PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 171

Finanse – nowe wyzwania teorii i praktyki 2011
Bankowość

Dariusz Wawrzyniak
Uniwersytet Ekonomiczny we Wrocławiu

ANALIZA EKONOMICZNO-FINANSOWA JAKO NARZĘDZIE ZARZĄDZANIA RYZYKIEM INFORMATYCZNYM W BANKU – WPROWADZENIE

Streszczenie: Dynamiczny rozwój informatyki oraz ekspansja jej zastosowań obejmująca już praktycznie wszystkie obszary współczesnego biznesu nadały problematyce zarządzania ryzykiem informatycznym nowego charakteru. Ryzyko to bowiem warunkuje dziś nie tylko poprawne funkcjonowanie, ale wręcz istnienie współczesnych instytucji, szczególnie instytucji finansowych. W artykule przedstawiono wybrane podstawowe zagadnienia związane z możliwościami zastosowań analiz ekonomiczno-finansowych w zarządzaniu ryzykiem informatycznym w banku. Przede wszystkim przedstawiono podstawy terminologiczne omawianego zagadnienia, wyszczególniono trzy jego fundamentalne obszary oraz wskazano na znaczenie identyfikacji kategorii ryzyka.

Słowa kluczowe: analiza ekonomiczno-finansowa, ryzyko informatyczne, bankowość.

1. Wstęp

Pojęcie ryzyka funkcjonuje dzisiaj w wielu dziedzinach i bazuje na potocznym rozumieniu tego terminu. Ryzyko to możliwość, prawdopodobieństwo, że coś się nie uda [*Uniwersalny*.... 2003, s. 1108][1]. Problematyka ryzyka znalazła swoje szczególne miejsce w naukach finansowych, zmieniając w pewnym sensie orientację zarówno badań teoretycznych, jak i praktyki biznesowej. Istotą funkcjonowania banków i instytucji finansowych jest dziś bowiem właśnie zarządzanie ryzykiem warunkowane zarówno przez wymogi skutecznego funkcjonowania na rynku usług finansowych, jak i wymogi regulacyjne. Ryzyko jest także immanentnym elementem procesów biznesowych realizowanych w obszarach niefinansowych. Systematyka ryzyk niefinansowych doczekała się już wielu opracowań, które łączy wyraźnie nasilająca się tendencja zestawiania pojęcia ryzyka ze wszystkimi niemal obszarami merytorycznymi (zob. np.: [Kaczmarek 2008]). O ile jednak ryzyka psychologiczne, socjo-

[1] Warto w tym miejscu zaznaczyć, że cytowany słownik nie dopuszcza użycia rzeczownika „ryzyko" w liczbie mnogiej. Inaczej problem traktuje natomiast *Słownik współczesnego języka polskiego* pod redakcją naukową Bogusława Dunaja, Wydawnictwo Wilga, 1996, w którym czytamy, że ryzyko w znaczeniu prawniczym – definiowane jako możliwość powstania szkody, obciążająca osobę poszkodowaną niezależnie od jej winy – ma liczbę mnogą (s. 990).

logiczne czy filozoficzne ciągle są dla większości pojęciami abstrakcyjnymi, o tyle ryzyko informatyczne nie jest już dla współczesnego społeczeństwa zjawiskiem ani nowym, ani zaskakującym. Co więcej, problematyka ryzyka informatycznego jest nierozerwalnie związana z każdym przejawem działalności biznesowej. Dynamiczny rozwój informatyki oraz ekspansja jej zastosowań obejmująca już praktycznie wszystkie obszary współczesnego biznesu w naturalny sposób implikują konieczność nadawania zagadnieniom związanym z ryzykiem informatycznym absolutnie najwyższych priorytetów. Artykuł niniejszy jest pierwszym z serii tekstów[2] prezentującym możliwości zastosowania narzędzi analizy finansowej w procesie zarządzania ryzykiem informatycznym w banku.

2. Bezpieczeństwo informatyczne i ryzyko informatyczne

Dyskusja nad problematyką finansowych aspektów zarządzania ryzykiem informatycznym nie może uniknąć przedstawienia fundamentalnego dla niej pojęcia, jakim jest pojęcie bezpieczeństwa. Bezpieczeństwem informatycznym nazywamy taki stan systemu[3], w którym określone atrybuty osiągnęły akceptowalny dla podmiotu dokonującego oceny bezpieczeństwa poziom[4]. Do atrybutów bezpieczeństwa zaliczamy:

- poufność – zapewniającą, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- integralność – gwarantującą, że dane nie zostały zmienione lub usunięte w sposób nieautoryzowany,
- autentyczność – zapewniającą, że tożsamość podmiotu lub zasobu jest taka jak deklarowana; dotyczy użytkowników, procesów, systemów lub nawet instytucji,
- dostępność – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo,
- rozliczalność – zapewniającą, że działania podmiotu mogą być jednoznacznie przypisane tylko temu podmiotowi,
- niezawodność – oznaczającą spójne, zamierzone zachowanie i skutki.

Zarządzanie bezpieczeństwem definiowane jest natomiast jako zespół cyklicznych procesów ukierunkowanych na zidentyfikowanie, osiągnięcie i utrzymanie założonego poziomu wymienionych powyżej atrybutów. Problematyka bezpieczeństwa przebyła w ostatnich latach bardzo długą drogę, podążając za rozwojem Internetu, zmianą świadomości informatycznej społeczeństwa, coraz większą dostępnością nowych technologii, a także rosnącym zakresem zastosowań informatyki, szczególnie w instytucjach finansowych. Bezpieczeństwo informatyczne przestało

[2] Interdyscyplinarny charakter omawianej problematyki ogranicza możliwość jej wyczerpującej prezentacji w ramach pojedynczego artykułu konferencyjnego.

[3] Znaczenie określenia „system" w przytoczonej definicji powinno być uwarunkowane jej kontekstem. Może być to zatem jeden konkretny system bądź ogół rozwiązań informatycznych wspomagających funkcjonowanie instytucji.

[4] Bezpieczeństwo informatyczne jest więc względne. Jego ocena zależy od założeń i kryteriów zdefiniowanych przez podmiot dokonujący tej oceny.

być postrzegane jako wyłączny problem specjalistów informatyków, zaczęło natomiast funkcjonować w świadomości społeczeństwa jako problem, który dotyczy nas wszystkich[5]. Efektem tych zmian jest m.in. swego rodzaju konwersja merytoryczna problemu, który coraz powszechniej analizowany jest w szerszym[6] kontekście ryzyka informatycznego – kategorii znanej i definiowanej od dawna, jednak trudnej do analizy i niełatwo poddającej się metodom ewaluacyjnym. Ryzyko informatyczne zyskało także na znaczeniu jako jeden z elementów ryzyka operacyjnego będącego przedmiotem rekomendacji Bazylejskiego Komitetu Nadzoru Bankowego[7]. Niewątpliwie jednym z istotniejszych głosów we współczesnej dyskusji terminologicznej nad pojęciem ryzyka informatycznego winny być definicje zawarte w normach ISO dotyczących zarządzania ryzykiem informatycznym. Jedną z takich norm jest ISO/IEC 27005:2008 będąca podstawą nowego standardu zarządzania bezpieczeństwem i ryzykiem informatycznym[8]. Zgodnie z normą ryzyko to kombinacja prawdopodobieństwa wystąpienia zdarzenia oraz potencjalnych strat wynikających z jego konsekwencji. Ryzyko według normy postrzegane jest zatem jako wartość pewnej funkcji dwóch zmiennych:

$$R = f(P(Z), S(Z)), \tag{1}$$

gdzie: R – ryzyko,
$P(Z)$ – prawdopodobieństwo wystąpienia zdarzenia Z,
$S(Z)$ – potencjalna strata wynikająca z wystąpienia zdarzenia Z.

[5] Jak pisze M.E. Johnson, ataki na systemy informatyczne coraz częściej wymierzone są przeciwko własności intelektualnej, tak więc o bezpieczeństwie informatycznym nie może już dzisiaj stanowić jedynie technologia – jego fundamentem musi być organizacyjna kultura bezpieczeństwa, w której każdy będzie w stanie zarządzać ryzykiem informatycznym na poziomie indywidualnych praw i obowiązków. Zob.: [Johnson 2005, s. 4]. Warto w tym kontekście zaznaczyć, że zmianę sposobu postrzegania problemów bezpieczeństwa determinuje w znacznym stopniu m.in. wzrost powszechności usług bankowości internetowej.

[6] Literatura przedmiotu prowadzi dyskusję nad wzajemnymi relacjami pomiędzy pojęciami bezpieczeństwa informatycznego i ryzyka informatycznego (zarządzania bezpieczeństwem i zarządzania ryzykiem). Większość autorów posługuje się modelem pojęciowym, w którym zarządzanie ryzykiem informatycznym jest jednym z procesów (elementów) zarządzania bezpieczeństwem. Jest to koncepcja dyskusyjna, jednak jej analiza wykracza poza główny temat niniejszego opracowania.

[7] Nowa Umowa Kapitałowa ma na celu międzynarodowe ujednolicanie regulacji nadzorczych dotyczących adekwatności kapitałowej – zob. np.: [Gospodarowicz 2009, s. 27-35]. Nie jest to więc regulacja bezpośrednio związana z problematyką ryzyka informatycznego, jednak zawarta w niej koncepcja postrzegania ryzyka operacyjnego w naturalny sposób implikuje m.in. konieczność ilościowego szacowania ryzyka informatycznego. Jest zatem NUK swego rodzaju katalizatorem zmian w procesach zarządzania ryzykiem informatycznym w bankowości. Szerszy opis tego zjawiska znaleźć można m.in. w: [Gospodarowicz, Wawrzyniak 2009, s. 57-70].

[8] Information technology. Security techniques. Information security risk management. Grupa norm ISO/IEC 27001, 27002, 27003, 27004, 27005 i następnych ma stanowić podstawę dla wszystkich norm ISO dotyczących omawianego zagadnienia. Podstawą terminologiczną norm jest ISO Guide 73:2009 – Risk Management – Vocabulary.

Powyższa definicja została niemal bezkrytycznie przyjęta przez literaturę przedmiotu i stanowi punkt wyjścia rozważań nad możliwościami ilościowego ujęcia ryzyka informatycznego. W poprzednich pracach autora niniejszego tekstu przeprowadzona została krytyka tego podejścia (zob. np.: [Wawrzyniak 2010, s. 183-203]). Zgodnie z zaproponowanymi w tych pracach definicjami ryzyko informatyczne *sensu stricto* to ilościowo bądź jakościowo wyrażone przekonanie podmiotu zarządzającego ryzykiem o przewidywanych atrybutach wystąpienia określonego zdarzenia (negatywnego z punktu widzenia bezpieczeństwa systemu) w danym okresie przyszłości. Atrybutami tymi najczęściej są liczność bądź czas trwania. Ryzyko informatyczne *sensu largo* to pewna syntetyczna miara ryzyk *sensu stricto* dotyczących danego obszaru, uzyskana w procesie szacowania ryzyka na podstawie założeń przyjętych przez podmiot zarządzający ryzykiem. Zarządzaniem ryzykiem informatycznym nazywamy natomiast kompleksowy proces identyfikowania, monitorowania oraz eliminowania lub minimalizowania wartości funkcji prawdopodobieństw realizacji zagrożeń bezpieczeństwa oraz ich skutków[9]. Szersza dyskusja nad terminologicznymi aspektami omawianego zagadnienia wykracza jednak poza ramy merytoryczne artykułu.

3. Analiza ekonomiczno-finansowa w przedsięwzięciach informatycznych

Analiza ekonomiczno-finansowa jest immanentnym elementem każdego procesu zarządzania. Jej głównym celem jest dostarczenie informacji o wynikach i sytuacji finansowej przedsiębiorstwa, niezbędnych w procesie zarządzania oraz wykorzystywanych przez otoczenie przedsiębiorstwa. Podstawowym kryterium oceny w procesie analizy ekonomiczno-finansowej winno być kryterium racjonalnego działania (por.: [Zaleska 2005, s. 9]). Interdyscyplinarność procesów biznesowych realizowanych przez współczesne instytucje – bez względu na branżę i specyfikę – doprowadziła do dywersyfikacji metod analizy finansowej pod kątem ich zastosowań w zarządzaniu poszczególnymi procesami – obszarami funkcjonowania instytucji. Jednym z wielu takich obszarów, które są przedmiotem analiz współczesnych metod finansowych, jest informatyka, a ściślej rzecz ujmując – jej zastosowania.

Problematyka ekonomicznej oceny i analizy przedsięwzięć informatycznych[10] jest obecnie przedmiotem wielu opracowań i prac badawczych. Przedsięwzięcie informatyczne definiowane jest w nich w sposób ogólny, pochodny definicji rekomendowanej przez stowarzyszenie Project Management Institute, zgodnie z którą przedsięwzięciem jest umiejscowiony w czasie zespół działań podejmowanych w celu stworzenia niepowtarzalnego produktu lub usługi [A Guide… 1996 i 2000], lub

[9] Definicja normatywna proponowana przez PN-ISO/IEC 27001:2007 definiuje zarządzanie ryzykiem jako skoordynowane działania kierowania organizacją i kontrolowania organizacji z uwzględnieniem ryzyka. Jest to definicja wyjątkowo dyskusyjna. Odchodzi bowiem od merytorycznych aspektów zagadnienia (identyfikacji, monitorowania, eliminowania), nie nawiązuje w żaden sposób do definicji ryzyka, pomija procesowy charakter problemu oraz jest niespójna wewnętrznie.

[10] Literatura przedmiotu, a przede wszystkim praktyka biznesowa, posługuje się także pojęciem projektu informatycznego.

w sposób bardziej szczegółowy – jako ogół działań, zasobów i powiązań między nimi mających na celu rozwiązanie problemu gospodarczego za pomocą narzędzi technologii informatycznej (ob. np.: [Lech 2007, s. 12]). H. Dudycz i M. Dyczkowski, prezentując podstawy terminologiczno-metodyczne problemu, wskazują m.in. na następujące atrybuty wyróżniające przedsięwzięcia w ujęciu ogólnym (tab. 1).

Tabela 1. Atrybuty przedsięwzięć

Atrybut	Charakterystyka
Celowość (zadaniowość, orientacja na wynik)	Celem przedsięwzięcia jest realizacja precyzyjnie zdefiniowanego efektu przedsięwzięcia*
Niepowtarzalność (jednokrotność, unikatowość)	Celem przedsięwzięcia jest zaspokojenie każdorazowo odmiennych potrzeb w różnych środowiskach i przy specyficznych ograniczeniach i wymaganiach
Złożoność	Przedsięwzięcia wymagają dekompozycji na zadania cząstkowe, koordynacji, zaangażowania różnorodnych zasobów
Ograniczoność czasowa	Przedsięwzięcia mają wyznaczone terminy rozpoczęcia i zakończenia
Znaczna autonomia funkcjonalna	Przedsięwzięcia są często niezależne i wyraźnie wydzielone z pozostałej, rutynowej działalności obiektu
Odrębność strukturalna	Przedsięwzięcia prowadzone są przez specyficzne struktury organizacyjne
Wielopodmiotowość	Uczestnikami przedsięwzięć są pracownicy różnych działów, także spoza obiektu
Specyfika zarządzania	Zarządzanie przedsięwzięciami oparte jest na specyficznych metodach

* Cytowani autorzy efekt przedsięwzięcia zastępują pojęciem „produktu lub usługi", co wydaje się jednak zawężać opis atrybutu, który powinien być możliwie jak najogólniejszy.

Źródło: opracowania własne na podstawie [Dudycz, Dyczkowski 2007, s. 16].

Czy na podstawie powyższych stwierdzeń można przyjąć, że działania realizowane w procesie zarządzania ryzykiem informatycznym ukierunkowane na systematyczne obniżanie poziomu tego ryzyka są przedsięwzięciami informatycznymi? Na potrzeby dalszych analiz przyjęto, że odpowiedź na tak postawione pytanie jest twierdząca, chociaż nie da się ukryć, że przedstawione powyżej charakterystyki atrybutów czynią tę odpowiedź dyskusyjną lub przynajmniej wymagającą uszczegółowienia[11]. Naturalnym następstwem tej odpowiedzi winna być konstatacja głosząca, iż analizy ekonomiczno-finansowe w obszarze zarządzania ryzykiem informa-

[11] Dyskusja na temat merytorycznych aspektów definicji przedsięwzięcia nie jest przedmiotem artykułu. Warto jednak zwrócić uwagę, że rozwój zastosowań informatyki rzadko poddaje się tego typu ograniczeniom pojęciowo-merytorycznym. W przypadku zarządzania ryzykiem informatycznym najbardziej dyskusyjnym atrybutem jest ograniczoność czasowa, chociaż wydaje się, że możliwe jest przyjęcie założenia, zgodnie z którym ograniczoność ta nie dotyczy działań wykonywanych w związku z realizacją określonego celu, lecz jest pochodną jedynie okresu analizy finansowej. Na przykład wykorzystywanie i udoskonalanie systemu wykrywania anomalii w bankowym systemie informatycznym nie jest ograniczone czasowo, a mimo to można wyodrębnić okresy, w ramach których system będzie oceniany np. pod kątem relacji nakładów do efektów.

tycznym mogą wykorzystywać te same narzędzia, z których korzystają procesy analizy i oceny efektywności przedsięwzięć informatycznych. Wiele opracowań naukowych w milczący sposób tezę taką przyjmuje. Czy jednak słusznie? Specyfika problematyki zarządzania ryzykiem informatycznym wyraźnie odbiega od standardowego modelu przedsięwzięcia informatycznego, który pomija (bądź przypisuje jej marginalne znaczenie) problematykę niewymiernych korzyści moralnych, a przede wszystkim niewymiernych strat moralnych, jakie z danym przedsięwzięciem mogą się wiązać. Podkreślić zatem należy, że rozdzielenie problematyki ekonomiki ryzyka informatycznego oraz ekonomiki zastosowań informatyki w sensie ogólnym jest warunkiem skutecznego zarządzania ryzykiem informatycznym. Nie oznacza to oczywiście, że oba obszary merytoryczne nie mają cech wspólnych. Wręcz przeciwnie, dotyczą ich podobne problemy wynikające z trudności w szacowaniu pewnych wartości, szczególnie związanych z zagadnieniem oceny efektywności.

4. Analiza ekonomiczno-finansowa w zarządzaniu ryzykiem informatycznym

Problematyka praktycznych aspektów bezpieczeństwa systemów informatycznych jest nierozerwalnie związana z ekonomicznymi aspektami tworzenia, implementowania i użytkowania systemów zabezpieczeń. Wątek finansowy przejawia się w omawianym zagadnieniu już w pierwszych – dzisiaj uznawanych za klasyczne – opracowaniach naukowych prezentujących teoretyczne i praktyczne problemy różnych obszarów zarządzania bezpieczeństwem. Za jeden z pierwszych istotnych głosów w dyskusji na temat finansowych aspektów omawianego zagadnienia uznać należy pracę R. Turna i N.Z. Shapiro [1972]. L.J. Hoffman, wskazując na doniosłość tych rozważań, cytuje następujący przykład [Hoffman 1982, s. 160 i nast.]: Załóżmy, że intruz pragnie zebrać listę N informacji, z których każda ma wartość rynkową k. Całkowita wartość listy wynosi więc $V = kN$. Żeby dokonać penetracji bazy danych, intruz dokonuje inwestycji X. Jeśli intruzowi potrzebny jest minimalny dochód rX, $r > 0$, to jego maksymalny wydatek w celu uzyskania listy wynosi:

$$X = \frac{kN}{1+r}. \tag{2}$$

W celu odparcia tego i innych zagrożeń osoba chroniąca bazę danych przeznacza na ochronę zasobów[12] wartość Y. Niech $I(X, Y)$ będzie przewidywaną ilością informacji uzyskiwaną przez intruza przeznaczającego X na przełamanie zabezpieczeń wdrożonych kosztem Y. Niech $f(N)$ będzie wartością N jednostek informacji uzyskanych przez intruza. Niech $g(N)$ będzie wartością tych informacji dla chroniącego. Dla określonych X i Y spodziewany zysk netto intruza, $v(X, Y)$, wynosi:

[12] Cytowany autor proponuje, aby przez wartość Y rozumieć nie nakłady inwestycyjne na ochronę, lecz ogół zastosowanych zabezpieczeń. Podejście takie wydaje się dyskusyjne, gdyż utrudnia dalszą analizę. Powyżej dokonano więc zamiany znaczenia Y na wartość inwestycji.

$$v(X,Y) = f\left(I(X,Y)\right) - X, \tag{3}$$

podczas gdy straty netto dla chroniącego informację wynoszą:

$$u(X,Y) = g\left(I(X,Y)\right) + Y. \tag{4}$$

Intruz może zmieniać swoje nakłady X w celu zmaksymalizowania wartości wyrażenia (3). Rozsądny obrońca będzie natomiast minimalizował wyrażenie (4). Wynika stąd, że jeżeli f i g oraz I są różniczkowalne w przedziale zawierającym X i Y, to wartości X i Y będą spełniały równania:

$$\begin{aligned} \frac{\partial}{\partial Y} f\left(I(X,Y)\right) \times \frac{\partial}{\partial X} I(Y,Y) = 1 \\ \frac{\partial}{\partial Y} g\left(I(X,Y)\right) \times \frac{\partial}{\partial Y} I(Y,Y) = -1 \end{aligned}. \tag{5}$$

L.J. Hoffman zauważa jednak, że tego typu analizy są niezwykle trudne do przeprowadzenia – a co za tym idzie – praktycznego zastosowania, ze względu na konieczność określenia $f(N)$, $g(N)$ oraz X[13].

W miarę rozwoju informatyki oraz ekspansji jej zastosowań problemy natury ekonomicznej zaczęły stanowić jedną z głównych determinant implementacji mechanizmów bezpieczeństwa, ograniczając możliwości wykorzystywania niektórych rozwiązań z powodu zbyt wysokich – w odniesieniu do potencjalnych korzyści – kosztów. Dostępność wielu różnych metod i mechanizmów bezpieczeństwa w naturalny sposób doprowadziła do powstania „obszarów substytucyjnych"[14] oferujących decydentom rozwiązania znacznie tańsze i jednocześnie gwarantujące akceptowalny – chociaż nie najwyższy z dostępnych – poziom bezpieczeństwa. Substytucyjność ta widoczna jest m.in. w mechanizmach bezpieczeństwa systemów detalicznych instytucji finansowych, które, kierując się względami ekonomicznymi, decydują się często na świadome obniżanie poziomu bezpieczeństwa oferowanych rozwiązań w zamian za ich znacznie niższe koszty. Sytuacja tego typu charakterystyczna jest m.in. dla krajowego rynku usług bankowości internetowej, na którym różnice w poziomie bezpieczeństwa oferowanych rozwiązań są bardzo widoczne[15]. Elektroniczna bankowość detaliczna przedkłada jednak aspekty kosztowe ponad aspekty bezpieczeństwa[16]. Nie

[13] Ta uwaga zasługuje na uznanie, gdyż wiele późniejszych opracowań w bezkrytyczny sposób traktowało problem wyznaczalności analogicznych wartości.

[14] Podkreślić należy, że substytucyjność ta ma w wielu przypadkach pozorny charakter, co wykazano w dalszej części.

[15] Na przykład w roku 2010 niektóre banki nadal wykorzystują w procesach autoryzacji operacji bankowości internetowej jawne listy haseł jednorazowych, podczas gdy wiele banków korzysta już wyłącznie z rozwiązań opartych na tokenach (sprzętowe, programowe, GSM). Różnice w poziomie bezpieczeństwa obu tych grup mechanizmów uznać należy za drastyczne.

[16] To dość radykalne stwierdzenie, jednak analiza rozwiązań wykorzystywanych przez bankowość internetową XXI wieku dostarcza zbyt wielu przykładów, aby uznawać je za dyskusyjne.

należy jednak traktować tego stwierdzania jako zarzutu. Elektroniczna bankowość detaliczna jest bowiem obszarem biznesu charakteryzującym się świadomą rezygnacją z wysokiego poziomu pewnych atrybutów bezpieczeństwa. Problematyka finansowych aspektów bezpieczeństwa i ryzyka informatycznego dotyczy jednak elektronicznej bankowości detalicznej w takim samym stopniu co innych obszarów działalności bankowej[17].

Współcześnie aspekt finansowy omawianego zagadnienia przejawia się w co najmniej trzech obszarach:

– zasobowym – związanym z szacowaniem wartości zasobów systemowych,
– zagrożeniowym – związanym z szacowaniem potencjalnych strat z punktu widzenia instytucji (bądź korzyści z punktu widzenia intruza) wynikających z realizacji zagrożeń bezpieczeństwa,
– inwestycyjnym – związanym z analizami opłacalności (efektywności) inwestycji w obszarze zarządzaniem ryzykiem[18].

Obszary te determinują podział zastosowań narzędzi analiz finansowych w procesach zarządzania ryzykiem informatycznym, aczkolwiek nie stanowią oddzielnych kategorii, lecz tworzą swego rodzaju hierarchię merytoryczną, w której wykonanie analiz obszaru niższego poziomu jest warunkiem możliwości wykonania analiz poziomu wyższego. Tak więc oszacowanie wartości zasobów systemowych jest konieczne do szacowania potencjalnych strat wynikających z realizacji zagrożeń bezpieczeństwa. Straty te zaś muszą być oszacowane, aby możliwe było wykonanie analiz efektywności. Hierarchiczność problemu znajduje także swoje odzwierciedlenie w merytorycznym zaawansowaniu metod analizy finansowej wykorzystywanych w poszczególnych obszarach. W obszarze zasobowym mogą to być bowiem:

– w przypadku zasobów sprzętowych i programowych – proste metody przypisujące zasobom wartości na podstawie księgowej wartości ich pozyskania lub wytworzenia,
– w przypadku danych – metody przypisujące zasobom szacunkowe wartości na podstawie eksperckich analiz.

W obszarze zagrożeniowym wśród możliwych do zastosowania metod analizy finansowej wskazać należy przede wszystkim na:

– statystyczne narzędzia oferujące analizy standardowych rozkładów zmiennych losowych,

---

[17] Elektroniczna bankowość detaliczna (szczególnie internetowa) jest także swego rodzaju papierkiem lakmusowym poziomu świadomości informatycznej społeczeństwa. Wykorzystuje ona bowiem niski poziom tej świadomości, oferując rozwiązania bardzo tanie, które jednak sprawiają wrażenie zaawansowanych.

[18] Problematyka pojęcia efektywności w informatyce oraz założeń metodycznych badania efektywności została wyczerpująco omówiona m.in. w: [Dudycz, Dyczkowski 2007]. Warto także zaznaczyć, że w ramach obszaru analizy efektywności mieści się również szacowanie kosztów implementacji mechanizmów bezpieczeństwa, co nierzadko postrzegane jest jako osobny problem. Wskazać też należy, że w ramach obszaru inwestycyjnego swoje miejsce znajduje zasygnalizowany powyżej problem „obszarów substytucyjnych".

– metody scenariuszowe,
– metody symulacyjne,
– metodę Monte Carlo.

Obszar inwestycyjny możliwy jest natomiast do analizy przy wykorzystaniu:
– standardowych metod oceny efektywności inwestycji,
– zaawansowanych metod efektywności.

Problematyka metod analizy finansowej możliwych do zastosowania w omawianym obszarze jest niezwykle ważnym zagadnieniem warunkującym efektywność procesu zarządzania ryzykiem informatycznym. Będzie ona przedmiotem bardziej szczegółowych rozważań kolejnych artykułów.

Fundamentem rozważań nad finansowymi aspektami zarządzania ryzykiem informatycznym jest przypisanie danej instytucji bankowej do kategorii ryzyka odpowiadającej relacji pomiędzy trzema elementami: wydatkami związanymi z bezpieczeństwem informatycznym, poziomem szacowanego ryzyka (bądź obserwowanego bezpieczeństwa) oraz wynikiem finansowym instytucji. Ich zestawienie wskazuje jednoznacznie na charakter instytucji istotny dla zarządzania ryzykiem informatycznym w ogóle oraz finansowaniem wydatków związanych z bezpieczeństwem szczególnie. Kategorie ryzyka wywodzą się zatem ze złożenia dwóch funkcji:
– $R = f_r(I)$ – opisującej zależność pomiędzy poziomem inwestycji związanych z mechanizmami bezpieczeństwa a szacowanym poziomem ryzyka informatycznego (bądź obserwowanym poziomem bezpieczeństwa),
– $F = f_w(R)$ – opisującej zależność pomiędzy szacowanym poziomem ryzyka informatycznego (bądź obserwowanym poziomem bezpieczeństwa) a wynikiem finansowym instytucji (lub ogólniej – szeroko rozumianą efektywnością jej funkcjonowania)[19].

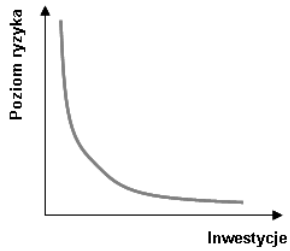
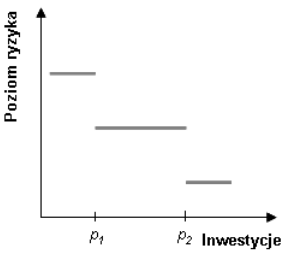
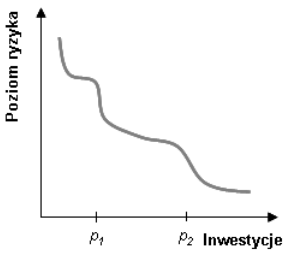
Modele funkcjonowania instytucji opisywane przez f_r prezentuje tab. 2.

Podkreślić należy, że powyższe zestawienie ma charakter uogólniający. W praktyce bowiem do różnych obszarów zarządzania ryzykiem przypisywać należy różne modele. Innymi słowy, model f_r – w większości przypadków – nie reprezentuje instytucji jako całości, ale poszczególne obszary zarządzania ryzykiem informatycznym. To ważne stwierdzenie, które wpisuje się w przewijający się w niniejszej pracy motyw konieczności uszczegóławiania procesów zarządzania ryzykiem. Tabela 3 prezentuje modele funkcjonowania instytucji opisywane przez funkcję f_w.

Złożenie funkcji f_r i f_w pozwala na przypisanie obszaru zarządzania ryzykiem w ramach banku do określonej kategorii ryzyka. W ujęciu modelowym można zatem wyróżnić piętnaście kategorii ryzyka. Istotne jest w konsekwencji pytanie: do której z tych kategorii należałoby przypisać bank komercyjny prowadzący obsługę zarów-

[19] Oczywiście $F = f_w(f_r(I))$, zatem pojęcie (poziomu) ryzyka mogłoby zostać pominięte w analizie. W znaczny sposób utrudniłoby to jednak zarówno konstruowanie funkcji, jak i interpretację modelu w konkretnym przypadku.

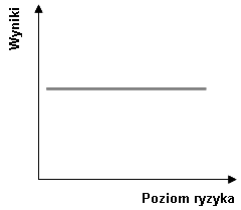
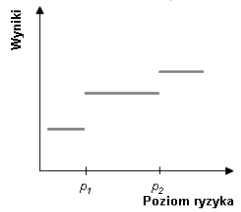
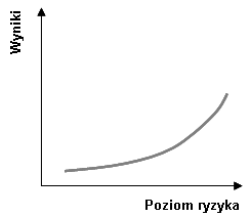
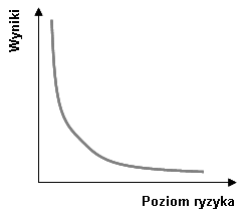
Tabela 2. Modele funkcjonowania instytucji w kontekście zależności inwestycje–ryzyko

Model, przykładowa reprezentacja graficzna funkcji	Charakterystyka modelu
Model klasyczny 	Brak sytuacji, w której inwestycja poniesiona z związku z zarządzaniem ryzykiem nie znajduje odzwierciedlenia w obniżeniu poziomu tego ryzyka. Poziom ryzyka asymptotycznie zbliża się do zera wraz ze wzrostem wydatków inwestycyjnych. Funkcja musi być monotonicznie malejąca
Model skokowy 	Nie wszystkie wydatki inwestycyjne skutkują obniżeniem poziomu ryzyka. Istnieje mechanizm progów inwestycyjnych (p_1, …, p_n), których przekraczanie determinuje obniżenie poziomu ryzyka. Wysokości poszczególnych progów uzależnione są m.in. od uwarunkowań natury prawnej i regulacyjnej
Model mieszany 	Połączenie modelu klasycznego i skokowego. W przedziałach odpowiadających modelowi klasycznemu każda inwestycja skutkuje obniżeniem poziomu ryzyka. Wykres funkcji może być zbliżony do wykresu w modelu klasycznym, jednak istnienie progów inwestycyjnych jest wyraźnie widoczne

Źródło: opracowania własne.

no tradycyjną, jak i internetową. Jak już wspomniano powyżej, jedna kategoria może nie być wystarczająca do opisu specyfiki ryzyka w banku. W przypadku praktycznego wykorzystania modeli wskazane byłoby zatem zaproponowanie podobszarów ryzyka informatycznego banku, które poddawałyby się modelowemu opisowi. Na przykład najprostszym podziałem tego typu mógłby być podział na obszar ryzyka wewnętrznych systemów bankowych oraz obszar ryzyka systemów bankowości elektronicznej. W bardziej szczegółowym ujęciu model mógłby być zastosowany np. do obszaru szkoleń pracowników banku. W kontekście zależności inwestycje–

Tabela 3. Modele funkcjonowania instytucji w kontekście zależności ryzyko–wyniki

Model, przykładowa reprezentacja graficzna funkcji	Charakterystyka modelu
Model płaski 	Stała funkcja opisująca brak zależności pomiędzy poziomem ryzyka informatycznego a osiąganymi przez instytucję wynikami. Sytuacja taka może być obserwowana w praktyce, gdyż szacowany poziom ryzyka nie musi być tożsamy z realizacją zagrożeń bezpieczeństwa w przyszłości. Poza tym nie każdy rodzaj działalności gospodarczej uwarunkowany jest charakterystykami funkcjonowania systemu informatycznego w kontekście jego bezpieczeństwa
Model wzrostowy skokowy 	Większy poziom ryzyka informatycznego wpływa na wzrost wyniku finansowego, jednak nie każde zwiększenie ryzyka ma taki wpływ. Istnieje mechanizm progów ryzyka (p_1, …, p_n), których przekraczanie determinuje generowanie wartości dodanej w ramach wyniku finansowego. Może to mieć związek np. z uruchamianiem nowych kanałów dostępu do produktów i usług bankowych
Model wzrostowy ciągły 	Każdy wzrost ryzyka informatycznego wpływa dodatnio na wynik finansowy. Jest to sytuacja możliwa do zaobserwowania w praktyce, lecz raczej hipotetyczna. Mogłaby się wiązać np. z obniżaniem wydatków związanych z bezpieczeństwem informatycznym, co w naturalny sposób prowadziłoby do zwiększenia wyniku
Model malejący skokowy 	Większy poziom ryzyka informatycznego wpływa ujemnie na wynik finansowy, jednak nie każde zwiększenie ryzyka ma taki wpływ. Istnieje mechanizm progów ryzyka (p_1, …, p_n), których przekraczanie determinuje generowanie wartości ujemnej w ramach wyniku finansowego. Może to mieć związek np. ze zmianami w obszarze mechanizmów bezpieczeństwa bankowości internetowej
Model malejący ciągły 	Każdy wzrost ryzyka informatycznego wpływa ujemnie na wynik finansowy

Źródło: opracowania własne.

ryzyko zastosowany mógłby być w tym przypadku model klasyczny, a w kontekście zależności ryzyko–wyniki mógłby to być model płaski, wzrostowy ciągły lub malejący ciągły[20].

5. Podsumowanie

Zarządzanie ryzykiem informatycznym w naturalny sposób związane jest z problemami natury finansowej. Dążenie banku do stałego podnoszenia poziomu bezpieczeństwa (obniżania poziomu ryzyka informatycznego) implikuje stały wzrost nakładów finansowych. Problematyka zarządzania finansowymi aspektami ryzyka informatycznego nabiera zatem charakteru strategicznego. W artykule zaprezentowano w propedeutycznym jedynie ujęciu problematykę możliwości zastosowań analizy ekonomiczno-finansowej w zarządzaniu ryzykiem informatycznym w banku. Z racji ograniczonej objętości tekstu zabrakło w nim prezentacji współczesnych narzędzi tej analizy, która będzie przedmiotem kolejnych artykułów.

Literatura

A Guide to the Project Management Body of Knowledge, Project Management Institute Standards Committee, 1996 i 2000.

Dudycz H., Dyczkowski M., *Efektywność przedsięwzięć informatycznych. Podstawy metodyczne pomiaru i przykłady zastosowań*, AE, Wrocław 2007.

Gospodarowicz A., *Ryzyko operacyjne i jego ocena w regulacjach Nowej Umowy Kapitałowej*, [w:] *Wyzwania współczesnych finansów*, K. Jajuga (red.), UE, Wrocław 2009.

Gospodarowicz A., Wawrzyniak D., *Ryzyko informatyczne jako ważny element ryzyka operacyjnego w banku – wybrane zagadnienia finansowania zarządzania ryzykiem informatycznym*, [w:] *Komputerowe systemy zarządzania*, W. Chmielarz, J. Turyna (red.), Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 2009.

Hoffman L.J., *Poufność w systemach informatycznych*, Wydawnictwa Naukowo-Techniczne, Warszawa 1982.

ISO Guide 73:2009 – Risk Management – Vocabulary.

Johnson M.E., *A Broader Context for Information Security*, „Financial Times", 16 September 2005.

Kaczmarek T.T., *Ryzyko i zarządzanie ryzykiem – ujęcie interdyscyplinarne*, Difin, Warszawa 2008.

Lech P., *Metodyka ekonomicznej oceny przedsięwzięć informatycznych wspomagających zarządzanie organizacją*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2007.

Turn R., Shapiro N.Z., *Privacy and Security in Databank Systems: Measures of Effectiveness, Costs, and Protector-Intruder Interactions*, AFIPS Joint Computer Conferences, Proceedings of the December 5-7, 1972.

[20] Wybór jednego z tych modeli możliwy byłby tylko na podstawie danych ilościowych obrazujących konkretny przypadek. Wydatki poniesione na szkolenia mogą bowiem przewyższyć korzyści wynikające z tych szkoleń, co może być efektem np. nieprawidłowego ich przeprowadzenia. Podkreślić należy, że sama identyfikacja charakteru tej zależności w danym przypadku ma istotne znaczenie dla zarządzania ryzykiem informatycznym.

Uniwersalny słownik języka polskiego, Dubisz S. (red.), Wydawnictwo Naukowe PWN, Warszawa 2003, tom III.

Wawrzyniak D., *Ryzyko informatyczne w działalności bankowej – w stronę nowego paradygmatu*, [w:] *Bankowość detaliczna – idee, modele, procesy*, A. Gospodarowicz (red.), UE, Wrocław 2010.

Zaleska M., *Ocena ekonomiczno-finansowa przedsiębiorstwa przez analityka bankowego*, Szkoła Główna Handlowa w Warszawie – Oficyna Wydawnicza, Warszawa 2005.

FUNDAMENTALS OF ECONOMIC ANALYSIS AS THE INFORMATION SECURITY RISK MANAGEMENT TOOL IN A BANK

Summary: Information security risk management is becoming more and more crucial problem due to dynamic information sciences development as well as their implementation in all business areas. The risk constitutes today a base for the activities of contemporary institutions. Moreover, in the context of financial institutions the risk should be seen as a crucial factor determining their existence. The article presents some fundamental aspects of economic and financial analysis that should constitute the basis for information security management process in banking. The most important definitions have been given and the three main areas of the problem have been identified. The importance of risk category determination for a given bank has been also emphasized.