MATERIAŁY I STUDIA

Zeszyt nr 205

Specyfika ryzyka bankowości elektronicznej

Jakub Henryk Górka

Warszawa, kwiecień 2006 r.

Składam serdeczne podziękowania za opiekę i wnikliwe uwagi
przy pisaniu niniejszej pracy promotorowi
prof. dr. hab. Marianowi Górskiemu.

Projekt graficzny:

Oliwka s.c.

Skład i druk:

Drukarnia NBP

Wydał:

Narodowy Bank Polski
Departament Komunikacji Społecznej
00-919 Warszawa, ul. Świętokrzyska 11/21
tel. (22) 653 23 35, fax (22) 653 13 21

Materiały i Studia rozprowadzane są bezpłatnie.

Dostępne są również na stronie internetowej NBP: **http://www.nbp.pl**

Spis treści

Wykaz obiektów graficznych

Streszczenie

Ryzyko towarzyszy każdej działalności gospodarczej, jednak wyjątkowo dużego znaczenia nabiera w segmencie pośrednictwa finansowego. Wynika to z faktu, że pośrednicy finansowi trudnią się transformacją ryzyka, której skutki są częstokroć widoczne nie tylko w skali mikro, lecz także makro.

Banki są *de facto* najsilniejszą i najbardziej charakterystyczną grupą instytucji pośrednictwa finansowego o ugruntowanej i bogatej tradycji działania. Jako jedyne cieszą się przywilejem kreacji pieniądza w gospodarce.

Otoczenie banków obfituje w zmiany będące efektem postępu technologicznego, globalizacji usług bankowych oraz presji konkurencyjnej. Rosnące wymagania klientów powodują m.in. konieczność rozwoju elektronicznych kanałów dystrybucji produktów bankowych (bankowości: terminalowej, telefonicznej, internetowej, komputerowo-modemowej oraz telewizyjnej). Dlatego instytucje kredytowe *nolens volens* muszą zaakceptować wielokanałowość (*multichanneling*) jako nieodzowny składnik swojej strategii działania. Pojawiają się jednak rozmaite pytania. Jakie to niesie skutki dla ich profilu ryzyka? Czy samo ryzyko bankowe także podlega przeobrażeniu? Jak należy na nie patrzeć i analizować?

Na te pytania autor szuka odpowiedzi w poniższej pracy.

Słowa kluczowe: ryzyko, bankowość elektroniczna (e-banking), elektroniczne kanały dystrybucji produktów bankowych.

Wstęp

Celem niniejszej pracy jest zbadanie szczególnego wymiaru ryzyka bankowego w elektronicznych kanałach dystrybucji.

Hipoteza główna pracy brzmi: *E-banking nie wprowadza nowego rodzaju ryzyka bankowego, jednakże jego specyfika powoduje, że tradycyjne rodzaje ryzyka nabierają odmiennego charakteru. Postęp technologiczny, wyraźna globalizacja usług bankowych oraz nieustanna presja konkurencyjna zarówno ze strony samych banków, jak i instytucji parabankowych zmieniają oblicze poszczególnych typów ryzyka. Na pierwszy plan wychodzą następujące rodzaje ryzyka: operacyjne, prawne i utraty reputacji. W konsekwencji ryzyko e-bankingu zmienia ogólny profil ryzyka bankowości.*

Hipoteza robocza nr 1: *Ryzyko bankowości elektronicznej komplikuje istotę ryzyka, narzucając służbom zarządczym banków obowiązek ciągłego przechodzenia procedury, na którą składają się trzy etapy: identyfikacja, pomiar i kontrola ekspozycji oraz monitoring ryzyka.*

Hipoteza robocza nr 2: *We współczesnym świecie banki muszą oferować swoje produkty przez elektroniczne kanały dystrybucji, bowiem tradycyjne oddziały nie są już dłużej w stanie zaspokajać rosnących potrzeb klientów. Poszczególne kanały dystrybucji pełnią w stosunku do siebie funkcje komplementarno-substytucyjne (w określonych przypadkach np. kanał internetowy może być substytutem dla oddziału lub tylko jego dopełnieniem wykorzystywanym okresowo). Tym samym każdy bank powinien posiadać służby potrafiące kontrolować i zarządzać ryzykiem w kanałach elektronicznych.*

Hipoteza robocza nr 3: *Te same rodzaje ryzyka bankowości tradycyjnej (oddziałowej): kredytowe, stopy procentowej, rynkowe, płynności nabierają odmiennego charakteru w kanałach elektronicznych. Są wzbogacane o nowe aspekty, częstokroć nastręczające poważnych trudności w zarządzaniu.*

W moim przekonaniu bankowość na świecie stoi u progu wielkich zmian. Intensywna konkurencja na rynkach światowych obliguje banki do nieustannego wdrażania innowacji i szukania potencjalnych przewag nad rywalami. Wyrazem tych tendencji jest rozwój elektronicznych kanałów dystrybucji, któremu powinna towarzyszyć właściwa analiza ryzyka. Ponieważ nie znalazłem takowej w żadnej ze znanych mi pozycji literatury fachowej lub też opracowania tematu były bardzo pobieżne i fragmentaryczne, więc uznałem za stosowne samemu zbadać problem. Praca powstała przede wszystkim na kanwie dokumentów i raportów Komitetu Bazylejskiego, artykułów z miesięcznika „Bank", źródeł prawa stanowionego w Polsce i Unii Europejskiej, szeregu pozycji książkowych oraz przepastnych zasobów Internetu.

Aby prowadzić jakąkolwiek działalność gospodarczą, należy pojąć lub przynajmniej dotknąć istoty jej ryzyka. Banki są instytucjami zaufania publicznego, których zadaniem jest transformacja ryzyka. Ten fakt powoduje, że ryzyko bankowe staje się wielowymiarowe i trudne do ogarnięcia. Można na nie patrzeć z szeregu perspektyw, analizować i kwantyfikować w celu sprawnego zarządzania. Ryzyko jednak zmienia się bardzo szybko, co wypływa wprost z jego natury. Każda zmiana w jego otoczeniu, a więc w środowisku banku, wywiera na nie wpływ. Parametry ujęte w modelach często tracą na aktualności, zaś służby bankowe stają przed coraz to nowymi wyzwaniami, których nie da się rozwikłać przy pomocy dotychczasowych rozwiązań. Powodem tego stanu rzeczy jest postęp, tak przecież dynamiczny w czasach obecnych. To postęp i konkurencja pociągają za sobą zmiany w środowisku, zmuszając banki do adekwatnych posunięć. Jeśli któryś bank się nie dostosuje, w szybkim tempie traci na znaczeniu i przegrywa w walce o klienta.

Pojawia się zatem pytanie, czy brak zaangażowania banku w elektroniczne kanały dystrybucji grozi jego marginalizacją w sektorze. Odpowiedź wydaje się być twierdząca, zwłaszcza po uwzględnieniu wyników analiz Instytutu Badań nad Gospodarką Rynkową. Do 2006 r. w Polsce[1]:

[1] Pawłowicz, Pietrzak, Sławiński (kwiecień 2002) oraz Lepczyński (luty 2003).

- około 60% klientów banków będzie preferowało wielokanałowy model dostępu do usług;
- około 10% klientów – wyłącznie elektroniczne i wirtualne kanały dystrybucji;
- około 30% klientów pozostanie wiernych tradycyjnej obsłudze w placówkach bankowych;
- około 50% obecnie rutynowych czynności będzie wykonywanych przez urządzenia samoobsługowe.

Wyniki badań IBnGRu są zbieżne z wynikami analiz McKinsey&Company. Polska nie odbiega w tym względzie od krajów wysokorozwiniętych. Jak bowiem głosi wspomniany raport – w najbliższej przyszłości może ukształtować się następująca struktura korzystania z różnych kanałów dystrybucji[2]:

- 20% klientów będzie korzystało wyłącznie z oferty bankowości elektronicznej;
- 60% będzie korzystało z różnych kanałów dystrybucji (*multichannel banking*), czyli z oddziałów, Internetu, telefonu, itp.;
- 20% będzie korzystało wyłącznie z świadczonych przez oddziały banków tradycyjnych.

Kanały dystrybucji produktów są dla klientów wizytówką banku, tworząc wizerunek banku nowoczesnego lub konserwatywnego. Dzięki nim bank funkcjonuje i oddziałuje na zachowania klientów. Pod pojęciem wielokanałowość (*multichanneling*) należy rozumieć oferowanie usług klientom przez kilka kanałów dystrybucji, które działają we wzajemnym powiązaniu informacyjnym i technicznym[3].

Wielokanałowy rozwój banku narzuca konieczność identyfikacji, pomiaru i integracji poszczególnych rodzajów ryzyka bankowego, które – w duchu postawionych hipotez – mogą nabierać odmiennego charakteru w bankowości elektronicznej. Proces ten jest powtarzalny, ponieważ ogólny profil ryzyka banku zmienia się zawsze, gdy wdrażane są innowacje i pojawiają się szanse rozwoju.

Przed bankami w Polsce stoi problem przełamania pewnych barier psychologicznych, które wciąż tkwią w świadomości klientów. Chodzi mianowicie o brak potrzeby korzystania z usług bankowości elektronicznej oraz obawy o bezpieczeństwo[4]. Dopiero po uporaniu się z tym problemem nastąpi gwałtowny rozwój bankowości elektronicznej.

Pisząc tę pracę, chciałem wyrobić swój własny pogląd na temat ryzyka e-bankingu. Poza tym moją intencją było poszerzenie wiedzy i przygotowanie do pracy zawodowej. W celu weryfikacji hipotez zastosowałem ankietę oraz opisowo-dedukcyjne metody badawcze. W pracy zabrakło analizy finansowej ze względu na trudności ze zdobyciem danych i fakt, że wiele z opisanych przeze mnie rodzajów ryzyka wymyka się kwantyfikacji.

Praca składa się z pięciu rozdziałów. W rozdziale pierwszym zatytułowanym „Klasyfikacja elektronicznych kanałów dystrybucji produktów bankowych" podano charakterystykę poszczególnych kanałów ze szczególnym uwzględnieniem aspektu bezpieczeństwa. Wydzielono też dodatkowy punkt o kartach i pieniądzu elektronicznym. W rozdziale drugim „Pojęcie ryzyka w bankowości i jego systematyka z uwzględnieniem natury e-bankingu" znalazły się definicje ryzyka i niepewności oraz rozmaite jego podziały ujęte w logicznej kolejności, począwszy od systematyki Z. Zawadzkiej, poprzez dynamiczną klasyfikację prof. M. Górskiego, a skończywszy na podziale Komitetu Bazylejskiego, który został uznany za wiodący dla całej pracy. Rozdział kończy się podaniem definicji wszystkich rodzajów ryzyka z systematyki Komitetu Bazylejskiego. Najobszerniejszy rozdział trzeci pod tytułem „Rodzaje ryzyka e-bankingu" stanowi serce pracy. Rozpoczyna się od analizy otoczenia bankowości elektronicznej, po którym następuje omówienie ryzyka: operacyjnego, prawnego i reputacji w bankowości elektronicznej. W dalszej części rozdziału wyodrębniono punkty: outsourcing, rzeczywiste ataki na e-banki jako przykład ryzyka: operacyjnego, prawnego oraz reputacji, podpis elektroniczny i Infrastruktura Klucza Publicznego, ryzyko a transgraniczny charakter banko-

[2] Makowska, Mackiewicz (2002).

[3] Ryznar (2003).

[4] Są to dwie najbardziej popularne przyczyny niechęci użytkowania kanałów elektronicznych – *vide* wyniki badań I-Metria Kawęczyńska E. (2003) oraz wyniki własnych badań ankietowych z ostatniego rozdziału pracy.

wości elektronicznej, związek bankowości elektronicznej z pieniądzem elektronicznym oraz ryzyko: kredytowe, płynności, rynkowe a także stopy procentowej. Przedostatni rozdział „Uwarunkowania prawne związane z ryzykiem bankowym w Polsce i UE (stan obecny i planowany)" podzielono na trzy części składowe noszące łacińskie nazwy. *Lex lege prim* odnosi się do obowiązujących wymogów kapitałowych w Polsce i UE, *lex ferenda* zawiera deskrypcję najważniejszych postanowień Nowej Umowy Kapitałowej, zaś *lex lege* bis opisuje polskie rozwiązania prawne ujmujące kwestie podpisu elektronicznego, elektronicznych instrumentów płatniczych, usług świadczonych drogą elektroniczną oraz kredytu konsumenckiego. Rozdział ostatni obejmuje wyniki i wnioski z przeprowadzonego badania ankietowego na temat percepcji ryzyka u klientów detalicznych e-bankingu, do którego kwestionariusz znajduje się w załączniku.

Na koniec wstępu pragnę zauważyć, że rozwiązania Nowej Umowy Kapitałowej są niewątpliwie dużym osiągnięciem w ewolucji procesu zarządzania ryzykiem i banki powinny je stopniowo adoptować. Ponadto, jak sądzę, zaangażowanie w bankowość elektroniczną przynosi bankom więcej korzyści niż zagrożeń.

Ostatnią uwagą wstępną, jaką chciałbym poczynić, jest to, że według mnie portale internetowe banków powinny zacząć pełnić funkcje kompleksowe (realizacja transakcji, zlecenia giełdowe, sprzedaż polis ubezpieczeniowych, dokonywanie zakupów, transakcji, itp.). Taki model bankowości internetowej, a więc tzw. supermarketów finansowych dominuje w Finlandii[5], zaś polskie banki wirtualne również powoli zmierzają w jego kierunku.

[5] Chojecki, Matysek (2003).

1
Klasyfikacja elektronicznych kanałów dystrybucji produktów bankowych

Analiza ryzyka bankowości elektronicznej wymaga podania klasyfikacji elektronicznych kanałów dystrybucji produktów bankowych. Warto jednakże ten punkt poprzedzić wywodem wyjaśniającym nagromadzone niejasności wokół słowa „elektroniczny" oraz przedrostka „e" z myślnikiem lub bez niego, występującym w zestawieniach typu „e-rzeczownik", np.: *e-commerce*, *e-banking*, *e-business*, itp. Prefiks ten został niejako zarezerwowany dla wszystkich terminów dotyczących Nowej Gospodarki, która opiera się na zdobyczach technik teleinformatycznych, z natury rzeczy o charakterze elektronicznym, a więc traktujących o elektronicznej gospodarce, czyli e-gospodarce. Tym niemniej istotą Nowej Gospodarki jest nie sama elektronika, ale nowe medium komunikacyjne – Internet. W ostatnim dziesięcioleciu ugruntował on swoją pozycję, ewoluując z zastosowań badawczych poprzez rozrywkowe do zastosowań edukacyjnych oraz biznesowych. W tym kontekście przedrostek „e" należałoby zamienić na „i", utożsamiając Nową Gospodarkę z i-gospodarką. Budowana jest ona przecież w oparciu o komunikację internetową, choć realizowaną od strony technicznej elektronicznie. Częstokroć zatem, mówiąc np. o e-commerce, ma się na myśli handel za pośrednictwem Internetu, nie zaś innych kanałów elektronicznych[6].

Stąd też pojawiają się rozbieżności w tym, co poszczególni specjaliści uznają za e-banking, a więc bankowość elektroniczną. Dla potrzeb tej pracy wydaje się właściwe przyjąć, że bankowość elektroniczna zawiera w sobie wszystkie elektroniczne kanały dystrybucji produktów bankowych, nie tylko Internet. Usługi bankowości świadczonej za pośrednictwem Internetu będą określane mianem bankowości internetowej lub i-bankingu.

Powyższa metodologia opiera się na szeregu definicji skonstruowanych przez grono badaczy. A. Janc i G. Kotliński[7] rozumieją bankowość elektroniczną jako całościową koncepcję zakładającą wykorzystywanie w praktyce operacyjnej systemów informatyczno-komunikacyjnych do usprawniania i przyspieszenia realizacji zleceń klientów banków, co prowadzi do przyspieszenia obiegu pieniądza bezgotówkowego. T. Porębska-Miąc[8] uważa, że istotę bankowości elektronicznej stanowi możliwość korzystania z usług bankowych niezależnie od miejsca i czasu. Według W. Chmielarza[9] podstawą koncepcji bankowości elektronicznej jest dążenie do stworzenia systemu, w którym rozliczenia finansowe odbywać się będą bez obiegu mediów papierowych. Komunikacja pomiędzy bankiem a jego klientami oraz w obrębie samego banku odbywać się będzie na drodze teletransmisji, natomiast wszelkie dane będą przechowywane i przetwarzane w bazach danych informatycznego systemu wspomagającego zarządzanie bankiem. B. Pilawski[10] wymienił cechy charakterystyczne bankowości elektronicznej, różniące je od tradycyjnych usług bankowych. Są to:

- brak konieczności fizycznej obecności w banku,
- możliwość wykonania czynności bankowej o dowolnej porze,
- brak pośrednictwa personelu banku,
- automatyzm decyzji w stosunku do żądań klienta i brak możliwości negocjowania warunków,
- ograniczone możliwości pozyskania porady.

[6] Opracowano na podstawie: Szyszka (red.) (2003).

[7] Janc, Kotliński (1999).

[8] Porębska-Miąc (2000).

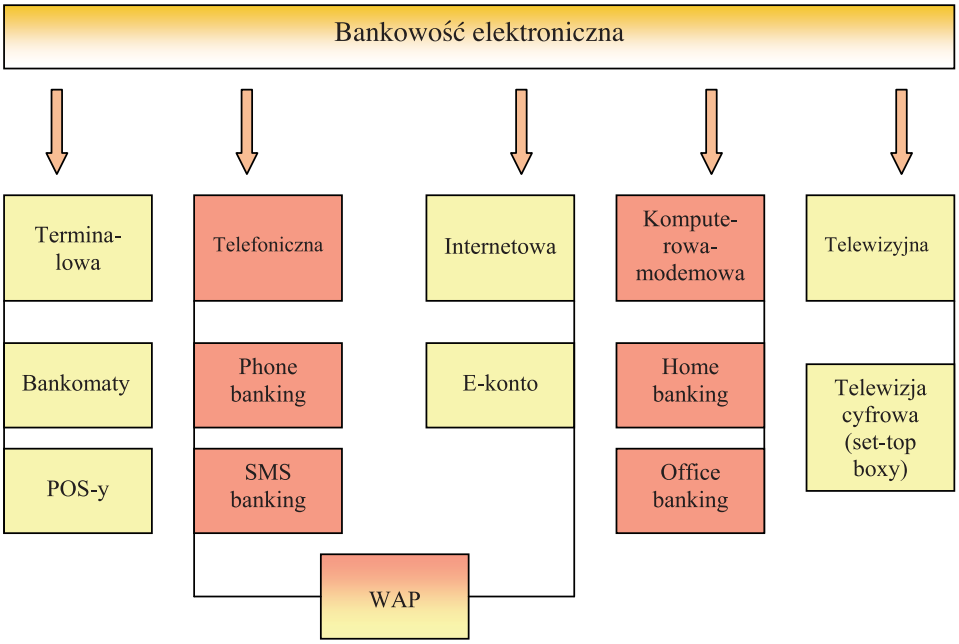
[9] Chmielarz (1999).

[10] Pilawski (2000).

Kierując się powyższymi definicjami i cechami e-bankingu można dokonać klasyfikacji elektronicznych kanałów dystrybucji właściwych dla banku (prezentacja na diagramie 1). Należy zwrócić uwagę na fakt, że kanały, które oferują jedną z trzech klas dostępu do rachunku bankowego (pasywna, aktywna, półaktywna)[11], wymagają niekiedy użycia instrumentu płatniczego, jakim jest karta elektroniczna. Za pośrednictwem kart płatniczych i elektronicznych portmonetek świadczona jest usługa płatnicza mieszcząca się w grupie czynności bankowych *sensu largo*. Warto podkreślić, że nie odbywa się ona tylko przez POS-y (*Point-of-Sale*)[12] oraz bankomaty, gdyż wspomniane instrumenty pozwalają na dokonywanie płatności w Internecie w trybie on-line. Ze względu na swoje znaczenie karty elektroniczne oraz pieniądz elektroniczny zostaną szerzej omówione w ostatnim punkcie rozdziału.

Zaprezentowany poniżej podział ma swoje następstwa, jeśli chodzi o ryzyko – zarówno z punktu widzenia banku, jak i jego klientów.

Diagram 1. Klasyfikacja kanałów dystrybucji w bankowości elektronicznej



Źródło: opracowanie własne na podstawie Maderak (2003).

W dalszej części rozdziału podana zostanie charakterystyka poszczególnych kanałów dystrybucji e-bankingu ze szczególnym uwzględnieniem aspektu ich bezpieczeństwa.

1.1. Bankowość terminalowa

Bankowość terminalowa stanowi najstarszą i jednocześnie najbardziej powszechną formę bankowości elektronicznej. Wspólną cechą bankomatów i POS-ów jest wykorzystywanie kart płatniczych jako niezbędnego elementu transakcji bankowej.

Bankomaty, czyli bankowe punkty samoobsługowe, można podzielić na dwa rodzaje:

- typ CD (*cash dispenser*) służący tylko do wypłaty gotówki,

[11] Klasy dostępu: pasywny – tylko informacje o stanie konta i jego zmianach, aktywny – pełen zakres operacji na koncie (łącznie z pomocniczymi: poczta, wnioski, lokaty, blokady, zastrzeżenia), półaktywny – dostęp do niektórych operacji (np. uprzednio zdefiniowanych w formie pisemnej lub za pośrednictwem operatora).

[12] Tu – elektroniczny terminal służący do autoryzacji kart płatniczych, w szerszym znaczeniu także placówka handlowa (sklep).

- typ ATM (*automated teller machine*) – wielofunkcyjny bankomat, za pomocą którego można, oprócz pobrania gotówki, sprawdzić stan konta, dokonać przelewu, itp.

Standardową operacją przeprowadzaną przy użyciu bankomatu jest wypłata gotówki tudzież sprawdzanie stanu konta. Jednakże coraz częściej klienci wykorzystują to urządzenie do bardziej zaawansowanych transakcji, jak choćby ulokowanie depozytu, obsługa czeku, czy wydanie dyspozycji historii rachunku.

Dużą wadą bankomatu, jako terminalu dostępowego, jest niski poziom „prywatności" klienta wykonującego operacje przy konsoli, szczególnie w popularnych miejscach korzystania z tego typu usług jak centra handlowe czy śródmieścia aglomeracji miejskich. Zwykle długość i niecierpliwość kolejki nie sprzyja swobodnemu operowaniu klawiaturą bankomatu.

Należy także wspomnieć o zwiększonym ostatnio zagrożeniu ze strony fałszywych lub odpowiednio zmodyfikowanych prawdziwych bankomatów. W obu typach bankomatów złodzieje instalują minikamerę do podglądania tajnych kodów PIN (*Personal Identity Number*) oraz zaawansowane urządzenie do kopiowania paska magnetycznego, czyli tzw. skimmingu. Kamera zostaje ukryta za świetlną reklamą, natomiast czytnik paska umieszcza się w szczelinie bankomatu przeznaczonej na kartę. Na podstawie skopiowanych danych tworzona jest idealna kopia karty, za pomocą której złodzieje (znając również PIN) pobierają gotówkę z bankomatu. Fałszywy bankomat działa na podobnej zasadzie, z tym że przy próbie wypłaty gotówki odpowiada, że transakcja nie może zostać zrealizowana[13].

Nie jest do końca jasne, kto odpowiada za transakcje przeprowadzone przez nieuprawnionego posiadacza sfałszowanej w ten sposób karty. W regulaminach banków zwykle znajduje się zapis, że bank nie odpowiada za operacje z użyciem karty potwierdzone kodem PIN, co jednakże należy skonfrontować z postanowieniami Ustawy z 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. 2002 nr 169 poz. 1385). Jeżeli bowiem bank nie potrafi wykazać winy klienta, wówczas sam musi pokryć straty.

Systemy EFT-POS (*Electronic Funds Transfer Point-of-Sale*), zwane popularnie POS-ami, integrują systemy informatyczne banków oraz centra autoryzacyjno-rozliczeniowe z elektronicznymi kasami sektora handlowego. W momencie zapłaty przez klienta kartą płatniczą za towar lub usługę sprzedawca dzięki terminalowi POS nawiązuje kontakt z centrum autoryzacyjno-rozliczeniowym, które z kolei jest połączone z systemem banku-wystawcy karty. Po identyfikacji klienta (weryfikacja podanego kodu PIN lub/i podpisanego rachunku) oraz sprawdzeniu, czy transakcja może zostać zatwierdzona (tzn. zbadaniu czy na rachunku klienta znajdują się wystarczające środki lub nie został przekroczony limit kredytowy) konto klienta jest obciążane kwotą transakcji[14].

1.2. Bankowość telefoniczna

Do bankowości telefonicznej zaliczamy phone banking oraz SMS banking. Pierwszy z nich jest realizowany za pośrednictwem telefonu z wybieraniem tonowym. Klient może mieć możliwość połączenia z automatem bądź z operatorem lub konsultantem. Funkcje automatu są ograniczone. Klient ma do dyspozycji pełną paletę usług pasywnych – zarówno dla rachunków bieżących, jak i terminowych – jednakże ze względu na ograniczenia techniczne może wykonać tylko nieliczne

[13] Przestępstwa z kopiowaniem paska magnetycznego mają zastosowanie tylko dla kart płaskich i embosowanych (tłoczonych, wypukłych), nie zaś dla kart z mikroprocesorem.

[14] Opis autoryzacji jest słuszny dla kart płaskich. W przypadku kart embosowanych autoryzacja następuje przy użyciu urządzenia zwanego imprinterem (powielaczem, żelazkiem) lub telefonicznie. W przypadku kart tłoczonych niewielkie transakcje (do około 400 zł. nie podlegają autoryzacji. Jednakże karty embosowane mają tę przewagę nad płaskimi, że umożliwiają zakupy drogą zdalną (np. przez telefon lub Internet). W przypadku dokonywania zakupów drogą zdalną użytkownik karty podaje sprzedawcy: imię i nazwisko, numer oraz termin ważności karty, następnie transakcja jest autoryzowana w centrum autoryzacyjno-rozliczeniowym. Posiadacz karty nie jest w żaden sposób weryfikowany, nie jest sprawdzany numer PIN ani nie następuje podpisanie rachunku, nie jest również wymagana fizyczna obecność karty. W przypadku zakupu produktu materialnego dodatkowa weryfikacja może polegać na sprawdzeniu zgodności adresów: adres klienta posiadany przez bank musi być zgodny z adresem, na który będą przesłane zakupy. W przypadku zakupów produktów cyfrowych (np. muzyczne pliki MP3) taka weryfikacja jest niemożliwa. Opracowano na podstawie zasobów portalu eBanki. pl.

operacje aktywne. W istocie rzeczy wykonanie np. przelewu przez telefon, bez kontaktu z konsultantem jest możliwe, ale tylko dla zlecenia predefiniowanego. Klient w trakcie połączenia podaje kwotę transakcji – jedyny zmienny parametr zlecenia. W przypadkach call center, gdzie zasiadają konsultanci, dostępne możliwości są znacznie bogatsze.

Zabezpieczenia bankowości telefonicznej są wielopłaszczyznowe. Do operacji pasywnych użytkownik ma dostęp po podaniu identyfikatora i kodu PIN, do operacji aktywnych najczęściej przy użyciu kolejnych kodów lub haseł jednorazowych. Ponadto stosowane są dodatkowe zabezpieczenia, takie jak:

- system VRS (*Voice Recognition System*),
- system z czytnikiem kart magnetycznych lub chipowych,
- system z autoryzacją transakcji.

Technologia VRS bazuje na systemie rozpoznającym głos właściciela rachunku. Wówczas, po podaniu numeru identyfikacyjnego, właściciel powinien też wypowiedzieć hasło, na podstawie którego system go rozpoznaje. Prócz tego ze względów bezpieczeństwa rozmowy na łączach call-center są nagrywane.

Klienci mogą otrzymywać od banków specjalne przystawki do aparatów telefonicznych z czytnikami kart magnetycznych lub chipowych. Dzięki temu dostęp do bankofonu mają wyłącznie posiadacze takich przystawek, znający kod inicjalizujący połączenie.

Niekiedy stosuje się procedurę autoryzacji transakcji, która polega na tym, że pracownik banku po przyjęciu zlecenia, ale przed jego wykonaniem, powiadamia klienta o zamiarze przeprowadzenia operacji. Czyni to o określonej godzinie i gdy klient potwierdzi zlecenie, jest ono wykonywane.

SMS banking jest częścią m-bankingu, czyli bankowości mobilnej. Jego zastosowania stale rosną, jak zresztą wszystkich kanałów dystrybucji bankowości elektronicznej. W SMS bankingu przeważają operacje pasywne (powiadomienie o wpływach i wypływach z rachunku, podanie salda bądź jego historii, informacje finansowe – np. kursy walut, akcji lub administracyjne – zmiana hasła dostępu, itp.), choć w niektórych bankach wprowadzono już szerszy wachlarz usług, w którego skład wchodzą dokonywanie przelewów czy płatność rachunków[15].

Bezpieczeństwo usługi realizowane jest poprzez mechanizmy operatora sieci zapewniające poufność i autoryzację transmisji. Przesyłanie informacji następuje tylko z lub do telefonu komórkowego, którego numer jest zdefiniowany w systemie. Czasami uwierzytelnienie opiera się na haśle SMS (tzw. telekodzie), identyfikatorze klienta lub numerze rachunku. Należy zaznaczyć, że transmisja wiadomości SMS nie jest szyfrowana[16].

1.3. Bankowość internetowa

E-konto[17] oferuje najszerszą gamę produktów ze wszystkich elektronicznych bankowych kanałów dystrybucji. Możliwości Internetu doprowadziły do powstania jednostek tylko i wyłącznie wirtualnych, które nie posiadają oddziałów w realnym świecie. Takie banki funkcjonują w sieci WWW (*World Wide Web*), dzięki czemu istnieją w środowisku multimedialnym (tekst, grafika, dźwięk). W banku wirtualnym nie ma fizycznego ruchu pieniędzy ani dokumentacji. Wszystko funkcjonuje w postaci zapisu elektronicznego. Rolę sali operacyjnej przejmują sieć komputerowa i poczta elektroniczna.

Dla banków wirtualnych granice państwowe stanowią znacznie mniejszy problem. Te banki nie muszą korzystać z pośredników, takich jak sprzedawcy usług czy banki korespondenci. Dzięki

[15] *Vide* oferta Inteligo (SMSMoney, Serwis SMS) czy mBanku.

[16] Realizowany właśnie przez Polską Telefonię Cyfrową (właściciela marki Era) projekt 'bezpieczna bankowość' umożliwia symetryczne (po obu stronach) szyfrowanie w standardzie DES3. Jednak to rozwiązanie nie jest jeszcze powszechnie używane przez banki.

[17] E-konto oznacza zarówno konto w banku wirtualnym, jak i tradycyjnym, który zapewnia klientom dostęp do ich rachunków poprzez Internet. Dostęp do E-konta wymaga jedynie posiadania przeglądarki stron WWW.

temu, że nie prowadzą obsługi kasowej i nie utrzymują zaplecza bankowego, ich koszty osobowe i rzeczowe ulegają niebagatelnej redukcji. Wszystkie operacje są dokonywane automatycznie i przeprowadzane w sieci komputerowej.

Banki wirtualne nieustannie wzbogacają własną ofertę, dodając do niej produkty komplementarne: ubezpieczeniowe i inwestycyjne. Sama oferta bankowa także jest rozszerzana. Prócz możliwości dokonywania przelewów, ustalania poleceń zapłaty, zleceń stałych wprowadza się możliwości zaciągania kredytu i popadania w debet[18].

Bezpieczeństwo kanału internetowego zapewniają przede wszystkim:

- szyfrowana transmisja danych za pomocą protokołu SSL[19];
- proste uwierzytelnianie[20] oparte na identyfikatorze użytkownika i haśle PIN;
- silne uwierzytelnianie oparte na tokenie, certyfikacie użytkownika, kluczu kryptograficznym, karcie haseł, karcie magnetycznej (urządzenia elektroniczne lub mechanizmy cyfrowe);
- podpis elektroniczny (cyfrowy).

Ponadto stosowane są dodatkowe metody zwiększające bezpieczeństwo. Należą do nich m.in. zapory ogniowe, czyli tzw. *firewalle*. Firewall chroni system przed bezpośrednimi atakami hakerów, nie pozwalając na niedozwolony sposób komunikacji z serwerem z innych portów TCP/IP. Prócz tego system rejestruje wszelkie ślady aktywności użytkownika oraz operacje jakie były wykonywane (np. próby logowania do systemu, odczyt historii konta, wykonanie przelewu, itp.), zapisywane dane obejmują również adres IP użytkownika. W przypadku kilkukrotnego (zwykle trzykrotnego) podania złych danych podczas logowania następuje automatyczna blokada konta. Przy braku aktywności użytkownika przez określony czas (np. 8 minut) inicjalizowane jest automatyczne zakończenie sesji i wylogowanie. Nie bez wpływu na bezpieczeństwo pozostają również jasne i logiczne procedury operacyjne dla administratorów sieci i doradców klienta.

Przy bezpieczeństwie całego systemu należy pamiętać, że jest ono tak mocne, jak najsłabszy jego element.

Zapewnienie bezpieczeństwa nie jest tylko problemem banku, ale również klienta. Niewskazane jest używanie do połączeń z serwerem banku nieznanych komputerów, szczególnie znajdujących się w kawiarenkach internetowych, klubach studenckich, itp. Realizacja oczekiwanego bezpieczeństwa może być równoznaczna z koniecznością rezygnacji z odmiejscowienia na rzecz korzystania z komputerów dedykowanych, podlegających ochronie. Wskazane jest zapoznanie się z konfiguracją użytkowanej przeglądarki internetowej, zwłaszcza w obszarze ustawień zabezpieczeń, zezwoleń, czy chociażby autouzupełniania[21].

1.4. WAP banking

WAP (*Wireless Aplication Protocol*, czyli Protokół Aplikacji Bezprzewodowych) umożliwia dostęp do Internetu z telefonu komórkowego. Dlatego też stanowi ogniwo łączące bankowość internetową z telefoniczną. WAP pozwala na oglądanie serwisów internetowych przygotowanych specjalnie pod kątem tego narzędzia. Klasyczne serwisy WWW są tworzone w języku HTML, serwisy WAP są tworzone w języku WML.

[18] Vide mBank i Inteligo.

[19] SSL (*Secure Socket Layer*) jest protokołem sieciowym używanym do bezpiecznych połączeń internetowych. SSL realizuje szyfrowanie, uwierzytelnienie serwera (ewentualnie użytkownika również) i zapewnienie integralności oraz poufności przesyłanych informacji. W momencie nawiązania połączenia z bezpieczną (wykorzystującą protokół SSL) stroną WWW następuje ustalenie algorytmów oraz kluczy szyfrujących, stosowanych następnie przy przekazywaniu danych między przeglądarką a serwerem WWW. W protokole SSL stosuje się różne algorytmy szyfrujące: asymetryczne (np. algorytm RSA) lub symetryczne (np. algorytm RC-4). Powszechnie przyjmuje się, że długości: klucza asymetrycznego – 1024 bity, a symetrycznego – 128 bitów są wystarczające.

[20] Uwierzytelnienie to identyfikacja, sprawdzenie tożsamości użytkownika.

[21] Kwestia ryzyka informatycznego (operacyjnego) została szerzej opisana w rozdziale temu poświęconym.

Do szyfrowania danych w połączeniach z użyciem WAPu służy protokół WTLS (*Wireless Transport Layer Security*). WTLS jest analogicznym rozwiązaniem do SSL (*Secure Socket Layer*) stosowanym dla stron WWW.

Komunikacja między użytkownikiem telefonu komórkowego a serwerami, na których umieszczone są poszczególne serwisy odbywa się poprzez sieci GSM i Internet, które łączy ze sobą tzw. WAP-gateway zwykle należący do operatora sieci GSM. Szyfrowanie WTLS odbywa się na drodze od telefonu do gateway'a, a na drodze od gateway'a do serwera banku jest stosowane szyfrowanie SSL.

Z powyższego zatem wynika, że do bezpiecznych połączeń przez komórkę niezbędne jest spełnienie trzech warunków:

- obsługa SSL (https: //) po stronie banku, adres internetowy musi rozpoczynać się od https;
- obsługa SSL oraz WTLS w WAP-Gateway;
- obsługa WTLS w telefonie/przeglądarce WAP.

Najbardziej zaawansowana klasa 3. szyfrowania WTLS jest równoważna z SSL. Specyfikacja klas WTLS wygląda następująco:

- WTLS klasa 1: szyfrowanie danych;
- WTLS klasa 2: szyfrowanie danych, weryfikacja certyfikatu serwera;
- WTLS klasa 3: szyfrowanie danych, weryfikacja certyfikatu serwera, weryfikacja certyfikatu klienta;
- WTLS cechy dodatkowe: współpraca z elektronicznymi kartami kryptograficznymi, kompresja danych[22].

Obecnie trwają prace w zakresie wprowadzenia do technologii WAP podpisu elektronicznego generowanego z telefonów komórkowych. W takim przypadku znajduje się on w telefonie, który służy jednocześnie jako medium komunikacyjne. Aparat można wykorzystać także jako narzędzie do tworzenia i przechowywania podpisu elektronicznego w bankowości internetowej. Wówczas podpis zapisany w telefonie służy dwóm kanałom dystrybucji e-bankingu[23].

1.5. Bankowość komputerowa – modemowa

Home banking i *office banking* należą do grupy usług tzw. banku domowego. W istocie rzeczy usługa jest ta sama, inny jest jednak jej beneficjent. *Home banking* adresowany jest do osób indywidualnych (prywatnych)[24], natomiast *office banking* do przedsiębiorstw i instytucji. Mimo wszystko występują pewne różnice między tymi dwoma typami usługi. W *office bankingu* na przykład, system bankowości elektronicznej powiązany jest z systemem księgowo-finansowym przedsiębiorstwa, czego ze zrozumiałych względów nie ma u osób indywidualnych. To rodzi pewne konsekwencje, m.in. takie, że systemy office bankingu są bardziej skomplikowane i podatne na zagrożenia. Ostatnia uwaga wynika choćby z faktu, że system użytkuje więcej osób.

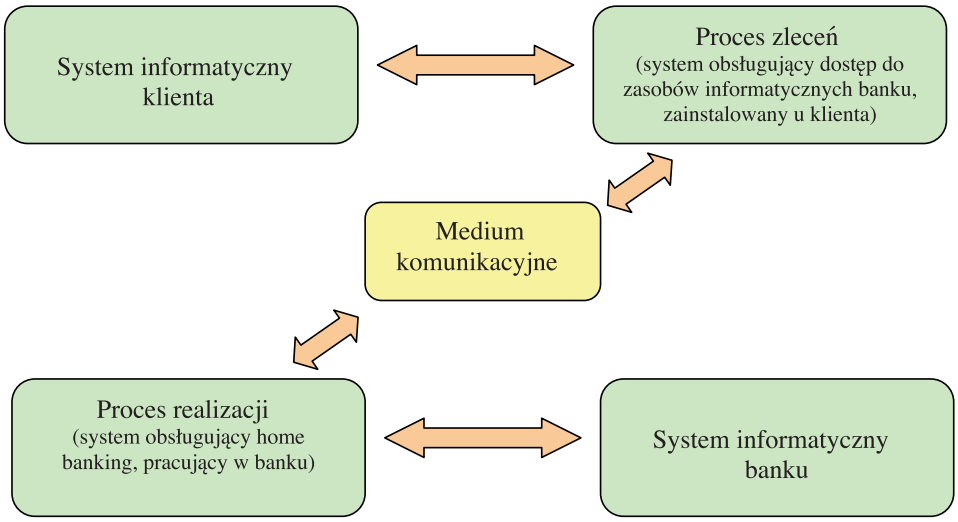
Diagram 2 prezentuje schemat połączenia między klientem a bankiem.

[22] Aby połączenie przez WAP było stosunkowo bezpieczne, telefon WAP musi posiadać: protokół szyfrowania WTLS co najmniej klasy 2, protokół szybkiej transmisji danych GPRS (*General Pocket Radio Service*), możliwość ustawienia kilku zestawień konfiguracji dla WAP-gateway, obsługę Cookies, wyświetlanie polskich znaków literowych w przeglądarce WAP, odpowiednio duży, kolorowy wyświetlacz. Opracowano na podstawie zasobów portalu eBanki. pl

[23] Opracowano na podstawie rozmowy z P. Czarneckim – dyrektorem wykonawczym ds. rozwoju i zarządzania produktami Polskiej Telefonii Cyfrowej przeprowadzonej przez W. Grobickiego. Vide Grobicki (2003).

[24] Stąd *private banking*.

Diagram 2. Schemat połączenia systemu informatycznego klienta home/office bankingu z systemem informatycznym banku



Źródło: Żuk (1997): Home banking – nowa metoda walki o klienta.

Komentarz do rysunku powinno się zacząć od medium komunikacyjnego. Może to być połączenie przez Internet (TCP/IP), łącze ISDN, modem-modem, itp. Zależnie od tego, czy system home bankingu jest on-line (przepływ informacji i aktualizacja odbywa się w sposób ciągły), czy off-line (informacje są przygotowywane, przesyłane oraz pobierane okresowo), wykorzystywane jest z reguły inne medium komunikacyjne. Występuje również inny poziom ryzyka. Systemy on-line uważa się powszechnie za bardziej niebezpieczne. Łatwiej jest bowiem zaatakować system, który stale ma połączenie z siecią. Natomiast w przypadku systemu off-line, połączenie jest krótkie – trwa tylko tyle, ile trzeba by wysłać wiązkę plików.

Funkcjonalność home bankingu jest podobna do i-bankingu, choć trzeba przyznać, że ten pierwszy jest przeznaczony do trochę innych celów. Wynika to z faktu, że systemy tego rodzaju częściej użytkują przedsiębiorstwa, które korzystają w większym stopniu z płatności masowych – czy to na rzecz kontrahentów, ZUS, czy własnych pracowników (wynagrodzenia). Systemy home bankingowe są bardziej dopasowane do potrzeb dużych firm.

Proces zleceń (*de facto* system home bankingowy) i proces realizacji (system analogiczny po stronie banku) muszą być kompatybilne z zapleczem informatycznym jednostek macierzystych. Transmisja danych, uwierzytelnianie odbywają się podobnie jak w bankowości internetowej. Ta sfera bezpieczeństwa praktycznie niczym się nie różni. Jednak istnieją pewne różnice w przypadku office bankingu w innym obszarze. Właściwe zasady ryzyka nakazują podział użytkowników w przedsiębiorstwie na trzy grupy: administratorów, użytkowników zwykłych i osoby z prawem autoryzacji. Administrator odpowiada za funkcjonowanie systemu w przedsiębiorstwie, jego współpracę z innymi programami, np. księgowymi, archiwizującymi, nadawanie i ograniczanie praw i zakresów dostępu oraz za przesyłanie danych i ich pobieranie z banku. Zwykły użytkownik korzysta z programu w ściśle określonym zakresie, wprowadza lub/i pobiera dane – jego możliwości mogą być rozszerzane bądź ograniczane. Osoba z prawem autoryzacji posiada, z tytułu zajmowanego stanowiska lub szczególnego umocowania, prawo do akceptowania w imieniu firmy płatności i innych operacji bankowych. Prawo to wynika bezpośrednio z uprawnień nadanych w karcie wzorów podpisów składanej w każdym banku, w którym przedsiębiorstwo otwiera rachunek główny lub pomocniczy. Nie należy łączyć uprawnień do administracji i autoryzacji. Pozwala to na dodatkową kontrolę dyspozycji przesyłanych za pomocą systemu do banku.

W banku także powinien występować podział uprawnień pracowników. Takie rozwiązanie wydatnie zmniejsza ryzyko ze strony nieuczciwych pracowników, którzy mogliby, posiadając zbyt szerokie uprawnienia, dokonywać malwersacji finansowych. Dla pracownika banku w departamen-

cie obsługi systemów home bankingowych nie stanowi problemu nadanie sobie uprawnień autoryzacyjnych dla zleceń w imieniu jakiegoś przedsiębiorstwa tudzież modyfikacja kodów dostępu do rachunku. Dlatego szybko działające mechanizmy kontrolne są niezbędne.

Komentując aspekt ryzyka home bankingu, a także bankowości internetowej i innych elektronicznych kanałów dystrybucji, należy wspomnieć o ostatnio zarysowanej tendencji do wyprowadzania poza bank pewnych funkcji. Banki nie muszą tworzyć własnych systemów informatycznych bankowości elektronicznej. Powinny raczej zawierać sojusze strategiczne z twórcami oprogramowania, sprzętu i dostawcami usług na zasadach outsourcingu. Nawet największe banki nie są w stanie nadążyć za tempem rozwoju technologii informatycznej i telekomunikacyjnej. Dzięki outsourcingowi zyskują także oszczędności kosztów. Jednakże służby bankowe muszą być zdolne do oceny ryzyka dzierżawionych systemów i stopnia konkurencyjności oferowanych usług[25].

1.6. Bankowość telewizyjna

Bankowość telewizyjna z racji swej prostoty może stać się alternatywą dla pozostałych kanałów dostępu. Na razie nie jest to popularna metoda kontaktu klienta z bankiem.

Set-top box jest urządzeniem pozwalającym na dekodowanie cyfrowego sygnału satelitarnego lub kablowego na formę umożliwiającą użytkownikowi odbieranie zrozumiałych dla niego komunikatów. Ponadto *set-top box* zawiera przeglądarkę internetową i protokół TCP/IP[26].

Elementy bezpieczeństwa w szyfrowaniu danych, uwierzytelnianiu, itp. są analogiczne w stosunku do bankowości internetowej. Tym niemniej wprowadzane zabezpieczenia dla bankowości telewizyjnej są jak dotychczas znacznie uboższe[27].

1.7. Karty i pieniądz elektroniczny

Karty elektroniczne oraz pieniądz elektroniczny wciąż zyskują na znaczeniu i ten fakt pozostaje bezsporny. Nie można również kwestionować, że obie formy podlegają szybkim zmianom, będąc nieustannie udoskonalane i dostosowywane do wymagań i oczekiwań środowiska. Karty stawiają do dyspozycji klienta coraz szersze spektrum możliwości. Obecnie nie tylko pozwalają na regulowanie płatności w sklepach czy zaciąganie kredytu odnawialnego, lecz także na spłatę zobowiązań podatkowych i ustanawianie poleceń zapłaty bezpośrednio z rachunku kartowego[28]. Klient może również czerpać korzyści z dodatkowych usług, już nie *stricte* bankowych, takich jak użytkowanie elektronicznej karty płatniczej do otwierania pomieszczeń zabezpieczonych czytnikiem kart lub wykonywanie telefonów z aparatów przystosowanych do obsługi kart z mikroprocesorem.

W kontekście ryzyka, dwa obszary wymagają przy tym punkcie głębszej analizy, a mianowicie bezpieczeństwo kart i instytucja pieniądza elektronicznego. Bezpieczeństwo użytkowania karty przez klienta niesie ze sobą ryzyko dla banku, jeśli chodzi o odpowiedzialność finansową za transakcje, które nie wynikły z winy klienta. W przypadku natomiast, gdy osoba trzecia wchodzi w posiadanie karty i/lub PINu klienta spowodowane jego niedbalstwem, wówczas należy uznać, że ten ostatni nie dopełnił ciążącego na nim obowiązku przechowywania kart z należytą starannością i w pełni odpowiada za wszelkie nieautoryzowane operacje.

---

[25] Wątek kosztów i ryzyka outsourcingu usług typu home banking na przykładzie systemu MultiCash został szerzej potraktowany w pracy: Górka, Markowski (2004): Teoria kosztów transakcyjnych a strategia firmy na przykładzie outsourcingu w Departamencie Bankowości Elektronicznej Raiffeisen Bank Polska SA.

[26] Tłumaczenie własne na podstawie informacji ze stron: http://searchnetworking.techtarget.com/sDefinition/0%2C%2Csid7_gci212971%2C00.html, http: //www.quinion.com/words/turnsofphrase/tp-set1.htm

[27] Pierwszym, i jak do tej pory, jedynym bankiem w Polsce, który oferuje usługi bankowości telewizyjnej jest InvestBank. Jego oferta sprowadza się do usług pasywnych i możliwości dokonania przelewu.

[28] Tego typu usługi są na przykład dostępne w USA w systemie MasterCard. Informacje ze strony http: //www.mastercard. com/cardholderservices

Według Ustawy o elektronicznych instrumentach płatniczych[29] bank odpowiada za (art. 28):

- operacje dokonane z użyciem utraconej karty płatniczej, jeżeli ich dokonanie nastąpiło wskutek nienależytego wykonania zobowiązania przez wydawcę lub akceptanta;
- operacje, w których karta płatnicza została wykorzystana bez fizycznego przedstawienia i elektronicznej identyfikacji posiadacza, o ile w umowie o kartę płatniczą nie zawarto możliwości dokonywania operacji na odległość bez fizycznego przedstawiania karty;
- operacje bez złożonego własnoręcznie podpisu posiadacza na dokumencie obciążeniowym;
- operacje zakwestionowane przez posiadacza z użyciem kodu identyfikacyjnego, chyba że został złożony podpis elektroniczny zgodnie z art. 5 ust. 1 Ustawy z 18 września 2001 r. o podpisie elektronicznym;
- operacje niewynikłe z winy klienta, przed zgłoszeniem przez niego utraty karty powyżej kwoty stanowiącej równowartość w złotych 150 euro.

Korzyścią dla bezpieczeństwa banku, a także jego klientów jest wprowadzanie kart z mikroprocesorem[30]. Powyżej zostały opisane niebezpieczeństwa związane z użytkowaniem kart magnetycznych (płaskich i embosowanych). Przy kartach chipowych nie ma możliwości skimmingu, czyli sczytania paska. Tak więc w celu użycia karty złodziej musi ją ukraść i zdobyć PIN, bowiem praktycznie nie jest w stanie stworzyć duplikatu.

Ze względu na znaczenie kart elektronicznych warto im poświęcić nieco miejsca. Dzielą się one na:

- karty pamięciowe (bez mikroprocesora),
- inteligentne karty pamięciowe[31],
- karty mikroprocesorowe (inteligentne, chipowe).

Karty mikroprocesorowe są najbardziej zaawansowanymi kartami elektronicznymi, będąc w praktyce swego rodzaju mikrokomputerami. Zapewniają wysoki poziom bezpieczeństwa, umożliwiając szyfrowanie danych za pomocą wielu algorytmów, które tkwią w układzie scalonym. W ich przypadku zminimalizowane jest także zagrożenie skopiowania danych z mikroprocesora. W pamięci układu scalonego można zapisać wielokrotnie więcej informacji niż na karcie magnetycznej. Dzięki chipowi z łatwością można za pomocą dedykowanego oprogramowania terminala zidentyfikować klienta oraz wykonać operację, sprawdzając – poprzez weryfikację salda rachunku klienta lub kontrolę zapisanych na karcie limitów transakcyjnych – możliwość jej przeprowadzenia. Są dwie metody autoryzacji karty chipowej w bankomacie – off-line i on-line. W pierwszym przypadku klient ma prawo wypłacić z bankomatu kwotę do wysokości zapisanego na karcie limitu środków i niepotrzebna jest każdorazowa łączność z rachunkiem bankowym. W drugim zaś przypadku łączność z rachunkiem jest nawiązywana i klient może wypłacić dowolną kwotę do limitu określonego przez bank (najczęściej tym limitem jest wysokość środków znajdujących się na rachunku).

---

[29] Zapisy ustawy są również komentowane w rozdziałach III: Rodzaje ryzyka e-bankingu i IV: Uwarunkowania prawne związane z ryzykiem bankowym w Polsce i UE (stan obecny i planowany).

[30] Wyraźnie widać to na przykładzie Francji, gdzie w latach 1996-2001 po wprowadzeniu kart z mikroprocesorem nastąpił lawinowy spadek strat banków francuskich z tytułu fałszerstw kart płatniczych (z 18 do niespełna 4 mln Euro). Dane ze strony: http: //www.kartyonline.net/stat_7.php

[31] Karty pamięciowe to najprostsze karty elektroniczne, gdyż element elektroniczny karty zawiera jedynie układy pamięci modyfikowalnej (EEPROM) i niemodyfikowalnej (EPROM) oraz logiczne układy pomocnicze. Karty te nie posiadają żadnych zaawansowanych zabezpieczeń przed odczytem i zmianą stanu ich pamięci. Inteligentne karty pamięciowe z wbudowanym systemem kontroli dostępu do danych mają możliwość odczytu lub zapisu danych wymagającą uprzedniego pomyślnego przejścia przez procedury kontrolne. Mogą one przykładowo polegać na podaniu odpowiedniego numeru PIN. Licznik błędów zlicza błędnie wprowadzane numery i po przekroczeniu ich ustalonej liczby (np. 3) karta jest blokowana. Karty pamięciowe o rozbudowanych funkcjach zabezpieczających stanowią większość obecnych na rynku elektronicznych kart telefonicznych. Najsilniejszym z zabezpieczeń jest procedura wyzwanie-odpowiedź (ang. challenge-response), stosowana w układach Eurochip i T2G, która pozwala na uwierzytelnienie karty w aparacie telefonicznym na podstawie danych wygenerowanych przez układ kryptograficzny karty.

Mikroprocesor jest wyposażony w pamięć stałą ROM (*Read Only Memory*), w której zapisany jest program operacyjny zarządzający obszarami pamięci i dostępem do nich. Prócz kodu PIN karta posiada jeszcze inne kody zabezpieczające i mechanizmy kryptograficzne. Karty mikroprocesorowe dają możliwość uwierzytelniania wydawcy i posiadacza karty w czasie rzeczywistym[32].

Poniżej w tabeli zaprezentowano różnice między kartami magnetycznymi i elektronicznymi.

Tabela 1. Cechy kart magnetycznych i elektronicznych

	Karta magnetyczna	Karta elektroniczna
Rok rozpowszechnienia	lata sześćdziesiąte	lata osiemdziesiąte
Zapis	jednokrotny	wielokrotny
Odczyt	wielokrotny	wielokrotny
Zasilanie	brak	niezbędne
Ochrona danych	brak zabezpieczeń przed odczytem zapisanych danych	karty pamięciowe – układy zabezpieczające (np. interfejs bezpieczeństwa lub blok bezpieczeństwa – funkcje kontroli dostępu pamięci oraz weryfikacja autentyczności karty karty mikroprocesorowe – procesor
Zapis informacji	nośnik magnetyczny	pamięć półprzewodnikowa z możliwością dodatkowego umieszczenia na karcie paska magnetycznego
Dokonywanie operacji logicznych i matematycznych	niemożliwe	możliwe we wbudowanym układzie scalonym
Pojemność pamięci	około 350 bitów	około kilkudziesięciu kilobajtów: różne rodzaje pamięci (ROM, PROM, EEPROM, RAM)
Odporność na zewnętrzne zakłócenia	brak	duża
Trwałość zapisu	1 rok	10 lat
Trwałość karty	1 rok	3 lata

Źródło: Molski: Karty elektroniczne a kontekst zabezpieczenia informacji. http: //www. bezpieczenstwoit. pl/Artykuly/Karty_inteligentne/M. Molski, Karty_elektroniczne_a_kontekst_bezpieczenstwa/index. html

Obok karty elektronicznej na potencjalne ryzyko jest podatny również pieniądz elektroniczny, który został zdefiniowany w art. 4 Ustawy z 29 sierpnia 1997 r. Prawo bankowe (Dz. U. 1997 nr 140 poz. 939). Zapis ustawowy brzmi następująco:

Pieniądz elektroniczny jest wartością pieniężną stanowiącą elektroniczny odpowiednik znaków pieniężnych, która spełnia następujące warunki:

- jest przechowywana na elektronicznych nośnikach informacji,
- jest wydawana do dyspozycji na podstawie umowy w zamian za środki pieniężne o nominalnej wartości nie mniejszej niż ta wartość,
- jest przyjmowana jako środek płatniczy przez przedsiębiorców innych niż wydający ją do dyspozycji,
- na żądanie jest wymieniana przez wydawcę na środki pieniężne,
- jest wyrażona w jednostkach pieniężnych.

Odnośnie pierwszego punktu definicji należy stwierdzić, że pieniądz elektroniczny przybiera bądź formę zapisu na karcie mikroprocesorowej, bądź na dysku komputera. Treść kart może zostać odczytana na komputerze w odpowiednio oprogramowanym czytniku. Karty będące nośnikiem

[32] Ponadto karta mikroprocesorowa jest wielofunkcyjna. Może realizować nie tylko funkcje płatnicze, ale także niezwiązane bezpośrednio z operacjami bankowymi – np. może być nośnikiem podpisu elektronicznego, identyfikatorem posiadacza, kartą rabatową, dowodem tożsamości, itp. Dla banku zaś stanowi nieocenione źródło informacji o kliencie, pozwalające na indywidualizację oferty, rozwijanie programów lojalnościowych i segmentację klientów.

pieniądza elektronicznego noszą nazwę elektronicznych portmonetek i należą do grupy kart przedpłaconych (*pre-paid*) używanych w trybie off-line bez potrzeby każdorazowej autoryzacji. Pieniądz zapisany na dysku komputera nosi miano *software* lub *network money*[33].

Bank odpowiada finansowo za przestępstwa dokonane z użyciem wydanego przez siebie pieniądza elektronicznego. Przykładowo, jeśli pieniądz zostanie wydany przez użytkownika dwukrotnie, to konsekwencje tego ponosi także bank.

W kontekście pieniądza elektronicznego i kart płatniczych należy wspomnieć o ryzyku utraty reputacji przez bank. Wszelkie przestępstwa wpływają negatywnie na wizerunek instytucji. Nie chodzi o samą odpowiedzialność finansową, ważniejszym aspektem jest utrata zaufania klientów, którzy po nieprzyjemnych doświadczeniach z użyciem kart lub *e-money* zrażają się do banku i nowoczesnych form płatności. Dlatego w żywotnym interesie banku leży zapewnienie klientom najwyższych możliwych zabezpieczeń oraz odpowiednia edukacja użytkowników tego typu rozwiązań tak, by sami potrafili unikać zagrożeń.

W rozdziale zaprezentowano podział bankowych elektronicznych kanałów dystrybucji oraz scharakteryzowano poszczególne kanały ze szczególnym uwzględnieniem aspektu bezpieczeństwa. Już na tym etapie pracy widać, że w wielu przypadkach ryzyko klientów jest jednoznaczne z ryzykiem banku. Większość z potencjalnych zagrożeń opisanych w tym rozdziale wchodzi w skład szeroko pojętego ryzyka operacyjnego, a także prawnego i reputacji banku[34].

Ostatni punkt został wyodrębniony ze względu na swoją wagę, nie da się bowiem ukryć, że ani karty elektroniczne, ani pieniądz elektroniczny nie są kanałem dystrybucji, a tylko nośnikiem danych lub nowoczesną formą środków płatniczych. Tym niemniej problemy, jakie stwarzają bankom, są istotne. Odpowiedzialność instytucji kredytowych za transakcje przeprowadzone przy pomocy skradzionych kart płatniczych, za oszustwa popełnione przy użyciu elektronicznych pieniędzy są niczym innym, jak tylko ryzykiem banków, którego korzenie tkwią w bankowości elektronicznej. Fakt wykorzystania skradzionej karty kredytowej przez złodzieja oznacza dla banku stratę finansową. Bank ponosi ryzyko kredytowe oraz płynności, które mają bezpośredni wpływ na wynik z jego działalności.

Stąd, że natura każdego z opisanych elektronicznych kanałów dystrybucji jest inna niż natura oddziałów oraz że wykorzystanie któregokolwiek z tych kanałów niesie ze sobą określone niebezpieczeństwa dla klienta i banku, można wysnuć wniosek, że te same rodzaje ryzyka bankowości tradycyjnej (oddziałowej): kredytowe, stopy procentowej, rynkowe, płynności nabierają odmiennego charakteru w kanałach elektronicznych. Jak wynika z treści rozdziału, poziom bezpieczeństwa transakcji w poszczególnych kanałach nie zawsze bywa doskonały, zaś banki mają ograniczoną możliwość kontroli otoczenia[35]. Prawdą jest zatem, że takie rodzaje ryzyka jak: operacyjne, prawne i reputacji wychodzą na pierwszy plan. Można tu się powołać na szereg zamieszczonych przykładów, choćby ten związany z ryzykiem oportunizmu pracowników użytkujących system home bankingu w przedsiębiorstwie. Przy nieprawidłowym podziale uprawnień pracowników, np. braku rozgraniczenia na administratorów, użytkowników zwykłych i osoby z prawem autoryzacji zwiększa się ryzyko operacyjne. Podobnie bywa w przypadku bankowości internetowej, np. gdy system autoryzacji zawodzi i pod klienta podszywają się niepowołane osoby. W dalszej kolejności ryzyko operacyjne implikuje ryzyko prawne i reputacji.

Banki nie rozwijają bynajmniej kanałów elektronicznych ze względu na swoje własne ambicje, czynią to w odpowiedzi na żądania rynku. Badania IBnGRu oraz McKinsey&Company, na które powołano się we wstępie pracy, jednoznacznie potwierdzają, że klientom nie wystarczają już same

[33] Elektroniczną portmonetką jest na przykład niemiecka GeldKarte lub polska CitiConnect z Citibanku. Zaś do *software money* zaliczają się przykładowo systemy: DigiCash, e-Cash, MiliCent, CyberCoin.

[34] Wątek został rozwinięty w rozdziale III: Rodzaje ryzyka e-bankingu.

[35] Por. także rozdział III: Rodzaje ryzyka e-bankingu niniejszej pracy oraz Szpringer (2003).

[36] Internet może też być kanałem komplementarnym w stosunku do oddziału.

oddziały. Szukają oni kanałów substytucyjnych (np. Internet[36]) lub komplementarnych (np. bankomat). Skłonność do takich działań wypływa wprost z chęci człowieka do upraszczania życia i zwiększania wygody. Zatem we współczesnym świecie banki muszą oferować produkty przez elektroniczne kanały dystrybucji, bowiem w przeciwnym razie same się unicestwią.

Natomiast do sprawnego zarządzania i kontroli ryzyka związanego z kanałami elektronicznymi banki potrzebują wysokowykwalifikowanych pracowników, którzy będą w stanie sprostać zadaniu, mimo trudności jakie niesie ze sobą rozwój e-bankingu i dodatkowe zmiany ryzyka, które się w efekcie pojawiają.

2
Pojęcie ryzyka w bankowości i jego systematyka z uwzględnieniem natury e-bankingu

Każda działalność gospodarcza niesie ze sobą ryzyko. Banki komercyjne pełnią w gospodarce rolę instytucji zajmujących się transformacją tego ryzyka. Rola ta jest bezpośrednio związana z funkcją pośrednictwa finansowego realizowanego przez banki pomiędzy podmiotami mającymi nadwyżki bądź niedobory finansowe. Przedsiębiorstwa i gospodarstwa domowe lokują w bankach swoje oszczędności, licząc na dochód w postaci odsetek, biorą kredyty, płacąc za nie pewną cenę lub szukają zabezpieczeń przed stratami u niewiarygodnych partnerów. Banki zaś przejmują na siebie wynikające z tego ryzyko, mając jednocześnie możliwość jego dywersyfikacji, zmniejszenia, kompensacji lub realokacji.

Pojęcie ryzyka bankowego jest bardzo złożone, co utrudnia precyzyjne i jednoznaczne jego zdefiniowanie. Samo słowo 'ryzyko' pochodzi od starowłoskiego risicare oznaczającego 'odważyć się'[37]. Obecnie jest ono używane w wielu znaczeniach. Większość osób rozumie pod nim zagrożenie nieosiągnięcia zamierzonych celów, choć przecież odchylenie od stanu oczekiwanego może przynieść także korzyści, nie zaś tylko straty. Posługując się przykładem banku, zmiana kursu walutowego lub stopy procentowej może przyczynić się do poprawy bądź pogorszenia sytuacji banku. Jednak ryzyku w działalności kredytowej nie sposób przeciwstawić dodatkowych szans[38]. Przyjmując za cel całkowitą spłatę przez wierzycieli kredytów wraz z należytymi odsetkami i prowizjami, w najlepszym przypadku można osiągnąć ów cel, lecz nie ma szansy, że kredytobiorca przekroczy płatności ustalone w umowie.

W literaturze specjalistycznej, podkreślając znaczenie czynnika czasu, rozróżnia się dwa terminy: ryzyko i niepewność. Pierwszy z nich dotyczy sytuacji, gdzie znane jest prawdopodobieństwo wystąpienia określonego zdarzenia. Natomiast w sytuacjach właściwych dla niepewności rozkład prawdopodobieństwa jest nieznany[39]. F. Knight nazywa ryzyko niepewnością mierzalną, zaś niepewność – niepewnością niemierzalną. Ryzyko występuje wówczas, gdy można je określić za pomocą prawdopodobieństwa matematycznego, statystycznego i szacunkowego, przez co ma wymiar obiektywny. Niepewność jest subiektywna.

Idąc tym tokiem rozumowania, widać wyraźnie, że w bankowości występuje często sytuacja niepewności, a nie ryzyka. Trudno bowiem w kategoriach prawdopodobieństwa zmierzyć niebezpieczeństwo włamania się przez hakerów do systemu bankowości elektronicznej w celu kradzieży danych zapisanych na kartach kredytowych lub ryzyko outsourcingu zaplecza informatycznego na rzecz zewnętrznego partnera.

Będąc świadomym ekonomiczno-matematycznych różnic znaczeniowych między niepewnością a ryzykiem, traktuję ryzyko w niniejszej pracy jako sumę obu pojęć.

Następstwem złożoności istoty ryzyka bankowego jest olbrzymia liczba jego klasyfikacji. Ograniczę się do prezentacji jedynie najważniejszych.

Na najwyższym poziomie hierarchii ryzyko dzieli się na systemowe i specyficzne[40]. Pierwsze z nich odnosi się do ogółu społeczeństwa. Jego przejawem są na przykład inflacja lub masowe bezrobocie. Choć samo wpływa na ryzyko działalności banków komercyjnych, to nie może być przez nie w jakikolwiek sposób kontrolowane. Banki mają natomiast wpływ na ryzyko

[37] Bernstein (1997).

[38] Zawadzka (2002).

[39] Na podstawie pracy Jaworski (red.) (2002) za Keynes (1921) i Knight (1971).

[40] Opracowano na podstawie Przybylska-Kapuścińska (red.) (2001).

specyficzne, określane także mianem indywidualnego. Jego przyczyny są związane z rozmaitymi elementami, takimi jak: zarządzanie bankiem, stopień konkurencji w sektorze, struktura pasywów i aktywów.

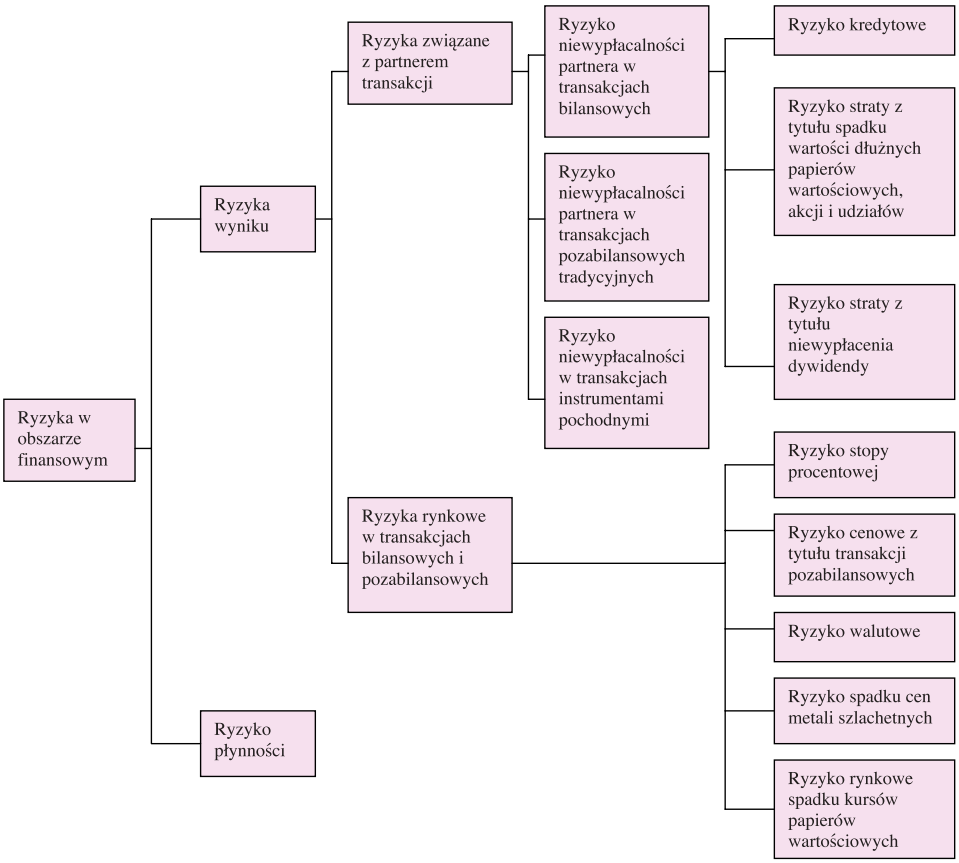
Na niższym szczeblu bank ma do czynienia z ryzykami strategicznym i operacyjnym, posiadającymi korzenie w ryzyku specyficznym. Głównym kryterium tego podziału jest horyzont działania oraz zakres skutków decyzji. Ryzyko strategiczne dotyczy długookresowej kondycji banku i jego miejsca w rynkowej sieci powiązań gospodarczych. Źródłem ryzyka strategicznego są decyzje zarządów oraz właścicieli kapitału banku w sferach o kluczowym znaczeniu – zasilanie banku w kapitał, ustalenie pola aktywności (np. czy bank skupia się na rynku korporacyjnym, czy detalicznym), wybór informatycznego systemu przetwarzania danych, szeroko zakrojone inwestycje na rzecz rozwoju bankowych elektronicznych kanałów dystrybucji. Na szczeblu operacyjnym uwidaczniają się skutki decyzji strategicznych. W tym miejscu podejmowane są decyzje bieżące, na przykład o przyznaniu kredytu danemu podmiotowi gospodarczemu, czy ustaleniu właściwej luki stopy procentowej dla pozycji bilansu do trzech miesięcy. Granica między ryzykiem strategicznym i operacyjnym bywa czasami bardzo płynna.

Z. Zawadzka proponuje podział ryzyka operacyjnego na[41]:

1. Ryzyko w obszarze finansowym.

2. Ryzyko w obszarze techniczno-organizacyjnym.

Diagram 3. Rodzaje ryzyka w obszarze finansowym



Źródło: opracowanie własne na podstawie Zawadzka (2002).

[41] Zawadzka (2002).

Według powyższego schematu poszczególne kategorie ryzyka oznaczają, co następuje:

1. Ryzyko płynności: zagrożenie przejściowej lub całkowitej utraty płynności przez bank.

2. Ryzyko wyniku: niebezpieczeństwo nieosiągnięcia przez bank założonego wyniku.

Wśród ryzyk wyniku występują:

2.1. Ryzyka związane z partnerem transakcji, czyli sytuacje, kiedy na skutek niewywiązywania się partnera transakcji ze swoich zobowiązań lub pogorszenia jego standingu (bonitetu, sytuacji finansowej), bank odnotowuje pewną stratę godzącą w założony wynik. Mogą to być:

2.1.1. Ryzyka podmiotowe z tytułu transakcji bilansowych, a więc takie ryzyka, na które bank jest narażony w przypadku:

- niespłacania przez kredytobiorcę zaciągniętych kredytów,
- straty z tytułu spadku wartości posiadanych walorów,
- niewypłacenia dywidendy przez spółki, w których bank ma udziały.

2.1.2. Ryzyka podmiotowe z tytułu transakcji pozabilansowych tradycyjnych, a więc udzielonych poręczeń i gwarancji.

2.1.3. Ryzyka podmiotowe z tytułu transakcji pozabilansowych instrumentami pochodnymi (swapowych, terminowych, opcyjnych), polegające na niewywiązywaniu się ze swoich zobowiązań partnera pierwotnej transakcji i w związku z tym konieczność pozyskiwania przez bank nowego partnera po wyższym koszcie.

2.2. Ryzyka rynkowe w transakcjach bilansowych i pozabilansowych, określane mianem cenowych, których przyczyną jest niekorzystne kształtowanie się na rynku cen instrumentów finansowych, tj. stóp procentowych, walut i kursów akcji. Mogą to być:

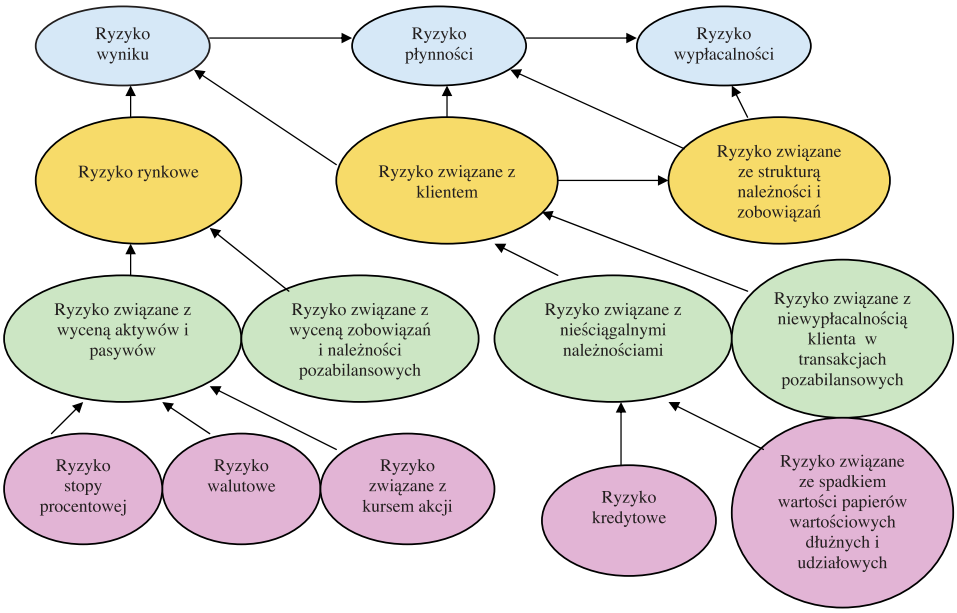
2.2.1. Ryzyka cenowe z tytułu transakcji bilansowych, spowodowane niekorzystnymi ruchami:

- stopy procentowej,
- waluty,
- cen metali szlachetnych,
- kursów papierów wartościowych, będącymi rezultatem ogólnego pogorszenia się sytuacji gospodarczej, a nie sytuacji konkretnej firmy.

2.2.2. Ryzyka cenowe z tytułu transakcji pozabilansowych (swapowych, terminowych, opcyjnych).

Profesor M. Górski dokonuje dynamicznego podziału ryzyka finansowego banku, zwracając uwagę na wzajemne relacje i oddziaływanie poszczególnych typów ryzyka (diagram 5, dynamiczny charakter obrazują strzałki). Przykładowo załóżmy, że polski bank w celu osiągnięcia wysokiego zysku zdecydował się na otwarcie znaczącej długiej pozycji w euro (wyższe ryzyko walutowe będące częścią rynkowego). Po pewnym czasie nastąpił trwały spadek wartości tej waluty, przed którym bank się nie zabezpieczył. Jednocześnie duża część zobowiązań banku w złotówkach, dla której pierwotnie pokryciem miał być przychód z kredytów udzielonych w euro, stała się wymagalna. W takiej sytuacji bank nie tylko nie osiągnął wysokiego zysku, ale jednocześnie naraził się na okresową utratę płynności (załóżmy, że nie udało mu się w porę refinansować na rynku międzybankowym lub w NBP). W krańcowej sytuacji utrata płynności mogłaby się przerodzić w trwałą niewypłacalność; na przykład wtedy, gdy bank znajdowałby się w złej kondycji finansowej, a informacje o kłopotach z płynnością spowodowałyby panikę na rynku i wycofanie wkładów z banku.

Diagram 4. Podział ryzyka finansowego banku



Źródło: Górski (2002).

Pobieżna analiza ryzyka banku w obszarze finansowym wskazuje, że nie ma istotnej różnicy w odpowiednich przekrojach ryzyka pomiędzy bankowością tradycyjną (oddziałową), a elektroniczną. Czyż bowiem na cenę akcji danej spółki lub złota ma wpływ fakt, że bank jest wirtualny bądź że zakupił walory za pośrednictwem platformy transakcyjnej w Internecie? Czy straty z tytułu spadku stopy procentowej lub kursu walutowego są inne tylko dlatego, że ponoszą je banki o odmiennym profilu wykorzystania kanałów dystrybucji. Z pewnością nie. Jednakże dokładniejsza analiza zespołu ryzyk finansowych doprowadza do uwypuklenia pewnych punktów. Istnieje niebezpieczeństwo, że ryzyko dla kredytów udzielanych drogą elektroniczną może być wyższe. Bank w kanale internetowym (do tej pory procedura kredytowa występuje tylko w tym kanale elektronicznym) musi szybciej opracowywać wniosek klienta. Poza tym służby bankowe w ograniczonym stopniu kontaktują się z nim osobiście i mają tym samym ograniczone pole manewru w ocenie (głównie na podstawie własnego doświadczenia i intuicji) czy wyjaśnienia klienta i dokumentacja przez niego przedstawiona są prawdziwe, spójne i pełne. Te elementy mogą wpłynąć na wzrost ryzyka kredytowego. Z drugiej strony zredukowany zostaje niepewny czynnik ludzki.

Należy zauważyć, że przyspieszenie działania banku i automatyzacja czynności w gospodarce elektronicznej naraża bank na utratę części kontroli. Służby bankowe nie są w stanie same nadzorować wszelkich operacji, muszą zdać się na niezawodność systemu. Dopóki jest on rzeczywiście niezawodny, problem nie istnieje[42].

Szersze zastosowanie systemów elektronicznych z jednej strony wpływa na wzrost ryzyka bankowego, z drugiej je redukuje. Jest to sprzeczność tylko pozorna, ponieważ korzystanie z systemów elektronicznych sprawia, że bank ma dostęp do stale aktualizowanych danych o kursach walut, akcji, poziomie stóp procentowych, itp. Na bieżąco może zbierać wszelkie wiadomości gospodarcze, które wywierają wpływ na jego funkcjonowanie, będąc zagrożeniem lub szansą. W konsekwencji jest w stanie szybciej reagować na zmiany w otoczeniu.

Trzeba by się także zastanowić, czy wzmożona działalność banków w kanałach elektronicznych i ich ekspansja na rynki zagraniczne tą drogą, wzrost wolumenu i użycia pieniądza elektronicznego, rozwój instytucji parabankowych, liberalizacja przepisów, globalizacja i internacjonalizacja rynków finansowych, postęp techniczny oraz coraz większe znaczenie Nowej Gospodarki nie powo-

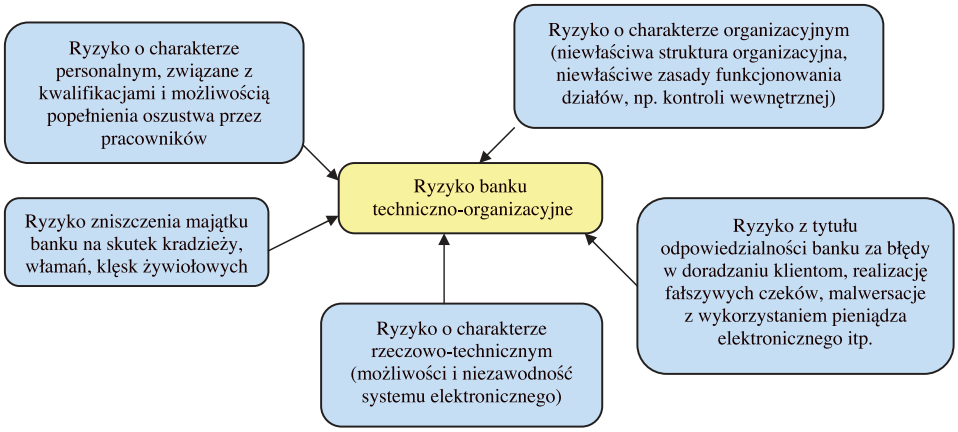
[42] Ryzyko operacyjne bankowości elektronicznej zostało szerzej omówione we właściwym rozdziale.

dują zmian w układzie ryzyka systemowego i specyficznego. Prawdopodobnie bowiem ryzyko systemowe rośnie. Tym niemniej te rozważania znajdują się poza głównym nurtem pracy.

Ten krótki wywód dowodzi, że niezależnie od medium komunikacyjnego, powyższe klasyfikacje ryzyka finansowego pozostają w mocy. Co prawda, bankowość elektroniczna może modyfikować ryzyko, nadając mu specyficzny charakter. Pokaże to dalsza weryfikacja postawionych we wstępie pracy hipotez.

Z. Zawadzka zdefiniowała również techniczno-organizacyjne ryzyko bankowe, którego systematykę pokazuje diagram 6. Na uwagę zasługuje fakt, że ta grupa ryzyk stanowi znakomite dopełnienie ryzyka w obszarze finansowym banku. Jak się później okaże, ryzyko techniczno-organizacyjne można utożsamiać z ryzykiem operacyjnym, stanowiącym element głównej klasyfikacji ryzyka przedstawionej w niniejszej pracy.

Diagram 5. Ryzyko banku w obszarze techniczno-organizacyjnym



Źródło: opracowanie własne na podstawie Zawadzka (2002).

Ostatnio bardzo wzrosło znaczenie Komitetu Bazylejskiego (*Basel Committee*) [43], założonego w 1974 r. przez grupę dziesięciu banków centralnych (tzw. *Group of Ten*) [44]. Należy podkreślić, że Komitet nie posiada jakiejkolwiek ponadnarodowej władzy prawnej, która pozwoliłaby mu narzucać krajom swoje rozwiązania. Jego zadaniem jest formułowanie na podstawie przeprowadzonych badań standardów nadzorczych, ogólnych wytycznych oraz dobrych praktyk dla banków. Od krajowych bankowych organów nadzorczych oczekuje się ich uwzględnienia w porządku prawnym państwa, pozostawiając tymże organom niezbędną przestrzeń do dopasowania rozwiązań do specyfiki systemu krajowego. Działania Komitetu są skierowane na minimalizację różnic w międzynarodowych standardach nadzorczych. Dąży on, aby zostały wdrożone dwie podstawowe zasady: każdy bank zagraniczny musi podlegać nadzorowi oraz nadzór musi być adekwatny.

W 1988 r. Komitet zaproponował nowatorski sposób pomiaru ryzyka kapitałowego. Swoje rozwiązania zawarł w regulacjach tzw. Umowy Kapitałowej (*Basel Capital Accord*). Zakładała ona przede wszystkim wprowadzenie współczynnika wypłacalności kapitałowej na poziomie co

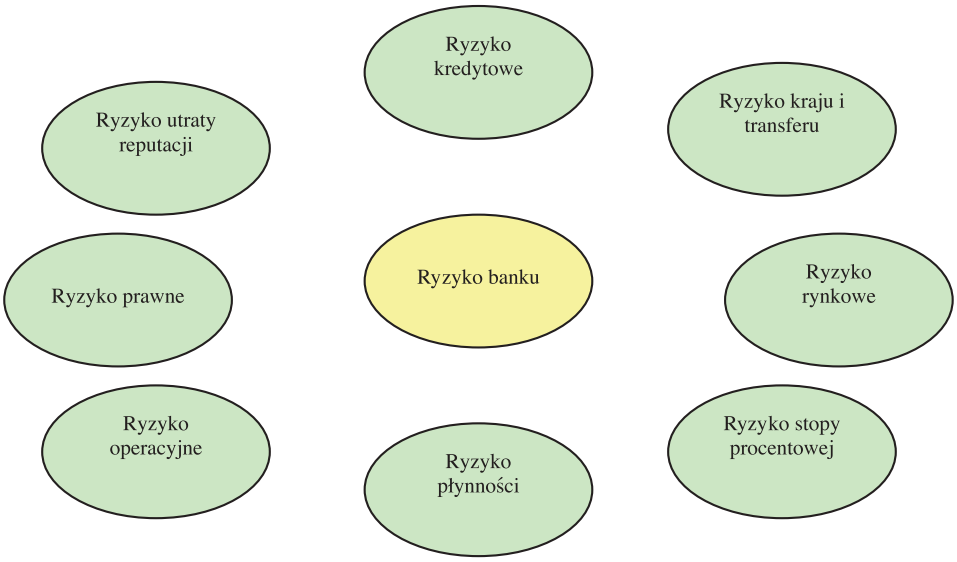
[43] Członkami Komitetu Bazylejskiego są obecnie: Belgia, Kanada, Francja, Niemcy, Włochy, Japonia, Luksemburg, Holandia, Hiszpania, Szwecja, Szwajcaria, Wielka Brytania i Stany Zjednoczone, a więc kraje o najlepiej rozwiniętych systemach bankowych na świecie. W Komitecie poszczególne państwa reprezentują właściwe banki centralne lub ciała krajowe zajmujące się nadzorem bankowym. Komitet Bazylejski ściśle współpracuje z Bankiem Rozliczeń Międzynarodowych (BIS – *Bank for International Settlements*), który jest bankiem banków centralnych oraz największą instytucją tego typu sprzyjającą rozwojowi międzynarodowej współpracy finansowej i monetarnej. Z BIS są związane (tłumaczenie własne): wspomniany już Bazylejski Komitet ds. Nadzoru Bankowego (*Basel Committee on Banking Supervision*), Komitet ds. Systemów Płatności i Rozliczeń (*Committee on Payment and Settlement Systems*), Komitet ds. Globalnych Systemów Finansowych (*Committee on the Global Financial System*) i Komitet Rynków (*Markets Committee*). W ramach komitetów pracują grupy robocze, np. Elektroniczna Grupa Robocza, działająca pod auspicjami Bazylejskiego Komitetu ds. Nadzoru Bankowego).

[44] Group of Ten składa się z reprezentantów jedenastu uprzemysłowionych krajów świata: Belgii, Kanady, Francji, Niemiec, Włoch, Japonii, Holandii, Szwecji, Szwajcarii, Wielkiej Brytanii oraz Stanów Zjednoczonych.

najmniej 8%, sugerując czas wdrożenia tego rozwiązania w bankowych systemach krajowych do 1992 r. Praktycznie cały świat podporządkował się zaleceniom. Istotna nowelizacja Umowy Kapitałowej z 1988 r. dotycząca ryzyka rynkowego została wprowadzona w 1996 r.[45] W czerwcu 1999 r. Komitet Bazylejski wydał dokument konsultacyjny pod tytułem Nowa Metodologia Adekwatności Kapitałowej (*A New Capital Adequacy Framework*), a następnie, po okresie konsultacji i poprawek, w czerwcu 2004 r. przyjął Nową Umowę Kapitałową (*Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework*). Obecnie obowiązuje kolejna zmodyfikowana wersja tego dokumentu z listopada 2005 r.. Oczekuje się, że Nowa Umowa Kapitałowa zostanie wprowadzona w życie do końca 2006 r., z ewentualnymi opóźnieniami po stronie krajów słabiej rozwiniętych. Do tego czasu wiążąca jest Umowa Kapitałowa z 1988 r.[46]

Zważywszy na znaczenie postanowień Komitetu Bazylejskiego i jego zasługi dla rozwoju systemów identyfikacji, pomiaru oraz zarządzania ryzykiem, wydaje się właściwe przyjąć w tej pracy następującą systematykę ryzyka[47]:

Diagram 6. Systematyka ryzyka bankowego według Komitetu Bazylejskiego



Źródło: opracowanie własne na podstawie: Komitet Bazylejski (wrzesień 1997).

Podane kategorie ryzyka występują we wszystkich bankowych kanałach dystrybucji, niezależnie od tego, czy są to oddziały, czy private- albo i-banking. Nawiązując do poprzednich klasyfikacji można zauważyć, że ostatni podział obejmuje (co dodatkowo wykażą zamieszczone dalej definicje poszczególnych rodzajów ryzyka)[48], całość problematyki – zarówno ryzyko finansowe, jak i techniczno-organizacyjne. Jednak, mimo tego że kategorie ryzyka są te same dla wszystkich kanałów dystrybucji, w kolejnych punktach pracy zostanie pokazana ich specyfika w e-bankingu.

Ryzyko kredytowe uznaje się za tradycyjny i podstawowy rodzaj ryzyka w bankowości, bowiem udzielanie kredytów stanowi zasadniczą działalność banków. Występuje ono wówczas, gdy kredytobiorca nie zwraca w całości lub części przypadających spłat rat kapitałowych wraz z uzgodnionymi odsetkami, prowizjami i innymi opłatami. Ryzyko kredytowe jest z reguły następstwem złej oceny zdolności kredytowej kredytobiorców tudzież nadmiernym zaangażowaniem finansowym banku wobec jednego lub grupy powiązanych ze sobą podmiotów. Duże koncentracje mogą rów-

[45] Basel Committee on Banking Supervision (1996).

[46] Opis wzmiankowanych rozwiązań został przedstawiony w rozdziale IV.

[47] Komitet Bazylejski (1997).

[48] Definicje oparto przede wszystkim na trzech źródłach: Komitet Bazylejski (wrzesień 1997); Jaworski (red.) (2002); Przybylska-Kapuścińska (2001).

nież powstać w określonych branżach, sektorach gospodarczych, czy regionach geograficznych lub poprzez posiadanie szeregu kredytów odznaczających się innymi cechami, które jednak narażają bank na działanie tych samych czynników gospodarczych (np. transakcje oparte na dużej dźwigni, o wysokim 'lewarowaniu'). W rzeczywistości ryzyko kredytowe dotyczy nie tylko kredytów, ale także innych zobowiązań banku, w równym stopniu bilansowych (np. inwestycje w papiery wartościowe), co pozabilansowych (np. udzielone gwarancje, poręczenia, akcepty, akredytywy). Banki narażają się na problemy kredytowe, gdy w porę nie rozpoznają złych aktywów i nie utworzą na nie rezerw albo gdy nie przestaną wliczać fikcyjnego dochodu w przychody odsetkowe. Ryzyko kredytowe często pojawia się w sytuacjach, gdy bank udziela kredytu jednostce, w której posiada udziały. Jest to spowodowane brakiem obiektywności w ocenie wniosku kredytowego. Warto także nadmienić, że kredyt odnawialny na karcie lub na rachunku oraz debety również wchodzą w zakres ryzyka kredytowego.

Z ryzykiem kredytowym ściśle wiąże się ryzyko kraju i transferu. W działalności zagranicznej bank musi brać pod uwagę czynniki ekonomiczne, polityczne i społeczne kraju kredytobiorcy. Ryzyko kraju najjaskrawiej widać na przykładzie kredytów udzielanych rządom i agencjom rządowym, dla których zwykle jedynym zabezpieczeniem jest wiarygodność państwa na arenie międzynarodowej. Na skutek zmiany sytuacji gospodarczej i politycznej kraj może zaprzestać spłaty zobowiązań[49]. Podobnie, nowe rządy mogą zakazać podległym przedsiębiorstwom prywatnym i osobom fizycznym regulowania zobowiązań. Bank może odczuć wpływ ryzyka kraju bezpośrednio lub pośrednio – poprzez pogorszenie sytuacji finansowej korzystających z kredytów importerów i eksporterów (klientów banku), prowadzących transakcje handlowe z danym państwem. Pod pojęciem ryzyka transferu kryje się niebezpieczeństwo, że waluta zobowiązania może stać się niedostępna dla kredytobiorcy bez względu na jego kondycję finansową. Ta sytuacja jest właściwa, gdy chodzi o zobowiązania denominowane w walucie obcej dla kredytobiorcy.

Ryzyko rynkowe wynika ze zmian cen rynkowych. Te fluktuacje mogą być zarówno korzystne, jak i niekorzystne dla banków. Podstawową częścią składową ryzyka rynkowego jest ryzyko walutowe, czyli niebezpieczeństwo pogorszenia się sytuacji finansowej banku w wyniku niepomyślnych zmian kursu walutowego. Na poziom tego kursu banki mają wpływ, ponieważ występują na rynku w charakterze tzw. market-makerów (tworzących rynek). Notują kursy walutowe dla swoich klientów oraz otwierają pozycje walutowe. W konsekwencji narażają się na potencjalne straty, nie potrafią bowiem precyzyjnie przewidzieć poziomu kursu. Ryzyko rynkowe stanowią także zmiany wartości towarów, akcji lub innych instrumentów finansowych, będących głównie częścią portfela handlowego banku (*trading*)[50].

Ryzyko stopy procentowej oznacza, że zmiany rynkowej stopy procentowej mogą narazić bank na straty. Ryzyko to wpływa zarówno na dochody banku, jak i na wartość ekonomiczną jego aktywów, pasywów i instrumentów pozabilansowych. Ryzyko stopy procentowej powiązane jest ściśle z ryzykiem rynkowym. Często zdarza się, że akcje, instrumenty dłużne, pozabilansowe oraz towary tracą na wartości ze względu na niekorzystne ruchy stopy procentowej[51]. Podstawowymi formami ryzyka stopy procentowej są:

1. Ryzyko przeszacowania (*repricing risk*) – wynik niedopasowania w czasie terminów zapadalności i wymagalności aktywów, pasywów oraz pozycji pozabilansowych banku dla stałej stopy procentowej oraz niedopasowania w czasie terminów przeszacowania pozycji bilansowych i pozabilansowych dla zmiennej stopy procentowej;
2. Ryzyko krzywej dochodowości (*yield curve risk*) – konsekwencja zmian nachylenia i kształtu krzywej dochodowości;

[49] Dlatego tak ważne jest korzystanie z raportów o ryzyku kraju i transferu międzynarodowych agencji ratingowych, takich jak: Fitch, Standard & Poor's, Moody's itp.

[50] Podział na portfel handlowy i bankowy został przedstawiony w części poświęconej sprawozdawczości banków komercyjnych w Polsce w świetle wymogów narzuconych przez organ nadzoru (KNB – Komisję Nadzoru Bankowego).

[51] Dlatego też np. Deutsche Bank traktuje ryzyko stopy procentowej jako element ryzyka rynkowego.

3. Ryzyko bazowe (*basis risk*) – rezultat niedoskonałej korelacji w dopasowywaniu stawek oprocentowania różnych instrumentów przychodowych i kosztowych, mimo że te instrumenty posiadają podobne charakterystyki przeszacowania;
4. Opcjonalność (*optionality*) – efekt jawnych lub ukrytych opcji wpisanych w szereg aktywów, pasywów i pozycji pozabilansowych banku.

Ryzyko płynności definiuje się jako zagrożenie przejściowej lub całkowitej utraty płynności przez bank. Występuje ono w sytuacjach, gdy bank ma obniżoną zdolność do regulowania zobowiązań na skutek gwałtownego wycofywania lokat lub niespłacania w ustalonym czasie rat kredytów. Warto jeszcze raz podkreślić związek między ryzykiem płynności a ryzykiem wyniku[52]. W skrajnych przypadkach niedostateczna płynność może prowadzić do niewypłacalności banku.

Ryzyko operacyjne odzwierciedla ryzyko techniczno-organizacyjne w systematyce Z. Zawadzkiej. Wiąże się z wadami mechanizmów kontroli wewnętrznej i zarządzania instytucją. Częstokroć jego źródłem są niewłaściwa procedura audytu i struktura organizacyjna. Na ryzyko operacyjne narażają bank nieetyczni lub niekompetentni pracownicy oraz nieostrożni i źle wykształceni przez bank klienci. Inne aspekty ryzyka operacyjnego wiążą się z uszkodzeniem systemów informatycznych banku, włamaniami do tego systemu lub wydarzeniami, takimi jak pożar czy klęski żywiołowe.

Ryzyko prawne przybiera rozmaitą postać. W przypadku nieprawidłowych porad prawnych pasywa banku mogą okazać się wyższe od zakładanych, zaś aktywa bez wartości. Wadliwie skonstruowane regulaminy lub umowy z klientami narażają bank na straty materialne, będące efektem wytoczonych i wygranych przez klientów spraw sądowych. Podobna sytuacja zachodzi, gdy na skutek niewystarczających zabezpieczeń dane klientów przechowywane przez bank zostaną skradzione i wykorzystane do innych celów. Banki muszą stale modyfikować regulaminy i być na bieżąco z wszelkimi nowelizacjami prawa. Ponadto te banki, które oferują swoje usługi za pośrednictwem Internetu, czy innych elektronicznych kanałów dystrybucji użytkownikom z innych państw, są zobligowane do uwzględnienia przepisów kraju goszczącego, niejednokrotnie inaczej traktujących rozmaite kwestie, np. ochronę klienta e-bankingu.

Ryzyko utraty reputacji może być następstwem nieprzestrzegania odpowiednich ustaw i przepisów, miernych zabezpieczeń systemu, niepomyślnie przeprowadzonych kampanii promocyjnych, złego podejścia do klientów, niesprawnie wykonanych operacji, itp. Bank jest przedsiębiorstwem zaufania publicznego. Jego opinia powinna być zatem nieposzlakowana, zaś dobro klienta stawiane zawsze na pierwszym miejscu.

Łatwo zauważyć, że poszczególne typy ryzyka są ściśle ze sobą powiązane. Jedna sytuacja może być źródłem kilku rodzajów ryzyka. Szczególnie wyraźnie widać to w bankowości elektronicznej, jeśli chodzi o ryzyko: operacyjne, prawne i reputacji. Na przykład bank, który nie udostępnił swoim klientom odpowiednich informacji dotyczących bezpiecznego użytkowania kart elektronicznych, naraża się zarówno na straty wynikające z ryzyka prawnego (niedopełnienie obowiązku publikacji instrukcji), ryzyka operacyjnego (transakcje przeprowadzone przez nieautoryzowanych użytkowników), jak i ryzyka utraty reputacji (postrzeganie banku jako instytucji nieprofesjonalnej).

W dalszej części pracy zostanie przedstawiona specyfika każdego rodzaju ryzyka bankowości elektronicznej.

Celem drugiego rozdziału było usystematyzowanie ryzyka bankowego i podanie definicji poszczególnych jego rodzajów właściwych bankowości elektronicznej.

Nie podlega dyskusji, że istnieje wiele klasyfikacji ryzyka bankowego. Są takie, które kładą nacisk na stopień kontroli ryzyka – czy bank ma nań wpływ, czy nie (podział na ryzyko systemowe i specyficzne), są też takie, które koncentrują się na zupełnie innym aspekcie, a mianowicie na zależnościach między poszczególnymi typami ryzyka (*vide* dynamiczny podział ryzyka finansowego wg prof. M. Górskiego). Za główną dla niniejszej pracy przyjęto klasyfikację Komitetu Bazylejskie-

[52] *Vide* podział dynamiczny ryzyka finansowego według prof. M. Górskiego.

go, która syntetyzuje wiele z innych podziałów ryzyka, a ze względu na swoją proweniencję wydaje się być najbardziej adekwatna do opisu specyfiki ryzyka bankowości elektronicznej i weryfikacji postawionych hipotez.

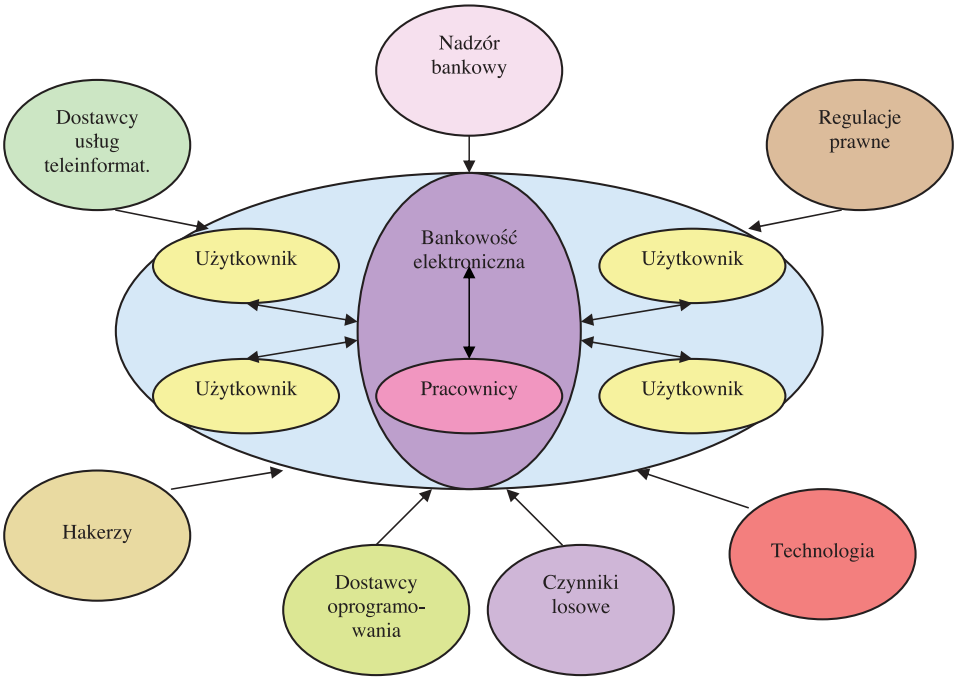
Przyjęta systematyka ryzyka bankowego nie różnicuje bankowości tradycyjnej i elektronicznej, nie wyróżniono w niej rodzajów ryzyka, które nie występowałyby w danym kanale dystrybucji. Natomiast zwrócono uwagę na wzajemne relacje między ryzykami i fakt, że jeden niepomyślny incydent może być źródłem wielu rodzajów ryzyka.

3
Rodzaje ryzyka e-bankingu

Specyfika bankowości elektronicznej polega między innymi na tym, że pewne ryzyka które są dla niej właściwe wymykają się kwantyfikacji. Istnieje możliwość pomiaru ryzyka kredytowego (*credit-rating*, *credit-scoring*, analiza dyskryminacyjna, itp.), czy stopy procentowej (metoda luki, analiza wrażliwości, metoda duracji, itp.). Natomiast pomiar różnych aspektów ryzyka operacyjnego, przykładowo takich jak: zawirusowanie informatycznego systemu bankowego, złamanie kodu szyfrującego (uznanego za nie do złamania), czy niezawodności sieci szkieletowej Internetu wykorzystywanej przez bank nastręcza poważnych trudności. Instytucja kredytowa może jednak starać się zminimalizować te ryzyka poprzez wykorzystanie najlepszych z dostępnych zabezpieczeń oraz awaryjnych procedur, które w przypadku usterki jednego elementu, pozwalają na bezproblemowe włączenie alternatywnego modułu. Dlatego, nawet mimo braku danych liczbowych, kierownictwo banku jest w stanie stworzyć wysoce odporny na zagrożenia system.

Przed rozpoczęciem dogłębnej analizy specyfiki ryzyka bankowości elektronicznej należy zidentyfikować czynniki i grupy interesariuszy wywierających wpływ na jej funkcjonowanie. Rysunek 1 przedstawia otoczenie e-bankingu.

Rysunek 1. Otoczenie bankowości elektronicznej



Źródło: opracowanie własne na podstawie: Dżega (2003).

Wszystkie elementy z rysunku niosą ze sobą ryzyko dla banku, choć dwa z nich: nadzór bankowy i regulacje prawne – w najmniejszym stopniu. Ich celem jest bowiem wyznaczenie odpowiednich ram działalności banków. Tym samym wpływają raczej na redukcję ryzyka niż jego wzrost, chyba że narzucane przez nie wymogi są błędne lub wieloznaczne.

Pozostałe czynniki i grupy interesariuszy stwarzają rozmaite ryzyka: operacyjne, prawne, reputacji, itp. Zwłaszcza te trzy wymienione zbiory ryzyk wydają się podatne na oddziaływanie oto-

czenia bankowości elektronicznej. Otoczenie pozostałych ryzyk jest podobne dla bankowości elektronicznej, jak i tradycyjnej. Dlatego rodzaje ryzyka, takie jak: kredytowe, płynności, kraju i transferu, rynkowe, stopy procentowej zmieniają się tylko o tyle, o ile wymaga tego charakter kanału elektronicznego (potencjalnie mogą to być duże zmiany).

Zważywszy na ten fakt, rozważania specyfiki ryzyka bankowości elektronicznej, będące *de facto* kontynuacją wątków z pierwszego i drugiego rozdziału, zostaną rozpoczęte od ryzyka: operacyjnego, prawnego i reputacji.

3.1. Rodzaje ryzyka: operacyjne, prawne oraz reputacji

W bankowości elektronicznej właśnie te rodzaje ryzyka wysuwają się na pierwszy plan. Powodem tego jest uzależnienie e-bankingu od technologii.

Według rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, bezpieczeństwo teleinformatyczne powinno być zapewnione przez:

- ochronę fizyczną, wydzielenie stref bezpieczeństwa w zależności od: klauzuli tajności informacji niejawnych, ilości tychże informacji, zagrożeń związanych z ujawnieniem, utratą bądź modyfikacją przez osoby nieuprawnione;
- instalację urządzeń zabezpieczających w pomieszczeniach chronionych przed nieuprawnionym dostępem, podglądem lub podsłuchem;
- ochronę elektromagnetyczną, umieszczenie urządzeń i połączeń w strefach bezpieczeństwa elektromagnetycznego lub ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych;
- ochronę kryptograficzną, szyfrowanie lub stosowanie innych mechanizmów kryptograficznych gwarantujących integralność[53] i zabezpieczenie przed nieuprawnionym dostępem przy przekazywaniu informacji poza strefy bezpieczeństwa;
- bezpieczeństwo transakcji;
- kontrolę dostępu do urządzeń systemu i sieci teleinformatycznej, dokonanie przydziału uprawnień użytkownikom.

Mając na uwadze powyższe rozporządzenie i otoczenie e-bankingu (rysunek 1), warto przyjrzeć się metodom identyfikacji klienta przez bank (sprawdzenie czy podana osoba łącząca się z systemem za pośrednictwem elektronicznego kanału dostępu jest tą za którą się podaje). W pierwszym rozdziale była już mowa o słabym i silnym uwierzytelnianiu. Do pierwszego zaliczono identyfikator i hasło PIN klienta, do drugiego kody TAN (*Transaction Authorisation Number*), tokeny, itp.

Token można określić jako urządzenie kryptograficzne generujące jednorazowe hasła, które stanowi alternatywę dla kodu TAN. Działa ono na zasadzie pytanie-odpowiedź, wyświetlanych w formie ciągu cyfr, który zmienia się na przykład co minutę[54]. Dana kombinacja cyfr jest ważna jedynie przez czas jej wyświetlania. Ciąg cyfr jest funkcją tajnego klucza zapisanego w urządzeniu oraz aktualnego czasu. Zegary tokena są zsynchronizowane z serwerem banku, poza tym każdy token jest dedykowany do jednego numeru rachunku.

[53] Integralność danych – właściwość polegająca na tym, że dane nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób. Integralność systemu – właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej. Definicje zaczerpnięto z: GINB (2002).

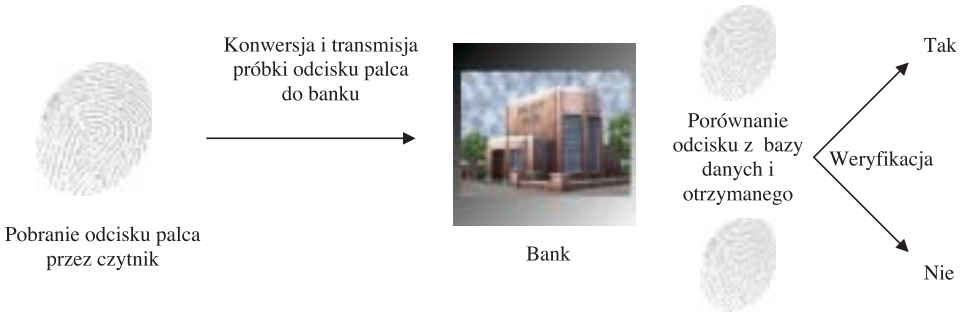
[54] Tak jest w banku internetowym Volkswagen B@nk Direct. Token generuje ciąg cyfr ważnych przez okres jednej minuty. Obok ciągu cyfr znajduje się pasek kresek, z których co dziesięć sekund jedna gaśnie, odmierzając w ten sposób upływ czasu ważności danego ciągu cyfr.

[55] Nowakowski, Toporowski, Tylski (2002).

Prócz powyższych sposobów uwierzytelniania istnieją jeszcze inne: biometryczna metoda identyfikacji oraz podpis elektroniczny (opisany dalej). Biometryczna metoda identyfikacji może polegać na rozpoznaniu głosu, tęczówki albo siatkówki oka, linii papilarnych palca, skanowaniu dłoni, podpisu, fotografii twarzy. Procedura zawsze przebiega tak samo:

- pobranie próbki cechy biometrycznej przez system;
- konwersja próbki do odpowiedniego formatu danych;
- transmisja próbki do systemu, który porównuje ją z danymi przechowywanymi w bazie;
- zwrot odpowiedzi przez system: tożsamość osoby, od której pobrano próbkę (lub też potwierdzenie podanej tożsamości lub odmowa dostępu)[55].

Rysunek 2. Przebieg autoryzacji na podstawie odcisku palca



Źródło: opracowanie własne.

Biometryczne metody autoryzacyjne, choć najbezpieczniejsze, wciąż są jeszcze za drogie, by banki mogły je wprowadzić do użytku na szerszą skalę. Tym niemniej kody TAN, tokeny oraz Infrastruktura Klucza Publicznego (PKI – *Public Key Infrastructure*) stanowią wystarczające zabezpieczenie. Niedostateczną ochroną jest natomiast autoryzacja tylko za pomocą identyfikatora i hasła. W jednym z polskich banków, który zapewnia dostęp do konta za pośrednictwem sieci, identyfikatorem jest numer karty kredytowej, zaś hasłem PIN do tej karty. Tak słabe zabezpieczenie nie chroni w wystarczający sposób klienta, a co za tym idzie samego banku, który może zostać narażony na straty materialne, prawne i reputacji. Ponadto należy zauważyć, że stosowanie wieloczynnikowego potwierdzenia tożsamości gwarantuje większą wiarygodność.

Autoryzacja podlega ryzyku manipulacji przez tzw. hakerów (dosłownie łamiących zabezpieczenia), którzy stosują w celu przejęcia kontroli nad danymi rozmaite techniki informatyczne. Posługują się między innymi snifferami (*sniff* z ang. wąchać), czyli analizatorami sieciowymi, służącymi do przechwytywania i analizy pakietów danych przesyłanych w sieci (np. haseł, kodów dostępu, itp.). Sniffing bardzo często stanowi preludium do spoofingu, czyli podszywania się pod inny komputer. Może ono polegać na zainstalowaniu odpowiedniego oprogramowania na własnym albo na obcym komputerze. Skutkuje to automatycznym przesyłaniem właściwych informacji z zainfekowanego komputera do hakera. Przestępcy sieciowi często wykorzystują w tym celu programy zwane końmi trojańskimi (trojanami). Taki program przechwytuje przykładowo ciągi znaków wprowadzanych na klawiaturę, po czym zapisuje je na dysku komputera lub przesyła pod wskazany adres poczty elektronicznej. Stosowane są także konie trojańskie, działające na zasadzie klient/serwer. Składają się one z programu dzięki któremu można niejako „wydawać polecenia", oraz „sługi" – zainstalowanemu na obcym komputerze programowi, wykonującemu te polecenia. Niekiedy trojany przybierają postać tzw. *back doorów* (z ang. tylne drzwi). Ta aplikacja, zainstalowana na serwerze, umożliwia hakerowi dostanie się do niego z ominięciem zabezpieczeń. Jest to bardzo często stosowana technika, za której pomocą haker może wielokrotnie powracać nawet na bardzo dobrze zabezpieczony serwer, nie włamując się ponownie od początku. Są też takie programy, nazywane exploitami, które wykorzystując dziury w systemach, mogą wpływać na ich działanie, np. zawieszając je lub nawet przejmując nad nimi kontrolę.[56]

[56] Opracowano na podstawie serwisu vaGla.pl *Prawo i Internet. Przestępczość w Internecie. Zagadnienia podstawowe* oraz Dżega (2003).

Przed hackingiem bank oraz klient mogą stosować różne zabezpieczenia. Dobrą metodą przeciw sniffingowi jest szyfrowanie danych. Moc szyfrowania zależy od długości klucza szyfrującego[57]. Praktycznie we wszystkich polskich bankach jest stosowana długość klucza albo 1024 bity dla szyfrowania asymetrycznego albo 128 bitów – dla symetrycznego. Kwestią jest tylko to, czy przeglądarka użytkownika obsługuje algorytmy kryptograficzne o takich długościach klucza (ostatnie wersje Internet Explorer i Netscape Communicator pokazują symbol kłódki z długością 128 bitów przy protokole SSL, oraz adres dla bezpiecznego połączenia zaczynający się od https: //, więc są bezpieczne).

Przed wirusami, końmi trojańskimi, itp. chronią odpowiednie pakiety oprogramowania. Ponadto banki powinny być świadome ryzyka ataków na swoje serwery typu DDoS (*Distributed Denial of Service*). Taki atak polega na jednoczesnym rozpoczęciu komunikacji z wielu serwerów z wybraną ofiarą i skutkuje zablokowaniem serwera z powodu sztucznie wywołanego ruchu. Klienci banku, do którego dostęp powinien być zapewniony przez 24 godziny na dobę i 7 dni w tygodniu niezależnie od okoliczności, nie mogą się z nim połączyć. System odmawia wykonania autoryzacji.

Zadaniem banków jest stworzenie takiego systemu, który zapewni transfer zintegrowanych danych, to znaczy takich, które po drodze nie zostały zmienione. System musi też pozwolić na niezaprzeczalne stwierdzenie z jakiego źródła informacje pochodzą, tak by klient nie mógł zanegować wykonanej przez siebie operacji, zaś w komunikacji odwrotnej, czyli bank? klient, ten drugi mógł być pewien, że otrzymał elektroniczną przesyłkę od banku, a nie od podmiotu, który się pod niego podszywa[58].

Słabym punktem bezpieczeństwa systemu bankowości elektronicznej jest czynnik ludzki. Problem hakerów został już omówiony, wiadomo jednak (patrz rysunek 1), że w otoczeniu e-bankingu są jeszcze użytkownicy, pracownicy, dostawcy oprogramowania oraz dostawcy usług telekomunikacyjnych.

Użytkownicy wymagają skrupulatnej edukacji ze strony banku, muszą być dokładnie instruowani jak reagować na odpowiednie incydenty, jak chronić bezpieczeństwa kart, dostępu z sieci do rachunku, danych potrzebnych do autoryzacji, jak zabezpieczyć komputer przed włamaniami, itd. Badania wykazują, że klienci banków są bardzo podatni na ataki z wykorzystaniem inżynierii socjalnej, polegającej na wykorzystaniu niewiedzy i naiwności ludzi celem uzyskania poufnych informacji (np. haseł, kodów dostępu). Hakerzy, podając się za pracowników banków, potrafią nawet zainstalować 'poprawki' na komputerze klienta (w istocie konie trojańskie). Warto także pamiętać, że edukacja klientów nabiera szerszego znaczenia przy transgranicznych usługach e-bankingu, gdzie potencjalni klienci z innego kraju mogą jedynie polegać na informacjach ze stron WWW, ponieważ bank jest po prostu nieobecny w innej formie (tradycyjnej – oddziałowej)[59].

Znaczne zagrożenie istnieje ze strony pracowników banków, administratorów sieci i dostawców technologii IT. Mogą oni posiadać dostęp do kluczowych zasobów banku lub mieć zbyt szerokie uprawnienia, co wystawia na próbę ich uczciwość (tzw. działanie oportunistyczne – oszustwo wynikające z przedłożenia korzyści własnych nad dobro instytucji[60]). W odpowiedzi na to zagrożenie kierownictwo banku musi określić odpowiedni podział obowiązków pracowników własnych lub powiązanych, ich kontrolę, a także właściwy audyt zewnętrzny (przeprowadzany okresowo). Konieczne są zabezpieczenia i procesy monitorowania dostępu zapobiegające wewnętrznemu i zewnętrznemu dostępowi do systemów aplikacji i baz danych bankowości elektronicznej. Łatwiejsze

[57] Im klucze są dłuższe, tym trudniej jest informacje odszyfrować. Powszechnie uważa się, że: 1. Dla kluczy asymetrycznych: 512 – to zbyt mało, 768 – stosunkowo bezpiecznie, 1024 – silne bezpieczeństwo (dane w bitach); 2. Dla kluczy symetrycznych: 40 – to zbyt mało, 56 – stosunkowo bezpiecznie, 128 – silne bezpieczeństwo (dane w bitach).

Łamanie kluczy metodą *brute force* (sprawdzanie po kolei możliwych kluczy) jest długotrwale: 1. Złamanie klucza 40 bitowego zajęło 3 godziny sieci komputerów; 2. Złamanie klucza 56 bitowego (w algorytmie RC5) zajęło 250 dni w ramach jednego z projektów distributed. net. Eksperyment został przeprowadzony przez sieć komputerów, których moc obliczeniowa była równoważna 26 tysiącom komputerów klasy Pentium 200; 3. Złamanie klucza 128 bitowego zajęłoby 1 bilion x 1 bilion lat (za pomocą pojedynczego superkomputera). Dane ze strony eBanki. pl.

[58] Najpopularniejszą techniką uniemożliwiającą negowanie dokonanych transakcji oraz zapewniającą poufność i rzetelność transakcji jest Infrastruktura Klucza Publicznego (PKI) opisana dalej.

[59] Wątek rozwinięty w punkcie Ryzyko a transgraniczny charakter bankowości elektronicznej.

[60] Definicja oportunizmu – *vide* Williamson (1998).

ukrycie, ewentualnie sfałszowania własnej tożsamości albo zbyt szerokie uprawnienia stanowią przesłankę do zachowania następujących zasad ostrożności:

- procesy i systemy transakcyjne powinny być zaprojektowane w taki sposób, żeby uniemożliwiły każdemu pojedynczemu pracownikowi/wynajętemu usługodawcy zainicjowanie, autoryzację i realizację transakcji. Każda decyzja powinna być zatwierdzana przez inną osobę (jeden pracownik inicjuje transakcję, inny ją autoryzuje, a jeszcze inny realizuje);
- należy zachować podział na osoby tworzące dane statyczne (np. treść stron internetowych) i osoby odpowiedzialne za rzetelność tych danych;
- systemy e-bankingu powinny być regularnie testowane w celu upewnienia się, że nie można obejść podziału obowiązków;
- należy zachować podział na konstruktorów i administratorów systemu bankowości elektronicznej[61].

Przy właściwym podziale obowiązków i dobrej kontroli, przestępstwo może zostać popełnione tylko w wyniku zmowy większej liczby osób.

Duże tempo zmian technologicznych zmusza bank do ciągłej aktualizacji systemu. W przeciwnym razie wzrasta zagrożenie ze strony jego słabej wydajności lub włamań zewnętrznych. Z drugiej strony istnieje również mozliwość, że częste implementacje nowych rozwiązań sprawią, iż pracownicy nie będą w pełni rozumieli ich natury, a to przełoży się na większe ryzyko operacyjne. Niestety same aktualizacje programów także pociągają za sobą pewne niebezpieczeństwo, bowiem hakerzy mogą przechwycić software i odpowiednio go zmodyfikować.

Ryzyko prawne e-bankingu, ściśle powiązane z pozostałymi pokrewnymi ryzykami, występuje przede wszystkim wówczas, gdy przepisy pierwotnie skonstruowane w odniesieniu do bankowości tradycyjnej, nie przystają do świata wirtualnego[62]. W takich sytuacjach bank musi brać pod uwagę regulacje mogące narazić sam bank lub jego klientów na niedogodności, czy nawet straty finansowe. Istnieją sytuacje, gdy co prawda nie ma bezpośredniego zagrożenia kondycji banku, lecz funkcjonuje on w swego rodzaju próżni prawnej[63].

Dzięki obecności w sieci bank zyskując dostęp do nowych rynków zbytu, równocześnie styka się z niebezpieczeństwem prania brudnych pieniędzy. Z powodu tego, że obrót pieniężny w e-bankingu ulega znacznemu przyspieszeniu, można dokonywać w krótkim czasie, z szeregu kont jednocześnie, wielu (nawet drobnych) przelewów na rozmaite rachunki. Aby nie narazić się na sankcje prawne wynikające z braku spełnienia tzw. wymogu „znaj swojego klienta" (*know your customer rule*), bank powinien wykształcić odpowiedni mechanizm rozpoznawania zagrożeń prania brudnych pieniędzy (wydajne metody uwierzytelniania, niskie limity doładowań elektronicznych portmonetek, ścieżki audytu, ciągły monitoring obrotu pieniężnego, itp.).

Klienci banku na skutek niepełnych lub mylących instrukcji i informacji zamieszczonych na stronach internetowych banków oraz w regulaminach, mogą błędnie pojmować swoje obowiązki lub nie być świadomi środków ostrożności, które należy zachować przy korzystaniu z danego kanału dostępu. To niebezpieczeństwo potęguje się, gdy bank zaczyna świadczyć usługi transgranicznie[64]. Klienci mogą w sytuacjach gdy ponieśli straty, wnosić oskarżenia przeciw bankowi.

Kolejną kwestią związaną z ryzykiem prawnym jest podstawowy obowiązek banku do zachowania poufnego charakteru danych o klientach. Ujawnienie ich nieupoważnionym stronom trzecim bez zgody klientów nie powinno się zdarzyć. Ponadto w ramach umów o outsourcingu, partnerzy

[61] Opracowano na podstawie: Komitet Bazylejski (maj 2001, lipiec 2003).

[62] Opracowano na podstawie: Basel Committee for Banking Supervision (październik 2000).

[63] Tak było np. przed wejściem w życie 16 sierpnia 2002 r. Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, kiedy banki miały już odpowiednią infrastrukturę i możliwości korzystania z dobrodziejstw podpisu elektronicznego, jednak do momentu wejścia w życie ustawy nie miał on mocy prawnej.

[64] *Vide* punkt: Ryzyko a transgraniczny charakter bankowości elektronicznej.

banku również muszą przestrzegać polityki ochrony danych, w przeciwnym razie to bank jest narażony na skutki oskarżeń o złamanie klauzuli poufności.

Ryzyko utraty reputacji pojawia się przy wszystkich opisanych powyżej aspektach ryzyka prawnego, a także przy zagrożeniach operacyjnych.

Reputacja banku może ucierpieć, gdy dostęp klientów do ich środków zostanie ograniczony na przykład na skutek nadmiernego ruchu sieciowego na serwerze banku, ataku typu DDoS albo innych awarii systemu. Podobnie dzieje się, gdy bank nie odpowiada na zapytania słane mu przez klientów, nie upublicznia ważnych informacji, dostarcza niepełne instrukcje i regulaminy.

Poważnym zagrożeniem reputacji banku jest także ujawnienie lub przedostanie się danych o klientach spowodowane własnym błędem lub błędem partnera, na rzecz którego bank scedował (wyoutsourcował) część działalności. Klienci mogą również poczuć się nieufni wobec nadsyłanych przez bank wiadomości zawierających hyperlinki do partnerów banku, jeśli nie są pewni w jakich relacjach z bankiem owi partnerzy się znajdują.

Wszelkie problemy związane z wydajnością i bezpieczeństwem systemu, szybkością realizacji transakcji oraz precyzyjnym wykonywaniem poleceń klientów grożą utratą reputacji i dobrego imienia banku.

Służby bankowe muszą kompleksowo traktować ryzyko e-bankingu w związku z imperatywem sprawnego świadczenia usług i ciągłości działania. Główne zagrożenie tkwi w tym, że duża część usług dostarczanych przez kanał elektroniczny (np. Internet, WAP, home banking) znajduje się poza kontrolą banku. Ten stan rzeczy jest widoczny tym bardziej, im mocniej bank odczuwa presję konkurencji oraz im gwałtowniej postęp technologiczny zmusza bank do zlecania na zewnątrz wielu funkcji, co prowadzi do uzależnienia go od stron trzecich[65]. Zadanie banku sprowadza się do zaprojektowania niezawodnego systemu z wysoce zawodnych elementów. Biorąc więc pod uwagę szereg rodzajów ryzyka (np. ataki hakerów, usterki sieci telekomunikacyjnej, oportunizm własnych pracowników, nagły wzrost popytu na transakcje w godzinach szczytu), bank musi zapewnić swoim klientom ciągłe i bezpieczne świadczenie usług drogą elektroniczną. Może to czynić przy pomocy:

- bieżącego pomiaru pojemności systemu bankowości elektronicznej i projekcji popytu, która umożliwi podjęcie decyzji o ewentualnej rozbudowie systemu;
- testowania awaryjnego systemu na wypadek ataków i oszacowania zdolności przetwarzania transakcji i wydajności systemu w przypadkach wystąpienia rozmaitych usterek i zagrożeń;
- różnych scenariuszy planów awaryjnych oraz planów niezwłocznego reagowania na incydenty;
- tworzenia kopii zapasowych danych (tzw. backupów);
- zapisywania wszelkich zdarzeń, operacji i incydentów;
- sprawnego powiadomienia władz nadzorczych w przypadku naruszenia bezpieczeństwa lub zakłóceń działalności w celu uzyskania wsparcia;
- właściwej komunikacji z rynkiem zewnętrznym, klientami i mediami, gdy wystąpią kłopoty[66].

3.2. *Outsourcing*

Ostatnio banki nasiliły współpracę z rozmaitymi firmami, zawierając z nimi umowy o outsourcing bądź wchodząc w alianse strategiczne. W praktyce obie formy kooperacji sprowadzają się do znacznego uzależnienia banku od partnera. Za outsourcing uważa się długoterminowe zlecenie na wyłączność realizacji pewnych funkcji lub procesów dotąd wykonywanych przez pracowników

[65] Szerzej w punkcie tego rozdziału poświęconym outsourcingowi.

[66] Jest to przykładowa, niewyczerpująca tematu lista reakcji na zagrożenia e-bankingu.

danego przedsiębiorstwa firmie zewnętrznej specjalizującej się w danej dziedzinie[67]. Banki najczęściej decydują się na outsourcing usług IT, w których postęp technologiczny jest tak szybki, że nawet dużym instytucjom spoza branży informatycznej jest niezwykle trudno pozostawać na bieżąco z najnowszymi osiągnięciami i rozwiązaniami. Do tego typu outsourcingu bankowego należy zlecanie firmom zewnętrznym obsługi call centre lub instalacji i serwisu u klienta oprogramowania typu home banking[68].

Outsourcing działa dwukierunkowo – pewne typy ryzyka zwiększa, inne zmniejsza. Paradoksalnie, jak się okazuje, może zwiększać i zmniejszać również te same rodzaje ryzyka np. operacyjne, prawne i reputacji. Z jednej strony bowiem uzależnia bank od strony trzeciej, za której działania ponosi odpowiedzialność, z drugiej zaś bank może scedować stworzenie infrastruktury zapasowej i planu awaryjnego na rzecz partnera, który w przypadku uszkodzenia systemu macierzystego banku, przejmuje na siebie ciężar obsługi klientów, udostępniając bankowi np. swoje serwery, pomieszczenia i zasoby przygotowane specjalnie na ten cel.

Warto wyjaśnić szerzej na czym polega to rozwiązanie na przykładzie firmy Hewlett Packard (HP). Oferuje ona możliwość tzw. disaster recovery, czyli zapewnienie środowiska zapasowego po awarii systemu. Dzięki temu, że usługa jest udostępniana wielu podmiotom, HP zyskuje korzyści skali, natomiast bank, który zdecydował się na outsourcing, ponosi mniejsze koszty i jednocześnie jest obsługiwany przez wysoce wyspecjalizowaną jednostkę. HP zmniejsza prawdopodobieństwo wystąpienia katastrofy u kilku klientów równocześnie, poprzez odpowiedni ich dobór. Dokłada starań, by systemy klientów nie były ze sobą powiązane, a użytkowane sieci – fizycznie wystarczająco od siebie oddalone. W Polsce między innymi WestLB Bank Polska SA zlecił utworzenie infrastruktury zapasowej i działań awaryjnych HP Polska. Nabył sobie tym samym prawo do robienia niezapowiedzianych testów, z czego skwapliwie korzysta. W ich wyniku system HP staje się coraz bardziej niezawodny, gdyż po każdej kontroli eliminowane są kolejne usterki[69].

Abstrahując od powyższego przykładu, dla banku outsourcing pociąga za sobą ryzyko prawne i reputacji. Umowy z firmą outsourcingową muszą precyzyjnie określać zakres jej obowiązków i sankcje przewidziane w wyniku nieprawidłowego zachowania. Jednak nawet najbardziej dotkliwe kary nałożone na nieuczciwego partnera nie uchronią banku przed utratą reputacji na rynku. W pewnych zaś sytuacjach cele partnera, zwykle identyczne z celami banku, mogą stać się rozbieżne.

Mimo zagrożeń zarządy banków decydują się na outsourcing, ponieważ zyskują znaczną redukcję kosztów[70], możliwość koncentracji na kluczowych obszarach działania, wzrost wydajności i stabilności środowiska banku (dzięki standaryzacji procedur i procesów) oraz możliwość wykorzystania outsourcingu jako metody na reorganizację przedsiębiorstwa. W bankowości elektronicznej wyróżnia się wiele modeli outsourcingu. Mają one z reguły charakter mniej lub bardziej informatyczny. Pierwszy model tradycyjnie polega na wykorzystaniu mocy obliczeniowej sprzętu instytucji zewnętrznej. Natomiast drugi dotyczy świadczenia usług związanych z konkretnym procesem biznesowym. Do niego zalicza się, między innymi, outsourcing usług typu helpdesk i hotline albo zlecenie firmom zewnętrznym dokonywania wydruków masowych.

Biorąc pod uwagę to, kto jest właścicielem sprzętu i serwerów oraz kto użycza miejsce do świadczenia usług, outsourcing dzielimy na kolokacyjny i hostingowy. Kolokacja występuje wówczas, gdy bank udostępnia usługodawcy własne komputery, zaś ten oferuje profesjonalnie wyposażone centrum przetwarzania danych oraz nadzór i obsługę. Hosting jest w pewnym sensie odwrotnością kolokacji, gdyż w tym przypadku outsourcer udostępnia bankowi swoje zasoby na przykład za pośrednictwem Internetu lub stałego łącza, tak że bank nie musi posiadać własnych serwerów. Niektóre firmy outsourcingowe oferują dodatkowo (gdy wykorzystywany jest hosting) możliwość zdalnego zarządzania danymi i aplikacjami oraz automatyczne przesyłanie danych na serwer ze sta-

[67] Definicja zaczerpnięta z artykułu Zielińska (2004): Kupowanie mocy obliczeniowej.

[68] Wątek kosztów i ryzyka outsourcingu usług typu home banking na przykładzie systemu MultiCash został szerzej potraktowany w pracy: Górka, Markowski (2004).

[69] Przykład z artykułu Marzec (2003): Gotowi na wszystko.

[70] Zielińska (2004): 'Dzięki outsourcingowi informatyki przedsiębiorstwo może ograniczyć bieżące wydatki na nią o 20-30 procent oraz wykorzystać dostawców usług do współfinansowania inwestycji w tym obszarze'.

cji roboczych klienta (*uploading*), co pozwala utrzymać synchronizację bazy danych. Nadzór bankowy zaleca, żeby w przypadku hostingu pracownicy firmy outsourcingowej nie mieli dostępu do danych klientów banku. Administrowanie tymi danymi powinno pozostać w gestii pracowników banku. Takie rozwiązanie wydatnie zmniejsza ryzyko.

Ciekawym przykładem outsourcingu na polskim rynku i-bankingu jest mBank, który zlecił obsługę całego procesu biznesowego. Powierzył on mianowicie zewnętrznym konsultantom biznesowym i firmie informatycznej projektowanie i bieżącą kontrolę witryny internetowej oraz opracowywanie wyglądu i produkcję kart magnetycznych. Nad pracą tego zespołu pieczę trzyma menedżer mBanku.

Konkurencyjne Inteligo jest ściśle powiązane z HP[71], świadczącym na jego rzecz usługi w zakresie integracji systemów informatycznych oraz dostarczania sprzętu i oprogramowania obsługującego centralny system informatyczny.

Warto jeszcze raz podkreślić, że wszelkie błędy partnera obciążają bank. Gdy klient ma kłopoty z wypłatą gotówki z bankomatu autoryzowanego przez bank, to choć należy on do firmy – partnera banku, ten ostatni ponosi odpowiedzialność[72].

O wadze outsourcingu i towarzyszących mu rodzajach ryzyka świadczą kwoty przeznaczonych na niego wydatków i liczba operacji. Poniższa tabela zawiera zestawienie oficjalnie ogłoszonych kontraktów na outsourcing IT w sektorze usług finansowych w ostatnich latach.

Tabela 2. Zestawienie oficjalnie ogłoszonych kontraktów na outsourcing IT w sektorze usług finansowych

Klient	Dostawca	Data ogłoszenia lub rozpoczęcia	Okres	Wartość (USD)	Główny przedmiot, uwagi
American Express	IBM	luty 2002	7 lat	4 mld	Utrzymanie światowej sieci systemów komputerowych i witryn internetowych. Oferta przejęcia 2000 pracowników.
Deutsche Bank	IBM	grudzień 2002	10 lat	2,5 mld	Przejęcie ośrodków danych, pojedynczych serwerów oraz komunikacji satelitarnej z lokalizacji europejskich. Nowy ośrodek danych w regionie Ren-Men. Zapłata tylko za czas użycia serwerów i mainframe, aplikacji i helpdesku (e-business on demand). Przejęcie 900 pracowników. Integracja głównych procesów biznesowych i systemów w środowisku otwartym dla sprzętu i oprogramowania, w tym konsolidacja, centralizacja i wirtualizacja serwerów. Zastosowanie rozwiązań dla samozarządzania i samonaprawy opartych na przetwarzaniu autonomicznym.
Bank of America	EDS	grudzień 2002	10 lat	4,5 mld	Zarządzanie sieciami telekomunikacyjnymi.
JPMorgan Chase	IBM	grudzień 2002	7 lat	5 mld	Operacje mainframe, ośrodków danych, help desków, przetwarzania rozproszonego, sieci transmisji danych i głosu. Zatrzymanie przez bank własnych specjalistów do utrzymania komputerów osobistych i technologii handlu (aplikacji dedykowanych ECN i Tibco/Triarch. Przejęcie około 4000 pracownków, pozostawienie około 2500.
ABN Amro	EDS	luty 2003	5 lat	1,3 mld	Usługi technologiczne, utrzymanie komputerów osobistych, sieci i technologii ośrodka danych oraz rozwój większości aplikacji dla Wholesale Client Strategic (WCS) Business Unit.

Źródło: opracowanie własne na podstawie Góralczyk (2003).

[71] Compaq stanowi po fuzji część HP.

[72] W Polsce coraz częściej banki nie utrzymują swoich bankomatów, tylko korzystają z wyspecjalizowanych sieci, takich jak Euronet. Z Euronetem współpracuje między innymi Inteligo.

3.3. Rzeczywiste ataki na e-banki jako przykład ryzyka: operacyjnego, prawnego i reputacji

W środę 28 stycznia 2004 r. w Polsce miał miejsce atak na kanał internetowy Citibanku Handlowy[73]. Część posiadaczy kont osobistych dostała e-mailem informację o uruchomieniu nowego systemu transakcji internetowych. Proszono w nim klientów o jak najszybsze zalogowanie się oraz sprawdzenie jego możliwości. W wiadomości znajdował się link www.online.citibank.pl (prawdziwy adres strony banku). Dla niepoznaki hakerzy dołączyli prośbę, by klienci przysyłali opinie o „nowym systemie".

Osoby, które kliknęły na wskazany link, były automatycznie kierowane na zupełnie inną stronę WWW, wyglądem do złudzenia przypominającą witrynę Citibanku. Hakerzy wykorzystali dziurę w zabezpieczeniach przeglądarki Internet Explorer Microsoftu, sprawiając że w pasku adresu cały czas wyświetlał się oryginalny adres strony Citibanku[74]. W konsekwencji klienci mogli poznać że są na nieprawdziwej stronie banku, tylko po braku w prawym dolnym rogu przeglądarki symbolu kłódki znamionującej połączenie szyfrowane. Ofiara po podaniu identyfikatora (numer karty kredytowej) i hasła (kod PIN do karty) zostawała automatycznie wyrzucana przez system ze sfałszowanej strony, zaś złodzieje mieli otwartą drogę do konta i jednocześnie do karty kredytowej klienta[75].

Podobny atak w Polsce został przeprowadzony w połowie 2003 r. na mBank. Hakerzy skopiowali jego stronę internetową i umieścili pod innym adresem. Jednakże klienci mogli wówczas zauważyć, że zostali skierowani w podejrzane miejsce, gdyż przeglądarka wyświetlała zmieniony adres.

Warto zauważyć, że istnienie dodatkowych zabezpieczeń w postaci karty haseł jednorazowych, tokena lub klucza prywatnego w przypadku opisanego powyżej ataku nie czyni szkód materialnych (pod warunkiem, że identyfikatorem do konta nie jest numer karty kredytowej klienta, zaś hasłem PIN do niej). Pomijając zatem utratę reputacji, bank nie ponosi bezpośrednio strat pieniężnych.

Okazuje się, że Polska nie była jedynym ani pierwszym krajem, w którym usiłowano wyłudzić od klientów dane umożliwiające dostęp do ich kont w sposób analogiczny do przypadku Citibanku. Ataki tego typu były podejmowane od września 2003 r., między innymi na banki: Barclays i Lloyd[76]. Doczekały się już nawet swojej nazwy: *phishing* (od ang. *fishing*), która wzięła się stąd, że oszuści działają tak jakby zarzucali sieci i czekali aż ktoś się w nie złapie. Według nieoficjalnych szacunków na hakerską przynętę łapie się około 5 procent osób, do których zostały wysłane listy. W tabeli 11 umieszczono kolejne przypadki ataków na e-banki lub/i rażącego niedbalstwa z ich strony w ostatnim czasie.

Tabela 3. Wybrane ataki na e-banki lub/i przypadki rażącego zaniedbania z ich strony

Data	Opis
Sierpień 2003	Omyłkowe umieszczenie w ogólnodostępnym serwisie internetowym adresów emailowych ponad 3 tys. klientów Bank West.
Lipiec 2003	'Wypompowanie' znacznej sumy pieniędzy przez wykorzystanie konia trojańskiego dołączonego do poczty elektronicznej adresowanej do klientów południowoafrykańskiego Absa Bank.
Lipiec 2003	Atak na program kontroli kart Visa, polegający na kradzieży numerów kart kredytowych, dotknął przede wszystkim klientów amerykańskiego Kearney Bank. Hakera szybko zlokalizowano, ale bank musiał ponieść koszty emisji nowych kart.

[73] Przykład opracowano na podstawie artykułu Samcik (2004): Internetowi złodzieje podrobili stronę banku oraz zasobów http: //www. mozillapl. org/forum/sutra32080. html.

[74] Podobno Microsoft wydał już „łatkę" na ten błąd w przeglądarce Internet Explorer.

[75] *Vide* uwaga na stronie 33 tego rozdziału o ryzyku niewystarczającego zabezpieczenia dostępu do e-konta.

[76] Włodarczyk (2004).

Luty 2003	Wykorzystanie luki w systemie zabezpieczeń przez nowojorskiego hakera i zdobycie dostępu do ponad 5 mln. transakcji przeprowadzonych kartami Visa i Maestro. Zagrożone zostały środki ponad 8 tys. klientów amerykańskiego Northeast Bank.
Styczeń 2002	Włamanie do bazy danych klientów amerykańskiej firmy specjalizującej się w sprzedaży usług bankowych Online Resources Corporation i jej częściowe opublikowanie w Internecie.
Lipiec 2001	Włamanie do systemu zabezpieczeń internetowego oddziału Commonwealth Bank Australia – Quickline Australia, zdobycie identyfikatorów i haseł klientów celem kradzieży środków zgromadzonych na rachunkach bankowych.
Styczeń 2001	Umieszczenie fałszywej kopii strony polskiego banku PBK na serwerze amerykańskim celem gromadzenia informacji o kartach kredytowych.
Wrzesień 2000	Włamanie do serwisu internetowego holenderskiego ABN Amro i przelanie depozytów klientów na konta hakerów, po uprzednim zgłoszeniu luk w systemie zabezpieczeń banku oraz instalacji konia trojańskiego na komputerach klientów.
Sierpień 2000	Włamanie do największego brytyjskiego banku internetowego Egg. com Łupem padło kilkanaście tysięcy funtów.

Źródło: opracowanie własne na podstawie: Dżega (2003).

3.4. Podpis elektroniczny i Infrastruktura Klucza Publicznego

Podpis elektroniczny w połączeniu z Infrastrukturą Klucza Publicznego (znaną pod akronimem PKI – *Public Key Infrastructure*) jest najbardziej zaawansowanym technologicznie i prawnie rozwiązaniem ograniczającym ryzyka: operacyjne, prawne i reputacji bankowości elektronicznej. Stanowi idealne dopełnienie innych metod uwierzytelniania klientów. Ponadto pozwala na przeniesienie z formy papierowej na elektroniczną wielu dokumentów niezbędnych do właściwego funkcjonowania podmiotów w obrocie gospodarczym. Nie oznacza to naturalnie, że rozwiązanie to nie jest pozbawione wad i nie stwarza ryzyka. Jednakże na obecnym etapie rozwoju technologicznego podpis elektroniczny wraz z towarzyszącymi mu metodami kryptograficznymi i kluczami szyfrującymi wydaje się być wystarczająco bezpieczny.

Zastosowanie Infrastruktury Klucza Publicznego i podpisu elektronicznego w bankowości elektronicznej spełnia następujące wymagania (zwane w literaturze „czterema filarami zaufania"):

- zapewnia identyfikację użytkownika w komunikacji za pośrednictwem Internetu,
- zapewnia poufność transakcji (dane są szyfrowane na drodze bank → klient i odwrotnie),
- zapewnia integralność danych transmitowanych w sieci (wszelkie zmiany w podpisanej transakcji są rozpoznawalne),
- zapewnia wiarygodność użytkownika (brak możliwości podszywania się innych pod określoną osobę) oraz niezaprzeczalność transakcji (brak możliwości wyparcia się złożonego przez autora podpisu)[77].

PKI i podpis cyfrowy zastępują w e-bankingu rzeczywistą kontrolę dokumentów, weryfikację podpisu odręcznego, czy nawet osobistą znajomość z pracownikami banku.

Zgodnie z zapisami w Polskiej Normie (PN-I-02000) podpisem elektronicznym jest przekształcanie kryptograficzne danych umożliwiające odbiorcy danych sprawdzenie ich autentyczności i in-

[77] Opracowano na podstawie: Szyszka (red.) (2003) oraz Nowakowski, Toporowski, Tylski (2002).

tegralności oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę. W myśl Ustawy z 18 września 2001 r. o podpisie elektronicznym istnieją dwa rodzaje podpisów: zwykły i bezpieczny. Zwykły podpis elektroniczny jest wiązką danych w postaci elektronicznej, która wraz z innymi danymi, do których została dołączona lub z którymi jest logicznie powiązana, służy do identyfikacji osoby składającej podpis elektroniczny (art. 3 ust. 1 ustawy). Bezpieczny podpis elektroniczny musi natomiast spełniać trzy warunki (art. 3 ust. 2 ustawy):

- być przyporządkowany wyłącznie do osoby składającej ten podpis,
- być sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
- być powiązany z danymi, do których został dołączony, w taki sposób, żeby jakakolwiek późniejsza zmiana tych danych była rozpoznawalna[78].

Podstawą PKI są klucze kryptograficzne (prywatny i publiczny) certyfikowane przez specjalne instytucje (o czym dalej w tym punkcie).

Podpis elektroniczny jest tworzony przy użyciu asymetrycznych algorytmów kryptograficznych, czyli wspomnianej pary kluczy. W przeciwieństwie zatem do tradycyjnego szyfrowania, utajnionej wiadomości nie da się odczytać przy użyciu jednego klucza. Do jej odczytania konieczny jest bowiem drugi klucz, korespondujący z pierwszym. Klucz publiczny użytkownika jest jawny i powszechnie znany, natomiast klucz prywatny musi być utrzymywany w sekrecie (ten kto by wszedł w jego posiadanie, mógłby z łatwością podszywać się pod właściciela). Znając klucz publiczny nie można poznać klucza prywatnego (jest to teoretycznie możliwe, lecz przy współczesnym stanie wiedzy niewykonalne obliczeniowo). W najczęściej używanym do szyfrowania asymetrycznego algorytmie RSA klucz prywatny składa się z dwóch dużych liczb pierwszych, zaś klucz publiczny jest ich iloczynem. Metoda złamania szyfru – czyli odtworzenia klucza prywatnego na podstawie klucza publicznego – wydaje się zatem teoretycznie prosta: należy tę liczbę rozłożyć na czynniki pierwsze. Szyfr jest jednak bezpieczny, ponieważ przy użyciu wszystkich aktualnie znanych metod matematycznych operacja rozkładu tak dużej liczby na czynniki pierwsze trwa nad wyraz długo[79].

Klient banku posiada parę kluczy: prywatny i publiczny. Klucz publiczny udostępniany jest bankowi, dzięki czemu ten może odszyfrowywać otrzymywane od klienta przesyłki (podpisane dokumenty, płatności, zlecenia, itp.). Bank również posiada swój zestaw kluczy, z których publiczny przekazuje do wiadomości klienta. Jeżeli zatem klient chce przesłać do banku wysoce bezpieczną przesyłkę, wówczas powinna ona zostać zaszyfrowana dwukrotnie: raz z wykorzystaniem klucza prywatnego klienta, drugi z wykorzystaniem klucza publicznego banku. Ten natomiast może ją rozszyfrować przy użyciu własnego klucza prywatnego oraz klucza publicznego klienta[80]. Należy silnie zaakcentować, że tylko podwójne szyfrowanie zapewnia poufność danych. Bowiem szyfrowanie przez klienta tylko jego kluczem prywatnym sprawia, że haker, który przejmie wiadomość, może ją łatwo odczytać przy pomocy jawnego klucza publicznego klienta. Co prawda bank będzie mógł sprawdzić w trakcie procesu weryfikacji wiadomości, że została ona zmieniona już po podpisaniu jej przez klienta. Jednak w tej sytuacji nie zostanie zachowany jeden z tzw. czterech filarów zaufania, to znaczy poufność transakcji (wątek rozwinięty poniżej).

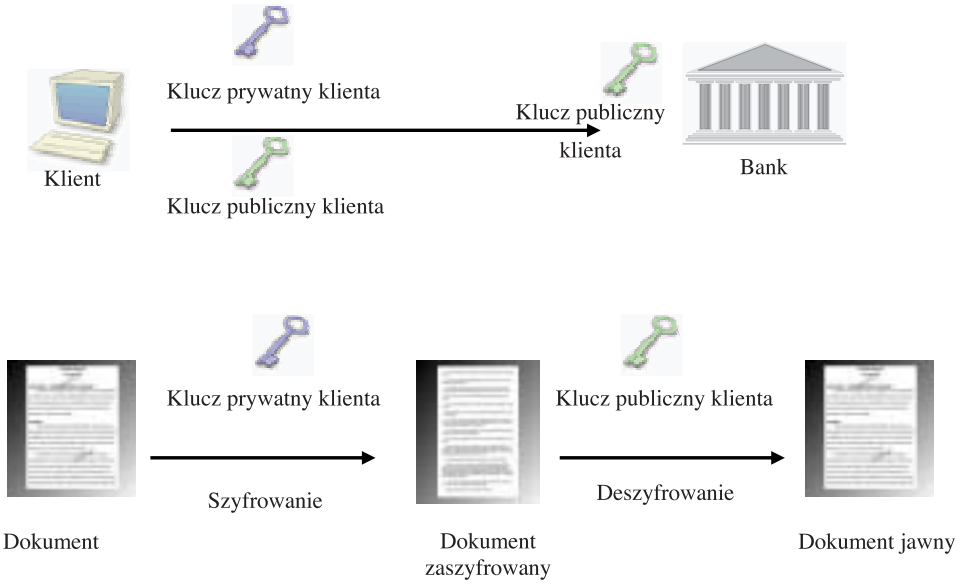
Zasadę działania systemu zabezpieczeń opartego na Infrastrukturze Klucza Publicznego z pojedynczym szyfrowaniem przy użyciu pary kluczy klienta banku przedstawia schemat 1.

78 Wysoki poziom komplikacji definicji ustawowych podpisu elektronicznego czyni je mało czytelnymi.

79 *Vide* długość klucza i czas jego łamania metodą *brute force* – przypis 57.

80 Łysakowski (2000).

Schemat 1. Zasada działania systemu zabezpieczeń opartego na Infrastrukturze Klucza Publicznego z pojedynczym szyfrowaniem przy użyciu pary kluczy klienta banku



Źródło: opracowanie własne.

Generowanie podpisu elektronicznego przez klienta oraz weryfikacja tego podpisu przez bank, prócz par kluczy kryptograficznych, wykorzystuje również algorytm funkcji hashującej[81]. Cały proces dopiero zapewnia, że zostaną zachowane autentyczność, integralność, niezaprzeczalność oraz poufność przesłanych danych. Pełna procedura odbywa się w sposób opisany poniżej i jest zaprezentowana na schemacie 2.

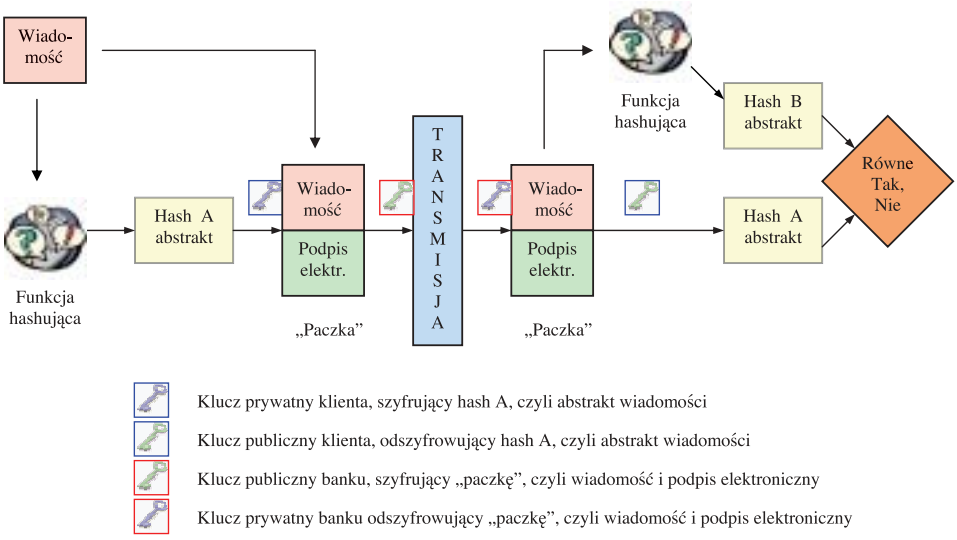
Klient banku przesyła wiadomość w dwóch formatach: jako wartość funkcji hashującej odpowiadającą komunikatowi, zaszyfrowaną jego kluczem prywatnym (łącznie podpis elektroniczny) oraz jako zwykły tekst. Powstała w ten sposób 'paczka' jest szyfrowana kluczem publicznym odbiorcy (banku). Dzięki temu również zwykły tekst w trakcie transportu elektronicznego do banku jest zaszyfrowany. Odbiorca deszyfruje otrzymaną 'paczkę' swoim kluczem prywatnym. Tekst wiadomości jest argumentem funkcji hashującej, na podstawie którego bank generuje hash B (abstrakt wiadomości). Hash B bank porównuje z hashem A, czyli wartością funkcji hashującej, zdeszyfrowaną kluczem publicznym nadawcy (klienta). Jeżeli obie wartości funkcji hash są sobie równe, to oznacza, że tekst wiadomości nie został zmieniony, podpis elektroniczny jest prawidłowy, a operacja może być wykonana. Algorytm hashujący zapewnia, że wszelkie dokonane modyfikacje w danych transakcji zostaną wykryte. Zaszyfrowane wiadomości hash uniemożliwiają zmiany w danych transakcji i odpowiednie jednoczesne do tych zmian podrobienie podpisu elektronicznego. Tym samym nawet jeżeli komuś udałoby się poznać klucz prywatny klienta i zmienić wiadomość, to bank będzie o tym wiedział.

Warto zaznaczyć, że np. opisany w pierwszym rozdziale protokół SSL wykorzystuje zabezpieczenia podobne do podpisu elektronicznego[82].

[81] Funkcja hashująca jest to tzw. funkcja mieszająca, która operuje na ciągu liter, przyporządkowując im pewną wartość – albo liczbową albo literową. Wartość ta jest z definicji krótsza niż ciąg znaków, który jest argumentem funkcji. Funkcja hashująca tworzy zatem swoisty abstrakt (skrót) wiadomości.

[82] Podobnie czynią to inne protokoły, jak np.: SET (*Secure Electronic Transaction*), czy PGP (*Pretty Good Privacy*).

Schemat 2. Generowanie oraz weryfikacja podpisu elektronicznego



Źródło: opracowanie własne.

Podpis elektroniczny w rzeczywistości jest plikiem chronionym hasłem, który może być przechowywany:

- na dysku twardym komputera,
- na nośniku danych, takim jak: dyskietka, CD-ROM, czy chip pod USB,
- w telefonie komórkowym,
- w karcie chipowej, komunikującej się z komputerem za pomocą specjalnego terminala.

Plik zawiera dane pozwalające ustalić tożsamość podpisującego oraz, czasami, informacje dodatkowe – czy nadawca występuje w imieniu własnym, czy innej osoby fizycznej, prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Do weryfikacji podpisów elektronicznych służą certyfikaty, a więc elektroniczne zaświadczenia potwierdzające przynależność danych osoby podpisującej do elektronicznego podpisu. Jak zostało udowodnione powyżej, gdy wiadomość daje się odszyfrować kluczem publicznym danej osoby, to znaczy że jej autorem jest faktycznie ta osoba. Jednakże nie ma pewności co do jej tożsamości. Osoba ta może być bowiem nie tym za kogo się podaje. Rozwiązaniem problemu weryfikacji autentyczności kluczy jest ich certyfikowanie. Certyfikowanie klucza polega na dołączeniu do niego informacji o tożsamości właściciela klucza i elektronicznym podpisaniu tak utworzonego dokumentu (certyfikatu) własnym kluczem prywatnym przez tzw. zaufaną trzecią stronę (*trusted third party*, TTP), która tym samym potwierdza tożsamość osoby, do której należy klucz[83].

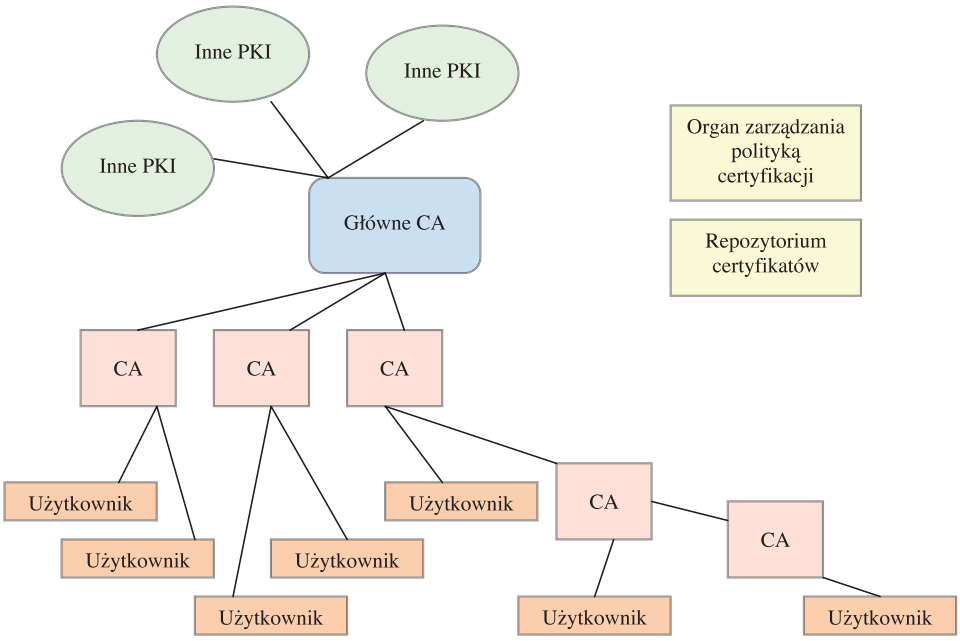
Zaufaną stroną trzecią jest urząd certyfikacyjny (*certification authority*, CA). Może to być bądź urząd państwowy, bądź firma komercyjna, której wiarygodność została w odpowiedni sposób potwierdzona. Urzędy certyfikacyjne tworzą hierarchię zwaną Infrastrukturą Klucza Publicznego (rysunek 14). Na jej szczycie stoi główny urząd certyfikacyjny (*root* CA)[84] stanowiący podstawę całego systemu. Główny urząd certyfikacyjny nie wystawia bezpośrednio certyfikatów żadnym użytkownikom końcowym, lecz jedynie certyfikuje klucze urzędów niższego szczebla, a dopiero te obsługują użytkowników. Hierarchia ta może być jeszcze bardziej rozbudowana, gdyż pomiędzy głównym CA, a końcowym użytkownikiem może znajdować się kilka szczebli urzędów certyfikacyjnych, które ko-

[83] Cwynar (2003).

[84] W Polsce jest nim od 22 sierpnia 2005 r. Narodowy Bank Polski, działający za pośrednictwem Narodowego Centrum Certyfikacji. NBP przejął kompetencje nadrzędnego urzędu certyfikacji od Centrum Zaufania i Certyfikacji Centrast. Od 1 października 2005 r. NBP prowadzi również rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Na rynku polskim cztery firmy mają prawo wydawać certyfikaty kwalifikowane: Unizeto Sp. z o. o., Sigillum PCCE (Polska Wytwórnia Papierów Wartościowych), TP Internet SA oraz Krajowa Izba Rozliczeniowa.

lejno certyfikują swoje klucze. Rozproszenie funkcji certyfikacyjnych ma na celu ograniczenie negatywnych skutków ujawnienia klucza prywatnego konkrentego CA[85]. Tym niemniej, bezpieczeństwo całego systemu zależy de facto od bezpieczeństwa klucza prywatnego głównego CA – jego ujawnienie poddaje bowiem w wątpliwość wiarygodność wszystkich podpisów elektronicznych.

Rysunek 3. Modelowe środowisko Infrastruktury Klucza Publicznego (PKI)



Źródło: opracowanie własne na podstawie: Cwynar (2003).

Również bank może być CA, lecz wydawane przez niego certyfikaty pełnią zwykle funkcje wewnętrzne. Są wydawane na potrzeby aplikacji e-bankingowych i zaliczają się jedynie do certyfikatów niekwalifikowanych[86]. Niezależnie od wybranego wariantu certyfikacji (czy w samym banku, czy w wyspecjalizowanym CA) odpowiedzialność za odpowiednie wykorzystanie PKI pozostaje po stronie banku.

Rozwiązaniem najlepszym z dostępnych jest korzystanie z podpisu elektronicznego (definicja podana powyżej) opatrzonego ważnym certyfikatem kwalifikowanym (definicja podana w przypisie).

Infrastruktura Klucza Publicznego pozwala skutecznie ograniczać ryzyko wśród klientów korporacyjnych, u których wartość dokonywanych transakcji jest zdecydowanie wyższa niż wśród klientów detalicznych. Poszczególni pracownicy mogą mieć różne uprawnienia wynikające z rangi ich podpisów elektronicznych. Autoryzacja pewnych transakcji może wymagać na przykład podpisów dwóch pracowników (tzw. podpis łączny)[87]. System bankowości elektronicznej automatycznie weryfikuje poziom uprawnień właściciela podpisu.

Warto dodać, że podpis elektroniczny pełni wszechstronne funkcje, ponieważ może służyć nie tylko do komunikacji z bankiem i do podpisywania w jej ramach zleceń płatniczych, lecz rów-

[85] Ujawnienie klucza prywatnego, czy to CA, czy innej osoby nosi nazwę kompromitacji klucza.

[86] Certyfikaty kwalifikowane mogą wydawać w Polsce jedynie autoryzowane przez Narodowe Centrum Certyfikacji instytucje certyfikujące (vide przypis powyżej). W myśl Ustawy z 18 września 2001 roku o podpisie elektronicznym certyfikat kwalifikowany musi zawierać co najmniej (art. 20 ust. 1): (a) numer certyfikatu, (b) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji, (c) określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę oraz numer pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, (d) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone, (e) dane służące do weryfikacji podpisu elektronicznego, (f) oznaczenie początku i końca okresu ważności certyfikatu, (g) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat, (h) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji, (i) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa.

[87] Brzezina (2003).

nocześnie do kontaktów z administracją, ZUSem, urzędami skarbowymi, firmami, itp.[88] Zatem podpis elektroniczny, zapewniając wysoki poziom bezpieczeństwa, niesie korzyści wielu podmiotom systemu gospodarczego (przyspiesza i upraszcza obrót oraz redukuje koszty).

Nawiązując do rodzajów zabezpieczeń opisanych wcześniej, należy stwierdzić, że podpisem elektronicznym nie jest ani kombinacja: identyfikator + hasło ani też kombinacja: identyfikator + hasło + liczba z tokena. Jednak ta ostatnia, poparta protokołem SSL o kluczu szyfrującym odpowiedniej długości, spełnia wszystkie wymagania 'czterech filarów zaufania' (a dzięki odpowiedniemu protokołowi – także problematyczny aspekt integralności danych).

3.5. Ryzyko a transgraniczny charakter bankowości elektronicznej

Elektroniczne kanały dystrybucji umożliwiają oferowanie produktów na szerszą skalę. Banki mogą w stosunkowo prosty sposób włączyć do grona swoich klientów firmy i osoby z innych krajów. Nie oznacza to koniecznie, że muszą być obecne na zagranicznym rynku w fizycznej formie – np. jako licencjonowane spółki-córki, przedstawicielstwa, filie, itp. Mogą z równym powodzeniem oferować swoje usługi w czysto wirtualnej formie internetowej poprzez własny serwis.

Dostarczanie produktów bankowych rezydentom obcych krajów wpływa z pewnością na ryzyko ponoszone przez bank. *De facto* każdy rodzaj ryzyka, a zwłaszcza operacyjne, prawne, reputacji oraz kraju i transferu ulegają modyfikacji. To zaś odbija się na całościowym profilu ryzyka banku, zmuszając bank do ponownego przechodzenia procesu identyfikacji, pomiaru i kontroli ryzyka.

Banki, angażując się w transgraniczną bankowość elektroniczną, napotykają rozmaite przeszkody prawne. Często bywa tak, że regulacje państwa goszczącego są zdecydowanie inne od regulacji państwa macierzystego. W takich przypadkach bank naraża się na ryzyko niedostosowania do przepisów prawnych dotyczących ochrony konsumenta, zapobiegania praniu brudnych pieniędzy, minimalnego poziomu zabezpieczeń autoryzacyjnych, publikacji instrukcji, oświadczeń, itp.[89] Wszelkie badania lokalnych ograniczeń prawnych i środowiskowych bywają bardzo kosztowne. To dodatkowo zniechęca zarządy banków, decydujące się na rozszerzenie działalności bankowej jedynie za pośrednictwem Internetu, do podejmowania odpowiednich kroków dostosowawczych. Powstaje również problem podległości banku odpowiedniemu organowi nadzoru – czy odpowiada on w zakresie wirtualnego świadczenia usług zagranicznym klientom przed swoim macierzystym urzędem, czy przed goszczącym, może zaś jest zobowiązany do uzyskania licencji na świadczenie usług bankowych w obcym kraju. Ponadto, odpowiadając przed macierzystym organem kontroli, jest bardziej prawdopodobne, że będzie musiał spełnić wymogi krajowe nie zaś zagraniczne, które potencjalnie mogą być bardziej rygorystyczne.

W myśl Drugiej dyrektywy bankowej[90], a następnie Skonsolidowanej dyrektywy bankowej[91], w Europejskim Obszarze Gospodarczym (EOG) bank posiadający zezwolenie w jednym z jego krajów podlega nadzorowi właściwego organu kraju macierzystego, nie zaś kraju goszczącego. Postanowienia dyrektywy tyczą się zarówno fizycznych, jak i wirtualnych oddziałów banku.

Natomiast w przypadku większości państw spoza EOG licencja na świadczenie usług bankowych jest konieczna. Poza tym bardzo często wymagane jest również utworzenie fizycznego przedstawicielstwa, bez którego nie wolno prowadzić działalności e-bankingowej.

[88] Coraz więcej instytucji wdraża rozwiązania oparte na podpisie elektronicznym i Infrastrukturze Klucza Publicznego.

[89] Basel Committee on Banking Supervision (marzec 1998).

[90] Druga koordynacyjna dyrektywa bankowa 89/646/EWG z 15 grudnia 1989 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych dotyczących podejmowania i prowadzenia działalności przez instytucje kredytowe oraz zmieniająca dyrektywę 77/780/EWG Dz. U. WE 1989, L386/1.

[91] Skonsolidowana dyrektywa bankowa 2000/12/WE z 20 marca 2000 r. odnosząca się do podejmowania i prowadzenia działalności przez instytucje kredytowe uchyla Drugą dyrektywę bankową.

Przed nastaniem ery Internetu, która umożliwiła świadczenie usług na odległość, doskonale sprawdzały się postanowienia Konkordatu Bazylejskiego uzupełnione kolejnymi zaleceniami[92], chętnie przenoszonymi przez państwa do ich porządków prawnych. Głównym założeniem Konkordatu Bazylejskiego była współpraca macierzystych i miejscowych jednostek nadzoru, natomiast większą rolę w sprawowaniu kontroli nad działalnością części zagranicznej banku tradycyjnie odgrywał organ kraju goszczącego. O ile pierwsze z założeń nadal pozostaje w mocy, o tyle drugie w coraz większym stopniu ulega erozji. Punkt ciężkości w bankowości elektronicznej przesuwa się z organu nadzoru kraju goszczącego na organ kraju macierzystego[93]. Zjawisko to jest naturalne, zważywszy na znikomą zdolność kontroli banków oferujących swe usługi jedynie w postaci wirtualnej przez instytucje krajów goszczących (serwery obsługujące system e-bankingu oraz sam bank znajdują się przecież w kraju macierzystym). Tym niemniej banki świadczące usługi bankowości elektronicznej w obcym kraju muszą spełniać miejscowe wymogi prawne i leży to w interesie nie tylko ich macierzystych organów nadzoru, lecz również goszczących. Te ostatnie mogą przejąć na siebie część obowiązków nadzorczych wobec świadczonych usług transgranicznych w przypadkach, gdy brak jest efektywnej kontroli instytucji kraju macierzystego[94].

Różnice prawne między poszczególnymi jurysdykcjami sprawiają, że odmiennie jest definiowana działalność bankowa. Może się więc zdarzyć, że pewne podmioty w danych państwach będą się wymykały restrykcyjnej kontroli, a w konsekwencji tego bankom przyjdzie konkurować w ramach tych samych usług z parabankami. Wbrew pozorom nie jest to tylko kwestia ryzyka strategiczno-biznesowego, bowiem działalność parabanków naraża banki właściwe na bezpośrednie zagrożenia operacyjne, prawne i reputacji. Pomijając takie usługi jak płatności p2p (*person-to-person*), czy EBPP (*Electronic Bill Presentment and Payment*) oferowane przez instytucje niebankowe, warto przeanalizować przypadek agregatorów finansowych. Są to aplikacje, które umożliwiają konsolidację na jednej witrynie internetowej informacji należących do danej osoby z różnych serwisów on-line. Obecnie nietrudno sobie wyobrazić[95] klienta mającego dwa rachunki bankowe z dostępem on-line, kartę kredytową wydaną przez MasterCard, inwestującego na giełdzie za pośrednictwem Internetu, posiadającego polisę ubezpieczeniową zakupioną w sieci, od czasu do czasu sprawdzającego stan konta w Otwartym Funduszu Emerytalnym. Dodatkowo taki klient sprawdza regularnie swoje konto pocztowe, jest subskrybentem kilku list dyskusyjnych oraz interesuje się nowościami z rynków finansowych.

Każda z wymienionych instytucji chroni swoich klientów przed oszustami stosując identyfikatory, hasła, kody TAN, tokeny etc. Oznacza to, że zapanowanie nad wszystkimi usługami, nie mówiąc już np. o analizie całościowego stanu finansów osobistych, może stać się bardzo kłopotliwe, czasochłonne i wymagające korzystania z wielu urządzeń. Odpowiedzią na te problemy jest agregacja usług finansowych.

Można wyróżnić dwa jej podstawowe modele: *screen-scraping* oraz *direct feed*. *Screen scraping* jest chronologicznie pierwszą i jak dotąd najbardziej popularną metodą agregacji danych. Polega na udostępnianiu instytucji oferującej usługi agregacji danych dostępowych – identyfikatorów, kodów PIN, haseł – do kont, które mają zostać poddane temu procesowi. Dane te są przechowywane w odpowiednio zabezpieczonych centrach danych lub zaszyfrowane w pamięci komputera użytkownika. W momencie, gdy użytkownik chce skorzystać z usług, oprogramowanie agregatora łączy się z właściwymi serwisami i „naśladując" go pobiera odpowiednie informacje, przetwarza je i prezentuje w skonsolidowanej formie na swojej witrynie internetowej.

[92] Konkordatem Bazylejskim zwany jest dokument Komitetu Bazylejskiego z maja 1983 r. pod tytułem Zasady nadzoru nad zagranicznymi placówkami banków. Został on uzupełniony szeregiem raportów: Information Flows Between Banking Supervisory Authorities (April 1990), Minimum standards for the Supervision of International Banking Groups and their Cross-Border Establishments (July 1992), The Supervision of Cross-Border Banking (October 1996), Core Principles for Effective Banking Supervision (September 1997), Core Principles Methodology (October 1999) i Essential Elements of a Statement of Co-operation Between Banking Supervisors (May 2001).

[93] Dotyczy tych przypadków, w których bank albo działa w formie oddziału na terytorium państwa goszczącego, albo czysto wirtualnie za pośrednictwem sieci.

[94] Basel Committee on Banking Supervision, (lipiec 2003). W tym dokumencie znajdują się również wskazówki mówiące o tym, kiedy można uznać, że bank świadczy usługi transgraniczne (Aneks I).

[95] W Polsce nadal jest to rzadkość, lecz wkrótce stanie się codziennością, tak jak w Stanach Zjednoczonych.

Direct feed z kolei opiera się na uzgodnieniach i umowach dotyczących standardów wymiany danych oraz ich bezpieczeństwa pomiędzy instytucjami uczestniczącymi w procesie agregacji usług finansowych. Najbardziej rozpowszechnionym standardem jest w tym wypadku OFX (*Open Financial Exchange*) oraz jego sukcesor IFX (*Interactive Financial Exchange*) oparty na formacie XML (*Extended Markup Language*).

Konieczność ścisłej współpracy między firmami w ramach modelu *direct feed*, dostosowania standardów bezpieczeństwa, a także konkurencja, powodują że jest on zdecydowanie mniej popularny od *screen-scrapingu*[96].

Wynika z tego, że banki są narażone na ryzyko operacyjne, prawne i reputacji, ponieważ nie posiadają żadnej kontroli nad instytucją zajmującą się screen-scrapingiem informacji o kliencie z ich baz danych, co więcej – w przeważającej części przypadków nie są świadome tego procederu. W konsekwencji mogą zostać pociągnięte do odpowiedzialności za niewłaściwe użycie wspomnianych informacji, straty finansowe klientów spowodowane źle zabezpieczonym dostępem do konta lub wyciek danych poufnych, itp.[97]

Bankom, które zdecydują się w ramach bankowości internetowej na współpracę outsourcingową z partnerem zagranicznym, grozi wzrost ryzyka operacyjnego. Przykładowo, trudniej jest monitorować oraz narzucać określone rozwiązania dostawcy usług teleinformatycznych ulokowanemu w obcym kraju. Ponadto z tą kwestią związane jest ryzyko kraju i transferu. Podmioty zagraniczne, od których bank będzie trwale uzależniony, mogą na skutek perturbacji polityczno-ekonomicznych zaprzestać regulowania swoich zobowiązań, zaś władze kraju mogą niechętnie patrzeć na tę formę świadczenia usług bankowych przez obcą instytucję i próbować zniechęcać ją do prowadzenia działalności na przeróżne sposoby.

Banki świadczące usługi za pośrednictwem Internetu lub innych elektronicznych kanałów dystrybucji w obcych krajach muszą liczyć się z prawdopodobieństwem wyższej ekspozycji na ryzyka: kredytowe, płynności, stopy procentowej i rynkowe. Aplikacje służące do oceny ryzyka kredytowego mogą okazać się w jakimś stopniu nieodpowiednie w ocenie zdolności kreytowej klientów zagranicznych. Akceptacja rozrachunków w walutach obcych naraża bank na ryzyko walutowe wchodzące w skład rynkowego. Banki powinny też wziąć pod uwagę różnice w stopach procentowych poszczególnych krajów. Przeważnie różnią się one poziomem stóp procentowych[98], więc może się okazać, że oferta banku zaprezentowana na witrynie internetowej będzie zupełnie nieadekwatna dla klientów obcego kraju (proste przetłumaczenie witryny i promocja e-banku bez całkowicie przemodelowanej oferty może nie wystarczyć).

Natura Internetu sprawia, że przepływ informacji jest zdecydowanie szybszy, a użytkownicy dowiadują się o pewnych zdarzeniach prawie natychmiast po ich zaistnieniu. W konsekwencji nietrudno o tzw. efekt domina. Kłopoty jednego e-banku zagranicznego mogą w błyskawicznym tempie dosięgnąć kolejne zagraniczne e-banki, bowiem wpadający w panikę klienci mogą masowo zacząć wycofywać swoje wkłady. To zaś przekłada się na trudności e-banku w czasowym regulowaniu zobowiązań (ryzyko płynności).

Transgraniczna bankowość elektroniczna potęguje ryzyko związane z praniem brudnych pieniędzy. Bankowi jest trudniej monitorować transakcje przeprowadzane przez rezydentów różnych krajów, ustanawiać na własny użytek odpowiednie limity operacji, które powinny być kontrolowane, czy choćby znajdować podejrzane relacje między pozornie niezwiązanymi ze sobą transakcjami[99].

---

[96] Przypadek agregatora finansowego opracowano na podstawie: Wielgosz, Rembiś (2002).

[97] W Stanach Zjednoczonych miały już miejsce procesy wytoczone przez banki instytucjom agregującym usługi finansowe, np.: First National Bank versus Pay Trust (ten ostatni został oskarżony o bezprawne gromadzenie danych finansowych klientów z ominięciem standardowych procedur zastrzeżonych w regulaminie banku).

[98] Nie dotyczy to państw członkowskich Europejskiej Unii Gospodarczej i Walutowej, gdzie obowiązujący poziom stóp procentowych ustala Europejski Bank Centralny. Rezultatem tego bank niemiecki, który rozpocznie działalność elektroniczną we Francji nie jest narażony na transgraniczne ryzyko stopy procentowej, wynikające z samej tylko różnicy podstawowych stóp procentowych – lombardowej, referencyjnej i depozytowej (pomijam tu pozostałe aspekty ryzyka stopy procentowej).

[99] Wątek prania brudnych pieniędzy ostatnio odżywa z powodu finansowania terroryzmu.

W celu ograniczania wspomnianych rodzajów ryzyka o charakterze transgranicznym banki powinny upewnić się, że stosują się do przepisów prawnych kraju goszczącego. Są również zobowiązane do odpowiedniej edukacji klientów zagranicznych poprzez opublikowanie w ich języku procedur bezpiecznego użytkowania kont, instrukcji i oświadczeń. W interesie banków leży także zaprojektowanie planów awaryjnych, np. w sytuacjach zakłóceń na łączach telekomunikacyjnych czy braku współpracy dostawcy oprogramowania (*software provider*) lub dostawcy usług internetowych (*internet service provider*). Z identyfikowaniem, pomiarem i kontrolą ryzyka wiążą się nieustanne testowanie systemu, kopii zapasowych, nadzór nad partnerami biznesowymi, zapewnianie okresowego audytu i szereg innych działań[100].

3.6. Związek ryzyka bankowości elektronicznej z pieniądzem elektronicznym

W kwestii pieniądza elektronicznego Parlament Europejski i Rada UE przyjęły 18 września 2000 r. dwie dyrektywy: Dyrektywę 2000/46/WE[101] w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego (IPE) oraz nadzoru ostrożnościowego nad ich działalnością, a także Dyrektywę 2000/28/WE[102], która nowelizuje Skonsolidowaną dyrektywę bankową 2000/12/WE[103] w celu włączenia instytucji pieniądza elektronicznego do definicji instytucji kredytowej. W odpowiedzi na to Polski Parlament uchwalił Ustawę z 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. 2002 nr 169 poz. 1385).

Definicja pieniądza elektronicznego została podana w pierwszym rozdziale (uregulowanie z Ustawy Prawo bankowe). Nośnikiem pieniądza elektronicznego są przeważnie albo chipowe karty przedpłacone z możliwością doładowania lub bez (*hardware money*), albo dysk (pamięć) komputera (*software*, *network money*).

Ustawodawstwo wielu krajów rozwiniętych, a także ustawodawstwo polskie stanowią, że wydawcą pieniądza elektronicznego nie musi być koniecznie bank[104]. W Polsce może to być spółka akcyjna o kapitale zakładowym nie niższym niż 1 mln euro, która uzyskała na tego typu działalność zezwolenie Komisji Nadzoru Bankowego (KNB)[105].

Wydaje się jednak naturalne, że banki angażujące się w bankowość elektroniczną powinny być jednocześnie wydawcami pieniądza elektronicznego. Pełniąc tę rolę, narażają się na rozmaite ryzyka, wchodzące w skład głównego zbioru ryzyk przyjętego w tej pracy dla bankowości elektronicznej (podział bazylejski).

Te ryzyka to przede wszystkim: operacyjne, prawne i reputacji, choć nie da się ukryć, że kredytowe czy płynności także tyczą się pieniądza elektronicznego (zobowiązania wynikające z jego emisji są brane pod uwagę przy liczeniu współczynnika adekwatności kapitałowej, który banki zobowiązane są utrzymywać na poziomie co najmniej 8%, a inni wydawcy na poziomie co najmniej 2%).

Rysunek 8: Otoczenie bankowości elektronicznej ilustruje grupy czynników rodzące ryzyko w odniesieniu do pieniądza elektronicznego. Potencjalne zagrożenia tkwią w technologii, niewłaściwych regulacjach prawnych, czynniku ludzkim (użytkownicy, pracownicy, hakerzy, dostawcy oprogramowania i usług teleinformatycznych). Większość zagrożeń np. w postaci nieodpowiedniego podziału uprawnień i obowiązków pracowników, braku planów awaryjnych, systemów kontro-

[100] *Vide* Basel Committee on Banking Supervision (lipiec 2003).

[101] Directive 2000/46/EC of 18 September 2000 of the European Parliament and of the Council on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275, 27 October 2000.

[102] Directive 2000/28/EC of 18 September 2000 of the European Parliament and of the Council amending Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions, OJ L 275, 27 October 2000.

[103] Directive 2000/12/EC of 20 March 2000 of the European Parliament and of the Council relating to the taking up and pursuit of the business of credit institutions, OJ L 126, 26 May 2000.

[104] M.in. w Stanach Zjednoczonych nie tylko banki są uprawnione do emisji pieniądza elektronicznego.

[105] Lista warunków, jaką musi spełnić kandydat na instytucję pieniądza elektronicznego, jest naturalnie znacznie szersza (vide Ustawa o elektronicznych instytucjach płatniczych).

li i audytu, została już opisana wcześniej. W tym miejscu należy dokonać kategoryzacji ryzyka e-banku w kontekście pieniądza elektronicznego. Zespół tych ryzyk przedstawia się następująco:

- Duplikacja elektronicznej portmonetki lub software money. Mogłoby to np. polegać na stworzeniu zduplikowanej karty wraz z kluczami kryptograficznymi, saldem i innymi informacjami, ewentualnie na stworzeniu karty pozwalającej na wielokrotne wydawanie tych samych elektronicznych pieniędzy.
- Modyfikacja lub powielenie danych lub software'u. To oszustwo sprowadza się do ładowania elektronicznej portmonetki lub aplikacji będącej nośnikiem network money pieniędzmi bez pokrycia.
- Przechwycenie i zmiana transakcji wykonanej za pośrednictwem urządzenia zawierającego pieniądz elektroniczny. Hakerzy mogą podejmować próby przechwytywania transakcji i zmiany ich przeznaczenia.
- Kradzież urządzenia zawierającego pieniądz elektroniczny. To przestępstwo polega na prostej kradzieży elektronicznej portmonetki i wykorzystaniu środków na niej zapisanych.
- Zaprzeczenie transakcji. Użytkownicy mogą twierdzić, że transakcja nie została wykonana.
- Niesprawność systemu. Nośniki pieniądza elektronicznego mogą działać nieprawidłowo z powodu zakłóceń pracy zapisanych w ich pamięci aplikacji, ewentualnie system obsługujący transakcje pieniądza elektronicznego może ulec destabilizacji[106].

Ustawa o elektronicznych instrumentach płatniczych w obecnym brzmieniu budzi niewątpliwie obawy banków. Instytucje pieniądza elektronicznego (IPE) zostały w pewnym sensie wkomponowane w kategorię instytucji kredytowych (chociaż do udzielania kredytów nie są naturalnie uprawnione)[107]. W konsekwencji klienci mogą identyfikować IPE z bankami, to zaś w przypadku kompromitacji systemu jednego z nich może poważnie zagrozić wizerunkowi banków[108]. Są one przedsiębiorstwami zaufania publicznego, których wiarygodność należy do najwyższych na rynku, zaś zaufanie do IPE będzie budowane od podstaw.

Modelowa struktura systemu, w którym występuje wielu emitentów pieniądza elektronicznego została przedstawiona na schemacie 15. W celu zachowania jasności ilustracji przyjęto, że centrum autoryzacyjno-rozliczeniowe i wydawca stanowią dwa odrębne podmioty, choć w określonych krajach jedna instytucja może pełnić obie funkcje.

Każdy z emitentów wydaje pieniądze elektroniczne swoim klientom (konsumentom), które są ładowane na elektroniczne portmonetki. Konsumenci dokonują tymi pieniędzmi płatności w sklepach, będących tzw. akceptantami. Akceptanci deponują pozyskane środki w centrach autoryzacyjno-rozliczeniowych. Operator systemu zbiera roszczenia pieniężne centrów autoryzacyjno-rozliczeniowych, konsoliduje je względem odpowiednich emitentów i im przesyła. Płatności powstałe w rezultacie roszczeń pieniądza elektronicznego są rozliczane przez krajowe izby rozliczeniowe.

Ten model umożliwia jedynie transfery pieniędzy elektronicznych między konsumentami a akceptantami (nie występują transfery między samymi konsumentami).

Wydawcą, a więc emitentem pieniądza elektronicznego jest bądź bank, bądź też instytucja pieniądza elektronicznego (w celu uproszczenia pomijamy drugi przypadek). W praktyce klient nie musi dokonywać wpłaty gotówkowej na swój rachunek, by bank doładował właściwą kwotą instrument pieniądza elektronicznego (np. elektroniczną portmonetkę). Bank obciąża bowiem rachunek klienta, jeśli znajdują się na nim właściwe fundusze, do wysokości załadowanej kwoty. Następuje transfer środków po stronie pasywów – z rachunku klienta na stworzony specjalnie do celów rozliczeń pieniądza elektronicznego rachunek banku. Zatem po załadowaniu środków w określonej wy-

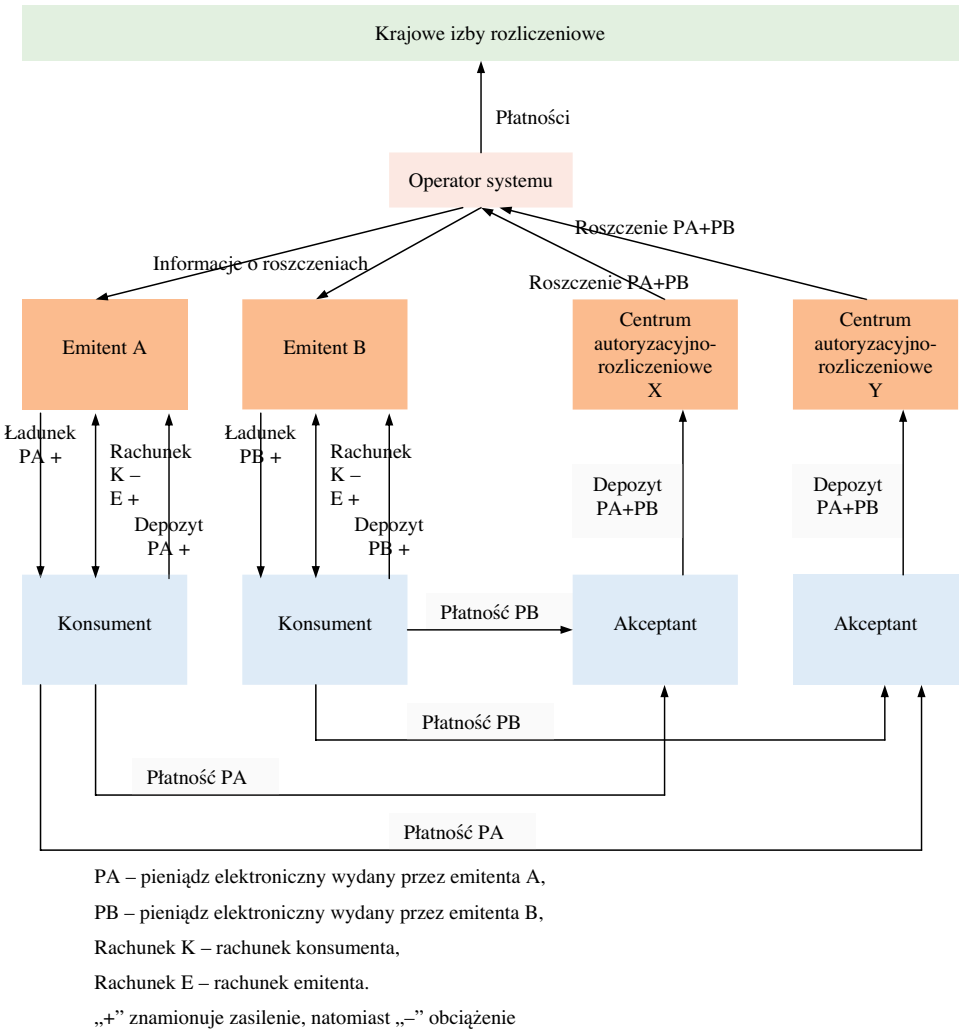
[106] Opracowano na podstawie Security of Electronic Money Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries August 1996.

[107] Szpringer (2002).

[108] Taką argumentację przedstawił Związek Banków Polskich w memorandum przeciw uchwaleniu Ustawy o elektronicznych instrumentach płatniczych z zapisem pozbawiającym banki monopolu na emisję pieniędzy elektronicznych.

sokości np. na elektroniczną portmonetkę pieniądz elektroniczny jest zobowiązaniem banku, które staje się wymagalne w momencie nadesłania informacji o odpowiednim roszczeniu i rozliczeniu płatności w krajowej izbie rozliczeniowej. E-money można porównać do czeku bankierskiego, w przypadku którego trasat przejmuje na siebie pierwotne zobowiązanie trasanta. Pieniądz elektroniczny również jest zobowiązaniem banku, równocześnie stanowiąc wygodny substytut tradycyjnej gotówki (banknotów i monet).

Schemat 3. Modelowy system pieniądza elektronicznego dla wielu emitentów



PA – pieniądz elektroniczny wydany przez emitenta A,

PB – pieniądz elektroniczny wydany przez emitenta B,

Rachunek K – rachunek konsumenta,

Rachunek E – rachunek emitenta.

„+" znamionuje zasilenie, natomiast „–" obciążenie

Źródło: opracowanie własne na podstawie: Security of Electronic Money Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries August 1996.

Tytułem komentarza do schematu należy dodać, że w Polsce nie ma podmiotu będącego operatorem systemu, natomiast centra autoryzacyjno-rozliczeniowe kontaktują się z bankami bezpośrednio przy pomocy dedykowanych terminali. W tej chwili istnieje pięć centrów: eServise, PolCard, CardPoint[109], CitiBank oraz Pekao CKC. Również trudno sobie wyobrazić w Polsce sytuację, w której bank – emitent pieniądza elektronicznego będzie jednocześnie centrum autoryzacyjno-rozliczeniowym, chyba że zdarzy się akurat tak, iż będzie to jeden z banków właścicieli danego centrum (CitiBank albo Pekao SA).

[109] Przedsiębiorstwo CardPoint stanowiło część BZ WBK, jednakże w 2004 r. zostało wyłączone ze struktur banku i zbyte na rzecz firmy holenderskiej z siedzibą w Rotterdamie NOVA euroConex Holdings B. V. (własność NOVA Information Systems – spółki zależnej U.S. Bancorp).

Im mniej jest instytucji jednocześnie zaangażowanych w obieg pieniądza elektronicznego nie powiązanych z bankami, tym banki ponoszą mniejsze ryzyko. Warto jednakże wspomnieć, że ryzyko banków odnośnie do pieniądza elektronicznego, ze względu na fakt, że jest to zjawisko nowe i nie do końca uregulowane, znajduje się wciąż na wysokim poziomie. Banki mogą się jednak kierować pewnymi wytycznymi, które zapewniają kompatybilność rozwiązań z różnych krajów. Chodzi mianowicie o standardy CEPS (*Common Electronic Purse Specification*)[110]. CEPS pomógł w stworzeniu jasnych wymogów, sposobów komunikacji oraz procedur pomiędzy poszczególnymi uczestnikami systemu pieniądza elektronicznego, a więc konsumentów, akceptantów, centrów autoryzacyjno-rozliczeniowych oraz wydawców (dotyczy elektronicznych portmonetek – *hardware money* nie zaś pieniądza sieciowego – *network money*).

CEPS jest wdrożony – w przypadku samej portmonetki – poprzez zastosowanie specjalnej aplikacji, która komunikuje się z terminalem zgodnie z zasadami ustalonymi w standardzie. Takie rozwiązanie zostało wprowadzone, ponieważ przed powstaniem specyfikacji wydano wiele portmonetek – kart chipowych zbudowanych w oparciu o różne platformy oprogramowania. Twórcom CEPS chodziło o zapewnienie użytkownikom obecnych portmonetek możliwości korzystania z nich poza ich macierzystą siecią, nie chodziło natomiast o budowanie systemu od nowa. Warto wspomnieć, że same karty chipowe też są standaryzowane i wszystkie wydawane portmonetki są w swej technicznej budowie takie same[111].

Banki powinny być zainteresowane wprowadzaniem elektronicznych portmonetek i innych kart mikroprocesorowych ze względów swojego i klientów bezpieczeństwa. Wiele rodzajów ryzyka właściwych kartom magnetycznym ulega redukcji.

Autoryzacja transakcji oraz PINu może być przeprowadzana off-line. Oznacza to, że nie występuje długotrwałe łączenie się terminala POS z centrum autoryzacyjno-rozliczeniowym. Skutkuje to spadkiem obciążenia sieci oraz zmniejszeniem ryzyka operacyjnego. Ponadto autentyczność karty oraz terminala POS jest weryfikowana podczas wykonywania transakcji. Natomiast złodziej karty nie może się nią ani posłużyć bez znajomości kodu PIN, ani skopiować, gdyż dane są zapisane w układzie scalonym zabezpieczonym przed odczytem, nie zaś na podatnym na skimming pasku magnetycznym[112].

Mikroprocesorowe karty EMV (Europay, MasterCard, Visa) zapewniają kontrolę kredytową użytkownika. Bank jest w stanie zmienić wiele z parametrów już po wydaniu karty, np. zdalnie ograniczyć limit kredytowy klientowi, który zaczął mieć problemy z terminowym regulowaniem należności. Mikroprocesor pozwala także na ustawienie wielu limitów na karcie (przykładowo: różnych co do wartości lub liczby transakcji w kraju i za granicą)[113].

Karty mikroprocesorowe, w tym elektroniczne portmonetki, dają również inne korzyści bankom i klientom. Oprócz funkcji płatniczej, karty te mogą być także dokumentem tożsamości, biletem w transporcie miejskim, nośnikiem podpisu elektronicznego, kartą lojalnościową, itp. W istocie oznacza to konieczność wchodzenia banków w alianse z innymi instytucjami, co prima facie wydaje się niebezpieczne i może być kojarzone ze wzrostem ryzyka reputacji i prawnego. W tym wypadku byłby to jednak pochopny wniosek.

3.7. Ryzyko: kredytowe, płynności, rynkowe oraz stopy procentowej

Celem tego podrozdziału jest analiza ewentualnych różnic pomiędzy ryzykiem bankowości elektronicznej a tradycyjnej. Powstaje bowiem pytanie, czy wykorzystanie elektronicznych kanałów

[110] Obecnie przeszło 30 organizacji z całego świata, które reprezentują ponad 90% wydawanych na świecie elektronicznych portmonetek, zgodziło się na adaptację systemów do standardu CEPS. Do sygnatariuszy układu należą między innymi Europay International, Visa International oraz MasterCard.

Vide http: //www. corporate. visa. com/mc/facts/smartcards/pdfs/smartcards_CEPS. pdf

[111] Żwiruk (2003), w: http: //www. kartyonline. net/arty. php? id=29

[112] Idczak, Lewandowska (2002).

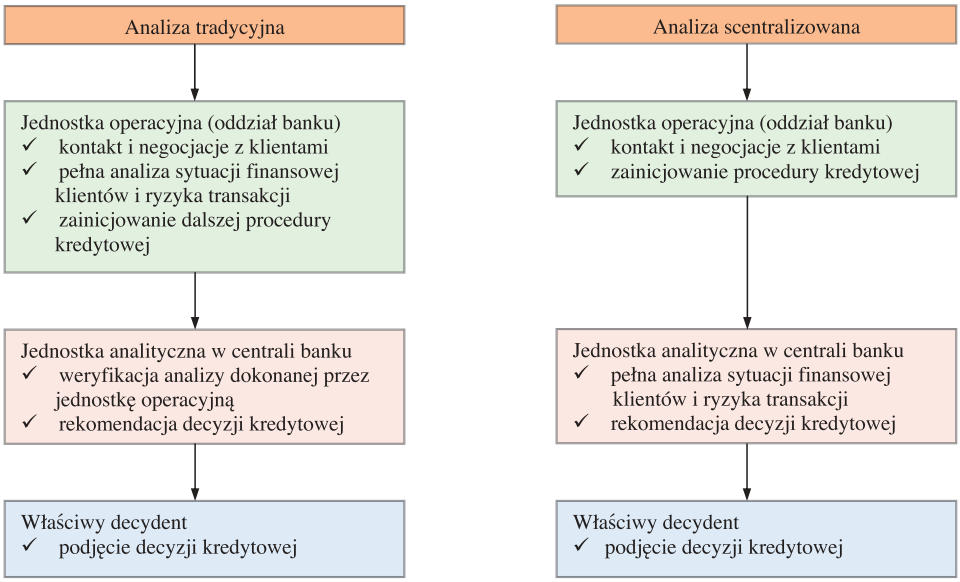
[113] Wyszomirski (2004), w: http: //www. kartyonline. net/arty. php? id=93

dystrybucji zmienia istotę wspomnianych w tytule podrozdziału rodzajów ryzyka. Na wstępie należy zaznaczyć, że wirtualne banki, takie jak mBank oraz Inteligo nie są *de facto* bankami. Pierwszy stanowi brand, czyli wydzieloną ze struktur BRE Banku SA markę, drugi jest zaś spółką o nazwie Inteligo Financial Services S.A., będącą 100% własnością PKO BP SA Zarządzanie ryzykiem tych banków, włącznie z obowiązkową sprawozdawczością do KNB leży w gestii spółek matek. Podobnie jest w przypadku innych banków, które posiadają elektroniczne kanały dystrybucji. Praktyka wygląda bowiem tak, że prowadzi się wspólną sprawozdawczość oraz pomiar ryzyka dla wszystkich kanałów. Banki z reguły nie różnicują procesu zarządzania ryzykiem, np. płynności, rynkowym, czy stopy procentowej między poszczególnymi mediami komunikacji z klientami, przyjmując że wzmiankowane ryzyka pozostają zawsze takie same[114]. Mając na uwadze postulat integracji ryzyka bankowego, tego typu strategia jest jak najbardziej słuszna[115]. W razie gdyby występowały jednak większe rozbieżności między odpowiednimi rodzajami ryzyka w poszczególnych kanałach dystrybucji podejście takie może okazać się błędne.

Warto prześledzić procedurę udzielania kredytów za pośrednictwem Internetu (jest to jedyne medium elektroniczne, w którym się ich udziela). Przed jej omówieniem należy jednakże zwrócić uwagę na pewien istotny fakt.

Obecnie istnieje tendencja, aby centralizować analizę kredytową, takie rozwiązanie przyspiesza udzielanie kredytu i zmniejsza koszty banku. Charakter kanału internetowego siłą rzeczy powoduje, że proces kredytowy musi być scentralizowany. Tym niemniej procesy kredytowe w oddziałach i placówce wirtualnej nie są identyczne. Co do zasady analiza procesu kredytowego w oddziałach wygląda następująco:

Diagram 7. Analiza procesu kredytowego w oddziałach



Źródło: Sociński A. (2003): Centralizacja procesu kredytowego. „Bank" nr 7-8.

W analizie tradycyjnej miała miejsce dokładna preselekcja klientów. Pracownik pierwszej linii mógł dokonać wstępnej oceny wiarygodności klienta, polegając nie tylko na ocenie dokumentów i danych przedstawianych przez klienta, lecz również na własnej intuicji. Na marginesie należy dodać, że ten stan rzeczy przejściowo uległ zmianie po wprowadzeniu scentralizowanej analizy kredytowej. Doradcy bankowi w placówkach stracili część swoich kompetencji na rzecz głównej jednostki analitycznej. W konsekwencji do central trafiały wszystkie wnioski, nawet te które na pierwszy rzut oka wykluczały możliwość udzielenia kredytu. Powodem tego były przede wszystkim brak uprawnień pracowników oddziałowych oraz system wynagradzania prowizyjnego od liczby

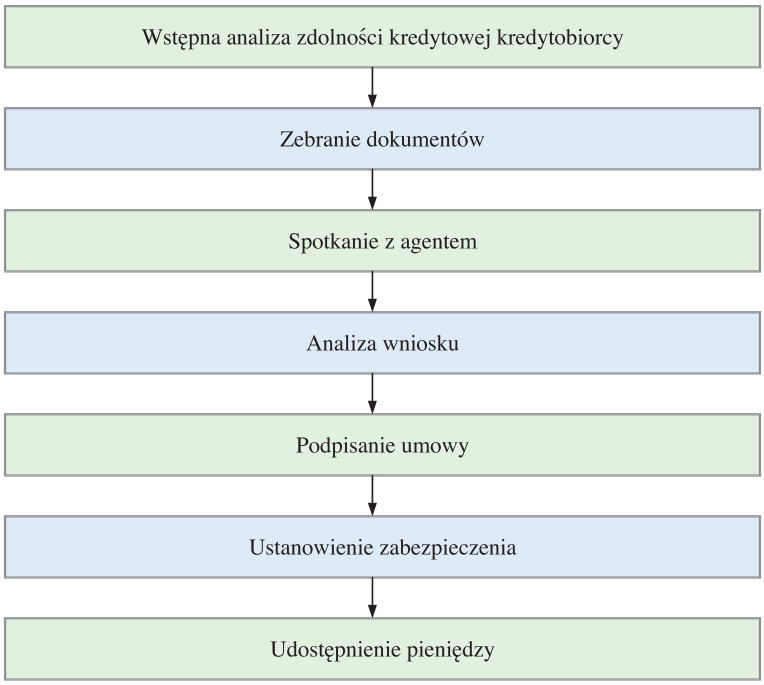
[114] Ten wniosek wyciągnąłem na podstawie przeprowadzonej przez siebie analizy środowiskowej.

[115] Racje przemawiające za integracją przedstawia Capiga (2003) w artykule Integracja ryzyka bankowego.

zawartych umów. W odpowiedzi na to większość banków wyposażyła swoich pracowników szeregowych w odpowiednie uprawnienia i zmieniła system wynagrodzeń po to, by preselekcja klientów nadal była dokonywana.

Ta związana z trudną do przecenienia rolą preselekcji dygresja znajduje odniesienie także w procedurze kredytowej za pośrednictwem Internetu, zaprezentowanej na poniższym schemacie:

Schemat 4. Procedura kredytowa w mBanku



Źródło: opracowanie własne na podstawie http: //www. mbank. com. pl

Procedura kredytowa w mBanku jest przeprowadzana w ramach tzw. mPLANU, a więc zgodnie z regulaminem banku (rozdział I) planu finansowego dającego możliwość skorzystania z oferty produktowej mBanku, w tym kredytu[116]. System preselekcji klientów sprowadza się do zbadania ich zdolności kredytowej. Potencjalny indywidualny kredytobiorca, np. starając się o kredyt na zakup mieszkania, musi wpierw wypełnić odpowiedni formularz on-line, który składa się z 4 części (dane ogólne kredytu, podstawowe informacje o wnioskodawcy/wnioskodawcach, dane głównego wnioskodawcy oraz status finansowy wnioskodawcy/wnioskodawców) zawierających w sumie 24 pola (nie wszystkie w każdym wypadku wymagają wypełnienia). Na podstawie wprowadzonych danych maszyna decyzyjna zbudowana z dynamicznych modułów, które pełnią funkcję systemu oceny punktowej klienta, a więc mechanizmu badania jego zdolności kredytowej, podaje wstępny wynik. Klient dowiaduje się na jaką maksymalną kwotę może zaciągnąć kredyt, ile wyniesie kwota raty kapitałowej oraz oprocentowanie. Podane wielkości ulegają zmianom, gdy zmieni się odpowiednie informacje w polach formularza. Ten system preselekcji działa wydajnie, ponieważ bank nie angażuje od początku swoich pracowników, redukując w ten sposób koszty, zaś klient uzyskuje natychmiastową informację na temat tego, na co może liczyć. Oportunizm klienta zostaje wyeliminowany, ponieważ wprowadzone dane zostaną i tak zweryfikowane w dalszych etapach procedury kredytowej, zatem podawanie błędnych informacji mija się z celem.

Podejście subiektywne (intuicja wykwalifikowanego pracownika banku) nie zostaje wyeliminowane. Podczas trzeciego etapu procedury kredytowej w mBanku, który *de facto* może składać się z kilku spotkań, pracownik banku ma kontakt z klientem, wówczas ocenia wstępnie zebrane przez niego dokumenty i dokonuje oględzin nieruchomości stanowiącej najczęstsze zabezpieczenie kre-

[116] Cały przypadek został opracowany na podstawie analizy własnej zasobów mBanku, w tym przejścia wstępnej procedury kredytowej, oraz artykułu Kredyt hipoteczny przez Internet „Bank" 2003 nr 9.

dytu. W tej fazie klient wypełnia również wniosek o udzielenie kredytu mPLANu. Dokonuje tego przy czynnej pomocy agenta banku.

Kolejny etap procedury stanowi analiza wniosku w centrali mBanku, która trwa przeciętne 14 dni od złożenia kompletu dokumentów[117]. Po tym czasie zostaje przekazana klientowi decyzja i albo kredyt zostaje udzielony, a więc umowa podpisana a pieniądze przelane na właściwe konto, albo wniosek zostaje odrzucony tudzież kwota wnioskowanego kredytu zmniejszona.

Interesującym rozwiązaniem w procedurze kredytowej mPLANU jest możliwość sprawdzania statusu wniosku przez Internet (opcja dostępna od 11 lipca 2003 r.). Tym samym klient jest na bieżąco informowany o postępach w analizie, ewentualnym przyspieszeniu rozpatrywania wniosku lub powstałych trudnościach, które mogą wpłynąć na opóźnienia.

Zatem wbrew pozorom procedura przyznawania kredytu za pośrednictwem Internetu nie jest wcale w pełni zdalna. Praktycznie tym tylko różni się od procedury tradycyjnej, że wstępną zdolność kredytową wylicza system elektroniczny po wprowadzeniu danych przez samego klienta oraz że istnieje możliwość sprawdzenia statusu wniosku on-line[118]. W procedurze kredytowej mBanku występują te same zabezpieczenia co w tradycyjnej, zaś głoszony argument, że natura Internetu wpływa na przyspieszenie opracowywania wniosku, co może rodzić niebezpieczeństwo, nie znajduje racji bytu. Wniosek jest przeciętnie rozpatrywany w terminie 14 dni. Zdarza się że niektóre placówki oddziałowe wydają decyzję kredytową znacznie szybciej.

W konsekwencji brak jest podstaw do stwierdzenia, bazując na powyższym przykładzie, że ryzyko kredytowe bankowości elektronicznej różni się od ryzyka tradycyjnego ze względu na wykorzystywany kanał dystrybucji[119].

Należy jednak przeanalizować problem głębiej. Choć opisany powyżej kazus przeczy istnieniu większego ryzyka kredytowego bankowości elektronicznej, to można wskazać na pewne elementy, które świadczą o zjawisku odwrotnym. Wykorzystanie Internetu zachęca banki do zwiększania akcji kredytowej oraz poszerzania kręgu klientów o zagranicę[120]. Ta tendencja może prowadzić do skrócenia czasu potrzebnego do rozpatrzenia wniosków kosztem jakości analizy, która negatywnie odbije się na profilu ryzyka kredytowego banku. Ponadto, należy wziąć pod uwagę fakt, że trudniej jest sprawdzić wiarygodność klientów zagranicznych. Coraz większa liczba małych banków o niewielkich funduszach własnych oraz krótkiej tradycji działania może dzięki obecności w sieci bardzo szybko się rozwinąć. Zwłaszcza dla takich banków pokusa gwałtownego zwiększenia akcji kredytowej i ekspansji transgranicznej jest wysoka. Natomiast ich upadek może mieć negatywne konsekwencje dla całego sektora bankowego.

Ryzyko kredytowe występuje niekiedy tylko w bankowości elektronicznej, nie znajdując odpowiednika w bankowości tradycyjnej. Przykładowo banki, które nabędą pieniądze elektroniczne od niebankowego emitenta w celu ich odsprzedaży swoim klientom, są narażone na ryzyko kredytowe w przypadku, gdy ich wystawca nie wywiąże się z zobowiązania wykupu. Podobne ryzyko wystąpi wówczas, gdy w ramach EBPP (*Electronic Bill Presentment and Payment*) jedna ze stron odmówi spłacenia należności. Bowiem bank, który wdrożył program, ponosi za niego

[117] W uzasadnionych przypadkach termin może uleć wydłużeniu.

[118] Kwestia kredytu odnawialnego wygląda inaczej. W znacznie większym stopniu jest zdalna. Jednakże, po pierwsze, dotyczy mniejszych kwot, po drugie zaś kredyt odnawialny w myśl art. 69 Prawa bankowego stanowi pożyczkę, ponieważ nie posiada ustalonego celu.

[119] Ciekawy pogląd usłyszałem w trakcie wywiadu przeprowadzonego z dr W. Bolanowskim – Dyrektorem Wydziału Rozwoju Kanałów Dostępu mBanku (faktycznie Departament Bankowości Elektronicznej BRE Banku S. A.). Stwierdził on, że suma sumarum ryzyko kredytowe mBanku jest mniejsze od analogicznego ryzyka MultiBanku (druga z części BRE Banku, zajmująca się obsługą klientów detalicznych). Jego zdaniem ten stan rzeczy spowodowany jest wydajniejszą kontrolą kredytową oraz lepszą 'jakością' klientów mBanku. MultiBank bowiem, choć swą ofertę pozycjonuje do bogatszego segmentu klientów indywidualnych, to jednocześnie udziela wielu kredytów osobom spoza kręgu własnych klientów. Często łamie zatem zasadę 'znaj swojego klienta' (know your customer rule), gdyż znaczna część kredytobiorców nie posiada wystarczającej historii rachunku, na podstawie której dałoby się zweryfikować ich wiarygodność. Z zacytowaną opinią można by polemizować.

[120] *Vide* punkt Ryzyko a transgraniczny charakter bankowości elektronicznej.

odpowiedzialność. Zwykle wyraża się ona udzieloną gwarancją na prawidłowy przebieg płatności[121].

Z 'tradycyjnymi' ryzykami w bankowości elektronicznej, a zwłaszcza z ryzykiem stopy procentowej wiąże się kwestia marży odsetkowej[122]. Z powodu braku placówek i niższych kosztów osobowych e-banki oferują wyższe oprocentowanie na depozytach. Jednocześnie starają się być bardziej konkurencyjne od swoich rywali w oprocentowaniu kredytów. W efekcie marża odsetkowa maleje, co w pewnych sytuacjach, przy nagłym wzroście kosztów, może spowodować straty. W myśl dynamicznej systematyki ryzyka prof. M. Górskiego, dalsze etapy tego scenariusza wyglądają tak, że ryzyko wyniku przeradza się w utratę płynności, a ta w niewypłacalność. Poza tym nie da się ukryć, że do tej pory wszystkie polskie banki wirtualne były nierentowne, ich straty musiały pokrywać spółki matki. Dopiero w lutym tego roku mBank osiągnął próg rentowności, po wprowadzeniu dodatkowych opłat m.in. za przelewy.

Prędkość z jaką informacja przemieszcza się w Internecie może wpływać na stopień ryzyka płynności. Nieprzychylne wiadomości, niezależnie od tego, czy są prawdziwe czy nie, mogą być z łatwością rozpowszechniane w sieci za pośrednictwem np. list dyskusyjnych albo portali i innych stron internetowych. Z dużym prawdopodobieństwem należy przyjąć, że deponenci banku, którzy natkną się na takowe ostrzeżenia, zaczną w szybkim tempie i na masową skalę wycofywać swoje wkłady. W owych sytuacjach niewątpliwe zalety kanału elektronicznego, takie jak dostęp do rachunku w trybie 24 godziny przez 7 dni w tygodniu i duża przepustowość serwerów banku, zamieniają się w olbrzymią wadę. W bardzo krótkim czasie bank staje w obliczu braku płynności.

Z drugiej strony błędem byłoby twierdzenie, że banki pozostają bezbronne wobec tego typu zagrożeń. Przede wszystkim dzięki naturze kanałów elektronicznych ich reakcje na incydenty mogą być znacznie szybsze. Jest to efektem ciągłego monitorowania płynności, który pozwala na natychmiastowe dostrzeżenie wszelkich zmian w wolumenie depozytów i pożyczek. Banki mogą też korzystać z innych dobrodziejstw Nowej Gospodarki, do których należą m.in.: uczestnictwo w czasie rzeczywistym w rynkach kapitałowych, pieniężnych i walutowych oraz bliskie relacje z innymi instytucjami finansowymi, owocujące współpracą i pomocą w sytuacjach zagrożenia. Uzyskanie funduszy z rynku międzybankowego jest bowiem dużo prostsze, gdy on jest on-line, a jego uczestnikami są instytucje z całego świata, zgłaszające rozmaite zapotrzebowania. Wówczas znalezienie partnera np. do swapu walutowego lub do FRA (*Forward Rate Agreement*) nie stanowi większego problemu.

Należy w tym miejscu dodać, że funkcjonujące banki wirtualne w Polsce oraz kanały internetowe banków tradycyjnych są najczęściej źródłem płynności dla swoich spółek matek[123]. W konsekwencji, gdyby sztucznie wydzielić ich aktywa z bilansu macierzystych jednostek, to okaże się, że stanowią one albo rezerwy podstawowe płynności (pierwszej linii), albo dodatkowe (drugiej linii)[124]. Z czasem będzie się to zmieniać, ma to już miejsce w mBanku, który rozpoczął działalność kredytową.

Wracając do globalnego charakteru bankowości elektronicznej, sieci powiązań miedzy instytucjami oraz światowych rynków finansowych należy podkreślić, że mogą się one istotnie przyczynić do usprawnienia zarządzania ryzykiem bankowym. Dzięki nowym możliwościom, wiele z tradycyjnych rodzajów ryzyka, które wydają się spotęgowane w bankowości elektronicznej, może zostać złagodzonych. Gdyby dalej rozwinąć wątek ryzyka płynności, to okaże się, że wysoka zmienność stanu depozytów w bankach elektronicznych wcale nie musi pociągać za sobą konieczności utrzy-

[121] Oba przykłady są w realiach polskich hipotetyczne, ponieważ nie funkcjonują instytucje pieniądza elektronicznego, od których bank mógłby nabyć wartość przedpłaconą, a podmioty gospodarcze nie rozliczają się ze sobą przy pomocy EBPP.

[122] Marża odsetkowa (spread) stanowi różnicę między dochodem odsetkowym uzyskanym z aktywów dochodowych a kosztem odsetkowym płaconym za zobowiązania. Wyrażana jest w pieniądzu lub jako odsetek aktywów dochodowych netto. W literaturze można się także spotkać z jej określeniem jako dochód odsetkowy netto. Definicje zaczerpnięto z Przybylska-Kapuścińska (red.) (2001).

[123] Makowska, Mackiewicz (2002).

[124] Rezerwy podstawowe obejmują gotówkę w kasie, depozyty w banku centralnym, salda na rachunkach w innych instytucjach depozytowych (rachunki Nostro) oraz gotówkę w drodze, zaś rezerwy dodatkowe są to krótkoterminowe, łatwo zbywalne papiery wartościowe o średnim terminie zapadalności do roku (bony skarbowe, obligacje skarbu państwa, akcepty bankowe, itp.), obciążone małym ryzykiem stóp procentowych. Źródło: Gruszka (2002).

mywania dużej bazy rezerw pierwszej i drugiej linii. Przy efektywnych rynkach elektronicznych zdobycie funduszy ze środków pozyskanych z sekurytyzacji[125] mniej płynnych aktywów, czyli kredytów nie będzie stanowiło dla banku problemu. Na pewno szybko znajdzie się instytucja, która chętnie przejmie na siebie ryzyko kredytowe banku w zamian za dochód pozyskany ze spłaty kredytów. Sekurytyzacja nie musi też prowadzić do zerwania kontaktu między bankiem a kredytobiorcą. Bank może zachować prawo do obsługi kredytu, czyli monitorowania i przyjmowania spłat. Jest to o tyle korzystne dla banku, że nie tylko zachowuje on wspomniany kontakt z klientem, lecz pozyskuje dodatkowe dochody pozaodsetkowe z tytułu obsługi kredytu[126].

Poważne zagrożenie dla e-banków jest związane ze zjawiskiem zwanym zmiennością (*volatility*), które nasila się w bankowości elektronicznej[127]. Zmienności podlegają zarówno depozyty (o czym była już mowa wcześniej), jak również ceny papierów wartościowych którymi handluje się w sieci. Zmienność stanu depozytów oraz cen papierów wartościowych stanowią części składowe ryzyka: rynkowego, płynności oraz stopy procentowej. Z jednej strony ceny instrumentów finansowych często się zmieniają, z drugiej zaś łatwiej je zbyć, nawet przed terminem wykupu, to zaś poprawia płynność.

Znamienny wzrost w sektorze finansowych usług elektronicznych konkurencji ze strony banków i parabanków, gwałtowny postęp technologiczny, nowe produkty finansowe, zwiększone uzależnienie banków od stron trzecich (outsourcing) także wywierają wpływ na tradycyjne rodzaje ryzyka bankowości elektronicznej. Przykładowo, agregatory finansowe (opisane we wcześniejszym punkcie) osłabiają związki lojalnościowe banków z klientami. Zdarza się, że korzystający z agregatora klient po prostu wybiera bardziej intratną lokatę z serii dostępnych w różnych bankach. Nie ma dla niego znaczenia, że nie jest to lokata określonego banku. W rezultacie wpływa to na niestabilność pasywów banku, ryzyko płynności, wyniku, itp. Receptą na ten problem wydaje się wzmacnianie więzi z klientem. Klient lojalny, który darzy bank zaufaniem, jest mniej podatny na zachęty wycofania z niego wkładów i przeniesienia ich do konkurencji z powodu niewielkich różnic w stopach procentowych.

Należałoby się zastanowić, czy natura bankowości elektronicznej i Nowej Gospodarki modyfikuje ryzyko samej bankowości elektronicznej, czy zmienia je w całej bankowości; bez względu na to czy są to oddziały, WAP, czy Internet. Trudno bowiem zakładać, że nie ma sprzężenia zwrotnego pomiędzy ryzykami w obu środowiskach. Tym niemniej wiele z opisanych powyżej zjawisk nie istnieje poza kanałami elektronicznymi, zaś poczyniona uwaga, choć może i słuszna *prima facie*, wykracza poza zakres weryfikowanych w tej pracy hipotez.

W elektronicznej gospodarce zmiany kwotowań papierów wartościowych czy kursów walut odbywają się w czasie rzeczywistym, zaś rynki finansowe funkcjonują na zasadzie naczyń połączonych. Niesie to konsekwencje dla ryzyka bankowości elektronicznej. Coraz mniejsze znaczenie odgrywa zjawisko arbitrażu, bowiem w praktyce ceny walorów lub kursy walut w różnych rejonach świata dostosowują się prawie natychmiast, z drugiej zaś strony te zmiany potrafią być nieprzewidywalne i nagłe. Stąd też banki, które dzięki możliwościom kanałów elektronicznych są w stanie szybko rozwinąć swoją działalność poza granicami kraju macierzystego, muszą liczyć się z niebezpieczeństwem, jakie stwarza wysoka chwiejność cen i kursów na rynkach międzynarodowych. Rośnie ryzyko rynkowe, zwłaszcza zaś jego część stanowiąca ryzyko walutowe[128].

[125] Pod pojęciem sekurytyzacji kryje się technika refinansowania, która polega na sprzedaży jednorodnych pod względem jakości kredytów przekształconych w pakiet papierów wartościowych, co pozwala na ich wyłączenie z bilansu, a tym samym stwarza możliwość rozwijania nowej akcji kredytowej na tej samej bazie kapitałowej. Jest to tzw. sekurytyzacja wtórna – *vide* Solarz (1997).

[126] Capiga (2003). Sekurytyzacja niesie ze sobą cały szereg korzyści, lecz jej istota pozostaje taka sama dla bankowości tradycyjnej, jak i elektronicznej, toteż jej dalsza analiza nie jest przedmiotem tej pracy.

[127] Electronic Banking Group Initiatives and White Papers Basel Committee for Banking Supervision October 2000.

[128] Szerzej o ryzykach związanych z transgranicznością w punkcie Ryzyko a transgraniczny charakter bankowości elektronicznej.

Ryzyka towarzyszące bankowości elektronicznej mogą być wyższe ze względu na to, że baza klientów banków wirtualnych jest bardziej płynna[129]. Klienci traktują je jako banki dodatkowe. Widać to najlepiej po liczbie rachunków pasywnych o niskim stanie środków w Inteligo i mBanku, to znaczy takich, na których nie dokonuje się żadnych lub prawie żadnych operacji[130]. Służby bankowe nie mają w takich sytuacjach wystarczającej ilości danych do oceny wzorca zachowań swoich klientów i ich wiarygodności.

W tym rozdziale, stanowiącym serce pracy, znalazło się gros dowodów na prawdziwość zawartych we wstępie pracy hipotez. Opisano specyficzne problemy bankowości elektronicznej w kontekście ryzyka bankowego. W pierwszej kolejności zostały określone elementy otoczenia bankowości elektronicznej, następnie zaś przeanalizowano, jakie zagrożenia powodują one dla e-banków w poszczególnych rodzajach ryzyka (podział bazylejski), a przede wszystkim w ryzyku: operacyjnym, prawnym i reputacji. W sześciu pierwszych punktach rozdziału położono nacisk na te trzy rodzaje ryzyka i została udowodniona hipoteza, że wychodzą one na pierwszy plan (*vide* hipoteza główna pracy).

Ponadto rozważania merytoryczne nie doprowadziły do zidentyfikowania nowego rodzaju ryzyka bankowego. Pokazano jednak, że postęp technologiczny, wyraźna globalizacja usług bankowych oraz nieustanna presja konkurencyjna zarówno ze strony samych banków, jak i innych instytucji parabankowych zaowocowały znaczącymi zmianami w funkcjonowaniu banków. Na skutek zjawisk: outsourcingu części usług bankowych (zwłaszcza infrastruktury IT), zwiększenia roli podpisu cyfrowego i PKI, transgranicznej działalności banków wirtualnych, ewolucji pieniądza w stronę formy elektronicznej, itp. banki znalazły się w innej, nowej rzeczywistości. W tych warunkach brak aktywności instytucji kredytowych na polu bankowości elektronicznej wydaje się wręcz niemożliwy (*vide* hipoteza robocza nr 2).

Ostatni punkt rozdziału (ryzyka: kredytowe, płynności, rynkowe oraz stopy procentowej) dowiódł, że tradycyjne ryzyka mogą nabierać odmiennego charakteru w bankowości elektronicznej (vide hipoteza główna pracy i robocza nr 3). W dużym stopniu jest to spowodowane nowymi produktami bankowymi (przykładowo systemami EBPP i agregatorami finansowymi), prędkością rozprzestrzeniania się informacji w Internecie, większą anonimowością klientów i trudnościami w ocenie ich wiarygodności, efektywnością finansowych rynków wirtualnych, zmiennością stanu depozytów i cen papierów wartościowych, itp.

Zwrócono również uwagę na fakt, że często jeden incydent (np. kradzież danych kart kredytowych przez hakerów i dokonanie z ich wykorzystaniem nieautoryzowanych transakcji) może być źródłem każdego rodzaju ryzyka. Natomiast niektóre zjawiska, jak np. outsourcing, mogą paradoksalnie jednocześnie zmniejszać i zwiększać te same rodzaje ryzyka – w tym wypadku operacyjne.

Hipotezy zostały zweryfikowane przez opis specyfiki e-bankingu, to znaczy tych jego elementów, które nie występują w bankowości oddziałowej. Z samego faktu różnic między poszczególnymi mediami komunikacyjnymi wynika, że ryzyko bankowości elektronicznej jest inne niż tej tradycyjnej. W kanałach elektronicznych występują inne zagrożenia, w odmienny sposób następuje identyfikacja klienta, a w ślad za nią autoryzacja transakcji. Niebezpieczeństwa e-bankingu często nie pokrywają się z niebezpieczeństwami oddziałów. Przykładowo, presja szybszego wykonywania operacji przeprowadzanych za pośrednictwem kanałów elektronicznych jest znacznie większa niż w przypadku oddziałów; to powoduje przyspieszenie obrotu pieniężnego, co z kolei zwiększa zagrożenie wycieku poufnych danych o klientach. Tym samym kontrola i przeciwdziałanie procederowi prania brudnych pieniędzy stają się trudniejsze, itp.

[129] Uwaga nie dotyczy elektronicznych kanałów tradycyjnych banków, które są dla klientów dopełnieniem oddziałów.

[130] Według nieoficjalnych szacunków liczba kont pasywnych o niskim stanie środków w polskich bankach wirtualnych oscyluje wokół 40% (dane z konferencji VI Forum Bankowości Elektronicznej – 12 grudnia 2003 r.). Tym niemniej do tej kwestii należy podchodzić z dużą ostrożnością, ponieważ banki niechętnie ujawniają informacje o rachunkach pasywnych i aktywności na nich, zatem dane są tylko szacunkowe. Jednakże na potwierdzenie tego faktu można się powołać na wypowiedź Wilkowicza Ł. z Gazety Bankowej 17.05.04: Wartość środków zdeponowanych w mBanku w przeliczeniu na jednego klienta jest coraz mniejsza i ostatnio tempo spadku przybrało na sile.

Nie można też zaprzeczyć, że w największym stopniu zmieniają się rodzaje ryzyka: operacyjne, prawne i reputacji. Coraz istotniejszą rolę odgrywa technologia, której zmiany wymuszają odpowiednią adaptację banków. Niestety, za tymi zmianami nie zawsze nadążają regulacje prawne i bywa, że banki muszą działać w porządku prawnym, którego unormowania nie przystają do świata wirtualnego.

Łatwo stwierdzić, że poszczególne rodzaje ryzyka w e-bankingu nabierają odmiennego charakteru przez zmianę otoczenia bankowości elektronicznej w stosunku do bankowości tradycyjnej. Pojawiają się takie podmioty jak hakerzy; zyskują na znaczeniu dostawcy oprogramowania i usług teleinformatycznych, inaczej zachowują się władze nadzorcze, a także – przez fakt korzystania z kanałów elektronicznych o odmiennej naturze – użytkownicy i pracownicy.

W rozdziale, prócz identyfikacji obszarów ryzyka, opisano sposoby przeciwdziałania pewnym zagrożeniom. Skoro bowiem pojawia się niebezpieczeństwo w bankowości elektronicznej, czy to związane z ryzykiem płynności, kredytowym, operacyjnym, czy reputacji, banki powinny odpowiednio na nie reagować. Wiedza jak sobie radzić z danym zagrożeniem jest bliska jego zrozumieniu, przynajmniej częściowemu. Dlatego np. sam opis podpisu cyfrowego i Infrastruktury Klucza Publicznego odpowiada poniekąd na pytanie, czym jest ryzyko operacyjne e-bankingu.

Przedstawione w rozdziale aspekty bankowości elektronicznej wyraźnie wskazują, że ryzyko *e-bankingu* zmienia ogólny profil ryzyka bankowości (*vide* hipoteza główna pracy), komplikuje istotę ryzyka bankowego, zmuszając służby bankowe do przechodzenia trzyetapowej procedury identyfikacji, pomiaru i kontroli ekspozycji oraz monitorowania ryzyka (vide hipoteza robocza nr 1) oraz nastręcza trudności w zarządzaniu (*vide* hipoteza robocza nr 3). Wiedza staje się kluczowym zasobem.

4
Uwarunkowania prawne związane z ryzykiem bankowym w Polsce i UE (stan obecny i planowany)

Banki pełnią rolę instytucji zaufania publicznego, dlatego też podlegają prawnej kontroli ze strony nadzoru bankowego. Muszą zatem spełniać szereg wymogów kapitałowych zapisanych w aktach normatywnych. Wymogi kapitałowe wchodzą w skład regulacji ostrożnościowych, które można określić jako normy prawne adresowane do instytucji finansowych, mające na celu określenie minimalnych standardów, sprzyjających ograniczaniu nadmiernie ryzykownej działalności instytucji finansowych, w tym banków[131].

Obecnie zauważa się tendencje do harmonizowania norm ostrożnościowych w skali międzynarodowej w celu stworzenia jednolitych warunków prawnych funkcjonowania banków oraz innych przedsiębiorstw finansowych. Duże zasługi na tym polu ma Komitet Bazylejski oraz inne komitety pracujące pod egidą banków centralnych Grupy G-10 i Banku Rozliczeń Międzynarodowych. Szczególnie silne tendencje do ujednolicania praw i ustaw są widoczne w Unii Europejskiej i państwach, które pragną do niej przystąpić lub uczyniły to niedawno[132].

Jednolite warunki prawne funkcjonowania banków oraz pozostałych przedsiębiorstw finansowych owocują wyższą efektywnością i konkurencyjnością całego systemu, wysokim bezpieczeństwem zaangażowanych środków jego uczestników, w tym przede wszystkim klientów, oraz niższymi kosztami działania.

M. Zaleska zwraca uwagę na fakt, że regulacje ostrożnościowe mogą być klasyfikowane według różnych kryteriów. Z punktu widzenia kryterium podmiotowego regulacje dzieli się na:

- zewnętrzne, uregulowane przez organy nadzorujące, będące niezbędnym narzędziem do sprawowania nadzoru bankowego;
- wewnętrzne, uregulowane przez organy poszczególnych banków.

Te pierwsze należą do tzw. instytucjonalnych (nadzorczych) form zabezpieczania się przed ryzykiem i znajdują swoje odzwierciedlenie w przepisach prawnych, które są dla banków obligatoryjne.

Regulacje zewnętrzne można podzielić według kryterium funkcjonalnego na dwie grupy:

- normy ograniczające ryzyko, czyli np. limity koncentracji, limity pozycji walutowych, rezerwy oraz regulacje w zakresie obrotu papierami wartościowymi;
- normy oceniające standing banku (sygnalizacyjne), m.in. współczynnik wypłacalności, współczynnik płynności i rezerwy celowe.

Wymienione regulacje mają charakter ilościowy, jednakże istnieją też wymogi jakościowe, opierające się na odpowiednim trybie postępowania, na skupianiu kompetencji zarządczych w rękach osób legitymizujących się odpowiednią wiedzą i umiejętnościami, itp.

W tym rozdziale zostaną opisane zewnętrzne unormowania prawne odnośnie ryzyka w Polsce i UE. Należy zaznaczyć, że powszechnie obowiązujące przepisy traktują ryzyko w sposób zbiorczy i nie istnieją różnice w wymogach ostrożnościowych odnośnie do bankowości elektronicznej i oddziałowej. Regulacje dotyczą *de facto* tradycyjnych rodzajów ryzyka, to znaczy: kredytowego, stopy procentowej, rynkowego i płynności. Ryzyko operacyjne, prawne oraz reputacji pozostają po-

[131] Zaleska (2002).

[132] 1 maja 2004 r. do UE przystąpiła Polska wraz z dziewięcioma innymi krajami (Łotwą, Litwą, Estonią, Czechami, Słowacją, Węgrami, Słowenią, Cyprem i Maltą).

za sferą normalizacyjną, chociaż Nowa Umowa Kapitałowa[133], która zacznie obowiązywać w ograniczonym zakresie od 2007 r., kładzie podwaliny pod budowę systemów zarządzania tymi ryzykami, sposobami ich identyfikacji i pomiaru.

Na świecie proces tworzenia przepisów prawnych w zakresie ryzyka bankowego jest logiczny i spójny. W początkowej fazie spotykają się gremia specjalistów, które prowadząc dialog z przedstawicielami banków, wypracowują wspólne strategie działań, rekomendacje i kodeksy dobrych praktyk. Na takiej zasadzie funkcjonuje Komitet Bazylejski, składający się z wysokich rangą reprezentantów władz nadzoru bankowego i banków centralnych krajów wysokorozwiniętych. Należy podkreślić, że tworzone w ten sposób zalecenia są wynikiem długich debat i konsultacji opartych na analizach prowadzonych w bankach całego świata, zarówno tych wiodących o charakterze globalnym, jak i mniejszych, lokalnych. Następnie wzmiankowane zalecenia są adaptowane do porządków prawnych poszczególnych państw. W UE przekuwa się je wpierw na dyrektywy, a dopiero później kraje członkowskie, bazując na tych dyrektywach, tworzą stosowne uregulowania.

W ten sposób powstał bodajże najważniejszy współczynnik oceniający standing banku, to znaczy współczynnik wypłacalności. Należy on do indeksów budowanych na podstawie proporcji kapitału własnego do pożyczek (tzw. *risk-asset ratio*). Stworzenie norm ostrożnościowych w bankach stało się koniecznością. W następstwie tzw. pierwszego i drugiego kryzysu naftowego w latach 70. oraz procesów towarzyszących sektor bankowy bardzo ucierpiał. Z tego oraz wielu innych powodów podjęto szeroko zakrojone prace nad znalezieniem właściwych rozwiązań na kilku forach jednocześnie, zwłaszcza zaś w ramach Banku Rozliczeń Międzynarodowych, gdzie powołano do tego specjalny Komitet ds. Regulacji Bankowych i Praktyk Nadzorczych zwany potocznie (od nazwiska przewodniczącego) Komitetem Cooka oraz we Wspólnotach Europejskich w ramach Bankowego Funduszu Doradczego[134]. Owocem prac było zawarcie w 1988 r. Umowy Kapitałowej (Basel I), która m.in. określiła zasady kalkulacji współczynnika wypłacalności. Owe zasady od tamtego czasu uległy pewnym modyfikacjom, jednak główna idea pozostała ta sama. W czerwcu 2004 r. zawarto Nową Umowę Kapitałową (Basel II), nad której kształtem pracowano intensywnie przez pięć lat od 1999 r., kiedy to Komitet Bazylejski opublikował swój Pierwszy dokument konsultacyjny dotyczący Nowej Metodologii Adekwatności Kapitałowej, opartej na trzech filarach (pierwszy – minimalne wymogi kapitałowe, drugi – badanie nadzorcze adekwatności kapitałowej, trzeci – dyscyplina rynkowa).

UE wydała szereg aktów prawnych zobowiązujących kraje członkowskie do przystosowania własnego ustawodawstwa do postanowień najpierw pierwszej, a później drugiej Umowy Kapitałowej. Pierwszą Umowę Kapitałową wprowadziły w życie: Dyrektywa 89/647/EWG[135] z 18 grudnia 1989 r. w sprawie wskaźnika wypłacalności dla instytucji kredytowych oraz Dyrektywa 93/6/WE[136] z 15 marca 1993 r. w sprawie adekwatności kapitału firm inwestycyjnych i instytucji kredytowych (tzw. *CAD – Capital Adequacy Directive*). Nową Umowę Kapitałową przenosi na grunt UE nowela Skonsolidowanej dyrektywy bankowej 2000/12/WE z 20 marca 2000 r.[137] oraz Dyrektywy CAD 93/6/WE. Nosi ona miano *Capital Requirements Directive (CRD)*.

Polska reguluje kwestie Basel I i Basel II w Ustawie Prawo bankowe z 29 sierpnia 1997 r. oraz w licznych uchwałach i zarządzeniach KNB[138].

[133] Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision November 2005.

[134] Piontek.W: Barcz (2005).

[135] Dyrektywa 89/647/EWG z 18 grudnia 1989 r. w sprawie wskaźnika wypłacalności dla instytucji kredytowych Dz. U. WE z 30 grudnia 1989 r., L386.

[136] Dyrektywa 93/6/WE z 15 marca 1993 r. w sprawie adekwatności kapitału firm inwestycyjnych i instytucji kredytowych Dz. U. WE z 11 czerwca 1993 r., L 141.

[137] Skonsolidowana dyrektywa bankowa 2000/12/WE z 20 marca 2000 r. odnosząca się do podejmowania i prowadzenia działalności przez instytucje kredytowe Dz. U. WE z 26 maja 2000 r.

[138] Ostatnie to m.in.: Uchwała nr 4/2004 z dnia 8 września 2004 r. w sprawie zakresu i szczegółowych zasad wyznaczania wymogów kapitałowych, Uchwała nr 5/2004 z dnia 8 września 2004 r. w sprawie określenia szczegółowych zasad ustalania wysokości funduszy własnych oraz Uchwała nr 6/2004 z dnia 8 września 2004 r. w sprawie określania limitów koncentracji zaangażowań kapitałowych.

4.1. *Lex lege prim*

Współczynnik wypłacalności jest miarą adekwatności kapitałowej i stanowi relację między funduszami własnymi banku a jego aktywami bilansowymi oraz pozycjami pozabilansowymi, którym przyporządkowano określone wagi ryzyka[139]. Wyliczony w ten sposób iloraz powinien być równy lub większy od 8%. Wielkość ta jest wartością modelową i została ustalona w sposób empiryczny. W uproszczeniu, im wyższy jest poziom współczynnika adekwatności kapitałowej, tym mniejsze ryzyko banku. W definicji ustawowej zarówno licznik wskaźnika, jak i mianownik wymagają wykładni.

W myśl Ustawy Prawo bankowe (art. 127) fundusze własne banku dzielą się na podstawowe i uzupełniające. Fundusze uzupełniające nie mogą przewyższyć funduszy rdzennych banku, zatem te drugie muszą stanowić co najmniej 4% aktywów i pozycji pozabilansowych (dla wskaźnika na poziomie 8%).

Fundusze podstawowe obejmują (pominięto tu różnice w nazewnictwie różnych form prawnych banków):

- kapitał zakładowy, zapasowy i rezerwowy (tzw. fundusze zasadnicze);
- fundusz ogólnego ryzyka na niezidentyfikowane ryzyko działalności bankowej;
- niepodzielony zysk z lat ubiegłych.

Pozycje pomniejszające fundusze podstawowe stanowią:

- akcje własne posiadane przez bank wycenione według wartości nabycia;
- wartości niematerialne i prawne;
- niepokryta strata z lat ubiegłych.

W skład funduszy uzupełniających wchodzą za zgodą KNB:

- kapitał z aktualizacji wyceny majątku trwałego;
- zobowiązania podporządkowane;
- inne fundusze tworzone ze środków obcych;
- zobowiązania z tytułu papierów wartościowych o nieokreślonym terminie wymagalności oraz inne instrumenty w części opłaconej[140].

Polskie unormowania w zakresie funduszy własnych z jednej strony różnią się od europejskich, z drugiej – w zasadniczych kwestiach pozostają te same. Wiele do powiedzenia ma w tym zakresie KNB, ponieważ to ona udziela zgody (biorąc pod uwagę indywidualną sytuację banku) na zakwalifikowanie wielu pozycji do funduszy własnych banku.

Mianownik współczynnika wypłacalności ma o wiele bardziej skomplikowaną budowę. W celu ilustracji najlepiej posłużyć się wzorami analitycznymi:

1. Aktywa ważone ryzykiem: $A1i = WAi \times Ki$

   gdzie:

   A1i – wartość i-tego aktywu ważonego ryzykiem,

   WAi – waga ryzyka dla i-tego aktywu,

   Ki – wartość netto i-tego aktywu.

2. Zobowiązania pozabilansowe ważone ryzykiem: $A2j = (WZPj \times WZKj) \times Zj$

   gdzie:

[139] Zaleska (2002).

[140] *Vide* Prawo bankowe oraz Uchwała KNB nr 5/2004 z dnia 8 września 2004 r. w sprawie określenia szczegółowych zasad ustalania wysokości funduszy własnych.

A2j – wartość j-tego zobowiązania pozabilansowego ważonego ryzykiem,

WZPj – waga ryzyka produktu dla j-tego zobowiązania pozabilansowego,

WZKj – waga ryzyka kontrahenta dla j-tego zobowiązania pozabilansowego,

Zj – wartość netto j-tego zobowiązania pozabilansowego.

3. Mianownik: $A = \sum_{i=1}^{n} A1 + \sum_{j=1}^{m} A2$

Kwestię problemową stanowi określenie wag ryzyka dla aktywów i zobowiązań pozabilansowych[141]. Według Dyrektywy 89/647/EWG, a w ślad za nią prawa polskiego, ważenie ryzyka dokonuje się według dwóch kryteriów: kraju pochodzenia dłużnika oraz rodzaju operacji bankowej (to kryterium można też określić jako rodzaj aktywu/zobowiązania pozabilansowego).

Kraje pochodzenia dłużnika dzieli się na dwie strefy: A i B. Do krajów strefy A należą kraje członkowskie EWG, OECD (Organizacji Współpracy Gospodarczej i Rozwoju) oraz kraje, które podpisały umowy dotyczące warunków kredytowania z MFW (Międzynarodowy Fundusz Walutowy) na podstawie tzw. Ogólnych Warunków Zaciągania Kredytów (*General Agreements to Borrow, GAB*). W skład strefy B należą pozostałe kraje. Prócz tego wyszczególniono także tzw. sektor niebankowy, a w nim: banki centralne, rządy centralne państw i rządy terytorialne oraz władze lokalne, a także Wspólnotę Europejską, Europejski Bank Inwestycyjny i tzw. banki ds. wielostronnego rozwoju (np. Karaibski Bank Rozwoju). W ramach sektora niebankowego także występuje podział na strefy krajów A i B.

Ustawodawca polski zaklasyfikował poszczególne podmioty krajów strefy A i B do jednej z trzech kategorii: podmioty klasy I, II lub III. Następnie zaś, uwzględniając klasę podmiotu oraz rodzaj operacji bankowej przyporządkował odpowiednim pozycjom aktywów i pozycji pozabilansowych daną wagę ryzyka (jedną z czterech: 0%, 20%, 50%, 100%). I tak przykładowo wagę ryzyka 0% mają: aktywa takie, jak kasa lub należności od podmiotów klasy I, zobowiązania pozabilansowe w postaci transakcji sprzedaży opcji lub niewykorzystane zobowiązania kredytowe z terminem zapadalności do jednego roku; wagę ryzyka 20%: aktywa – należności od podmiotów klasy II, w części nie objętej wagą ryzyka 0%, dłużne papiery wartościowe, których emitentem jest podmiot klasy III, ale które są gwarantowane przez podmioty klasy II, zobowiązania pozabilansowe – udzielone akredytywy dokumentowe, dla których zabezpieczenie stanowi wysłany towar; wagę 50%: aktywa – należności od podmiotów klasy III, w części nie objętej wagami ryzyka 0% i 20%, ale zabezpieczonej hipoteką ustanowioną na nieruchomości, zobowiązana pozabilansowe – udzielone gwarancje jakości odsprzedawanych towarów i gwarancje zapłaty odszkodowania, wagę 100%: aktywa – papiery wartościowe w części nie objętej wagami 0%, 20% lub 50%, zobowiązania pozabilansowe – udzielone akcepty i poręczenia wekslowe.

Współczynnik wypłacalności oraz opisane dalej limity koncentracji wierzytelności, inwestycji kapitałowych, system rezerw celowych oraz metoda wyznaczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka są takie same dla bankowości elektronicznej i tradycyjnej. Można dyskutować czy same metody są słuszne, czy np. podział podmiotów na klasy i dobór wag ryzyka zostały przeprowadzone prawidłowo i czy nie można by ich zastąpić innymi bardziej adekwatnymi[142]. Jednak niezależnie od tych wątpliwości należy stwierdzić, że obecne metody pomiaru ryzyka biorą implicite pod uwagę różnice między ryzykami w bankowości elektronicznej i tradycyjnej. Zapewnia to konstrukcja odpowiednich wskaźników i wymogów kapitałowych. Aby zilustrować tę myśl, trzeba odwołać się do następującego, chociaż hipotetycznego w polskich warunkach, przykładu: wymóg z tytułu ryzyka walutowego dla czysto wirtualnego banku i banku tradycyjnego w świetle Uchwały KNB nr 4/2004 jest identyczny. Obliczany metodą podstawową stanowi 8% pozycji walutowej całkowitej – jeżeli pozycja walutowa całkowita przewyższa 2% funduszy własnych banku lub 0 – jeżeli pozycja walutowa całkowita nie przewyższa 2% funduszy własnych banku. Nie oznacza to naturalnie, że ryzyko walutowe banku wirtualnego i tradycyjnego jest takie samo. Tym

[141] Precyzyjne wagi ryzyka dla poszczególnych aktywów i zobowiązań pozabilansowych zostały ustalone Zarządzeniem KNB 5/98 z dnia 2 grudnia 1998 r.

[142] Nowa Umowa Kapitałowa wprowadza innowacje w tym zakresie.

niemniej skwantyfikowany wymóg kapitałowy, wkomponowany we współczynnik wypłacalności, stanowi pewien bufor bezpieczeństwa banku i spełnia funkcję jaką powinien, będąc elementem normy ograniczającej ryzyko. Dlatego też nie istnieją podstawy, aby podważać celowość regulacji ostrożnościowych. Należy natomiast dyskutować i pracować nad kreacją takich metod pomiaru ryzyka, które w lepszy sposób odzwierciedlą specyfikę bankowości elektronicznej. Na pewno trzeba też się zastanowić, jakie metody pomiaru ryzyka operacyjnego należy stworzyć, żeby można było je uwzględnić w regulacjach ostrożnościowych.

Limity koncentracji są to limity zaangażowania banku (*exposure*) w danego typu przedsięwzięcia. Przepisy klasyfikują limity na: koncentracji wierzytelności i inwestycji kapitałowych. Istnieją też limity nieuregulowane w drodze ustawy, np. branżowe, geograficzne czy wobec grup klientów (np. świadczenie usług tylko dla małych firm)[143].

Dyrektywa Rady 92/121/EWG[144] w sprawie kontroli wielkich kredytów z 21 grudnia 1992 r. definiuje duży kredyt (*large exposure*) jako kredyt przekraczający 10% funduszy własnych instytucji kredytowej. Takowa instytucja nie może udzielić pojedynczemu klientowi lub grupie powiązanych ze sobą klientów kredytu przekraczającego 25% jej funduszy własnych. Równocześnie został ustanowiony próg 20% dla kredytów wewnątrzkorporacyjnych w obrębie grupy, do której należy instytucja kredytowa. Łączny limit dużych kredytów został określony na poziomie 800% funduszy własnych. Polskie uregulowania w tym zakresie są identyczne.

Limity inwestycji kapitałowych w innych przedsiębiorstwach określa art. 51 Skonsolidowanej dyrektywy bankowej 2000/12/WE z 20 marca 2000 r. Zgodnie z tym przepisem instytucja kredytowa nie może posiadać znacznego pakietu akcji, przekraczającego 15% jej funduszy własnych, w przedsiębiorstwie, które nie jest ani instytucją kredytową, ani finansową lub też nie świadczy dla niej usług pomocniczych. Art. 128 ust. 3 Prawa bankowego w Polsce wymienia enumeratywnie jakich przedsiębiorstw nie bierze się pod uwagę przy obliczaniu progu koncentracji kapitałowej po objęciu w nich przez banki znacznego pakietu akcji lub udziałów (do tych instytucji zalicza się m.in., prócz instytucji kredytowych i finansowych, zakłady ubezpieczeniowe, izby rozliczeniowe, międzybankowe przedsiębiorstwa telekomunikacyjne, w których banki posiadają ponad 75% akcji lub udziałów). Łączna wartość znacznych pakietów akcji lub udziałów w przedsiębiorstwach innych niż instytucje kredytowe i finansowe w myśl Skonsolidowanej dyrektywy bankowej oraz art. 128. ust 2. pkt. 2 Prawa bankowego nie powinna przekroczyć 60% funduszy własnych banku.

Warto również wspomnieć o kontroli przepływów kapitałowych w bankach, gdyż do tej pory nie została w tej pracy poruszona kwestia oportunizmu ich właścicieli. Naczelną ideą tej regulacji jest niedopuszczenie do przejęcia banku lub uzyskania znaczących wpływów na jego zarządzanie przez akcjonariuszy niezapewniających stabilności finansowej banku[145]. Art. 16 Skonsolidowanej dyrektywy bankowej nałożył na osoby fizyczne i prawne obowiązek zawiadomienia organów nadzoru o nabyciu lub zmianie wysokości znacznego pakietu akcji, to znaczy takiego, który stanowi 10% i więcej kapitału lub daje prawo do 10% i więcej głosów na walnym zgromadzeniu, ewentualnie umożliwia wywieranie istotnego wpływu na kierowanie przedsiębiorstwem. Notyfikacji oraz zgody organu nadzoru w UE podlega także zamiar zwiększenia już posiadanego znacznego pakietu akcji, jeśli w jego wyniku zostałyby przekroczone progi 20%, 33% lub 50%. Równocześnie władze nadzorcze w UE sprawują kontrolę nad podmiotami, które posiadają pakiety akcji w wysokości kwalifikowanej, mogą więc m.in. zawiesić wykonywanie praw do podejmowania decyzji podmiotu wynikających z posiadanych przez niego akcji. Polskie Prawo bankowe nie przewiduje możliwości sprawowania tak daleko idącej kontroli przez organy nadzoru, jednakże jest bardziej restrykcyjne pod względem liczby progów udziałów kwalifikowanych, których przekroczenie wymaga zgody KNB. Jest ich aż siedem: 10%, 20%, 25%, 33%, 50%, 66% i 75% (art. 25) i oznaczają one procent głosów podczas walnego zgromadzenia akcjonariuszy, a więc siłę prawa podmiotu do wpływania na decyzje banku. Dodatkowo został określony próg 5% głosów, którego przekroczenie nakłada na

[143] Górski (2003).

[144] Dyrektywa Rady 92/121/EWG z 21 grudnia 1992 r. w sprawie monitorowania i kontroli koncentracji ryzyka kredytowego Dz. U. WE. z 5 lutego 1993 r., L 29.

[145] Zaleska (2002).

bank i właściwy podmiot obowiązek poinformowania władz nadzorczych. Zarówno w świetle prawa unijnego, jak i polskiego osoba zamierzająca sprzedać akcje, w rezultacie zbycia których pozostałby w jej posiadaniu pakiet akcji uprawniający do wykonywania mniej niż wartości progowe procentu głosów na walnym zgromadzeniu akcjonariuszy banku, musi o tym fakcie powiadomić organ nadzoru (w UE punktem odniesienia jest nie tylko procent głosów na walnym zgromadzeniu, lecz także wielkość udziału w kapitale spółki).

Banki tworzą rezerwy na ryzyko związane z działalnością gospodarczą, które stanowią zabezpieczenie przed zakłóceniami w spłatach należności oraz przymusem spłaty udzielonych zobowiązań pozabilansowych. Rezerwy bankowe dzieli się na ogólne i celowe. Podział taki został dokonany po raz pierwszy w Dyrektywie Czwartej Bis[146]. Art. 130 Prawa bankowego precyzuje, co kryje się pod pojęciem rezerwy ogólnej. Jest to fundusz na ogólne ryzyko działalności gospodarczej bez wyraźnego przeznaczenia. Kryterium przeznaczenia różni rezerwy ogólne od celowych, bowiem te ostatnie są tworzone w celu kompensacji konkretnego rodzaju ryzyka.

Tworzenie rezerw celowych wynika z zasad ostrożnej wyceny i jest rodzajem „samoubezpieczenia się" przed ryzykiem[147]. Mimo to banki niechętnie tworzą znaczne rezerwy celowe, ponieważ jako niepracujący składnik aktywów i pozycja kosztów wpływają one niekorzystnie na wynik finansowy, powodując nawet straty, jeśli w portfelu banku znajdzie się duża liczba „złych" kredytów.

Ze względu na fakt, że realia w poszczególnych krajach są częstokroć zupełnie inne, nie występują ujednolicone zasady tworzenia rezerw celowych i Unia na tym polu nie narzuca krajom członkowskim gotowych rozwiązań. W konsekwencji w Polsce odpowiednie regulacje wydaje KNB, opierając się na własnych doświadczeniach. Obecnie po wielu nowelizacjach i zmianach przepisów w mocy pozostaje Uchwała nr 8/99 z dnia 22 grudnia 1999 r. Według punktu 1 załącznika do tej uchwały przy ustalaniu ryzyka bankowego i wysokości rezerw celowych bank wykorzystuje do oceny jakości należności i udzielonych zobowiązań pozabilansowych dwa kryteria: terminowość spłaty kapitału lub odsetek oraz sytuację ekonomiczno-finansową dłużnika. I tak banki szeregują należności i zobowiązania pozabilansowe w pięć grup: normalne, pod obserwacją, poniżej standardu, wątpliwe i stracone, przyporządkowując im odpowiednio wagi ryzyka: 0%, 1,5%, 20%, 50% i 100%. Należy dodać, że Skarb Państwa traktuje się na zasadzie preferencyjnej, gdyż terminy spłat należności są dla niego znacznie wydłużone. Istnieją też zabezpieczenia pomniejszające podstawę tworzenia rezerw celowych. Należą do nich m.in. gwarancje i poręczenia banków centralnych i rządów krajów, zastaw rejestrowy, hipoteka, przelew wierzytelności z rachunku lokaty złożonej w innym banku niż bank posiadający należność lub udzielone zobowiązanie pozabilansowe wraz z oświadczeniem o blokadzie lokaty, przeniesienie praw własności papierów wartościowych, polisa ubezpieczeniowa KUKE (Korporacji Ubezpieczeń Kredytów Eksportowych SA), itp.

Zwieńczeniem dzieła w regulacjach związanych z ryzykiem w Polsce jest Uchwała KNB nr 4/2004 z dnia 8 września 2004 r.[148] Przepisy w niej zawarte pozwalają na obliczenie całkowitego wymogu kapitałowego banku, stanowiącego wypadkową wielu rodzajów ryzyka, i ujęcie go w rachunku adekwatności kapitałowej banku.

Przede wszystkim Uchwała wprowadza podział operacji bankowych na portfel handlowy i bankowy. Portfel handlowy obejmuje czynności banku nakierowane na zysk i związane ze sprzedażą i kupnem papierów wartościowych, transakcjami spekulacyjnymi opartymi o zmiany kursów walut, indeksów giełdowych, stóp procentowych, itp. W skład portfela handlowego wchodzą też operacje repo i reverse repo (odpowiednio umowy z udzielonym i otrzymanym przyrzeczeniem od-

[146] Dyrektywa Rady IV Bis 86/635/EWG z dnia 8 grudnia 1986 r. w sprawie rocznych zamknięć rachunkowych i bilansów skonsolidowanych banków i innych instytucji finansowych.

[147] Zaleska (2002).

[148] Uchwała nr 4/2004 Komisji Nadzoru Bankowego z dnia 8 września 2004 r. w sprawie zakresu i szczegółowych zasad wyznaczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka oraz zakresu stosowania metod statystycznych i warunków, których spełnienie umożliwia uzyskanie zgody na ich stosowanie, sposobu i szczegółowych zasad obliczania współczynnika wypłacalności banku, zakresu i sposobu uwzględniania działania banków w holdingach w obliczaniu wymogów kapitałowych i współczynnika wypłacalności oraz określenia dodatkowych pozycji bilansu banku ujmowanych łącznie z funduszami własnymi w rachunku adekwatności kapitałowej oraz zakresu, sposobu i warunków ich wyznaczania (Dz. Urz. NBP Nr 15, poz. 25).

kupu), transakcje zabezpieczające ryzyka pozycji pierwotnych zaliczonych do portfela handlowego, opłaty, prowizje, odsetki naliczone od dnia sprawozdawczego, dywidendy i depozyty zabezpieczające transakcje giełdowe, bezpośrednio związane z operacjami zaliczonymi do portfela handlowego[149]. Portfel bankowy obejmuje operacje niezaliczone do portfela handlowego banku, w szczególności zaś udzielone kredyty, pożyczki oraz przyjęte depozyty i lokaty.

Banki wyliczają obowiązujące wymogi kapitałowe z tytułu (§ 6 ust. 1):

1. ryzyka kredytowego;
2. ryzyka rynkowego, w tym:
   a) ryzyka walutowego,
   b) ryzyka cen towarów,
   c) ryzyka cen kapitałowych papierów wartościowych,
   d) ryzyka szczególnego cen instrumentów dłużnych,
   e) ryzyka ogólnego stóp procentowych;
3. ryzyka rozliczenia-dostawy oraz ryzyka kontrahenta,
4. przekroczenia limitu koncentracji zaangażowań i limitu dużych zaangażowań,
5. przekroczenia progu koncentracji kapitałowej,
6. innych rodzajów ryzyka – w zakresie i wysokości adekwatnej do ponoszonego ryzyka.

W zależności od tego, czy skala działalności handlowej banku jest znacząca czy nie, bank zobowiązany jest do odmiennego wyliczenia wymogów kapitałowych. W przypadku znaczącej działalności handlowej bank wylicza wymogi kapitałowe dla wszystkich rodzajów ryzyka, natomiast w sytuacji gdy skala działalności nie jest znacząca, bank kalkuluje wymogi kapitałowe dla rodzajów ryzyka z punktów: 1, 2a, 2b oraz 4, 5, 6. Uchwala definiuje precyzyjnie w § 3, kiedy skalę działalności handlowej banku uznaje się za znaczącą.

Do obliczania wymogów kapitałowych bank może stosować w świetle Uchwały trzy metody: podstawową, wartości zagrożonej i mieszaną (na stosowanie dwóch ostatnich wymagana jest zgoda KNB). Najbardziej zaawansowaną jest ta środkowa, zaś polskie władze nadzoru dopuszczając jej wykorzystanie, nie ustępują w niczym organom nadzorczym najbardziej rozwiniętych krajów świata.

Skalkulowane za pośrednictwem jednej z metod wymogi kapitałowe służą do obliczenia współczynnika wypłacalności. Według § 11 Uchwały:

Współczynnik wypłacalności banku oblicza się w procentach jako pomnożony przez 100 ułamek, którego:

1. licznikiem jest wartość funduszy własnych powiększona o kapitał krótkoterminowy (powiększenie o kapitał krótkoterminowy jest możliwe tylko dla banków, których skala działalności handlowej jest znacząca).
2. mianownikiem jest pomnożony przez 12,5 całkowity wymóg kapitałowy.

We właściwych paragrafach Uchwały oraz jej załączników zawarto zalecenia, jak należy obliczyć wymogi kapitałowe z tytułu poszczególnych rodzajów ryzyka, następnie zaś – w jaki sposób zagregować je w całkowity wymóg kapitałowy oraz policzyć ewentualną wielkość niedoboru kapitału na pokrycie ryzyka[150]. Warto nadmienić, że niezależnie od stosowanej metody przy wyliczaniu

[149] Dokładna lista operacji zaliczonych do portfela handlowego znajduje się w § 2 ust. 2 i ust. 4 Uchwały KNB nr 4/2004.

[150] Doskonale strukturę funduszy własnych i wymogów kapitałowych ilustruje Załącznik nr 13 do Uchwały. Składa się on z dwóch tabel z wyszczególnionymi częściami składowymi funduszy własnych i całkowitego wymogu kapitałowego.

wymogu kapitałowego dla danego rodzaju ryzyka, często konieczne jest skalkulowanie pozycji pierwotnej w danym instrumencie bazowym[151], np. dla ryzyka walutowego lub cen towarów.

Współczynnik wypłacalności wyliczony zgodnie z Uchwałą nr 4/2004 różni się tym od wskaźnika opisanego wcześniej w tym punkcie, że uwzględnia nie tylko ryzyko kredytowe, lecz również szereg innych ryzyk. Niezmiennie natomiast stanowi normę oceniającą standing banku, a pośrednio też ograniczającą ryzyko.

4.2. *Lex ferenda*

Milowym krokiem naprzód w dziedzinie ryzyka było opublikowanie w czerwcu 1999 r. przez Komitet Bazylejski ds. Nadzoru Bankowego pierwszego dokumentu konsultacyjnego pod tytułem Nowa Metodologia Adekwatności Kapitałowej[152]. Kładł on podwaliny pod Nową Umowę Kapitałową (NUK, Basel II), która została przyjęta przez Komitet Bazylejski w czerwcu 2004 r. w dokumencie 'Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework'[153]. Jego aktualizacja miała miejsce w listopadzie 2005 r.[154] *De facto* na NUK składa się wiele aktów[155], chociaż jej rdzeń stanowi wspomniany dokument.

4

Należy zaznaczyć, że Nowy układ zdecydowanie w większym stopniu niż stary bierze pod uwagę specyfikę bankowości elektronicznej. Wyrazem tego jest choćby nacisk położony na rozwój metod identyfikacji i pomiaru ryzyka operacyjnego w bankach, wprowadzenie trzech filarów w miejsce jednego lub stworzenie dla banków możliwości stosowania wewnętrznych podejść do zarządzania ryzykiem[156]. Intencją rewizji Umowy kapitałowej z 1988 r. była poprawa sposobu, w jaki określone prawem wymogi kapitałowe odzwierciedlały leżące u podstaw tych wymogów ryzyka. Ponadto, dążono do pełniejszego uwzględnienia innowacji finansowych, które pojawiły się w ostatnich latach, np. sekurytyzacji aktywów. W rezultacie pojawiania się tych innowacji okazało się, że wymogi kapitałowe wprowadzone przez Stary układ nie odpowiadają rzeczywistemu profilowi ryzyka banku.

NUK obejmuje trzy filary, pierwszy nosi nazwę minimalne wymogi kapitałowe, drugi – badanie nadzorcze adekwatności kapitałowej, trzeci zaś – dyscyplina rynkowa.

Można śmiało stwierdzić, że pierwszy z filarów, mimo znacznego rozszerzenia, stanowi kontynuację metodologii ujętej w Bazylei I. Formuła współczynnika wypłacalności pozostaje niezmienna, jak również graniczny próg 8%. Natomiast zaproponowano modyfikację wag ryzyka dla poszczególnych rodzajów podmiotów wraz z wykorzystaniem ratingów przyznawanych przez zewnętrzne wyspecjalizowane instytucje oceny wiarygodności kredytowej, takie jak: Standard & Poor's, Moody's, Fitch ICBA. Stosując klasyfikację Standard & Poor's należnościom o najwyższym ratingu – od AAA do AA- przyporządkowano wagi ryzyka 0% dla rządów i 20% dla banków oraz innych przedsiębiorstw, zaś podmiotom o najniższym ratingu, czyli poniżej B- wagę ryzyka 150%. W Starej Umowie Kapitałowej były tylko cztery wagi ryzyka: 0%, 20%, 50%, 100%, a więc nie występowała waga 150%.

Celem drugiego filaru Nowej Umowy Kapitałowej, a więc badania adekwatności kapitałowej przez nadzór, jest zapewnienie spójności pozycji kapitałowej banku z jego ogólnym profilem i stra-

[151] Pozycja pierwotna długa (krótka) w danym instrumencie bazowym oznacza saldo Wn (Ma) wynikające z operacji, której przedmiotem jest dany instrument bazowy.

[152] Nowa Metodologia Adekwatności Kapitałowej Komitet Bazylejski Czerwiec 1999.

[153] Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision June 2004.

[154] Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision November 2005.

[155] Są to m.in. raporty i zalecenia Komitetu Bazylejskiego ds. Nadzoru Bankowego, takie jak: Podstawowe zasady efektywnego nadzoru bankowego wrzesień 1997; Zarządzanie ryzykiem operacyjnym wrzesień 1998; Nowa metodologia adekwatności kapitałowej – filar 3 – dyscyplina rynkowa styczeń 2000; Zasady zarządzania ryzykiem w bankowości elektronicznej maj 2001itp.

[156] Temat został szerzej rozwinięty w pracy Górka (2004).

tegią działania[157]. Badanie to stwarza możliwość wczesnych interwencji nadzoru bankowego, gdy pojawią się określone anomalie w profilu ryzyka banku. Ponadto, drugi filar ma zapewnić właściwą kooperację organów nadzoru z zarządami banków. Na marginesie trzeba dodać, że uprawnienia władz nadzorczych są raczej szerokie, np. mogą one narzucić bankowi utrzymywanie kapitału na poziomie powyżej określonego prawem minimum.

Trzeci filar, to jest dyscyplina rynkowa, promuje stosowanie wyższych standardów w zakresie publicznie dostępnych informacji finansowych oraz zwiększenie roli uczestników rynku w zachęcaniu banków do utrzymywania adekwatnego kapitału.

Główną innowacją Nowego układu w stosunku do poprzedniej wersji jest wprowadzenie w ramach pierwszego filaru trzech możliwości kalkulacji ryzyka kredytowego i trzech innych związanych z ryzykiem operacyjnym. Komitet Bazylejski jest przekonany, że jedna standardowa metoda pomiaru ryzyka nie sprawdza się w przypadku wszystkich banków, zwłaszcza tych wysoko wyspecjalizowanych. Dlatego też proponuje trzy podejścia do ryzyka, uszeregowane od najmniej do najbardziej zaawansowanego.

Tabela 4. Podejścia do ryzyka kredytowego i operacyjnego

Ryzyko kredytowe	Ryzyko operacyjne
Podejście standardowe	Podejście oparte o wskaźniki podstawowe
Podejście podstawowe oparte o wewnętrzne ratingi banków	Podejście standardowe
Podejście zaawansowane oparte o wewnętrzne ratingi banków	Podejście pomiaru zaawansowanego (AMA – Advanced Measurement Approach)

Źródło: opracowanie własne na podstawie Overview of the New Basel Capital Accord Consultative document Basel Committee on Banking Supervision July 2003.

Podejście standardowe do ryzyka kredytowego, co zostało opisane powyżej, przewiduje zmiany w klasyfikacji wag ryzyka. Prócz tego dostarcza bankom szeroką paletę instrumentów ograniczających je i dopuszcza redukcję wymogów kapitałowych w sytuacjach, gdy zostaną udzielone bankowi odpowiednie gwarancje i poręczenia. Do grona wiarygodnych gwarantów dołączają wszystkie firmy, które mogą wykazać, że przekroczyły odpowiednią wartość ratingu.

Podejścia do ryzyka kredytowego oparte na wewnętrznych ratingach tym różnią się od standardowego, że pozwalają na stosowanie własnych metod banków do identyfikacji i szacowania tzw. kluczowych nośników ryzyka (*key risk drivers*), które służą jako wejściowe parametry do obliczania wymogów kapitałowych. Przy tej zaawansowanej technice zakres swobody banku jest większy, aczkolwiek implementacja własnych metod musi być skonsultowana z organem nadzoru i wymaga jego wyraźnej zgody. Idea wewnętrznych ratingów opiera się na tym, że albo banki dostosowują swoje wewnętrzne ratingi do standardowych wag ryzyka (w rozszerzonym systemie wag), albo też organ nadzoru w ślad za zaleceniami Komitetu Bazylejskiego projektuje obciążenia kapitałowe odzwierciedlające wewnętrzne ratingi stosowane przez banki.

Metody pomiaru ryzyka operacyjnego podlegają nieustannym przeobrażeniom, niemniej jednak w najbliższym czasie (według wszelkiego prawdopodobieństwa) nie staną się tak precyzyjne, jak metody kwantyfikacji ryzyk: rynkowego i kredytowego. Nie zmienia to faktu, że Komitet Bazylejski zachęca banki do rozwijania metod pomiaru tego ryzyka, zauważa przy tym kilka możliwych podejść do oszacowania kapitału niezbędnego do zabezpieczania się przed tym ryzykiem, począwszy od zastosowania prostego punktu odniesienia (metoda oparta o wskaźniki podstawowe oraz metoda standardowa), a skończywszy na zaawansowanych technikach modelowania (metoda pomiaru zaawansowanego – AMA). Komitet uważa, że jeśli chodzi o punkt

[157] Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision November 2005.

odniesienia, to mogą nim być ogólne wskaźniki charakteryzujące rozmiar działalności gospodarczej, takie jak przychody brutto, przychody z prowizji, koszty działalności, wielkość zarządzanych aktywów i suma aktywów odniesiona do zobowiązań pozabilansowych lub kombinacja wyżej wymienionych wielkości. Powyższe wielkości mogą być zrównoważone poprzez ich odniesienie do bilansu. Szczególną uwagę należy zwrócić na możliwości arbitrażu kapitału, a także na wszelkie ewentualne bodźce niesprzyjające lepszej kontroli ryzyka, które mogą powstać wskutek przyjęcia poszczególnych rozwiązań. Komitet jest świadomy także tego, że są inne możliwe metody alokacji kapitału wymaganego do zabezpieczenia się przed ryzykiem operacyjnym. Jedna z nich polegałaby na zezwoleniu instytucjom bankowym na stosowanie modeli. Ponadto, Komitet utrzymuje, że instytucje nadzorcze powinny również stosować ocenę jakościową, opartą na ocenie adekwatności systemu kontroli w bankach[158].

W Nowym układzie znajdują się też zalecenia, mówiące o stworzeniu podstawy do wprowadzenia obciążeń kapitałowych z tytułu ryzyka stopy procentowej w portfelach bankowych banków, nie zaś tylko w handlowych (dla tych banków, w których poziom ryzyka stopy procentowej jest znacznie wyższy od przeciętnego).

Uwzględniając postanowienia Bazylei II oraz liczne nowelizacje Bazylei I, wyraźnie widać, że systemy identyfikacji, pomiaru i monitorowania poszczególnych rodzajów ryzyka stają się coraz bardziej skomplikowane i zaawansowane metodologicznie. Banki mogą rozwijać własne metody estymacji ryzyka, a następnie obliczać na ich podstawie wymogi kapitałowe. Rozwiązania takie są o tyle korzystne dla banków, że biorą pod uwagę ich indywidualną sytuację, nie nakładają tym samym nieadekwatnych obciążeń. Z drugiej strony wpływają negatywnie na transparentność systemu bankowego. Klientom trudniej jest zrozumieć, jaki jest faktyczny profil ryzyka ich banku. Wadę złożoności systemów zarządzania ryzykiem oraz ich mniejszej przejrzystości neutralizują dwa ostatnie filary NUKu. Tworzenie i stosowanie własnych metod wymaga ciągłego dialogu z organami nadzoru, zaś obowiązek publikacji w przystępny i spójny sposób informacji dotyczących kapitału oraz metod zarządzania ryzykiem pozwala klientom zorientować się w profilu ryzyka banku. Jawność informacji zwiększa dyscyplinę rynkową i pozwala uczestnikom rynku ocenić adekwatność kapitałową banku[159].

4.3. *Lex lege bis*

Ten punkt ujmuje kwestie związane przede wszystkim z ryzykami: strategicznym, prawnym i reputacji w bankowości elektronicznej, choć można się w jego treści doszukać śladów także innych ryzyk. Poruszone zostaną wątki podpisu elektronicznego, elektronicznych instrumentów płatniczych, usług świadczonych drogą elektroniczną oraz kredytu konsumenckiego[160].

Ustawa z 18 września 2001 r. o podpisie elektronicznym stanowi w swej zasadniczej części przeniesienie unijnej Dyrektywy 99/93/WE z 13 grudnia 1999 r. w sprawie stworzenia wspólnotowych ram prawnych podpisu elektronicznego. Podpis elektroniczny upraszcza obrót gospodarczy, zwiększa jego pewność i bezpieczeństwo.

Zgodnie z ustawą istnieją dwa rodzaje podpisu elektronicznego: zwykły i bezpieczny. Bezpieczny podpis różni się w praktyce tym od zwykłego, że jest poświadczony ważnym kwalifikowanym certyfikatem urzędu certyfikującego, w konsekwencji zaś sądowa wartość dowodowa dokumentu opatrzonego takim podpisem jest znacznie wyższa. Każdy bezpieczny podpis elektroniczny w ramach Infrastruktury Klucza Publicznego zapewnia w duchu swej funkcjonalności opisane powyżej „cztery filary zaufania".

---

[158] Akapit opracowano na podstawie dokumentów: Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision November 2005, Nowa Metodologia Adekwatności Kapitałowej Komitet Bazylejski ds. Nadzoru Bankowego Czerwiec 1999 oraz Overview of the New Basel Capital Accord Consultative document Basel Committee on Banking Supervision, July 2003.

[159] Nowa metodologia adekwatności kapitałowej – filar 3 – dyscyplina rynkowa Komitet Bazylejski ds. Nadzoru Bankowego styczeń 2000.

[160] Pragnę zwrócić uwagę tylko na pewne aspekty prawne tychże wątków. Analiza będzie miała zatem charakter pobieżny. Rozwinięć odpowiednich kwestii należy szukać w innych częściach pracy lub w bibliografii.

Ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych dostosowuje polskie prawo do przepisów Unii Europejskiej. Przede wszystkim przenosi na polski grunt prawny przepisy Dyrektywy Parlamentu Europejskiego i Rady 2000/46/WE z 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością oraz Zalecenie Komisji Europejskiej 97/489/ WE z dnia 30 lipca 1997 r. w sprawie transakcji prowadzonych przy użyciu elektronicznych instrumentów płatniczych, a w szczególności stosunków między wydawcą a posiadaczem.

Dla ryzyka bankowego dwa zagadnienia zawarte w ustawie mają olbrzymie znaczenie: pierwsze – wydawców kart płatniczych i pieniądza elektronicznego, drugie – stopnia odpowiedzialności banku za transakcje przeprowadzone z użyciem skradzionej karty płatniczej. Oba rodzą konsekwencje dla ryzyka strategicznego, wyniku, reputacji, itp. Legitymacja ustawowa do wydawania kart płatniczych i pieniędzy elektronicznych dla podmiotów niebędących bankami w myśl argumentacji Związku Banków Polskich naraża uczestników rynku na kłopoty związane z niską wiarygodnością finansową tych instytucji w sytuacjach braku gwarancji bankowych obejmujących zobowiązania z tytułu dokonywanych rozliczeń[161]. Jeżeli zaś chodzi o zagadnienie drugie, to posiadacz karty – jak głosi Ustawa – nie ponosi żadnej odpowiedzialności za operacje dokonane przy użyciu jego karty, których zlecenia nie potwierdził po zgłoszeniu w banku faktu utraty karty (art. 5), natomiast jego odpowiedzialność do momentu owego zgłoszenia ogranicza się do równowartości w złotych 150 Euro (art. 28 ust. 2). Wystawca karty zobowiązany jest do całodobowego przyjmowania zgłoszeń utraty lub zniszczenia kart klientów (art. 22).

Oparta m.in. o Dyrektywy 95/46/WE oraz 97/66/WE o ochronie danych osobowych Ustawa o świadczeniu usług drogą elektroniczną (Dz. U. 2002 nr 144 poz. 1204) określa zasady ochrony danych osób fizycznych korzystających z tego rodzaju usług. Dla banków jest to o tyle istotne, że muszą one w dobie coraz częściej zawieranych umów outsourcingowych przekazywać partnerowi poufne informacje o klientach. Odpowiedzialność za nadużycia związane z niedopatrzeniami kooperanta, skutkujące ujawnieniem nieuprawnionym podmiotom danych klientów, spoczywa na banku.

Ustawa z 20 lipca 2001 r. o kredycie konsumenckim (Dz. U. 2001 nr 100 poz. 1081) koresponduje z rozwiązaniami ujętymi w Dyrektywie 87/102/EWG z 22 grudnia 1986 r. w sprawie ujednolicenia ustaw i przepisów wykonawczych państw członkowskich dotyczących kredytów konsumenckich, a nawet wykracza poza ustanowione w tym akcie prawa wspólnotowego minimum ochrony konsumenta. Do najważniejszych postanowień Ustawy należy zapis nakładający na podmioty udzielające kredytów konsumenckich, w tym banki, obowiązek informowania explicite klientów o rzeczywistej stopie procentowej kredytu, która zawiera koszty odsetek oraz inne opłaty i prowizje. Jednakże abstrahując od licznych przepisów Ustawy sankcjonujących zasady ochrony konsumenta, warto zauważyć, że kredytów konsumenckich mogą udzielać nie tylko banki, lecz również inne przedsiębiorstwa. W konsekwencji banki muszą się liczyć ze zwiększoną konkurencją w segmencie pożyczek udzielanych osobom fizycznym na cele konsumpcyjne. Może to rodzić zagrożenia ich reputacji w sytuacjach, gdy klienci zaczną transponować na nie kłopoty niewystarczająco wiarygodnych firm kredytowych. W Polsce problem ten znajduje się w ostatnim czasie na wokandzie, bowiem wiele z przedsiębiorstw kredytowych niebędących bankami albo bankrutuje, albo dokonuje malwersacji finansowych. W rezultacie klienci tracą zaufanie do wszystkich podmiotów trudniących się udzielaniem kredytów, także banków.

Reasumując, należy podkreślić, że rozwiązania światowe zmierzają ku bardziej zaawansowanym i adekwatnym metodom zarządzania ryzykiem bankowym. Panuje tendencja, by przy kalkulacji wymogów kapitałowych w większym stopniu brać pod uwagę indywidualną sytuację banku oraz obiektywne ratingi wyspecjalizowanych w ich przyznawaniu agencji. Poza tym krajowe regulacje prawne uwzględniają coraz szerszą gamę rodzajów ryzyka, stopniowo adoptując zalecenia Komitetu Bazylejskiego. Przykładowo, w najbliższej przyszłości w myśl NUKu banki będą zobligowane do zabezpieczania się przed ryzykiem operacyjnym oraz stopy procentowej w portfelu bankowym, nie zaś tylko handlowym.

[161] Jakubie, Szcześ (2002).

Polskie i europejskie prawodawstwo nie pomija specyfiki ryzyka bankowości elektronicznej. Dowodem tego są liczne uregulowania prawne traktujące o różnych aspektach tego ryzyka, jak choćby polskie ustawy oraz unijne dyrektywy odnośnie do podpisu elektronicznego, elektronicznych instrumentów płatniczych, czy usług świadczonych drogą elektroniczną.

Nie sposób zaprzeczyć, że ten stricte prawny rozdział idzie w sukurs pozytywnej weryfikacji zamieszczonych we wstępie pracy hipotez. Punkt *lex lege prim* wskazuje na fakt, że banki muszą w restrykcyjny sposób podchodzić do ryzyka, nieustannie przechodząc trzyetapową procedurę identyfikacji i pomiaru, kontroli ekspozycji oraz monitoringu ryzyka. Opisane we wzmiankowanym punkcie regulacje ostrożnościowe są identyczne dla bankowości elektronicznej i oddziałowej, lecz częstokroć ich budowa uwzględnia specyfikę e-bankingu. Z punktu *lex lege bis* wyraźnie wynika, że ryzyko bankowości elektronicznej komplikuje istotę ryzyka bankowego. Natomiast podrozdział l*ex ferenda* stanowi potwierdzenie hipotezy, że choć e-banking nie wprowadza nowego rodzaju ryzyka bankowego, to jego specyfika powoduje, że konieczne staje się doskonalenie metod zarządzania ryzykiem i tworzenie doskonalszych narzędzi temu służących.

Wszystkie punkty rozdziału dowodzą, że ryzyko bankowe jest labilne, zmienia się na skutek transformacji otoczenia banków, postępu technologicznego, globalizacji usług bankowych oraz presji konkurencyjnej. Gdyby nie pojawiły się nowe media komunikacji, jak chociażby telefon komórkowy, czy Internet, uchwalanie nowych ustaw związanych z bankowością elektroniczną – przykładowo o elektronicznych instrumentach płatniczych – nie miałoby racji bytu.

Nowe regulacje prawne są odpowiedzią na nową rzeczywistość i ujawniają zmiany w ogólnym profilu ryzyka bankowego spowodowane wpływem ryzyka e-bankingu. Należy mieć nadzieję, że zalecenia Komitetu Bazylejskiego (np. Zasady zarządzania ryzykiem w bankowości elektronicznej) będą przez banki przyjmowane.

5
Badanie percepcji ryzyka u klientów detalicznych e-bankingu

Opis problemu badawczego

Celem przeprowadzonego badania było poznanie percepcji ryzyka u klientów indywidualnych w stosunku do bankowych kanałów dystrybucji.

Po pierwsze zależało mi na sprawdzeniu z jakich kanałów klienci korzystają najczęściej oraz co powstrzymuje ich przed wykorzystaniem elektronicznych kanałów dystrybucji.

Następnie moją intencją było określenie, które elementy ryzyka związanego z użytkowaniem kanałów elektronicznych klienci uważali za wysokie bądź niskie oraz jak wyglądało porównanie tych elementów ryzyka pomiędzy bankowością elektroniczną a tradycyjną.

W dalszej kolejności zweryfikowałem stopień znajomości zabezpieczeń elektronicznych kanałów dystrybucji produktów bankowych w odczuciu respondentów oraz kwestię ich wrażliwości na ryzyko.

Na końcu zbadałem, jak respondenci widzą przyszłość kształtowania się ryzyka elektronicznych kanałów dystrybucji produktów bankowych.

Wszystkie obiekty graficzne w tym rozdziale są opracowaniem własnym.

Dane o badaniu

Badanie zostało przeprowadzone na próbie 56 osób, do których dotarłem bądź drogą elektroniczną, bądź osobiście. Ankiety rozprowadziłem też w kilku instytucjach, przykładowo w fundacji. Dobór próby miał zatem charakter nielosowy i uznaniowy.

W kwestionariuszu wykorzystałem przede wszystkim pytania dychotomiczne, politomiczne, wielokrotnego wyboru, otwarte oraz skalę Likerta i ocen – obie o podobnej budowie.

Dane demograficzne próby przedstawiają się następująco:

Tabele liczności 5, 6, 7 i 8. Wiek, płeć, zawód i wykształcenie respondentów

Kategoria	Tabela liczności: wiek	
	Liczność	Procent
19-26	37	66,07
27-35	7	12,50
pow 35	12	21,43
Braki	0	0,00

Kategoria	Tabela liczności: płeć	
	Liczność	Procent
mężczyzna	23	41,07
kobieta	33	58,93
Braki	0	0,00

Kategoria	Tabela liczności: zawód	
	Liczność	Procent
student	23	41,07
pr_budż	8	14,29
bezrobotny:	2	3,57
student+umowa zlecenie:	1	1,79
student+pr_pp:	2	3,57
pr_pp	7	12,50
student+przedsiębiorca	2	3,57
wolny zawód:	4	7,14
emerytka:	1	1,79
pr_fundacji:	6	10,71
Braki	0	0,00

Legenda:

pr_budż – pracownik sfery budżetowej
student+umowa zlecenie – student pracujący dodatkowo na umowę zlecenie
student+pr_pp – student będący jednocześnie pracownikiem przedsiębiorstwa prywatnego
student+przedsiębiorca – student pracujący jednocześnie na własny rachunek
wolny zawód – osoba wykonująca wolny zawód
pr_fundacji – pracownik fundacji

Kategoria	Tabela liczności: wykształcenie	
	Liczność	Procent
średnie	34	60,71
wyższe	22	39,29
Braki	0	0,00

W badaniu wzięły udział przede wszystkim osoby młode, o czym świadczy wysoki procent uczestników w przedziale wiekowym 19-26 lat wynoszący aż 66%, a więc 2/3. Jednakże starałem się uzyskać opinię także ludzi starszych i stąd 21,5 % osób w przedziale wiekowym powyżej 35 lat.

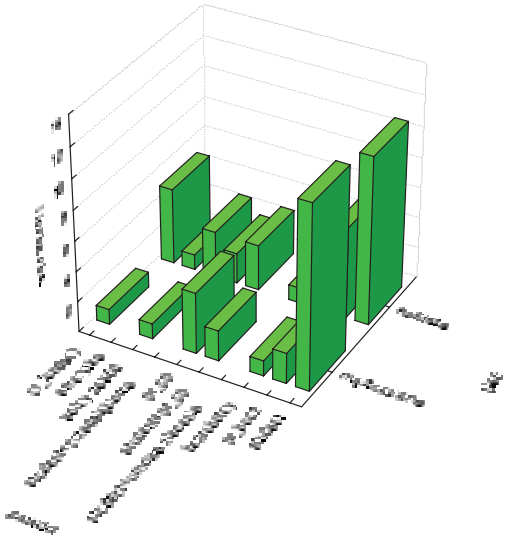
Odpowiedzi udzieliła nieco większa liczba kobiet (58%).

W przekroju zawodu na pierwszym miejscu znaleźli się studenci (41 % próby).

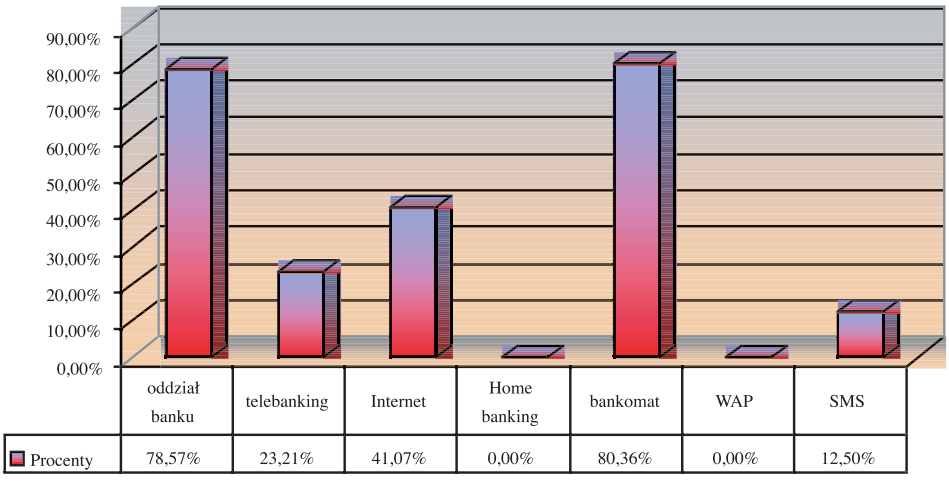
Respondenci ankiety zaliczają się do osób wykształconych (60% – wykształcenie średnie, 40% – wyższe).

W przekroju płeć – zawód rozkłady są dość równomierne. Nieznacznie więcej mężczyzn studiuje, a także studiuje i jednocześnie pracuje w przedsiębiorstwie prywatnym. Natomiast wśród kobiet – więcej jest pracowników fundacji, wykonujących wolny zawód oraz pracowników budżetowych.

Histogram dwu zmiennych 1.: Płeć i zawód



Wykres 1. Procent respondentów korzystających z danego kanału dystrybucji



	oddział banku	telebanking	Internet	Home banking	bankomat	WAP	SMS
Procenty	78,57%	23,21%	41,07%	0,00%	80,36%	0,00%	12,50%

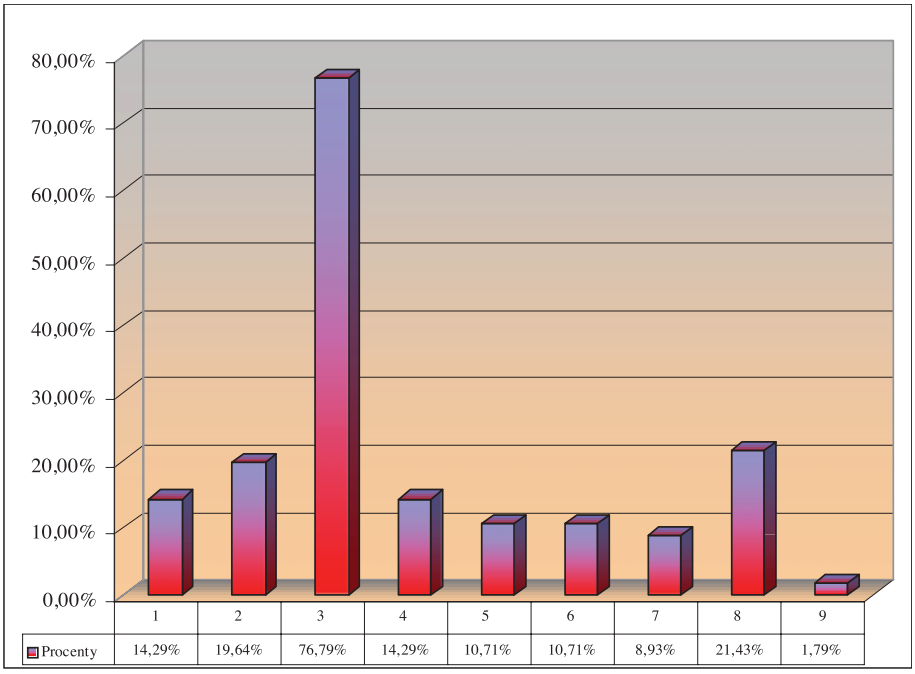
Zgodnie z moimi oczekiwaniami najczęściej wykorzystywanym kanałem był oddział banku i bankomat. Korzystało z nich po około 80% badanych osób. Na drugim miejscu znalazł się Internet (41%), a na trzecim telebanking, za którego pośrednictwem łączył się z bankiem co czwarty badany. Niestety, WAP i home banking nie znalazły klientów. SMSu jako kanału dystrybucji używał co dziesiąty respondent.

W grupie powyżej 35 lat aż 92% wybrało oddział banku, a tylko 17% Internet, przy 33% dla telebankingu i 66% dla bankomatu. Natomiast w grupie poniżej 35 lat 47% korzysta z Internetu, 84% z bankomatu, ale tylko 20% z telebankingu, co wydaje się niespodzianką. W tej grupie 75% wybrało oddział banku. Rozkład procentowy dla kanału SMSowego wygląda podobnie w obu grupach.

Zainteresowało mnie, czy można stwierdzić, że Internet jest alternatywą dla oddziału banku. Z analizy porównawczej klientów oddziału i Internetu wynika, że 15 osób na 56 korzystało jednocześnie z obu kanałów, a więc 26,7%. Zatem z dużym prawdopodobieństwem potwierdza to moją hipotezę. Jednocześnie widać, że bankomat jest kanałem komplementarnym w stosunku do pozostałych. Klienci, niezależnie od preferencji wyboru Internetu lub oddziału banku za podstawową drogę kontaktu, korzystają z bankomatu – 80% wszystkich klientów.

Zadałem sobie też pytanie, czy studenci, jako grupa najbardziej otwarta na wszelkie innowacje technologiczne, wybiera w przeważającej mierze elektroniczne kanały dystrybucji produktów bankowych. Grupa studentów stanowi niespełna połowę respondentów. Okazuje się, że 78% studentów wybrało oddział i bankomat, 43% – Internet, a więc wyniki są zbliżone do całości próby. Natomiast tylko 17% skorzystało z telebankingu (o 6% mniej od wszystkich respondentów) oraz 8% z SMSów (o 4,5% mniej od wszystkich respondentów). Pokazuje to więc, że studenci nawet trochę częściej używają tradycyjnych kanałów dystrybucji niż pozostali ankietowani.

Wykres 2. Powody powstrzymujące klientów przed wykorzystaniem elektronicznych bankowych kanałów dystrybucji



Objaśnienia do wykresu:
1 – Brak dostępu do danego kanału
2 – Brak zaufania do tej formy kontaktów z bankiem
3 – Brak potrzeby
4 – Brak umiejętności korzystania z usługi
5 – Zbyt wysoki koszt usługi
6 – Przeświadczenie, że obsługa w oddziale jest lepsza
7 – Trudności i niedogodności techniczne
8 – Lenistwo
9 – Inne

Powyższy wykres pozwala jednoznacznie stwierdzić, że najważniejszym powodem powstrzymującym badanych przed wykorzystaniem elektronicznych bankowych kanałów dystrybucji jest brak potrzeby (77% wskazań). Drugi w kolejności powód to lenistwo, które wybrało 21,5% respondentów. Tuż za nim plasuje się brak zaufania do tej formy kontaktów z bankiem (19,5%). Pozostałe powody zebrały od 9 do 14% wskazań (prócz kategorii inne). Kategoria inne została wybrana przez jedną osobę, która zdefiniowała powód powstrzymujący ją przed wykorzystaniem elektronicznych bankowych kanałów dystrybucji jako brak czasu na zapoznanie się z tymi kanałami.

W przekroju zawodowym nie widać większych odchyleń od próby.

Istnieją jednak pewne różnice dla przekroju wiekowego (powyżej 35 lat i poniżej). Brak dostępu do danego elektronicznego kanału deklaruje o około 14% więcej respondentów starszych. Podobnie zaufaniem nie darzy tej formy kontaktów z bankiem o 18% więcej osób powyżej 35 roku życia. Także o 7% więcej osób z tej grupy żywi przekonanie, że obsługa w oddziale jest lepsza. W pozostałych kategoriach (z wyjątkiem inne) tendencja jest o dziwo odwrotna. Wśród osób młodych jest o 6% więcej osób leniwych. 11% więcej respondentów z tej grupy widzi problem w trudnościach i niedogodnościach technicznych kanału dystrybucji, przy czym tego problemu nie dostrzega żadna osoba starsza. Nie czuje potrzeby korzystania z elektronicznych kanałów dystrybucji o 13% więcej osób z próbki poniżej 35 lat. Dla osób młodszych większy kłopot stanowią również: brak umiejętności korzystania z usługi oraz jej zbyt wysoki koszt (odpowiednio różnica na niekorzyść młodszej grupy – 7 i 13,5%).

W przekroju płci różnice w powodach niekorzystania z elektronicznych kanałów dystrybucji produktów bankowych nie przekraczają 5%.

Czy bankowość tradycyjna jest bezpieczniejsza od elektronicznej? (na podstawie pytania nr 3 – skala Likerta)

Pytanie zostało postawione w sposób następujący: Czy zgadza się Pan/Pani, że bankowość tradycyjna (oddziałowa) jest bezpieczniejsza od bankowości elektronicznej (skala od 1 do 5)?

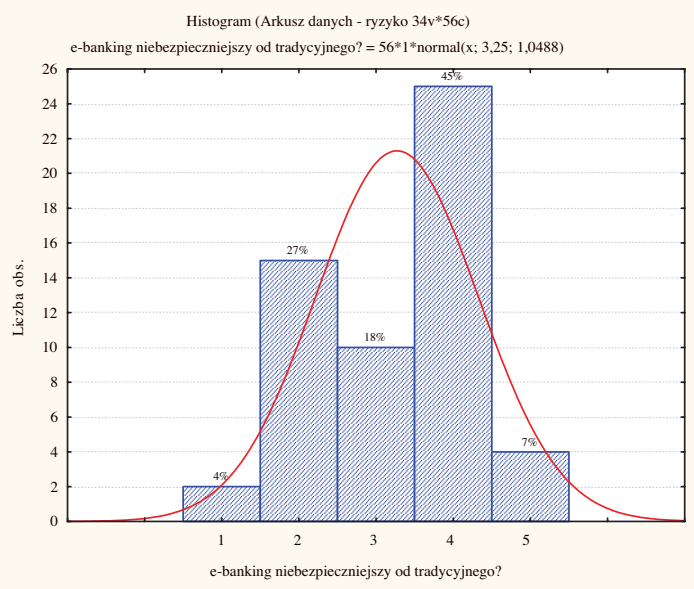
Tabela 9. Statystyki opisowe do pytania nr 3

Średnia	Ufność -95,00%	Ufność +95,00%	Mediana	Moda	Odchylenie standardowe	Skośność	Kurtoza
3,25	2,97	3,53	4	4	1,04	-0,33	-0,94

Średnia arytmetyczna wymyka się prostej interpretacji ze względu na kształt rozkładu odpowiedzi (wartość 3,25). Duże odchylenie standardowe wskazuje, że respondenci mieli często odmienne zdania, co zresztą widać na histogramie, który jest bimodalny. Prawie 45% badanych (dominanta) odpowiedziało, że zgadza się z twierdzeniem, że bankowość tradycyjna jest bezpieczniejsza od elektronicznej. Drugą dominantą (27% odpowiedzi) była odpowiedź przeciwna. Tylko 18% osób nie widziało istotnej różnicy w ryzyku pomiędzy tymi dwoma rodzajami kanałów dystrybucji – tradycyjnym i elektronicznym.

Nie mniej niż 50% ankietowanych – mediana – przyznało, że bankowość tradycyjna jest bezpieczniejsza od elektronicznej. Współczynnik skośności dowodzi lewostronnej asymetrii, a Kurtoza – spłaszczenia rozkładu, jednakże ich istotność statystyczna jest znikoma w obliczu bimodalnego rozkładu. Należy jeszcze dodać, że z prawdopodobieństwem 95% średnia w populacji znalazłaby się w przedziale (2,97; 3,53). Błąd standardowy wyniósł 0,14, błędy skośności i Kurtozy odpowiednio po 0,32 i 0,63.

Histogram 2. E-banking niebezpieczniejszy od tradycyjnego?



Ryzyko zagregowane bankowości elektronicznej w porównaniu z tradycyjną.

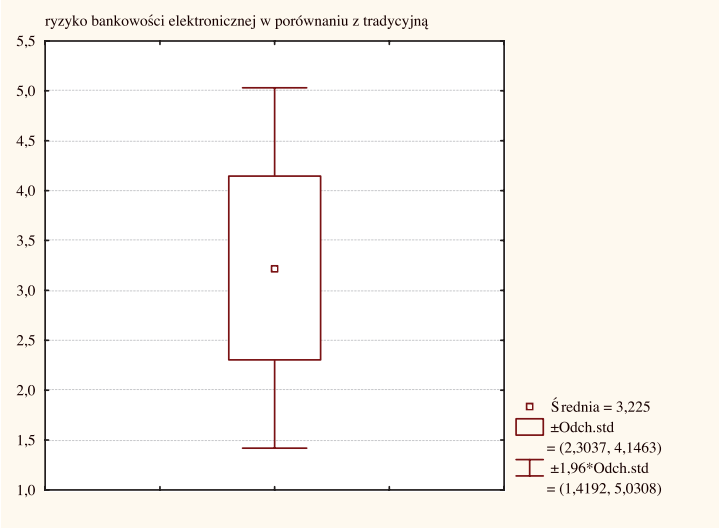
Pytanie 5 kwestionariusza jest podzielone na podpunkty, które zawierają porównanie poszczególnych aspektów ryzyka bankowości elektronicznej i tradycyjnej. Odpowiedzi 1, 2 oznaczają, że to ryzyko jest niższe w elektronicznej, a 4 i 5 – że wyższe. Jest to typowa skala ocen.

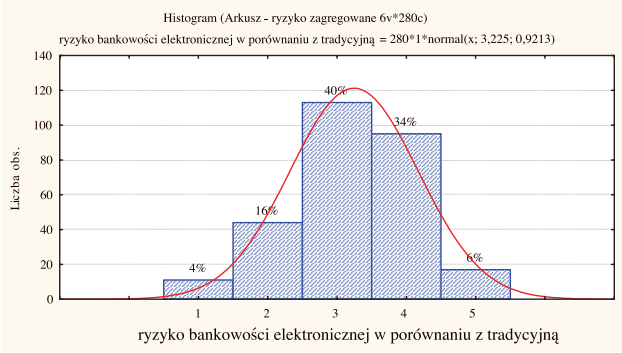
Dokonałem agregacji poszczególnych podpunktów, otrzymując 280 elementów w próbie (5x56).

Wyniki pomiaru ryzyka zagregowanego pozwolą mi zweryfikować prawdziwość wniosków otrzymanych z analizy pytania 3 (skala Likerta).

Tabela 10. Statystyki opisowe dla zagregowanego pytania nr 5, Pudełko z wąsami 1. Ryzyko bankowości elektronicznej w porównaniu z tradycyjną, Histogram 3. Ryzyko bankowości elektronicznej w porównaniu z tradycyjną

Średnia	Ufność -95,00%	Ufność +95,00%	Mediana	Moda	Odchylenie standardowe	Skośność	Kurtoza
3,22	3,11	3,33	3	3	0,92	-0,29	-0,12





Bankowość elektroniczna w odczuciu ankietowanych jest nieznacznie bardziej niebezpieczna od tradycyjnej (średnia równa 3,22). Tak twierdzi 40% badanych w porównaniu do 20% zdań przeciwnych. Aż 40% (mediana i moda) ocenia ryzyka na tym samym poziomie. Rozkład cechy przypomina w dużym stopniu rozkład normalny. Zróżnicowanie jest spore (*vide Box and Whisker plot*), zwłaszcza w obszarze środkowym, a więc dwóch centralnych kwartyli. Świadczy o tym długi korpus pudełka z wąsami i odchylenie standardowe rzędu 0,92. Rozkład przybrał postać lewostronnie asymetrycznego (skośność równa –0,29) i lekko spłaszczonego (Kurtoza równa –0,12). Dzięki licznej próbie średnia w przybliżeniu odpowiada średniej w populacji (błąd standardowy tylko 0,05).

Okazuje się, że otrzymaliśmy podobny wynik jak w pytaniu nr 3. Ryzyko w bankowości elektronicznej jest wyższe niż w bankowości tradycyjnej.

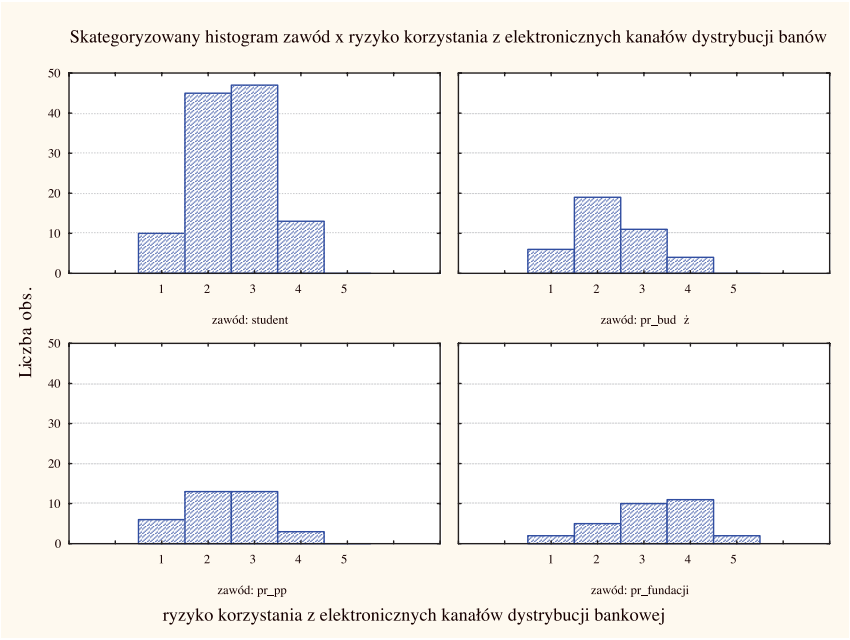
Łączne ryzyko korzystania z elektronicznych kanałów dystrybucji produktów bankowych (agregacja wyników do pytania nr 4 – w próbie znalazło się 280 elementów).

Tabela 11. Statystyki opisowe do zagregowanego pytania nr 4

Średnia	Ufność -95,00%	Ufność +95,00%	Mediana	Moda	Odchylenie standardowe	Skośność	Kurtoza
2,57	2,46	2,66	3	3	0,90	0,21	-0,18

Łączne ryzyko, jak wynika z badań, znajduje się poniżej średniego (średnia 2,57). Cztery najliczniejsze grupy wśród respondentów odpowiadały następująco:

Histogram skategoryzowany 4.

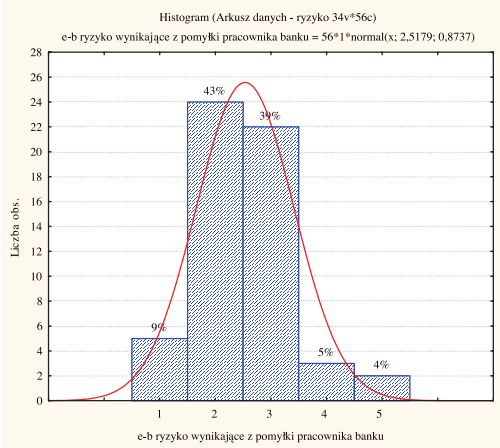


Najbardziej sceptyczni wobec bezpieczeństwa elektronicznych kanałów dystrybucji byli pracownicy fundacji. Pracownicy budżetowi natomiast w przeważającej części opowiedzieli się za opcją niskiego ryzyka w bankowości elektronicznej.

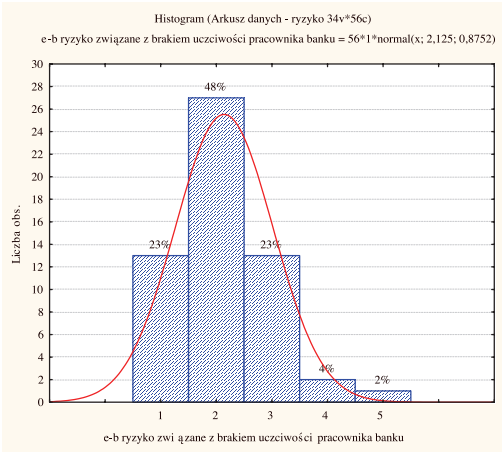
Teraz zwrócę uwagę na interesujące aspekty poszczególnych elementów ryzyka w elektronicznych kanałach dystrybucji oraz przy porównaniu bezpieczeństwa elektronicznych kanałów z tradycyjnymi.

Ryzyko wynikające z pomyłki oraz braku uczciwości pracownika banku w bankowości elektronicznej w porównaniu do bankowości tradycyjnej (pytania: 4 i 5)

Histogram 5. Ryzyko wynikające z pomyłki pracownika banku w bankowości elektronicznej



Histogram 6. Ryzyko związane z brakiem uczciwości pracownika banku w bankowości elektronicznej



Oba wykresy są silnie leptokurtyczne (Kurtoza w granicach 1). Średnia w ryzyku związanym z brakiem uczciwości pracownika banku oscyluje wokół 2,12, w ryzyku wynikającym z pomyłki pracownika – wokół 2,51. Oba wykresy są prawostronnie asymetryczne (skośność około 0,6 do 0,8). Można zatem na tej podstawie wysnuć wniosek, że klienci indywidualni ufają pracownikom banku. Tym niemniej uważają, że bankowość elektroniczna jest pod tym względem bezpieczniejsza (średnia dla porównania tych dwóch rodzajów ryzyka w bankowości elektronicznej z tradycyjną wynosi około 2,8).

Bankowość elektroniczna versus tradycyjna w ryzyku wynikającym z własnej pomyłki, zawodności technicznej kanału dystrybucji oraz wynikającym z możliwości złożenia zlecenia przez osobę nieupoważnioną.

Respondenci ocenili, że dla tych trzech elementów ryzyko bankowości elektronicznej jest wyższe niż tradycyjnej. W szczególności ryzyko zawodności technicznej elektronicznych kanałów dystrybucji produktów bankowych zostało wysoko oszacowane w porównaniu z tradycyjnym (średnia 3,55).

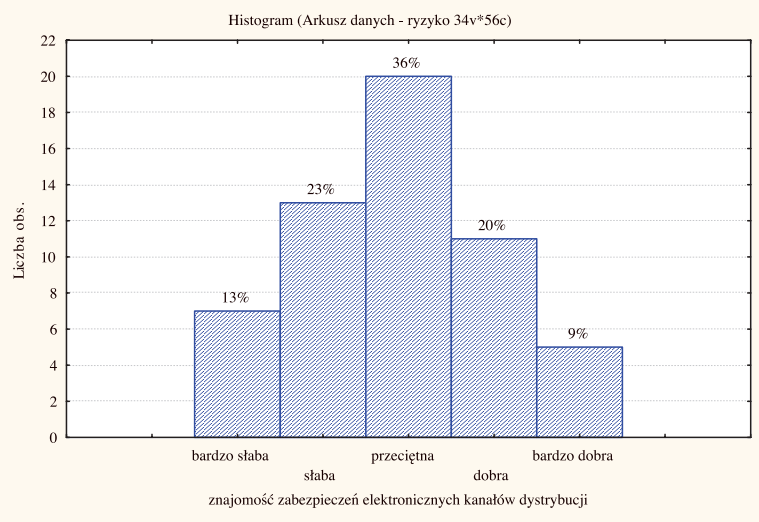
Rzetelność pomiaru dla pytań: trzeciego, czwartego i piątego

```
Liczba pozycji na skali: 11

             Liczba ważnych przyp.: 56
   Liczba przypadków z brak. danych: 0
             Braki danych usuwano: przypadk.

                    PODSUMOWANIE STATYSTYK SKALI
               Śred:32,232142857                Suma: 1805,0000000
   Odchylenie stand.: 5,774524212           Wariancja: 33,345129870
          Skośność: -,036910764              Kurtoza:   ,808017029
           Minimum:17,000000000           Maksimum: 46,000000000
     Alfa Cronbacha:   ,812969436   Alfa standaryzow.:   ,808650869
                       Średnia kor. między pozycjami:   ,284370808

1. połowa          2. połowa

     Liczba pozycji:      6                5
            Średnia: 18,303571429        13,928571429
               Suma: 1025,0000000        780,00000000
     Odchylenie std.  3,582379315         2,655061327
          Wariancja: 12,833441558         7,049350649
     Alfa Cronbacha:   ,737905735          ,583433125

 Korelacja między pierwszą i drugą połową:     ,707692117
     Korel. skoryg. ze wzgl. na tłumienie:        --

                   Rzetelność połówkowa:     ,828828698
             Rzetelność połówkowa Guttmana:  ,807454505
```

Powyższa analiza ilustruje fakt, że dane skale mierzą to samo, czyli że kolejne pytania stawiane osobie ankietowanej dały wyniki zbliżone. Wartości współczynników alfa Cronbacha, alfa Cronbacha standaryzowanego oraz rzetelności połówkowej i rzetelności połówkowej Guttmana wyniosły około 0,8 (sporo powyżej progu akceptowalności).

Stopień znajomości zabezpieczeń elektronicznych kanałów dystrybucji produktów bankowych w odczuciu respondentów.

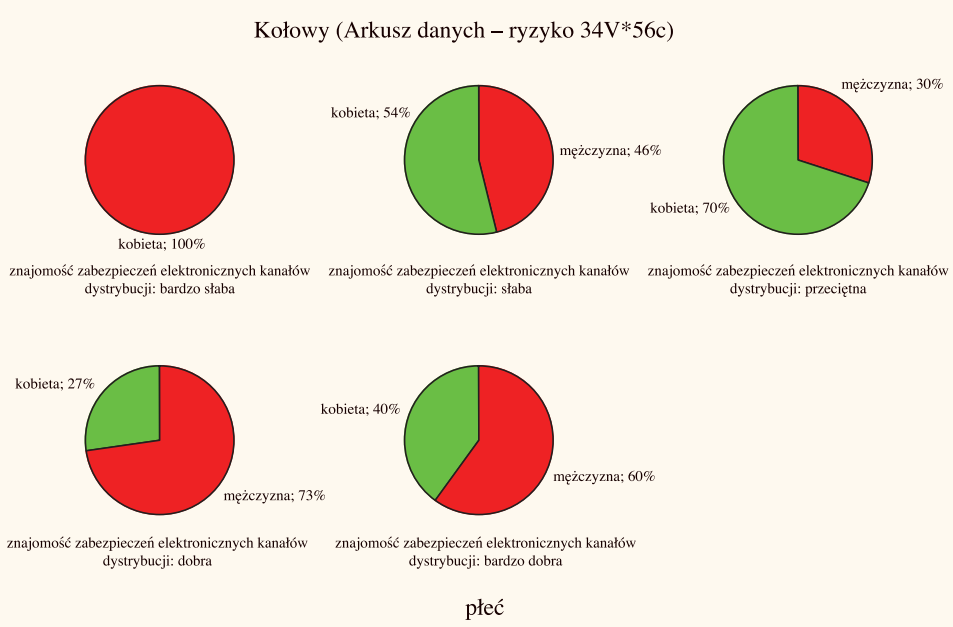
Histogram 7. Znajomość zabezpieczeń elektronicznych kanałów dystrybucji



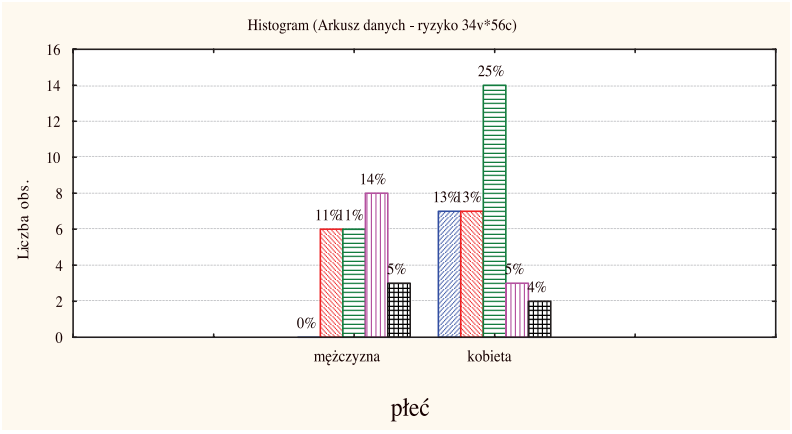
Histogram jest prawostronnie asymetryczny. Respondenci oceniają w większości swoją znajomość zabezpieczeń elektronicznych kanałów dystrybucji produktów bankowych jako przeciętną lub poniżej przeciętnej (70% wskazań). Tylko 30% określiło swoją wiedzę jako dobrą i bardzo dobrą.

Przy kategoryzacji ze względu na płeć wyniki wyglądają ciekawiej.

Wykres 3. (kołowy skategoryzowany ze względu na pleć)
Znajomość zabezpieczeń elektronicznych kanałów dystrybucji



Histogram 8. (skategoryzowany ze względu na płeć)
Znajomość zabezpieczeń elektronicznych kanałów dystrybucji
Słupki kolejno: znajomość zabezpieczeń elektronicznych kanałów dystrybucji: bardzo słaba



znajomość zabezpieczeń elektronicznych kanałów dystrybucji: słaba
znajomość zabezpieczeń elektronicznych kanałów dystrybucji: przeciętna
znajomość zabezpieczeń elektronicznych kanałów dystrybucji: dobra
znajomość zabezpieczeń elektronicznych kanałów dystrybucji: bardzo dobra

Okazuje się, że kobiety są zdecydowanie bardziej krytyczne wobec swojej wiedzy. Żaden mężczyzna nie przyznał się do bardzo słabej znajomości tematu. Dominanta w podzbiorze mężczyzn (35% odpowiedzi tego podzbioru) przypadła na wskazanie dobra (14% całej próby). W podzbiorze kobiet zaś moda liczyła 42% odpowiedzi i przypadła na wskazanie przeciętna (25% całej próby). Prawie połowa mężczyzn określiła swoją wiedzę jako dobrą lub bardzo dobrą w porównaniu do 17% kobiet (odpowiednio: 19% i 9% całej próby).

Wrażliwość respondentów na ryzyko

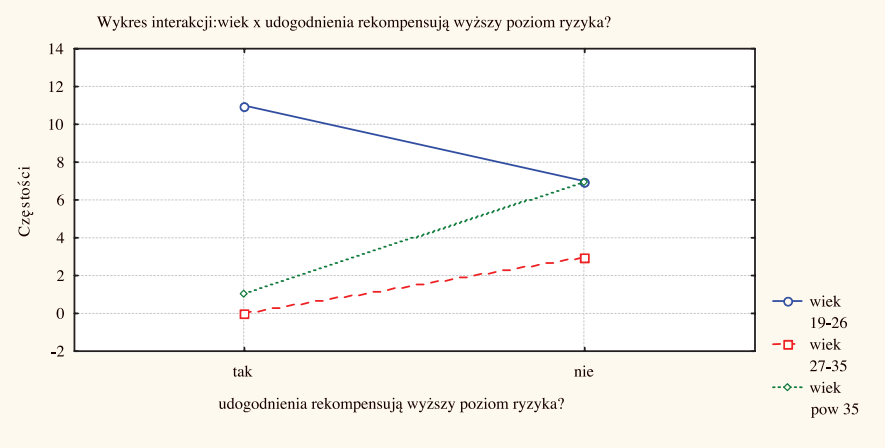
Tabela liczności 12.

Kategoria	Tabela liczności: udogodnienia rekompensują wyższy poziom ryzyka	
	Liczność	Procent
tak	12	41,38
nie	17	58,62
Braki	0	0,00

59% tej grupy ankietowanych, którzy zdefiniowali w pytaniu 3 ryzyko elektronicznych kanałów dystrybucji produktów bankowych jako wyższe od ryzyka kanałów tradycyjnych, stwierdziło że żadne udogodnienia nie są w stanie zrekompensować im tego ryzyka. Sprowadza się to do konstatacji, że póki będą oni postrzegać wspomniane kanały dystrybucji jako niebezpieczne, póty nie będą z nich korzystać i żadne udogodnienia w postaci możliwości wyboru elektronicznego kanału dystrybucji produktów bankowych, dowolnego kształtowania miejsca i czasu korzystania z usług bankowych oraz brak strat czasu związanych z oczekiwaniem na obsługę nie są w stanie ich do tego zachęcić.

Uznałem za warte zachodu, by sprawdzić czy wiek respondentów miał wpływ na taką odpowiedź.

Wykres interakcji 4. Wiek x udogodnienia rekompensują wyższy poziom ryzyka?



Wykres interakcji pokazuje dobitnie, że wiek miał tu duży wpływ. 61% osób z przedziału 19-26 lat, które stanowią 38% całości próbki adekwatnej do tego pytania byłoby skłonne zdeprecjonować ryzyko za pewne udogodnienia. Natomiast 100% osób z przedziału środkowego oraz 88% osób z przedziału powyżej 35 lat, gdzie obie podgrupy stanowią łącznie 39% subpróby, podało że żadne udogodnienia nie zrekompensują im wyższego ryzyka.

Przyszłość kształtowania się ryzyka elektronicznych kanałów dystrybucji produktów bankowych

Tabela 13. Przyszłość ryzyka bankowości elektronicznej

Kategoria	Tabela liczności: przyszłość ryzyka w e-b	
	Liczność	Procent
a	28	50,00
b	24	42,86
c	4	7,14
Braki	0	0,00

Legenda:

a – ryzyko e-bankingu zmaleje

b – ryzyko e-bankingu pozostanie na tym samym poziomie

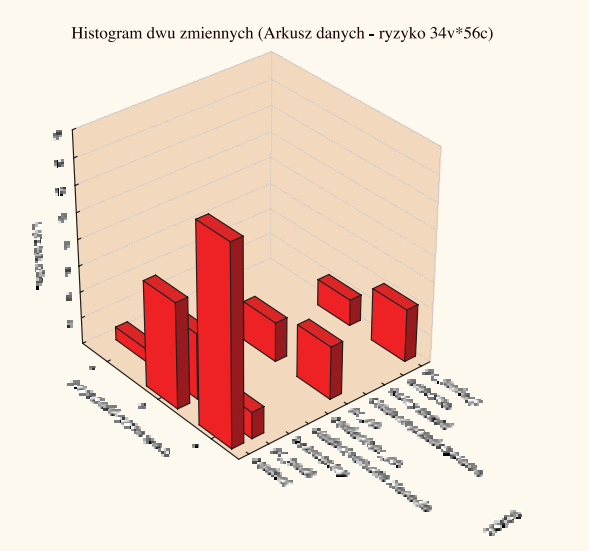
c – ryzyko e-bankingu wzrośnie

Dokładnie 50% ankietowanych odpowiedziało, że ryzyko elektronicznych kanałów dystrybucji produktów bankowych w przyszłości będzie się zmniejszać na skutek zastosowania coraz doskonalszych technologii i systemów. 43% orzekło, że to ryzyko pozostanie mniej więcej na tym samym poziomie co obecnie, gdyż redukcji zagrożeń w jednych obszarach będą towarzyszyć wzrosty zagrożeń w innych. Tylko 7% okazało się pesymistami twierdząc, że ryzyko związane z korzystaniem z elektronicznych kanałów dystrybucji produktów bankowych wzrośnie. W ich opinii ryzyko zwiększy się, ponieważ wzrosną umiejętności hakerów, zwłaszcza że poprzez upowszechnienie się wykorzystywania elektronicznych kanałów dystrybucji będą oni mieli większą możliwość nabycia doświadczenia i poszerzenia zakresu swych umiejętności.

Sprawdziłem, jakie miały odczucia w tej kwestii cztery najbardziej liczne podgrupy badanych.

2/3 studentów oraz pracowników fundacji jest zdania, że ryzyko zmaleje. Także 57% pracowników przedsiębiorstwa prywatnego podziela ten pogląd. Z kolei prawie 63% pracowników budżetowych sądzi, że poziom ryzyka się nie zmieni w przyszłości, a 12,5% tej grupy zakłada jego wzrost.

Histogram dwu zmiennych 9. Zawód x przyszłość ryzyka w bankowości elektronicznej



Wnioski syntetyczne z przeprowadzonej ankiety

Najczęściej wykorzystywanym kanałem dystrybucji w opinii badanych jest oddział banku i bankomat (po około 80% wskazań). Internet wykorzystuje 41% ankietowanych. Można też przyjąć, że jest on alternatywą dla oddziału.

Najważniejszym powodem powstrzymującym respondentów przed wykorzystaniem elektronicznych kanałów dystrybucji jest brak potrzeby (80% wskazań), zaś drugim w kolejności lenistwo (21,5% wskazań).

Ryzyko elektronicznych kanałów dystrybucji produktów bankowych jest w odczuciu badanych nieco wyższe, aczkolwiek niewiele, niż tradycyjnych. W trzech przekrojach: w ryzyku wynikającym z własnej pomyłki, zawodności technicznej kanału dystrybucji oraz wynikającym z możliwości złożenia zlecenia przez osobę nieupoważnioną, zostało ono ocenione na poziomie wyższym dla bankowości elektronicznej niż dla tradycyjnej; w dwu pozostałych: w ryzyku wynikającym z pomyłki oraz braku uczciwości pracownika banku w bankowości elektronicznej, na poziomie niższym.

Respondenci określili ryzyko korzystania z elektronicznych kanałów dystrybucji produktów bankowych jako niskie, zwłaszcza jeden jego element, wynikający z braku uczciwości pracownika banku.

Stopień znajomości zabezpieczeń elektronicznych kanałów dystrybucji produktów bankowych w odczuciu respondentów jest raczej przeciętny lub niski. Kobiety są zdecydowanie bardziej krytyczne w stosunku do swojej wiedzy niż mężczyźni.

W kwestii wrażliwości na ryzyko należy zaznaczyć, że większości respondentów udogodnienia wynikające z natury elektronicznych kanałów dystrybucji produktów bankowych nie rekompensują wysokiego w ich opinii ryzyka towarzyszącemu użytkowaniu tych kanałów. Jednakże w grupie osób młodszych z przedziału 19-26 lat, studentów panuje odwrotna tendencja.

Dokładnie połowa ankietowanych twierdzi, że ryzyko korzystania z elektronicznych kanałów dystrybucji produktów bankowych w przyszłości spadnie. Ponad 40% uważa, że się nie zmieni, zaś jedynie 7% – że wzrośnie.

Wyniki ankiety nie są reprezentatywne dla całej populacji. Dobór próby miał charakter nielosowy i uznaniowy, liczba obserwacji wyniosła tylko 56, respondenci mieli średnie i wyższe wykształcenie, mieszkali w Warszawie i 41% z nich stanowili studenci.

6
Zakończenie

Finis coronat opus… lecz nie w tej pracy. Jestem głęboko przekonany, że jest ona jedynie wierzchołkiem tematu ryzyka bankowości elektronicznej i jego specyfiki. Tym niemniej wierzę, że udało mi się osiągnąć zamierzony cel – ukazać specyfikę bankowości elektronicznej i zweryfikować zamieszczone we wstępie hipotezy.

Nie zidentyfikowałem nowego rodzaju ryzyka bankowości elektronicznej, który by nie występował w bankowości oddziałowej. Natomiast udowodniłem, że tradycyjne ryzyka nabierają odmiennego charakteru w bankowości elektronicznej na skutek jej specyfiki, postępu technologicznego, globalizacji usług bankowych oraz nieustannej presji konkurencyjnej. Wykazałem również, że ryzyka: operacyjne, prawne i reputacji są istotne, zaś ryzyko e-bankingu zmienia ogólny profil ryzyka bankowości.

Bez wątpienia banki, by sprostać nowym wyzwaniom, muszą znać ten profil, a mogą to uczynić jedynie poprzez ciągłe przechodzenie procedury, na którą składają się trzy etapy: identyfikacja, pomiar i kontrola ekspozycji oraz monitoring ryzyka.

Wielokanałowość (*multichanneling*) stał się koniecznością. Bank, który chce zachować lub zdobyć silną pozycję na rynku, nie może pozostać pasywny i zrezygnować z rozwijania elektronicznych kanałów dystrybucji. Do tego zaś potrzebne mu są wykwalifikowane służby potrafiące kontrolować i zarządzać ryzykiem wszystkich kanałów. Nie oznacza to jednak, że jest to zadanie proste, wręcz przeciwne – nastręcza poważnych trudności, choćby ze względu na fakt, że te same rodzaje ryzyka bankowości tradycyjnej (oddziałowej): kredytowe, stopy procentowej, rynkowe, płynności nabierają odmiennego charakteru w kanałach elektronicznych.

W zakończeniu każdego z rozdziałów zostały zebrane wnioski i argumenty przemawiające za prawdziwością hipotez. W najobszerniejszym rozdziale trzecim (ryzyka e-bankingu) znalazła się większość dowodów potwierdzająca hipotezy: główną, roboczą nr 1 i nr 3. Hipoteza robocza nr 2 została najpełniej zweryfikowana w rozdziale ostatnim (badania ankietowe), we wstępie i rozdziale pierwszym. W rozdziale czwartym ujęto badane zagadnienie od strony prawnej, zwracając uwagę na przyszłe zmiany prawne w kontekście ryzyka bankowego i postęp, jaki zachodzi w tym obszarze.

Przykładowo można wskazać, w jaki sposób hipotezy zostały udowodnione. W pierwszym rozdziale pokazano, że wszystkie kanały elektroniczne różnią się między sobą, zaś korzystanie z nich wymaga używania pewnych narzędzi (np. kart elektronicznych), które nie zawsze gwarantują pełne bezpieczeństwo. W rozdziale trzecim opisano rzeczywiste ataki na e-banki jako przykład ryzyk: operacyjnego, prawnego i reputacji, problemy outsourcingu, transgranicznego charakteru bankowości elektronicznej i pieniądza elektronicznego, podpis cyfrowy i Infrastrukturę Klucza Publicznego. Uwypuklona została rola technologii i nakreślone różnice w otoczeniu bankowości elektronicznej i tradycyjnej. Obie grupy czynników bezpośrednio wpływają na specyfikę bankowości elektronicznej.

Przez wskazanie takich problemów jak: prędkość dyfuzji informacji w Nowej Gospodarce, anonimowość klientów e-bankingu i trudności w ocenie ich wiarygodności, rozwój nowych produktów oferowanych przez podmioty niebankowe, różnice w regulacjach prawnych poszczególnych jurysdykcji, itp. udowodniono, że ryzyko bankowości elektronicznej komplikuje istotę ryzyka bankowego. Z kolei potwierdzeniem tego, że ryzyka bankowości tradycyjnej nabierają odmiennego charakteru w kanałach elektronicznych, były m.in. przeanalizowane zjawiska: przyspieszonego obrotu pieniężnego, większej zmienności stanu depozytów i cen papierów warto-

ściowych, efektywności finansowych rynków wirtualnych, presji na szybsze wykonywanie operacji, imperatywu działania non-stop, itp.

Perspektywa, z której spojrzałem na ryzyko, miała być w zamierzeniu przede wszystkim perspektywą banku. Jednak w toku pracy okazało się, że bardzo często ryzyko banku jest tożsame z ryzykiem klienta. Przykładowo ataki hakerów, będące źródłem ryzyk: operacyjnego, prawnego i reputacji, rodzą konsekwencje dla obu stron. Natomiast odpływ klientów z banku, spowodowany utratą przez niego reputacji na skutek włamań do systemu elektronicznego, może mu przeszkodzić w osiągnięciu zysku. Według wszelkiego prawdopodobieństwa efektem tego po pewnym czasie będą kłopoty banku z płynnością, a w skrajnym przypadku nawet bankructwo. Dlatego bank jako instytucja zaufania publicznego powinien być świadom tego, że bezpieczeństwo klienta i jego percepcja ryzyka bankowego są priorytetem.

Przeobrażenia w środowisku banku, zaostrzająca się konkurencja ze strony parabanków, choćby takich jak podmioty zajmujące się agregacją usług finansowych oraz coraz szerszy zakres usług bankowych implikują zmiany ryzyka. Bywa, że są one bardzo nagłe i nieprzewidywalne, zaś wiele z nowych aspektów ryzyka okazuje się niezwykle trudnymi do kwantyfikacji. Ponadto, te same rodzaje ryzyka w różnych bankach, w zależności od ich indywidualnej sytuacji posiadają odmienny wpływ na ogólny profil ryzyka każdego z banków. Z tego powodu uznaję za słuszne zapisy Nowej Umowy Kapitałowej, która pozwala instytucjom kredytowym na wykształcenie własnych metod pomiaru ryzyka. Moim zdaniem rola Komitetu Bazylejskiego w tym obszarze jest nie do przecenienia i dobrze się dzieje, że właśnie to gremium proponuje krajom właściwe rozwiązania. Mechanizm działania Komitetu Bazylejskiego gwarantuje adekwatność tworzonych przez niego zaleceń, bowiem są one efektem dogłębnych analiz dokonywanych przez banki i władze nadzorcze z całego świata.

Uważam, że warto by było przeprowadzić dalsze badania ryzyka bankowości elektronicznej. Można by, na przykład, przy użyciu metod ilościowych porównać poziom ryzyka bankowego w przekroju poszczególnych jego rodzajów w banku wirtualnym i tradycyjnym. Być może okazałoby się, że istnieją pewne różnice. W Polsce jest to o tyle trudne, że wszystkie banki wirtualne działające na rynku są wydzielonymi tworami większych jednostek macierzystych (mBank – BRE Banku SA, Inteligo – PKO BP SA, Volkswagen Bank Direct – Volkswagen Banku Polska SA), które zarządzają ryzykiem zagregowanym i nie czynią dystynkcji między poszczególnymi kanałami dystrybucji. Pytanie czy jest to słuszne podejście.

W trakcie pisania pracy zrozumiałem, że moja wiedza o ryzyku bankowym jest bardzo wąska. Postęp w tej dziedzinie jest nadzwyczaj szybki. W zarządzaniu ryzykiem znajdują zastosowanie coraz bardziej skomplikowane i zmatematyzowane modele, rośnie znaczenie sekurytyzacji i derywatów, których *nota bene* wciąż powstają nowe rodzaje i mutacje. Pojąłem, że zarządzanie ryzykiem banku jest w istocie kluczową funkcją. Ten kto ją pełni, określa strategię banku i podejmuje najważniejsze decyzje. Wynika to z faktu, że w instytucji zaufania publicznego, która zajmuje się transformacją ryzyka, zarządzanie tym ryzykiem ma kardynalne znaczenie.

7
Załącznik

Ankieta została przygotowana przez Jakuba Górkę.

Jest ona całkowicie anonimowa, jej celem jest zbadanie percepcji ryzyka klientów detalicznych w stosunku do bankowych kanałów dystrybucji.

Czas starannego wypełnienia ankiety wynosi 5-10 minut.

Ankieta zostanie wykorzystana do celów naukowych.

Zachęcam do starannego wypełnienia kwestionariusza, gdyż może to uświadomić Państwu własny stosunek do korzystania z różnych bankowych kanałów dystrybucji.

Sposób odpowiedzi na pytania jest dowolny (np. przez zmianę koloru lub podkreślenie).

Wypełnione ankiety proszę przesyłać na adres j_gorka21@hotmail. com lub wood_elf@op. pl

Uprzejmie dziękuję!!!

Kwestionariusz ankietowy

1. Z jakich kanałów dystrybucji produktów (usług) bankowych Pan/Pani korzysta?

- ☐ Oddział banku
- ☐ Telebanking (usługi świadczone przez telefon)
- ☐ Internet
- ☐ Home banking (łącze prywatne)
- ☐ Bankomat
- ☐ WAP
- ☐ SMS

2. Jeżeli nie korzysta Pan/Pani, z któregoś z bankowych kanałów dystrybucji elektronicznej, to powodem tego jest (można zaznaczyć dowolną liczbę):

- ☐ Brak dostępu do danego kanału
- ☐ Brak zaufania do tej formy kontaktów z bankiem
- ☐ Brak potrzeby
- ☐ Brak umiejętności korzystania z usługi
- ☐ Zbyt wysoki koszt usługi
- ☐ Przeświadczenie, że obsługa w oddziale jest lepsza
- ☐ Trudności i niedogodności techniczne wynikające z niezadowalającego działania kanału (np. długi czas oczekiwania na połączenie z pracownikiem banku w przypadku telebankingu lub zbyt wąski zakres świadczonych usług np. przez SMS)
- ☐ Lenistwo
- ☐ Inne (proszę podać)

3. Czy zgadza się Pan/Pani, że bankowość tradycyjna (oddziałowa) jest bezpieczniejsza od bankowości elektronicznej (skala od 1 do 5)? Proszę zaznaczyć odpowiednie pole.

Całkowicie się nie zgadzam 1	Całkowicie się nie zgadzam 2	Całkowicie się nie zgadzam 3	Całkowicie się nie zgadzam 4	Całkowicie się nie zgadzam 5
☐	☐	☐	☐	☐

4. Proszę określić, jak ocenia Pan/Pani ryzyko korzystania z elektronicznych kanałów dystrybucji produktów bankowych w następujących przekrojach:

A. Ryzyko własnej pomyłki

Praktycznie zerowe	Nie zgadzam się	Nie mam zdania	Zgadzam się	Całkowicie się zgadzam
1	2	3	4	5

B. Ryzyko wynikające z pomyłki pracownika banku

Praktycznie zerowe	Niskie	Średnie	Wysokie	Bardzo wysokie
1	2	3	4	5

C. Ryzyko związane z brakiem uczciwości pracownika banku

Praktycznie zerowe	Niskie	Średnie	Wysokie	Bardzo wysokie
1	2	3	4	5

D. Ryzyko zawodności technicznej kanału dystrybucji

Praktycznie zerowe	Niskie	Średnie	Wysokie	Bardzo wysokie
1	2	3	4	5

E. Ryzyko wynikające z możliwości złożenia zleceń przez osobę nieuprawnioną

Praktycznie zerowe	Niskie	Średnie	Wysokie	Bardzo wysokie
1	2	3	4	5

5. Proszę dokonać porównania ryzyka bankowości elektronicznej z tradycyjną (oddziałową) w przekrojach podanych w poprzednim pytaniu.

A. Jakie jest ryzyko własnej pomyłki w bankowości elektronicznej w porównaniu do tradycyjnej (oddziałowej)?

Dużo niższe	Niższe	Takie samo	Wyższe	Dużo wyższe
1	2	3	4	5

B. Jakie jest ryzyko wynikające z pomyłki pracownika banku w bankowości elektronicznej w porównaniu do tradycyjnej (oddziałowej)?

Dużo niższe	Niższe	Takie samo	Wyższe	Dużo wyższe
1	2	3	4	5

C. Jakie jest ryzyko związane z brakiem uczciwości pracownika banku w bankowości elektronicznej w porównaniu do tradycyjnej (oddziałowej)?

Dużo niższe	Niższe	Takie samo	Wyższe	Dużo wyższe
1	2	3	4	5

D. Jakie jest ryzyko zawodności technicznej kanału dystrybucji w bankowości elektronicznej w porównaniu do tradycyjnej (oddziałowej)?

Dużo niższe	Niższe	Takie samo	Wyższe	Dużo wyższe
1	2	3	4	5

E. Jakie jest ryzyko wynikające z możliwości złożenia zleceń przez osobę nieuprawnioną w bankowości elektronicznej w porównaniu do tradycyjnej (oddziałowej)?

Dużo niższe	Niższe	Takie samo	Wyższe	Dużo wyższe
1	2	3	4	5

6. Jak ocenia Pan/Pani swoją znajomość zabezpieczeń elektronicznych kanałów dystrybucji produktów bankowych?

- ☐ Bardzo dobra
- ☐ Dobra
- ☐ Przeciętna
- ☐ Słaba
- ☐ Bardzo słaba

7. (Dotyczy osób, które w pytaniu 3 udzieliły odpowiedzi 4 lub 5) Czy rozmaite udogodnienia, w postaci wyboru elektronicznego kanału dystrybucji produktów bankowych, dowolnego kształtowania miejsca i czasu korzystania z usług bankowych oraz brak strat czasu związanych z oczekiwaniem na obsługę, są w stanie zrekompensować Panu/Pani wyższy poziom ryzyka?

Tak ☐ Nie ☐

8. Proszę zaznaczyć jedno ze stwierdzeń, które najbardziej Panu/Pani odpowiada:

- ☐ Uważam, że w przyszłości, na skutek zastosowania coraz doskonalszych technologii i systemów, ryzyko związane z korzystaniem z elektronicznych kanałów dystrybucji produktów bankowych spadnie
- ☐ Sądzę, iż ryzyko związane z korzystaniem z elektronicznych kanałów dystrybucji produktów bankowych pozostanie mniej więcej na tym samym poziomie co obecnie, gdyż redukcji zagrożeń w jednych obszarach będą towarzyszyć wzrosty zagrożeń w innych

- ☐ Moim zdaniem, ryzyko związane z korzystaniem z elektronicznych kanałów dystrybucji produktów bankowych wzrośnie

9. (Dotyczy osób, które w pytaniu 8 wybrały ostatnią opcję) Dlaczego uważa Pan/Pani, że ryzyko związane z korzystaniem z elektronicznych kanałów dystrybucji produktów bankowych wzrośnie?

Metryczka respondenta

10. Płeć Mężczyzna ☐ Kobieta ☐

11. Wiek 15-18 ☐ 19-26 ☐ 27-35 ☐ więcej niż 35 ☐

12. Zawód

- ☐ Uczeń
- ☐ Student
- ☐ Pracownik sfery budżetowej
- ☐ Pracownik przedsiębiorstwa prywatnego
- ☐ Manager, konsultant, osoba wykonująca wolny zawód, przedsiębiorca
- ☐ Bezrobotny
- ☐ Inne (proszę podać)

13. Wykształcenie

- ☐ Podstawowe
- ☐ Średnie
- ☐ Wyższe

Serdecznie dziękuję za wypełnienie kwestionariusza!

8
Bibliografia

Pozycje książkowe, materiały wykładowe i konferencyjne

1. Barcz J. (2005): *Prawo Unii Europejskiej*. *Prawo materialnej polityki. Warszawa.* Wydawnictwo Prawo i Polityka Gospodarcza

2. Barth J., Caprio G., Levine Jr. (2002): *Bank regulation and supervision: what works best?* Cambridge: National Bureau of Economic Research.

3. Bernstein P. (1997): *Przeciw bogom. Niezwykłe dzieje ryzyka*. Warszawa, WIGPRESS.

4. Carosiere J. (2002): *Evolution of the international financial system*. Warsaw. Leon Koźmiński Academy of Entrepreneurship and Management.

5. Chateau J., Wu J. (2003): *Basle II capital adequacy computing the "fair" capital charge for loan commitment "true" credit risks*. Rouen, Ecole Superieure de Commerce.

6. Chmielarz W. (1997): *Komputer i Bank.* Warszawa, Wyższa Szkoła Bankowości, Finansów i Zarządzania w Warszawie.

7. Chmielarz W. (1999): *Systemy elektronicznej bankowości i cyfrowej płatności*. Warszawa, Wyższa Szkoła Ekonomiczno-Informatyczna w Warszawie.

8. Chmielarz W. (2001): *Handel elektroniczny nie tylko w gospodarce cyfrowej*. Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

9. Galat R. (2003): *Internet – aspekty prawne*. Warszawa, Difin.

10. GINB (2001): *Podręcznik inspekcji na miejscu: ryzyko operacyjne technologii informatycznej i bankowości elektronicznej*. Warszawa, NBP.

11. Gospodarowicz A. (red.) (2003): *Innowacje w operacjach bankowych*. Wrocław, Wydawnictwo Akademii Ekonomicznej.

12. Górski M. (2005): *Architektura systemu finansowego gospodarki*. Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

13. Górski M. (2002): *Materiały wykładowe z przedmiotu Pieniądz i rynki pieniężne*. Wydział Zarządzania Uniwersytet Warszawski.

14. Górski M. (2003): *Materiały wykładowe z przedmiotu Pieniądz i bankowość*. Wydział Zarządzania Uniwersytet Warszawski.

15. Gregor B., Stawiszyński M. (2002): *E-commerce*. Bydgoszcz, Łódź, Oficyna Wydawnicza Branta.

16. Hunter W. (2002): *Research in banking and finance*. Amsterdam, JAI.

17. Krzyżkiewicz Z. (1999): *Podręcznik do nauki bankowości*. Warszawa, Biblioteka Menedżera i Bankowca.

18. Jakubiec S., Szcześ M. (luty 2002): *Elektroniczne usługi finansowe – charakterystyka rynku, wyzwania i inicjatywy regulacyjne*. NBP 'Materiały i Studia', Zeszyt nr 139.

19. Janc A., Kotliński G. (1999): *Determinanty wykorzystania bankowości elektronicznej w rozwoju wybranych usług bankowych*. W: Gospodarowicz A. (red.): *Zastosowania rozwiązań informatycznych w bankowości*. „Prace Naukowe Akademii Ekonomicznej we Wrocławiu'"nr 828, Wrocław, Wydawnictwo AE.

20. Janson N. (2003): T*he development of electronic money: toward the privatization of money issue*. Rouen, Ecole Superieure de Commerce.

20. Jurkowski A. (2001): *Bankowość elektroniczna*. Warszawa, NBP.

21. Łazowski A. (red.) (2003): *Prawo Unii Europejskiej: testy, kazusy, tablic*e. Warszawa, Wydawnictwo C. H. Beck.

22. Masiota J. (2003): *Elektroniczne instrumenty płatnicze*. Bydgoszcz, Poznań, Oficyna Wydawnicza Branta.

23. Materiały konferencyjne z V Forum Bankowości Elektronicznej organizowanego przez Centrum Promocji Informatyki pod patronatem Związku Banków Polskich Warszawa 8 maja 2003.

24. Materiały konferencyjne z VI Forum Bankowości Elektronicznej organizowanego przez Centrum Promocji Informatyki pod patronatem Związku Banków Polskich Warszawa 12 grudnia 2003.

25. Przybylska-Kapuścińska W. (red.) (2001): *Zarządzanie ryzykiem i płynnością banku komercyjnego*. Poznań, Wydawnictwo Akademii Ekonomicznej w Poznaniu.

26. Przybylska-Kapuścińska W. i Ziarko-Siwek U. (red.) (2002): *Nowe usługi finansowe w Polsce*. Wydawnictwo Akademii Ekonomicznej w Poznaniu.

27. Pawłowicz L., Pietrzak E., Sławiński A. (kwiecień 2002): *Kluczowe zewnętrzne uwarunkowania rozwoju banków do 2006 roku*. Gdańsk, Instytut Badań nad Gospodarką Rynkową.

28. Piotrowska-Marczak K. i Mikołajczyk B. (red.) (2002): *Wybrane problemy transformacji finansów i bankowości*. Łódź, Wydawnictwo Uniwersytetu Łódzkiego.

29. Pluskota P. (2003): *Współczesne kanały dystrybucji produktów bankowych*. Szczecin, Uniwersytet Szczeciński Wydawnictwo Naukowe.

30. Podreckiego P. (red.) (2004): *Prawo Internetu*. Warszawa, Wydawnictwo Prawnicze Lexis Nexis.

31. Porębska-Miąc T. (2000): *Bankowość elektroniczna jako element e-biznesu*. W: Gospodarowicz A. (red.): *Zastosowania rozwiązań informatycznych w bankowości*. „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" nr 855, Wrocław, Wydawnictwo AE.

32. Raport Poziom Bezpieczeństwa IT w polskiej bankowości elektronicznej Marzec – Maj 2002 Warszawa, AVET 2002.

33. Solarz J. (1996): *Koncepcje rozwoju systemów bankowych*. Warszawa, „Materiały i studia" NBP nr 61.

34. Solarz J. (1997): *Zarządzanie strategiczne w bankach*. Warszawa, Poltext.

35. Szpringer W. (1999): *Ochrona klienta usług bankowych w Polsce i Unii Europejskiej*. Warszawa, Biblioteka bankowca Twigger.

36. Szpringer W. (2000): *Handel elektroniczny – konkurencja czy regulacja.* Warszawa, Difin.

37. Szpringer W. (2002): *E-commerce, E-banking: wyzwania globalizacji*. Warszawa, Difin.

38. Szpringer W. (2003): *Dystrybucja w gospodarce cyfrowej*. Warszawa, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

39. Szyszka G. (red.) (2003): *Elektroniczna Gospodarka w Polsce*. Raport 2002. Poznań, Biblioteka Logistyka.

40. Williamson O. E. (1998): *Ekonomiczne instytucje kapitalizmu*. Warszawa, PWE.

41. Jaworskiego W. L. (red.) (2002): *Współczesny Bank*. Warszawa, Poltext.

Artykuły w czasopismach fachowych i prasie

42. Błach J. (2004): *Transakcje opcyjnie*. „Bank" nr 2.

43. Brzezina J. (2003): *Bezpieczeństwo bankowości elektronicznej*. „Bank" nr 7-8.

44. Capiga M. (2003): *Nowe aspekty zarządzania ryzykiem kredytowym*. „Bank" nr 2.

45. Capiga M. (2003): *Integracja ryzyka bankowego*. „Bank" nr 3.

46. Chojecki T. (2003): *Elektroniczne usługi w bankach skandynawskich*. „Bank" nr 2.

47. Chojecki T., Matysek A. (2003): *Bankowość elektroniczna w europejskich systemach bankowych: Finlandia*. „Bank i Kredyt" nr 1.

48. Chojecki T., Matysek-Jędrych A. (2003): *Bankowość elektroniczna w europejskich systemach bankowych: Szwecja*. „Bank i Kredyt" nr 4.

49. Cwynar A. (2003): *Zabezpieczone podpisem*. „Bank" nr 9.

50. Drozdowski K. (2004): *Wirtualni pośrednicy*. „Bank" nr 3.

51. Dżega D. (2003): *(Nie) bezpieczny bank w „Internet"*. Warszawa: Wydawnictwo AVT nr 10.

52. Garside T., Pedersen C. (2002): *The Basel II prompts strategic rethinks.* "EUROMONEY" nr 12.

53. Gołdecka E. (2002): *Perspektywy nowoczesnych kanałów dystrybucji w polskiej bankowości.* „Bank" nr 7-8.

54. Gołoś S. (20030: *Pomiędzy bankiem a klientem*. „Bank" nr 4.

55. Grobicki W. (2003): *Nadchodzi era bankowości mobilnej*. „Bank" nr 6.

56. Góralczyk A. (2003): *Druga fala*. „Bank" nr 5.

57. Górka J., Markowski A. (styczeń 2004): *Teoria kosztów transakcyjnych a strategia firmy na przykładzie outsourcingu w Departamencie Bankowości Elektronicznej Raiffeisen Bank Polska S.A.*. Wydział Zarządzania Uniwersytet Warszawski.

58. Górka J. (styczeń 2004): *The New Basel Capital Accord (Basel II) and its influence over Poland and other countries*. Wydział Zarządzania Uniwersytet Warszawski.

59. Grobicki J. (2004): *Bank w komórce*. „Bank" nr 4.

60. Jackowicz K. (2003): *Nowe kanały dystrybucji produktów bankowych a wybrane problemy zarządzania bankiem*. „Bank i Kredyt" nr 1-2.

61. Jóźwiak S., Wiśniewski P. (2003): *Europejski rynek sekurytyzacji nr 9*.

62. Kalasińska M. (2003): *Poprawiając wskaźniki*. „Bank" nr 4.

63. Kałużny R. (2004): *Strzegąc swego banku*. „Bank" nr 3.

64. Kawęczyńska E. (2003): *Bank na szklanym ekranie*. „Bank" nr 10.

65. Korabiewski W. (2003): *Wszystko dla klienta*. „Bank" nr 6.

66. Kowalczyk A. (2003): *Oddziały z przyszłości*. „Bank" nr 5.

67. Kowalczyk A. (2003): *Multimedialny bank wirtualny*. „Bank" nr 6.

68. Krajewski P., Ołdakowski (2004): *Usystematyzować ryzyko*. nr 3.

69. *Kredyt hipoteczny przez Internet*. „Bank" 2003, nr 9.

70. Lepczyński B. (2003): *Nadal szybki wzrost*. „Gazeta Bankowa" 17.02.03.

71. Łysakowski P. (2000): *Elektroniczne usługi finansowe*. „Bank" nr 7.

72. Maderak K. (2003): *Bank którego nie widać*. „Bank" nr 10.

73. Marcinek T. (2002): *Ryzykowny brak pośpiechu*. „Computerworld" nr 12.

74. Marzec S. (2003): *Gotowi na wszystko*. „Bank" nr 9.

75. Meder M., Rehker M. (2001): *Modernizacja dystrybucji produktów bankowych*. „Bank" nr 9.

76. Paprotna I. (2003): *Gwarancja bankowa w formie elektronicznej*. „Bank" nr 4.

77. Pietrzak J. (2003): *Wpływ modelu dystrybucji na konkurencyjność banku*. „Bank i Kredyt" nr 3.

78. Pluskota P. (2003): *SWOT w e-bankingu*. „Bank" nr 12.

79. Raport specjalny: *Bankowość Elektroniczna*. „Bank" 2003, nr 10.

80. Rolek M. (2003): *Karta unormowana*. „Bank" nr 10.

81. Rolek M. (2003): *Jaką kartę wybrać*. „Bank" nr 10.

82. Rolek M. (2004): *Zajrzyj do wirtualnego portfela*. „Bank" nr 4.

83. Ryznar Z. (2003): *Multichanneling, czyli wielokanałowość*. „Bank" nr 7-8.

84. Samcik M. (2004): *Internetowi złodzieje podrobili stronę banku*. „Gazeta Wyborcza Gospodarka" 05.02.2004.

85. Senderecki M. (2003): *Maszyny zamiast człowieka*. „Bank" nr 5.

86. Sociński A. (2003): *Centralizacja procesu kredytowego*. „Bank" nr 7-8.

87. Sowa A. (2003): *Z gotówką czy bez*. „Bank" nr 2.

88. Sowa A. (2003): *Ryzyko płynności a cele banku*. „Bank" nr 4.

89. Szambelańczyk J. (2004): *Mądra kontrola pieniędzy*. „Bank" nr 4.

90. Szydłowska A. (2003): *Zostawcie nam oddziały*. „Bank" nr 6.

91. Thor W. (2003): *Altman w Warszawie*. „Bank" nr 9.

92. Tomala P. (2002): *Systemy home ranking*. „Bank" nr 7-8.

93. Wikariak S. (2003): *Podpisz się elektronicznie*. W: Prawo co dnia Rzeczpospolita 18.08.03.

94. Wilkowicz Ł. (2004): *Polemika*. Gazeta Bankowa 17.05.04.

95. Włodarczyk E. (marzec 2004): *50 największych banków w Polsce*. Edycja IX, wydawcy: „Bank", „Finansista", „Życie Warszawy".

96. Zielińska D. (2004): *Kupowanie mocy obliczeniowej*. „Bank" nr 1.

97. Zieliński T. (2003): *Pieniądz elektroniczny: monetarne dylematy emisji*. „Bank" nr 2.

98. Zombirt J. (2003): *Sekurytyzacja w Bazylei (cz. II)*. „Bank" nr 2.

99. Zombirt J. (2003): *NUK Kto straci, kto zyska*. „Bank" nr 7-8.

100. Zombirt J. (2003): *NUK – poprzeczka wyżej*. „Bank" 2003 nr 9 – przedruk z „The Banker" nr 8.

101. Zombirt J. (2003): *Transfer ryzyka operacyjnego*. „Bank" nr 11.

102. Żuk P. (19970: *Home banking – nowa metoda walki o klienta*. „Bank" nr 6.

Polskie i unijne akty prawne oraz dokumenty Komitetu Bazylejskiego

103. Ustawa z 29 sierpnia 1997 r. Prawo bankowe Dz. U. 1997 nr 140 poz. 939

104. Ustawa z 20 lipca 2001 r. o kredycie konsumenckim Dz. U. 2001 nr 100 poz. 1081

105. Ustawa z 18 września 2001 r. o podpisie elektronicznym Dz. U. 2001 nr 130 poz. 1450

106. Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną Dz. U. 2002 nr 144 poz. 1204

107. Ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych Dz. U. 2002 nr 169 poz. 1385

108. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych

109. Zarządzenie KNB 5/98 z dnia 2 grudnia 1998 r.

110. Uchwała nr 4/2004 Komisji Nadzoru Bankowego z dnia 8 września 2004 r. w sprawie zakresu i szczegółowych zasad wyznaczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka oraz zakresu stosowania metod statystycznych i warunków, których spełnienie umożliwia uzyskanie zgody na ich stosowanie, sposobu i szczegółowych zasad obliczania współczynnika wypłacalności banku, zakresu i sposobu uwzględniania działania banków w holdingach w obliczaniu wymogów kapitałowych i współczynnika wypłacalności oraz określenia dodatkowych pozycji bilansu banku ujmowanych łącznie z funduszami własnymi w rachunku adekwatności kapitałowej oraz zakresu, sposobu i warunków ich wyznaczania (Dz. Urz. NBP Nr 15, poz. 25)

111. Uchwałą nr 5/2004 Komisji Nadzoru Bankowego z dnia 8 września 2004 r. w sprawie wysokości, zakresu i warunków pomniejszania funduszy własnych banku o zaangażowania kapitałowe w instytucje finansowe, instytucje kredytowe, banki i zakłady ubezpieczeń oraz zakresu i sposobu uwzględniania działania banków w holdingach przy określaniu sposobu obliczania funduszy własnych (Dz. Urz. NBP Nr 15, poz. 26)

112. Uchwała nr 6/2004 Komisji Nadzoru Bankowego z dnia 8 września 2004 r. w sprawie szczegółowych zasad i warunków uwzględniania zaangażowań przy ustalaniu przestrzegania limitu koncentracji zaangażowań i limitu dużych zaangażowań, określenia innych zaangażowań, wobec których nie stosuje się przepisów dotyczących limitów koncentracji zaangażowań i dużych zaangażowań, oraz zakresu i sposobu uwzględniania działania banków w holdingach, w obliczaniu limitów koncentracji zaangażowań (Dz. Urz. NBP Nr 15, poz. 27)

113. Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanymi przez banki Generalny Inspektorat Nadzoru Bankowego, Warszawa 2002 Tekst zaktualizowany

114. Druga koordynacyjna dyrektywa bankowa 89/646/EWG z 15 grudnia 1989 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych dotyczących podejmowania i prowadzenia działalności przez instytucje kredytowe oraz zmieniająca dyrektywę 77/780/EWG Dz. U. WE 1989, L386/1

115. Dyrektywa Rady IV Bis 86/635/EWG z 8 grudnia 1986 r. w sprawie rocznych zamknięć rachunkowych i bilansów skonsolidowanych banków i innych instytucji finansowych

116. Dyrektywa 87/102/EWG z 22 grudnia 1986 r. w sprawie ujednolicenia ustaw i przepisów wykonawczych państw członkowskich dotyczących kredytów konsumenckich

117. Dyrektywa 89/647/EWG z 18 grudnia 1989 r. w sprawie wskaźnika wypłacalności dla instytucji kredytowych Dz. U. WE z 30 grudnia 1989 r., L386

118. Dyrektywa Rady 92/121/EWG z 21 grudnia 1992 r. w sprawie monitorowania i kontroli koncentracji ryzyka kredytowego Dz. U. WE. z 5 lutego 1993 r., L 29

119. Dyrektywa 93/6/WE z 15 marca 1993 r. w sprawie adekwatności kapitału firm inwestycyjnych i instytucji kredytowych Dz. U. WE z 11 czerwca 1993 r., L 141

120. Dyrektywa 95/46/WE oraz 97/66/WE o ochronie danych osobowych

121. Zalecenie Komisji Europejskiej 97/489/ WE z dnia 30 lipca 1997 r. w sprawie transakcji prowadzonych przy użyciu elektronicznych instrumentów płatniczych, a w szczególności stosunków między wydawcą a posiadaczem

122. Dyrektywa 99/93/WE z 13 grudnia 1999 r. w sprawie stworzenia wspólnotowych ram prawnych dla podpisu elektronicznego

123. Directive 2000/12/EC of 20 March 2000 of the European Parliament and of the Council relating to the taking up and pursuit of the business of credit institutions, OJ L 126, 26 May 2000 Skonsolidowana dyrektywa bankowa 2000/12/WE z 20 marca 2000 r. odnosząca się do podejmowania i prowadzenia działalności przez instytucje kredytowe Dz. U. WE z 26 maja 2000 r.

124. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), OJ L 178, 8 June 2000

125. Directive 2000/46/EC of 18 September 2000 of the European Parliament and of the Council on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275, 27 October 2000 Dyrektywa Parlamentu Europejskiego i Rady 2000/46/WE z 18 września 2000 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością

126. Directive 2000/28/EC of 18 September 2000 of the European Parliament and of the Council amending Directive 2000/12/EC relating to the taking up and pursuit of the business of credit institutions, OJ L 275, 27 October 2000

127. Zasady nadzoru nad zagranicznymi placówkami banków, czyli tzw. Konkordat Bazylejski Komitet Bazylejski maj 1983

128. Information Flows Between Banking Supervisory Authorities Basel Committee on Banking Supervision April 1990

129. Minimum standards for the Supervision of International Banking Groups and their Cross-Border Establishments Basel Committee on Banking Supervision July 1992

130. Amendment to the capital accord to incorporate market risks Basel Committee on Banking Supervision June 1996

131. Supervisory framework for the use of 'backtesting' in conjunction with the internal models approach to market risk capital requirements Basel Committee on Banking Supervision June 1996

132. Overview of the amendment to the capital accord to incorporate market risks Basel Committee on Banking Supervision June 1996

133. Security of Electronic Money Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries August 1996

134. The Supervision of Cross-Border Banking Basel Committee on Banking Supervision October 1996

135. Core Principles for Effective Banking Supervision Basel Committee on Banking Supervision October September 1997

136. Podstawowe zasady efektywnego nadzoru bankowego Komitet Bazylejski wrzesień 1997

137. Risk Management for Electronic Banking and Electronic Money Activities Basel Committee on Banking Supervision March 1998

138. Zarządzanie ryzykiem operacyjnym Komitet Bazylejski ds. Nadzoru Bankowego wrzesień 1998

139. Nowa Metodologia Adekwatności Kapitałowej Komitet Bazylejski ds. Nadzoru Bankowego Czerwiec 1999

140. Core Principles Methodology Basel Committee on Banking Supervision October 1999

141. Nowa metodologia adekwatności kapitałowej – filar 3 – dyscyplina rynkowa Komitet Bazylejski ds. Nadzoru Bankowego styczeń 2000

142. Electronic Banking Group Initiatives and White Papers Basel Committee for Banking Supervision October 2000

143. Zasady zarządzania ryzykiem w bankowości elektronicznej Komitet Bazylejski, maj 2001

144. Essential Elements of a Statement of Co-operation Between Banking Supervisors Basel Committee on Banking Supervision May 2001

145. Management and Supervision of Cross-Border Electronic Banking Activities Basel Committee on Banking Supervision July 2003

146. Overview of the New Basel Capital Accord Consultative document Basel Committee on Banking Supervision July 2003

147. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision June 2004

148. Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework Basel Committee on Banking Supervision November 2005

Zasoby Internetu

149. Bank wiedzy stworzony pod auspicjami NBP www.nbportal.pl

150. Forum dyskusyjne http://www.mozillapl.org/forum/sutra32080.html

151. Informacje o standardzie CEPS (Common Electronic Purse Specification) http://www. corporate.visa.com/mc/facts/smartcards/pdfs/smartcards_CEPS.pdf

152. Molski M. Karty elektroniczne a kontekst zabezpieczenia informacji http://www.bezpieczenstwoit.pl/Artykuly/Karty_inteligentne/M. Molski, Karty_elektroniczne_a_kontekst_bezpieczenstwa/index. html

153. Serwis o bankowości elektronicznej www.eBanki.pl

154. Serwis www.vaGla.pl Prawo i Internet, Przestępczość w Internecie. Zagadnienia podstawowe

155. Serwis o bezpieczeństwie użytkownika Internetu http: //www.cert.pl/index2.html?action=show_linki&id=132#132

156. Serwis prawny Unii Europejskiej http://europa.eu.int/eur-lex/en/search/search_lif. html

157. Serwis o handlu elektronicznym http://www.e-fakty.pl/

158. Strona Narodowego Banku Polskiego www.nbp.pl

159. Strona Inteligo www.inteligo.pl

160. Strona mBanku www. mbank.com.pl

161. Strona Volkswagen Bank direct http://www.vwbdirect.pl

162. Strona Citibanku www. online. citibank. pl

163. Strona o bezpieczeństwie kart płatniczych http://www.bezpieczenstwoit.pl/Karty_inteligentne.html

164. Strony o telewizji cyfrowej i set-top boxach: http://searchnetworking.techtarget. com/sDefini-

tion/0%2C%2Csid7gci212971%2C00. html; http://www.quinion.com/words/turnsofphrase/tp--set1. htm

165. Strona MasterCard http://www.mastercard.com/cardholderservices

166. Wortal www.Bankier.pl

167. Wortal www.Money.pl

168. Wortale o kartach bankowych: www.kartyonline.net;www.kartybankowe.net; www. karty. pl; http: //www.cardco.pl/pliki/microp.htm

169. Wyszomirski F. Oberthur Card Systems – lider rynku kart EMV 15.04.2004 http://www. karty-online.net/arty.php? id=93

170. Żwiruk K. Elektroniczne portmonetki czyli nowe wcielenie pieniądza 19.05.2003 http: //www.kartyonline.net/arty.php?id=29

171. Banks, Budget and Basel II Bob Reynolds Cedalion http://www.cedalion.co. uk/pdf/FYI_Oct_2003.pdf

172. Basel II generates controversy Pratt's Letter, December 22 2003 http://www.prattsletter.com/free/20031222_1.html

173. Basel II solutions http: //www. sungard. com/products_and_services/stars/challenges+for+banks. htm

174. Basel II the New Capital Accord, Deutsche Bundesbank http://www.bundesbank. de/bank/bank_basel. en. php

175. Costs of Basel II implementation http://www.silicon.com/management/itdirector/0,39024673,39117669,00.htm

176. Data base about Electronic Money http://www.ex.ac. uk/~RDavies/arian/emoney. html

177. Electronic Payment Systems http://ws19.webpark.pl/

178. Service Bank Technology News http://www.banktechnews.com/btn/m_btn2.shtml

179. Website of BIS (Bank for International Settlement) www.bis.org

180. Website of European Central Bank www.ecb.int

181. 3 pillars of Basel II http: //www.misys.com/mys/banking/products/risk/data/baselII/