PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1062 — 2005
Finanse, Bankowość, Rachunkowość 3

Michał Kisiel

WYBRANE TECHNICZNO-TECHNOLOGICZNE UWARUNKOWANIA ROZWOJU BANKOWOŚCI INTERNETOWEJ W POLSCE W LATACH 2000-2003 (STAN Z LUTEGO 2004 ROKU)

1. Wstęp

Spośród wszystkich obszarów otoczenia banku najszybszym przemianom podlega bez wątpienia środowisko techniczno-technologiczne. Technologią mającą dla banków znaczenie pierwszoplanowe stał się w ostatnich latach internet. Jego rola w działaniu banku stale się rozszerza – początkowo był wyłącznie narzędziem komunikacji z rynkiem, następnie kanałem dystrybucji, a stopniowo staje się również podstawą kreowania nowych produktów, wyróżniających ofertę banku na rynku. Świadczenie usług bankowych za pośrednictwem sieci często określane jest mianem bankowości internetowej. Pojęcie to wraz ze wzrastającą popularnością sieci i jej nowych zastosowań obejmuje kolejne zjawiska, jak np. agregacja rachunków czy systemy płatności w handlu elektronicznym, wykraczając poza wąskie rozumienie bankowości internetowej jako „internetowego dostępu do rachunku". Z tych względów analiza zewnętrznych uwarunkowań mających wpływ na rozwój bankowości internetowej w Polsce nabiera dla banków znaczenia strategicznego.

Istotą internetu jest ciągły rozwój podporządkowany logice „zawłaszczania" kolejnych sieci i włączania ich do swojej struktury. Przemianom podlega również zasięg sieci, jej zawartość (coraz szersze pasmo oznacza możliwość transmitowania coraz bogatszych przekazów, jak np. wideo czy dźwięk) oraz technologie rządzące jej funkcjonowaniem (kolejne wersje protokołów komunikacyjnych). Czynniki te sprawiają, że trudno jest całościowo uchwycić charakter internetu – jest on wciąż płynny, podlega stałym zmianom. Dlatego też oparcie strategii konkurencyjnej na wykorzystaniu tej technologii, wymaga ciągłej analizy zmian i śledzenia innowacji mogących wywrzeć wpływ na funkcjonowanie banku i atrakcyjność jego oferty rynkowej.

Dla banku oferującego bankowość internetową wymiar strategiczny mają przede wszystkim zagadnienia:

- dostępności internetu i rozwoju technologii dających dostęp do zasobów sieci,
- jakości dostępnych rozwiązań technologicznych zapewniających bezpieczeństwo komunikacji w internecie i głównych kierunków przemian w tej dziedzinie,
- rozmiarów i form zagrożeń bezpieczeństwa komunikacji w internecie.

Wymienione czynniki nie stanowią całokształtu uwarunkowań techniczno-technologicznych istotnych z punktu widzenia banku, lecz koncentrują w sobie najważniejsze i najbardziej pilne problemy hamujące rozwój bankowości internetowej w Polsce. W artykule zaprezentowane zostaną główne kierunki przemian w wymienionych wyżej obszarach i wynikające z nich konsekwencje dla banków rozwijających bankowość internetową w Polsce.

2. Infrastruktura internetu w Polsce i jej dostępność

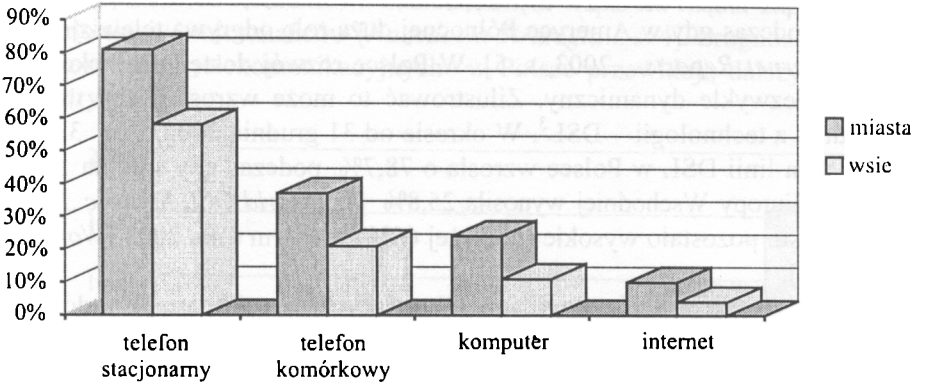
Szeroka dostępność internetu jest czynnikiem warunkującym niezakłócony rozwój gospodarki elektronicznej, ma zatem bezpośredni wpływ również na możliwości rozwoju bankowości internetowej. W Polsce w latach 2000-2003 miał miejsce skok zarówno jakościowy, mierzony liczbą stosowanych technologii dostępu i szerokością pasma, jak i ilościowy – znajdujący swój wyraz w znacznym zwiększeniu się liczby użytkowników sieci.

Dostępność internetu ograniczona jest w pierwszym rzędzie przez liczbę komputerów i telefonów komórkowych znajdujących się w dyspozycji gospodarstw domowych w Polsce. Urządzenia te pozwalają na korzystanie z sieci w szerszym lub węższym zakresie[1]. Liczba komputerów osobistych na 100 mieszkańców wyniosła w Polsce w 2003 r. 12,5. Jest to niepokojąco niski wskaźnik – wśród krajów wchodzących do Unii Europejskiej w gorszej sytuacji były tylko Węgry [*Polska na końcu...* 2004]. Penetracja sieci telefonii stacjonarnej (liczba linii na 100 mieszkańców) osiągnęła w 2003 r. poziom 34,7, a telefonii komórkowej – 43[2]. Nasycenie komputerami i telefonami komórkowymi stale wzrasta, utrzymuje się jednak wciąż niekorzystna dysproporcja między miastem a wsią (rys. 1). Dysproporcja ta rzutuje następnie na możliwości dostępu do sieci (rys. 2).

Zagadnienie dostępności internetu w Polsce jest ściśle powiązane ze strukturą rynku telekomunikacyjnego – odchodzenie od monopolu Telekomunikacji Polskiej SA przyczynia się do zwiększenia możliwości wyboru zarówno technologii dostępu, jak i podmiotów świadczących takie usługi. Do roku 1999 jedynym pow-

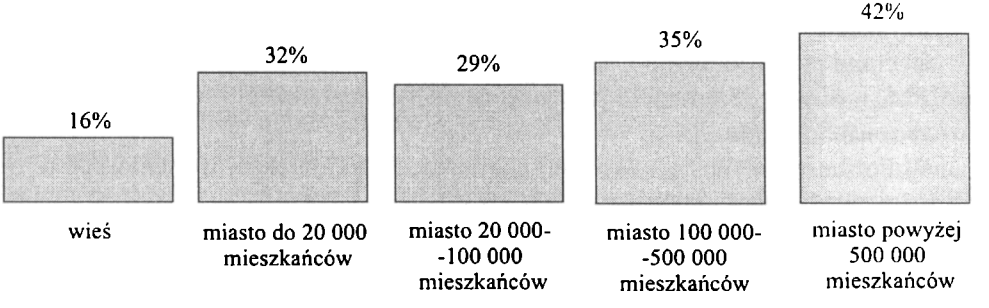
[1] Współczesne telefony komórkowe, tzw. drugiej generacji, w większości posiadają wbudowaną przeglądarkę WAP, pozwalającą korzystać ze specjalnie przystosowanych do telefonów stron w języku WML. Znaczna część banków oferujących bankowość internetową w Polsce udostępnia również serwisy transakcyjne WAP.

[2] Dane za: [*Telekomunikacyjne bariery...* 2004]. Wskaźniki te są w dalszym ciągu znacznie niższe niż w wielu krajach regionu (np. Czechach, czy na Węgrzech).



Rys. 1. Wyposażenie gospodarstw domowych w Polsce w urządzenia telekomunikacyjne i dostęp do internetu w 2001 r.

Źródło: *Warunki życia ludności w 2001 r.*, wyniki badań ankietowych GUS, http://www.stat.gov.pl/serwis/nieregularne/wzl.htm



Rys. 2. Odsetek badanych mających dostęp do internetu w zależności od miejsca zamieszkania (lipiec-sierpień 2003 r.)

Źródło: informacja prasowa TNS OBOP, 30.09.2003, http://www.e-biznes.pl/download/interbus0903.doc

szechnie dostępnym sposobem łączenia się z siecią był ogólnopolski numer dostępowy TP SA (*dial-up*). Połączenie takie ma dwie zasadnicze wady: jest stosunkowo wolne (do 56 kbit/s), a rozliczanie płatności za usługę następuje na podstawie czasu zestawionego połączenia (co oznacza nieopłacalność stałego połączenia). Wprowadzanie kolejnych, bardziej nowoczesnych usług, pozwalających na stały i szybszy dostęp do internetu (SDI, Neostrada itp.) spotkało się z ogromnym zainteresowaniem wśród klientów indywidualnych i firm. Dominujący operator w pewnym momencie nie był w stanie poradzić sobie z rosnącym popytem, co skutkowało długim czasem czekania na instalację usług.

Tendencja zastępowania wolnego połączenia *dial-up* innymi technologiami, tzw. szerokopasmowymi (*broadband*), jest zbieżna ze zmianami zachodzącymi na

świecie. W Europie i Azji największą popularność zdobyły różne wersje technologii DSL, podczas gdy w Ameryce Północnej dużą rolę odgrywa telewizja kablowa [*ITU Internet Reports...* 2003, s. 5]. W Polsce rozwój dostępu szerokopasmowego jest niezwykle dynamiczny. Zilustrować to może wzrost liczby użytkowników jednej z technologii – DSL[3]. W okresie od 31 grudnia 2002 r. do 31 marca 2003 r. liczba linii DSL w Polsce wzrosła o 78,7%, podczas gdy średnia wszystkich państw Europy Wschodniej wynosiła 25,8% (za [*World DSL Statistic...* 2004]). Tempo wzrostu pozostało wysokie (powyżej 60%) w całym roku 2003 [*World DSL Lines...* 2004].

Wśród pozostałych technologii umożliwiających szerokopasmowy dostęp do internetu wymienić należy:

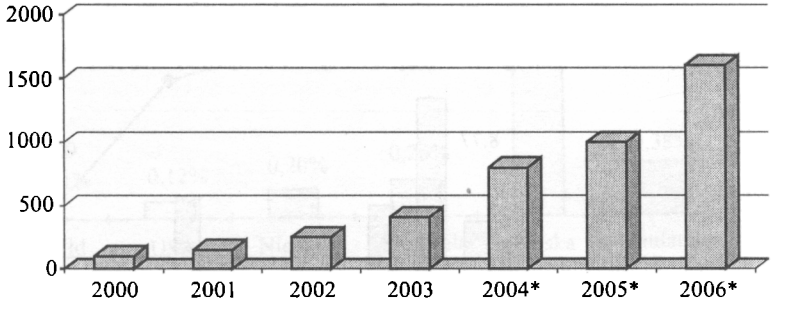
- radiowe sieci dostępowe (LMDS),
- transmisję satelitarną,
- WLAN – Wireless Local Area Network – bezprzewodową sieć lokalną (znaną również pod nazwą WiFi), opartą na wykorzystaniu częstotliwości w nieregulowanym paśmie ~2,4GHz,
- UMTS, czyli telefonię komórkową trzeciej generacji (3G), pozwalającą na uzyskanie transferu danych o prędkościach porównywalnych z dzisiejszymi sieciami przewodowymi LAN,
- PLC – dostęp do internetu przy użyciu sieci energetycznej (na podstawie [*Narodowa Strategia...*]).

W Polsce, gdzie dostępność stacjonarnej sieci telefonicznej w niektórych rejonach jest w dalszym ciągu niewielka, szczególne nadzieje wiązać można z technikami bezprzewodowymi. Wadą rozwiązań typu WLAN jest stosunkowo wysoki koszt urządzeń, trudno zatem oczekiwać, że w najsłabiej rozwiniętych pod względem infrastruktury telekomunikacyjnej regionach kraju powstaną bezprzewodowe sieci. Z kolei dostęp przez telefony komórkowe obecnej generacji (technologia GPRS) nie oferuje przepustowości większej niż modem w telefonii stacjonarnej. Dodatkowo oligopolistyczna struktura rynku telefonii komórkowej w Polsce sprawia, że ceny przesyłu danych i głosu są wysokie w porównaniu chociażby do krajów regionu [Janiec 2004]. Bez finansowego wsparcia ze strony rządu czy samorządów lokalnych pewne części Polski nie będą miały możliwości korzystania ze względnie taniego dostępu do sieci.

Dostęp szerokopasmowy oferują, oprócz TP SA także inni operatorzy telefonii stacjonarnej oraz sieci telewizji kablowej i inne podmioty (np. obsługujące tzw. sieci osiedlowe). Według szacunków Ministerstwa Infrastruktury, szybki dostęp do sieci miało pod koniec 2003 r. 461 tys. użytkowników, co stanowi zaledwie 1,2% ludności Polski. Dla porównania, średnia w Unii Europejskiej kształtuje się na po-

[3] Na technologii DSL bazuje m.in. usługa Neostrada TP S.A. Dostęp do internetu za pomocą DSL możliwy jest wszędzie tam, gdzie istnieje stacjonarna sieć telefoniczna i odpowiednio wyposażone centrale telefoniczne.

ziomie 5%, a Korea Południowa zdołała, dzięki wsparciu rządu, zapewnić szybki dostęp do sieci ¼ mieszkańców [*Narodowa Strategia*... s. 4]. Prognozy rozwoju tego sektora usług telekomunikacyjnych w Polsce przewidują dalszy dynamiczny wzrost (rys. 3).



* Prognoza.

Rys. 3. Internet szerokopasmowy – liczba użytkowników w Polsce w latach 2000-2006 (w tys.)
Źródło: dane Ministerstwa Infrastruktury za: [Świderek 2004].

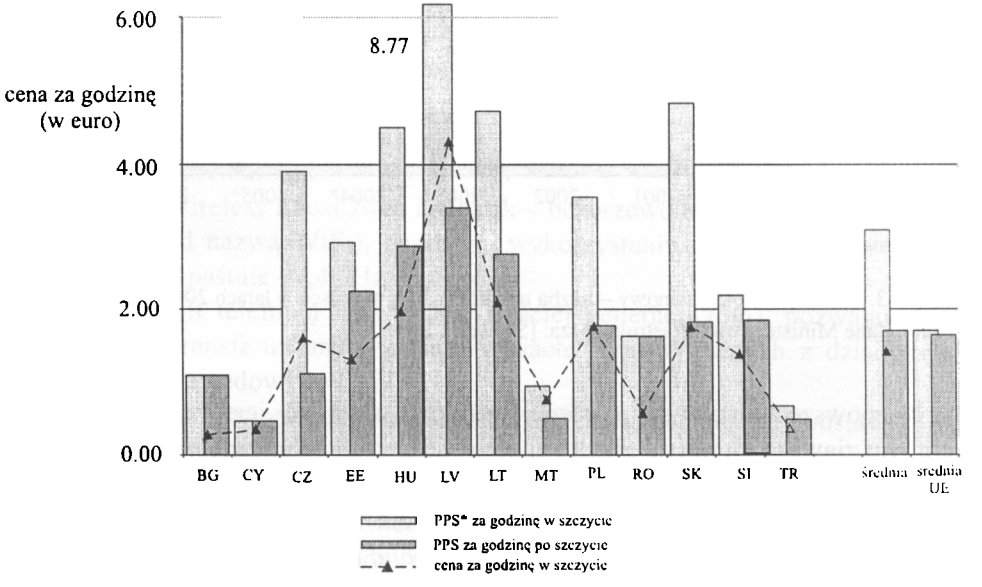
Rozpowszechnienie się dostępu szerokopasmowego jest znacznie bardziej istotnym zjawiskiem niż mógłby to sugerować czysto techniczny opis stosowanych rozwiązań. Doświadczenia krajów o większym nasyceniu szerokopasmowym internetem pokazują, że dopiero taki dostęp pozwala na pełne wykorzystanie możliwości tkwiących w sieci. Użytkownicy *broadband* spędzają więcej czasu w sieci i aktywniej korzystają z możliwości stwarzanych przez handel elektroniczny, elektroniczne usługi publiczne oraz, co szczególnie ważne w kontekście poruszanych tu problemów, e-finanse [Umino 2002, s. 9-11]. Szerokopasmowy internet tworzy zatem popyt na usługi świadczone w środowisku elektronicznym. Dlatego też upowszechnienie szerokopasmowego dostępu często wymienia się jako jeden z filarów budowy społeczeństwa informacyjnego [*ePolska. Plan*... 2001, s. 12-13].

O rozpowszechnieniu dostępu do internetu decydują, oprócz technicznych możliwości, również koszty usług oferowanych przez ich dostawców[4]. Prezentowane w różnych analizach porównania wskazują, że ceny dostępu do internetu w Polsce są stosunkowo wysokie. Dotyczy to zarówno dostępu *dial-up* w sieci telefonii stacjonarnej (rys. 4), jak i dostępu szerokopasmowego (rys. 5). Problem ten jest od wielu lat wskazywany w publikacjach naukowych[5] oraz w opracowaniach

[4] Badania Międzynarodowej Unii Telekomunikacyjnej sugerują, że czynnik ten jest bardziej istotny niż dostępność infrastruktury. Nowe rozwiązania techniczne pozwalają bowiem na szybką rozbudowę sieci (np. bezprzewodowych), podczas gdy wysoki koszt użytkowania sieci może skutecznie ograniczyć jej rozwój [*ITU Digital Access* 2003].

[5] Na przykład w literaturze dotyczącej rozwoju bankowości internetowej w Polsce, m.in.: [Jurkowski 2001, s. 72; Świecka 2002, s. 22; Kański 2000, s. 191-205; Grzechnik 2000, s. 66].

różnych instytucji rządowych i pozarządowych[6] jako jedna z podstawowych barier rozwoju gospodarki sieciowej, a nawet gospodarki w ogólności w Polsce [Streżyńska, Jasiński 2002]. Również wyniki badań społecznych wskazują na cenę dostępu jako główny element hamujący wzrost popularności internetu[7]. Winą za utrzymywanie *status quo* obarcza się najczęściej podmiot dominujący na rynku telekomunikacyjnym (TP SA), jak również brak zdecydowanych działań legislacyjnych zmierzających do faktycznej, a nie tylko ustawowej demonopolizacji i deregulacji tego rynku.



* Parytet siły nabywczej, wyrażany jako jednostka niezależna od walut narodowych, stanowi średnią ważoną współczynników cen względnych w odniesieniu do jednolitego koszyka dóbr i usług

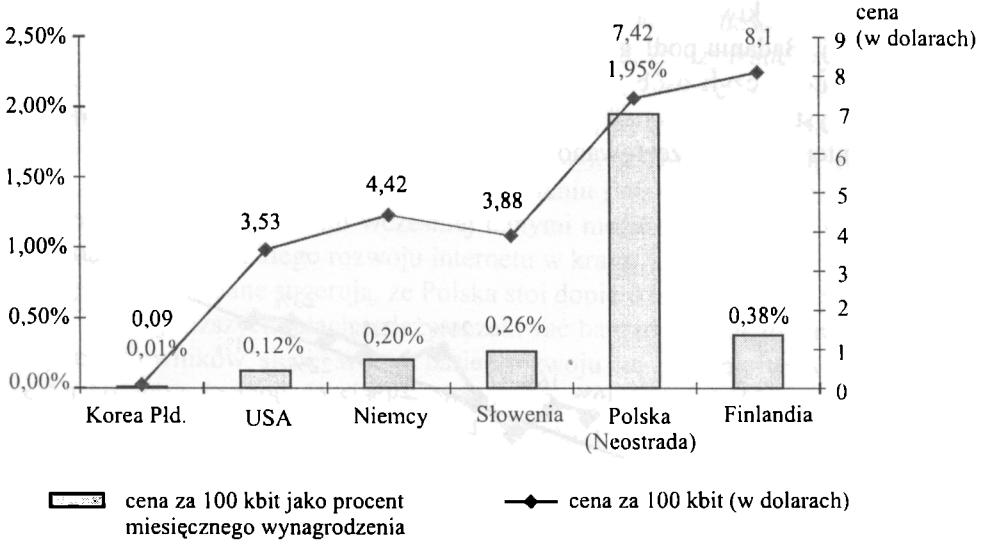
Rys. 4. Koszty dostępu *dial-up* do internetu w 2002 r. w krajach kandydujących do UE, koszt liczony z uwzględnieniem parytetu siły nabywczej *PPS* (Purchasing Power Standard)*.
Źródło: [*Pierwszy raport o* ... 2002].

Pomimo niekorzystnych uwarunkowań dostępności sieci i cen usług dostępu, liczba użytkowników internetu stale wzrasta. O dynamice tego zjawiska świadczyć mogą zarówno wskaźniki „twarde", jak np. liczba hostów internetowych[8], natężenie ruchu w sieciach dostawców internetu, jak i wskaźniki „miękkie", których dostarczają badania ankietowe prowadzone przez podmioty monitorujące rynek w Polsce.

[6] [*ePolska. Plan* ...2001, s. 12-13; Janiec 2004].

[7] Niemal 70% badanych podczas Diagnozy Społecznej 2003, ogólnopolskich badań socjologicznych, wymieniło ten powód jako podstawowy, podczas gdy brak odpowiedniego sprzętu wymieniło 18% respondentów (dane za: [*Telekomunikacyjne bariery*... 2004]).

[8] Co w pewnym uproszczeniu oznacza liczbę komputerów podłączonych do sieci na stałe. W liczbie tej mieszczą się zarówno komputery większości użytkowników korzystających z usług szerokopasmowych, jak i serwery internetowe, na których działają usługi WWW itp.



Rys. 5. Ceny za 100 kbit pasma w wybranych krajach
(dane za rok 2003, dochód miesięczny liczony na podstawie GNP *per capita*)
Źródło: opracowanie własne na podstawie danych zawartych w: [*ITU Internet Reports* ... 2003, s. 20].

Liczba hostów internetowych w Polsce wzrasta bardzo dynamicznie. W roku 2003 było ich ok. 1,3 mln, co stanowiło 3,8% wszystkich hostów w Europie[9]. Przyrost w tym roku stawiał Polskę w czołówce państw europejskich, zwłaszcza że w najbardziej nasyconych internetem państwach (np. skandynawskich) tempo wzrostu wyraźnie zmalało. Jednocześnie liczba hostów na 1000 mieszkańców w dalszym ciągu jest znacznie mniejsza niż średnia w Unii Europejskiej, a nawet w Europie w całości (tab. 1). Wskaźnik ten jest miarą niedorozwoju polskiej sieci.

Problem dostępu do sieci jest także przedmiotem badań ośrodków badania opinii społecznej oraz firm prowadzących ba-

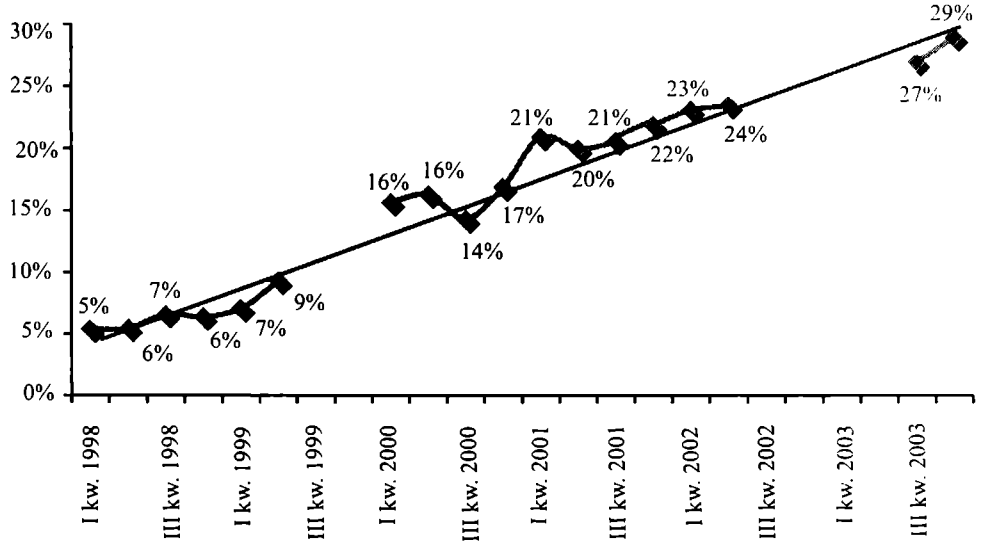
Tabela 1. Liczba hostów internetowych na 1000 mieszkańców w wybranych krajach europejskich w 2003 r.

Kraj	Liczba hostów na 1000 mieszkańców
Islandia	381,4
Holandia	215,5
Estonia	82,8
Węgry	35,8
Czechy	35,5
Polska	33,6
Ukraina	2,6
Średnia piętnastki UE	74,8
Średnia w Europie	48,0

Źródło: *Data on Internet Activity in Europe – hostcount*; ttp://www.gandalf.it/data/data2.htm.

[9] Dane przedstawione w tym akapicie podano za: *Data on Internet Activity in Europe – hostcount*, http://www.gandalf.it/data/data2.htm. Informacje na temat liczby hostów agreguje organizacja RIPE zajmująca się przydzielaniem adresów IP poszczególnym komputerom podłączonym do sieci.

dania rynku. Uzyskiwane wyniki ankietowe są w dużej mierze zależne od przyjętych definicji. Badaniu podlega zarówno deklarowany dostęp do sieci, jak i grupa tzw. internautów, czyli osób, które w określonym okresie czasu poprzedzającym badanie korzystały z internetu[10]. Kształtowanie się odsetka badanych deklarujących dostęp do internetu zaprezentowano na wykresie 6.



Rys. 6. Odsetek badanych deklarujących posiadanie dostępu do internetu w latach 1998-2004
Źródło: opracowanie własne na podstawie informacji prasowych TNS OBOP.

Uzyskanie całościowego obrazu rozwoju internetu w Polsce wymaga połączenia zaprezentowanych wskaźników w syntetyczny miernik. Próbą dokonania takiej syntezy, znacznie ułatwiającej międzynarodowe porównania, jest przygotowany przez Międzynarodową Unię Telekomunikacyjną (ITU) Digital Access Index [*Digital Access...* 2003]. W jego skład wchodzi pięć grup czynników:
- stan infrastruktury (penetracja telefonii stacjonarnej i komórkowej),
- ekonomiczna dostępność internetu (ceny dostępu do sieci),
- edukacja (poziom wykształcenia mieszkańców),
- jakość i szerokość pasma (liczba użytkowników internetu szerokopasmowego i przepustowość łączy międzynarodowych),
- wykorzystanie sieci (liczba użytkowników internetu).

[10] O zróżnicowaniu definicji świadczyć może fakt, że TNS OBOP w definicji internauty przyjął, zgodnie z wytycznymi Internet Advertising Bureau, że jest to osoba korzystająca z sieci w ciągu miesiąca poprzedzającego badanie. W badaniach realizowanych przez inne ośrodki (np. Pentor) przyjmowane bywa także ostrzejsze kryterium – korzystanie z sieci w ciągu 7 dni poprzedzających badanie.

Oprócz czynników dotyczących technologii i jej dostępności do konstrukcji miernika włączono także poziom edukacji, co sprawia, że uzyskane wyniki mówią nie tylko o technicznej stronie rozwoju sieci, ale także o istniejącym potencjale jej wykorzystania. Polska uzyskała w 2003 r. ocenę 0,59, co stawia ją na 39 miejscu na świecie i 5 w Europie Środkowo-Wschodniej, gdzie przewodzą Słowenia i Estonia. Potwierdza to tezę o pewnym zapóźnieniu Polski w tej dziedzinie, lecz w połączeniu z przedstawionymi wcześniej danymi może być również sygnałem, że należy oczekiwać szybkiego rozwoju internetu w kraju.

Przedstawione dane sugerują, że Polska stoi dopiero na początku internetowego boomu – w najbliższych latach należy oczekiwać bardzo szybkiego tempa wzrostu liczby użytkowników sieci. Wśród barier rozwoju na plan pierwszy wybija się kwestia kosztów dostępu do sieci – obecnie są one zbyt wysokie w stosunku do zamożności polskiego społeczeństwa. Usunięcie tej bariery jest ściśle związane z rozwojem sytuacji na polskim rynku telekomunikacyjnym. Bardzo silna pozycja dotychczasowego monopolisty, sprawia że mimo faktycznej deregulacji na rynku tym wciąż nie ma konkurencji [Streżyńska, Jasiński 2002, s. 74-75]. Powoduje to powstawanie błędnego koła hamującego rozwój gospodarki sieciowej: wysokie ceny usług telekomunikacyjnych sprawiają, że popyt na nie jest niewielki. Brak „masy krytycznej" internautów zniechęca przedsiębiorców do działania w sieci – podaż i różnorodność usług *on-line* jest niewielka, co sprawia, że internet nie jest z punktu widzenia polskiego użytkownika atrakcyjny pod względem np. handlu elektronicznego. Dodatkowo brak szybkich postępów w komputeryzacji administracji publicznej i wprowadzaniu elektronicznych usług sprawia, że potencjał sieci jako wygodnego i oszczędzającego czas medium „zarządzania życiem codziennym"[11] nie jest wykorzystywany w pełni.

Dla banków rozwijających bankowość internetową wymienione czynniki mają strategiczne znaczenie. Po pierwsze – stosunkowo niska penetracja internetu i sytuacja na rynku telekomunikacyjnym wydają się nie sprzyjać rozwojowi gospodarki sieciowej w Polsce, co sprawia, że promowanie bankowości internetowej niesie ze sobą spore ryzyko. Bez wątpienia jest to czynnik nakazujący dużą rozwagę i raczej obserwowanie rozwoju sytuacji niż angażowanie się w daleko idące zmiany w strategii konkurencji. Z drugiej strony – tempo i kierunek przemian pokazują dobitnie, że rozwój internetu i gospodarki sieciowej w Polsce jest dopiero w fazie początkowej. Fala przemian nabiera rozpędu i chociaż dzieje się to z pewnym opóźnieniem w stosunku do państw przodujących w tej dziedzinie, to nie ma już odwrotu – gospodarka sieciowa będzie środowiskiem, w

[11] Ten wyjątkowo trafny termin pojawił się m.in. w raporcie badawczym firmy Datamonitor, gdzie wskazano, że indywidualni użytkownicy internetu używają go na kilka sposobów. Sieć może być wykorzystana m.in. jako narzędzie rozrywki (gry *on-line*, czat, słuchanie muzyki itp.), ale także jako narzędzie „administrowania życiem codziennym" (*life administration*) – opłacania rachunków, zasięgania porad medycznych, zarządzania finansami osobistymi itd. [(*Is the Internet reaching...* 2001].

którym banki będą zmuszone konkurować. Co więcej, jest to ostatnia chwila, by zająć w nowej rzeczywistości korzystne pozycje – nie jest jeszcze za późno, by włączyć się w prąd przemian i przygotować się do zmian w otoczeniu. Za 2-3 lata może to być już niemożliwe – bank, który będzie chciał wówczas zmienić swoją filozofię działania znajdzie się w nieporównanie gorszej sytuacji. Na uzyskanie przewagi pierwszeństwa jest już w Polsce za późno, wciąż jednak możliwe jest przygotowanie takiej pozycji konkurencyjnej, która pozwoli bankowi z powodzeniem funkcjonować na rynku w najbliższych latach.

3. Bezpieczeństwo komunikacji w internecie – technologie i zagrożenia

Anonimowość internetu i specyfika jego otwartej architektury sprawiają, że wykorzystanie sieci w działalności banku wymaga zastosowania wielu dodatkowych środków, które zmniejszą prawdopodobieństwo dostania się poufnych informacji w niepowołane ręce. Zabezpieczenia w bankowości internetowej to zagadnienie bardzo szerokie, a zestaw rozwiązań technologicznych stosowanych w tym obszarze stale się powiększa[12]. Szybki rozwój internetu sprawił, że banki zmuszone zostały do opanowania i wykorzystania dorobku kryptografii, a utrzymanie bezpieczeństwa funkcjonowania w sieci nakłada na nie dodatkowy obowiązek śledzenia zmian w działaniach przestępców komputerowych.

Omawiane zagadnienia dotyczą wyłącznie jednego z wymiarów bezpieczeństwa systemów informatycznych – bezpieczeństwa komunikacji klient–bank. O ile bowiem niedostatki zabezpieczeń systemów działających we wnętrzu banku są równie niebezpieczne dla jego funkcjonowania co niedostateczne zabezpieczenie systemów dostępnych z zewnątrz (np. bankowości internetowej), o tyle z punktu widzenia klienta znacznie większą wagę ma ten obszar, z którym styka się on bezpośrednio. Dlatego też dbałość o bezpieczeństwo internetowego *front end* i podkreślanie znaczenia tych zagadnień w komunikacji z klientem jest niezbędnym elementem działania banku opierającego przewagę konkurencyjną na świadczeniu usług bankowości internetowej.

Z punktu widzenia praktyki bankowej, „złotym środkiem" byłby taki zestaw zabezpieczeń, który umożliwiałby:
- poufność przesyłanych danych,
- identyfikację i uwierzytelnienie obu stron komunikacji,
- integralność przesyłanego komunikatu (brak możliwości ingerencji w jego treść),
- prostą obsługę, niewymagającą zaangażowania użytkownika,
- zachowanie niskich kosztów zastosowanych rozwiązań.

[12] Przegląd zasad budowania systemów zabezpieczeń i technologii stosowanych w bankowości internetowej przedstawiono m.in. w: [*Technologie informatyczne*... 2002, s. 169-208; Fray, Pejaś 2002].

Poufność przesyłanych w internecie danych zapewnia szeroko rozpowszechniony standard SSL (Secure Sockets Layer)[13], wykorzystywany nie tylko przez banki, ale również sklepy internetowe, systemy płatności elektronicznych i inne podmioty, których działalność wymaga takich zabezpieczeń. SSL, oparty na 128-bitowym kluczu szyfrującym, jest uznawany za standard zapewniający wysoki poziom poufności przesyłanych danych i ich integralność. Wbudowany w SSL system certyfikatów cyfrowych pozwala jednoznacznie zidentyfikować przynajmniej jedną ze stron transakcji. Dodatkowe mechanizmy, jak np. wygasające sesje[14], zmniejszają prawdopodobieństwo dostępu niepowołanych osób do systemu transakcyjnego banku. Sferą, w której brak jest powszechnie przyjętego standardu, jest uwierzytelnienie użytkownika.

W praktyce banków oferujących bankowość internetową stosuje się różne sposoby **uwierzytelniania** klienta. Oferują one bowiem albo lepszy poziom bezpieczeństwa, ale mniejszą wygodę użytkowania i większe koszty[15], albo prostotę używania i niższy poziom bezpieczeństwa[16]. Przegląd sposobów uwierzytelnienia użytkownika stosowanych w bankach działających w Polsce przedstawia tab. 2.

Spośród przyszłościowych rozwiązań dotyczących uwierzytelniania stron w internecie podpis elektroniczny jest tym, z którym można wiązać największe nadzieje[17]. Szczególnie istotne jest istnienie w Polsce uregulowań prawnych gwarantujących wiarygodność e-podpisu i regulujących działalność podmiotów odpowiedzialnych za tzw. infrastrukturę klucza publicznego (PKI). Nie bez znaczenia jest także uniwersalność podpisu elektronicznego, który służyć może jego użytkownikowi nie tylko w stosunkach z bankami, ale również z niemal każdym podmiotem działającym w sieci. Należy oczekiwać, że podpis elektroniczny stanie się w perspektywie najbliższych lat najpopularniejszym sposobem uwierzytelniania użytkowników bankowości internetowej. Warunkiem takiego rozwoju sytuacji jest jednakże większe zaangażowanie administracji państwowej i samorządowej w elektroniczne usługi publiczne i wykorzystanie przez nie podpisu elektronicznego. Banki, szczególnie te działające na rynku detalicznym, nie będą chciały ponosić kosztów popularyzacji e-podpisu wśród swoich klientów, ponieważ wypracowane

[13] Opiera się on na kombinacji technik kryptografii asymetrycznej i symetrycznej oraz wykorzystaniu certyfikatów poświadczających autentyczność przeglądanych stron internetowych. Specyfikacja standardu SSL dostępna jest na http://wp.netscape.com/eng/ssl3/ssl-toc.html.

[14] Jeśli przez określony czas użytkownik nie podejmie żadnych działań, to strona internetowa np. systemu bankowości internetowej traci ważność i konieczne jest ponowne zalogowanie.

[15] Przykładem może być użytkowanie tzw. tokena, czyli urządzenia generującego kod na zasadzie „pytanie–odpowiedź".

[16] Przykładem może być system oparty na wykorzystaniu hasła dostępu jako jedynego sposobu uwierzytelnienia użytkownika.

[17] Zasadę działania podpisu elektronicznego przedstawiono szeroko m.in. w: [Szaniawski, Kościelny 2003, s. 15-42].

Tabela 2. Wady i zalety sposobów uwierzytelniania użytkownika stosowanych w systemach bankowości internetowej dla użytkowników indywidualnych w Polsce

Sposób uwierzytelniania	Wady	Zalety	Banki w Polsce stosujące ten rodzaj zabezpieczenia
Listy haseł jednorazowych (TAN)	teoretycznie możliwe jest przechwycenie przesyłki z listą haseł, lecz jej aktywacja wymaga znajomości numeru użytkownika i hasła dostępu do systemu bankowości internetowej	bardzo proste użytkowanie, niski koszt dla banku	Multibank, mBank, Inteligo (PKO BP SA), Nordea Bank SA
Token	możliwość rozsynchronizowania tokena, wysoki koszt dla użytkownika (dodatkowa opłata za użytkowanie tokena), trudniejsza obsługa niż w przypadku TAN	wysoki stopień bezpieczeństwa	Pekao SA, BZWBK SA, BGŻ SA, Lukas Bank SA, PKO BP SA
Podpis elektroniczny	konieczność przechowywania klucza prywatnego w bezpiecznym miejscu, stosunkowo skomplikowana obsługa	wysoki stopień bezpieczeństwa	Fortis Bank SA, BPHPBK SA
Jednorazowe hasła wysyłane SMS-em	dodatkowy koszt dla użytkownika (koszt SMS-a)	proste i wygodne użytkowanie, pełna mobilność użytkownika	BZWBK SA
Unikalny identyfikator użytkownika i hasło	niski poziom bezpieczeństwa – tzw. słabe uwierzytelnienie, możliwość przechwycenia danych przez specjalne oprogramowanie (tzw. keyloggery), konieczność bezpiecznego przechowywania danych używanych do uwierzytelnienia	bardzo proste użytkowanie, pełna mobilność użytkownika (do wykorzystania systemu bankowości internetowej nie jest potrzebne dodatkowe urządzenie ani dane)	niemal wszystkie banki posiadające systemy bankowości internetowej stosują ten rodzaj zabezpieczenia przy podstawowej identyfikacji

Źródło: opracowanie własne na podstawie informacji dostępnych na stronach internetowych banków.

przez nie rozwiązania dają obecnie zadowalający stopień bezpieczeństwa[18]. Dopiero pewien poziom rozpowszechnienia stosowania podpisu elektronicznego może skłonić je do przyjęcia tej technologii jako podstawy uwierzytelniania w świadczeniu usług bankowości internetowej.

Dla funkcjonowania banków szczególne znaczenie mają **zagrożenia bezpieczeństwa** wynikające z działania w sieci. Z jednej strony bank musi być „dostępny" dla wybranych grup (np. klientów bankowości internetowej), z drugiej – musi być ściśle izolowany od otoczenia, tak aby nie dopuścić do naruszenia bezpieczeństwa jego funkcjonowania. Połączenie ze sobą tych dwóch wyzwań w

[18] Przy założeniu, że w najbliższych latach nie nastąpi jakościowy skok w rozwoju technik stosowanych przez przestępców komputerowych.

otwartym środowisku internetu jest zadaniem wyjątkowo trudnym. Najważniejsze zagrożenia w tym obszarze stanowią:

- wirusy, robaki, konie trojańskie i inne szkodliwe programy rozprzestrzeniające się za pomocą sieci[19],
- wady oprogramowania wykorzystywanego w banku, jak również niedostateczna dbałość o bezpieczeństwo wśród wykorzystujących sieć pracowników,
- działania przestępców komputerowych.

Zagrożenia związane z działaniem **wirusów komputerowych** mają w bankach taki sam charakter jak w przypadku każdego z użytkowników internetu, jednakże ich konsekwencje mają znacznie większy ciężar gatunkowy. Pouczającym przykładem może być wypadek, który przytrafił się fińskiej części banku Nordea. W sierpniu 2003 r. internetowy robak Blaster, niezwykle szybko rozprzestrzeniający się po całym świecie, doprowadził do zamknięcia na jeden dzień 80 oddziałów tego banku [*Blaster Worm* ... 2003]. Mimo że intruz nie był szczególnie destruktywny (jego działanie ograniczało się do restartowania komputerów), to sam fakt przerwania ciągłości działania banku był wystarczającym ciosem dla jego reputacji. Ten sam robak w innej mutacji zaatakował również sieci bankomatów [*Deebold Takes Virus* ... 2003]. Warto zauważyć, że na takie sytuacje narażone są wszystkie banki korzystające z internetu w swojej działalności, tzn. nie tylko te, które oferują bankowość internetową, ale również ograniczające się wyłącznie do wykorzystania np. poczty elektronicznej. Nic nie wskazuje na to, że można uniknąć w przyszłości tego typu przypadków – twórcy wirusów zawsze wyprzedzają o krok firmy zajmujące się neutralizowaniem działalności ich wytworów.

Wady oprogramowania stanowią poważne zagrożenie dla bezpieczeństwa systemów banku. W przypadku specjalistycznego oprogramowania stosowanego wyłącznie w bankach wady te mogą zagrozić ciągłości funkcjonowania banku, lecz nie narażają go na ataki z zewnątrz. Szczególne znaczenie mają wady oprogramowania odpowiedzialnego za komunikację z siecią (przeglądarek internetowych, programów pocztowych, *firewalls*, programów antywirusowych itd.). Tak zwane dziury w aplikacjach pozwalają twórcom wirusów i innych szkodliwych programów uzyskać dostęp do komputerów wykorzystujących wadliwe oprogramowanie. Służby IT banku muszą zatem troszczyć się nie tylko o działanie systemów najważniejszych z operacyjnego punktu widzenia, ale również o stałe uaktualnianie oprogramowania używanego we wszystkich częściach banku[20]. Na tę konieczność zwrócił uwagę m.in. amerykański fundusz gwarantowania depozytów FDIC, kierując do instytucji finansowych zalecenia dotyczące budowy systemu monitorowania wad oprogramowania [*Guidance on Developing*... 2003].

---

[19] Lista różnego rodzaju komputerowych szkodników stale się rozrasta, patrz: [Ryznar 2002: *Attackers and Their Tools*...].

[20] Pomóc w realizacji tego zadania mogą specjalne programy komputerowe (tzw. *patch management*).

Nieuwaga pracowników może mieć destrukcyjne skutki dla bezpieczeństwa funkcjonowania banku. Nowe technologie umożliwiają pracownikom większą mobilność (np. laptopy i internet pozwalają na pracę w domu lub w podróży), ale stwarzają również dodatkowe zagrożenie. Systemy pracy zdalnej muszą spełniać znacznie surowsze wymagania bezpieczeństwa niż systemy bankowości internetowej. W banku szeroko wykorzystującym sieć jako narzędzie komunikacji wewnętrznej zastosowanie powinny znaleźć najbardziej wyrafinowane technologie uwierzytelniania (np. biometria) oraz zabezpieczania przesyłanych danych, np. wirtualne sieci prywatne wykorzystujące SSL[21].

Wzrost popularności bankowości internetowej zrodził zainteresowanie nie tylko potencjalnej klienteli, ale również **świata przestępczego**. Strony internetowe instytucji finansowych były w 2003 r. najchętniej wybieranym obiektem ataków typu *phishing* [*Phishing Attack* ... 2004], mających na celu zdobycie kodów dostępu do serwisów transakcyjnych. Pomysłowość oszustw dokonywanych w internecie (tab. 3) stawia przed bankami trudne zadanie. Problem przestępczości komputerowej ma charakter globalny – bank może zostać zaatakowany z dowolnego miejsca na świecie, a ściganie winnych jest w tym przypadku szczególnie trudne[22]. Czynnikiem decydującym jest tu nie tyle technologia, co czynnik ludzki, gdyż schematy oszustw opierają się najczęściej na podstępie, a rozwiązania techniczne mają znaczenie drugoplanowe. Rozpowszechnieniu się ataków sprzyja często niedostateczne bezpieczeństwo stosowanych przez bank sposobów uwierzytelnienia klienta. W sytuacji, gdy jedynym środkiem identyfikacji jest numer klienta i hasło, przestępca komputerowy ma przed sobą stosunkowo łatwe zadanie.

Najlepszą obroną przed przestępcami komputerowymi jest edukowanie klientów na temat możliwych schematów działania oszustów, szybka reakcja w razie wystąpienia sytuacji kryzysowej oraz wykorzystanie specjalistycznego oprogramowania monitorującego aktywność użytkowników bankowości internetowej[23].

Dla banku promującego bankowość internetową jako podstawę konkurowania na rynku bezpieczeństwo ma znaczenie pierwszoplanowe, ponieważ nawet niewielki incydent może nadszarpnąć zaufanie klientów, a odzyskanie zaufania jest procesem długotrwałym i trudnym. Jednocześnie wysokie bezpieczeństwo transakcji może być czynnikiem budującym przewagę konkurencyjną – likwidując jedną z głównych barier powstrzymującą klientów przed zarządzaniem swoimi finansami w internecie, bank łatwiej może pozyskać nowych klientów i zatrzymać obecnych. Dlatego też rozwiązania technologiczne, zwłaszcza dotyczące uwierzytelnienia

[21] Wirtualna sieć prywatna (VPN – Virtual Private Network) to „bezpieczny kanał" tworzony w internecie; umożliwia wykorzystanie publicznej sieci do stworzenia bezpiecznego połączenia pomiędzy wybranymi maszynami. Szerzej o SSL–VPN jako narzędziu zdalnego dostępu w: [Laubchan].

[22] Przykładowo atak typu *phishing* na mBank dokonany został przy użyciu serwera znajdującego się w Czechach.

[23] Rozwiązania mogące znaleźć zastosowanie w przeciwdziałaniu przestępstwom komputerowym omawia [Bilski 2000, s. 397-408]. Powstają także systemy pomagające monitorować zagrożenia związane z atakami typu *phising* [*Coyota Launches*...].

Tabela 3. Wybrane przykłady oszustw internetowych wymierzonych w klientów instytucji finansowych

Atakowana instytucja i data ataku	Schemat działania	Źródło informacji
1	2	3
Banki w Australii i Nowej Zelandii, sierpień 2003	Oszuści działali z terytorium Danii. Przygotowali dwie witryny internetowe udające strony instytucji finansowych powiązanych z najbardziej znanymi bankami w Australii i Nowej Zelandii. Wybrani internauci otrzymywali e-maile uprzedzające ich, że otrzymają przelew, który mają następnie przesłać na wskazane konto. Za tę czynność mają prawo pobrania prowizji w wysokości 500 dolarów australijskich. Po szczegóły odsyłano do podrobionej strony, gdzie internauta miał podać numer swojego konta. Internauci którzy wykonali instrukcję otrzymywali przelew i tego samego dnia przekazywali go, po potrąceniu wynagrodzenia, na wskazane konto. Jednocześnie w ciągu 24 godzin przelew od oszustów był anulowany, na co pozwala prawo w Australii i Nowej Zelandii. W efekcie ofiara traciła wysłane pieniądze.	*New Zealand Police Warn of New Net Banking Scam*, Finextra.com 2.08.2003
Citibank, Polska, styczeń 2004	Typowe oszustwo typu *phishing*. Oszuści rozesłali pocztą elektroniczną wiadomości sugerujące (zarówno wyglądem, jak i adresem nadawcy), że pochodzą one z Citibanku. W treści listu opisywano nowości w systemie bankowości internetowej i zachęcano do zalogowania się w systemie. Link prowadzący do strony logowania był fałszywy, prowadził do spreparowanej strony przypominającej stronę logowania Citibanku. Wpisując swój identyfikator i hasło oszukany przekazywał je automatycznie oszustom. Dzięki wykorzystaniu luki w przeglądarce Internet Explorer adres strony WWW widniejący na pasku statusu był poprawny, co nie budziło podejrzeń oszukanych. Podobny schemat działania wykorzystano w przypadku oszustw skierowanych do klientów Inteligo i mBanku.	Stankiewicz P., *Podaj mi swoje hasło*, „Rzeczpospolita" 5.02.2004; Macierzyński M., *Sieciowi oszuści znowu zaatakowali*, http://wiadomosci.prnews.pl/index.php/display,4382;
Westpac, Australia, luty 2004	Oszustwo oparte na modyfikacji typowego *phishingu*. Klienci banku otrzymali e-maile przypominające komunikat marketingowy z banku. W treści znalazło się nawet stwierdzenie, że „Westpac nigdy nie poprosi Cię o podanie swojego ID czy numeru Social Security". Klikając w zawarty w liście link, internauta otwierał podrobioną stronę logowania do serwisu transakcyjnego przygotowaną przez oszustów. Nowość ataku polegała na tym, że po wpisaniu identyfikatora i hasła dostępu pojawiał się komunikat o błędzie w logowaniu i użytkownik był niezauważalnie przekierowywany tym razem do prawdziwej strony logowania Westpac. Oczywiście wpisane wcześniej dane były poprawne i trafiały do oszustów. Atak był szczególnie niebezpieczny ponieważ wielu klientów nie zwróciło uwagi na nietypowe zachowanie przeglądarki, myśląc, że po prostu pomyliło się przy wpisywaniu hasła.	*Nowa technika wyłudzenia haseł dostępowych do kont bankowych*, Hacking.pl 6.03.2004, http://www.hacking.pl/news.php?id=3466

cd. tabeli 3

1	2	3
TD Waterhouse, USA, lipiec 2003	Nowatorskie oszustwo przy wykorzystaniu tzw. konia trojańskiego (programu rezydującego w komputerze ofiary i przekazującego na zewnątrz informacje) oraz keyloggera (programu śledzącego i zapisującego znaki wpisywane z klawiatury). Oszust wysłał na jedną z grup dyskusyjnych poświęconych rynkowi opcji zaproszenie do testowania przygotowanego przez niego programu analitycznego. W programie ukryty był koń trojański i keylogger. Oszust uzyskał w ten sposób kody dostępu do rachunku inwestycyjnego jednej z ofiar i złożył w jej imieniu zlecenie zakupu 7200 opcji na akcje firmy Cisco. Zlecenie to korespondowało ze zleceniem sprzedaży wystawionym przez oszusta w jego biurze maklerskim. Oszust uniknął w ten sposób straty w wysokości 37000 dolarów. Oszustem okazał się nastolatek, a sprawa była pierwszą sprawą o kradzież tożsamości (*ID theft*) prowadzoną przez SEC.	*SEC prosecutes teen for online brokerage hacking*, Finextra.com 10.10.2003, http://www.finextra.com/topstory.asp?id=10185

Źródło: opracowanie własne na podstawie wskazanych w tabeli źródeł.

użytkownika, pełnią w tym obszarze tak ważną rolę. Wprowadzając nowe, lepsze metody identyfikacji, bank nie tylko podnosi bezpieczeństwo swojego funkcjonowania i odstrasza potencjalnych „komputerowych włamywaczy", ale również wzmacnia swoją pozycję w stosunku do konkurentów. Rozwój technologii przynosi nadzieję na lepsze zabezpieczenie transakcji internetowych – szczególnie obiecujące wydają się obecnie biometryczne metody identyfikacji oraz karty mikroprocesorowe.

Metody biometryczne opierają się na sprawdzeniu wybranych niepowtarzalnych cech konkretnej osoby – odcisku palca, wzoru siatkówki oka, tonu głosu. W sektorze finansowym stosuje się je obecnie w wąskim zakresie – najczęściej służą one kontroli dostępu do pomieszczeń oraz terminali komputerowych [Krebsbach 2003]. Podobnie jak w przypadku podpisu elektronicznego, czynnikiem hamującym rozpowszechnienie biometrii w relacjach klient–bank są wysokie koszty oraz przekonanie o wystarczającej sile stosowanych obecnie zabezpieczeń. Wzrost liczby przestępstw polegających na „kradzieży tożsamości" w środowisku elektronicznym (*identity theft*), może przyczynić się do popularyzacji biometrycznej identyfikacji. Podobny efekt może dać spadek cen urządzeń wykorzystywanych w tym procesie. Dopóki rachunek ekonomiczny nie uzasadnia wprowadzenia nowych rozwiązań, trudno oczekiwać, by sama technologiczna wyższość mogła sprawić, że biometria znajdzie szerokie zastosowanie w jakiejkolwiek dziedzinie.

Co najmniej równie istotne jak rozwiązania technologiczne w kontekście działań rynkowych banku jest zapewnienie klientowi poczucia bezpieczeństwa w wymiarze psychologicznym[24]. Służyć temu może np. gwarancja braku finansowej od-

[24] Zestaw „najlepszych praktyk" w tej dziedzinie skompilowany na podstawie przeglądu działań banków amerykańskich i australijskich przedstawiono w: [Tubin 2003].

powiedzialności za wszelkie straty wynikające z użytkowania serwisu transakcyjnego[25]. Istotną rolę odgrywa również pełna i rzetelna informacja o zagrożeniach związanych z wykorzystywaniem sieci i zasadach, jakich należy przestrzegać, aby się przed nimi ustrzec. Edukacja klienta staje się coraz ważniejsza w miarę wzrostu skali działania internetowych oszustów. O tym, że banki w Polsce również dostrzegają tę konieczność, świadczy eksponowanie na stronie głównej serwisów wskazówek dla użytkowników.

4. Podsumowanie

Zmiany technologiczne są dla banku promującego bankowość internetową szczególnie istotne, technologia ma bowiem znaczenie fundamentalne dla uzyskania i utrzymania przewagi konkurencyjnej banku. Jednocześnie obszar ten podlega bardzo szybkim przemianom – nowe rozwiązania pojawiają się w nim nieustannie. Identyfikacja zjawisk mogących mieć znaczący wpływ na działanie banku jest zadaniem bardzo trudnym. Odnosi się to zwłaszcza do rozwiązań technologicznych posiadających duży potencjał zastosowań, ale krótką historię funkcjonowania. Ocena ich strategicznego znaczenia nie może być jednoznaczna. Historia rozwoju internetu i pokładanych w nim nadziei dobrze ilustruje ten fenomen – sieć potencjalnie może znaleźć zastosowanie w niemal każdej dziedzinie życia społeczno-gospodarczego. Wiedziano o tym na długo przed masową popularnością tego medium. Nie można jednak było przewidzieć, jakie będą konkretne zastosowania internetu i jak wiele zmieni on np. w bankowości. Stąd oczekiwania wobec tego zjawiska były bardzo zróżnicowane – od nierealistycznej euforii i wieszczenia rychłego końca tradycyjnego modelu bankowości aż do lekceważenia i negowania potencjału komputerowej sieci. Podobny mechanizm zauważono w przypadku innych zjawisk technologicznych – przykładem może być telefonia komórkowa trzeciej generacji (UMTS), w której upatrywano rewolucyjnego potencjału, ale oczekiwania te do tej pory nie ziściły się nawet w niewielkiej części.

Ze względu zatem na zmiany zachodzące w sferze technologii bank musi zwracać uwagę, nie tylko na potencjał innowacji, ale przede wszystkim na to, czy jest ona wystarczająco dojrzała, by móc odegrać istotną rolę w jego działaniu. Dopiero bowiem wyłonienie się powszechnie akceptowanego standardu i uzyskanie krytycznej masy użytkowników czyni z technicznej nowinki narzędzie gotowe do wykorzystania. Spośród omawianych w tej części pracy technologii, w warunkach polskich niektóre można uznać za niemal w pełni dojrzałe (np. internet, telefonia komórkowa), inne są w fazie zyskiwania akceptacji (np. podpis elektroniczny), a część w dalszym ciągu jest niewiadomą (np. biometria).

[25] Przykładowo Bank of America wprowadził zasadę „0$ *liability*" polegającą na zwolnieniu użytkownika serwisu bankowości internetowej z odpowiedzialności za wszelkie nieautoryzowane transakcje (http://www.bankofamerica.com/onlinebanking/index.cfm?template=guarantee).

Rozwój technologii stwarza także nowe zagrożenia. Z punktu widzenia banku oferującego bankowość internetową na plan pierwszy wybija się problem przestępczości komputerowej i różnego rodzaju sieciowych „szkodników". Bank działający w sieci jest nieustannie narażony na przypadkowy, będący wynikiem działania np. wirusa, lub umyślny atak. Skala i charakter zagrożeń wynikających z obecności w wirtualnej przestrzeni są zupełnie inne niż w tradycyjnej bankowości. Wymaga to wypracowania odpowiednich procedur zarządzania ryzykiem i ciągłej obserwacji zmieniających się zagrożeń. Dbałość o bezpieczeństwo jest nie tylko warunkiem koniecznym niezakłóconego funkcjonowania banku, ale może być również elementem walki konkurencyjnej. Obawy związane z korzystaniem z sieci są w dalszym ciągu jednym z głównych czynników hamujących rozwój bankowości internetowej, a ich zmniejszenie, także za pomocą rozwiązań technologicznych, oznacza uzyskanie przewagi nad konkurentami.

Podsumowanie szans i zagrożeń w otoczeniu techniczno-technologicznym w Polsce zaprezentowano w tab. 4.

Tabela 4. Główne szanse i zagrożenia w otoczeniu techniczno-technologicznym dla banków oferujących bankowość internetową

Szanse	Zagrożenia
1	2
Dostępność i stan rozwoju internetu w Polsce	
1. Wszelkie mierniki, odnoszące się zarówno do infrastruktury, jak i do liczby użytkowników, mówią o stałym wzroście popularności internetu w Polsce. Oznacza to, że grono potencjalnych klientów elektronicznych usług finansowych poszerza się i w najbliższych latach tendencja ta będzie się utrzymywać aż do osiągnięcia poziomu nasycenia siecią [*Is the Internet* ... 2001]. 2. Przyrost użytkowników szerokopasmowego internetu jest bardzo dynamiczny. Świadczy to dużym zapotrzebowaniu na szybki dostęp do sieci. W miarę rozpowszechniania się szerokiego pasma należy oczekiwać wzrostu popytu na wszelkie usługi świadczone drogą elektroniczną. 3. Oferta technologii dających szybki dostęp do internetu stale rośnie. Szczególne nadzieje należy wiązać z technologiami bezprzewodowymi, które przy założeniu spadku cen mogą pozwolić na wyrównanie nierównomiernego do tej pory rozwoju infrastruktury telekomunikacyjnej.	1. Słabo rozwinięta infrastruktura telekomunikacyjna w Polsce jest czynnikiem hamującym rozwój internetu. Szczególnie dotyczy to terenów wiejskich, gdzie dostęp do telefonii stacjonarnej jest najgorszy. Wyłącza to pewne grupy społeczeństwa z zasięgu gospodarki sieciowej, w tym elektronicznych usług bankowych. 2. Struktura rynku telekomunikacyjnego w Polsce sprawia, że ceny dostępu do sieci są relatywnie wysokie, a wybór technologii dostępu jest wciąż zawężony. Dotyczy to zwłaszcza terenów, na których nie ma alternatywy wobec oferty TP SA. Wysokie ceny hamują wzrost liczby użytkowników sieci i wszelkich świadczonych za jej pomocą usług. 3. Szerokopasmowy internet jest dostępny głównie dla mieszkańców miast, a ceny kształtują się na poziomie wyższym niż w wielu krajach regionu. Brak powszechnego dostępu do szybkiego internetu ogranicza rozwój niektórych z potencjalnych zastosowań sieci w działalności banku, np. doradztwa *on-line* z wykorzystaniem wideokonferencji.

1	2
Bezpieczeństwo komunikacji w internecie	
1. Bezpieczeństwo komunikacji w sieci jest areną działania wielu podmiotów tworzących nowe rozwiązania technologiczne, zapewniające poufność przesyłanych danych i uwierzytelnienie stron biorących udział w tym procesie. Standard SSL, jak również idea infrastruktury klucza publicznego to rozwiązania mogące poprawić bezpieczeństwo komunikacji w sieci. Polski bank może korzystać z szeregu sprawdzonych rozwiązań i dobierać je pod względem wybranych cech (koszt, poziom bezpieczeństwa, łatwość użytkowania) do potrzeb swoich i obsługiwanego segmentu. 2. Nowe technologie, takie jak weryfikacja biometryczna czy podpis elektroniczny, mają znacznie poprawić bezpieczeństwo korzystania z internetu. Ich wykorzystanie dać może bankowi przewagę konkurencyjną, likwidując barierę obaw o bezpieczeństwo, szczególnie silną wśród klientów indywidualnych. 3. Obszar technologii bezpieczeństwa sieciowego może być wykorzystany jako jedna ze sfer działalności banku. Dostarczanie rozwiązań zapewniających identyfikację w środowisku elektronicznym to jedna z szans dywersyfikacji działalności w oparciu o zgromadzony kapitał zaufania, szansy, którą banki otrzymują wraz z rozwojem gospodarki sieciowej.	1. Wzrost popularności internetu pociąga za sobą wzrost przestępczości wykorzystującej tę technologię. Tendencja ta zauważalna jest również w Polsce. Banki są szczególnie narażone na atak, co oznacza, że muszą one na bieżąco monitorować zjawiska pojawiające się w tym obszarze i inwestować w rozwiązania technologiczne minimalizujące ryzyko. Rozmiary zagrożenia są tym większe, w im większym stopniu bank wykorzystuje sieć w swojej działalności. Bank promujący bankowość internetową znajduje się w tym obszarze w mniej korzystnej pozycji niż konkurenci wybierający mniej uzależniony od sieci model działania. 2. Coraz ważniejsza rola sieci w każdej dziedzinie życia sprawia, że powstają nowe zagrożenia związane z komunikacją. Wszelkiego rodzaju szkodliwe programy krążące w sieci stają się globalnym zagrożeniem i mogą zakłócić funkcjonowanie banku, narażając go na utratę reputacji. Dotyczy to przede wszystkim banków szeroko wykorzystujących internet w różnych sferach działalności. 3. Wykorzystanie w Polsce podpisu elektronicznego jako narzędzia uwierzytelnienia klienta detalicznego w bankowości napotyka na bariery ekonomiczne. Rozwiązanie to wiąże się z nieproporcjonalnie wyższymi, w stosunku do wzrostu bezpieczeństwa, kosztami.

Źródło: opracowanie własne.

Przegląd otoczenia techniczno-technologicznego w Polsce wskazuje na kilka istotnych zjawisk. Pierwszoplanowe znaczenie ma tutaj dynamiczny wzrost wykorzystania internetu, mierzony zarówno liczbą użytkowników, jak i rozwojem jego infrastruktury. Czynnik ten wskazuje dobitnie na istotną rolę sieci w działalności banków – wykorzystanie bankowości internetowej jest koniecznością dla utrzymania obecnej i budowania przyszłej konkurencyjności. Co więcej, zbieg kilku czynników, takich jak oznaki wzrostu konkurencji w telekomunikacji (pojawienie się tańszych i szybszych ofert dostępu do sieci u różnych operatorów) i rozwój technologii dostępowych (szczególnie szerokopasmowych), oznaczać może początek przyspieszenia popularyzacji internetu w Polsce. Dla banków przyjmujących postawę oczekiwania na rozwój wypadków, uzasadnioną przez omówione w tej części pracy bariery, stanowi to sygnał do ponownej analizy oczekiwań związanych z wykorzystaniem sieci.

Literatura

Attackers and Their Tools: How McAfee Entercept Protects Servers, case study Network Associates, http://wp.bitpipe.com/resource/org_930709924_7/Attackers_WP.pdf .

Blaster Worm Claims Nordea, Finextra.com 14.08.2003, http://www.finextra.com/topstory.asp?id=9744

Bilski T., *Nowe narzędzia do ochrony systemów informatycznych w bankowości*, [w:] *Zastosowania rozwiązań informatycznych w bankowości*, red. A. Gospodarowicz, AE, Wrocław 2000.

Coyota Laundches Anti-Phising Service, Finextra.com 27.01.2004, http://www.finextra.com/fullstory.asp?id=11040.

ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006, Ministerstwo Łączności, 14.06.2001.

Diebold takes virus protection measures after worm spreads to cash machines, Finextra.com 12.12.2003, http:www.finextra.com/topstory.asp?id=10791

El Fray I., Pejaś J., *Zasady projektowania bezpiecznych bankowych systemów informatycznych*, [w:] *Nowoczesne technologie w sferze usług finansowych*, red. B. Świecka, Uniwersytet Szczeciński, Szczecin 2002.

Gospodarowicz A. (red.), *Zastosowania rozwiązań informatycznych w bankowości*, AE, Wrocław 2000.

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

Is the Internet Reaching Maturity?, Datamonitor 12/2001, http://www.researchandmarkets.com/reportinfo.asp?report_id=1778&t=t&cat_id=41

Guidance on Developing an Information System Patch Management Program to Address Software Vulnerabilities, FDIC FIL-43-2003, 29.05.2003, http://www.fdic.gov/news/news/financial/2003/FIL0343a.html.

ITU Internet Reports: Birth of Broadband – Executive Summary, International Telecommunication Union, September 2003, http://www.itu.int/osg/spu/publications/sales/birthofbroadband/BoBexecsumm.pdf

ITU Digital Access Index: World's First Global ICT Ranking. Education and Affordability Key to Boosting New Technology Adoption, 19.11.2003, http://www.itu.int/newsarchive/press_releases/2003/30.html

Janiec M., *Telekomunikacyjne bariery rozwoju gospodarki opartej na wiedzy w Polsce*, Instytut III Rzeczpospolitej, Warszawa 13.01.2004, http://www.rzeczpospolita.pl/tematy/case-seminarium/-2003/3m_janiec3.htm/

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

Kański R., *Bankowość elektroniczna w Polsce – bariery i kierunki rozwoju*, [w:] A. Gospodarowicz (red.), *Zastosowania rozwiązań informatycznych w bankowości*, AE, Wrocław 2000, s. 191-205.

Krebsbach K., *The Rise of Biometrics*, „Bank Technology News" 3.11.2003, http://www.paybytouch.com/media_word_docs/bank_tech_news.doc

Laubchan J., *SSL-VPN: Improving ROI and Security of Remote Access*, Rainbow Technologies Whitepaper, http://www.rainbow.com/Library/8/SSL%20VPN%20%20Improving%20ROI%20and%20Security%20of%20Remote%20Access.pdf

Macierzyński M., *Sieciowi oszuści znowu zaatakowali*, 13.07.2003, http://wiadomosci..prnews.pl/index.php/display,4382

Narodowa Strategia Rozwoju Dostępu Szerokopasmowego do Internetu na lata 2004-2006, Ministerstwo Infrastruktury, Ministerstwo Nauki i Informatyzacji, http://www.mi.gov.pl/prezentacje/-jednostki/1/dokumenty/narodowa_strategia_-_internet.doc

New Zealand Police Warn of New banking Scam, Finextra.com. *02.08.2003*, http://finextra.com/fullstory.asp?id=9849

Nowa technika wyłudzenia haseł dostepowych do kont bankowych, Hacking.pl 06.03.2004, http://www.hacking.pl/news.php?id=10185

Phishing Attack Trends Report January 2004, Antiphishing Working Group, http://www.antiphishing.org/APWG.Phishing.Attack.Report.Jan2004.pdf
Pierwszy raport o postępach we wdrażaniu eEurope+ w krajach kandydujących, Ljubljana 3-4 czerwca 2002 r., http://www.kbn.gov.pl/gsi/prog_pl.rtf
Polska na końcu stawki w kategorii telefonii i komputeryzacji, 8.03.2004, http://www.marketer.pl/index.php?pg=mms&msgnr=1579
Ryznar Z., *Co umie haker?* „Gazeta Bankowa" 16.04.2002.
SEC prosecutes teen for online brokerage hacking, Finextra.com 10.10.2003, http://www.finextra.com/topstory.asp?id=10185
Stankiewicz P., Podaj mi swoje hasło, „Rzeczpospolita" 5.02.2004
Strężyńska A., Jasiński P., *Likwidacja barier regulacyjnych w telekomunikacji jako warunek wzrostu gospodarczego i cywilizacyjnego Polski*, Zeszyty Instytutu Badań nad Gospodarką Rynkową nr 33. Warszawa-Gdańsk 2002.
Szaniawski K., Kościelny T., *Ustawa o podpisie elektronicznym. Komentarz*, Kantor Wydawniczy Zakamycze, Kraków 2003.
Świderek T., *Bogatsza oferta dla polskich internautów*, „Rzeczpospolita" 16.02.2004.
Świecka B. (red.), *Nowoczesne technologie w sferze usług finansowych*, Uniwersytet Szczeciński, Szczecin 2002.
Technologie informatyczne w bankowości, red. A. Gospodarowicz, AE, Wrocław 2002.
Telekomunikacyjne bariery rozwoju gospodarki opartej na wiedzy w Polsce, Instytut III Rzeczpospolitej, Warszawa 13.01.2004, http://www.markom.krakow.pl/~mjaniec/pdf/bariery_20040113.pdf.
Tubin G., *Security Fears Stymie Online Banking Adoption*, „Bank Systems & Technology" 22.6.2003, http://www.banktech.com/story/BSTeNews/BNK20030623S0001
Umino A., *Broadband Infrastructure Deployment: The Role of Government Assistance*, OECD, DSTI/DOC (2002)15, 22.05.2002
World DSL Statistics Q1 2003, Point Topic Ltd. June 2003, http://point-topic.com
World DSL Lines Approach 64m in 2003, Point Topic Ltd. March 2004, http://www.point-topic.com/content/dslanalysis/Q4%202003%20DSL%20analysis.htm

THE INFLUENCE OF THE TECHNOLOGICAL FACTORS ON THE DEVELOPMENT OF INTERNET BANKING IN POLAND BETWEEN 2000 AND 2003 (STATE OF FEBRUARY 2004)

Summary

The technological factors are of great importance in the development of Internet banking in Poland. In the article the main existing barriers were presented: the underdevloped telecommunication infrastructure and the high costs of Internet access services. The technologies of authentification used by Polish internet banks as well as the innovations in this area (biometrics) were described. The article also covers the specific threats faced by banks offering the internet banking – the danger of identity theft and other forms of computer attacks.

Mgr Michał Kisiel jest doktorantem w Katedrze Finansów Akademii Ekonomicznej we Wrocławiu.