*Mirosława Capiga**

WIELOWYMIAROWOŚĆ BEZPIECZEŃSTWA FINANSOWEGO BANKU – na przykładzie polskich regulacji prawnych

WSTĘP

Bezpieczeństwo finansowe to szczególne uwarunkowanie działalności operacyjnej każdej instytucji w każdych warunkach gospodarczych. Najczęściej jest ono ujmowane jako bezpieczeństwo szeroko rozumianego otoczenia, w jakim funkcjonuje instytucja i bezpieczeństwo wewnętrzne samej instytucji. Celem niniejszego opracowania jest zaprezentowanie wielowymiarowości obu podejść do bezpieczeństwa finansowego i ich wzajemnych powiązań. Pierwsza część opracowania dotyczy bezpieczeństwa otoczenia, czyli bezpieczeństwa zewnętrznego, które dla banków oznacza stabilność finansową nie tylko sektora bankowego, ale systemu finansowego. Stabilność finansowa to przede wszystkim sieć bezpieczeństwa finansowego w ujęciu instytucjonalnym i skuteczność jej działań. Zasygnalizowano tu kwestie wymiany informacji między poszczególnymi instytucjami sieci, zwłaszcza w związku z powołaniem organu koordynującego te działania, jakim stał się Komitet Stabilności Finansowej.

Druga część opracowania dotyczy bezpieczeństwa finansowego w ujęciu mikro, czyli tzw. bezpieczeństwa wewnętrznego. Rozważania skoncentrowano na przedstawieniu wielowymiarowości bezpieczeństwa banku, co najlepiej obrazują zależności typu ryzyko–bezpieczeństwo. W tym kontekście podjęto próbę zdefiniowania

* Profesor dr hab. Mirosława Capiga jest profesorem w Katedrze Bankowości i Rynków Finansowych Uniwersytetu Ekonomicznego w Katowicach.

bezpieczeństwa banku, które właśnie w przypadku banku odzwierciedla sprawność zarządzania ryzykiem bankowym.

W obu częściach opracowania zaprezentowano wybrane regulacje prawne odnoszące się do poszczególnych wymiarów bezpieczeństwa.

1. ZEWNĘTRZNY WYMIAR BEZPIECZEŃSTWA FINANSOWEGO

Bezpieczeństwo zewnętrzne banku to bezpieczeństwo otoczenia w jakim bank funkcjonuje, a więc szeroko ujmowane bezpieczeństwo ekonomiczne, dla zachowania którego szczególne znaczenie ma aspekt finansowy, czyli bezpieczeństwo finansowe.

Bezpieczeństwo finansowe nie zostało wprawdzie zdefiniowane, ale najczęściej sprowadza się ono do stabilności finansowej, czyli takiego stanu systemu finansowego, w którym jest on zdolny prawidłowo wypełniać swoje funkcje, co oznacza ciągłość, płynność i efektywność w osiąganiu założonych celów. Nie wyklucza to oczywiście występowania przejściowych szoków i zakłóceń, ale podejmowane przedsięwzięcia na rzecz minimalizowania ryzyka systemowego i zapobiegania kryzysom finansowym pozwalają uniknąć destabilizacji systemu finansowego. W tej sytuacji pytanie: czy bezpieczeństwo finansowe należy utożsamiać ze stabilnością finansową, czy też ujmować jako jej cechę? należy traktować jako otwarte.

Nie ulega jednak wątpliwości, że bezpieczeństwo finansowe to pojęcie wielowymiarowe, które należy analizować jako:

- bezpieczeństwo instytucji finansowych,
- bezpieczeństwo transakcji finansowych,
- bezpieczeństwo segmentów rynku finansowego,
- bezpieczeństwo klienta rynku finansowego[1].

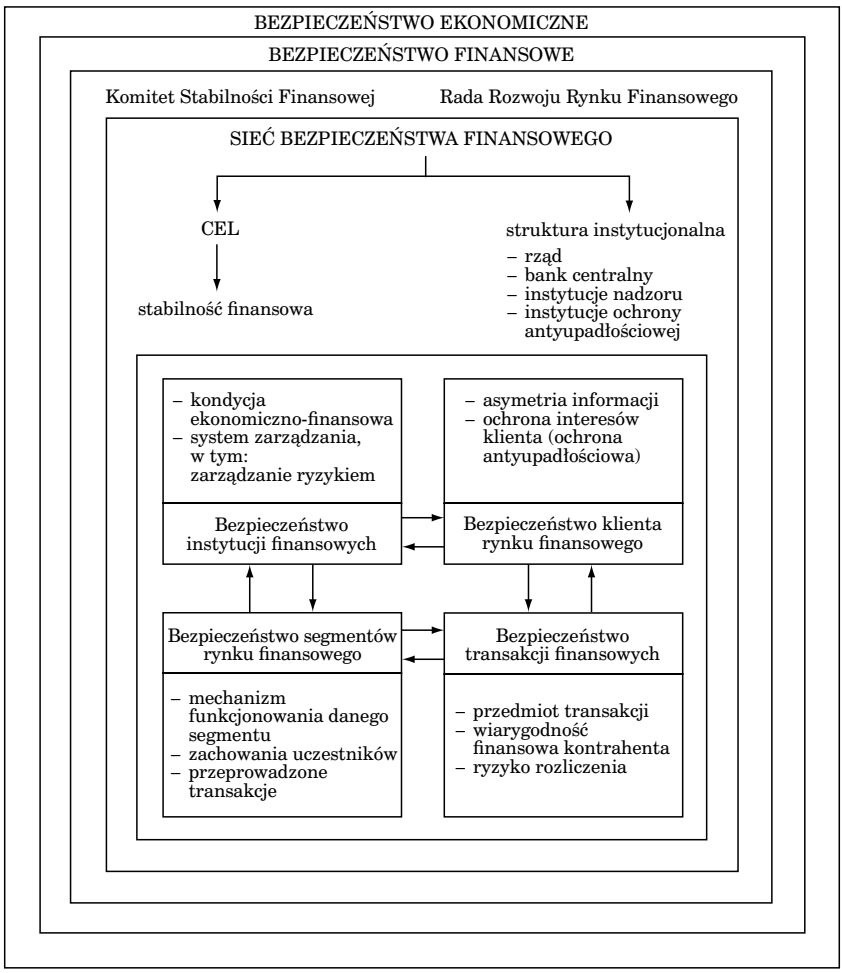
Całokształt instytucji i regulacji, mających na celu ochronę systemu finansowego przed destabilizacją, to sieć bezpieczeństwa finansowego, którą tworzą: rządy, reprezentowane przez ministerstwa finansów, banki centralne, instytucje nadzorcze i instytucje antyupadłościowe. Struktura instytucjonalna sieci bezpieczeństwa finansowego w Polsce to przede wszystkim rząd, Narodowy Bank Polski, Komisja Nadzoru Finansowego i Bankowy Fundusz Gwarancyjny (por. wykres 1).

Rząd w sieci bezpieczeństwa finansowego spełnia funkcje głównego regulatora, twórcy norm prawnych oraz dysponenta środków publicznych. Zapewnienie krajowi bezpieczeństwa finansowego stanowi jedno z kluczowych zadań Ministra Finansów. Kompleksowy charakter tego działania przejawia się w szerokim polu działalności: począwszy od sprawnego zarządzania budżetem państwa, poprzez pobór danin publicznych po kształtowanie polityki podatkowej oraz w sieci wyspe-

[1] M. Capiga, W. Gradoń, G. Szustak, *Sieć bezpieczeństwa finansowego*, wyd. I. CeDeWu.Pl Platinium, Warszawa 2010, s. 12 i dalsze.

cjalizowanych służb zajmujących się ochroną systemu finansowego (np. kontrola skarbowa, jednostki walki z praniem pieniędzy)[2]. W 2006 r. Minister Finansów powołał Radę Rozwoju Rynku Finansowego, będącą organem opiniodawczym i doradczym w sprawach rynku finansowego.

Wykres 1. Wielowymiarowość bezpieczeństwa finansowego



Źródło: opracowanie własne. Por. M. Capiga, W. Gradoń, G. Szustak, *Sieć bezpieczeństwa finansowego*, CeDeWu.Pl. Platinium, wyd. I, Warszawa 2010, s. 12 i dalsze.

[2] www.mf.gov.pl/bezpieczeństwo finansowe (dostęp: 21.09.2011 r.).

Najbardziej znaną instytucją sieci bezpieczeństwa finansowego pozostają banki centralne, dla których działania na rzecz stabilności finansowej nie zawsze stanowią cel ustawowy, ale zawsze były one w takie działania zaangażowane.

Wynikało to nie tylko z często występującego w wielu krajach umiejscowienia nadzoru bankowego w banku centralnym, ale:

- z realizowanych od lat przez banki centralne takich klasycznych funkcji, jak: kredytodawca ostatniej instancji (czyli tzw. awaryjne wsparcie płynności), zapewnienie sprawnego i bezpiecznego funkcjonowania systemów płatności,
- z nowego podejścia do stabilności finansowej, czyli zaangażowania banku centralnego w opracowywanie analiz makroostrożnościowych oraz wzrost znaczenia polityki informacyjnej (przejrzystość, czyli transparentność banku centralnego)[3].

Podstawowym, ustawowym celem działania banku centralnego, w tym również Narodowego Banku Polskiego, jest utrzymanie stabilnego poziomu cen. Działania na rzecz stabilności finansowej krajowego systemu finansowego stały się zadaniem ustawowym NBP dopiero w 2008 r.[4]

Kolejnym ogniwem sieci bezpieczeństwa finansowego jest instytucja nadzoru nad rynkiem finansowym, którą, zgodnie z koncepcją zintegrowanego nadzoru, sprawuje w Polsce od 2006 r. Komisja Nadzoru Finansowego. Celem ustawowym zintegrowanego nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku [5]. W przypadku nadzoru, zarówno stabilność jak i bezpieczeństwo, są celem ustawowym, które KNF realizuje poprzez podejmowanie działań służących prawidłowemu funkcjonowaniu rynku finansowego, mających na celu jego rozwój i konkurencyjność.

Integralną częścią sieci bezpieczeństwa finansowego są instytucje ochrony antyupadłościowej. W Polsce, pomimo nadzoru zintegrowanego, ochrona klienta nadal ma charakter sektorowy: w odniesieniu do rynku bankowego instytucją taką jest Bankowy Fundusz Gwarancyjny, w odniesieniu do rynku kapitałowego system rekompensat dla inwestorów, a w odniesieniu do rynku ubezpieczeniowego Ubezpieczeniowy Fundusz Gwarancyjny. Najbardziej znanym rozwiązaniem w zakresie ochrony klienta rynku finansowego są systemy gwarantowania depozytów, które (pomimo zróżnicowanych rozwiązań w poszczególnych krajach) są ukierunkowane przede wszystkim na ochronę klienta (zwrot środków gwarantowanych do określonej wysokości wynoszącej aktualnie 100 tys. euro), oraz na bank (udzielanie

---

[3] O. Szczepańska, *Stabilność finansowa jako cel banku centralnego. Studium teoretyczno-porównawcze*, Wydawnictwo Naukowe SHOLAR, Warszawa 2008.

[4] Art. 3. Ustawa o Narodowym Banku Polskim z dnia 29 sierpnia 1997 r., Dz.U. 1997 Nr 140 poz. 938 z późn. zm.

[5] Art. 2. Ustawa o nadzorze nad rynkiem finansowym z dnia 21 lipca 2006 r., Dz.U. 2006 Nr 157, poz. 1119 z późn. zm.

pomocy zwrotnej). Bankowy Fundusz Gwarancyjny prowadzi zarówno działalność gwarancyjną, jak i pomocową. To właśnie w ramach działalności pomocowej pojawia się termin niebezpieczeństwo niewypłacalności. Zadaniem ustawowym BFG jest udzielanie zwrotnej pomocy finansowej oraz nabywanie wierzytelności banków, w których powstało niebezpieczeństwo niewypłacalności[6].

W 2008 r. państwa UE zobowiązały się do utworzenia Komitetów Stabilności Finansowej, mających na celu usprawnienie współpracy między instytucjami sieci bezpieczeństwa finansowego. W Polsce Komitet Stabilności Finansowej został utworzony w listopadzie 2008 r. Celem ustawowym działania Komitetu jest zapewnienie efektywnej współpracy w zakresie wspierania i utrzymania stabilności krajowego systemu finansowego poprzez wymianę informacji, opinii i ocen sytuacji w systemie finansowym w kraju i za granicą oraz koordynację działań w tym zakresie[7]. Członkami Komitetu są: Minister Finansów, Prezes Narodowego Banku Polskiego i Przewodniczący Komisji Nadzoru Finansowego[8]. Z powyższych regulacji prawnych wynika, że Komitet Stabilności Finansowej tworzą instytucje sieci bezpieczeństwa finansowego, których ustawowa działalność wymaga gromadzenia, przetwarzania i przekazywania informacji o stabilności systemu finansowego.

Przykładowo: naczelne organy państwowe, organy administracji rządowej i samorządu terytorialnego, banki przekazują do NBP dane niezbędne do ustalania polityki pieniężnej państwa, okresowych ocen sytuacji pieniężnej państwa, sporządzania bilansu płatniczego, międzynarodowej pozycji inwestycyjnej, dokonywania ocen funkcjonowania rozliczeń pieniężnych i rozrachunków międzybankowych. Ponadto banki mają obowiązek przekazywać dane niezbędne do oceny ich sytuacji finansowej oraz stabilności i ryzyka systemu bankowego [9]. Na podstawie powyższych informacji NBP opracowuje raporty o stabilności systemu finansowego i raporty o rozwoju systemu finansowego, a więc ocenia nie tylko funkcjonowanie systemu bankowego, ale również stabilność krajowego systemu finansowego. Obowiązek przekazywania do NBP danych niezbędnych do wykonywania zadań NBP, wynikających z ustawy oraz uczestnictwa w Europejskim Systemie Banków Centralnych, obejmuje również dane objęte ochroną na podstawie odrębnych ustaw, w tym informacje objęte tajemnicą bankową[10].

To właśnie informacje gromadzone przez NBP, w ramach jego ustawowych uprawnień, mogą być udostępniane Ministrowi Finansów i Komisji Nadzoru Fi-

---

[6] Art. 4. Ustawa o Bankowym Funduszu Gwarancyjnym z dnia 14 grudnia 1994 r., Dz.U. 1995 Nr 4 poz. 18, z późn. zm.

[7] Art. 3. Ustawa o Komitecie Stabilności Finansowej z dnia 7 listopada 2008 r., Dz.U. Nr 2009, poz. 1317.

[8] *Ibidem*, art. 4.

[9] Art. 23. Ustawa o NBP.., *op. cit.*

[10] *Ibidem*, art. 23.

nansowego w zakresie niezbędnym dla realizacji celu działalności i zadań Komitetu Stabilności Finansowej[11].

Podobne obowiązki w zakresie przekazywania informacji mają banki wobec Komisji Nadzoru Finansowego, co wynika z realizowanych przez ten organ funkcji nadzorczych oraz wobec Bankowego Funduszu Gwarancyjnego, co wynika z działalności pomocowej i analitycznej Funduszu. Na podstawie przekazywanej informacji KNF opracowuje Raporty o sytuacji banków oraz Raporty o funkcjonowaniu polskiego rynku finansowego w ujęciu międzysektorowym. BFG dokonuje analiz sytuacji ekonomiczno-finansowych banków komercyjnych, banków spółdzielczych oraz całego sektora krajowego.

Przewodniczący Komisji Nadzoru Finansowego i Prezes NBP mają ustawowe prawo przekazywania sobie informacji, w tym niejawnych, w zakresie niezbędnym do wykonywania ich ustawowo określonych zadań[12].

Zadania Komitetu Stabilności Finansowej nie sprowadzają się tylko do dokonywania ocen sytuacji w krajowym systemie finansowym, co stanowiłoby powielanie działań NBP, KNF i BFG, ale obejmują również:

- ❖ opracowywanie i przyjmowanie procedur współdziałania na wypadek wystąpienia zagrożenia dla stabilności krajowego systemu finansowego,
- ❖ koordynowanie działań członków Komitetu w sytuacji bezpośredniego zagrożenia dla stabilności krajowego systemu finansowego[13].

W kontekście powyższych zadań, Komitet Stabilności Finansowej należy postrzegać jako organ koordynujący działalność instytucji tworzących sieć bezpieczeństwa finansowego.

2. WEWNĘTRZNY WYMIAR BEZPIECZEŃSTWA FINANSOWEGO

Bezpieczeństwo finansowe w skali makro (zewnętrzne) to podstawa bezpieczeństwa wewnętrznego banku, które najczęściej jest interpretowane jako wypłacalność lub jako stan równowagi. Bezpieczeństwo banku utożsamiane z jego wypłacalnością to kłopoty z płynnością, określaną jako zdolność do terminowego spłacania wszystkich zobowiązań pieniężnych, które prowadzą do zagrożenia wypłacalności, określanej jako nadwyżka wartości rynkowej aktywów nad wartością zobowiązań, a to oznacza utratę wiarygodności finansowej banku, a tym samym prowadzi do spadku bezpieczeństwa funkcjonowania[14].

---

11 *Ibidem*, art. 23.

12 Art. 16. Ustawa o nadzorze nad rynkiem finansowym z dnia 21 lipca 2006 r., Dz.U. Nr 157, poz. 1119 z późn. zm.

13 Art. 3. Ustawa o Komitecie..., *op. cit.*

14 B. Zdanowicz, *Podstawowe dylematy i kryteria wyboru formuły systemu gwarantowania depozytów w świetle teorii i doświadczeń międzynarodowych*, „Bezpieczny Bank" Nr 1 (34)/ 2007.

Bezpieczeństwo banku jako stan równowagi oznacza, że bank osiąga równowagę ekonomiczną, finansową i majątkową, co pozwala mu bezpiecznie realizować jego funkcje nawet w przypadku wystąpienia okresowych szoków zewnętrznych[15].

Oba podejścia do definiowania bezpieczeństwa banku, które można uznać za podejścia klasyczne, są wzajemnie ze sobą powiązane. Oba podejścia opierają się na zagrożeniach, które mogą prowadzić do wystąpienia różnych rodzajów ryzyka, jak: ryzyko obniżenia lub utraty płynności, do zachowania której bank jest ustawowo zobowiązany (art. 8 ustawy Prawo bankowe), ryzyko niewypłacalności, ryzyko kapitałowe, ryzyko bankructwa.

Coraz to nowe zagrożenia dla funkcjonowania banku oznaczają, że jest on narażony na różne rodzaje ryzyka bankowego, które stały się w ostatnich latach przedmiotem regulacji nadzorczych mających zapewnić bezpieczną działalność banku. Zarządzanie ryzykiem bankowym zdominowało działalność każdego banku, co znalazło odzwierciedlenie w ustawowym ujęciu systemu zarządzania bankiem, jako zbiorze zasad i mechanizmów odnoszących się do procesów decyzyjnych, zachodzących w banku oraz do oceny prowadzonej działalności bankowej. Tak interpretowany system zarządzania powinien obejmować co najmniej system zarządzania ryzykiem i system kontroli wewnętrznej[16]. Zadaniem systemu zarządzania ryzykiem jest identyfikacja, pomiar lub szacowanie oraz monitorowanie ryzyka występującego w działalności banku, służące zapewnieniu prawidłowości procesu wyznaczania i realizacji szczegółowych celów prowadzonej przez bank działalności[17].

Ustawowe ujęcie systemu zarządzania ryzykiem odnosi się do ryzyka bankowego, co w praktyce bankowej wymaga przełożenia na konkretne rodzaje ryzyka. Nie jest to zadanie proste, ponieważ występuje wiele rodzajów ryzyka bankowego. Obok klasycznych rodzajów ryzyka bankowego, jak: ryzyko kredytowe, ryzyko stóp procentowych czy ryzyko niedopasowania aktywów i pasywów, pojawiło się wiele nowych rodzajów, czego przykładem są: ryzyko outsourcingu, ryzyko ładu korporacyjnego, ryzyko zgodności (*compliance*).

Wszystkie rodzaje ryzyka bankowego są przedmiotem licznych regulacji prawnych i mają bezpośrednie przełożenie na bezpieczeństwo funkcjonowania banku w takich kategoriach, jak: bezpieczeństwo ekonomiczne, bezpieczeństwo środków pieniężnych, bezpieczeństwo bankowości elektronicznej, bezpieczeństwo informacji, bezpieczeństwo systemów informatycznych (zob. tabela 1).

---

15 Szerzej o podejściu autorów do definiowania bezpieczeństwa banku [w:] M. Capiga, W. Gradoń, G. Szustak, *Adekwatność kapitałowa w ocenie bezpieczeństwa banku*, CeDeWu.Pl. Platinium, Warszawa 2011, s. 10 i dalsze.

16 Art. 9. Ustawa Prawo bankowe…, *op. cit.*

17 *Ibidem*, art. 9a.

Tabela 1. Przykładowe regulacje prawne wybranych kategorii bezpieczeństwa funkcjonowania banku

Regulacja prawna	Kategorie zagrożenia	Kategorie bezpieczeństwa
USTAWA PRAWO BANKOWE		
Art. 30 Utworzenie banku może nastąpić, jeżeli: zostało zapewnione wyposażenie banku w pomieszczenia posiadające odpowiednie urządzenia techniczne, należycie zabezpieczające przechowywane w banku wartości, z uwzględnieniem zakresu i rodzaju prowadzonej działalności bankowej	Ryzyko techniczne	Bezpieczeństwo techniczne
Art. 30 Założyciele oraz osoby przewidziane do objęcia w banku stanowisk członków zarządu, w tym prezesa, dają rękojmię ostrożnego i stabilnego zarządzania bankiem	Ryzyko personalne	Bezpieczeństwo personalne (osobowe)
Art. 30 Przedstawiony przez założycieli plan działalności banku na okres co najmniej trzyletni wskazuje, że działalność ta będzie bezpieczna dla środków pieniężnych gromadzonych w banku Art. 50 Bank dokłada szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych	Ryzyko planowania	Bezpieczeństwo środków pieniężnych
Art. 104 Bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje	Ryzyko poufności danych osobowych	Bezpieczeństwo informacji
Art. 126 W celu zapewnienia bezpieczeństwa ekonomicznego banki są obowiązane posiadać fundusze własne, dostosowane do rozmiaru prowadzonej działalności	Ryzyko kapitałowe	Bezpieczeństwo ekonomiczne

USTAWA O PODPISIE ELEKTRONICZNYM		
Art. 3 2) Bezpieczny podpis elektroniczny, to podpis elektroniczny, który: a) jest przyporządkowany wyłącznie do osoby składającej ten podpis, b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego, c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna. 9) Bezpieczne urządzenie służące do weryfikacji podpisu elektronicznego – urządzenie służące do weryfikacji podpisu elektronicznego spełniające wymagania określone w ustawie	Ryzyko poufności danych osobowych Ryzyko dostępu do systemu Ryzyko techniczne	Bezpieczeństwo bankowości elektronicznej
USTAWA O ELEKTRONICZNYCH INSTRUMENTACH PŁATNICZYCH		
Art. 31 Bank, świadcząc usługi na podstawie umowy o usługi bankowości elektronicznej, obowiązany jest do: 1) zapewnienia posiadaczowi bezpieczeństwa dokonywania operacji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych	Ryzyko techniczne	Bezpieczeństwo bankowości elektronicznej
Art. 32 Posiadacz jest obowiązany do nieujawniania informacji o działaniu elektronicznego instrumentu płatniczego, udostępnianego w ramach umowy o usługi bankowości elektronicznej, których ujawnienie może spowodować brak skuteczności mechanizmów zapewniających bezpieczeństwo zlecanych operacji.	Ryzyko informacji	Bezpieczeństwo informacji

USTAWA O PRZECIWDZIAŁANIU PRANIU PIENIĘDZY ORAZ FINANSOWANIU TERRORYZMU		
Art. 8 1) Instytucja obowiązana przeprowadzająca transakcję, której równowartość przekracza 15 000 euro, ma obowiązek zarejestrować taką transakcję również w przypadku, gdy jest ona przeprowadzana za pomocą więcej niż jednej operacji, których okoliczności wskazują, że są one ze sobą powiązane i zostały podzielone na operacje o mniejszej wartości, z zamiarem uniknięcia obowiązku rejestracji. 3) Instytucja obowiązana przeprowadzająca transakcję, której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, ma obowiązek zarejestrować taką transakcję, bez względu na jej wartość i charakter. Art. 8b Instytucje obowiązane stosują wobec swoich klientów środki bezpieczeństwa finansowego. Zakres stosowania jest określany na podstawie oceny ryzyka prania pieniędzy i finansowania terroryzmu, zwanej dalej „oceną ryzyka", dokonanej w wyniku analizy, z uwzględnieniem w szczególności rodzaju klienta, stosunków gospodarczych, produktów, transakcji.	Ryzyko prania pieniędzy	Bezpieczeństwo finansowe

Źródło: Ustawa Prawo Bankowe z dnia 29 sierpnia 1997 r. Dz.U. Nr 140, poz. 939 z późn. zm.; Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 16 listopada 2000 r., Dz.U. 2010, Nr 46, poz. 276 z późn. zm.; Ustawa o podpisie elektronicznym z dnia 18 września 2001 r., Dz.U. 2001, Nr 130, poz. 1450 z późn. zm.; Ustawa o elektronicznych instrumentach płatniczych z dnia 12 września 2002 r., Dz.U. 2002 r., Nr 169, poz. 1385 z późn. zm.

Najbardziej szeroką kategorią bezpieczeństwa, regulowaną ustawowo (art. 126 ustawy Prawo bankowe), jest bezpieczeństwo ekonomiczne, czyli obowiązek posiadania przez bank odpowiedniej wysokości funduszy własnych. Jest to jedna z najstarszych regulacji prawnych odnoszących się do bezpieczeństwa banku, która aktualnie wydaje się podejściem dość wąskim. Obok kapitału księgowego w zarządzaniu bankiem mamy do czynienia z innymi kategoriami kapitałów. Pojawiły się one w związku z pracami Bazylejskiego Komitetu ds. Nadzoru Bankowego dotyczącymi pomiaru adekwatności kapitałowej, czyli pomiaru różnych rodzajów ryzyka

bankowego i szacowania kapitału niezbędnego na pokrycie strat z tytułu ich wystąpienia. Takimi kategoriami kapitału są kapitał regulacyjny i kapitał ekonomiczny[18].

Występujące w ustawie Prawo bankowe fundusze własne to polski odpowiednik kapitału regulacyjnego, którego elementy składowe określa art. 127 Prawa bankowego. Kapitał ekonomiczny, ujmowany w literaturze najczęściej jako kapitał absorbujący nieoczekiwane straty z tytułu różnych rodzajów ryzyka bankowego, w ustawie Prawo bankowe został zdefiniowany jako oszacowana przez bank kwota niezbędna do pokrycia wszystkich zidentyfikowanych, istotnych rodzajów ryzyka występujących w działalności banku oraz zmian otoczenia gospodarczego, uwzględniająca przewidywany poziom ryzyka, czyli kapitał wewnętrzny[19]. M. Iwanicz-Drozdowska określa kapitał regulacyjny i kapitał ekonomiczny mianem kapitału finansowego[20].

Mówiąc o bezpieczeństwie ekonomicznym banku, należy więc uwzględniać obie kategorie kapitału, czyli kapitał regulacyjny i kapitał wewnętrzny, w odniesieniu do których obowiązują liczne regulacje nadzorcze.

Bezpieczeństwo ekonomiczne to oczywiście podstawa bezpieczeństwa funkcjonowania banku, ale nie jest ono równoznaczne z bezpieczeństwem banku w jego różnych wymiarach.

Bank, jako instytucja zaufania publicznego, przywiązuje szczególne znaczenie do bezpieczeństwa środków pieniężnych pozyskanych od klientów, stanowiących podstawę jego działalności operacyjnej. Bezpieczeństwo środków pieniężnych przekłada się na bezpieczeństwo klienta banku. Szczególnym przykładem może być bankowość elektroniczna. Szybki rozwój elektronicznych kanałów dystrybucji produktów bankowych oznaczał zupełnie nowe zagrożenia, a tym samym konieczność doboru odpowiednich zabezpieczeń. Powszechnie znany podział zagrożeń bankowości elektronicznej to:

- zagrożenia wspólne dla serwera i klienta związane z podsłuchiwaniem lub modyfikacją danych przesyłanych sieciami, czyli *sniffing* (podsłuchiwanie), *spoofing* (podszywanie się pod komputer w sieci), *network snooping* (wstępne rozpoznanie parametrów sieci), *phishing* (wyłudzanie poufnych informacji osobistych), sabotaż komputerowy i cyberterroryzm,
- zagrożenia serwera, czyli zagrożenia związane z atakami na zasoby serwera typu ataki blokujące DoS oraz DDoS, wykorzystywanie specyficznych programów umożliwiających ingerencję w systemy informatyczne (jak bakterie, robaki, konie trojańskie), ataki na bazy danych,

---

18 M. Iwanicz-Drozdowska, *Zarządzanie finansowe bankiem*, PWE, wyd. II, Warszawa 2010, s. 216 i dalsze; M. Marcinkowska, *Standardy kapitałowe banków. Bazylejska Nowa Umowa Kapitałowa w polskich regulacjach nadzorczych*, Regan Press, Gdańsk 2009, s. 116 i dalsze.

19 Art. 128 Ustawa Prawo bankowe..., *op. cit.*

20 M. Iwanicz-Drozdowska, *Zarządzanie...*, *op. cit.*, s. 214.

- zagrożenia klienta związane z procedurami logowania się do systemu oraz pracy z oprogramowaniem klienta, jak: identyfikator, hasło, błędy w oprogramowaniu)[21].

Poszczególne grupy zagrożeń to poszczególne kategorie bezpieczeństwa bankowości elektronicznej. Najbardziej znane zabezpieczenia bankowości elektronicznej to przede wszystkim podpis elektroniczny oraz bezpieczeństwo informacji i systemów informatycznych. Podpis elektroniczny, zwłaszcza tzw. bezpieczny podpis elektroniczny, regulowany ustawowo i związane z tym bezpieczne urządzenia służące do składania podpisu elektronicznego oraz bezpieczne urządzenia służące do jego weryfikacji, to typowy przykład bezpieczeństwa prawnego i bezpieczeństwa technicznego w odniesieniu do bankowości elektronicznej (zob. tabela 1)[22]. Chodzi przede wszystkim o warunki, jakie powinny spełniać te urządzenia, jak: łatwe rozpoznawanie istotnych dla bezpieczeństwa zmian w urządzeniu do składania podpisu, rzetelnie weryfikowana autentyczność i ważność certyfikatów lub innych danych poświadczonych elektronicznie, poprawnie i czytelnie wykazywany wynik weryfikacji identyfikacji osoby składającej podpis elektroniczny, sygnalizowanie istotnych dla bezpieczeństwa zmian w urządzeniu służącym do weryfikacji podpisu elektronicznego[23].

Warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi zostały określone ustawowo. Stanowią one, obok regulacji o ochronie danych osobowych, tajemnicy bankowej, regulacji odnoszących się do zasad wydawania i używania elektronicznych instrumentów płatniczych, tzw. prawną kategorię środków ochrony bankowości elektronicznej. Do tej kategorii bezpieczeństwa bankowości elektronicznej zalicza się również znormalizowane środki ochrony, czyli normy ISO[24]. Należą do nich między innymi:

- norma ISO IEC 9126, która określa jakość oprogramowania w zakresie funkcjonalności, niezawodności, użyteczności, wydajności, utrzymywalności i przenośności,
- norma ISO IEC 27001, która definiuje takie cechy bezpieczeństwa, jak: poufność, integralność, dostępność i rozliczalność,
- norma ISO 15408, która określa kryteria wykorzystywane do oceny właściwości zabezpieczeń produktów i systemów teleinformatycznych[25].

---

21 Por. A. Gospodarowicz (red.), *Bankowość elektroniczna*, PWE, Warszawa 2005, s. 72 i dalsze; S. Wojciechowska-Filipek, *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010, s. 77 i dalsze.

22 Art. 18. Ustawa o podpisie elektronicznym z dnia 18 września 2001 r., Dz.U. 2001, Nr 130, poz. 1450 z późn. zm.

23 *Ibidem*.

24 S. Wojciechowska-Filipek, *Technologia…*, *op. cit.*, s. 83.

25 *Ibidem*.

Badania bezpieczeństwa IT, przeprowadzone przez uczestniczące w projekcie instytucje: KPMG, ZBP, miesięcznik „BANK", wykazały, że:

- główne czynniki powodujące zagrożenia bezpieczeństwa transakcji realizowanych za pośrednictwem kanałów elektronicznych to: brak lub niewystarczająca świadomość zagrożeń istniejących po stronie użytkowników (47%), luki w bezpieczeństwie oferowanych na rynku rozwiązań (29%) oraz niewystarczające mechanizmy bezpieczeństwa zaimplementowane w kanałach elektronicznych (19%),
- najczęściej występującymi w bankach rodzajami incydentów z zakresu bezpieczeństwa systemów informatycznych są incydenty związane z usługą e-mail typu *spamming* oraz *phishing* (21%),
- wdrożone standardy bezpieczeństwa funkcjonujące w bankach to środki bezpieczeństwa w postaci normy ISO/IEC 27001 (wdrożyło je 54% respondentów), 36% wdrożyła normę ISO/IEC 17799, a 27% normę BS 7799[26].

W kontekście bezpieczeństwa bankowości elektronicznej istotne jest rozróżnienie między bezpieczeństwem informacji a bezpieczeństwem teleinformatycznym. Jak pisze A. Białas: „bezpieczeństwo teleinformatyczne, czyli odnoszące się do systemów teleinformatycznych, związane jest ze spełnieniem pewnych właściwości, czyli tzw. atrybutów bezpieczeństwa w systemach oraz w ich otoczeniu"[27]. Chodzi o tzw. aspekty bezpieczeństwa, do których zalicza się: integralność, poufność, dostępność, autentyczność, rozliczalność oraz niezawodność. „Bezpieczeństwo teleinformatyczne dotyczy instytucji wykorzystujących technologie informatyczne w swojej działalności i służy niezakłóconemu funkcjonowaniu tych instytucji…bezpieczeństwo informacji ma szersze znaczenie…gdyż obejmuje także informację znajdującą się poza systemami teleinformatycznymi, a więc występującą na przykład w postaci dokumentów papierowych, mikrofilmów oraz w postaci zapamiętanej, i wymieniane przez człowieka bezpośrednio lub za pomocą środków łączności"[28].

System nadzoru oparty na analizie ryzyka z wykorzystaniem metodyki BION (badanie i ocena nadzorcza), uruchomiony w KNF, wprowadził kategorię ryzyka bezpieczeństwa. Mapa klas ryzyka zawiera nie tylko rodzaje ryzyka bankowego, ale również ich definicje. Ryzyko bezpieczeństwa definiowane jest jako ryzyko zakłócenia funkcjonowania podmiotu lub strat finansowych w wyniku niedostatecznej ochrony jego zasobów i informacji[29]. Tak interpretowane ryzyko bezpieczeństwa obejmuje praktycznie wszystkie rodzaje ryzyka bankowego ponieważ:

---

[26] www.kpmg.pl/bezpieczeństwo IT w bankach (dostęp: 21.09.2011 r.).
[27] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, wyd. II, Wydawnictwa Naukowo-Techniczne, Warszawa 2007, s. 28.
[28] *Ibidem*, s. 27–28.
[29] www.knf.gov.pl/o nas/Urząd Komisji (dostęp: 20.09.2011 r.).

- ryzyko zakłócenia funkcjonowania podmiotu jest najszerszą kategorią ryzyka, czyli praktycznie każdy rodzaj ryzyka bankowego może być przyczyną zakłócenia funkcjonowania banku,
- każde zakłócenie to ryzyko wystąpienia straty, która ze względu na pomiar (lub szacowanie) ryzyka ma wymiar finansowy,
- podstawowymi komponentami ryzyka bezpieczeństwa są posiadane przez bank zasoby, zarówno materialne, jak i niematerialne.

Wszystkie rodzaje ryzyka, odnoszące się do zasobów banku i informacji, wzajemnie się przenikają, co prowadzi do ryzyka obniżenia lub utraty płynności, następnie ryzyka kapitałowego, a w ostatecznym efekcie do ryzyka zarządzania bankiem, które można uznać za jednoznaczne ze spadkiem lub brakiem bezpieczeństwa funkcjonowania banku (por. wykres 2).

Niedostateczna ochrona zasobów to ochrona zasobów ludzkich, rzeczowych, kapitałowych, a takimi są przede wszystkim środki pieniężne, w przypadku których może wystąpić ryzyko prania brudnych pieniędzy. Jest ono definiowane przez KNF jako ryzyko poniesienia strat w wyniku zamieszania w proceder prania brudnych pieniędzy prowadzony przez klientów, pośredników lub pracowników. Bank, jako instytucja obowiązana, przeprowadzająca transakcję, której równowartość przekracza 15 000 euro, ma obowiązek ją zarejestrować[30].

W przypadku wystąpienia ryzyka prania brudnych pieniędzy (np. przy zawieraniu umowy, przeprowadzaniu transakcji z klientem lub gdy istnieje podejrzenie prania pieniędzy), bank stosuje środki bezpieczeństwa finansowego, które polegają na:

- identyfikacji klienta i weryfikacji jego tożsamości, na podstawie dokumentów lub informacji publicznie dostępnych,
- podejmowaniu czynności w celu identyfikacji beneficjenta rzeczywistego i stosowaniu uzależnionych od oceny ryzyka odpowiednich środków weryfikacji jego tożsamości, w tym ustaleniu struktury własności i zależności klienta,
- uzyskiwaniu informacji dotyczących celu i zamierzonego przez klienta charakteru stosunków gospodarczych,
- bieżącym monitorowaniu transakcji gospodarczych z klientem, a w miarę możliwości badaniu źródła pochodzenia wartości majątkowych oraz bieżącym aktualizowaniu posiadanych dokumentów i informacji[31].

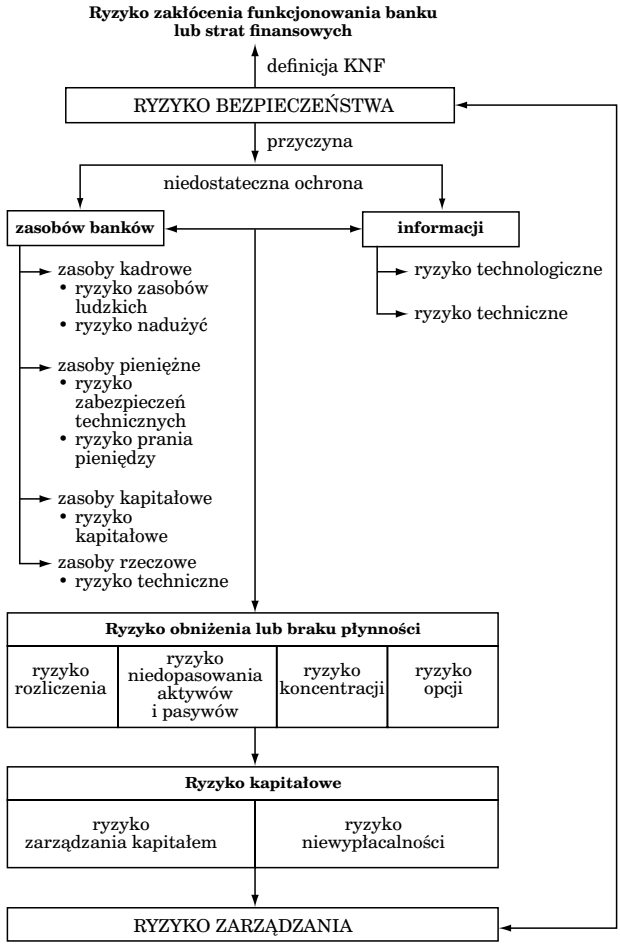
Powyższy przegląd wybranych, ustawowych regulacji w zakresie szeroko ujmowanego bezpieczeństwa funkcjonowania banku wyraźnie wskazuje na swoistą triadę zależności typu: zagrożenia – ryzyko – bezpieczeństwo.

---

[30] Art. 8. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 16 listopada 2000 r., Dz.U. z 2010 r., Nr 46, poz. 276.

[31] *Ibidem*, art. 8b.

Wykres 2. Komponenty ryzyka bezpieczeństwa i ich powiązania



Źródło: opracowanie własne.

W tym kontekście można mówić o trzecim podejściu do definiowania bezpieczeństwa banku. Bezpieczeństwo banku to stan, w którym bank:

- ma sprawny system monitorowania i kontrolowania zagrożeń,
- ma mechanizmy i instrumenty pozwalające zapobiegać przekształceniu zagrożeń w konkretne rodzaje ryzyka bankowego,
- zarządza ryzykiem bankowym tak, aby wielkość podejmowanego ryzyka mieściła się w ustalonych granicach określonych regulacjami nadzorczymi (np. limitami, normami),

- ma zdolność do absorpcji nieoczekiwanych strat w przypadku wystąpienia szoków zewnętrznych i wewnętrznych.

Zarządzanie bezpieczeństwem banku to zarządzanie ryzykiem bankowym.

PODSUMOWANIE

Powyższe rozważania to jedynie zasygnalizowanie złożoności zarządzania bezpieczeństwem banku, co wynika z jego wielowymiarowości. Zarządzanie bankiem to zarządzanie bezpieczeństwem, czyli zarządzanie ukierunkowane na przeciwdziałanie zagrożeniom, które mogą przekształcić się w konkretny rodzaj ryzyka, który po przekroczeniu optymalnego poziomu powoduje spadek bezpieczeństwa banku. Przedstawione w opracowaniu problemy wielowymiarowości bezpieczeństwa i odnoszące się do nich regulacje prawne zostały ograniczone do krajowego systemu bankowego. Nie należy zapominać, że jest to wprawdzie jedynie ujęcie mikro, ale w dobie globalizacji i integracji rynku finansowego bezpieczeństwo finansowe instytucji finansowych i kredytowych to podstawa nowej architektury finansowej, a przede wszystkim większej harmonizacji regulacji prawnych w tym zakresie.

Bibliografia

Wydawnictwa zwarte

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, wyd. II, Wydawnictwa Naukowo-Techniczne, Warszawa 2007.

Capiga M., Gradoń W., Szustak G., *Adekwatność kapitałowa w ocenie bezpieczeństwa banku*, CeDeWu.Pl. Platinium, Warszawa 2011.

Capiga M., Gradoń W., Szustak G., *Sieć bezpieczeństwa finansowego*, wyd. I, CeDeWu. Pl Platinium, Warszawa 2010.

Gospodarowicz A. (red.), *Bankowość elektroniczna*, PWE, Warszawa 2005.

Iwanicz-Drozdowska M., *Zarządzanie finansowe bankiem*, PWE, wyd. II, Warszawa 2010.

Marcinkowska M., *Standardy kapitałowe banków. Bazylejska Nowa Umowa Kapitałowa w polskich regulacjach nadzorczych*, Regan Press, Gdańsk 2009.

Szczepańska O., *Stabilność finansowa jako cel banku centralnego. Studium teoretyczno-porównawcze*, Wydawnictwo Naukowe SHOLAR, Warszawa 2008.

Wojciechowska-Filipek S., *Technologia informacyjna w usługach bankowości elektronicznej*, Difin, Warszawa 2010.

Artykuły prasowe

Zdanowicz B., *Podstawowe dylematy i kryteria wyboru formuły systemu gwarantowania depozytów w świetle teorii i doświadczeń międzynarodowych*, „Bezpieczny Bank" Nr 1 (34)/2007.

Dokumenty prawne

Ustawa o Bankowym Funduszu Gwarancyjnym z dnia 14 grudnia 1994 r., Dz.U. 1995 Nr 4 poz. 18, z późn. zm.

Ustawa o Narodowym Banku Polskim z dnia 29 sierpnia 1997 r., Dz.U. 1997 Nr 140 poz. 938 z późn. zm.

Ustawa Prawo Bankowe z dnia 29 sierpnia 1997 r., Dz.U. Nr 140 poz. 939 z późn. zm.

Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 16 listopada 2000 r., Dz.U. z 2010 r. Nr 46, poz. 276.

Ustawa o podpisie elektronicznym z dnia 18 września 2001 r., Dz.U. 2001 Nr 130, poz. 1450 z późn. zm.

Ustawa o elektronicznych instrumentach płatniczych z dnia 12 września 2002 r., Dz.U. 2002 r. Nr 169 poz. 1385 z późn. zm.

Ustawa o nadzorze nad rynkiem finansowym z dnia 21 lipca 2006 r., Dz.U. 2006 Nr 157, poz. 1119 z późn. zm.

Ustawa o Komitecie Stabilności Finansowej z dnia 7 listopada 2008 r., Dz.U. Nr 2009, poz. 1317.

Materiały internetowe

www.knf.gov.pl/o nas/Urząd Komisji (dostęp: 20.09.2011 r.).

www.kpmg.pl/bezpieczeństwo IT w bankach (dostęp: 21.09.2011 r.).

www.mf.gov.pl/bezpieczeństwo finansowe (dostęp: 21.09.2011 r.).