Spis treści

Wstęp

Ryzyko towarzyszy finansom od początków ich istnienia. W różnych okresach przypisywano problematyce ryzyka finansowego różne priorytety i odmienny był wpływ tej problematyki na rozwój społeczeństwa i gospodarki. Niezmiennie jednak ryzyku każdej działalności finansowej zawsze towarzyszyło z jednej strony przekonanie o potencjalnych korzyściach, jakie można osiągnąć, ponosząc to ryzyko, z drugiej zaś świadomość konieczności jego ograniczania. W starożytnym Egipcie procent od udzielonej pożyczki nie mógł przekraczać dwukrotnej wartości kapitału[1]. W XII wieku w zachodniej Europie zaczął upowszechniać się weksel imienny, pozwalający na bezpieczniejsze przekazywanie kapitału na odległość[2]. W drugiej połowie XVII wieku złotnicy angielscy przeprowadzali emisje kwitów depozytowych, których wartość przekraczała wartość posiadanych przez nich zasobów złota, gdyż mało prawdopodobne było – jak uważali – że wszyscy posiadacze kwitów zgłoszą się po swoje złoto jednocześnie[3]. Dzisiaj, szczególnie w kontekście ostatniego kryzysu światowych rynków finansowych, uzasadnione jest stwierdzenie, zgodnie z którym współczesne finanse determinowane są przez zarządzanie różnego rodzaju ryzykami. Aby jednak ryzykiem zarządzać, należy umieć dokonywać jego pomiaru. Stwierdzić zatem można, że funkcjonowanie współczesnego systemu finansowego warunkowane jest przez naszą umiejętność ilościowego opisu ryzyka we wszystkich niemal jego przejawach. Znakomicie uogólnił ten problem P.L. Bernstein, pisząc, że umiejętność formułowania precyzyjnych prognoz dotyczących możliwego przebiegu przyszłych zdarzeń i dokonywania wyborów między rozmaitymi alternatywami jest najistotniejszym aspektem życia współczesnych społeczeństw[4].

Ryzyko w potocznym znaczeniu i codziennym zastosowaniu jest konglomeratem różnorodnych problemów, które rozpatrujemy w odniesieniu do indywidualnych zjawisk czy sytuacji. Wydawać by się więc mogło, że wielość aspektów, w jakich należy analizować potocznie rozumiane ryzyko, nie pozwala na jego efektywną formalizację czy opis ilościowy. W wielu przypadkach tak rzeczywiście jest. Czy potrafimy bowiem podać dokładną wartość obrazującą ryzyko przegrania partii szachowej związane z wykonaniem danego posunięcia, ryzyko utraty środków zainwestowanych w zakłady bukmacherskie, ryzyko wypadku związane z rozmawianiem przez telefon komórkowy w czasie prowadzenia samochodu czy ryzyko określonych konsekwencji wynikających z opóźnienia w złożeniu na czas tekstu pracy naukowej? Nawet gdyby w każdym z tych przykładów zdefiniować tylko jeden poten-

[1] W. Morawski, *Zarys powszechnej historii pieniądza i bankowości*, Trio, Warszawa 2002, s. 16.
[2] Tamże, s. 49.
[3] Tamże, s. 78.
[4] P.L. Bernstein, *Przeciw bogom. Niezwykłe dzieje ryzyka*, WIG Press, Warszawa 1997, s. XIV.

cjalny skutek przytoczonych stanów, jaki powinna uwzględnić analiza, to i tak liczba zmiennych tej analizy praktycznie by ją uniemożliwiła. A jednak problemy tego typu – a także wiele innych – udaje się w pewien sposób rozwiązywać. W beznadziejnym – na pozór – starciu z nieobliczalnym ryzykiem ludzkiej działalności we wszelkich jej wymiarach z pomocą przychodzi prawdopodobieństwo – fundamentalny instrument kontrolowania ryzyka, pozwalający podejmować decyzje w tych sytuacjach, w których podejścia deterministyczne nie dają się w żaden sposób zastosować. Prawdopodobieństwo pozwala nie tylko określić pewien poziom ryzyka związanego z daną sytuacją, ale także umożliwia zdefiniowanie poziomu ryzyka dającego się zaakceptować. Konstruktor rakiety, która wyniosła na orbitę misję księżycową Apollo 1, ujął to w taki oto sposób: „Potrzebny ci jest zawór, który nie przecieka, i robisz wszystko, co w twojej mocy, żeby taki zawór skonstruować. Ale w realnym świecie istnieją tylko nieszczelne zawory. Musisz więc określić, jaki poziom nieszczelności jesteś w stanie tolerować”[5]. Czy jednak prawdopodobieństwo w każdym przypadku jest właściwym narzędziem opisu ryzyka? Na tak postawione pytanie stara się między innymi odpowiedzieć niniejsza praca.

Ryzyko we współczesnym świecie przejawia się w wielu aspektach. Niewątpliwie jednak najwięcej starań podejmujemy, aby kontrolować ryzyko tam, gdzie od naszych ryzykownych decyzji zależą szeroko rozumiane kwestie finansowe. Dotyczy to zarówno finansów osobistych, jak i świata wielkiego biznesu. Praca niniejsza jest próbą odniesienia problematyki ryzyka do jednego z obszarów funkcjonowania współczesnego biznesu, jakim jest wykorzystywanie rozwiązań informatycznych w bankowości. Jest to obszar szczególny, z jednej strony bowiem wymaga rozwiązań o bardzo wysokim poziomie bezpieczeństwa informatycznego, z drugiej zaś – musi umożliwiać dostęp do systemów bankowości internetowej milionom klientów. Co więcej, w żadnym innym obszarze zastosowań informatyki incydenty związane z bezpieczeństwem nie przekładają się w tak dużym stopniu na straty reputacyjne, a w konsekwencji – na finansowe. Między innymi te cechy systemów informatycznych w bankowości czynią przedmiotowy obszar pracy szczególnie interesującym.

Funkcjonowanie instytucji bankowych nie jest dzisiaj możliwe bez zastosowania nowoczesnych technologii informatycznych. Stwierdzenie to można – a nawet powinno się – rozwinąć: technologie informatyczne warunkują poprawne funkcjonowanie instytucji bankowych, których specyfika działalności wymaga stosowania nowoczesnych, lecz jednocześnie sprawdzonych i bezpiecznych narzędzi informatycznych. Bankowość i informatyka stały się więc dziedzinami nierozerwalnie ze sobą związanymi. Co więcej, ich ścisła integracja ma charakter dynamiczny. Z jednej strony rozwój technologii informatycznych otwiera przed bankami nowe możliwości, z drugiej zaś rosnące potrzeby banków, związane głównie z bezpieczeństwem przetwarzania i przesyłania danych w postaci elektronicznej, stymulują rozwój i doskonalenie tych technologii. Niewątpliwie jednak właśnie problemy związane z po-

[5] Tamże, s. XV.

ufnością, integralnością i dostępnością danych w największym stopniu spowalniają implementację nowych, elektronicznych produktów i usług bankowych. Warty zauważenia jest również fakt, że problemy te dotyczą w równym stopniu systemów bankowych w krajach wysoko rozwiniętych, jak i w krajach, gdzie informatyka bankowa stawia dopiero pierwsze kroki. Między innymi dlatego wśród ryzyk związanych z działalnością bankową coraz częściej na eksponowanym miejscu wymienia się ryzyko operacyjne, a w szczególności jeden z jego elementów – ryzyko informatyczne.

Wybór obszaru tematycznego niniejszej pracy nie jest więc przypadkowy. Wolumen oraz wartość danych przetwarzanych w bankowych systemach informatycznych są wyzwaniem dla współczesnej informatyki. Bezpieczeństwo tych danych decyduje bowiem już nie tylko o efektywności funkcjonowania banku, lecz wręcz o jego istnieniu. Zarządzanie ryzykiem informatycznym w bankowości stało się więc jednym z kluczowych elementów procesu zarządzania bankiem. Element ten, nie będąc związany bezpośrednio z problematyką bankową, tworzy swego rodzaju klamrę umożliwiającą optymalne funkcjonowanie instytucji bankowej.

Celem głównym niniejszego opracowania jest przedstawienie problematyki ryzyka informatycznego w działalności bankowej. Dyskusyjne byłoby stwierdzenie, że jest to problematyka nowa. Ryzyko związane z zastosowaniami rozwiązań informatycznych w bankowości dostrzegane i analizowane było zarówno w rozważaniach teoretycznych, jak i praktycznych od dawna. Analizy te jednak najczęściej pomijały szczegółowy opis najistotniejszego elementu omawianej tematyki, jakim jest szacowanie ryzyka, prezentując je w sposób uproszczony i pozbawiony kompleksowych koncepcji ilościowych.

Realizacja celu głównego ukierunkowała zakres tematyczny pracy, tworząc jednocześnie wiązkę celów pobocznych, wśród których na szczególną uwagę zasługują:

– przyjęcie koncepcji terminologicznej wykorzystywanej w pracy oraz wprowadzenie do problematyki ryzyka informatycznego i zarządzania tym ryzykiem, podkreślające merytoryczną relację pomiędzy oboma pojęciami,
– identyfikacja specyficznych dla bankowości atrybutów oraz obszarów zarządzania ryzykiem informatycznym,
– wskazanie na problematykę ilościowego szacowania ryzyka informatycznego jako na kluczowy czynnik warunkujący jakość procesu zarządzania ryzykiem oraz przedstawienie wybranych metod ilościowych, które są bądź mogłyby być wykorzystywane w procesach szacowania ryzyka informatycznego,
– omówienie podstaw finansowych aspektów zarządzania ryzykiem informatycznym,
– zaproponowanie nowej, oryginalnej koncepcji definiowania, szacowania i opisu ryzyka informatycznego.

Powyższa wiązka celów została zdefiniowana na bazie następujących założeń badawczych:

1. Ilościowe podejście do zarządzania ryzykiem informatycznym w polskojęzycznej literaturze przedmiotu praktycznie nie istnieje[6]. Monograficzna literatura angielskojęzyczna rozpatruje je natomiast głównie w aspekcie standardowych, prostych metod, wykorzystujących najczęściej klasyczne podejścia, bazujące na koncepcjach straty oczekiwanej oraz jej pochodnych. Wśród wielu zagranicznych publikacji konferencyjnych znajdują się jednak bardzo wartościowe przykłady opisów projektów badawczych, ukierunkowanych na analizę możliwości zastosowań metod ilościowych w szeroko rozumianym zarządzaniu bezpieczeństwem informatycznym oraz zarządzaniu ryzykiem informatycznym. Przeglądowy wybór tych publikacji powinien być przedstawiony w postaci zwartego opracowania tak, aby zobrazować dostępne możliwości wspomagania procesu szacowania ryzyka informatycznego.

2. Ryzyko informatyczne nie jest zjawiskiem nowym. Dotychczas ryzyko to opisywane było jednak głównie w kontekście problematyki bezpieczeństwa informatycznego. Znaczenie ryzyka informatycznego – szczególnie w bankowości – nakazuje jednak, aby nadawać mu charakter zagadnienia wiodącego, które integruje inne obszary problemowe.

3. Terminologiczne podstawy ryzyka informatycznego nie są ujednolicone. Dyskusyjność definicji normatywnych przekłada się na wielość i brak spójności propozycji literaturowych.

4. Problematyka ryzyka informatycznego jest istotna w kontekście rekomendacji Komisji Nadzoru Finansowego, związanych z zarządzaniem ryzykiem operacyjnym w bankowości.

Praca ma charakter interdyscyplinarny. Łączy w sobie zagadnienia związane z informatyką, bankowością, metodami ilościowymi, narzędziami analizy finansowej, a także praktyką tworzenia i eksploatacji rozwiązań informatycznych. Głównym obszarem zainteresowań autora jest jednak bankowość, stąd zarówno prezentacje problemów informatycznych, jak i opisy teoretycznych podstaw i praktycznych aspektów zastosowań metod ilościowych ukierunkowane są na przedstawienie możliwości, jakimi dysponować może współczesny bank w obszarze ilościowego wspomagania zarządzania ryzykiem informatycznym. Czytelnik zainteresowany zagadnieniami wykraczającymi poza główny temat pracy może skorzystać z bogato zaprezentowanej informacji bibliograficznej. Interdyscyplinarny charakter opracowania niewątpliwie traktować należy jako cechę, która w zależności od kontekstu może być postrzegana jako zaleta bądź wada. Autor wszak uznał, że owa interdyscyplinarność może stanowić o nowatorskim charakterze sposobu prezentacji omawianej problematyki.

Opracowanie ukierunkowane zostało na udowodnienie przedstawionych poniżej hipotez:

---

[6] Wskazać jednak należy na wyjątki, jakimi są wielokrotnie przytaczane w niniejszej pracy opracowania A. Białasa oraz K. Lidermana. Jednak i one nie prezentują zagadnienia w ujęciu kompleksowym.

1. Specyfika działalności bankowej implikuje konieczność przypisywania problematyce zarządzania ryzykiem informatycznym szczególnego charakteru, odzwierciedlającego wagę i znaczenie zarządzania tym rodzajem ryzyka w banku.

2. Ilościowe szacowanie ryzyka informatycznego, wykorzystujące metody spełniające wymagania definiowane w procesie zarządzania ryzykiem, jest kluczowym czynnikiem warunkującym jakość tego procesu.

3. Analiza finansowych aspektów zarządzania ryzykiem informatycznym w banku nie jest zadaniem prostym. Jej efektywność musi być pochodną wielu założeń i uproszczeń analizowanego zagadnienia.

4. Ryzyko informatyczne w banku nie w każdym przypadku może być postrzegane przez pryzmat standardowych narzędzi statystycznych, dlatego na uwagę zasługują koncepcje szacowania i opisu ryzyka nie wykorzystujące pojęć prawdopodobieństwa i rozkładu zmiennej losowej, korzystające natomiast z atrybutów metod oceny bezpieczeństwa informatycznego.

Praca składa się z pięciu rozdziałów. Rozdział pierwszy wprowadza w problematykę ryzyka informatycznego. Wprowadzenie to rozpoczyna krótki zarys merytoryczny problemu ryzyka we współczesnej nauce, wzbogacony przykładami propozycji systematyki ryzyka w ujęciu ogólnym. W rozdziale przedstawiono także podstawowe pojęcia związane bezpośrednio lub pośrednio z omawianym zagadnieniem. Szczególnie dużo miejsca poświęcono terminologicznym i merytorycznym analizom pojęć ryzyka, niepewności i prawdopodobieństwa. Wskazano również na rosnące we współczesnej bankowości znaczenie ryzyka operacyjnego jako pojęcia szerszego niż ryzyko informatyczne. Dokonano także niezwykle istotnej – z punktu widzenia merytorycznej poprawności opracowania – analizy współzależności bezpieczeństwa informatycznego i ryzyka informatycznego oraz zarządzania bezpieczeństwem informatycznym i zarządzania ryzykiem informatycznym. Podkreślono związki i relacje istniejące pomiędzy tymi pojęciami. W ostatnim podrozdziale przedstawiono kluczową dla dalszych treści analizę współistnienia metod oceny bezpieczeństwa oraz metod szacowania ryzyka, nawiązującą do czwartej z wymienionych powyżej tez pracy. Rozdział przedstawia także normatywno-literaturowe ujęcie problemu zarządzania ryzykiem informatycznym. Za postawę opisu wybrano normę PN ISO/IEC 27005, niemniej opis ten w wielu miejscach wzbogacono odniesieniami do innych norm, analizami literatury przedmiotu, a przede wszystkim krytycznym spojrzeniem autora na treść norm ISO dotyczących omawianego zagadnienia[7]. Szczególnie wiele miejsca poświęcono w rozdziale problematyce analizy ryzyka.

[7] Zakresowi wykorzystania w niniejszej pracy treści norm ISO należy się komentarz. Każda dziedzina charakteryzuje się odmiennym wpływem dokumentów normatywnych zarówno na rozważania teoretyczne, jak i na praktykę. W dziedzinie szeroko rozumianego zarządzania finansami normy ISO (oraz ich polskojęzyczne odpowiedniki) nie są powszechnie akceptowaną podstawą rozpraw naukowych. W dziedzinach związanych z technologiami informatycznymi sytuacja ta jest jednak wyraźnie inna. Literatura przedmiotu zastosowań informatyki za punkt wyjścia swoich rozważań powszechnie przyjmuje właśnie koncepcje normatywne. Praca niniejsza jest jednym z niewielu polskojęzycznych opracowań, które treść najważniejszych dla omawianej problematyki norm poddaje krytyce.

Rozdział drugi prezentuje praktyczne problemy zarządzania ryzykiem informatycznym w banku, koncentrując swoją uwagę na takich zagadnieniach, jak prawne i rekomendacyjne aspekty bezpieczeństwa informatycznego oraz zagrożenia, podatności i środki ochrony w bankowych systemach informatycznych. W rozdziale przedstawiono w ramowym ujęciu specyficzne cechy rozwiązań informatycznych wykorzystywanych we współczesnej bankowości. Przybliżono takie zagadnienia, jak zakres funkcjonalny systemów informatycznych w bankowości oraz ich architektura techniczno-aplikacyjna. Wskazano również na specyficzne atrybuty użytkowników bankowych systemów informatycznych oraz środowiska, w którym funkcjonują. Istotnym elementem rozdziału jest także krótka dyskusja terminologiczna nad pojęciem bankowości elektronicznej. Nieco więcej miejsca poświęcono w rozdziale opisowi obszarów ryzyka informatycznego w bankowości, podkreślając ich specyfikę oraz wpływ na funkcjonowanie współczesnych banków. W ramach opisu wybranych obszarów znalazły się między innymi prezentacje takich zagadnień, jak zastosowania kryptografii, problemy kontroli dostępu i wykrywania anomalii czy organizacyjne aspekty zarządzania ryzykiem informatycznym. Identyfikacji obszarów ryzyka informatycznego w działalności bankowej dokonano między innymi na podstawie analizy konstrukcji i zawartości systemu ZORO (Zdarzeń z Obszaru Ryzyka Operacyjnego) zarządzanego przez Centrum Prawa Bankowego i Informacji.

Rozdział trzeci przedstawia przegląd wybranych metod ilościowych wspomagających proces szacowania ryzyka informatycznego w banku. Przegląd poprzedzono podstawowym wprowadzeniem do problematyki teorii pomiaru. Za podstawę prezentacji metod uznano podział na metody wykorzystujące teorie matematyczne oraz metody będące prostymi algorytmami, tworzonymi na potrzeby szacowania ryzyka. Wszystkie metody prezentowane w rozdziale zostały scharakteryzowane przez zestaw atrybutów istotnych z punktu widzenia możliwości implementacji tych metod w praktyce bankowej. W podsumowaniu rozdziału wskazano na możliwości zastosowań poszczególnych metod w zdefiniowanych wcześniej obszarach ryzyka informatycznego działalności bankowej.

W rozdziale czwartym przedstawione zostały najważniejsze informacje dotyczące finansowych aspektów zarządzania ryzykiem informatycznym. W rozdziale podkreślono nierozerwalny związek praktyki tworzenia, implementowania i użytkowania systemów zabezpieczeń z ich ekonomicznymi atrybutami. Zdefiniowane zostały trzy finansowe obszary zarządzania ryzykiem informatycznym: zasobowy – związany z szacowaniem wartości zasobów systemowych, zagrożeniowy – związany z szacowaniem potencjalnych strat z punktu widzenia banku, wynikających z realizacji zagrożeń bezpieczeństwa, oraz inwestycyjny – związany z analizami efektywności inwestycji w obszarze zarządzania ryzykiem informatycznym. W ramach tak zidentyfikowanych obszarów dokonano prezentacji metod finansowej analizy problemu. Wyboru dyskutowanych koncepcji dokonano pod kątem możliwości ich zastosowań w praktyce bankowej.

Rozdział ostatni zawiera propozycję nowego spojrzenia na problematykę ryzyka informatycznego w działalności bankowej. Zaproponowano w nim nową definicję ryzyka informatycznego, krytyce poddano opisywane w poprzednich rozdziałach klasyczne podstawy analizy i oceny problemu, w szczególności interpretacje prawdopodobieństwa wystąpienia zdarzenia oraz możliwości szacowania strat w ujęciu pieniężnym. Na potrzeby prowadzonej w rozdziale dyskusji zdefiniowano cztery tezy[8], które poddano próbie uzasadnienia. Najistotniejszym elementem koncepcji jest propozycja nowej metody szacowania ryzyka informatycznego na potrzeby zarządzania tym ryzykiem w działalności bankowej.

Realizacja celów i weryfikacja hipotez badawczych wymagały zastosowania odpowiednich metod badawczych. Zwłaszcza osiągnięcie celu głównego możliwe było dzięki analizie i krytyce piśmiennictwa, wzbogaconym analizami porównawczymi. Weryfikacja hipotez została natomiast zrealizowana z użyciem eksperymentów myślowych. Uzupełnieniem tych metod była analiza danych empirycznych, pozyskanych dzięki uprzejmości Związku Banków Polskich.

W pracy wykorzystano zarówno polską, jak i obcojęzyczną literaturę przedmiotu, ze zdecydowaną przewagą tej drugiej w rozdziałach trzecim i czwartym. Znaczny udział w spisie literatury mają publikacje pochodzące z materiałów specjalistycznych konferencji poświęconych zagadnieniom ewaluacyjnych i ekonomicznych aspektów bezpieczeństwa i ryzyka informatycznego. Warto także podkreślić, że praca nie dokonuje podziału na literaturę związaną z bezpieczeństwem informatycznym oraz ryzykiem informatycznym. Pojęcia te bowiem przenikają się w opracowaniach naukowych, a ich wzajemne relacje nie są jednoznacznie zdefiniowane. Dyskusja nad tym problemem jest także jednym z wątków pracy.

Do najważniejszych elementów pracy, stanowiących oryginalny wkład w literaturę przedmiotu, zaliczyć należy:

- krytyczne spojrzenie na terminologiczne aspekty omawianej problematyki, szczególnie w kontekście definicji normatywnych (rozdział 1),
- zdefiniowanie relacji pomiędzy bezpieczeństwem informatycznym i ryzykiem informatycznym w różnych obszarach merytorycznych (podrozdział 1.7),
- próbę stworzenia podstaw klasyfikacji metod ilościowych możliwych do wykorzystania w procesach szacowania ryzyka informatycznego (rozdział 3),
- wieloaspektową ocenę wybranych metod szacowania ryzyka informatycznego (rozdział 3),
- krytykę powszechnie cytowanych koncepcji finansowej analizy problematyki ryzyka informatycznego (rozdział 4),
- propozycję nowego spojrzenia na problematykę ryzyka informatycznego, w szczególności dotyczącego metodyki szacowania i opisu tego ryzyka w działalności bankowej (rozdział 5).

[8] Są to tezy rozwijające hipotezy przedstawione powyżej.

Obszerne fragmenty książki są wynikiem prac badawczych prowadzonych w ramach projektu 1 H02B 016 30, zatytułowanego *Zastosowanie metod ilościowych w zarządzaniu ryzykiem informatycznym w bankowości z wykorzystaniem systemu SAP ERP*, realizowanego w latach 2006-2008 i finansowanego przez Ministerstwo Edukacji i Nauki.

* * *

Składam szczególne podziękowania prof. dr hab. Małgorzacie Iwanicz-Drozdowskiej oraz dr. hab. Krzysztofowi Jackowiczowi za niezwykle cenne i wzbogacające wartość merytoryczną rozprawy uwagi zawarte w recenzjach wydawniczych oraz prof. dr. hab. Andrzejowi Gospodarowiczowi za życzliwość, wsparcie merytoryczne i motywowanie do pracy. Dziękuję także Prezesowi Związku Banków Polskich Krzysztofowi Pietraszkiewiczowi za pomoc w uzyskaniu dostępu do zawartości baz danych zarządzanych przez Centrum Prawa Bankowego i Informacji.

Dariusz Wawrzyniak