PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 124
Bankowość detaliczna: idee – modele – procesy 2010

Dariusz Wawrzyniak
Uniwersytet Ekonomiczny we Wrocławiu

RYZYKO INFORMATYCZNE W DZIAŁALNOŚCI BANKOWEJ – W STRONĘ NOWEGO PARADYGMATU

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 zagadnienia związane z problematyką szacowania ryzyka informatycznego. Ich prezentację ukierunkowano na wskazanie głównych przeszkód implementacji rozwiązań normatywnych. Ważnym elementem artykułu jest także przedstawienie podstaw nowej koncepcji szacowania ryzyka informatycznego, która poddaje pod dyskusję fundamentalne elementy dotychczasowych analiz omawianego zagadnienia, jakimi są prawdopodobieństwo wystąpienia zdarzenia oraz wartość potencjalnej straty.

Słowa kluczowe: ryzyko informatyczne, szacowanie ryzyka informatycznego.

1. Wstęp

Ryzyko stale towarzyszy działalności bankowej. Interdyscyplinarny charakter ryzyka bankowego wymaga jednak odmiennego traktowania poszczególnych jego składowych. Niektóre z nich bowiem podlegają okresowym wahaniom uwarunkowanym m.in. kryzysami i spowolnieniami gospodarczymi, inne zaś wykazują tendencje rozwojowe niezależne od zmian gospodarczych. Jednym z rodzajów ryzyka, które jest nieodłącznym elementem działalności bankowej, bez względu na sytuację ekonomiczną, jest ryzyko informatyczne.

Pojęcie ryzyka funkcjonuje dzisiaj w wielu dziedzinach i opiera się na potocznym rozumieniu tego terminu. Ryzyko to możliwość, prawdopodobieństwo, że coś się nie uda[1]. Problematyka ryzyka ma szczególne miejsce w naukach finansowych,

[1] *Uniwersalny słownik języka polskiego* pod redakcją naukową Stanisława Dubisza, Wydawnictwo Naukowe PWN, t. III, Warszawa 2003, s. 1108. Warto w tym miejscu zaznaczyć, że cytowany słownik nie dopuszcza użycia rzeczownika „ryzyko" w liczbie mnogiej. Inaczej problem traktuje na-

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[2]. O ile jednak ryzyka psychologiczne, socjologiczne 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.

2. Podstawy terminologiczne

Dyskusja nad problematyką 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,

tomiast *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, obciążającej osobę poszkodowaną niezależnie od jej winy – posiada liczbę mnogą (s. 990).

[2] Zob. np.: T.T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem – ujęcie interdyscyplinarne*, Wydawnictwo Difin, Warszawa 2008.

[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.

– 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 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

[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. Por.: M.E. Johnson, *A Broader Context for Information Security*, „Financial Times", 16 Sept. 2005, s. 4. Warto w tym kontekście zaznaczyć, że zmianę sposobu postrzegania problemów bezpieczeństwa determinuje w znaczącym stopniu m.in. wzrost powszechności usług bankowości internetowej.

[6] W literaturze przedmiotu prowadzona jest dyskusja 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.: A. Gospodarowicz, *Ryzyko operacyjne i jego ocena w regulacjach Nowej Umowy Kapitałowej*, (w:) K. Jajuga (red.), *Wyzwania współczesnych finansów*, Weje, Wrocław 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. Obszerniejszy opis tego zjawiska znaleźć można m.in. w: A. Gospodarowicz, D. Wawrzyniak, *Ryzyko informatyczne jako ważny element ryzyka operacyjnego w banku – wybrane zagadnienia finansowania zarządzania ryzykiem informatycznym*, (w:) W. Chmielarz, J. Turyna (red.),

terminologicznej nad pojęciem ryzyka informatycznego powinny 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.

Powyższa definicja została niemal bezkrytycznie przyjęta przez literaturę przedmiotu i stanowi punkt wyjścia rozważań nad możliwościami ilościowego ujęcia ryzyka informatycznego. Warto jednak zauważyć, że definicja opisuje nie ryzyko, lecz jego miarę[9]. Można ten fakt postrzegać przez pryzmat praktycznych aspektów zarządzania ryzykiem, nie można jednak obronić definicji przez zarzutem semantycznej niepoprawności. Ryzykiem informatycznym *sensu stricto* powinno nazywać się prawdopodobieństwo wystąpienia określonego zdarzenia wpływającego negatywnie na bezpieczeństwo systemu informatycznego bądź innymi słowy – prawdopodobieństwo, że realizacja konkretnego zagrożenia wykorzysta konkretną podatność systemu. Iloczyn tego prawdopodobieństwa oraz wyrażonych w pieniądzu negatywnych jego skutków będzie natomiast jedną z miar ryzyka[10]. Ryzyko informatyczne odpowiada zatem negatywnej koncepcji ryzyka, a więc oznacza ono możliwość nieosiągnięcia oczekiwanego efektu[11], jakim jest nienaruszenie bezpieczeństwa systemu (brak zdarzenia, które wpłynęłoby negatywnie na bezpieczeństwo). O ryzyku informatycznym *sensu largo* – a więc w odniesieniu

Komputerowe systemy zarządzania, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 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*. Wersji polskojęzycznej doczekała się na razie (marzec 2010) tylko norma 27001 (PN-ISO/IEC 27001:2007).

[9] Ciekawa w tym kontekście jest analiza poprzednich norm ISO, np. PN-I-02000:2002 (*Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*), która definiowała ryzyko informatyczne jako możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych. Trudno stwierdzić, jakie założenia legły u podstaw tej istotnej i bardzo dyskusyjnej zmiany terminologicznej.

[10] Można ją utożsamić z oczekiwaną stratą związaną z pojedynczym zdarzeniem.

[11] Por.: K. Jajuga (red.), *Zarządzanie ryzykiem*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 13.

do całego systemu czy instytucji – można mówić jedynie w sensie określonej syntezy miar ryzyk *sensu stricto*.

Zarządzaniem ryzykiem informatycznym nazywamy natomiast kompleksowy proces identyfikowania, monitorowania oraz eliminowania lub minimalizowania wartości funkcji prawdopodobieństw realizacji zagrożeń bezpieczeństwa oraz ich skutków[12].

3. Bezpieczeństwo a ryzyko

Zestawienie pojęć oceny bezpieczeństwa oraz szacowania ryzyka jest fundamentem rozważań nad możliwościami zastosowań metod ilościowych w procesie zarządzania ryzykiem informatycznym. Bezpieczeństwo informatyczne zdefiniowane powyżej jako stan systemu charakteryzujący się określonym poziomem atrybutów bezpieczeństwa jest pojęciem definiowanym na innym poziomie merytorycznym niż pojęcie ryzyka informatycznego, z drugiej jednak strony wzajemna relacja pomiędzy tymi pojęciami jest wyraźnie zauważalna i istotna dla optymalizacji procesów zarządzania ryzykiem i zarządzania bezpieczeństwem. Bezpieczeństwo informatyczne mówi nam bowiem o stanie systemu, ale jednocześnie pośrednio wskazuje na pewien poziom ryzyka informatycznego charakteryzującego dany system. Wskazanie to może być dokładniejsze, jeśli zestawione zostaną oceny poziomu bezpieczeństwa wielu minionych okresów. Otrzymany w ten sposób trend może posłużyć jako narzędzie zarządzania ryzykiem. Czy jednak można postawić znak równości pomiędzy oceną bezpieczeństwa a oceną ryzyka? W szczególnym przypadku tak, w ogólnym przypadku zdecydowanie nie. Przypadek szczególny to sytuacja, w której oceniany system nie podlega zmianom wewnętrznym i wpływowi otoczenia. Tylko wtedy bowiem można zaryzykować stwierdzenie, że obserwowane zmiany poziomu bezpieczeństwa odpowiadają zmianom poziomu ryzyka informatycznego. Jest to jednak założenie na tyle hipotetyczne i niepraktyczne, że jego szczegółowa analiza nie wydaje się istotna. Pozostaje zatem konstatacja, zgodnie z którą ocena poziomu bezpieczeństwa i ocena poziomu ryzyka informatycznego to dwa różne problemy, powiązane ze sobą, jednak wymagające innych metodologii, narzędzi, danych źródłowych, a także ukierunkowane na inne cele oraz atrybuty informacji wynikowych.

Na wstępie rozważań nad możliwościami oceny poziomu bezpieczeństwa należy wyraźnie rozróżnić dwa aspekty:

[12] Definicja normatywna proponowana przez PN-ISO/IEC 27001:2007 definiuje zarządzanie ryzykiem jako skoordynowane działania kierowania 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.

– teoretyczny poziom bezpieczeństwa systemu wynikający z zastosowanych w nim rozwiązań,
– obserwowany poziom bezpieczeństwa systemu będący efektem działalności jego użytkowników.

Pierwszy z nich jest stosunkowo łatwy do wyznaczenia. Najczęstszym sposobem określania poziomu teoretycznego jest odniesienie zastosowanych w systemie środków bezpieczeństwa do kryteriów jednego z wielu standardów. Wynikiem takiego porównania jest przypisanie systemu do określonej klasy bezpieczeństwa. Nie niesie jednak ono odpowiedzi na pytania, czy zastosowane mechanizmy okazały się skuteczne oraz czy będą skuteczne także w przyszłości, co jest o wiele bardziej istotnym zagadnieniem z punktu widzenia zarządzania ryzykiem. Ocena obserwowanego poziomu bezpieczeństwa jest zagadnieniem relatywnie nieskomplikowanym, szczególnie w warstwie metodologicznej[13]. Najogólniej rzecz ujmując, ocena poziomu bezpieczeństwa sprowadza się do ilościowego ujęcia zbioru danych historycznych dotyczących wybranego podobszaru systemu. Czy jednak oparcie procedur ewaluacyjnych jedynie na danych historycznych jest wystarczające do ilościowego opisu ryzyka informatycznego? Odpowiedź na tak postawione pytanie musi być jednoznacznie przecząca, co wynika zarówno z definicji ryzyka informatycznego, jak i z praktycznych aspektów implementacji metod zarządzania tym ryzykiem. Metody oceny bezpieczeństwa mogą jednak być istotnym elementem wspomagającym procedury szacowania ryzyka. Jak już wspominano, szacowanie ryzyka to przede wszystkim określanie prawdopodobieństw wystąpienia pewnych zdarzeń. Nie można w procesie określania tych prawdopodobieństw pomijać ich historycznego aspektu. Innymi słowy, każdy zestaw danych historycznych, zarówno w postaci pierwotnej, jak i przetworzonej przez metodę oceny bezpieczeństwa stanowi podstawę informacyjną metod szacowania ryzyka. Te drugie w naturalny sposób tworzone są przez zestawienie dwóch obszarów merytorycznych:
– obszaru informacyjnego,
– obszaru obliczeniowego.

Obszar informacyjny to właśnie dane historyczne uzupełnione (zmodyfikowane) ich ekspercką analizą. Obszar obliczeniowy natomiast to sposób matematycznego przekształcenia obszaru informacyjnego w miary wynikowe, które mogą wspomagać proces zarządzania ryzykiem informatycznym.

4. Problemy szacowania ryzyka informatycznego

Jak już wspomniano, ryzyko informatyczne *sensu stricto* mierzone może być wartością kombinacji prawdopodobieństwa wystąpienia określonego zdarzenia oraz

[13] Podkreślić jednak należy, że w literaturze przedmiotu spotkać można śladowe wręcz próby stworzenia uniwersalnych wskaźników liczbowych opisujących w ogólnym, całościowym ujęciu poziom bezpieczeństwa systemów informatycznych.

wartości potencjalnej straty wynikającej z tego zdarzenia. Oba elementy składające się na tę miarę charakteryzuje problem, któremu można nadać roboczą nazwę „problemu praktycznej wyznaczalności". Zarówno bowiem prawdopodobieństwo wystąpienia, jak i wartość straty są w praktyce trudne do oszacowania. W szczególności, do najistotniejszych czynników warunkujących tę trudność zaliczyć należy:

– niejednoznaczność interpretacyjną pojęcia prawdopodobieństwa w kontekście ryzyka informatycznego,
– niemożność posługiwania się jedynie danymi historycznymi w procesach szacowania prawdopodobieństw wynikającą ze zbyt dużej zmienności, jakiej poddawane są problemy bezpieczeństwa informatycznego,
– brak możliwości dokładnego wyznaczania wartości strat.

Czynniki te zostały pokrótce scharakteryzowane poniżej.

Czym jest prawdopodobieństwo w ryzyku informatycznym? W teorii prawdopodobieństwa funkcjonują cztery jego definicje[14]. Definicja klasyczna mówi, że jeśli zbiór zdarzeń elementarnych ma skończoną liczbę elementów i wszystkie zdarzenia losowe jednoelementowe są jednakowo prawdopodobne, to prawdopodobieństwo zdarzenia A jest równe

$$P(A) = \frac{\overline{\overline{A}}}{\overline{\overline{\Omega}}}, \tag{2}$$

gdzie: $\overline{\overline{A}}$ – liczba zdarzeń elementarnych należących do zdarzenia A,

$\overline{\overline{\Omega}}$ – liczba wszystkich zdarzeń elementarnych.

Aby podać geometryczną definicję prawdopodobieństwa, należy rozparzyć przypadek, w którym zbiór zdarzeń elementarnych jest zbiorem punktów prostej, płaszczyzny lub przestrzeni. Zakłada się, że

a) zbiór Ω jest mierzalny o skończonej mierze, tzn. ma skończoną długość, pole lub objętość,

b) wszystkie punkty zbioru Ω mają jednakowe szanse wylosowania.

Prawdopodobieństwo dowolnego zdarzenia A, będącego podzbiorem mierzalnym zbioru Ω, wyraża się wzorem:

$$P(A) = \frac{\text{miara } A}{\text{miara } \Omega}, \tag{3}$$

gdzie przez miarę rozumiemy długość, pole lub objętość, w zależności czy zbiór Ω leży na prostej, płaszczyźnie lub w przestrzeni.

W praktyce nie zawsze znana jest liczebność zbioru zdarzeń elementarnych, która jest potrzebna przy wykorzystaniu definicji klasycznej bądź nie jest łatwo do-

[14] Por. np.: M. Cieciura, J. Zacharski, *Metody probabilistyczne w ujęciu praktycznym*, Wydawnictwo VIZJA PRESS&IT, Warszawa 2007, s. 21 i n.

liczyć się liczby zdarzeń elementarnych sprzyjających poszczególnym zdarzeniom losowym. Podobnie nie zawsze są znane miary potrzebne do skorzystania z definicji geometrycznej. Znajomości tych wielkości nie wymaga definicja statystyczna, której koncepcja zakłada, że w długiej serii doświadczeń obserwuje się wystąpienie zdarzenia A. Jeżeli częstość n/N zdarzenia A, gdzie N jest długością serii, a n liczbą doświadczeń, w których pojawiło się zdarzenie A, przy wzrastaniu długości serii zbliża się do pewnej liczby p, oscylując wokół tej liczby, i jeśli wahania częstości zdarzenia przejawiają tendencję malejącą przy wzrastającym N, to liczba p nazywana jest prawdopodobieństwem zdarzenia A.

$$P(A) = \lim_{N\to\infty} \frac{n}{N}. \tag{4}$$

Żadna z powyższych definicji nie jest pozbawiona wad. I tak:

- definicja klasyczna jest tautologią, gdyż definiując prawdopodobieństwo, posługuje się pojęciem zdarzeń jednakowo możliwych, czyli jednakowo prawdopodobnych,
- definicja geometryczna wymaga znajomości miary zbiorów, którymi się posługuje,
- definicja statystyczna nie jest ścisła, bo nie jest sprecyzowana granica w niej występująca.

Wspólną wadą tych definicji jest to, że definiując prawdopodobieństwo, odnoszą się do określonego typu doświadczenia. Takich wad nie ma podana poniżej definicja aksjomatyczna, gdyż dotyczy ona wszystkich rodzajów doświadczeń losowych.

Jeśli każdemu zdarzeniu losowemu A przyporządkowano liczbę rzeczywistą $P(A)$, zwaną prawdopodobieństwem zdarzenia A, w taki sposób, aby spełnione były następujące warunki:

I. Prawdopodobieństwo zdarzenia jest większe lub równe zeru i mniejsze lub równe jedności

$$0 \le P(A) \le 1.$$

II. Prawdopodobieństwo zdarzenia pewnego jest równe 1

$$P(\Omega) = 1.$$

III. Jeżeli zdarzenia A_1, A_2, A_3, …, A_n, … wykluczają się parami, wtedy prawdopodobieństwo sumy tych zdarzeń jest równe sumie ich prawdopodobieństw

$$P(A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots) = P(A_1) + P(A_2) + \ldots + P(A_n) + \ldots,$$

to określoną w ten sposób funkcję P nazywamy prawdopodobieństwem. Podane wcześniej definicje klasyczna, geometryczna i statystyczna są szczególnymi przypadkami definicji aksjomatycznej.

Innym, powszechnie znanym ujęciem omawianej problematyki jest podział prawdopodobieństwa na obiektywne i subiektywne. Są to jednak pojęcia równo-

znaczne z przedstawionymi powyżej koncepcjami prawdopodobieństwa statystycznego i aksjomatycznego[15].

Przytoczone analizy nie są oczywiście jedynymi głosami w dyskusji nad pojęciem prawdopodobieństwa. Niezwykle ciekawe i w istotny sposób kształtujące nasze postrzeganie omawianego problemu są także rozważania filozoficzne. Znakomitym ich przykładem jest analiza przeprowadzona przez R. Carnapa, w której autor prezentuje koncepcje prawdopodobieństwa statystycznego i logicznego[16].

M. Heller pisze natomiast, że we współczesnym ujęciu teoria prawdopodobieństwa jest szczególnym przypadkiem teorii miary. Miara – pisze dalej – w sensie matematycznym jest funkcją zdefiniowaną na podzbiorach pewnej przestrzeni, zwanej przestrzenią miary. Podzbiory – zwane podzbiorami mierzalnymi – można interpretować jako obiekty, które mogą być mierzone. Funkcja zdefiniowana na podzbiorach mierzalnych przypisuje każdemu z tych podzbiorów dodatnią liczbę rzeczywistą, którą możemy utożsamić z wynikiem pomiaru. Prawdopodobieństwem jest natomiast miara spełniająca jeszcze jeden, dodatkowy warunek: miara całej przestrzeni musi równać się jedności[17].

Rozważania filozoficzne nie są – wbrew pozorom – merytorycznie oddalone od problematyki ryzyka informatycznego. Wręcz przeciwnie, prawdopodobieństwa, jakimi posługuje się omawiany obszar zarządzania ryzykiem informatycznym, z rzadka jedynie będą prawdopodobieństwami dającymi opisać się za pomocą definicji klasycznej. W większości przypadków będą to szacunkowe, arbitralnie przyjmowane wartości, wynikające bardziej z pewnych subiektywnych oczekiwań i doświadczenia, a nie matematycznych pojęć typu *zbiór zdarzeń* czy *liczba elementów*. Innymi słowy, zagadnienie prawdopodobieństwa w omawianym w opracowaniu obszarze jest zupełnie innym problemem niż ten, przed którym stanął w XVII w. Blaise Pascal. Mógł on bowiem założyć, że każdy rezultat rzutu kostką jest jednakowo prawdopodobny. Niestety, żaden administrator bezpieczeństwa informatycznego o takim luksusie marzyć nie może.

Niezwykle istotnym elementem problematyki definiowania ryzyka w otaczającej nas rzeczywistości są także zagadnienia ryzyka porządkowego. Z ryzykiem tego typu mamy do czynienia, gdy nie określamy liczbowej wartości ryzyka, ale

---

[15] Zob. np.: J. Orzeł, *Rola metod heurystycznych, w tym grupowej oceny ekspertów, oraz prawdopodobieństwa subiektywnego w zarządzaniu ryzykiem operacyjnym*, „Bank i Kredyt", Narodowy Bank Polski, maj 2005, s. 4 i n.

[16] Zob.: R. Carnap, *Wprowadzenie do filozofii nauki*, Fundacja Aletheia, Warszawa 2000, s. 27 i n.

[17] M. Heller, *Filozofia i wszechświat*, Wydawnictwo UNIVERSITAS, Kraków 2006, s. 64 i n. Problematyka definiowania pojęcia prawdopodobieństwa we współczesnej nauce jest przedmiotem wielu rozpraw filozoficznych. Zob. np.: M. Zabierowski, *Wszechświat i metafizyka*, Wydawnictwo Naukowe PWN, Warszawa 1998. Co więcej, problem jest dzisiaj stale aktualny przede wszystkim w kontekście konieczności ponownego definiowania pewnych pojęć na potrzeby rozwijających się dziedzin fizyki, takich jak np. mechanika kwantowa. Zob. np.: G. Milburn, *Inżynieria kwantowa*, Wydawnictwo Prószyński i S-ka, Warszawa 1999.

stwierdzamy, że jakieś zdarzenie jest bardziej prawdopodobne od innego, czyli gdy porządkujemy zdarzenia pod względem ryzyka[18].

Nasuwa się więc pytanie – czy analizując omawiane zagadnienie, możemy w ogóle posługiwać się pojęciem ryzyka określanym za pomocą pojęcia prawdopodobieństwa wystąpienia określonych zdarzeń? Odpowiedź na to pytanie ma dwojaki charakter. Z jednej strony jest bowiem w pewien sposób wymuszona przez oczekiwania praktyki biznesowej związane z organizacyjnymi aspektami zarządzania bezpieczeństwem systemów informatycznych. Z drugiej strony natomiast podlega krytyce tejże samej praktyki związanej z problemami natury implementacyjnej. Niemniej jednak jest to odpowiedź twierdząca. Abstrahując na tym etapie rozważań od możliwych do zastosowania sposobów wyznaczania prawdopodobieństw, stwierdzić zależy, że przyjęcie założenia o niemożności ich wyznaczania skazałoby omawiane zagadnienie na konieczność stosowania jedynie opisowych, mało precyzyjnych i słabo sformalizowanych metod i narzędzi analitycznych[19]. Innymi słowy, problematyka analizy i oceny ryzyka informatycznego w świadomy – chociaż oczywiście dyskusyjny – sposób wykorzystuje pojęcie prawdopodobieństwa po to, by *de facto* w ogóle móc zaistnieć. Trudno bowiem mówić o znajomości rozkładów prawdopodobieństw zmiennych opisujących zagrożenia bezpieczeństwa systemów informatycznych, skoro wpływ i znaczenie tych zagrożeń ulegają permanentnym zmianom, co więcej – stale pojawiają się nowe rodzaje zagrożeń[20]. W konsekwencji pojawia się pytanie kolejne: w jaki sposób określamy prawdopodobieństwa zdarzeń w obszarze ryzyka informatycznego? Odpowiedź na tak postawione pytanie wydaje się bardzo trudna i łatwa jednocześnie. Z punktu widzenia definicji prawdopodobieństwa przytoczonych powyżej wydaje się, że ryzyko informatyczne powinno być opisywane przez prawdopodobieństwo w ujęciu aksjomatycznym, aczkolwiek wykazanie tej tezy nie byłoby trywialne. Natomiast z punktu widzenia praktyki zarządzania ryzykiem – czyli celów stawianych przed procesami przypisywania prawdopodobieństw do określonych zdarzeń – prawdopodobieństwami są po prostu ilościowo przedstawione możliwości wystąpienia określonych zdarzeń. Problemem nie jest więc teoretyczna konstrukcja pojęcia, sta-

[18] Zob. np.: H. Sosnowska, *Prawdopodobieństwo subiektywne a reguły rachunku prawdopodobieństwa*, (w:) S. Forlicz (red.), *Metody ilościowe w ekonomii*, Wydawnictwo Wyższej Szkoły Bankowej w Poznaniu, Poznań 2008, s. 10.

[19] Stwierdzenie to jest pozornie sprzeczne z tezami przedstawionymi w dalszej części artykułu uzasadniającymi poprawność propozycji nowej metodyki szacowania ryzyka. Niewykorzystanie pojęcia prawdopodobieństwa w tej metodyce nie oznacza bowiem rezygnacji z ilościowego ujęcia problemu.

[20] Można oczywiście założyć, że w systemie, w którym przez określony czas nie zmieniają się sprzęt, oprogramowanie oraz użytkownicy, a także nie istnieje połączenie z sieciami zewnętrznymi, dane historyczne dotyczące zdarzeń negatywnie wpływających na bezpieczeństwo są wystarczającą i wiarygodną podstawą do szacowania rozkładu prawdopodobieństw związanych z ryzykiem informatycznym. Założenie takie – szczególnie w kontekście systemów wykorzystywanych w bankowości – jest jednak czysto hipotetyczne.

ją się nim natomiast jego interpretacja oraz dostępność informacji, na podstawie których możliwości takie można ująć w liczbach[21].

Warto zatem zadać w tym miejscu kolejne ważne pytanie: skoro wiadomo, że przez pojęcie prawdopodobieństwa w ryzyku informatycznym rozumiemy pewną wartość, szacowaną i przybliżaną na podstawie głównie eksperckiej wiedzy, to czy nie warto by rozważyć podejście, w którym do szacowania tego ryzyka niepotrzebne byłoby pojęcie prawdopodobieństwa? Próbę rozwinięcia tego zagadnienia przedstawiono w dalszej części artykułu.

Innym wspomnianym uprzednio problemem jest możliwość finansowego ujęcia strat wynikających z realizacji zagrożeń bezpieczeństwa. Czy jest to zadanie wykonalne? W prostych przypadkach tak. W większości przypadków jednak nie, czego głównym powodem jest trudność wartościowania zasobów systemowych. A. Białas identyfikuje następujące problemy wartościowania zasobów systemowych związane z[22]:

- opracowaniem dla instytucji jednolitej metody wyceny zasobów, które z natury są bardzo różnorodne i najczęściej niemożliwe do przedstawienia w postaci kwot pieniężnych,
- uwzględnieniem efektów propagacji i kumulacji wartości cząstkowych,
- uwzględnieniem efektu obniżania się wartości na skutek powielarności zasobu lub łatwości jego odtwarzania,
- wyrażeniem skomplikowanych, nie w pełni poznanych zależności między zasobami.

Autor zauważa także, że trudno jest wyrazić wartość zasobu w sposób czysto ilościowy, dlatego nierzadko trzeba posługiwać się miarami umownymi – jakościowymi. W cytowanym opracowaniu nie odnajdujemy zatem konkretnych propozycji rozwiązań problemu wyceny, wart jednak podkreślenia jest fakt zaproponowania mechanizmu wspomagającego proces wyceny, związanego z ilościowym ujęciem czynników wpływających na wartość zasobów. Znajdują się wśród nich[23]: zakłócenie ciągłości procesów biznesowych składających się na misję instytucji, zagrożenie dla zdrowia lub życia, zagrożenie dla środowiska naturalnego, zakłócenie porządku publicznego, możliwość naruszenia prawa lub zobowiązań, straty finansowe, utrata reputacji instytucji, możliwość zastąpienia, pozytywne cechy oso-

[21] Wiele dziedzin podejmuje problem wyznaczania prawdopodobieństw w oderwaniu od naukowych podstaw probabilistyki, traktując prawdopodobieństwo jako pewne oczekiwanie – często wsparte danymi historycznymi, nierzadko jednak także subiektywne.

[22] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006, s. 254 i n.

[23] *Ibidem*, s. 256. Cytowany autor dzieli zasoby na kilka kategorii poziomów, m.in.: funkcje wewnętrzne i zewnętrzne instytucji – jej wizerunek i zaufanie klientów, infrastruktura techniczna, personel, dokumentacja, oprogramowanie.

bowe, poziom wiedzy, fachowości, poniesiony koszt wyszkolenia, autorytet, wartość księgowa, koszt odtworzenia.

O krok dalej w swoich rozważaniach idzie A. Jaquith, który generalnie odrzuca sensowność przypisywania zasobom jakichkolwiek wartości wyrażonych w pieniądzu, tłumacząc to brakiem możliwości realizacji takiego zadania w sposób konsekwentny i wiarygodny[24].

K. Liderman przedstawia omawiany problem raczej skrótowo, niemniej jednak wskazuje na istotne jego atrybuty niewymienione powyżej. Pisze on, że oceniając wartość zasobów informacyjnych, należy brać pod uwagę[25]:

- bezpieczeństwo osobiste i poufne informacje osobiste,
- zobowiązania prawne i regulaminowe firmy oraz personelu,
- obowiązujące przepisy prawa,
- interesy handlowe i ekonomiczne firmy,
- możliwe straty finansowe w przypadku utraty poufności, integralności lub dostępności informacji albo przerwania czy zniszczenia procesów biznesowych,
- porządek publiczny,
- politykę działania firmy,
- utratę reputacji firmy.

Problem wartościowania zasobów w naturalny sposób przekłada się na problem wartościowego ujęcia negatywnych skutków realizacji zagrożeń bezpieczeństwa. Skutki te są nieprzewidywalne, a co się z tym wiąże – nie można przypisywać im stałych wartości wyrażonych w pieniądzu[26]. Przykładem złożoności omawianego zagadnienia niech będzie poniższa analiza trywialnego przypadku kradzieży komputera przenośnego.

Analiza powyższych opinii nakazuje zadać dość istotne pytanie: czy wartościowanie zasobów oznaczać musi przypisanie do każdego zasobu odpowiadającej mu wartości wyrażonej w pieniądzu lub niemianowanej wartości liczbowej, czy raczej celem wartościowania jest przypisanie zasobów do określonych grup (kategorii) odpowiadających wymaganiom prawnym i biznesowym? Prawidłowa odpowiedź zdecydowanie bliższa jest drugiej opcji. Wartościowanie w procesie zarządzania ryzykiem powinno przypisać zasoby do określonych przez instytucję kategorii – stworzonych zgodnie z wymogami procesu szacowania ryzyka – niekoniecznie nadając tym zasobom stałe wartości wyrażane w pieniądzu.

---

[24] A. Jaquith, *Security Metrics*, Addison-Wesley, Pearson Education Inc., 2007, s. 95 i n.

[25] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 35 i n.

[26] Oczywiście wielu specjalistów proponuje pewne podejścia ułatwiające realizację wartościowania strat w praktyce, niemniej jednak ich wspólną cechą jest jedynie przechodzenie na niższy poziom informatycznej szczegółowości i pozostawienie pełnej arbitralności szacowanych wartości. Por. np.: A. Munteanu, *Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma, Managing Information in the Digital Economy: Issues & Solutions*, s. 227 i n. Tekst dostępny m.in. w serwisie Social Science Research Network (http://www.ssrn.com/).

Tabela 1. Wartościowanie strat wynikających z kradzieży komputera

Obszar wartościowania	Możliwe przypadki	Wpływ wartościowania	Uwagi
Wartość komputera	Znana wartość	Deterministyczny – zwiększający	Najprostszy w analizie element wartościowania – nierzadko traktowany jako jedyny.
Wartość danych	Znana zawartość dysku	Deterministyczny – zwiększający	Deterministyczny wpływ wartościowania przy założeniu znanej zawartości dysku jest oczywiście pewnym uproszczeniem. Nie można bowiem jednoznacznie przewidzieć sposobu wykorzystania danych. Pod uwagę należy wziąć także dane usunięte z dysku. Możliwe bowiem jest ich odzyskanie z wykorzystaniem specjalistycznej wiedzy i oprogramowania. Koszt tej wiedzy zmniejsza wartość straty związanej z kradzieżą komputera.
	Nieznana zawartość dysku	Probabilistyczny – zwiększający	
Wartość potencjalnych strat moralnych	Nieznane	Probabilistyczny – zwiększający	Wartość strat moralnych jest pochodną sposobu wykorzystania danych zawartych na dysku komputera.
Wartość przychodu z ewentualnego ubezpieczenia	Znana wartość	Deterministyczny – zmniejszający	Wartość znana, chociaż okoliczności utraty komputera mogą mieć na nią wpływ.
Wartość odtworzenia	Znana wartość	Deterministyczny – zwiększający	W uproszczonym modelu można przyjąć, że wartość odtworzenia równa jest wartości utraconego składnika majątku.

Źródło: opracowania własne.

Wszystkie powyżej opisane czynniki – mimo że konsekwentnie pomijane przez normy ISO oraz większą część literatury przedmiotu – w istotny sposób ograniczają możliwość ilościowego ujęcia problemów ryzyka informatycznego w praktyce. Zasadne wydaje się zatem kolejne pytanie: czy ilościowe szacowanie ryzyka informatycznego jest praktycznie wykonalne w takim zakresie, aby mogło istotnie wspomagać proces zarządzania tym rodzajem ryzyka? Z pewnością ogólnej odpowiedzi na tak sformułowane pytanie udzielić się nie da, chociaż możliwe jest przedstawienie i uzasadnienie odpowiedzi twierdzącej w konkretnych przypadkach. Przypadek ogólny jednak takiej odpowiedzi nie akceptuje. W dalszej części artykułu przedstawiono ramową koncepcję nowej metodyki szacowania ryzyka, u źródeł której legła przede wszystkim krytyka interpretacji dwóch podstawowych dla omawianego zagadnienia pojęć, jakimi są prawdopodobieństwo wystąpienia zdarzenia oraz wartość straty[27].

[27] Nie chodzi oczywiście o krytykę pojęć jako takich, lecz krytykę ich interpretacji oraz możliwości zastosowań w klasycznym (rekomendowanym głównie przez współczesne normy i standardy) podejściu do problematyki szacowania ryzyka informatycznego.

5. Nowy paradygmat

Jak już wspomniano, współcześnie rekomendowane podejście do omawianej problematyki charakteryzuje się aksjomatycznym niemal traktowaniem składowych definicyjnych ryzyka informatycznego, jakimi są prawdopodobieństwo wystąpienia zdarzenia oraz wartość potencjalnej straty. Podstawą koncepcyjną prezentowanego w dalszej części paradygmatu są następujące tezy sprzeczne ze wspomnianymi aksjomatów aksjomatami.

Teza 1. Problemy bezpieczeństwa informatycznego nie poddają się statystycznej analizie wykorzystującej rozkłady zmiennych losowych, dlatego prawdopodobieństwa wystąpienia określonych zdarzeń w przyszłości nie są znane.

Teza 2. Nie da się określić wartościowo negatywnych skutków wystąpienia tych zdarzeń.

Uzasadnienie tezy 1. System informatyczny rozumiany jako zbiór powiązanych ze sobą elementów, wśród których znajdują się sprzęt, oprogramowanie i użytkownicy, podlega ciągłym zmianom warunkowanym jego eksploatacją, rozwojem, dynamiką otoczenia, wpływem czynnika ludzkiego itp. Nie można zatem przypisywać współczesnym systemom informatycznym atrybutów długookresowej stabilności. Analiza danych historycznych obrazujących działanie systemu musi ograniczać się do niezbyt długiego okresu poprzedzającego analizę. Nawet jednak przy takim podejściu wyniki analizy nie powinny być traktowane jako stałe parametry funkcjonowania systemu w ujęciu statystycznym. Nie jest zatem prawdziwe propagowane przez wiele opracowań twierdzenie, zgodnie z którym problematyka ryzyka informatycznego daje się w praktyce opisywać ustalonymi rozkładami zmiennych losowych. Jedyną wiarygodną statystyką obrazującą omawianą problematykę może być liczność występowania określonego zdarzenia w zadanym okresie. Arbitralna zamiana tej liczności na prawdopodobieństwo jest subiektywna i dyskusyjna. Co więcej, już na wczesnym etapie procesu szacowania ryzyka wprowadza element sztucznie zniekształcający obraz obserwacji. Dodatkowym elementem wartym zaznaczenia jest to, że w niektórych obszarach zastosowanie prawdopodobieństwa nie wydaje się zasadne. Przykładowo, jak przy wykorzystaniu wartości z przedziału <0; 1> opisać ryzyko związane z bezawaryjnym działaniem serwera w okresie przyszłym?

Uzasadnienie tezy 2. Negatywne skutki zdarzeń naruszających bezpieczeństwo informatyczne mają wieloraki charakter. Jedynie niewielka grupa zdarzeń (incydentów bezpieczeństwa) skutkuje jednowątkowym następstwem finansowym. Większość przypadków ma wieloaspektowe konotacje, przede wszystkim w obszarze trudności w szacowaniu wartości przetwarzanych danych, a także w obszarze niewymiernych strat moralnych i wizerunkowych.

Proponowana metodyka umożliwia szacowanie ryzyka *sensu stricto*[28]. Warunkiem jej implementacji jest zatem zdefiniowanie obszaru zarządzania ryzykiem, który poddaje się prostej analizie ilościowej ukierunkowanej na zliczanie wystąpień określonych zdarzeń w zadanym przedziale czasowym. Metodyka nie posługuje się pojęciem prawdopodobieństwa, wykorzystuje natomiast pojęcie i teoretyczne podstawy zbiorów rozmytych.

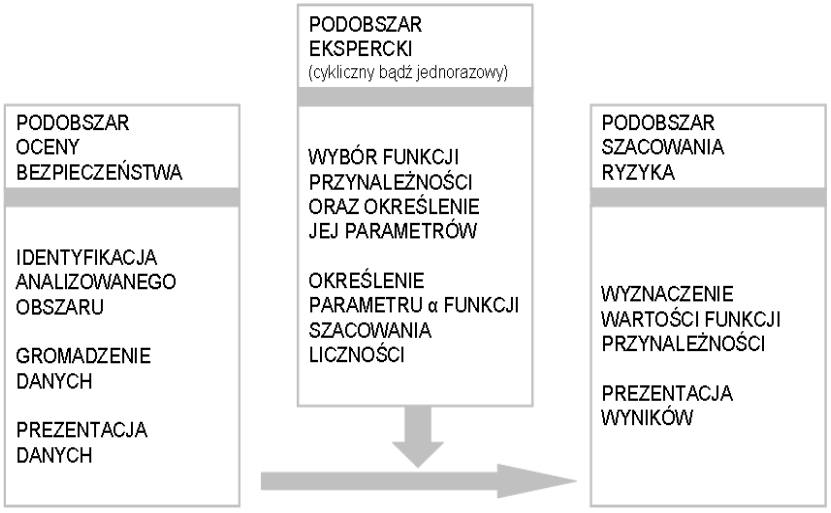
Zbiorem rozmytym można nazwać elementy niepustego zbioru, jeśli dane jest odwzorowanie przyporządkowujące tym elementom ich funkcję przynależności[29]. Często spotykana, formalna definicja zbioru rozmytego przedstawia ten zbiór za pomocą równości[30]:

$$A = \{(x, \mu_A(x)) : x \in X, \mu_A(x) \in [0,1]\}, \tag{5}$$

gdzie $\mu_A : X \to [0,1]$ jest funkcją przynależności elementów X do zbioru A.

Zbiory rozmyte mają zastosowanie tam, gdzie nie posiadamy wystarczającej wiedzy o modelu matematycznym rządzącym danym zjawiskiem, oraz tam, gdzie stworzenie takiego modelu staje się nieopłacalne lub nawet niemożliwe.

Ramowy schemat proponowanej metodyki przedstawiono na rys. 1.



Rys. 1. Schemat ideowy proponowanej metodyki

Źródło: opracowania własne.

[28] Jak już wspomniano, ryzyko informatyczne *sensu largo* jest pewną sumą ryzyk *sensu stricto*. Sposób jego wyznaczenia może być zatem rozwinięciem proponowanej metodyki.

[29] Dokładniejszą definicję znaleźć można np. w: A. Łachwa, *Rozmyty świat zbiorów, liczb, relacji, faktów, reguł i decyzji*, Akademicka Oficyna Wydawnicza EXIT, Warszawa, 2001, s. 13 i n.

[30] *Ibidem*, s. 15.

Do stałych elementów metodyki zalicza się:
- normalny (czyli taki, którego wysokość wynosi 1) zbiór rozmyty o nazwie „Nieakceptowalna częstość występowania zdarzenia",
- ogólną postać funkcji szacowania liczności występowania zdarzenia w okresie następnym daną wzorem:

$$n_{t+1} = \alpha n_t , \tag{6}$$

gdzie: n_{t+1} – szacowana liczność występowania zdarzenia w okresie następnym (będącym okresem, dla którego szacowane jest ryzyko),
n_t – zaobserwowana liczność występowania zdarzenia w okresie analizy,
α – ekspercki parametr obrazujący oczekiwany poziom zmiany przybierający dowolne wartości rzeczywiste.

Na proponowaną metodykę składają się trzy obszary, które w praktyce można utożsamiać z etapami postępowania. Pierwszy z nich dotyczy gromadzenia danych historycznych obrazujących funkcjonowanie analizowanego obszaru systemu w zadanym okresie. Etap ten ma na celu wyznaczenie poziomu bezpieczeństwa oraz ukonstytuowanie bazy dla analiz ukierunkowanych na szacowanie poziomu ryzyka.

Etap drugi związany jest z wyznaczeniem przez czynnik ekspercki parametrów modelu dla analizowanego obszaru. Etap ten może być wykonywany każdorazowo, w odniesieniu do analizy konkretnego problemu, bądź sporadycznie – w odniesieniu do grupy problemów lub nawet całego procesu zarządzania ryzykiem. Do zadań realizowanych w tym etapie zalicza się:

a) wybór postaci funkcji przynależności,

b) określenie wartości parametrów a oraz b,

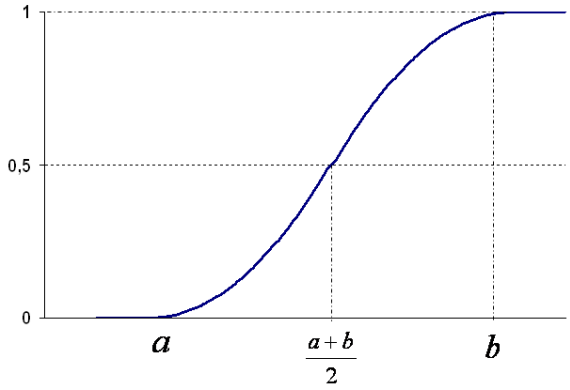
c) określenie parametru α funkcji szacowania liczności występowania zdarzenia w okresie następnym.

Ad a). Literatura przedmiotu proponuje kilka klas funkcji przynależności o dziedzinie w zbiorze liczb rzeczywistych[31]. Na potrzeby funkcjonalnego opisu zbioru „Nieakceptowalna częstość występowania zdarzenia" najwłaściwsza wydaje się funkcja klasy s dana wzorem:

$$s_{a,b}(x) = \begin{cases} 0 & dla \quad x \le a \\ 2 \cdot \left(\dfrac{x-a}{b-a} \right)^2 & dla \quad a < x \le \dfrac{a+b}{2} \\ 1 - 2 \cdot \left(\dfrac{x-b}{b-a} \right)^2 & dla \quad \dfrac{a+b}{2} < x < b \\ 1 & dla \quad x \ge b \end{cases} . \tag{7}$$

Wykres funkcji klasy s przedstawiono na rys. 2.

[31] *Ibidem*, s. 18 i n.



Rys. 2. Wykres funkcji klasy *s*

Źródło: opracowania własne.

Trudno oczywiście wykazać przewagę tej klasy nad innymi. Przyjęta w konkretnym przypadku postać funkcji przynależności musi być wynikiem analiz eksperckich oraz specyfiki analizowanego obszaru.

Ad b). Wartości parametrów *a* oraz *b* muszą być ustalane w ścisłym związku z przyjętą postacią funkcji przynależności oraz analizowanym zagadnieniem. W przypadku ogólnym, można zaproponować, aby wartość *a* była bliska zera (brak lub sporadyczne wystąpienia określonego zdarzenia), natomiast wartość *b* powinna być równa najmniejszej liczności nieakceptowalnej z punktu widzenia czynnika eksperckiego.

Ad c). Wartość parametru α może określać procentowy przyrost (spadek) szacowanej liczności występowania zdarzenia. Sposób wyznaczania parametru jest dowolny. Może być on efektem analiz delfickich, miarą zmiany w dwóch poprzedzających (delta) okresach bądź wyznacznikiem trendu. Warto podkreślić, że wartość parametru jest kluczowym elementem warunkującym jakość informacji wynikowej proponowanej metodyki.

W etapie ostatnim na podstawie przyjętych parametrów modelu szacowana jest wartość wynikowa funkcji przynależności oraz określana jest jej jakościowa interpretacja.

Zaproponowana powyżej metodyka jest procedurą deterministyczną. Może być jednocześnie narzędziem oceny bezpieczeństwa, jak i szacowania ryzyka. O ile determinizm w pierwszym przypadku jest cechą wszystkich metod oceny bezpieczeństwa, o tyle niestochastyczność w przypadku szacowania ryzyka należy uznać za atrybut nieczęsto spotykany. Metodyka zmienia sposób postrzegania problematyki ryzyka informatycznego, odsuwając w cień rekomendacje normatywne. Wprowadza dwa nowe elementy, jakimi są:

– pominięcie pojęcia prawdopodobieństwa oraz problemów związanych z jego szacowaniem,
– pominięcie pojęcia straty związanej z danym zdarzeniem.

Zastosowanie zbioru rozmytego do wyznaczania ilościowej miary ryzyka informatycznego ma uzasadnienie w łatwości przełożenia wartości funkcji przynależności na interpretację jakościową – niezbędną w procesie zarządzania ryzykiem informatycznym. Co więcej, postać funkcji przynależności nie musi determinować interpretacji wyników – innymi słowy, polityka banku w obszarze zarządzania ryzykiem informatycznym może zakładać, że postać funkcji przynależności jest elementem definiowanym przez zespół ekspercki i nie musi być znana osobom podejmującym decyzje na podstawie wyników analizy. Atrybuty zbioru rozmytego w naturalny sposób dostosowują się także do specyfiki omawianego zagadnienia, w którym nieprzewidywalność przyszłych zdarzeń oraz wynikająca z niej konieczność podejmowania decyzji w warunkach niepewności[32] są elementami nieuniknionymi.

6. Krytyka

Krytyka metodyki może wskazać na następujące elementy dyskusyjne:

1. Pominięcie pojęcia prawdopodobieństwa jest pozorne – parametr α jest bowiem swego rodzaju substytutem tego pojęcia.

To prawda, jednak zmiana ta ma także wymiar praktyczny. Wyznaczenie wartości α przez czynnik ekspercki nie napotyka problemów interpretacyjnyche – jest to bowiem wartość opisująca oczekiwaną zmianę. Określenie tej samej zmiany z wykorzystaniem pojęcia prawdopodobieństwa jest znacznie trudniejsze. Przykładowo, w analizowanym okresie bezawaryjny czas pracy serwera systemu bankowości internetowej wyniósł 98%. W proponowanej metodyce oznaczałoby to dwa zdarzenia naruszające bezpieczeństwo systemu oraz 2α zdarzeń przewidywanych (szacowanych) na okres następny[33]. Innymi słowy, szacowany bezawaryjny czas pracy serwera wynosi $(100\text{-}2\alpha)\%$. W jaki natomiast sposób oszacować bezawaryjny czas pracy serwera z wykorzystaniem prawdopodobieństwa? Możliwe jest oczywiście przyjęcie przez analogię wartości $p(x) = 1–(1 – 2\alpha/100)$, ale jaką interpretację można takiej wartości nadać? Czy wartość $p(x)$ oznacza, że serwer w okresie przyszłym będzie z prawdopodobieństwem równym 1 niedostępny przez $2\alpha\%$ czasu? Problem interpretacyjny jest w tym przypadku aż nadto widoczny.

2. Pominięcie wartości potencjalnych strat powoduje zmniejszenie zawartości informacyjnej wyników szacowania ryzyka informatycznego.

Opisane powyżej zagadnienia związane z problemem szacowania wartości potencjalnych strat wskazują na pozorną jedynie zawartość informacyjną wartości straty wyrażonej w pieniądzu. Kontynuując powyższy przykład: czy 2% niedostępności serwera w danym okresie można przełożyć tylko i wyłącznie na straty wynikające z kosztów jego ponownego uruchomienia? Przecież straty wizerunkowe wynikające z natychmia-

[32] Dyskusja na temat różnic pomiędzy ryzykiem a niepewnością wykracza poza ramy niniejszego opracowania.

[33] Pozostawienie miar procentowych również jest możliwe.

stowych bądź przyszłych reakcji klientów, a także medialnego oddźwięku są nieporównywalnie większe oraz praktycznie niemożliwe do oszacowania.

7. Podsumowanie

Zaproponowana metodyka nie uzurpuje sobie prawa do zastąpienia koncepcji klasycznych, normatywnych, standardowych. Może być jednak ich znakomitym uzupełnieniem w wielu sytuacjach, szczególnie tych, które nie poddają się łatwo procedurom szacowania prawdopodobieństw wystąpienia okresowych zdarzeń, oraz tych, dla których trudno jest wyznaczyć wartość potencjalnych strat. Rozwiązanie przedstawione powyżej nie jest także pierwszą próbą zastosowania zbiorów rozmytych w obszarze zarządzania ryzykiem informatycznym[34], analiza literatury przedmiotu wskazuje jednak na to, że jako pierwsze pomija pojęcia prawdopodobieństwa oraz potencjalnej straty.

Literatura

Beck U., *Społeczeństwo ryzyka*. *W drodze do nowej rzeczywistości*, Wydawnictwo SCHOLAR, Warszawa 2004.

Bernstein P.L., *Przeciw bogom. Niezwykłe dzieje ryzyka*, WIG PRESS, Warszawa 1997.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.

Carnap R., *Wprowadzenie do filozofii nauki*, Fundacja Aletheia, Warszawa 2000.

Carr V., Tah J.H.M., *A Fuzzy Approach to Construction Project Risk Assessment and Analysis*: *Construction Project Risk Management System*, „Advances in Engineering Software" 2001, Vol. 32.

Cieciura M., Zacharski J., *Metody probabilistyczne w ujęciu praktycznym*, Wydawnictwo VIZJA PRESS&IT, Warszawa 2007.

Cremonini M., Martini P., *Evaluating Information Security Investments from Attackers Perspective: The Return-on-Attack (ROA)*, 4th Workshop on the Economics on Information Security Proceedings, 2005.

CSI Computer Crime & Security Survey, 2008, http://www.cse.msstate.edu/~cse6243/readings/CSI survey2008.pdf.

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

Finne T., A *Conceptual Framework for Information Security Management*, „Computers & Security" 1998, Vol. 17.

Flasiński M., *Zarządzanie projektami informatycznymi*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Gordon L.A., Loeb M.P., *The Economics of Information Security Investment*, „ACM Transactions on Information and System Security" 2002, Vol. 5, No. 4, s. 438-457.

[34] Por. np.: V. Carr, J.H.M. Tah, A *Fuzzy Approach to Construction of Project Risk Assessment and Analysis*: *Construction of Project Risk Management System*, „Advances in Engineering Software" 2001, Vol. 32, s. 847.

Gospodarowicz A., *Ryzyko operacyjne i jego ocena w regulacjach Nowej Umowy Kapitałowej*, (w:) K. Jajuga (red.), *Wyzwania współczesnych finansów*, UE, Wrocław 2009, s. 27-35.

Gospodarowicz A., Wawrzyniak D., *Ryzyko informatyczne jako ważny element ryzyka operacyjnego w banku – wybrane zagadnienia finansowania zarządzania ryzykiem informatycznym*, (w:) W. Chmielarz, J. Turyna (red.), *Komputerowe systemy zarządzania*, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 2009, s. 57-70.

Heller M., *Filozofia i wszechświat*, Wydawnictwo UNIVERSITAS, Kraków 2006.

Hulthen R., *Communicating the Economic Value of Security Investments*; Value at Security Risk, WEIS2008 – Workshop on the Economics of Information Security Proceedings, 2008.

Jajuga K. (red.), *Zarządzanie ryzykiem*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Jakubczyk J., *Metody oceny projektu gospodarczego*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Jaquith A., *Security Metrics*, Addison-Wesley, Pearson Education Inc., 2007.

Johnson E.M., *A Broader Context for Information Security*, „Financial Times", 16 Sept. 2005, s. 4.

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

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Łachwa A., *Rozmyty świat zbiorów, liczb, relacji, faktów, reguł i decyzji*, Akademicka Oficyna Wydawnicza EXIT, Warszawa, 2001.

Measuring the Return on IT Security Investments, Intel Information Technology, White Paper, 2007.

Milburn G., *Inżynieria kwantowa*, Wydawnictwo Prószyński i S-ka, Warszawa 1999.

Munteanu A., *Information Security Risk Assessment*: *The Qualitative Versus Quantitative Dilemma*, *Managing Information in the Digital Economy*: *Issues & Solutions*, http://www.ssrn.com/.

Olovsson T., *A Structured Approach to Computer Security*, Technical Report No. 122, Chalmers University of Technology, 1992.

Orzeł J., *Rola metod heurystycznych*, *w tym grupowej oceny ekspertów*, *oraz prawdopodobieństwa subiektywnego w zarządzaniu ryzykiem operacyjnym*, „Bank i Kredyt", Narodowy Bank Polski, maj 2005.

PN-I-02000:2002, *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*, Polski Komitet Normalizacyjny.

PN-ISO/IEC 27001:2007, *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Polski Komitet Normalizacyjny.

Purser S.A., *Improving the ROI of the Security Management Process*, „Computers & Security" 2004, Vol. 23, s. 542-546.

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

Schechter S.E., *Computer Security Strength & Risk*: *A Quantitative Approach*, Harvard University, Boston 2005.

Słownik współczesnego języka polskiego pod redakcją naukową Bogusława Dunaja, Wydawnictwo Wilga, 1996.

Sonnenreich W., *Return on Security Investment (ROSI): A Practical Quantitative Model*, A summary of Research and Development conducted at SageSecure.

Sosnowska H., *Prawdopodobieństwo subiektywne a reguły rachunku prawdopodobieństwa*, (w:) S. Forlicz (red.), *Metody ilościowe w ekonomii*, Wydawnictwo Wyższej Szkoły Bankowej w Poznaniu, Poznań 2008.

Tsiakis T., Stephanides G., *The Economic Approach of Information Security*, „Computers & Security" 2005, Vol. 24, s. 105-108.

Uniwersalny słownik języka polskiego pod redakcją naukową Stanisława Dubisza, Wydawnictwo Naukowe PWN, t. III, Warszawa 2003.

Wawrzyniak D., *Information Security Risk Assessment Model for Risk Management*, (w:) S. Fisher-Hubner, S. Furnell, C. Lambrinoudakis (Eds.), *Trust, Privacy, and Security in Digital Business*, Third International Conference, TrustBus 2006 Proceedings, Springer, 2006, s. 21-30.

Wawrzyniak D., *Wybrane problemy oceny ryzyka informatycznego w działalności bankowej*, „Rachunkowość Bankowa" 2006, nr 10(23), s. 57-65.

Willemson J., *On the Gordon&Loeb Model for Information Security Investment*, WEIS2006 – Workshop on the Economics of Information Security Proceedings, 2006.

Zabierowski M., *Wszechświat i metafizyka*, Wydawnictwo Naukowe PWN, Warszawa 1998.

INFORMATION SECURITY RISK IN BANKING – TOWARDS NEW PARADIGM

Summary: Information security risk management is becoming more and more crucial problem due to dynamic information sciences development as well as their implementations in all business areas. The risk constitutes today a base for contemporary institutions activities. More to say, in the context of financial institutions the risk should be seen as a crucial factor determining their existence. The article presents chosen aspects of assessment problems dealing with security risk management as well as the foundations of a new information security risk assessment paradigm. This paradigm brings two fundamental aspects of security risk analysis into question. They are: the probability of an event and potential loss value.