INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 4(30) · 2013

ISSN 1507-3858

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu
e-mail: artur.rot@ue.wroc.pl

EFEKTYWNOŚĆ EKONOMICZNA W ANALIZIE RYZYKA NA POTRZEBY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Streszczenie: Zarządzanie ryzykiem to proces ograniczania ryzyka poprzez stosowanie odpowiednich środków bezpieczeństwa. Efektywne zarządzanie ryzykiem w organizacji wymaga systemowego podejścia do analizy ryzyka. Na podstawie jej wyników dobiera się zabezpieczenia, które powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagania biznesowe i wynikające z przeprowadzonej analizy ryzyka zasobów mających wartość dla funkcjonowania organizacji. Efektywność ekonomiczną w tym przypadku można określić jako dążenie do minimalizacji całkowitych kosztów związanych z zarządzaniem ryzykiem. Artykuł przedstawia wybrane modele, metody i wskaźniki mogące znaleźć zastosowanie w ocenie efektywności inwestycji w obszarze bezpieczeństwa systemów informatycznych.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, analiza ryzyka, zarządzanie ryzykiem, efektywność ekonomiczna.

1. Wstęp

Zarządzanie ryzykiem jest powiązane z wieloma czynnikami, a jednym z istotniejszych jest aspekt finansowy. Literatura przedmiotu często nie zauważa problematyki kwestii ekonomicznych tego procesu, a przecież zarządzanie ryzykiem jest ciągłym procesem związanym z permanentnymi wydatkami. Dotyczą one m.in. działań, których finansowanie należy uwzględnić podczas procesu analizy ryzyka; są nimi:

- przeprowadzanie analizy ryzyka,
- planowanie i projektowanie zasad, procedur i adekwatnych zabezpieczeń,
- zakup sprzętu (technicznych i fizycznych mechanizmów zabezpieczających),
- zakup programowych implementacji mechanizmów bezpieczeństwa,
- wdrażanie zasad i procedur bezpieczeństwa,
- monitorowanie, audyt, ocena wdrożenia i eksploatacji zabezpieczeń,
- dodatkowa praca specjalistów,

- opracowanie i wdrożenie programu szkoleniowo-uświadamiającego,
- zatrudnienie dodatkowych pracowników działu bezpieczeństwa,
- koszty organizacyjne wydatkowane na nowe struktury i zarządzanie,
- ciągłe doskonalenie poziomu zabezpieczeń itp.

Analiza ryzyka jest punktem wyjścia do kolejnych etapów procesu zarządzania ryzykiem, pozwalających na zrównoważenie operacyjnych i ekonomicznych kosztów środków ochrony z uzyskanym wynikiem w dążeniu do skuteczności.

Celem niniejszego artykułu jest przedstawienie modeli efektywności inwestycji redukujących ryzyko w organizacji, które powinny zostać uwzględnione w procesie analizy ryzyka, jak również analiza zależności pomiędzy poniesionymi wydatkami a osiągniętym poziomem bezpieczeństwa.

2. Analiza ryzyka informatycznego jako element procesu zarządzania ryzykiem

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, finansami, prawem, matematyką, ze statystyką, z rachunkowością i wieloma innymi. Ryzyko i niepewność nieodłącznie towarzyszą podejmowaniu decyzji gospodarczych. Ponieważ nie można całkowicie uniknąć ryzyka, należy poznać rządzące nim mechanizmy i nauczyć się nim zarządzać.

Szczególnym rodzajem ryzyka, którego dotyczą rozważania podejmowane w niniejszym artykule, jest ryzyko systemów informatycznych (SI), określane często w literaturze jako ryzyko informatyczne. Termin ten nie jest definiowany w sposób jednoznaczny, słowo „ryzyko" ma bowiem wiele znaczeń. W większości z nich jest jednak związane z pojęciem „straty", co pozostaje w zgodzie 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, w której jest rozpatrywana możliwość wykorzystania podatności przez zagrożenie w celu spowodowania niekorzystnych następstw dla instytucji [Białas 2006, s. 75]. W kontekście bezpieczeństwa SI ryzyko 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. Jedną z najprostszych, a jednocześnie najlepiej oddającą istotę ryzyka SI jest definicja sformułowana przez stowarzyszenie ISACA (Information Systems Audit and Control Association), stanowiąca, że: „Ryzyko jest możliwością wystąpienia zdarzenia, które będzie miało niepożądany wpływ na organizację i jej systemy informatyczne" [ISACA – Standard 050.050.030…].

Jest wiele innych standardów próbujących regulować tę problematykę. I tak np. standard ISO/IEC TR 13335 zawiera pewne wskazówki, od czego zależy wielkość

ryzyka związana z funkcjonowaniem systemów informatycznych: „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" [ISO/IEC TR 13335-1…; Liderman 2008, s. 70].

Zarządzanie ryzykiem informatycznym odgrywa obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji; polega ono głównie na identyfikacji zagrożeń i podatności, szacowaniu ryzyka oraz wyborze określonych środków bezpieczeństwa. Jego najważniejszym elementem jest analiza ryzyka (*risk analysis*). Termin ten jest bardzo często używany w literaturze przedmiotu, przy czym różni autorzy podają odmienny zakres przedsięwzięć składających się na proces analizy ryzyka. Analiza ryzyka polega na ocenie wszystkich negatywnych skutków badanego przedsięwzięcia i odpowiadających im prawdopodobieństw (częstości występowania). K. Liderman podaje najbardziej ogólną definicję analizy ryzyka na potrzeby bezpieczeństwa SI, formułując ją następująco: „Analiza ryzyka (…) jest procesem identyfikacji (jakościowej i ilościowej) ryzyka utraty bezpieczeństwa teleinformatycznego" [Liderman 2001].

Analiza ryzyka jest głównym procesem zarządzania ryzykiem; identyfikuje i ocenia ryzyko, które ma być kontrolowane lub akceptowane. Obejmuje ona także ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, autentyczności i niezawodności zasobów systemu informatycznego. Podstawowym jej celem jest dostarczenie informacji niezbędnej w podejmowaniu decyzji o zastosowaniu określonych metod, środków, narzędzi bezpieczeństwa.

3. Efektywność ekonomiczna inwestycji redukujących ryzyko w organizacji

Ryzyko jest wartością, którą organizacja musi uwzględnić w swojej działalności, a zatem w ramach analizy ryzyka powinna ona porównać ryzyko ze swoimi możliwościami pokrycia ewentualnych strat, gdy straty takie powstaną. Wielkość kosztów, jakie instytucja może ponieść w sytuacji naruszenia bezpieczeństwa, określona jest przez maksymalne dopuszczalne ryzyko (MDR). Jest to wielkość funduszy własnych, z jakich stratą liczy się organizacja w razie niekorzystnych zdarzeń, wraz z częścią zysków operacyjnych (*cash flow*), które także mogą pomóc we wchłonięciu ryzyka, a także gwarancje, zwłaszcza o charakterze odszkodowań, obejmujące dany typ zdarzeń, zatem [*Biała Księga* 1995]:

$$MDR = \alpha FW + \beta Zysk + \gamma Gwarancje, \tag{1}$$

gdzie: α – część funduszy własnych (np. 20% ustalone jako maksymalny limit strat w przypadku katastrofy),

β – część rocznego zysku operacyjnego brutto, pozwalającego na wchłonięcie skutków katastrofy,

γ – szacunkowy wskaźnik odszkodowań (przy zbadaniu prawdopodobieństwa ich otrzymania) jako ewentualnej rekompensaty pieniężnej (bądź technicznej) w przypadku szkód powstałych w systemie informatycznym.

Zarządzanie ryzykiem to proces ograniczania ryzyka do rozmiarów mniejszych od MDR przez stosowanie środków bezpieczeństwa. Efektywne zarządzanie ryzykiem w organizacji wymaga systemowego podejścia do analizy ryzyka. Na podstawie jej wyników dobiera się zabezpieczenia, które powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagania biznesowe i wynikające z przeprowadzonej analizy ryzyka zasobów mających wartość dla funkcjonowania organizacji. Całkowity koszt związany z tym ryzykiem musi zawierać składowe opisane następującym wzorem [Szczepankiewicz 2006]:

$$K_c = K_r + K_b + K_z, \tag{2}$$

gdzie: K_c – koszt całkowity w zakresie ryzyka bezpieczeństwa SI w przyjętym okresie,

K_r – straty związane z ryzykiem bezpieczeństwa SI w przyjętym okresie po zastosowaniu przewidzianych środków redukcji lub transferu ryzyka,

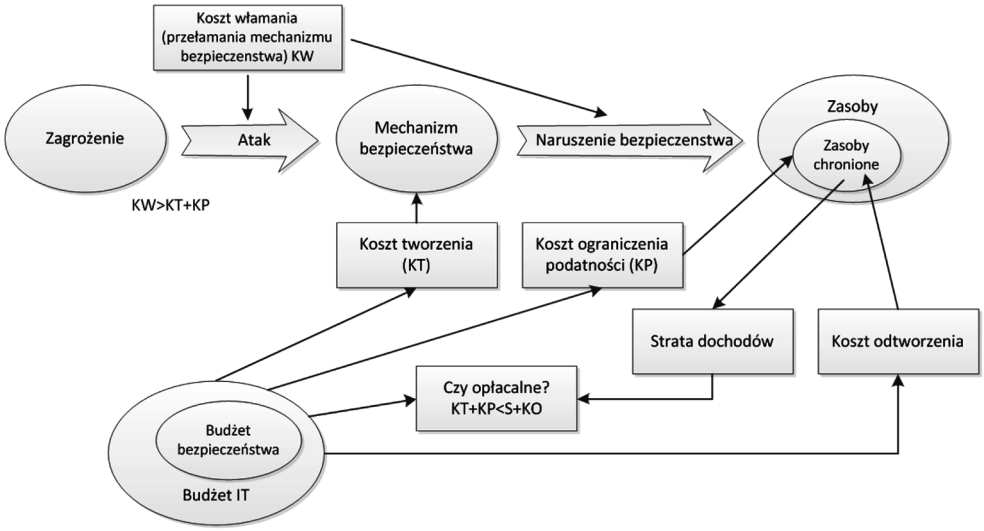
K_b – koszty wdrożenia i eksploatacji środków redukcji lub transferu ryzyka,

K_z – koszty związane z procesem zarządzania ryzykiem, w tym związane: z gromadzeniem danych, z analizą ryzyka, ze wsparciem informatycznym, z usługami konsultantów zewnętrznych, przygotowaniem decyzji, kontrolą.

Analizując wzór (2), można zauważyć, że zasadniczym celem efektywnego ekonomicznie procesu analizy ryzyka nie jest minimalizacja strat związanych z ryzykiem, ale minimalizacja łącznych kosztów obejmujących: potencjalne straty, koszty zabezpieczeń oraz koszty związane z procesem zarządzania.

W literaturze pojawiają się modele efektywności inwestycji redukujących ryzyko w organizacji, które powinny znaleźć zastosowanie w procesie analizy ryzyka. Jednym z nich jest model rentowności wydatków związanych z bezpieczeństwem SI. Jego ideę zobrazowano na rys. 1.

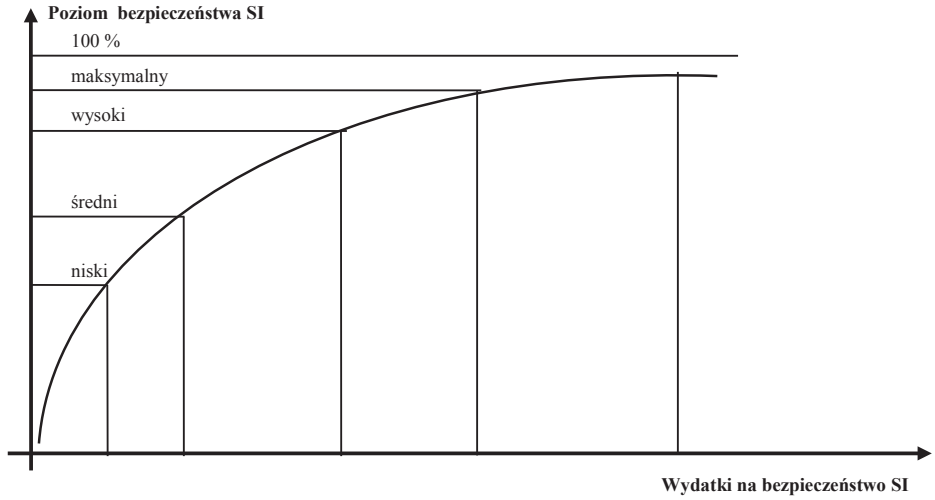
Zabezpieczenia muszą być adekwatne względem wartości dóbr chronionych, zagrożeń SI i gotowości do podjęcia ryzyka. Finanse przeznaczone na zarządzanie ryzykiem muszą być zawsze porównywane z otrzymywanymi z tego tytułu korzyściami. Koszty redukcji i transferu ryzyka, w postaci zastosowania dodatkowych środków ochrony, ubezpieczenia od ryzyka, outsourcingu itp., są ekonomicznie uzasadnione tylko wtedy, gdy zmniejszenie strat będzie istotnie mniejsze w porównaniu z kosztem ich wdrożenia i utrzymania. Zwiększanie zabezpieczeń wiąże się, oczy-



Rys. 1. Model rentowności wydatków związanych z zarządzaniem ryzykiem

Źródło: [Mizzi 2011].

wiście, ze zwiększonymi kosztami ich wprowadzenia, utrzymania i kontrolowania (rys. 2). Zaprezentowana na rys. 2 krzywa redukcji ryzyka obrazuje umowny poziom bezpieczeństwa w zależności od poniesionych nakładów.

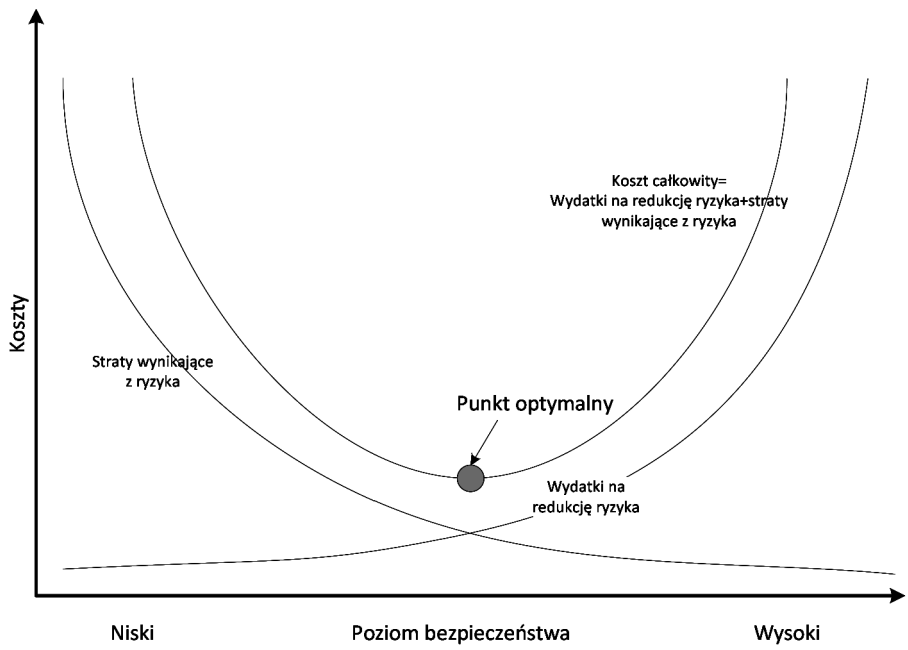


Rys. 2. Krzywa redukcji ryzyka – związek między poziomem bezpieczeństwa SI a poniesionymi wydatkami

Źródło: opracowanie własne na podstawie [*Biała Księga* 1995].

Jak wynika z przedstawionego wykresu, osiągnięcie 100-procentowego bezpieczeństwa nie jest w praktyce możliwe (teoretycznie, aby osiągnąć taki stan, należałoby mieć na ten cel nieograniczone środki). Doskonalenie systemu bezpieczeństwa, gdy mamy względnie wysoki poziom zabezpieczeń (np. wysoki), jest już relatywnie bardziej kosztowne i przeznaczone na ten cel środki finansowe nie dają takich efektów, jak w początkowym stadium.

W pracy autorstwa L.A. Gordona i M.P. Loeba [Gordon, Loeb 2002, s. 438--457] przedstawiono propozycję modelu optymalnych wydatków na zarządzanie ryzykiem. Zgodnie z nim (rys. 3) optymalny poziom wydatków jest osiągany, gdy łączny koszt zabezpieczeń i przewidywanych strat (mogących wystąpić w przypadku niezastosowania określonych zabezpieczeń) zostaje zminimalizowany. Zarówno z tego, jak i z poprzedniego wykresu wynika, że wydatki na zarządzanie ryzykiem są opłacalne do pewnego poziomu, określonego jako optymalny. Dalsze inwestycje są mniej racjonalne, gdyż nie mają już tak zasadniczego wpływu na zwiększenie poziomu bezpieczeństwa. Natomiast w początkowym stadium redukcji ryzyka największe efekty uzyskuje się przy względnie niewielkich nakładach przeznaczonych na środki bezpieczeństwa i przy zastosowaniu w miarę uproszczonych metod analizy ryzyka.



Rys. 3. Model optymalnych wydatków na zarządzanie ryzykiem

Źródło: [Dynes, Brechbühl, Johnson 2005].

Zasadniczym celem zarządzania ryzykiem będzie zatem osiągnięcie optymalnego poziomu bezpieczeństwa przy możliwie jak najmniejszym koszcie całkowitym (K_c) w zakresie ryzyka bezpieczeństwa SI w przyjętym okresie. W analizie ryzyka, podczas ustalania wydatków na określone mechanizmy, należy się kierować następującymi zasadami:

- nie przeznaczać dużych sum na zabezpieczanie zasobów małej wartości,
- nie przeznaczać wielkich wydatków na zabezpieczenie informacji, których ujawnienie będzie nieszkodliwe,
- przeznaczyć większą część środków na zabezpieczenie zasobów cennych dla konkurencji/otoczenia oraz takich, które w razie ujawnienia mogłyby przynieść wielką szkodę tym, których one dotyczą.

Zabezpieczanie wszystkiego i wszędzie nie jest działaniem racjonalnym i może w efekcie doprowadzić do nadmiernych kosztów i sparaliżować funkcjonowanie organizacji, nadmiar środków ochrony zmniejsza efektywność działania systemów informatycznych, a także często zwiększa koszty ich administrowania. Całkowita otwartość informacyjna jest niebezpieczna, lecz ograniczenia nakładane na przepływy informacji mogą utrudniać innowacyjność, zniechęcać klientów, uniemożliwiać rozpoznawanie nowych potrzeb rynku. Również bezwzględne egzekwowanie rygorystycznych procedur bezpieczeństwa przynosi w praktyce więcej szkody niż pożytku. W związku z tym w analizie ryzyka, przy formułowaniu założeń dotyczących bezpieczeństwa, trzeba mieć na względzie, że firmy muszą być nakierowane na klienta i otwarte na partnerów biznesowych.

W odniesieniu do ryzyka związanego z bezpieczeństwem SI przy szukaniu optymalnego rozwiązania, podobnie w wielu innych dziedzinach życia, warto pamiętać o regule Pareto 80/20. W literaturze przedmiotu proponuje się stosować ją również do zarządzania ryzykiem bezpieczeństwa SI [Kabay 2003; Partida, Andina 2010, s. 18]. W tym przypadku reguła ta wyrażałaby się następującymi zależnościami [Scott 2010]:

- 20% wszystkich czynników ryzyka powoduje 80% incydentów w obszarze bezpieczeństwa SI (należy zidentyfikować, jakie to czynniki ryzyka),
- wdrożenie 20% środków bezpieczeństwa o najwyższym priorytecie znacznie wpłynie na redukcję ryzyka w organizacji, eliminując 80% zagrożeń (należy zidentyfikować, jakie są to środki; często należą do nich najprostsze i najtańsze rozwiązania, np. szkolenia, działania uświadamiające użytkowników systemów, instrukcje, efektywne zastosowanie już wdrożonych rozwiązań zabezpieczających itp.).

W literaturze przedmiotu można odnaleźć różne narzędzia ilościowe, których celem jest ocena efektywności inwestycji w omawianym obszarze. Mogą się one okazać cennym narzędziem w procesie analizy ryzyka przy określaniu wydatków i poziomu inwestycji na bezpieczeństwo SI w organizacji.

Ciekawą propozycją odnoszącą się do zaprezentowanego optymalnego modelu autorstwa L.A. Gordona i M. P. Loeba jest koncepcja, którą opracowali C.D. Huang,

Q. Hu i R.S. Behara [Huang, Hu, Behara 2008, s. 793-800]. Według niej po ustaleniu budżetu i innych ograniczeń dotyczących budżetu inwestycji w ramach procesu analizy ryzyka organizacja musi podjąć decyzję, w które zabezpieczenia inwestować. Wybór opiera się często na analizie korzyści i kosztów i analizie finansowej bazującej na takich wskaźnikach, jak ROI, NPV, IRR (bardziej szczegółowo przedstawionych w dalszej części artykułu) [Gordon, Loeb 2002].

Według modelu zaproponowanego przez Huanga prawdopodobieństwo naruszenia bezpieczeństwa jest opisane następującą funkcją [Huang 2008]:

$$p = p(t, v, S), \text{ gdzie } 0 \le p \le 1, \tag{3}$$

$$p(t, v, 0) = tv, \tag{4}$$

gdzie: p – prawdopodobieństwo naruszenia bezpieczeństwa zasobu systemu jest funkcją wystąpienia zagrożenia (t), podatności zasobu (v) oraz nakładów finansowych przeznaczonych na zabezpieczenie zasobu (S).

Model ten, podobnie jak model autorstwa L.A. Gordona i M.P. Loeba, zakłada, że prawdopodobieństwo realizacji zagrożenia zmniejsza się wraz ze wzrostem wydatków na środki bezpieczeństwa, a krańcowy wzrost poziomu bezpieczeństwa zmniejsza się ze wzrostem rozchodów [Wawrzyniak, Gospodarowicz 2009, s. 67-68]:

$$\frac{\delta p}{\delta S} \le 0, \tag{5}$$

$$\frac{\delta^2 p}{\delta S^2} \ge 0. \tag{6}$$

Ryzyko bezpieczeństwa, przed jakim stoi organizacja (R), może być zapisane jako:

$$R = p \cdot L, \tag{7}$$

gdzie L określa potencjalne straty związane z incydentem.

Biorąc pod uwagę, iż $p(t, v, 0) = tv$, ryzyko bezpieczeństwa przy braku inwestycji ze strony organizacji w mechanizmy bezpieczeństwa można opisać jako: $R = tvL$.

Jeśli organizacja wdraża określone systemy bezpieczeństwa, redukcja ryzyka może zostać opisana wzorem $\Delta R = (tv - p)L$. Zatem korzyść wynikającą z wdrożenia określonych mechanizmów bezpieczeństwa można opisać następującą zależnością:

$$\prod(S, t, v) = (tv - p)L - S. \tag{8}$$

Zależności te podczas procesu analizy ryzyka ułatwiają określenie optymalnych środków finansowych przeznaczonych na dobór mechanizmów bezpieczeństwa.

W literaturze pojawiają się także inne metody wyboru optymalnych inwestycji minimalizujących ryzyko; wśród nich wyróżnić można metodę AHP (*Analytic Hierarchical Process*). Jest ona jedną z wielokryterialnych metod hierarchicznej analizy problemów decyzyjnych, umożliwiającą dekompozycję złożonego problemu decyzyjnego oraz utworzenie rankingu finalnego dla skończonego zbioru wariantów.

Wskaźnikiem, który szybko zyskuje na popularności, jest wskaźnik umożliwiający określenie zwrotu z inwestycji w bezpieczeństwo – ROI (*Return on Investment*). Jest on syntetycznym wskaźnikiem efektywności wszelkich projektów, w tym również informatycznych. Można go stosować również w odniesieniu do inwestycji w bezpieczeństwo SI. W najprostszym ekonomicznym ujęciu zwrot z inwestycji jest różnicą między korzyściami będącymi skutkiem inwestycji a poniesionymi nakładami. Podkreślić należy, że w projektach informatycznych poszukiwanie ROI, wyrażonego w udokumentowanych wartościach, może być bardzo trudne. Dlatego też ROI w ujęciu ekonomicznym może się opierać na podstawowym podejściu rachunkowości zarządczej, w którym dopuszcza się w pomiarze miary naturalne i szacunki.

W procesach analizy ryzyka bardzo przydatny, prócz wskaźnika ROI, jest również model ROSI (*Return on Security Investment*), bazujący na wspomnianym już wskaźniku ROI, który jest definiowany jako [Wei i in. 2001]:

$$ROSI = \frac{ALE_0 - ALE_1}{k}, \tag{9}$$

gdzie: ALE_0 – *ALE* (opisany wcześniej wskaźnik, *Annual Loss Expected*) przed zastosowaniem zabezpieczeń,
ALE_1 – *ALE* po zastosowaniu mechanizmów bezpieczeństwa,
k – koszt wdrożonych mechanizmów bezpieczeństwa.

Wskaźnik *ALE* (zgodnie z wcześniejszymi wzorami zaprezentowanymi w pracy) obliczany jest według następującego wzoru:

$$ALE = \sum_{i=1}^{n} I(O_i)F_i, \tag{10}$$

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.

Model ten w literaturze przedmiotu jest czasem poddawany pewnym niewielkim modyfikacjom – m.in. w pracach autorstwa W. Sonnenreicha [Sonnenreich 2002] i A. Davisa [Davis 2006], a ma on następującą postać:

$$ROSI = \frac{(E \cdot S_m) - S_c}{S_c}, \tag{11}$$

gdzie: E – ryzyko przed wdrożeniem zabezpieczeń,
S_m – procent eliminacji ryzyka przez zabezpieczenie (90% = 10% ryzyka szczątkowego),
S_c – całkowity koszt inwestycji (zabezpieczeń).

Analizując tę metodę obliczeń, dostrzega się, że oszacowanie pewnych kosztów, takich jak: koszt odzyskania poniesionych strat, potencjalnych strat dochodu, koszt zaimplementowania nowego zabezpieczenia, utraty reputacji, mogą nastręczyć pewnych problemów. Obliczanie dodatkowych nakładów, takich jak: koszty pracy, koszt przestoju w pracy użytkowników, koszt wymiany sprzętu lub oprogramowania, jest względnie łatwe, dużo trudniej jednak obliczyć wszelkie wydatki uboczne związane z incydentem.

W analizie ryzyka wykorzystywać można również tradycyjne wskaźniki stosowane w naukach o finansach, takie jak metody analizy przepływów pieniężnych, oraz wewnętrzną stopę zwrotu [Wawrzyniak, Gospodarowicz 2009]. Zastosowanie znaleźć mogą dyskontowe metody rachunku ekonomicznego, z których najczęściej w praktyce wykorzystywane są: metoda wartości zaktualizowanej netto (*Net Present Value*, NPV) i metoda wewnętrznej stopy zwrotu (*Internal Rate of Return,* IRR).

Celem metody wartości zaktualizowanej netto jest wyznaczenie aktualnej wartości NPV wpływów i wydatków związanych z projektem (w naszym przypadku inwestycją związaną z redukcją ryzyka), przy założeniu stałej stopy dyskontowej (procentowej). Stopa ta powinna odpowiadać stopie zwrotu, jaką można uzyskać, gdyby kapitał został zainwestowany w najbardziej bezpieczne aktywa. Metoda ta pozwala określić rzeczywistą (aktualną) wartość nakładów i efektów związanych z danym przedsięwzięciem [Dudycz, Dyczkowski 2007, s. 91]. Definiuje się ją jako sumę zdyskontowanych oddzielnie dla każdego roku przepływów pieniężnych netto, zrealizowanych w całym okresie objętym rachunkiem, przy stałym poziomie stopy dyskontowej. Wielkość NPV obliczamy za pomocą wzoru [Flasiński 2007, s. 146]:

$$NPV = \sum_{t=0}^{n} NCF_t \cdot DF_t, \tag{12}$$

gdzie: n – kolejny rok n-letniego okresu obliczeniowego,
NCF_t – przepływy pieniężne netto w roku t, $t = 0, \ldots,$
DF_t – współczynnik dyskontowy w roku t, który dla stopy procentowej r wynosi:

$$DF_t = \frac{1}{(1+r)^t}. \tag{13}$$

Projekt (zatem także inwestycja w mechanizmy redukujące ryzyko) jest opłacalny, jeśli $NPV \geq 0$.

Metoda wewnętrznej stopy zwrotu (IRR) jest drugą powszechnie stosowaną metodą oceny opłacalności przedsięwzięć, obrazującą, jaka jest stopa rentowności badanych przedsięwzięć. Analizowany projekt będzie opłacalny, jeżeli jego wewnętrzna stopa zwrotu będzie wyższa od najniższej akceptowalnej stopy granicznej. Metoda ta przebiega w trzech zasadniczych etapach; są nimi:

- ustalenie wartości przepływów pieniężnych netto NCF_t dla kolejnych lat okresu obliczeniowego (podobnie jak w zaprezentowanej metodzie NPV),
- oszacowanie metodą kolejnych przybliżeń dwóch wielkości stopy procentowej i_i oraz i_2,
- obliczenie wskaźnika IRR za pomocą następującego wzoru [Flasiński 2007, s. 149]:

$$IRR = i_1 + \frac{PV \cdot (i_2 - i_1)}{PV + |NV|} \cdot \tag{14}$$

Jest możliwe, że analiza przedsięwzięcia przy zastosowaniu metody IRR i NPV da przeciwstawne rezultaty. W takiej sytuacji zalecane jest przyjęcie metody NPV jako tej bardziej wiarygodnej.

Zaprezentowane modele i metody mogą być przydatne jako forma wsparcia dla typowych metod (wspomaganych często komputerowo) analizy ryzyka. Sama analiza ryzyka, a przez to i ocena efektywności inwestycji w bezpieczeństwo, jest zadaniem bardzo trudnym, nie jest bowiem łatwe opisanie liczbowo czynników ryzyka, w szczególności w dynamicznie zmieniających się warunkach. Ponadto osoba, która dokonuje analizy ryzyka i oceny efektywności ekonomicznej inwestycji w bezpieczeństwo, nie dysponuje pełnymi informacjami o tym, co ma wpływ na jakość i trafność tej oceny. Decyzja o wyborze konkretnej metody zależy od specyfiki inwestycji, a przede wszystkim od zakresu posiadanych danych i informacji. Odpowiednią metodę należy tak dobrać, aby dostarczyć możliwie jak najwięcej rzetelnych informacji ułatwiających późniejsze procesy decyzyjne.

4. Zakończenie

Pomimo wielu różnych teoretycznych modeli i współczynników, których dostarcza literatura, a których celem jest wsparcie procesu analizy ryzyka w obszarze optymalizacji finansowania działań redukujących ryzyko, w praktyce korzysta się z nich, niestety, w bardzo ograniczonym wymiarze. Podstawową trudność stanowi bowiem identyfikacja rozkładów zmiennych losowych opisujących prawdopodobieństwo realizacji zagrożeń w obszarze bezpieczeństwa SI [Wawrzyniak, Gospodarowicz 2009, s. 68-69]. Zarówno w teorii, jak i w praktyce spotkać można inne modele i metody stosowane w ocenie efektywności inwestycji. Również one mogą stanowić uzupełnienie i wsparcie dla narzędzi typowych dla obszaru ryzyka bezpieczeństwa SI. Są to m.in.: zdyskontowany okres zwrotu (*Discounted Payback Period*, DPB),

wskaźnik zyskowności inwestycji (indeks rentowności, czyli *Profitability Index*, PI) oraz zmodyfikowana wewnętrzna stopa zwrotu (*Modified Internal Rate of Return*, MIRR). Wiele z tych modeli i wskaźników, stosowanych w tradycyjny sposób, nie uwzględniają specyfiki bezpieczeństwa SI, ale mogą one stanowić uzupełnienie i wsparcie innych metodologii ukierunkowanych na niniejszą problematykę.

Literatura

Biała Księga, tytuł oryginału: *Livre Blanc sur la sécurité des systèmesd'information des établissements de credit,* kierownik publikacji, J-LButsch, Sekretariat Generalny Komisji Bankowej (Secrètariatgènèral de la Commissionbancaire), 1995, za: F. Wołowski, *Zarządzanie ryzykiem związanym z systemami informacyjnymi, „*Problemy Jakości", październik 2004, s. 28.

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

Cremonini M., Martini P., *Evaluating Information Security Investments from Attackers Perspective: The Return-On-Attack (ROA)*, Proceedings of Fourth Workshop on the Economics of Information Security, University of Cambridge, 2005, http://infosecon.net/workshop/pdf/23.pdf [dostęp: 27.03.2012].

Davis A., *Return on security investment – proving it's worth it*, "Network Security" 2006, no. 11.

Dudycz H., Dyczkowski M., *Efektywność przedsięwzięć informatycznych. Podstawy metodyczne pomiaru i przykłady zastosowań,* Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wroclaw 2007, s. 91.

Dynes S., Brechbühl H., Johnson M.E., *Information Security in the Extended Enterprise: Some Initial Results From A Field Study of an Industrial Firm*, Glassmeyer/McNamee Center for Digital Strategies Tuck School of Business at Dartmout, 13.04.2005, http://www.tuck.dartmouth.edu/digital/assets/images/InfoSecurity%20(1).pdf [dostęp: 29.03.2012].

Flasiński M., *Zarządzanie projektami informatycznymi*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 146.

Gordon L.A., Loeb M.P., *Return on information security investments: Myths vs. realities*, "Strategic Finance" 2002, 84(5), s. 26-3.

Huang C.D., *Optimal Investment in Information Security: A Business Value Approach*, Proceedings of Pacific-Asia Conference on Information Systems, 2008, http://www.pacis-net.org/file/2010/S11-01.pdf [dostęp: 04.02.2012].

Huang C.D., Hu Q., Behara R.S., *Economics of information security investment in the case of simultaneous attacks*, "International Journal of Production Economics" 2008, 114 (2), s. 793-80.

ISACA – 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.*

IT Grundschutzhandbuch (IT Baseline Protection Manual), Bundesamt für Sicherheit in der Informationstechnik, Bonn, DIN-Berlin, 2000-2003.

Kabay M.E., *Information Security on a Budget: Where to Invest First*, Lecture delivered via Vermont Interactive Television to the Network World Deutschland Security Conference – 9 April 2003, http://www.mekabay.com/infosecmgmt/security_budget.pdf [dostęp: 23.03.2012].

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 SA, Warszawa 2008.

Mizzi A., *Return on Information Security Investment. Are You Spending Enough? Are You Spending Too Much?,* www.infosecwriters.com/text.../pdf/ROISI.pdf [dostęp: 8.12.2011].

Partida A., Andina D., *IT Security Management: IT Securiteers – Setting up an IT Security Function*, Springer, 2010, s. 18.

Scott C., *Applying the Pareto Principle to Information Security Management*, SANS Institute, 18.03.2010, http://www.sans.edu/research/leadership-laboratory/article/mgt421-scott-pareto [dostęp: 26.03.2012].

Sonnenreich W., *Return on Security Investment (ROSI): A Practical Quantitative Model*, A Summary Of Research And Development Conducted at SageSecure, 2002.

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

Wawrzyniak D., *Zarządzanie ryzykiem informatycznym – wybrane aspekty ekonomiczne,* [w:] *Wybrane problemy budowy aplikacji dla gospodarki elektronicznej*, red. M. Niedźwiedziński, K. Lange-Sadzińska, Wydawnictwo Marian Niedźwiedziński – CONSULTING, Łódź 2009, s. 107.

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

Wei H., Frinke D., Carter O., Ritter C., *Cost-Benefit Analysis for Network Intrusion Detection Systems*, Proceedings of the 28-th Annual Computer Security Conference, Cupertino 2001.

ECONOMIC EFFICIENCY IN INFORMATION SYSTEMS SECURITY RISK ANALYSIS

Summary: IS/IT Risk management is the process of risk reduction through the appropriate security measures. Effective risk management in an organization requires a composite approach to risk analysis. Based on the risk analysis results, the author selected the safeguards which should be cost-effective and take into account law requirements, business needs and requirements resulting from the risk analysis. Economic efficiency, in this case, can be described as an attempt to minimize the total cost of the information system security risks management. The paper presents selected models, methods and indicators that can be used in achieving the effectiveness of investment in information systems security.

Keywords: IS/IT security, risk analysis, IT/IS risk management, economic efficiency.