PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 55
Informatyka Ekonomiczna 13 2009

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

PODEJŚCIE ILOŚCIOWE I JAKOŚCIOWE W ANALIZIE RYZYKA INFORMATYCZNEGO W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH

Streszczenie: Technologie informacyjne pozwalają osiągnąć organizacjom nową jakość funkcjonowania, jednocześnie rośnie stopień zdeterminowania sprawnego zarządzania od nowoczesnych, lecz bezpiecznych rozwiązań teleinformatycznych. W miarę postępu technologicznego, a szczególnie gwałtownego rozwoju Internetu, ryzyko związane z funkcjonowaniem systemów informatycznych staje się coraz bardziej powszechne i przybiera różnorodne formy. Brak odpowiedniego przygotowania na ryzyko może prowadzić firmę do upadku, stąd też właściwe reagowanie na nie stanowi często o możliwościach przetrwania i rozwoju przedsiębiorstwa. Bardzo istotna jest więc analiza ryzyka, będąca głównym procesem zarządzania ryzykiem, polegająca na identyfikacji i ocenie ryzyka. Niniejszy artykuł jest wprowadzeniem do zagadnień ryzyka informatycznego, a zwłaszcza problematyki jego ilościowej i jakościowej analizy. W artykule przedstawiono m.in. następujące metody ilościowe: model ALE (Annual Loss Expected) i wskaźniki pochodne, metodę Courtneya, model ISRAM (Information Security Risk Analysis Method). Kolejno zostały omówione również następujące metody jakościowe: FMEA (Failure Mode and Effects Analysis) i FMECA (Failure Mode and Effects Criticality Analysis), FRAP (Facilitated Risk Analysis Process) oraz popularne metodologie NIST 800-30 i CRAMM (CCTA's Risk Analysis and Management Methodology).

Słowa kluczowe: technologie informacyjne, ryzyko informacyjne, modele oceny ryzyka.

1. Wstęp

Ryzyko związane z szerokim zastosowaniem technologii informatycznych w biznesie rośnie wraz ze zwiększaniem się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i ilości czynników ryzyka. Przy niedostatecznych inwestycjach w bezpieczeństwo informacji znaczenia nabiera problematyka zarządzania ryzykiem technologii informacyjnych (IT), koncentrująca się na poszukiwaniu optymalnego stosunku zagrożeń do kosztów zabezpieczeń zasobów informatycznych. Przy tak dynamicznym rozwoju technologii informatycznych skraca się zdecydowanie czas wymagany na odpowiednią reakcję wobec ryzyka. Brak odpowiedniego przygotowania może prowadzić fir-

mę do upadku, stąd też właściwe reagowanie na ryzyko stanowi o możliwościach przetrwania i rozwoju przedsiębiorstwa. Problematyka zarządzania ryzykiem IT jest zagadnieniem bardzo złożonym. Jednym z najważniejszych etapów tego procesu jest analiza ryzyka, służąca minimalizacji strat związanych z ryzykiem. Kluczowym jej elementem jest etap oceny czy też szacowania ryzyka. Celem niniejszego artykułu jest wprowadzenie do zagadnień ryzyka informatycznego oraz zaprezentowanie wybranych metod ilościowych i jakościowych jego analizy i oceny, które mogą być stosowane w sektorze małych i średnich przedsiębiorstw. Jak pokazuje praktyka, w tych właśnie przedsiębiorstwach podejście do problematyki zarządzania ryzykiem informatycznym ma charakter fragmentaryczny, a sam proces analizy i szacowania ryzyka informatycznego niejednokrotnie nie jest w ogóle przeprowadzany.

2. Podstawy ryzyka systemów informatycznych

Istnieje wiele ujęć i definicji ryzyka. W związku z wszechobecnością występowania ryzyka w życiu społecznym i gospodarczym człowieka pojęcie to stało się przedmiotem badań wielu dyscyplin naukowych związanych z teorią ekonomii, teorią ubezpieczeń, finansami, prawem, matematyką, statystyką, rachunkowością i wieloma innymi. Należy jednak pamiętać o tym, że w różnych dziedzinach naukowych ryzyko jest postrzegane inaczej. Również w odmiennych formach działalności biznesowej będziemy mieli do czynienia z indywidualnymi formami ryzyka. Inne typy ryzyka wystąpią przecież w przedsiębiorstwie produkcyjnym, inne natomiast np. w sektorze finansowym. Ryzyko i niepewność nieodłącznie towarzyszą podejmowaniu decyzji gospodarczych. Ponieważ nie można całkowicie uniknąć ryzyka, należy poznać rządzące nim mechanizmy i nauczyć się nim zarządzać.

Etymologia ryzyka nie została dotychczas jednoznacznie wyjaśniona. Według Encyklopedii Brockhausa znaczenie tego słowa wywodzi się z języka łacińskiego, gdzie czasownik *risicare* znaczy omijać coś. Greckie *riza*, podobnie jak włoskie *ris(i)co* oznacza rafę, którą statek powinien ominąć, a więc niebezpieczeństwo, którego powinien uniknąć [Kaczmarek 2003, s. 11-12]. Chodzi tu zatem o niebezpieczeństwa, których powinni unikać żeglarze i handlowcy. W tym sensie ryzyko jest wyborem, a nie nieuchronnym przeznaczeniem.

Na temat pojęcia ryzyka i jego różnorodnych kwalifikacji napisano już wiele. Ryzyko jest mieszaniną wielu wciąż zmieniających się czynników, dlatego i praktycy, i teoretycy nie podają jednej uniwersalnej definicji, stąd też istnieje ich wiele. Jak pisze W. Ostasiewicz w pracy [*Składki i ryzyko*… 2004], intuicyjny sens tego pojęcia jest oczywisty i jest to coś, co może się zdarzyć, a czego nie chcemy lub czego się boimy. Autor jednocześnie podaje definicję tego terminu, określając ryzyko jako niechciane, niepewne zdarzenie, i traktuje je jako możliwość niepewnej straty, którą jest najczęściej strata finansowa [*Składki i ryzyko*… 2004, s. 11].

Szczególnym rodzajem ryzyka, którego dotyczą rozważania podejmowane w niniejszym artykule, jest ryzyko systemów informatycznych, określane często w lite-

raturze przedmiotu jako ryzyko informatyczne. Podobnie jak przy definicji samego ryzyka, termin ten nie jest definiowany w sposób jednoznaczny. Jak wskazano, termin **ryzyko** ma wiele odcieni znaczeniowych. W większości jednak jest związany z pojęciem **straty**, co jest zgodne również z intuicyjnym rozumieniem tego pojęcia. Najogólniej jest to możliwość lub prawdopodobieństwo wystąpienia niekorzystnego w skutkach zdarzenia. Takie ujęcie ryzyka odpowiada jego znaczeniu w informatyce, gdzie jest rozpatrywana możliwość wykorzystania podatności przez zagrożenie w celu spowodowania niekorzystnych następstw dla instytucji [Białas 2006, s. 75]. W kontekście bezpieczeństwa systemów informatycznych ryzyko systemów informatycznych najczęściej jest traktowane jako zbiorcza miara prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu, a zatem pośrednią lub bezpośrednią szkodę dla organizacji.

Wydaje się, że na potrzeby bezpieczeństwa systemów informatycznych można przytoczyć następującą definicję podaną w normie IEC 61508: „Ryzyko oznacza miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażoną jako iloczyn prawdopodobieństwa (lub możliwości) wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat)" [Liderman 2001]. Z kolei ryzyko informatyczne definiowane przez Polską Normę PN-I-02000 to możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych [Polska Norma PN-I-02000...].

Jedna z najprostszych, a jednocześnie najlepiej oddająca istotę ryzyka systemów informatycznych, to definicja podana przez stowarzyszenie ISACA (*Information Systems Audit and Control Association)*: „Ryzyko jest możliwością wystąpienia zdarzenia, które będzie miało niepożądany wpływ na organizację i jej systemy informatyczne" [ISACA 2000].

W literaturze ryzyko systemów informatycznych określane jest również jako zagrożenie, iż technologia informatyczna stosowana w danej organizacji (niezależnie od jej rodzaju i skali działalności) [Ryba 2006, s. 13]:

– nie spełnia wymogów biznesowych,
– nie zapewnia odpowiedniej integralności, poufności i dostępności danych,
– nie została odpowiednio wdrożona i nie działa zgodnie z założeniami.

Norma ISO/IEC TR 13335-1 traktuje ryzyko systemów informatycznych jako miarę prawdopodobieństwa i definiuje je jako zbiorczą miarę prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu informacyjnego, a zatem pośrednią lub bezpośrednią szkodę dla instytucji [ISO/IEC TR 13335-1...]. Ta i inne wspomniane definicje nawiązują do terminu podatności (*vulnerability*), obejmującej według normy ISO/IEC TR 13335-3 słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie oraz atrakcyjność aktywów informacyjnych [ISO/IEC TR 13335-3...]. Norma ta zawiera również pewne wskazówki, od czego zależy wielkość ryzyka: „[...] ryzyko jest funkcją wartości zasobów objętych ryzykiem, możliwości

wystąpienia zagrożeń, łatwości wykorzystania podatności przez zagrożenia oraz istniejących (lub planowanych, gdy szacuje się ryzyko dla projektowanych systemów bezpieczeństwa) zabezpieczeń mogących zredukować ryzyko" [Polska Norma PN-I-13335...; Liderman 2008, s. 70].

3. Analizy ryzyka informatycznego jako element zarządzania ryzykiem

Zarządzanie ryzykiem informatycznym odgrywa obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji. Polega ono na identyfikacji zagrożeń i podatności, szacowaniu ryzyka oraz rekomendowaniu dodatkowych środków zabezpieczeń. Analiza ryzyka wskazuje, że wprowadzając zabezpieczenia zgodne z wymaganiami, chronimy te zasoby przed zagrożeniami i zmniejszamy ryzyko ich wystąpienia.

Termin **analiza ryzyka** (*risk analysis*) w literaturze przedmiotu jest używany bardzo często, przy czym różni autorzy podają różny zakres przedsięwzięć składających się na proces analizy ryzyka. Generalnie analiza ryzyka polega na ocenie wszystkich negatywnych skutków badanego przedsięwzięcia i odpowiadających im prawdopodobieństw (częstości występowania) [Liderman 2001]. K. Liderman podaje najbardziej ogólną definicję analizy ryzyka na potrzeby bezpieczeństwa teleinformatycznego, formułując ją następująco: Analiza ryzyka (na potrzeby bezpieczeństwa teleinformatycznego) jest procesem identyfikacji (jakościowej i ilościowej) ryzyka utraty bezpieczeństwa teleinformatycznego [Liderman 2001].

W ramach analizy ryzyka można wyróżnić następujące etapy szczegółowe [Szczepankiewicz 2006]:

- identyfikacja aktywów chronionych,
- wycena wartości chronionych,
- identyfikacja zagrożeń i podatności,
- oszacowanie zagrożeń oraz podatności,
- oszacowanie ryzyka poprzez oszacowanie prawdopodobieństwa i oszacowanie skutków wystąpienia danego zdarzenia.

Zadaniem procesu szacowania i oceny ryzyka jest wskazanie aktywów najbardziej zagrożonych w firmie (miejsc o relatywnie wysokim prawdopodobieństwie zmaterializowania się zagrożenia), dzięki czemu wiemy, którymi aktywami należy się zająć w pierwszej kolejności i wdrożyć dla nich odpowiednie zabezpieczenia (fizyczne, techniczne lub organizacyjne). Zatem analiza ryzyka jest zasadniczo głównym procesem zarządzania ryzykiem, identyfikuje ryzyko i dokonuje oceny ryzyka, które ma być kontrolowane, minimalizowane lub też akceptowane. Podstawowym celem analizy ryzyka jest dostarczenie informacji niezbędnej w podejmowaniu decyzji o zastosowaniu określonych metod, środków, narzędzi bezpieczeństwa IT w organizacji.

Ze względu na złożoność procesu analizy ryzyka, a szczególnie szacowania ryzyka, przejawiającą się m.in. w ilości danych, które należy wziąć pod uwagę, wykorzystuje się oprogramowanie wspomagające. Przykładem takiego oprogramowania jest Certus Risk Analyzer Professional, który jest narzędziem wspomagającym przeprowadzenie procesu analizy ryzyka związanego z aktywami i zasobami, w sposób systematyczny, umożliwiający późniejsze porównywanie poziomów ryzyka. Podstawowym zastosowaniem tej aplikacji jest m.in. konieczność okresowego przeprowadzania analizy ryzyka na potrzeby systemu zarządzania bezpieczeństwem informacji według standardu ISO 27001 [*Certus Risk*…].

4. Analiza ryzyka – podejście ilościowe i jakościowe

Do analizy ryzyka, na jakie są narażone aktywa organizacji, stosuje się dwie zasadnicze grupy metod [Szczepankiewicz, Szczepankiewicz 2006; Białas 2006, s. 76]:

- Ilościowe (*quantitative*), gdzie oszacowanie wartości ryzyka wiąże się z wykorzystaniem miar liczbowych – wartość zasobów jest określana kwotowo, częstotliwość wystąpienia zagrożenia − liczbą przypadków, a podatność − wartością prawdopodobieństwa ich utraty; metody te prezentują wyniki w postaci wskaźników. Przykłady metod ilościowych: metoda Courtneya, metoda Fishera.
- Jakościowe (*qualitative*), które nie operują na danych liczbowych, przedstawiając wyniki w postaci opisów, zaleceń, gdzie oszacowanie ryzyka wiąże się z:
  - opisem jakościowym wartości aktywów, określeniem skal jakościowych dla częstotliwości wystąpienia zagrożeń i podatności na dane zagrożenie, albo
  - opisem tzw. scenariuszy zagrożeń poprzez przewidywanie głównych czynników ryzyka.

Wyniki w tych metodach uzyskuje się w postaci określeń typu: ryzyko wysokie, średnie niskie, większe niż …, mniejsze niż …, podobne jak …, aczkolwiek sam proces analizy może być bardzo szczegółowy, pracochłonny i wymagać dużego doświadczenia i wiedzy. Przykłady metod jakościowych: FMEA/FMECA, FRAP, The Microsoft Corporate Security Group Risk Management Framework, metodyka NIST SP 800-30 oraz metodyka CRAMM.

Tabela 1. Najważniejsze zalety oraz wady ilościowych i jakościowych metod analizy ryzyka IT

Analiza ryzyka	Metody ilościowe	Metody jakościowe
1	2	3
Wybrane zalety	• Pozwalają określać konsekwencje wystąpienia incydentów w sposób ilościowy, co ułatwia przeprowadzenie analizy kosztów i korzyści podczas wyboru zabezpieczeń • Dają dokładniejszy obraz ryzyka	• Pozwalają uszeregować ryzyka według priorytetu • Pozwalają wyznaczyć w krótkim czasie i bez większych nakładów obszary zwiększonego ryzyka • Analiza jest stosunkowo łatwa i tania

1	2	3
Wybrane wady	• Ilościowe miary zależą od zakresu i dokładności zdefiniowanej skali pomiarowej • Wyniki analizy mogą być nieprecyzyjne, a nawet mylące • Zwykle metody te muszą być wzbogacone o opis jakościowy (w postaci komentarza, interpretacji) • Analiza przeprowadzona przy zastosowaniu tych metod jest na ogół droższa, wymaga większego doświadczenia i zaawansowanych narzędzi	• Nie pozwalają wyznaczyć prawdopodobieństw i skutków następstw za pomocą miar liczbowych • Trudniejsza jest analiza kosztów-korzyści (*costs-benefits*) podczas doboru zabezpieczeń • Uzyskane wyniki mają charakter ogólny, przybliżony itp.

Źródło: opracowanie własne na podstawie [Białas 2006, s. 107].

W zależności od wagi danego zagrożenia można stosować różne miary ryzyka − od bardzo prostych ocen, określających ryzyko jako wysokie, średnie lub niskie, do dokładnych wskaźników wyrażonych jako prawdopodobieństwo wystąpienia danego zdarzenia. Dobór odpowiednich metod analizy ryzyka jest bardzo istotny, gdyż prawidłowe oszacowanie ryzyka i ocena prawdopodobieństwa jego wystąpienia daje jasny obraz jego wpływu na funkcjonowanie całego systemu informacyjnego w organizacji.

5. Wybrane metody ilościowe w analizie ryzyka informatycznego

Przy wykorzystaniu metod ilościowych istnieje problemem właściwego oszacowania wartości niezbędnych do kalkulacji. Wartość ryzyka może być wyrażona za pomocą różnego rodzaju skal lub bezpośrednio w wymiarze finansowym, jako przewidywana wielkość strat związanych z danym rodzajem ryzyka, w założonym okresie. Podstawowe zależności stosowane do szacowania ryzyka, prezentowane w literaturze przedmiotu, przedstawiają się następująco [Szczepankiewicz, Szczepankiewicz 2006]:

$$R = P \times W \text{ oraz } P = F \times V, \tag{1}$$

gdzie:

R – wartość ryzyka,
P – prawdopodobieństwo lub przewidywana liczba wystąpień incydentu powodującego utratę wartości aktywów w przyjętym okresie,
W – wartość straty – przewidywana średnia utrata wartości aktywów w wyniku wystąpienia pojedynczego incydentu,
F – częstotliwość wystąpienia zagrożenia,
V – podatność systemu informatycznego (lub jego elementu) na zagrożenie; jest to miara prawdopodobieństwa wykorzystania określonej podatności przez dane zagrożenie.

Wynika z tego, iż ocena ryzyka informatycznego wyrażana jest najczęściej jako wartość oczekiwanych strat, która opiera się na określeniu trzech podstawowych wielkości [Szczepankiewicz, Szczepankiewicz 2006]:

– wartości zasobu (np. informacji) dla prawidłowego funkcjonowania przedsiębiorstwa, określonej kwotowo,
– częstotliwości występowania zagrożenia dla zasobu (np. przetwarzanej informacji), określonej jako liczba wystąpień – w praktyce dla określenia częstotliwości zagrożeń ustala się okres, w jakim będzie się rozpatrywać ich występowanie (najczęściej okres jednego roku),
– podatności systemu informatycznego (lub jego wybranych elementów) na zagrożenie, określonej jako miernik prawdopodobieństwa wystąpienia strat na skutek wystąpienia zdarzenia.

Dość powszechną i w miarę często stosowaną metodą ilościową analizy ryzyka jest metoda wykorzystująca model **ALE** (*Annual Loss Expected*), bazujący na idei straty oczekiwanej, przedstawiany często w literaturze przedmiotu w postaci jednego z następujących wzorów [Wawrzyniak 2007]:

$$\textbf{\textit{ALE}} = \textit{(prawdopodobieństwo zdarzenia)} \times \textit{(wartość straty)}, \tag{2}$$

$$ALE = \sum_{i=1}^{n} I(O_i) F_i , \tag{3}$$

gdzie: $\{O_1, O_2, ..., O_n\}$ – zbiór negatywnych skutków zdarzenia,
$I(O_i)$ – wartościowo wyrażona strata wynikająca ze zdarzenia,
F_i – częstotliwość i-tego zdarzenia.

Roczna strata oczekiwana dla organizacji będzie wyznaczona przez sumę wszystkich oczekiwanych rocznych strat. Istnieje wiele innych modeli oceny i szacowania ryzyka informatycznego bazujących na powyższej metodzie. Są one dostosowywane do konkretnych potrzeb i sytuacji istniejącej w danej organizacji. Wśród takich metod warto zwrócić uwagę na metodę opracowaną przez R. Courtneya. Według tej koncepcji oczekiwana roczna strata wyraża się wzorem [Ryba 2006, s. 38]:

$$ALE = \frac{10^{f+i-3}}{3}, \tag{4}$$

gdzie: f – indeks określający szacowaną częstotliwość wystąpienia zdarzenia powodującego stratę,
i – indeks określający szacowaną wysokość straty spowodowanej wystąpieniem zdarzenia powodującego tę stratę.

Przedstawiana metoda Courtneya wyróżnia sześć zasadniczych grup zagrożeń: przypadkowe ujawnienie danych, przypadkowa modyfikacja danych, przypadkowe usunięcie danych, celowe ujawnienie danych, celowa modyfikacja danych, celowe

usunięcie danych. Metoda ta została zaakceptowana przez instytucje państwowe USA jako oficjalna metoda analizy ryzyka.

Rozwinięciem metody Courtneya w pełną metodykę projektowania rozwiązań bezpieczeństwa systemów informatycznych jest metoda Fishera opracowana w 1984 r. Aby ją prawidłowo zastosować, dana organizacja musi posiadać politykę bezpieczeństwa informacji. Metodyka ta wyróżnia następujące fazy procesu zarządzania ryzykiem systemów informatycznych [Ryba 2006, s. 39-40]:

– faza 1 – zebranie informacji (identyfikacja i klasyfikacja zasobów systemów informatycznych podlegających dalszej analizie);
– faza 2 – identyfikacja zagrożeń − proces mapowania zagrożeń (wymienione wcześniej 6 grup zagrożeń metody Courtneya) na 11 punktów kontrolnych Fishera, takich jak m.in.: pozyskiwanie, przekazywanie, zmiana formy, transport, odbiór, przetwarzanie, migracja, usuwanie, użytkowanie danych itp.;
– faza 3 – ocena ryzyka, bazująca na następującej zależności:

$$R = P \times C, \tag{5}$$

gdzie: P – prawdopodobieństwo wystąpienia określoną ilość razy w ciągu roku zdarzenia powodującego stratę dla organizacji,
C – strata dla organizacji w wyniku pojedynczego wystąpienia zdarzenia;

– faza 4 – projektowanie mechanizmów kontrolnych;
– faza 5 – ocena biznesowa zidentyfikowanych mechanizmów z wykorzystaniem wskaźnika ROI (Return on Investment), wyrażanego często wzorem [Ryba 2006, s. 39-40]:

$$ROI = \frac{Zysk\ operacyjny\ w\ danym\ okresie}{Wartość\ zainwestowanego\ kapitału}. \tag{6}$$

Wyznaczona w tej metodzie wielkość ryzyka dla poszczególnych mechanizmów kontrolnych interpretowana jest jako zysk operacyjny dla analizowanego okresu, a szacowany koszt mechanizmu kontrolnego traktowany jest jako wartość inwestowanego kapitału.

Model ISRAM (Information Security Risk Analysis Method) jest metodą analizy ryzyka bazującą na omówionej wcześniej metodzie Annual Loss Expected (ALE), jednakże wykorzystuje jako główne narzędzie badania ankietowe. Ocena ryzyka informatycznego jest dokonywana przy zastosowaniu następującej formuły [Karabacak, Sogukpinar 2005; Wawrzyniak 2007]:

$$Risk = \left(\frac{\sum_m T_1 \left(\sum_i w_i p_i \right)}{m} \right) \left(\frac{\sum_m T_2 \left(\sum_j w_j p_j \right)}{n} \right), \tag{7}$$

gdzie: i – liczba pytań ankiety dotyczącej szacowania prawdopodobieństw wystąpienia incydentów,
j – liczba pytań ankiety dotyczącej szacowania konsekwencji,

m,n – liczba uczestników ankiet,
w_i, w_j – wagi pytań „i” „j”,
p_i, p_j – wartości odpowiadające wybranym odpowiedziom na pytania „i” „j”,
T_1 – tabela prawdopodobieństw wystąpienia zdarzeń,
T_2 – tabela wartości negatywnych skutków wystąpienia zdarzeń.

W pracy [Schechter 2004] przedstawiono kilka pochodnych wskaźników dotyczących szacowania ryzyka, bazujących m.in. na zaprezentowanej metodzie straty oczekiwanej (ALE). Wskaźniki te oraz sposoby wyznaczania ich wartości zaprezentowano w tab. 2.

Tabela 2. Strata oczekiwana i wybrane wskaźniki pochodne

Lp.	Wskaźnik	Symbol	Sposób wyznaczenia wartości
1	Oczekiwana strata	ALE (*Annual Loss Expected*)	$ALE = \sum_{i=1}^{n} I(O_i)F_i$
2	Zysk z tytułu zastosowanych zabezpieczeń	S (*Savings – reduction in ALE*)	$S = ALE - ALE_{\text{(z zabezpieczeniami)}}$
3	Wartość dodana	B (*Benefit*)	$B = S +$ *nowe możliwości*
4	Zwrot z inwestycji	ROI (*Return on Investment*)	$ROI = \frac{B}{C}$ C – *koszty zabezpieczeń*
5	Wewnętrzna stopa zwrotu (IRR)	IRR (*Internal Rate of Return*)	$C_0 = \sum_{t=1}^{n} \frac{VA_t - C_t}{(1+IRR)^t}$ C_0 – *początkowy koszt inwestycji* C_t – *kosz inwestycji w roku t*

Źródło: opracowanie własne na podstawie [Schechter 2004; Wawrzyniak 2007].

Przykładem metody ilościowej wzbogaconej o elementy jakościowe jest metoda Parkera, stworzona na potrzeby Computer Security Institute w 1981 r., obejmująca 5 zasadniczych etapów, takich jak: identyfikacja i wycena zasobów, identyfikacja zagrożeń, ocena ryzyka, identyfikacja, wybór i implementacja zabezpieczeń oraz wdrożenie systemu zabezpieczeń. Przy ocenie ryzyka wykorzystywana jest metoda Courtneya, rozbudowana o macierz analizy zagrożeń (Exposure Analysis Matrix). U podstaw tej metody leży założenie, iż istotność zagrożeń jest funkcją liczby osób mogących spowodować stratę, co z kolei prowadzi do analizy ryzyka w podziale na poszczególne grupy zawodowe w przedsiębiorstwie. Zatem Parker w swojej metodzie wykorzystuje metodę Courtneya, poszerzając ją o jakościową analizę ryzyka, formalizuje również wpływ czynnika ludzkiego na ryzyko, co wyróżnia tę metodę spośród pozostałych [Ryba 2006, s. 40].

6. Podejście jakościowe w analizie ryzyka informatycznego

W przypadku wyceny ryzyka bezpieczeństwa informacji w systemie informatycznym przeprowadza się zwykle jakościową analizę ryzyka. Metody te opierają się najczęściej na kryteriach bezpieczeństwa informacji, takich jak: poufność, integralność i dostępność. Pełna analiza ryzyka może być przeprowadzana oddzielnie dla każdego z wymienionych kryteriów. Do celów analizy ustala się skalę wartości informacji (niska, średnia, wysoka). Dla każdego typu zagrożeń należy ocenić częstotliwość zagrożeń ich wystąpienia, używając predefiniowanej skali, która może być różna od przyjętej do wartościowania informacji lub taka sama jak dla wartości informacji. Ponadto dla każdego badanego obszaru systemu informatycznego i każdego typu zagrożenia należy ocenić podatność, stosując skalę, która może być taka sama lub różna od powyższej. Ostatecznie wartość ryzyka można określić jako np. bardzo niską, niską, średnią, wysoką i bardzo wysoką. W celu dokładniejszej kategoryzacji ryzyka metodą analizy jakościowej można zwiększyć skalę wartości, np. od 1 do 10. Wówczas każdy czynnik ryzyka podlega klasyfikacji jako:

– wysokie ryzyko – bardzo istotne i nierozwiązane lub nierozpoznane zagrożenie, które może spowodować poważne negatywne skutki; duże prawdopodobieństwo jego wystąpienia,
– średnie ryzyko – zidentyfikowano problem, jednak potencjalne szkody i/lub prawdopodobieństwo wystąpienia są stosunkowo niskie,
– niskie ryzyko – problem jest rozpoznany i pod kontrolą; istnieje małe prawdopodobieństwo jego wystąpienia.

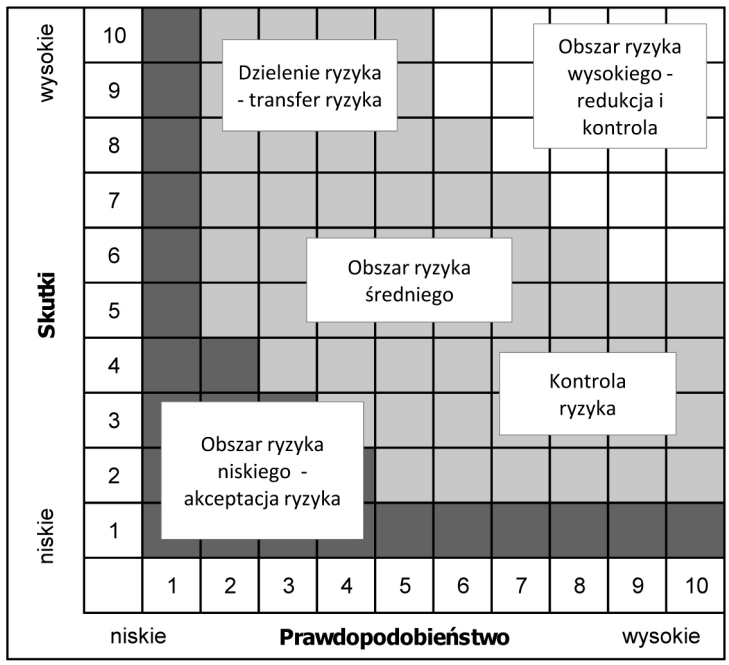
Następnie każdą zmienną ocenia się w skali od 1 do 10, określając następujące wartości:

– prawdopodobieństwa (1 – małe prawdopodobieństwo, ..., 10 – bardzo wysokie prawdopodobieństwo, istnieje niemal pewność wystąpienia),
– skutków (1 – niewielki problem, ..., 10 – znaczące zagrożenie).

Przykładową kategoryzację ryzyka według powyższych kryteriów zobrazowano na rys. 1.

Istnieje wiele jakościowych metod analizy ryzyka. Kolejno zostaną omówione następujące wybrane popularne metody jakościowe stosowane w analizie ryzyka: metody FMEA/FMECA, FRAP oraz metodyki NIST 800-30 i CRAMM.

Metody FMEA (Failure Mode and Effects Analysis) oraz FMECA (Failure Mode and Effects Criticality Analysis) mają swój początek w latach pięćdziesiątych ubiegłego stulecia, gdy opracowano je w celu analizy niezawodności uzbrojenia, i są do dziś stosowane m.in. w przemyśle lotniczym, kosmicznym i elektronicznym. Istotą FMEA/FMECA jest analiza wpływu każdego potencjalnego defektu na funkcjonowanie całego systemu oraz uszeregowanie potencjalnych defektów według stopnia ich dotkliwości. Metoda FMECA dodatkowo wprowadza analizę stopnia dotkliwości defektu oraz bada, czy nie ma on charakteru krytycznego dla funkcjonowania całego ocenianego systemu. Metody te są dość pracochłonne, wymagają wiedzy i



Rys. 1. Kategoryzacja ryzyka i podstawowe strategie postępowania z ryzykiem

Źródło: [Szczepankiewicz, Szczepankiewicz 2006].

doświadczenia osób je stosujących, wspierane są specjalistycznymi narzędziami wykorzystującymi elementy inżynierii wiedzy oraz logiki rozmytej (*fuzzy logic*) [Białas 2006, s. 83].

Głównym celem opracowanej przez T. Petliera metody FRAP (Facilitated Risk Analysis Process) jest odejście od idei metod ilościowych i ograniczenie się głównie do identyfikacji potencjalnych niepożądanych zdarzeń mogących mieć negatywny wpływ na realizację celów biznesowych organizacji. Analiza ryzyka metodą FRAP odbywa się w trakcie sesji analizy ryzyka, podczas których analizie poddawany jest jeden system, aplikacja, obszar biznesowy itp. Zaleceniem jest, aby w sesjach tych uczestniczyły zespoły liczące 7-15 osób, składające się z ekspertów od konkretnego systemu, przedstawicieli kadry zarządzającej, administratorów systemu i jego użytkowników. W trakcie takiej sesji członkowie ci na zasadzie burzy mózgów (*brainstorming*) identyfikują potencjalne zagrożenia i podatności oraz wynikające z nich potencjalne straty. Kolejny etap metody FRAP to nadanie priorytetów zidentyfikowanym zagrożeniom na podstawie doświadczenia członków zespołu. Kolejne działanie to identyfikacja przez zespół mechanizmów kontrolnych i zabezpieczających,

jakie mogłyby zostać zaimplementowane w celu minimalizacji zidentyfikowanych rodzajów ryzyka. Jednakże ostateczna decyzja co do wyboru określonych mechanizmów stosowanych w celu ograniczenia podatności zasobów i ich zagrożeń należy do kadry zarządzającej [Ryba 2006, s. 48-49].

Proces oceny ryzyka informatycznego według metodyki NIST SP 800-30 podzielony został na 9 następujących podstawowych faz [Ryba 2006, s. 41-42]:

- Wybór systemów objętych oceną, określenie zakresu oceny.
- Identyfikacja zagrożeń ocenianych systemów.
- Identyfikacja podatności ocenianych systemów.
- Analiza stosowanych i planowanych mechanizmów kontrolnych i zabezpieczających.
- Określenie prawdopodobieństw wykorzystania podatności przez zidentyfikowane źródła zagrożeń (prawdopodobieństwa określa się jako: niskie, średnie, wysokie).
- Analiza i określenie wpływu incydentów na system, dane i organizację (wpływ określony za pomocą trzystopniowej skali: wysoki, średni, niski).
- Wyznaczenie za pomocą macierzy poziomu ryzyka (Risk Level Matrix) całkowitego ryzyka dla zidentyfikowanych zagrożeń. Macierz ta powstaje w wyniku wymnożenia prawdopodobieństw wystąpienia incydentów (prawdopodobieństwo wysokie otrzymuje wagę 1,0, średnie – 0,5, a niskie – 0,1) i wielkości wpływu incydentów (wpływ wysoki otrzymuje wagę 100, średni – 50, a niski – 10). Na podstawie macierzy określany jest poziom całkowitego ryzyka dla każdego zidentyfikowanego zagrożenia, określany jako wysoki dla iloczynu z przedziału (50,100], średni dla przedziału (10, 50] oraz niski dla przedziału [1,10]. Przykład macierzy bazującej na metodyce opracowanej przez NIST zawarto w tab. 3.
- Opracowanie rekomendacji dla mechanizmów kontrolnych i zabezpieczających oraz innych rozwiązań, których celem jest minimalizacja ryzyka do akceptowalnego poziomu.
- Przygotowanie dokumentacji wyników przeprowadzonej oceny ryzyka informatycznego w postaci raportu dla kadry zarządzającej.

Tabela 3. Przykład macierzy według metodyki NIST

Prawdopodobieństwo wystąpienia zagrożenia	Następstwa		
	niskie (10)	średnie (50)	wysokie (100)
Wysokie (1,0)	niskie 10×1,0 = 10	średnie 50×1,0 = 50	wysokie 100×1,0 = 100
Średnie (0,5)	niskie 10×0,5 = 5	średnie 50×0,5 = 25	średnie 100×0,5 = 50
Niskie (0,1)	niskie 10×0,1 = 1	niskie 50×0,1 = 5	niskie 100×0,1 = 10

Źródło: [Białas 2006, s. 115].

Metodyka CRAMM (CCTA's Risk Analysis and Management Methodology) została przyjęta przez CCTA (U.K. Goverment Central Computer and Telecommunications Agency) jako rządowy standard analizy i zarządzania ryzykiem. Proces zarządzania ryzykiem według tej metodyki składa się z trzech kolejnych etapów [Ryba 2006, s. 44]:

– identyfikacji i wyceny zasobów,
– oceny zagrożeń i podatności,
– wyboru oraz rekomendacji mechanizmów kontrolnych i zabezpieczających.

Głównym celem oceny ryzyka jest określenie prawdopodobieństwa zajścia incydentów zakłócających prawidłowe funkcjonowanie zasobów, gdzie zidentyfikowane zasoby są przydzielane do grup zasobów (*asset groups*), dla których generowane są wykazy zagrożeń mogących dotyczyć danej grupy zasobów i wyznaczany jest poziom ryzyka dla każdej grupy (skala pięciostopniowa). Metodyka wykorzystuje dedykowane oprogramowanie, będące jej integralnym elementem wspierającym wymienione etapy.

7. Zakończenie

Korzyści wynikające z odpowiedniego przeprowadzenia procesu analizy ryzyka, a szczególnie jego oceny, są wielopłaszczyznowe, gdyż mogą pomóc w utrzymaniu równowagi między stratami a kosztami zaimplementowanych zabezpieczeń, pomagają w planowaniu wydatków, wskazują zasadność lub brak podstaw do dodatkowych inwestycji w bezpieczeństwo IT, wskazują także na najważniejsze trendy w obszarze bezpieczeństwa systemów informatycznych. Praktycy twierdzą, że sukces w szacowaniu strat osiąga się poprzez systematyczne i rzetelne podejście do zagadnienia, np. poprzez wykonanie m.in. audytów wewnętrznych. Jednakże w praktyce, a zwłaszcza w sektorze małych i średnich przedsiębiorstw, obecnie rzadko przeprowadza się rzetelnie proces szacowania potencjalnych strat, na co prawdopodobnie ma wpływ wiele czynników, takich jak m.in. brak wiedzy, brak chęci i brak wymagań ze strony kierownictwa tych firm. Ponadto bardzo często nie bierze się w ogóle pod uwagę ilościowych metod oceny ryzyka, koncentrując się jedynie na nielicznych, wybranych metodach jakościowych. Jest to z pewnością spowodowane dużą trudnością przeprowadzenia tego procesu i doboru odpowiednich metod pomiaru. Dlatego też w publikacjach z omawianego zakresu prezentuje się najczęściej proste metody jakościowe, również m.in. te wskazane w artykule, gdzie oszacowanie wartości ryzyka IT wiąże się jedynie z opisem jakościowym, określeniem skal jakościowych dla częstotliwości wystąpienia zagrożenia lub opisem tzw. scenariuszy zagrożeń. Omówione w artykule metody, zarówno o charakterze ilościowym, jak i jakościowym, mogą stanowić cenne narzędzie w zakresie analizy ryzyka IT w małych i średnich przedsiębiorstwach.

Literatura

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

Certus Risk Aalyzer Professional, Witryna internetowa Centrum Doskonalenia Zarządzania MERITUM: http://centrum-doskonalenia.pl/show.php?component=Text&op=ShowText&id=60.

ISACA – Information Systems Audit and Control Association – *Standard 050.050.030 – IS Auditing Guideline – Use of Risk Assessment in Audit Planning*, ISACA, 2000.

ISO/IEC TR 13335-1 *Information Technology – Security techniques – Guidelines for the management of IT security – Part 1: Concepts and models of IT security.*

ISO/IEC TR 13335-3 *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT security.*

Kaczmarek T.T., *Zarządzanie zdywersyfikowanym ryzykiem w świetle badań interdyscyplinarnych*, Wydawnictwo Wyższej Szkoły Zarządzania i Marketingu, Warszawa 2003.

Karabacak B., Sogukpinar I., *Information security risk analysis method*, "Computers&Security Magazine" 2005 no. 24 (marzec).

Liderman K., *Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki WAT" 2001 nr 16.

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

Polska Norma PN-I-02000 – *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia,* Polski Komitet Normalizacyjny, 1998.

Polska Norma PN-I-13335 – *Zarządzanie zabezpieczeniami systemów informatycznych*, Polski Komitet Normalizacyjny, 1999.

Ryba M., *Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M*, rozprawa doktorska, 2006.

Schechter E., *Computer security strength & risk: a quantitative approach*, Harvard University, Cambridge, Massachusetts, USA 2004.

Składki i ryzyko ubezpieczeniowe. Modelowanie stochastyczne, red. W. Ostasiewicz, AE, Wrocław 2004.

Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, Cz. 1. *Wybór podejścia do analizy,* „Monitor Rachunkowości i Finansów" 2006 nr 6.

Szczepankiewicz E.I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, Cz. 2. *Etap oszacowania ryzyka*, „Monitor Rachunkowości i Finansów" 2006 nr 7.

Wawrzyniak D., *Modele oceny ryzyka informatycznego – podejścia klasyczne i możliwości ich rozwoju*, [w:] *Wybrane problemy elektronicznej gospodarki*, red. M. Niedźwiedziński, Wyd. Marian Niedźwiedziński – CONSULTING, Łódź 2007.

QUANTITATIVE AND QUALITATIVE APPROACH IN IT RISK ANALYSIS IN SMALL AND MEDIUM ENTERPRISES

Summary: The risk connected with the wide application of information technologies in business grows together with the increase of organization's correlation from its customers, business partners and outsourced operations. IT risk management currently plays more and more important role in almost all aspects of contemporary organizations' functionality. It requires

reliable and cyclical realization of its key task which is risk analysis. Literature of subject presents problems of risk analysis in different way, most often skipping or selectively treating the problem of quantitative methods application for the purpose of risk analysis. Quantitative and qualitative methods which are two fundamental groups of methods are applied for the analysis of risk on which assets are exposed in organizations. The article presents the issue of one of the most significant stages of risk analysis which is assessment of IT risk, especially focusing on chosen quantitative methods such as ALE (Annual Loss Expected) method, Courtney method, Fisher's method, using survey research ISRAM model (Information Security Risk Analysis Method) and other derived ratios. There are also briefly presented chosen qualitative methods – FMEA (Failure Mode and Effects Analysis) and FMECA (Failure Mode and Effects Criticality Analysis), FRAP (Facilitated Risk Analysis Process), NIST SP 800-30 method and CRAMM methodology, which can be applied in the small and medium enterprises.