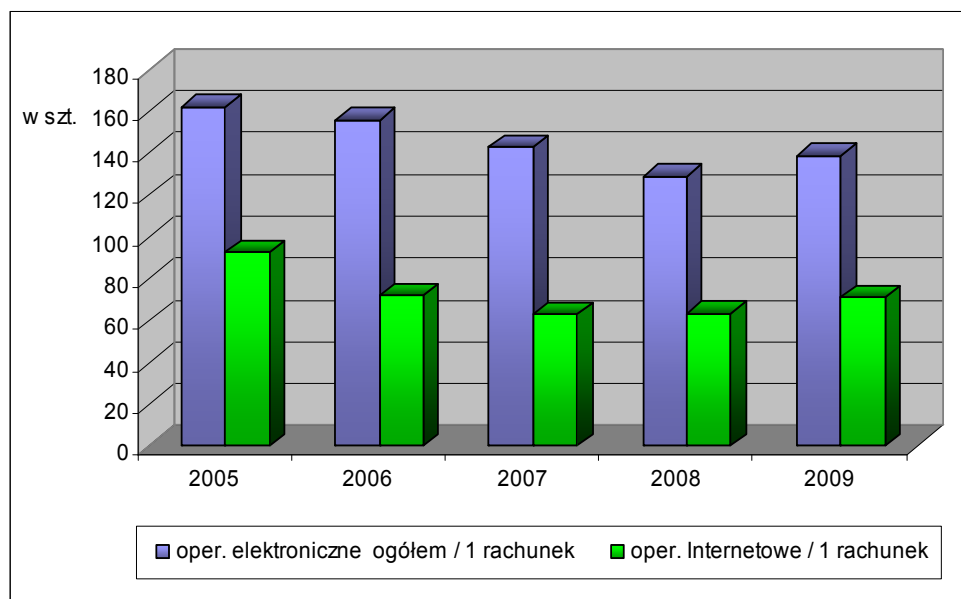
bankowości internetowej. Na podstawie danych pozyskanych z banków można także stwierdzić, że rachunki, do których uruchomiono dostęp internetowy, charakteryzowały się wyższą średnią liczbą wykonywanych operacji i większym ich wolumenem w porównaniu z rachunkami, do których takiego dostępu nie uruchomiono.

Zgodnie z wynikami badań TNS OBOP³² występuje korelacja pomiędzy faktem korzystania z bankowości internetowej a cechami różnicującymi badaną zbiorowość. Najczęściej z bankowości internetowej korzystali respondenci posiadający: stały dostęp do Internetu (32 %), w wieku 20 – 39 lat, posiadający wykształcenie licencjackie i wyższe (39 %). Początkowo jako powód braku korzystania z bankowości internetowej wymieniano koszt sprzętu i dostępu do Internetu, obecnie główne wskazania to: obawa o bezpieczeństwo środków, brak umiejętności poruszania się w środowisku internetowym oraz niskie dochody. Kierunek obserwowanych zmian rynkowych i osłabienie czynników ograniczających rozwój skali wykorzystania bankowości internetowej dają podstawę do prognozowania dalszego wzrostu znaczenia tej formy świadczenia usług w najbliższych latach.

Lata 2005 – 2010 charakteryzowały się szybkim rozwojem funkcjonalności portali i oferty rynkowej banków w zakresie usług świadczonych za pośrednictwem bankowości internetowej. Silna konkurencja na rynku usług bankowych, skutkująca m.in. wprowadzeniem do oferty rachunków bezpłatnych skłania część klientów do posiadania więcej niż jednego rachunku z dostępem przez Internet. Ocenia się, że zjawisko to jest korzystne z punktu widzenia wzrostu jakości i konkurencyjności usług bankowych oraz dywersyfikacji środków i zapewnienia alternatywnego dostępu do środków np. na wypadek wystąpienia awarii systemu bankowości internetowej w jednym z banków. Do 2008 r. występował spadek średniej liczby operacji w przeliczeniu na jeden rachunek rocznie, co dotyczy zarówno łącznej liczby transakcji elektronicznych na rachunku, jak również transakcji internetowych (wykres nr 19).

³² Raport z 2006 roku.

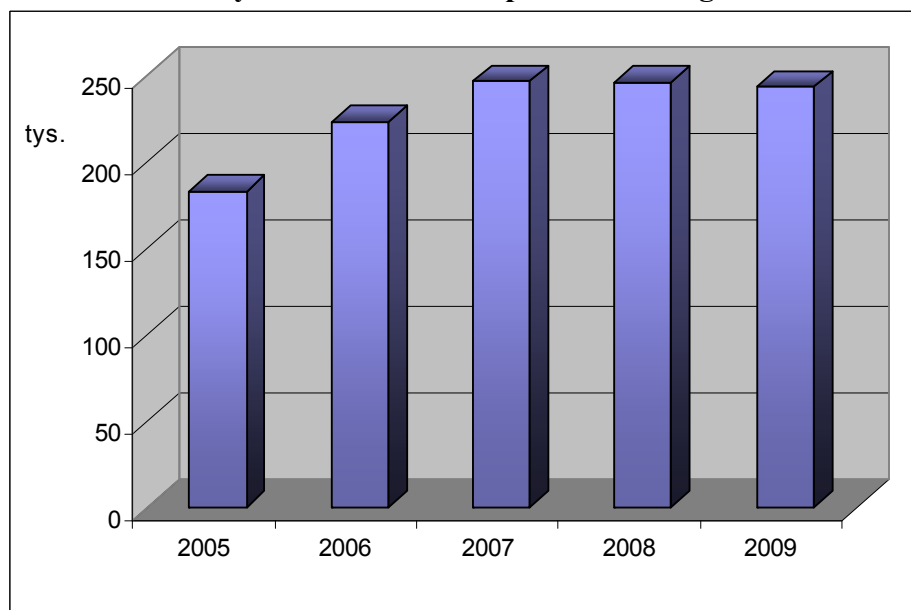
Wykres 19. Średnia liczba transakcji zrealizowanych za pomocą bankowości internetowej na tle transakcji zrealizowanych wszystkimi kanałami bankowości elektronicznej w przeliczeniu na 1 rachunek bankowy



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N = 22.

Nieco inaczej wygląda statystyka operacji w systemach home/corporate banking. Liczba rachunków bankowych (wykres nr 20) z dostępem za pośrednictwem systemów home/corporate banking (dedykowane do obsługi podmiotów gospodarczych i instytucji) w analizowanym okresie nieco spadła, co może być spowodowane m.in. stopniową migracją klientów korzystających z ww. usług do systemów bankowości internetowej.

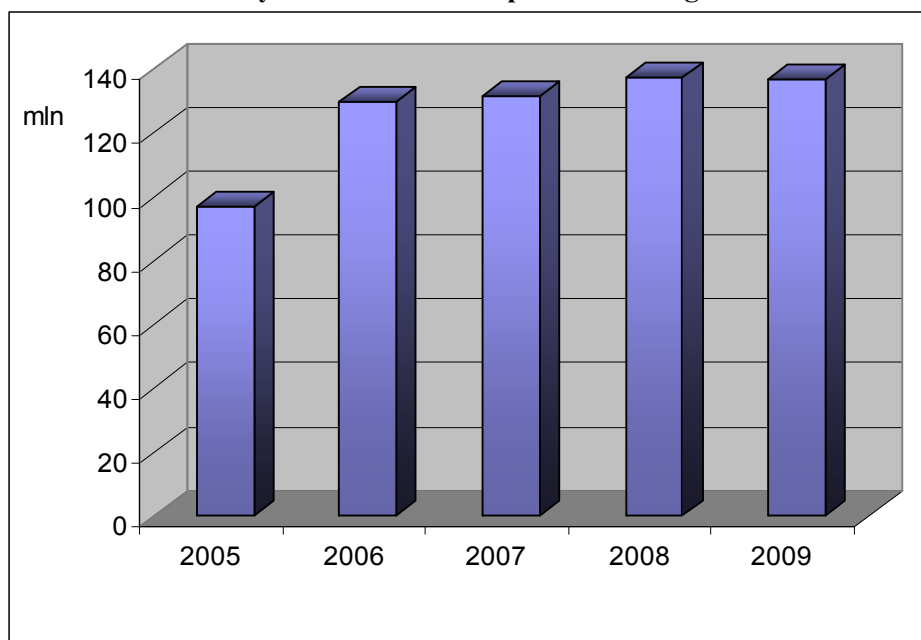
Wykres 20. Liczba rachunków bankowych z dostępem za pośrednictwem systemów home / corporate banking



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N=19.

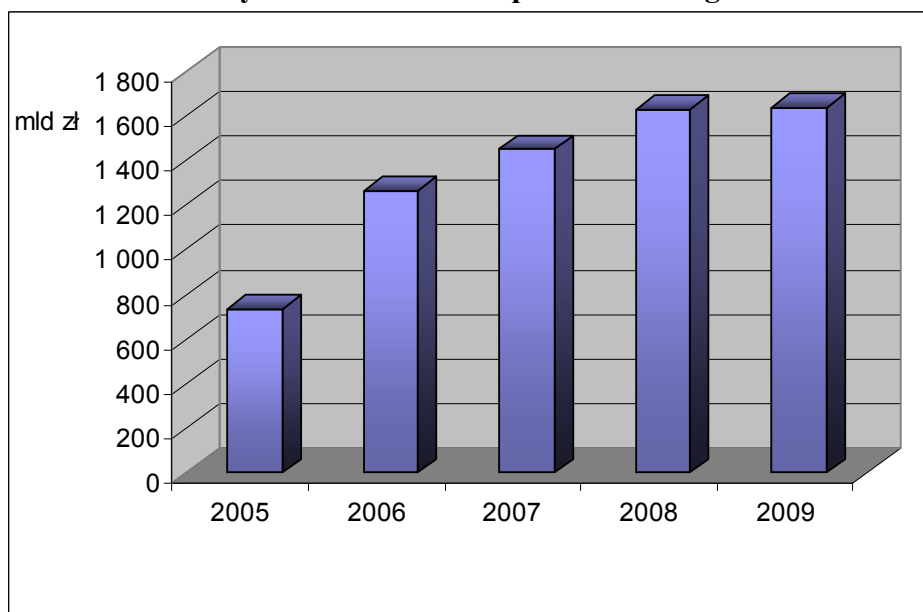
Liczba oraz wartość nominalna transakcji zrealizowanych za pośrednictwem systemów home/corporate banking przedstawiona została na wykresach nr 21 i 22. Zauważalna jest porównywalna liczba oraz wartość tych transakcji w latach 2008 i 2009. Skala realizowanych za pośrednictwem systemów home/corporate banking transakcji jest skorelowana głównie z aktywnością gospodarczą obsługiwanych podmiotów.

Wykres 21. Liczba transakcji zrealizowanych za pośrednictwem systemów home / corporate banking



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N=19

Wykres 22. Wartość transakcji zrealizowanych za pośrednictwem systemów home / corporate banking



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N=19.

Zasadniczym czynnikiem branym pod uwagę przez klientów przy podejmowaniu decyzji o korzystaniu z bankowości internetowej jest bezpieczeństwo środków na rachunku oraz bezpieczeństwo realizowanych transakcji.

Na podstawie monitoringu najpopularniejszych (nie specjalistycznych) portali internetowych, przeprowadzonego w okresie luty – kwiecień 2010 r. na potrzeby niniejszego Raportu, stwierdzono, że obecny w tych mediach przekaz, dotyczący aspektów bezpieczeństwa bankowości internetowej przedstawiał to zagadnienie dość jednostronnie, głównie w kontekście negatywnych wydarzeń: awarii i błędów systemów teleinformatycznych (w tym banków funkcjonujących za granicą) oraz opisu potencjalnych zagrożeń. Niewiele miejsca poświęcono natomiast na pokazanie korzyści związanych z wykorzystaniem systemu bankowości internetowej (czas obsługi i jej wygoda, dostępność systemów, niskie koszty wykonania transakcji oraz ich bezpieczeństwo).

Znaczna część systemów informatycznych obsługujących bankowość internetową dostępnych obecnie na polskim rynku, została wdrożona lub zmodernizowana w latach 2005 – 2009. Kilkuletnie opóźnienie we wprowadzaniu usług bankowości internetowej przez banki w Polsce w stosunku do banków działających w tzw. „starych” krajach Unii Europejskiej i USA, umożliwiło wykorzystanie zdobytych tam doświadczeń i zastosowanie bardziej skutecznych systemów zabezpieczeń.

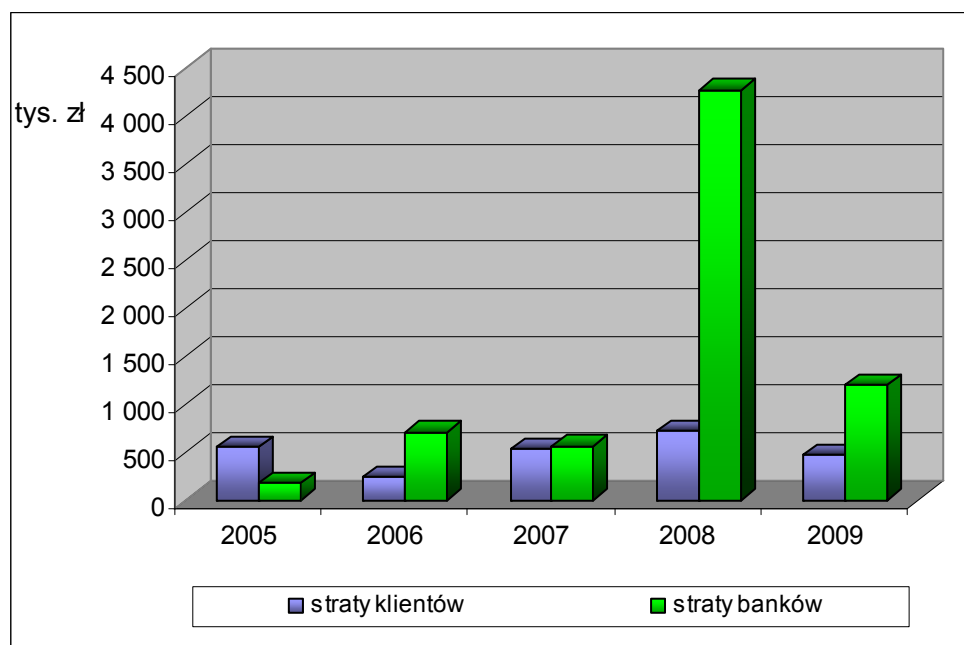
Systemy bankowości internetowej blokują konto użytkownika najczęściej po 3 – 5 błędnie podanych hasłach. Odblokowanie dostępu zwykle wymaga osobistego kontaktu klienta z bankiem. Wszystkie ankietowane banki stosowały ochronę kryptograficzną dla transmisji pomiędzy platformą transakcyjną banku a komputerem klienta. Standardowo stosowany jest w tym celu protokół SSL (128 bitów), co przy uwzględnieniu charakteru protokołu transmisji danych (IP), w praktyce uniemożliwia zdekodowanie tak zabezpieczonej transmisji w czasie rzeczywistym przy użyciu dostępnych, „cywilnych” metod dekryptażu. Na podstawie analizy danych przekazanych przez banki stwierdzono, że 7 banków zabezpiecza transakcje podpisem elektronicznym, w tym 2 podpisem cyfrowym w rozumieniu przepisów ustawy o podpisie elektronicznym.

Liczba strat poniesionych w związku z korzystaniem z systemów bankowości internetowej, zarówno przez klientów jak i same banki przedstawiona została na wykresie³³ nr 23. Straty poniesione w 2009 roku przez klientów rozpatrywanych banków były mniejsze niż w roku poprzednim (spadek o 36 %). Największe straty zostały poniesione w 2008 roku

³³ Wykres sporządzono na podstawie danych o transakcjach oszukańczych w systemach bankowości internetowej zebranych od 10 banków komercyjnych (bez transakcji oszukańczych wykonanych w Internecie z wykorzystaniem kart wirtualnych, które zostały przedstawione w rozdziale dotyczącym kart płatniczych).

(zadecydowały o tym wyjątkowo wysokie straty dwóch banków), przy czym w 2009 roku ich liczba znacznie się zmniejszyła.

Wykres 23. Straty klientów oraz banków poniesione na skutek transakcji oszukańczych w bankowości internetowej (bez kart wirtualnych).



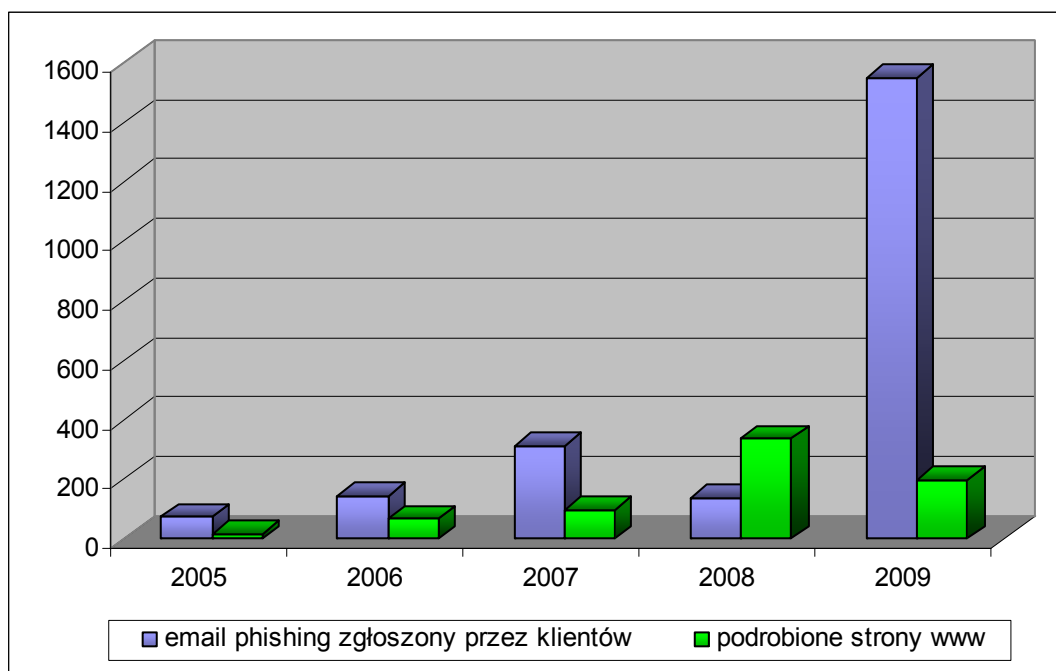
Źródło: Wyniki badań KNF przeprowadzonych wśród krajowych banków komercyjnych, N = 10.

Zaznaczyć należy, że ze względu na niejednolite zasady gromadzenia danych o stratach operacyjnych w poszczególnych bankach (w tym różne wartości minimalnych rejestrowanych strat, klasyfikacja przyczyn strat itp.), faktyczna kwota i liczba strat operacyjnych związanych z funkcjonowaniem systemów bankowości internetowej może być większa, niż prezentowana na wykresie.

Na podstawie danych otrzymanych z banków można stwierdzić, że wyższe ryzyko związane jest z wykonywaniem płatności kartami bankowymi w Internecie, niż realizowanych za pomocą systemów bankowości internetowej, wymagających dwuetapowej autoryzacji i wykorzystujących system haseł jednorazowych.

Zagrożenia związane z funkcjonowaniem systemów bankowości internetowej, wskazywane przez ankietowane banki dotyczyły głównie phishingu i oprogramowania typu „koń trojański”. 13 banków komercyjnych stwierdziło występowanie przypadków sfalszowania ich stron internetowych a 9 banków zarejestrowało zgłoszenia klientów dotyczące prób wyłudzenia informacji autoryzacyjnych.

Wykres 24. Próby wyłudzenia informacji autoryzacyjnych



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych, N = 13.

Ocenia się, że ze względu na złożoność procesu identyfikacji i dokumentacji zagrożeń internetowych oraz brak jednolitych zasad klasyfikacji i ewidencji incydentów bezpieczeństwa, część nieudanych prób wyłudzenia pieniędzy poprzez systemy bankowości internetowej mogła nie zostać zarejestrowana i uwzględniona w otrzymanych danych. Znaczna liczba przypadków phishingu w 2009 roku, widoczna na wykresie nr 24, wynika głównie ze zgłoszeń klientów jednego z banków.

Liczba reklamacji dotyczących usług bankowości internetowej w badanych bankach wzrasta, jednak szybciej rośnie liczba reklamacji niezasadnych. Świadczy to o konieczności podejmowania przez banki działań mających na celu właściwe (i w przystępnej formie) informowanie klientów o zasadach korzystania z systemów bankowości internetowej.

Usługi home/corporate banking charakteryzowały się dobrym poziomem bezpieczeństwa i znikomą liczbą reklamacji.

Jak już wspomniano w rozdziale 3 przy opisie charakterystyki bankowości internetowej, transakcja może zostać zrealizowana pod warunkiem działania zarówno elementów systemu będących w gestii banku, jak również infrastruktury zewnętrznej, niezależnej od banku. Banki oferujące usługi bankowości internetowej mają obowiązek wprowadzenia rozwiązań zapewniających stałą dostępność tych usług dla klientów, również w sytuacji awaryjnej. Jedynie 2 banki komercyjne (nieznaczące systemowo) poinformowały o braku zapasowego systemu bankowości internetowej (a 1 bank w przypadku usług dla przedsiębiorstw) na

wypadek awarii zasobów podstawowych. W większości banków wykonano testy rozwiązań awaryjnych. Przeprowadzone testy wykazały, że odtworzenie funkcjonowania systemów bankowości internetowej w 23 znaczących systemowo bankach było możliwe w oparciu o zasoby awaryjne w czasie do 6 godzin.

Dane otrzymane z banków komercyjnych pokazują, że w 2009 roku łączny czas niedostępności systemów bankowości internetowej w 10 bankach nie przekraczał 12 godzin (w każdym z banków), w 8 bankach było to 12 do 24 godzin, w 3 bankach łączny czas niedostępności w ciągu roku przekroczył 48 godzin. Część banków nie przekazała danych. Łączny czas niedostępności systemów bankowości internetowej w latach 2005 – 2009 wykazywał tendencję rosnącą od 306 godzin w 2005 r. do 507 godzin w 2009 r. rocznie, jednak w obserwowanym okresie, przypadki niedostępności usług bankowych w Internecie, w istotnych systemowo bankach nie przekraczały 1 dnia roboczego.

Część banków korzysta z przepisów ustawy Prawo bankowe, pozwalających między innymi na powierzenie utrzymania zasobów obsługujących bankowość internetową podmiotom zewnętrznym (krajowym i zagranicznym) na zasadzie outsourcingu. Z opcji outsourcingu krajowego korzystało 7 banków, z usług podmiotów zagranicznych (głównie wchodzących w skład grup kapitałowych) korzystały 4 banki, w pozostałych przypadkach systemy bankowości internetowej funkcjonowały w zasobach własnych banków.

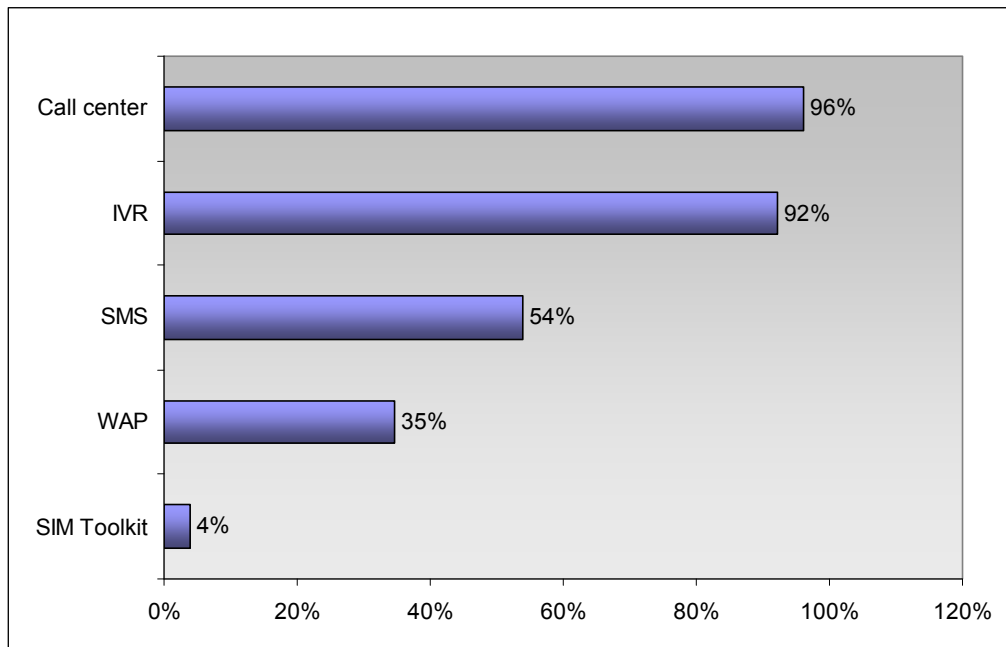
W I półroczu 2010 roku zanotowano 3 istotne przypadki niedostępności systemów bankowości internetowej (w tym jeden obejmujący kilka banków). Ich przyczyną, według wyjaśnień banków, było przeciążenie zasobów odpowiedzialnych za obsługę ruchu internetowego (w tym obsługiwanych przez przedsiębiorcę zagranicznego) oraz w jednym przypadku przeciążenie głównego systemu informatycznego banku, skutkującego niedostępnością wszystkich bankowych kanałów obsługi.

5.3 Bankowość telefoniczna

Bankowość telefoniczna zaliczana jest do jednych z pierwszych zautomatyzowanych usług oferowanych klientom banków. Na koniec 2009 roku spośród badanych przez UKNF 35 krajowych banków komercyjnych (których łączne aktywa stanowiły 92 % całkowitej sumy bilansowej wszystkich krajowych banków komercyjnych) usługi bankowości telefonicznej oferowało 26 banków (74 % badanej próby).

Na wykresie nr 25 przedstawiono poszczególne usługi bankowości telefonicznej oferowane przez 26 krajowych banków komercyjnych. Najbardziej powszechną usługą jest call center, którą świadczyło 25 banków (96 % badanej próby). Dostęp do rachunku bankowego za pośrednictwem automatycznego serwisu IVR oferowany był przez 24 banki (92 % próby). Spośród usług, w ramach bankowości mobilnej, najczęściej oferowaną usługą jest SMS banking, którą oferowało 14 banków (54 % próby), zaś usługi WAP oferowane były przez 9 banków (35 % próby). Tylko 1 bank oferował usługi bankowości mobilnej oparte na rozwiązaniach SIM Toolkit.

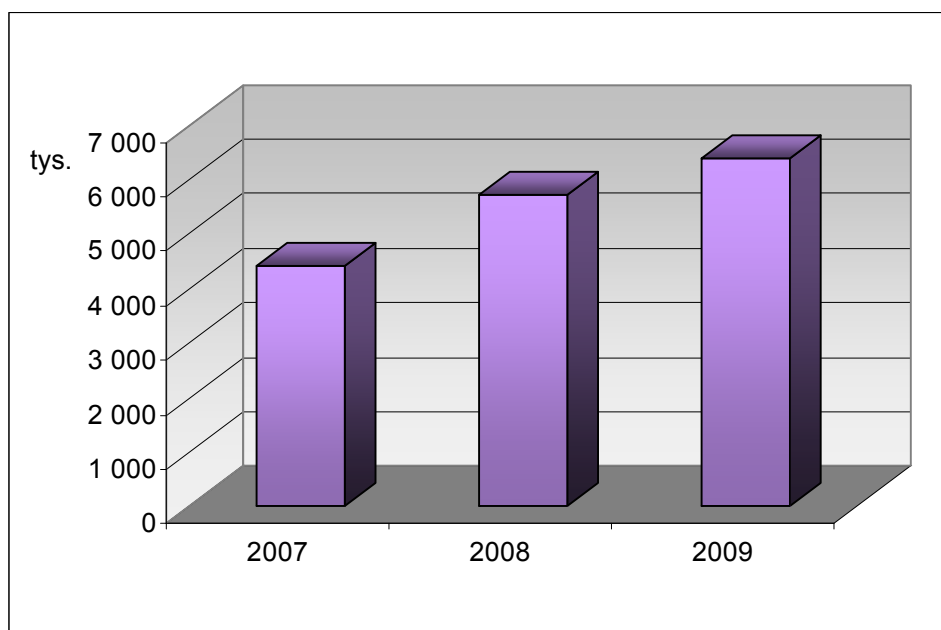
Wykres 25. Usługi bankowości telefonicznej oferowane przez krajowe banki komercyjne



Źródło: Wyniki badań UKNF wśród krajowych banków komercyjnych świadczących usługi z zakresu bankowości telefonicznej na koniec 2009, N = 26

Z uwagi na wzrost ogólnej liczby rachunków bankowych, rośnie także liczba aktywnych rachunków bankowych z dostępem za pośrednictwem bankowości telefonicznej, co przedstawiono na wykresie nr 26. W 2009 roku nastąpił przyrost o 12 % w porównaniu do roku poprzedniego, ale dynamika przyrostu maleje.

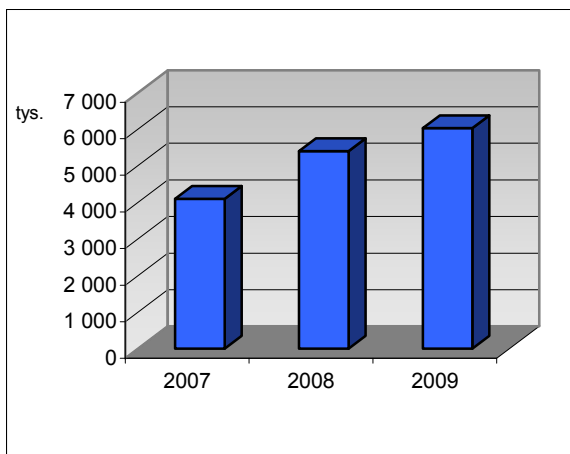
Wykres 26. Liczba aktywnych rachunków bankowych (rachunki bieżące oraz ROR) z dostępem za pośrednictwem kanałów bankowości telefonicznej



Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych świadczących usługi z zakresu bankowości telefonicznej, N = 12.

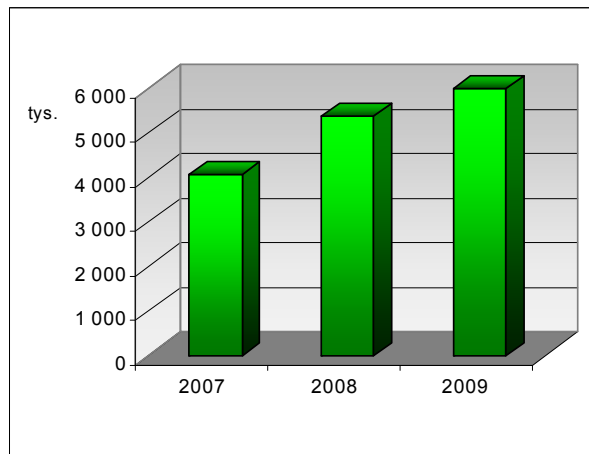
Liczbę aktywnych rachunków bankowych z dostępem za pośrednictwem poszczególnych usług bankowości telefonicznej przedstawiono na wykresach nr 27-30. Liczba aktywnych rachunków bankowych z dostępem za pośrednictwem wszystkich rodzajów bankowości telefonicznej wzrasta. W 2009 roku największy wzrost liczby aktywnych rachunków (27 %) nastąpił w przypadku usługi WAP, zaś najmniejszy (8 %) w przypadku usługi SMS.

Wykres 27. Aktywne rachunki bankowe - Call center



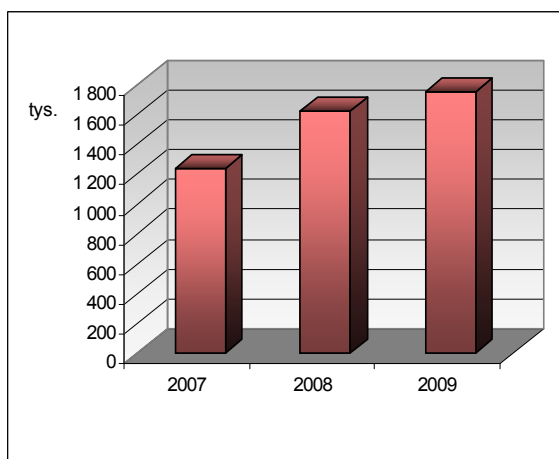
Źródło: Badanie UKNF wśród banków komercyjnych, N = 12

Wykres 28. Aktywne rachunki bankowe - IVR



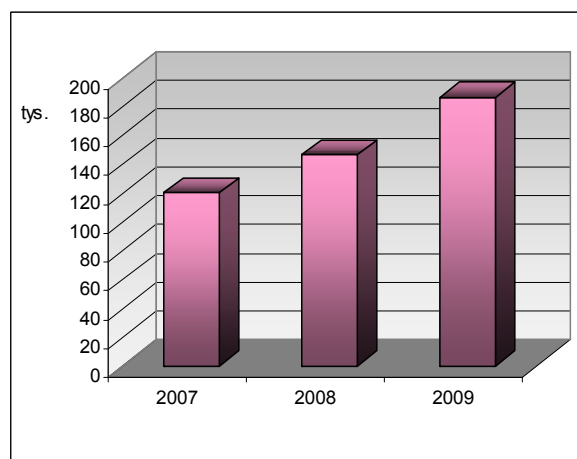
Źródło: Badanie UKNF wśród banków komercyjnych, N = 11

Wykres 29. Aktywne rachunki bankowe - SMS



Źródło: Badanie UKNF wśród banków komercyjnych, N = 7

Wykres 30. Aktywne rachunki bankowe - WAP

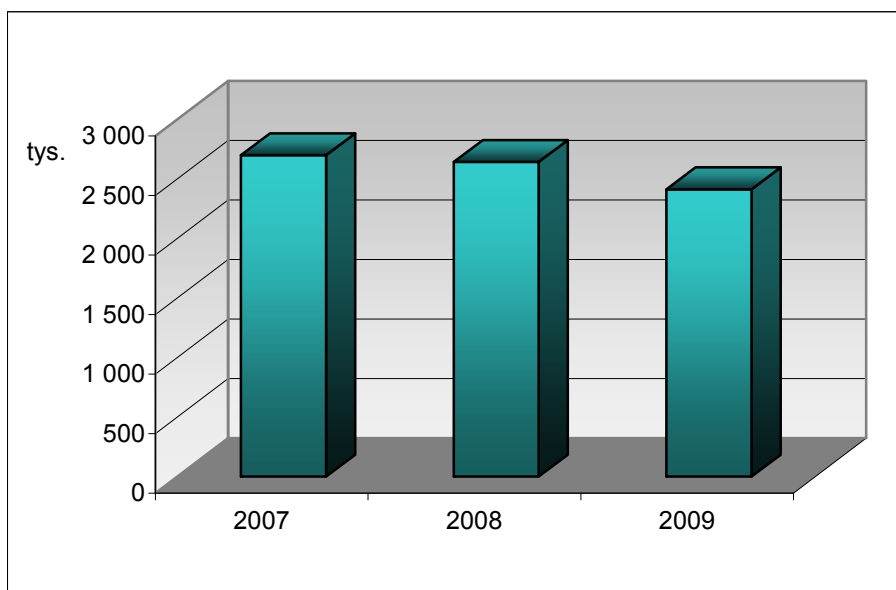


Źródło: Badanie UKNF wśród banków komercyjnych, N = 2

Liczba transakcji wykonanych za pośrednictwem kanałów bankowości telefonicznej przez klientów krajowych banków komercyjnych w latach 2007-2009 przedstawiona została na wykresie nr 31. Widzimy, że począwszy od 2007 roku liczba wykonanych transakcji ma tendencję spadkową (spadek w 2009 roku o 9 % wobec roku poprzedniego).

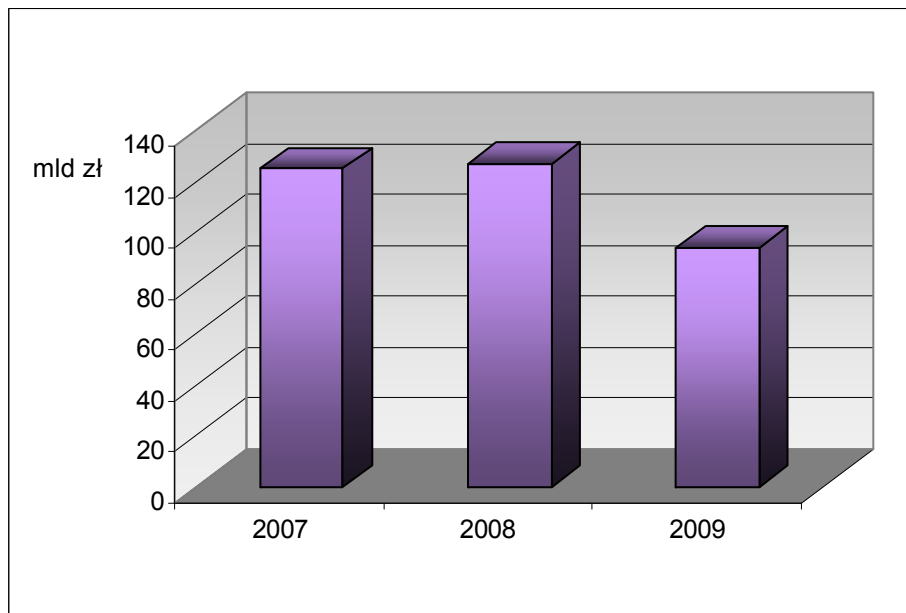
Analizując wartość nominalną transakcji wykonanych przez klientów banków komercyjnych w latach 2007-2009 za pośrednictwem kanałów bankowości telefonicznej (wykres nr 32) można zauważyć nieznaczny wzrost (1 %) wartości transakcji zrealizowanych w 2008 roku w porównaniu do roku poprzedniego oraz spadek o 25 % wartości transakcji w 2009 roku.

Wykres 31. Liczba transakcji zrealizowanych przez klientów banków komercyjnych za pośrednictwem kanałów bankowości telefonicznej (tys.)



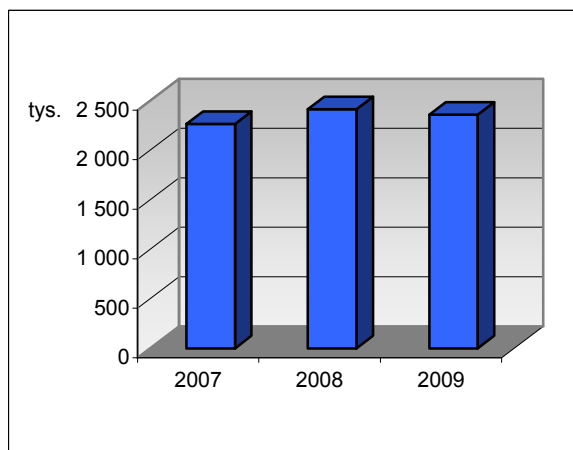
Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych świadczących usługi z zakresu bankowości telefonicznej, N = 14.

Wykres 32. Wartość transakcji zrealizowanych przez klientów banków komercyjnych za pośrednictwem kanałów bankowości telefonicznej (mld zł)



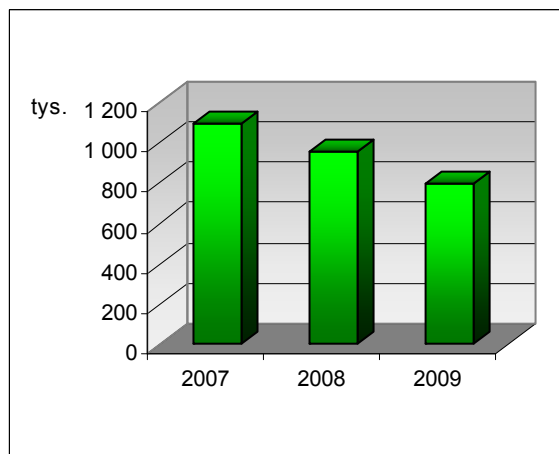
Źródło: Wyniki badań UKNF przeprowadzonych wśród krajowych banków komercyjnych świadczących usługi z zakresu bankowości telefonicznej, N = 14.

Wykres 33. Liczba wykonanych transakcji - Call center



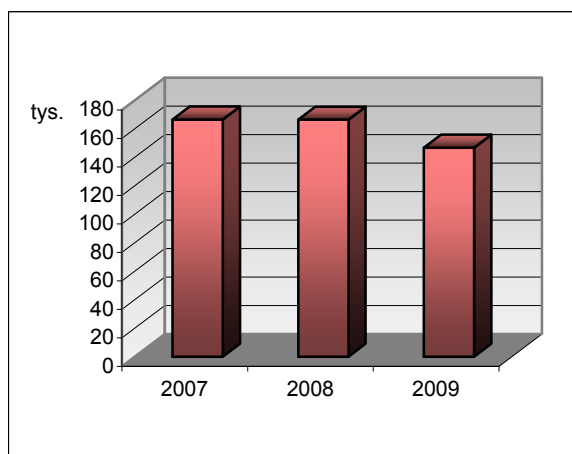
Źródło: Badanie UKNF wśród banków komercyjnych, N = 16

Wykres 34. Liczba wykonanych transakcji - IVR



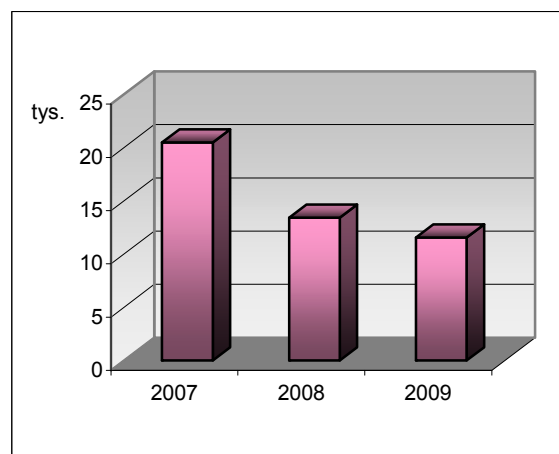
Źródło: Badanie UKNF wśród banków komercyjnych, N = 12

Wykres 35. Liczba wykonanych transakcji - SMS



Źródło: Badanie UKNF wśród banków komercyjnych, N = 8

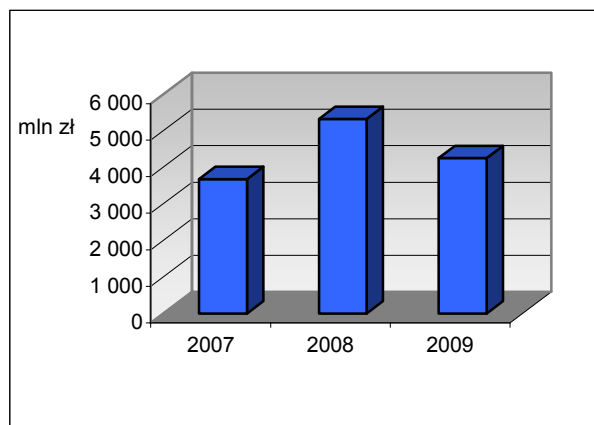
Wykres 36. Liczba wykonanych transakcji - WAP



Źródło: Badanie UKNF wśród banków komercyjnych, N = 4

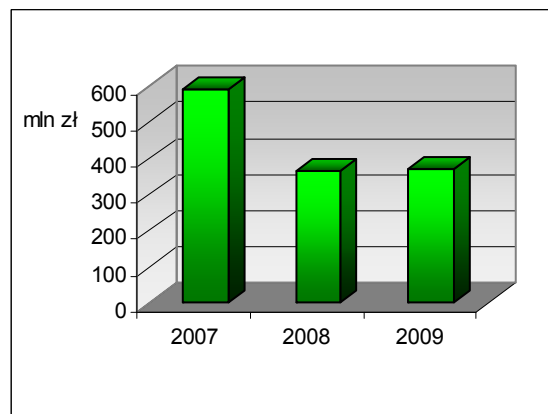
Liczba transakcji wykonanych przez klientów krajowych banków komercyjnych w latach 2007-2009 za pomocą poszczególnych kanałów bankowości telefonicznej przedstawiona została na wykresach nr 33-36. W porównaniu do 2008 roku liczba wykonanych transakcji za pośrednictwem usługi call center spadła o 2 %, a począwszy od roku 2007 zauważalna jest stosunkowo silna tendencja spadkowa liczby transakcji wykonanych za pomocą usługi IVR (w 2009 roku liczba ta była mniejsza o 16 % w porównaniu z rokiem 2008). Liczba transakcji wykonanych za pośrednictwem usługi SMS w 2009 r. spadła o 12 % w stosunku do roku poprzedniego. Podobnie wygląda sytuacja w przypadku usługi WAP - począwszy od 2007 roku również zauważalny jest spadek liczby wykonanych transakcji (spadek o 14 % w 2009 roku wobec roku poprzedniego).

Wykres 37. Wartość wykonanych transakcji - Call center



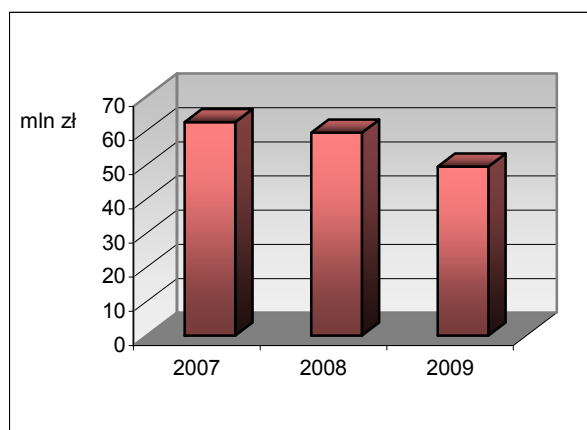
Źródło: Badanie UKNF wśród banków komercyjnych, N = 16

Wykres 38. Wartość wykonanych transakcji - IVR



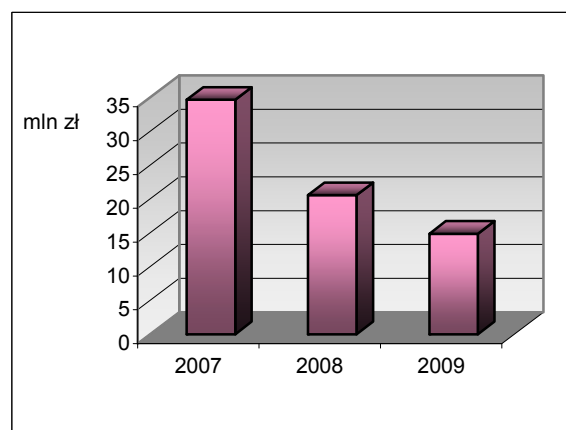
Źródło: Badanie UKNF wśród banków komercyjnych, N = 12

Wykres 39. Wartość wykonanych transakcji - SMS



Źródło: Badanie UKNF wśród banków komercyjnych, N = 8

Wykres 40. Wartość wykonanych transakcji - WAP



Źródło: Badanie UKNF wśród banków komercyjnych, N = 4

Wartość transakcji wykonanych przez klientów krajowych banków komercyjnych w latach 2007-2009 za pomocą poszczególnych kanałów bankowości telefonicznej przedstawiona została na wykresach nr 37-40. Z wykresów tych wynika, że w porównaniu do 2008 roku wartość wykonanych transakcji za pomocą usługi call center w 2009 roku spadła o 20 %. Wartość transakcji wykonanych za pomocą usługi IVR spadła w 2009 roku o około 1 % w porównaniu do roku poprzedniego, natomiast wartość transakcji wykonanych za pośrednictwem usługi SMS począwszy od roku 2007 przyjmuje tendencję spadkową (w 2009 roku nastąpił spadek o 17 %). Wartość transakcji wykonywanych za pomocą usługi WAP w poszczególnych latach malała i w 2009 roku spadła o blisko 28 % w stosunku do roku poprzedniego.

PODSUMOWANIE

Bankowość elektroniczna stała się w polskim sektorze bankowym usługą powszechnie dostępną, ale jak pokazują dane np. w przypadku bankowości terminalowej - pod względem stopnia wykorzystania jej przez społeczeństwo - wyprzedza nas wiele innych krajów Unii Europejskiej.

Dane pokazują, że najbardziej rozwijającą się w Polsce formą świadczenia usług w ramach bankowości elektronicznej jest bankowość internetowa, która od strony banków charakteryzuje się dobrym poziomem bezpieczeństwa, ale trzeba pamiętać, że wymaga ona zapewnienia odpowiednich warunków technicznych również ze strony klienta. Traci na znaczenie bankowość telefoniczna, natomiast bankowość mobilna wykorzystywana jest głównie przez zaawansowanych użytkowników telefonii komórkowej lub jako kanał przepływu informacji pomiędzy bankiem i klientem. Z uwagi na nieustanny rozwój technik informatycznych i telekomunikacyjnych trudno dziś ocenić, na ile te tendencje są stałe.

Największą rolę w rozwoju bankowości elektronicznej odgrywają same banki – szukając przewagi konkurencyjnej - oraz ich klienci, którzy stawiają bankom coraz wyższe wymagania dotyczące funkcjonalności i bezpieczeństwa świadczonych usług. Istotne znaczenie w procesie upowszechniania usług bankowości elektronicznej mają media, gdyż to w dużej mierze na podstawie przekazu medialnego klienci podejmują decyzje o rozpoczęciu korzystania z tych usług. Tym ważniejsza staje się jakość informacji prezentowanych w prasie i mediach elektronicznych.

Usługi bankowości elektronicznej stają się coraz bardziej bezpieczne dla jej użytkowników. Przykładem może być upowszechnienie kart z mikroprocesorem i pełne wdrożenie standardu EMV, co wyeliminuje takie uciążliwe zagrożenia, jak kopiowanie pasków magnetycznych z kart. Jednak korzystanie z bankowości elektronicznej - wygodne z punktu widzenia użytkownika - wymaga od klienta podstawowej wiedzy i przestrzegania zasad określonych w przepisach prawa oraz regulaminach bankowych. Główne obawy klientów dotyczą bezpieczeństwa transakcji. W przypadku bankowości internetowej dodatkowym aspektem jest obawa przed zagrożeniami związanymi z korzystaniem z Internetu.

Warunkiem bezpiecznego wykonywania transakcji bankowych drogą elektroniczną jest świadomość klienta w zakresie występujących zagrożeń i zachowanie przez niego zasad bezpieczeństwa.

W porównaniu z operacjami gotówkowymi płatności i transakcje elektroniczne cechują się znacznie lepszymi możliwościami ich zabezpieczenia, dokumentowania (elektronicznego)

i monitorowania. Korzystając z usług bankowości elektronicznej należy jednak pamiętać, że zapewnienie ich bezpieczeństwa jest procesem ciągłym, i że w dużym stopniu zależy od jej użytkowników.

Monitorowaniem rynku transakcji elektronicznych zajmuje się między innymi Narodowy Bank Polski i Związek Banków Polskich. Rosnąca skala omawianego zjawiska wymaga również ciągłego dostosowywania mechanizmów kontrolnych i nadzorczych do jego skali i charakteru, głównie poprzez opracowanie jednolitych zasad i narzędzi oceny ryzyka z tym związanego. Niniejszy Raport i *Przewodnik klienta usług bankowości elektronicznej* stanowią jeden z etapów takich działań, podejmowanych przez Komisję Nadzoru Finansowego.



URZĄD KOMISJI NADZORU FINANSOWEGO
Plac Powstańców Warszawy 1
00-950 Warszawa

tel. (+48 22) 262-50-00
fax (+48 22) 262-51-11 (95)
e-mail: knf@knf.gov.pl

Departament Relacji Zewnętrznych
tel. (+48 22) 262 56 66

www.knf.gov.pl