Honorata Balicka

BEZPIECZEŃSTWO TRANSAKCJI BANKOWYCH REALIZOWANYCH ZA POŚREDNICTWEM INTERNETU

WSTĘP

Jakość i pewność zabezpieczeń w banku, w którym świadczy się usługi za pośrednictwem ogólnoświatowej sieci, są czynnikami o kluczowym znaczeniu. Uzyskanie zaufania klienta w odniesieniu do bezpieczeństwa bankowości internetowej warunkuje dalszy rozwój bankowych serwisów webowych. Zapewnienie bezpieczeństwa w przypadku serwisu internetowego jest o tyle trudne, że część systemu informatycznego musi być dostępna z zewnątrz dla nabywców usług świadczonych poprzez Sieć. Elektroniczna obsługa klienta wymaga włączenia, go jako użytkownika, do skomputeryzowanego systemu bankowego[1]. Kierownictwo banku powinno zatem z jednej strony umożliwić usługobiorcom jak najszerszy dostęp do danych, a z drugiej – uniemożliwić nieuprawnioną komunikację z Internetu do wewnętrznego systemu informatycznego banku.

Rozwój technologii informacyjnych umożliwia zwiększanie bezpieczeństwa przy zachowaniu przejrzystości transakcji[2]. W bankach, ze względu na skalę i znaczenie działalności, stosuje się przetestowane i zaawansowane programy komputero-

---

[1] J. Gliniecka, *Bankowe usługi świadczone przy użyciu elektronicznych nośników informacji,* [w:] J. Gliniecka, *System bankowy w regulacjach polskich i unijnych*, Oficyna Wydawnicza Branta, Bydgoszcz 2003, s. 135.

[2] W. Szpringer, *E-commerce e-banking – wyzwania globalizacji*, Difin, Warszawa 2002, s. 143.

we[3]. Problem polega na tym, że oprogramowanie systemowe banku jest niezwykle skomplikowane, co tym bardziej utrudnia wykluczenie występowania w nim błędów zmniejszających bezpieczeństwo systemu.

Dla rozwoju bankowości internetowej duże znaczenie ma zarówno stan rzeczywisty, jak i percepcja poziomu bezpieczeństwa przez klientów. Nagłaśnianie przez środki masowego przekazu włamań hakerskich do systemów komputerowych należących do dużych korporacji powoduje, że wiele osób podchodzi do przekazywania poufnych danych przez Internet z dużą dozą ostrożności. Mimo że spektakularnie traktowane włamania hakerskie zazwyczaj nie dotyczą banków, zapadają jednak w świadomość ich klientów.

W krajach, w których możliwość dokonywania transakcji internetowych ma dłuższą tradycję niż w Polsce, można skupić się na podkreślaniu wygody i szybkości działania oraz na promocji nowych usług bankowości internetowej[4]. Natomiast do głównych zadań w bankach krajowych należy przede wszystkim przekonanie konsumentów o bezpieczeństwie przyjętych rozwiązań. Istotne są wówczas różnice w poziomie bezpieczeństwa bankowych serwisów WWW, ze szczególnym uwzględnieniem krajowych banków wirtualnych. Odmienne rozwiązania występują zwłaszcza na poziomie logowania się do systemu i uwierzytelniania użytkownika.

Celem niniejszego opracowania jest typologia oraz charakterystyka rodzajów zabezpieczeń stosowanych w bankowości internetowej. Na podstawie tak określonego celu sformułowano zagadnienie badawcze, polegające na analizie poziomu bezpieczeństwa zapewnianego w krajowych bankach wirtualnych. Zdeterminowanie celu pracy oraz sformułowanie zagadnienia badawczego pozwoliło na sprecyzowanie następującej hipotezy roboczej*:* Akceptowalny poziom bezpieczeństwa gwarantuje łączenie różnych rodzajów zabezpieczeń, a także edukacja użytkownika w zakresie zasad prawidłowego korzystania z serwisu internetowego.

Pod pojęciem bezpiecznej transakcji internetowej rozumie się transakcję o akceptowalnym dla banku oraz klienta poziomie autentyczności, poufności, integralności oraz niezaprzeczalności[5]. Z perspektywy instytucji bankowej do kluczowych atrybutów bezpieczeństwa należą autentyczność, integralność oraz niezaprzeczalność transakcji. Autentyczność oznacza prawidłową identyfikację osoby uprawnionej do wykonania transakcji bankowej za pośrednictwem Internetu. W celu zapewnienia autentyczności dostęp do systemu transakcyjnego bankowości internetowej jest poprzedzany uwierzytelnieniem użytkownika. Integralność gwarantuje brak modyfikacji danych w czasie ich przesyłania między komputerem ban-

---

[3] S. Baldi, *Sicherheit im Internet-Banking*, [w:] T. Burkhardt, K. Lohmann (red.), *Banking und Electronic Commerce in Internet,* Springer Verlag, Berlin 1998, s. 235.

[4] M. J. Cronin (red.), *Banking and finance on the Internet,* John Wiley & Sons, New York 1997, s. 243.

[5] A. Gospodarowicz, *Bankowość elektroniczna*, PWE, Warszawa 2005, s. 56.

ku a komputerem klienta. Niezaprzeczalność jest jednoznaczna z brakiem możliwości zakwestionowania transakcji dokonanej przez uprawnionego użytkownika.

Z punktu widzenia prywatnego odbiorcy usług, fundamentalne znaczenie mają takie cechy bezpieczeństwa, jak autentyczność, poufność oraz integralność. W tym sensie autentyczność jest tożsama z gwarancją korzystania z prawdziwej witryny Web banku. Poufność dotyczy braku możliwości nieuprawnionego dostępu do prywatnych danych, przechowywanych w systemie informatycznym banku. Integralność to gwarancja, że dane związane z realizowaną transakcją nie są modyfikowane podczas transmisji przez osoby trzecie.

Punkt odniesienia dla rozważań podjętych w niniejszym artykule stanowi pojęcie **bankowości internetowej**. Pod tym pojęciem rozumie się formę usług, umożliwiającą dostęp do rachunku oraz dokonywanie transakcji bankowych za pośrednictwem Internetu, komputera lub innego urządzenia elektronicznego. Bankowość internetowa jest jednym z najmłodszych i najszybciej rozwijających się rodzajów bankowości elektronicznej[6].

W artykule niniejszym poruszono problematykę bezpieczeństwa transakcyjnych serwisów WWW banków, zdefiniowano kluczowe pojęcia dotyczące: bezpiecznej transakcji internetowej oraz bankowości internetowej. Dokonano taksonomii zabezpieczeń istniejących w bankowości internetowej. Scharakteryzowano metody uwierzytelniania użytkownika, sposoby bezpiecznej transmisji danych oraz zabezpieczania serwerów banku. Opisano kluczowe zasady ochrony danych i programów na komputerze klienta. Wskazano możliwości wzmacniania stosowanych rozwiązań oraz kierunki dalszego rozwoju systemów bezpieczeństwa.

1. Klasyfikacja zabezpieczeń stosowanych w bankowości internetowej

Zapewnienie bezpieczeństwa, czyli poufności, integralności, niezaprzeczalności oraz autentyczności danych przetwarzanych w procesie realizowania transakcji w bankowości internetowej, dotyczy trzech obszarów. Pierwszy obszar związany jest z bezpieczeństwem transmisji danych między serwerem banku a komputerem klienta. Obszar drugi to bezpieczeństwo systemów informatycznych instytucji bankowej, w których to systemach są przechowywane i przetwarzane dane użytkownika bankowości internetowej. Obszar trzeci odnosi się do bezpieczeństwa danych i programów na komputerze usługobiorcy.

[6] Strona WWW Rady Bankowości Elektronicznej przy Związku Banków Polskich (2003), http://www.rbe.pl

Taksonomii zabezpieczeń stosowanych w bankowości elektronicznej, w tym również w bankowości internetowej, można dokonać ze względu na dwa kryteria[7]. Pierwszym kryterium jest metoda stosowanego zabezpieczenia. Na podstawie tego kryterium wyróżnia się:

- uwierzytelnianie proste (np. hasła, pytania osobiste, PIN),
- uwierzytelnianie silne (np. token, karta kryptograficzna, klucz prywatny),
- szyfrowanie transmisji danych,
- podpis elektroniczny.

Pierwsza i druga metoda nawiązują do autentyczności strony transakcji. Obie metody służą do identyfikacji poprzez weryfikację tożsamości osoby mającej prawo dostępu do systemu oraz wykonywania w nim operacji bankowych. Trzecia metoda, odwołująca się do poufności oraz integralności transferowanych danych, jest związana z kryptografią. Jej stosowanie ma uniemożliwić dostęp do poufnych danych oraz ich nieuprawnioną modyfikację podczas transmisji. Czwarta metoda wiąże się przede wszystkim z niezaprzeczalnością transakcji, polegającą na uniemożliwieniu klientowi zanegowania dokonanej przez niego operacji.

Druga klasyfikacja zabezpieczeń jest oparta na kryterium rodzaju zastosowanej techniki. Wyróżnia się zabezpieczenia:

- programowe (podstawową techniką jest kodowanie, system haseł i uwierzytelnianie),
- sprzętowe (wykorzystujące urządzenia zabezpieczające dane przed ujawnieniem),
- globalne (urządzenia techniczne współpracujące z oprogramowaniem, np. *firewall*).

W bankowości internetowej korzysta się zazwyczaj z zabezpieczeń podobnych do tych, jakie funkcjonują w handlu elektronicznym. Alternatywą jest stosowanie w bankach indywidualnych rozwiązań, które nie są powszechnie stosowane w Internecie. Mimo że wiążą się one z dodatkowymi kosztami i niedogodnościami dla klienta, jednak w znaczący sposób zwiększają bezpieczeństwo transakcji.

Realizację transakcji bankowej za pośrednictwem Sieci poprzedza uwierzytelnianie użytkownika. Brak powszechnie akceptowanego standardu jest przyczyną występowania różnorodnych metod elektronicznej identyfikacji eksploatatora internetowego kanału dystrybucji usług bankowych. Jednym z najczęściej stosowanych rozwiązań jest podwójna identyfikacja usługobiorcy. Polega ona na podawaniu **identyfikatora**, będącego indywidualnym numerem użytkownika (ang. *login*) oraz **hasła logowania** do systemu, tzw. hasła dostępu.

W trakcie procedury logowania z reguły wykorzystuje się hasła statyczne. Należy jednak zaznaczyć, że wyższy poziom bezpieczeństwa zapewniają hasła jedno-

[7] A. Jurkowski, *Bankowość elektroniczna*, Materiały i Studia NBP, Zeszyt 125, Warszawa 2001, s. 19.

razowe, zamieszczane na karcie kodów lub generowane każdorazowo przez specjalistyczne urządzenie – token lub kartę kryptograficzną. Przed zdobyciem hasła przez osoby nieuprawnione skuteczną ochronę zapewnia również stosowanie haseł maskowanych. Ich działanie polega na tym, że przy logowaniu się do serwisu bankowości internetowej nie podaje się pełnego hasła, lecz określone znaki, losowo wybrane przez system komputerowy banku. W wypadku hasła maskowanego istnieje możliwość przechwycenia go przez program komputerowy – „koń trojański".

Innym rozwiązaniem jest stosowanie pytań osobistych. Wspomniana metoda opiera się na udzielaniu przez klienta odpowiedzi na zadawane przez system informatyczny banku pytania. Są one formułowane na etapie rejestracji użytkownika do systemu. Pytania osobiste, podobnie jak hasła, umożliwiają proste uwierzytelnianie, które nie chroni przed destruktywnym działaniem „konia trojańskiego".

Bezpieczne logowanie się do systemu gwarantuje stosowanie klucza prywatnego. Może być on zapisany na dysku twardym serwera banku. Zalecane jest jednak przechowywanie klucza na nośniku klienta: w pamięci karty mikroprocesorowej lub na dysku twardym komputera. Logowanie do systemu z wykorzystaniem karty mikroprocesorowej polega na podaniu jej identyfikatora oraz kodu PIN. W wypadku klucza przechowywanego na dysku twardym komputera użytkownika lub w repozytorium banku, należy podać jednorazowe hasło chroniące klucz, które klient otrzymuje poprzez SMS.

Optymalne rozwiązanie zarówno w zakresie prawidłowego logowania się do systemu, jak i bezpiecznej transmisji danych stanowi **podpis elektroniczny, weryfikowany za pomocą kwalifikowanego certyfikatu**. Kluczowa rola kwalifikowanego podpisu cyfrowego w zapewnianiu bezpieczeństwa transakcji *online* zostanie opisana w dalszej części artykułu.

Do perspektywicznych metod wiarygodnej identyfikacji nabywców usług bankowych należą **metody biometryczne**. Umożliwiają one badanie takich cech fizycznych użytkownika, jak: tęczówka lub siatkówka oka, linie papilarne, układ naczyń krwionośnych na dłoni, kształt dłoni, kształt ucha, cechy twarzy, rozkład temperatur na twarzy, kształt i rozmieszczenie zębów, zapach oraz DNA. Przedmiotem analizy mogą być również cechy behawioralne użytkownika, jak: sposób chodzenia, podpis odręczny, technika pisania za pomocą klawiatury komputera, głos oraz fale mózgowe. Daktyloskopia była wykorzystywana już w latach 70. XIX wieku. Natomiast w drugiej połowie XX wieku wdrożono komputerowe metody biometryczne, wykorzystujące zazwyczaj: rogówkę oka, kształt twarzy oraz właściwości tembru głosu. Stosowanie wymienionych metod wymaga użycia czytnika, w celu pobrania odpowiednich danych, które następnie są porównywane z bazą danych.

Jednym z pierwszych przykładów zastosowań metod biometrycznych jest rozwiązanie zaproponowane przez amerykańską firmę Pay By Touch w odniesieniu do płatności za pomocą karty. Realizując transakcję płatniczą z wykorzystaniem karty, użytkownik składa odcisk palca na czytniku w momencie zapłaty, a transakcja zo-

staje zaliczona w poczet rachunku jego karty płatniczej, skojarzonej z odciskiem. Dokonywanie tego typu płatności wymaga rejestracji, która polega na przeciągnięciu karty płatniczej przez czytnik oraz złożeniu odcisku palca. W ten sposób obraz linii papilarnych jest kojarzony z kartą płatniczą. Pilotażową wersję tego systemu wdrożono w wybranych supermarketach brytyjskich oraz w sieci amerykańskich sklepów spożywczych Piggly Wiggly.

Kluczową rolę w wiarygodnej identyfikacji uczestników transakcji oraz w ochronie danych transmitowanych w Sieci odgrywa prawidłowy dobór technik kryptograficznych[8]. Do szyfrowania używa się algorytmów symetrycznych oraz algorytmów niesymetrycznych. Algorytmy symetryczne umożliwiają szybsze szyfrowanie, ale do ich wykorzystania konieczna jest wcześniejsza wymiana tajnego klucza. Algorytmy niesymetryczne są tej wady pozbawione, ale z powodu złożonych obliczeń szyfrowanie i deszyfrowanie są znacznie wolniejsze.

W odróżnieniu od zabezpieczeń serwerów banków, szyfrowanie przesyłanej informacji powinno opierać się na standardowych i dostępnych rozwiązaniach. W przeciwnym wypadku należałoby dostarczać klientom dedykowane oprogramowanie oraz sprzęt, jak np. w wypadku niemieckiego Sparda Banku. Wspomniane rozwiązanie podwyższa koszty i zmniejsza wygodę usługobiorcy. W konsekwencji niwelowane są zalety bankowości internetowej, do których zalicza się niskie koszty transakcji oraz sprawny dostęp do usług bankowych.

Mając na uwadze powyższe względy, powszechnie stosowanym protokołem bezpiecznego przesyłania wiadomości w postaci zaszyfrowanej jest *Secure Sockets Layer* (SSL) w wersji 3.0. Umożliwia on uwierzytelnianie serwerów biorących udział w połączeniu, zapewnia poufność oraz integralność transmitowanych danych. Standard SSL obsługiwany jest przez przeglądarki WWW, jak: Internet Explorer, Opera, Mozilla, Firefox oraz Netscape Navigator.

Wykorzystanie protokołu SSL jest związane z posiadaniem certyfikatu cyfrowego, który wystawia niezależna instytucja, tak zwana trzecia strona (ang. *Trusted Third Party*). W bankach krajowych wykorzystuje się zazwyczaj certyfikaty wystawiane przez dwie instytucje: VeriSign lub Thawte. Proces komunikacji bazujący na standardzie SSL rozpoczyna się wzajemną identyfikacją uczestniczących stron: banku oraz użytkownika bankowości internetowej. Identyfikacja banku polega na akceptacji przez przeglądarkę certyfikatu banku. Po akceptacji na ekranie użytkownika pojawia się ikona informująca o tym fakcie. Ikona ma z reguły symbol zamkniętej kłódki. Identyfikacja użytkownika może nastąpić również za pomocą certyfikatu, który w wybranych bankach oferuje się klientom jako dodatkowe zabezpieczenie.

---

[8] Opisu metod kryptograficznych stosowanych w bankowości internetowej dokonano, [w:] R. Opplinger, *IT – Sicherheit*, Verlag Vahlen, Braunschweig 1997.

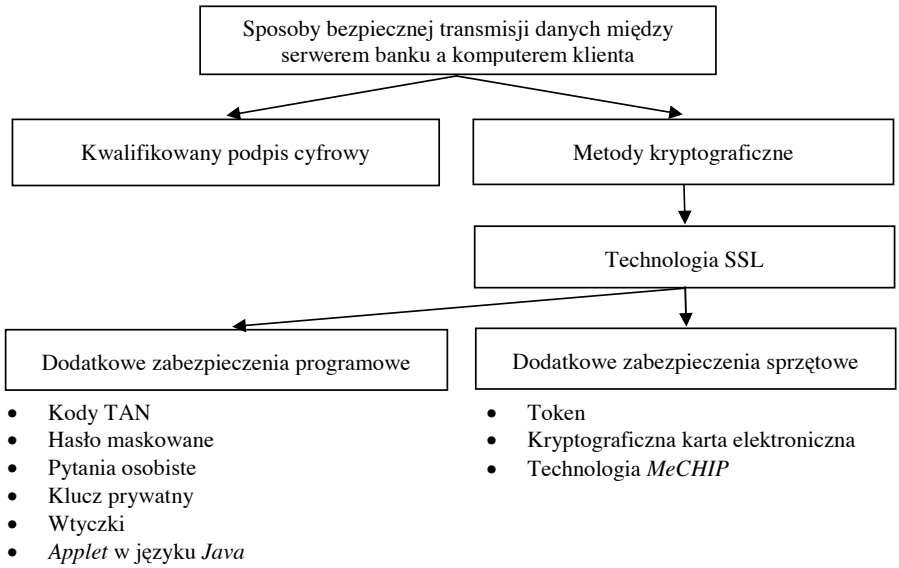
Po wzajemnej identyfikacji następuje wymiana kluczy sesyjnych, które są różne dla każdego połączenia. Następnie uzgadniane są stosowane procedury szyfrujące między serwerem banku a komputerem klienta. Po uzgodnieniu procedur szyfrujących użytkownik bankowości internetowej może przystąpić do wymiany właściwych danych z instytucją bankową. Długość stosowanego klucza sesyjnego nazywana jest mocą szyfrowania, którą wyraża się za pomocą liczby bitów. Im dłuższy klucz, tym połączenie jest bezpieczniejsze. Uważa się, że długość klucza sesyjnego równa 128 bitów, stosowanego najczęściej w bankach krajowych, stanowi silne bezpieczeństwo. Konieczne jest jednak stosowanie coraz dłuższych kluczy ze względu na rosnące moce obliczeniowe komputerów, za pomocą których łamie się szyfry.

Szyfrowanie za pomocą odpowiednio długiego klucza sesyjnego było do 2000 r. znacząco utrudnione. Wynikało to z prawa obowiązującego w USA, zabraniającego eksportu technologii szyfrowania stosujących klucze dłuższe niż 56 bitów. Ze względu na fakt, że przeglądarki WWW są produktami pochodzącymi z USA, ich wersje przeznaczone na eksport były ograniczone. Stwarzało to istotną barierę w rozwoju bankowości internetowej. Dopiero regulacja eksportowa dotycząca kryptografii z 14 stycznia 2000 r. wydana przez Departament Handlu rządu USA umożliwiła stosowanie kluczy 128-bitowych w zastosowaniach internetowych.

W stosunkowo niewielu bankach wykorzystuje się wyłącznie standard SSL. W celu zwiększenia poziomu bezpieczeństwa komunikacji w Internecie, implementuje się dodatkowe rozwiązania, wzmacniające standard SSL. Należą do nich rozwiązania programowe oraz sprzętowe (por. wykres 1).

Wśród zabezpieczeń stosowanych w bankowości internetowej kluczową rolę odgrywa podpis elektroniczny, weryfikowany za pomocy kwalifikowanego certyfikatu. Tego typu podpis określany jest mianem kwalifikowanego podpisu cyfrowego lub bezpiecznego podpisu cyfrowego. Podpis ten zapewnia zachowanie wszystkich atrybutów bezpiecznej transakcji *online*, to jest jej autentyczności, poufności, integralności oraz niezaprzeczalności.

Wykres 1. Zabezpieczenia stosowane w bankowości internetowej



Źródło: opracowanie własne.

Należy podkreślić, że nie każdy podpis elektroniczny jest cyfrowy i nie każdy podpis cyfrowy jest kwalifikowany. Pod pojęciem podpisu elektronicznego rozumie się dane w postaci elektronicznej, jak np. imię i nazwisko dołączone do dokumentu w formie elektronicznej. Podpis cyfrowy z kolei to podpis elektroniczny, w którym zastosowano metody kryptograficzne, opierające się głównie na asymetrycznych algorytmach kodujących. Natomiast podpis kwalifikowany to podpis cyfrowy potwierdzony certyfikatem. Pod pojęciem certyfikatu rozumie się zaświadczenie elektroniczne, zawierające dane służące do weryfikacji podpisu elektronicznego, głównie informacje dotyczące osoby, której został wydany, oraz podmiotu świadczącego usługi certyfikacyjne.

Podpis kwalifikowany zapewnia odbiorcy sprawdzenie autentyczności i integralności przesyłanych danych oraz gwarantuje niezaprzeczalność transakcji, a nadawcy – umożliwia skuteczną ochronę przed sfałszowaniem danych przez odbiorcę. Podstawową korzyścią dla klienta banku, wynikającą z wykorzystania podpisu kwalifikowanego, jest możliwość elektronicznego sygnowania dokumentów w obrocie prawnym i handlowym, w tym umów o prowadzenie rachunków bankowych oraz umów kredytowych. Podpis kwalifikowany jest bowiem równoważny pod względem skutków prawnych podpisowi własnoręcznemu.

Pierwszym bankiem w Polsce, w którym od marca 2006 r. umożliwia się klientom korzystanie z podpisu kwalifikowanego jest Nordea Bank Polska. Jednak w zdecydowanej większości banków krajowych wykorzystuje się podpis cyfrowy niekwalifikowany. Służy on do sygnowania elektronicznych wyciągów bankowych, przesyłanych usługobiorcom, np. PKO BP, Inteligo, mBanku i Multibanku. W programie Microsoft Outlook *e-mail* z podpisem cyfrowym zawiera ikonę stylizowaną na czerwoną pieczęć, umieszczoną w prawym górnym rogu listu. Podpis cyfrowy gwarantuje autentyczność danych zawartych w wyciągu i uwierzytelnia jego wydawcę. Dlatego też wyciągi z podpisem cyfrowym mogą być przekazywane w formacie PDF osobie trzeciej, np. w celu potwierdzenia dokonania operacji.

Istotne jest także ustawowe upoważnienie do świadczenia w instytucji bankowej usług certyfikacyjnych. Na podstawie przyznanego upoważnienia banki mogą odgrywać rolę gwaranta bezpieczeństwa transakcji i pełnić funkcję „zaufanej trzeciej strony" w infrastrukturze kwalifikowanego podpisu cyfrowego. Możliwość świadczenia usług certyfikacyjnych otworzyła nowy rynek usług, umożliwiający generowanie znaczących przychodów.

Mimo korzyści, jakie wynikają ze stosowania podpisu kwalifikowanego dla klienta oraz instytucji bankowej, usługa ta nie upowszechniła się jeszcze na rynku polskim. Analiza sposobów zabezpieczania transakcji internetowych w bankach krajowych prowadzi do wniosku, że do czasu szerszej implementacji podpisu kwalifikowanego optymalne jest stosowanie rozwiązań hybrydowych. Polegają one na łączeniu różnych rodzajów zabezpieczeń.

W funkcjonujących w Polsce trzech bankach wirtualnych akceptowalny poziom bezpieczeństwa uzyskuje się poprzez wzmacnianie standardowego protokołu szyfrującego SSL dodatkowymi zabezpieczeniami programowymi lub sprzętowymi (tabela 1). Pod pojęciem banku wirtualnego rozumie się jednostkę gospodarczą nie mającą innych kanałów dystrybucji poza Internetem, a w szczególności placówek stacjonarnych, lub taką, w której te kanały odgrywają marginalną rolę[9].

W ramach dodatkowych zabezpieczeń programowych powszechne zastosowanie mają hasła. Najczęściej wykorzystuje się kody TAN (ang. *Transaction Authorization Number*). Pod pojęciem kodu TAN, nazywanego także jednorazowym identyfikatorem transakcji, rozumie się hasło numeryczne przydzielone przez system informatyczny banku na wniosek posiadacza rachunku. Można je stosować do logowania się do systemu oraz do zatwierdzania transakcji, jak w Nordea Bank Polska. Użytkownik otrzymuje kody za pośrednictwem poczty tradycyjnej w postaci: karty kodów, jak np. w PKO BP czy Banku Pekao, lub karty uwierzytelniającej, jak np. w Nordea Bank Polska.

Coraz częściej stosuje się rozwiązanie polegające na przesyłaniu hasła SMS-em, jak np. w mBanku, Banku Pekao, Banku BPH, Citibanku czy ING Banku Ślą-

[9] J. Grzechnik, *Bankowość internetowa*, Internetowe Centrum Promocji, Gdańsk 2000, s. 56.

skim. Natomiast w związku z uruchomieniem internetowej przeglądarki głosowej *Intelligent Web Reader* w serwisie WWW Nordea Bank Polska, wprowadzono nowy rodzaj kart z jednorazowymi kodami, drukowanymi alfabetem Braille'a dla osób z dysfunkcją wzroku.

Tabela 1. Zabezpieczenia stosowane w bankach wirtualnych w Polsce

Lp.	Bank	Wystawca certyfikatu cyfrowego (technologia SSL)	Token	Kody TAN	Niekwalifikowany podpis cyfrowy	Inne
1.	mBank	1	–	+	+	Powiadamianie SMS-owe i mailowe
2.	Inteligo	1	–	+	+	Powiadamianie SMS-owe i mailowe
3.	VW Bank Direct	1	+	–	–	–

Objaśnienie symboli: 1 – VeriSign Public Primary; (+) stosuje się; (–) nie stosuje się.

Źródło: opracowanie własne na podstawie informacji zamieszczonych na stronach WWW banków; stan na dzień 01.02.2008 r.

Mimo że transmisja haseł w Internecie odbywa się w zaszyfrowany sposób, stosowanie kodów TAN wiąże się z dość istotnym ryzykiem. Istnieje bowiem możliwość zdobycia hasła przez osobę nieuprawnioną na skutek podpatrzenia momentu wprowadzania kodu do komputera przez użytkownika. Przed zdobyciem hasła przez niepowołane osoby chronią użytkownika hasła maskowane. Idea ich stosowania polega na losowym generowaniu fragmentu hasła przez system komputerowy banku, jak np. w Banku BPH, Banku Pekao, ING Banku Śląskim oraz w BZ WBK. Istnieje jednak zagrożenie przechwycenia hasła przez program komputerowy – „koń trojański".

Przed destruktywnym działaniem „konia trojańskiego" nie chroni także stosowanie pytań osobistych. Udzielanie odpowiedzi na pytania zadawane przez system informatyczny banku mogą być również przechwycone przez osoby niepowołane.

Do bardziej zaawansowanych rozwiązań programowych zalicza się klucz prywatny. Jest on generowany w postaci ciągu cyfr za pomocą algorytmu asymetrycznego RSA, po złożeniu przez klienta wniosku za pośrednictwem Internetu. RSA jest najpopularniejszym asymetrycznym algorytmem kodującym. Klucz prywatny

wykorzystuje się jako podpis elektroniczny, służący do logowania się do systemu oraz do potwierdzania transakcji. Użytkownicy biznesowi Banku BPH mogą otrzymać klucz prywatny zapisany w pamięci karty mikroprocesorowej, wydawanej wraz z czytnikiem do dyspozycji usługobiorcy. Natomiast klientom ING Banku Śląskiego oferuje się klucz prywatny zapisany na serwerze banku, bądź na nośniku usługobiorcy: dysku twardym komputera lub na dyskietce.

Wśród zaawansowanych rozwiązań programowych na uwagę zasługują wtyczki (ang. *plug-ins*). Pod pojęciem *plug-in* rozumie się niesamodzielny program rozszerzający funkcjonalność przeglądarki. Program przeznaczony jest do działania w wybranym systemie operacyjnym. Wtyczki mogą korzystać ze standardowych mechanizmów bezpieczeństwa przeglądarki, takich jak SSL. Programy tego typu mogą także rozszerzać mechanizmy bezpieczeństwa przeglądarki lub zastępować je własnymi rozwiązaniami. Przykładem tej ostatniej sytuacji jest wtyczka A & O stosowana przez Allgemeine Deutsche Directbank (Deutsche Directbank 2007)[10]. We wtyczce A & O używana jest procedura Triple-DES z dwoma kluczami. DES jest najpopularniejszym symetrycznym algorytmem kodującym. Do identyfikacji klienta stosowany jest cyfrowy podpis RSA z kluczem o długości 768 bitów. Wśród banków funkcjonujących w Polsce, w których stosuje się rozwiązanie programowe oparte na wtyczce *ActiveX*, znajduje się Bank BPH.

Inne rozwiązania technologiczne, opierające się na języku programowania komputerów ***Java***, również umożliwiają rozszerzenie funkcjonalności przeglądarki. Różnią się jednak znacząco od wtyczek. Przede wszystkim odpowiedni program – *applet* ładowany jest z Internetu. Ułatwia to aktualizację programu i nie wiąże klienta z konkretnym komputerem. Ładowany przez komputer klienta *applet* jest zaszyfrowany i sygnowany cyfrowym podpisem banku.

Program napisany w języku *Java* jest niezależny od systemu operacyjnego klienta, co sprawia, że w banku nie trzeba przygotowywać różnych wersji programu. Egzemplifikacją opisywanego rozwiązania jest system Brokat X-PRESSO, stosowany w Deutsche Banku 24. W appletach X-PRESSO wykorzystuje się podczas komunikacji z serwerem banku własny protokół SRT (ang. *Secure Request Technology*). Dokonano implementacji 1024-bitowej procedury RSA oraz 128-bitowej procedury IDEA. IDEA jest symetrycznym algorytmem szyfrującym, typowanym na następcę algorytmu DES. Elementy systemu X-PRESSO można aktualizować, co utrudnia potencjalne ataki wirusów komputerowych. W Polsce *applety* języka *Java* stosuje się między innymi w podsystemie bankowości internetowej *Makler* Banku BPH oraz w systemie bankowości internetowej *ING BankOnLine* ING Banku Śląskiego.

Program pisany w *Javie* jest rozwiązaniem z wielu względów bardzo korzystnym. Po pierwsze, nie wiąże klienta z jednym komputerem. Po drugie, nie wymaga

[10] Strona internetowa Deutsche Directbank (2007), http://www.directbank.de

dodatkowych komponentów sprzętowych. Po trzecie, w wypadku wystąpienia luki w systemie bezpieczeństwa można ją automatycznie aktualizować.

W bankach wykorzystuje się również dodatkowo zabezpieczenia sprzętowe. Jednym z nich jest token. Pod tym pojęciem rozumie się urządzenie kryptograficzne, którego działanie polega na generowaniu unikatowych ciągów cyfr, będących jednorazowymi hasłami. Token chroniony jest hasłem lub PIN-em. Urządzenie to pełni rolę podpisu elektronicznego, wykorzystywanego do identyfikacji użytkownika oraz do akceptacji dyspozycji internetowych. Opisywane zabezpieczenie sprzętowe znalazło zastosowanie m.in. w bankach: BZ WBK, Nordea Bank Polska oraz VW Bank Direct.

Kryptograficzne karty elektroniczne, to karty chipowe, używane zazwyczaj do ochrony i przechowywania klucza prywatnego klienta. Wbudowany mikroprocesor wykonuje obliczenia związane z weryfikacją klucza. Zastosowanie karty chipowej uniemożliwia przechwycenie prywatnego klucza klienta banku za pomocą „konia trojańskiego". Wadą karty jest konieczność stosowania czytnika kart podłączonego do komputera użytkownika.

Zaawansowanym rozwiązaniem sprzętowym jest technologia *MeCHIP*. Jej elementem jest układ elektroniczny włączany między komputer a klawiaturę. Układ szyfruje wpisywane dane jeszcze przed ich dotarciem do pamięci komputera. Wykorzystanie technologii *MeCHIP* uniemożliwia przechowywanie danych w postaci niezaszyfrowanej.

Kolejnym ważnym obszarem bezpieczeństwa w bankowości internetowej jest ochrona systemów informatycznych banku. Decydującą rolę odgrywa odpowiednie zabezpieczenie komputera centralnego, które uniemożliwiałoby osobom nieuprawnionym wgląd do transakcji, kont oraz danych podlegających prawnej ochronie lub tajemnicy bankowej.

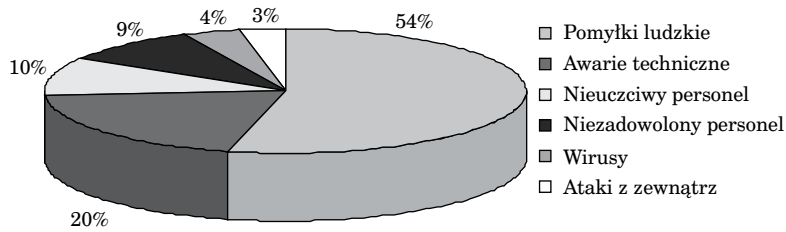
Bezpieczeństwo systemu komputerowego banku zapewnia się przede wszystkim za pomocą technologii *firewall*. Przez zabezpieczenia typu *firewall* do wewnętrznego systemu komputerowego banku nie przedostają się wiadomości pochodzące z nieuprawnionych źródeł. Omawiana technologia opiera się na stałym filtrowaniu danych przesyłanych z zewnątrz do wewnętrznej sieci banku. Zastosowanie technologii *firewall* zapewnia niewidzialność wewnętrznej struktury sieci komputerowej banku dla użytkownika Internetu[11].

Podkreślenia wymaga fakt, że ataki i wirusy stanowią jedynie 7% udział w zagrożeniach bezpieczeństwa systemu informatycznego banku. Znacznie większy udział w zagrożeniach ma działalność pracowników banku – 73%, na którą to działalność składają się pomyłki ludzkie – 54%, nieuczciwy personel – 10% oraz

[11] W. R. Chestwick, S. M. Bellovin, A. D. Rubin, *Firewalle i bezpieczeństwo w sieci*, Wydawnictwo Helion, Gliwice 2003.

niezadowolony personel – 9%. Pozostałe zagrożenia wynikają z awarii technicznych – 20% (wykres 2).

Wykres 2. Zagrożenia bezpieczeństwa systemu informatycznego banku



Źródło: A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.

Ważną rolę odgrywa **polityka bezpieczeństwa banku**, związana z rozsądnym przydzieleniem uprawnień pracownikom banku[12]. Wspomniana polityka obejmuje maksymalne ograniczenie bezpośredniego dostępu do systemu zabezpieczeń w myśl zasady „minimalnych niezbędnych uprawnień"[13]. Konieczne jest również wyznaczenie osoby bezpośrednio odpowiedzialnej za bezpieczeństwo systemu. Ponadto, w banku przygotowuje się awaryjne procedury na wypadek naruszenia bezpieczeństwa.

Ważnym elementem skutecznej ochrony systemu informatycznego banku jest **systematyczne testowanie oraz unowocześnianie zabezpieczeń w miarę postępu technicznego**. Podobnie w miarę zwiększania się liczby klientów oraz usług bankowego serwisu WWW, kluczowego znaczenia nabiera odpowiedni dobór metod zapewniających należytą przepustowość infrastruktury sieciowej oraz chroniących przed nadmiernym obciążeniem serwerów banku. Niedostateczna przepustowość infrastruktury może doprowadzić do zablokowania serwerów, a w konsekwencji do nieuprawnionego dostępu hakerów do wewnętrznego systemu informatycznego banku.

W miarę wzrostu liczby klientów lub usług, serwis internetowy można stosunkowo sprawnie rozbudować do wymaganej przepustowości. Odbywa się to zazwyczaj przez dokupienie serwerów lub przez powiększenie przepustowości infrastruktury sieciowej. Wydajność banku internetowego można również zwiększyć za pomocą

[12] S. Giannakoudi, *Internet banking. The digital voyage of banking and money in cyberspace*, „Information & Communications Technology Law", 1999 Vol. 8, No. 3.

[13] J. Gliniecka, *Tajemnica finansowa*, Wyd. Branta, Bydgoszcz–Gdańsk 2007.

równoważenia obciążeń serwerów bankowych[14]. Wykazano, że za pomocą odpowiedniego przydziału modułów programistycznych można kilkakrotnie zmniejszyć obciążenie newralgicznego serwera w systemie bankowym[15]. Przyjmując, że moc obliczeniowa serwerów bankowych, które dostępne są na rynku, podwaja się co półtora roku, zastosowanie optymalizacji obciążenia serwerów bankowych umożliwia uzyskanie przewagi konkurencyjnej banku na trzy lata w zakresie wydajniejszego serwisu internetowego. Ostatnia z wymienionych możliwości nabiera szczególnego znaczenia wobec szukania w bankach sposobów ograniczania kosztów, co pozwoliłoby efektywniej wykorzystać zasoby informatyczne.

Bankowość tradycyjna jest pod tym względem nieporównywalnie mniej elastyczna. Oddziału tradycyjnego nie można zazwyczaj w relatywnie szybki sposób rozbudować ze względu na ograniczenia organizacyjne i przestrzenne[16].

Trzecim, i jednocześnie najtrudniejszym obszarem do zapewnienia bezpieczeństwa w bankowości internetowej, jest ochrona danych i programów na komputerze klienta. Sprzęt i oprogramowanie wykorzystywane przez usługobiorcę jest najsłabszym ogniwem systemu ochrony w bankowości internetowej, ponieważ na ich konfigurację i poziom bezpieczeństwa personel banku ma niewielki wpływ. Ponadto, użytkownik indywidualny nie ma zazwyczaj wiedzy ani środków wystarczających do profesjonalnego zabezpieczenia własnego komputera[17].

W czasie połączenia z siecią Internet komputer usługobiorcy może stać się tak samo obiektem włamania jak system informatyczny banku. Raport firmy Symantec z 2006 r. ujawnił nasilenie się ataków na aplikacje w komputerach indywidualnych odbiorców usług finansowych (86% przypadków) w celu osiągnięcia korzyści materialnych. Drugie miejsce zajęły przedsiębiorstwa świadczące usługi finansowe, natomiast trzecie – sektor administracyjno-rządowy[18].

Do najczęstszych sposobów ataków hakerskich na oprogramowanie klienta zalicza się *phishing* oraz „konie trojańskie". Atak typu *phishing* polega na próbie uzyskania przez osobę trzecią poufnych informacji użytkownika bankowości internetowej poprzez sfałszowaną stronę WWW banku. Natomiast atak za pomocą „konia trojańskiego" polega na przesyłaniu Siecią programu komputerowego, który użytkownik uruchamia, nie wiedząc o jego ukrytych funkcjach. Programy te mogą

---

14 H. Balicka, J. Balicki, *Pareto-optimal Load Solutions in the I-Banking by Evolutionary Algorithm*, „Inteligencia Artyficial, Revista Iberoamericana de Inteligencia Artyficial", 2005, Vol. 9, No. 28, Invierno, s. 33–40.

15 H. Balicka, J. Balicki, *Effective Program Module Assignment in the Internet Banking by Tabu-based Evolutionary Algorithm,* „WSEAS Transactions on Mathematics", 2004, Issue 3, Vol. 3, s. 527–532.

16 J. Pietrzak, *Czynniki przewagi konkurencyjnej na rynku bankowych usług detalicznych*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2002, s. 125.

17 Na temat zagrożeń na poziomie systemu informatycznego banku oraz komputera użytkownika bankowości internetowej, [w:] D. Dżega, *(Nie)bezpieczny e-bank*, „Internet", 2003, nr 10.

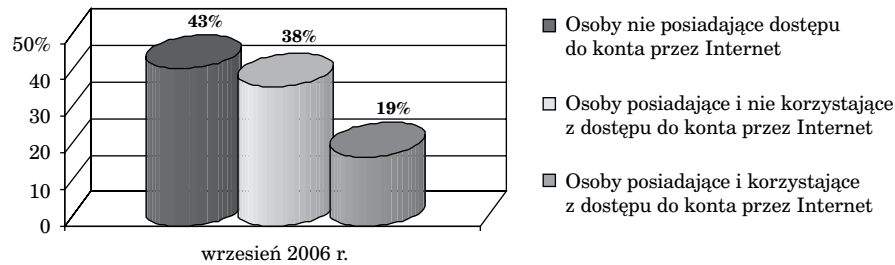
18 Strona WWW Symantec (2006), http://www.symantec.com/pl

przejąć kontrolę nad aplikacją bankową lub pozyskać poufne dane internauty bez jego wiedzy. Mechanizmy *phishingu* oraz „konia trojańskiego" znajdują się zazwyczaj w e-mailu wysłanym do prywatnego użytkownika od nieznanego nadawcy.

W kontekście zwiększania poziomu bezpieczeństwa najsłabszego ogniwa w bankowości internetowej należy podkreślić ważną, edukacyjną rolę bankowych serwisów informacyjnych WWW. Za ich pośrednictwem użytkownik może zapoznać się między innymi z kluczowymi zasadami bezpiecznego korzystania z konta bankowego za pośrednictwem Internetu. Bezpieczeństwo danych i programów na komputerze klienta zależy przede wszystkim od zachowania przez niego podstawowych środków ostrożności. Należą do nich głównie: systematyczne aktualizowanie systemu operacyjnego oraz programu antywirusowego, stosowanie programów typu *firewall* oraz *antydialer*. Ponadto, ważne jest, aby korzystać z tzw. silnych haseł, generowanych przez dodatkowe urządzenia, jak: token czy karta kryptograficzna.

Stan rzeczywisty, jak również percepcja poziomu bezpieczeństwa transakcji internetowych, odgrywa kluczową rolę w budowaniu zaufania użytkownika bankowego serwisu WWW, a w konsekwencji wpływa na rozwój bankowości internetowej. W Polsce odnotowano istotną dysproporcję między odsetkiem osób posiadających i nie korzystających z dostępu do konta przez Internet (38%), a odsetkiem osób posiadających i korzystających z dostępu do konta za pośrednictwem Sieci (19%) (wykres 3).

Wykres 3. Użytkowanie konta z dostępem do Internetu przez klientów banków w Polsce

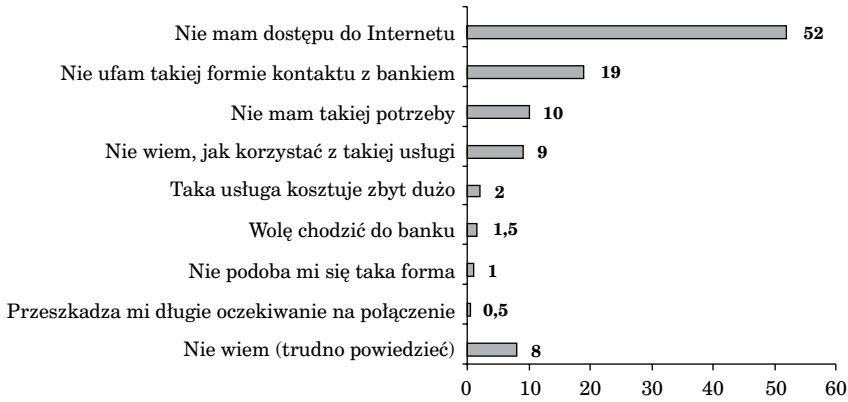


Źródło: opracowanie własne na podstawie wyników badań: TNS OBOP (2006), www.tns-global.pl

Do jednej z głównych przyczyn zaistnienia wspomnianej dysproporcji można zaliczyć stosunkowo słabo rozwiniętą infrastrukturę telekomunikacyjną kraju z punktu widzenia gęstości sieci, jej jakości oraz kosztów użytkowania. Wymienione przeszkody są szczególnie odczuwalne poza największymi miastami Polski. Nie posiadanie dostępu do Internetu, ale także brak zaufania do tej formy kontaktu z bankiem były najczęściej wymienianymi przyczynami niechęci wobec bankowości internetowej wśród ankietowanych klientów banków krajowych (wykres 4).

Natomiast na pierwszym miejscu w hierarchii barier rozwoju bankowości internetowej, wskazanych przez ekspertów w Polsce, znalazł się brak poczucia bezpieczeństwa (tabela 2). Przekonanie usługobiorców o skuteczności przyjętych rozwiązań może przyczynić się do zmniejszenia dysproporcji między klientami korzystającymi i nie korzystającymi z dostępu do konta przez Internet.

Wykres 4. Przyczyny niechęci wobec bankowości internetowej wskazywane przez klientów banków w Polsce



Źródło: Na podstawie badań przeprowadzonych wśród klientów banków przez firmę ARC Rynek i Opinia, [w:] R. Bratek, *Czas ekspansji*, „Bank", 2003, nr 3; (respondent mógł wybrać więcej niż jedną odpowiedź).

Skłonność usługobiorców do regularnego użytkowania serwisu WWW banku jest problemem złożonym, obejmującym między innymi: wzrost dostępności usług telekomunikacyjnych, obniżenie kosztów komputerów, zmniejszenie opłat za korzystanie z Internetu oraz zwiększenie poziomu zaufania do internetowej formy kontaktu z bankiem. Na wzrost zainteresowania serwisem webowym wpływa również wdrażanie zaawansowanych usług bankowości internetowej[19].

[19] H. Balicka, *Stopień zaawansowania oferty internetowej a konkurencyjność banku*, „Bank i Kredyt", 2008, nr 6, s. 37–57.

Tabela 2. Hierarchia barier rozwoju bankowości internetowej w Polsce

Lp.	Bariera	Ocena (od 1 do 10 pkt.)
1	Bezpieczeństwo transakcji (subiektywnie odczuwane przez klientów)	2,3
2	Wysokie koszty sprzętu komputerowego	1,9
3	Nawyki klientów przyzwyczajonych do tradycyjnej obsługi	1,7
4	Wysokie koszty połączeń z Internetem	1,1
5	Mała przepustowość sieci i trudności z dostępem do niej	1,0
6	Przeświadczenie, że korzystanie z Internetu wymaga specjalnej wiedzy i umiejętności	0,7
7	Zmonopolizowany rynek telekomunikacyjny w Polsce	0,7
8	Brak rozwiązań prawnych i systemowych gwarantujących bezpieczeństwo transakcji	0,6

Źródło: Na podstawie badań przeprowadzonych na grupie ekspertów przez Instytut Badań nad Gospodarką Rynkową, Gdańsk, luty 2002 r., [w:] R. Bratek, *op. cit.*

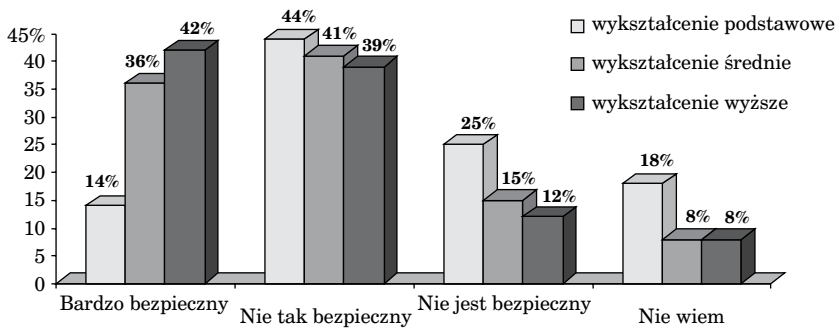
Ze względu na większe zaawansowanie bankowości internetowej w Niemczech cenne wskazówki, co do rozwoju bankowych serwisów WWW w Polsce, stanowią wyniki badania percepcji poziomu bezpieczeństwa bankowości internetowej przez konsumentów niemieckich[20]. Podział badanych ze względu na wykształcenie pozwolił stwierdzić, że zaufanie do poziomu bezpieczeństwa banków jest wprost proporcjonalne do poziomu wykształcenia (zob. wykres 5).

Wraz z rosnącą liczbą osób z wyższym wykształceniem i osiągających wyższe dochody w Polsce należy spodziewać się wzrostu zainteresowania ofertą serwisów internetowych banków. Ponadto, potrzebę rozwoju transakcyjnych serwisów bankowości internetowej wymusza dynamicznie rozwijający się elektroniczny rynek usług finansowych w kształtującej się erze gospodarki elektronicznej. Internet jest jednym z najnowocześniejszych kanałów dystrybucji, który odgrywa kluczową rolę

[20] Badanie zostało przeprowadzone przez Związek Banków Niemieckich we współpracy z Mannheimer Forschungsgruppe Wahlen Online GmbH w czasie od 26 lipca do 16 sierpnia 2000 r. Próba objęła zarówno korzystających, jak i nie korzystających z Internetu. Szczegółowe wyniki badania opublikowano na stronie internetowej Związku Banków Niemieckich, http://www.bdb.de/, grudzień 2000.

w zwiększeniu zdolności konkurencyjnych banku we współczesnych realiach konkurowania[21].

Wykres 5. Percepcja poziomu bezpieczeństwa bankowości internetowej ze względu na wykształcenie



Źródło: Związek Banków Niemieckich (2000), http://www.bdb.de/

Za dynamicznym rozwojem serwisów WWW przemawiają przede wszystkim takie argumenty, jak możliwość redukcji kosztów oraz zwiększenia jakości usług[22]. Dążenie do wzrostu konkurencyjności poprzez zmniejszenie kosztów, zwiększenie jakości i dostępności usług, a także szybkości ich wykonania stanowi kluczową przesłankę do wprowadzania efektywnych rozwiązań internetowych[23]. Podkreślenia wymaga w szczególności fakt, że wykorzystanie ogólnoświatowej sieci ma znaczący wpływ na rozwój nowoczesnych instrumentów finansowych[24].

WNIOSKI

Stosowane w bankach rozwiązania zapewniają akceptowalny poziom bezpieczeństwa zarówno w obszarze komunikacji między serwerem banku a komputerem klienta, jak i w obszarze systemu informatycznego banku. Skuteczność stosowanych mechanizmów wynika z łączenia różnorodnych technik zapewniania bezpie-

---

21 J. K. Solarz, *Bankowość międzynarodowa*, Twigger S.A., Warszawa 2004.

22 B. Pietrzak, *System bankowy – perspektywy rozwoju*, [w:] B. Pietrzak, Z. Polański, B. Woźniak (red.), *System finansowy w Polsce*, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 111.

23 W. Baka, *Przemiany potencjału bankowego – wpływ nowych technologii,* [w:] W. Baka, *Bankowość europejska*, Wydawnictwo Naukowe PWN, Warszawa 2005, s. 248.

24 E. Pietrzak, *Główne ośrodki obrotów pochodnymi instrumentami finansowymi w świecie*, [w:] Pietrzak E., Markiewicz M. (red.), *Finanse, bankowość i rynki finansowe*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2006, s. 435–443.

czeństwa. Rozwiązania hybrydowe dotyczą zwłaszcza dodatkowych zabezpieczeń sprzętowych i programowych, stosowanych w celu prawidłowego uwierzytelniania użytkownika. Dodatkowe zabezpieczenia wzmacniają standardowy protokół szyfrujący SSL.

Efektywną ochronę systemu informatycznego banku zapewniają rozwiązania globalne, typu *firewall*. Polegają one na wykorzystaniu urządzeń technicznych współpracujących z oprogramowaniem. Ponadto, istotną rolę odgrywa przestrzeganie w bankach zasady „minimalnych niezbędnych uprawnień" dostępu personelu do systemu zabezpieczeń.

Najtrudniej jest zapewnić bezpieczeństwo danych i programów umieszczonych na komputerze klienta. Dlatego do głównych zadań w bankach należy wspieranie edukacji w zakresie bezpiecznego korzystania z serwisów internetowych. Aktywnym podejściem personelu banku we wspomnianym obszarze jest tworzenie w serwisie WWW tzw. centrum edukacyjno-doradczego. Obejmuje ono informacje dotyczące m.in. kluczowych zasad właściwego postępowania użytkownika bankowości internetowej oraz środków bezpieczeństwa stosowanych w banku.

Należy podkreślić, że istotnym elementem polityki bezpieczeństwa w banku jest systematyczne analizowanie nowości technologicznych oraz ich testowanie pod kątem możliwości wzmocnienia bezpieczeństwa serwisów WWW. Nie można bowiem wykluczyć potencjalnego naruszenia istniejących metod kryptograficznych przez osoby nieuprawnione w najbliższej przyszłości.

Bibliografia

Baka W., *Bankowość europejska*, Wydawnictwo Naukowe PWN, Warszawa 2005.

Balicka H., *Stopień zaawansowania oferty internetowej a konkurencyjność banku*, „Bank i Kredyt", 2008, nr 6.

Balicka H., Balicki J., *Pareto-optimal Load Solutions in the I-Banking by Evolutionary Algorithm*, „Inteligencia Artyficial. Revista Iberoamericana de Inteligencia Artyficial", 2005, Vol. 9, No. 28.

Balicka H., Balicki J., *Effective Program Module Assignment in the Internet Banking by Tabu-based Evolutionary Algorithm,* „WSEAS Transactions on Mathematics", 2004, Issue 3, Vol. 3.

Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.

Bratek R., *Czas ekspansji*, „Bank", 2003, nr 3.

Burkhardt T., Lohmann K. (red.), *Banking und Electronic Commerce in Internet,* Springer Verlag, Berlin 1998.

Chestwick W. R., Bellovin S. M., Rubin A. D., *Firewalle i bezpieczeństwo w sieci*, Wydawnictwo Helion, Gliwice 2003.

Cronin M. J. (red.), *Banking and finance on the Internet,* John Wiley & Sons, New York 1997.

Dżega D., *(Nie)bezpieczny e-bank*, „Internet", nr 10 2003.

Giannakoudi S., *Internet banking. The digital voyage of banking and money in cyberspace*, „Information & Communications Technology Law", 1999, Vol. 8, No. 3.

Gliniecka J., *System bankowy w regulacjach polskich i unijnych*, Oficyna Wydawnicza Branta, Bydgoszcz 2003.

Gliniecka J., *Tajemnica finansowa*, Wyd. Branta, Bydgoszcz–Gdańsk 2007.

Gospodarowicz A., *Bankowość elektroniczna*, PWE, Warszawa 2005.

Grzechnik J., *Bankowość internetowa*, Internetowe Centrum Promocji, Gdańsk 2000.

Jurkowski A., *Bankowość elektroniczna*, Materiały i Studia NBP, Zeszyt 125, Warszawa 2001.

Opplinger R., *IT – Sicherheit*, Verlag Vahlen, Braunschweig 1997.

Pietrzak B., Polański Z., Woźniak B. (red.), *System finansowy w Polsce*, Wydawnictwo Naukowe PWN, Warszawa 2003.

Pietrzak E., Markiewicz M. (red.), *Finanse, bankowość i rynki finansowe*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2006.

Pietrzak J., *Czynniki przewagi konkurencyjnej na rynku bankowych usług detalicznych*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2002.

Solarz J. K., *Bankowość międzynarodowa*, Twigger S. A., Warszawa 2004.

Szpringer W., *E-commerce e-banking – wyzwania globalizacji*, Difin, Warszawa 2002.