PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 118
Informatyka Ekonomiczna 17 2010

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

ZARZĄDZANIE RYZYKIEM NA POTRZEBY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH – STRATEGIE POSTĘPOWANIA Z RYZYKIEM

Streszczenie: Zarządzanie ryzykiem informatycznym jest dyscypliną integrującą wiele różnorodnych technologii służących identyfikacji, analizie, ocenie incydentów i zagrożeń, a także wdrażaniu środków zwiększających bezpieczeństwo. Odgrywa ono obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji. Jednym z istotnych elementów tego złożonego procesu jest wybór strategii postępowania z ryzykiem. Artykuł zawiera omówienie tematyki zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji ze szczególnym uwzględnieniem możliwych reakcji na zidentyfikowane ryzyko w tym obszarze.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, zarządzanie ryzykiem, strategie postępowania z ryzykiem.

1. Wstęp

Ryzyko związane z szerokim zastosowaniem technologii informatycznych w biznesie rośnie w miarę zwiększania się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Obecny postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i liczby czynników ryzyka. Brak odpowiedniego przygotowania na ryzyko może prowadzić przedsiębiorstwo do bankructwa, stąd też właściwe reagowanie na nie stanowi o możliwościach przetrwania i rozwoju organizacji. W tym kontekście bardzo istotnym procesem jest odpowiednia reakcja na ryzyko. Literatura przedmiotu, a także normy, standardy i dobre praktyki w tym obszarze wśród możliwych reakcji na ryzyko wymieniają unikanie ryzyka, jego kontrolowanie, transfer ryzyka oraz retencję (zatrzymanie) ryzyka. Celem niniejszego artykułu jest wprowadzenie do problematyki zarządzania ryzkiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji ze szczególnym uwzględnieniem strategii postępowania ze zidentyfikowanym ryzykiem.

2. Etymologia i analiza pojęcia ryzyka

Ryzyko towarzyszy człowiekowi i jego działalności od początku dziejów. Od najdawniejszych czasów głównym źródłem ryzyka dla człowieka były żywioły przyrody, takie jak trzęsienia ziemi, powodzie, nawałnice, huragany, nieprzewidywalne oraz ponadprzeciętne upały i susze, jak również mrozy. Drugim zasadniczym źródłem ryzyka towarzyszącym człowiekowi jest aktywność ludzi. W wyniku rozwoju cywilizacji, kultury, nauki, organizacji, techniki, gospodarki i innych dziedzin powstają nowe obszary działalności człowieka, które stale generują nowe rodzaje ryzyka [Ronka-Chmielowiec 2004, s. 11]. Do przyspieszenia tempa zmian przyczynia się głównie postęp technologiczny. Ma on skokowy charakter, a zależności, które generuje, wywołują wzrost różnorodności, złożoności, nieokreśloności oraz liczby czynników 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. 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* oznacza omijać coś. Greckie *riza*, podobnie jak włoskie *ris(i)co* (lub *rischio*), oznacza rafę, którą statek powinien ominąć, a więc niebezpieczeństwo, którego powinien uniknąć [Kaczmarek 2003, s. 11-12]. P.L. Bernstein twierdzi, iż słowo „ryzyko" pochodzi od starowłoskiego *riscare* oznaczającego tyle, co odważyć się [Bernstein 1997]. W tym sensie ryzyko jest wyborem, a nie nieuchronnym przeznaczeniem. W języku angielskim *risk* oznacza sytuację powodującą niebezpieczeństwo lub możliwość, że zdarzy się coś złego. Ponadto w języku angielskim bliskie pojęciu ryzyka jest słowo *hazard*, które jest synonimem właśnie ryzyka, a także niebezpieczeństwa lub potencjalnego źródła niebezpieczeństwa, zagrożenia [Kaczmarek 20087, s. 51]. Najczęściej jednak w literaturze podaje się, że słowo „ryzyko" (ang. *risk*, fr. *risque*, niem. *risiko*) pochodzi od łacińskiego *risicum* oznaczającego szansę, prawdopodobieństwo wystąpienia zdarzenia pozytywnego lub negatywnego, sukcesu lub porażki [Nahotko 2001, s. 37-38].

Na temat pojęcia ryzyka i jego różnorodnych kwalifikacji napisano już wiele. Ryzyko jest mieszaniną wielu wciąż zmieniających się czynników, dlatego zarówno praktycy, jak i teoretycy nie podają jednej uniwersalnej definicji, stąd też istnieje ich wiele. W literaturze podkreśla się, iż jest to termin wieloznaczny i trudny do syntetycznego zdefiniowania. Jak pisze W. Ostasiewicz, 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 [Ostasiewicz 2004, s. 11].

Nauka o ryzyku jest praktycznie rozwijana w większości nauk i stosowana we wszystkich technologiach. Obecnie nie istnieje jeszcze jednolita teoria ryzyka. Ryzyko możemy rozpatrywać na wielu poziomach i niemalże we wszystkich dziedzinach działalności człowieka. W zależności od autora i charakteru opracowania czy też ze względu na różną perspektywę przedmiotową, branżową czy dyscyplinarną uzyskujemy różne sposoby ujmowania zagadnienia związanego z ryzykiem [Krupa 2002, s. 15].

Największe osiągnięcia w dziedzinie ryzyka ma nauka amerykańska (zob. m.in.: [Willet 1901; Knight 1921; Arrow 1979; Vaughan 1997; Williams, Heins 1989]). Początek naukowego zainteresowania ryzykiem wiążę się z opublikowaniem w 1901 r. przez A.H. Willeta pracy *The Economic Theory of Risk and Insurance* (*Ekonomiczna teoria ryzyka i ubezpieczeń*). Autor zdefiniował w niej ryzyko jako „zobiektywizowaną niepewność dotyczącą wystąpienia niepożądanego zdarzenia" [Willet 1901, s. 6]. Znaczny wpływ na myśl ekonomiczną i teorię ryzyka miały prace F.H. Knighta, pochodzące z lat 20. ubiegłego wieku, poruszające zagadnienia ryzyka. W roku 1921 F.H. Knight, uważany za klasyka teorii ryzyka i twórcę teorii mierzalnej i niemierzalnej, w pracy *Risk, Uncertainty and Profi*t stwierdził, że „ryzyko to niepewność mierzalna, a niepewność sensu stricte to niepewność niemierzalna" [Knight 1921]. Opracowane przez niego definicje ryzyka i niepewności są do dzisiaj powszechnie stosowane w badaniach i literaturze nauk ekonomicznych [Klimczak 2007]. Obecnie żaden ekonomista nie może w swoich analizach pomijać problemu ryzyka. Od czasu owych pierwszych prób włączenia ryzyka do teorii ekonomicznych nastąpił znaczny rozwój teorii ryzyka oraz zarządzania ryzykiem w organizacjach. Korzystając ze wzrastającej mocy obliczeniowej komputerów oraz powstawania nowych narzędzi matematycznych, ekonomiści przetwarzali coraz więcej informacji, aby określić miary ryzyka. Jednak droga od zastosowania ryzyka w wybranych obszarach analizy finansowej i wspomagania podejmowania decyzji do włączenia go w spójną teorię rynku okazała się bardzo trudna [Klimczak 2007].

3. Istota i kategorie ryzyka systemów informatycznych

Szczególnym rodzajem ryzyka, którego dotyczą rozważania podejmowane w niniejszym artykule, jest ryzyko systemów informatycznych, określane często w literaturze przedmiotu jako ryzyko informatyczne. Podobnie jak przy definicji samego ryzyka termin ten nie jest definiowany w sposób jednoznaczny. Jak wskazano w poprzednich podrozdziałach, słowo „ryzyko" ma wiele odcieni znaczeniowych. W większości z nich jednak jest związane z pojęciem straty, co jest zgodne również z intuicyjnym rozumieniem tego terminu. 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 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.

Dla potrzeb 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 [PN-I-02000 1998].

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].

Biorąc pod uwagę powyższe definicje, należy stwierdzić, że ryzyko systemów informatycznych rozpatrywane może być z punktu widzenia następujących kategorii [Ryba 2006, s. 13-14]:

- użyteczności (*relevance risk*) – w kategorii tej wyróżnia się ryzyko, iż zebrane informacje nie są wykorzystane lub okazują się nieprzydatne bądź także aktualność otrzymanej i opracowanej informacji jest niewystarczająca;
- integralności (*integrity risk*) – w kategorii tej wyróżnia się ryzyko, iż wykorzystywane dane i programy nie są wolne od błędów, nie zapewniają poprawności i kompletności informacji lub nie przedstawiają wiernie zdarzeń gospodarczych. Utrata integralności może być konsekwencją błędów w procesie przetwarzania informacji (także w wyniku awarii sprzętowych), zakłóceń, działania wirusów, błędów oprogramowania itp.;
- poufności (*confidentiality risk*) – w tej kategorii ryzyko dotyczy niedostępności treści zawartej w danych dla wszystkich podmiotów nieuprawnionych do jej odczytania. Danym, których ujawnienie byłoby kosztowne, przypisuje się odpowiednio wysoki poziom bezpieczeństwa (poufne, tajne itp.). Jednym ze sposobów zapewnienia poufności jest szyfrowanie danych. Utrata poufności może być skutkiem zarówno niewłaściwego zabezpieczenia informacji, jak i celowego ataku – włamania do systemu [Szmit 2003, s. 104];
- dostępności (*availability risk*) – ryzyko dotyczy ograniczenia możliwości korzystania z systemów i danych przez uprawnionych do tego użytkowników lub zachwiana zostaje zdolność systemów do przetwarzania danych na potrzeby kluczowych procesów w organizacji. Informacja powinna być zatem dostępna dla

osób upoważnionych, w określonym miejscu, czasie i postaci. Naruszenie dostępności może być efektem działań nieupoważnionego użytkownika, błędów popełnionych przez użytkownika systemu, a także wynikiem awarii, zakłóceń transmisji, błędów oprogramowania [Stokłosa, Bilski, Pankowski 2001, s. 18];

- adekwatności infrastruktury (*infrastructure risk*) – w kategorii tej wyróżnia się ryzyko, iż kluczowe procesy informatyczne (definiowanie i wdrożenie systemów w zakresie ich funkcjonalności, zapewnienie działania systemów i sieci, zarządzanie bazami danych, zarządzanie bezpieczeństwem informacji, procesy odtworzenia działalności na wypadek awarii itp.) nie zapewniają w sposób efektywny odpowiedniego wsparcia dla kluczowych potrzeb organizacji.

Wyżej wymienione kategorie ryzyka informatycznego są rozszerzeniem o elementy biznesowe (właściwości użyteczności i adekwatności infrastruktury) atrybutów bezpieczeństwa informacji zdefiniowanych w standardzie BS 7799 opracowanym przez BSI (Brytyjski Instytut Normalizacyjny). W roku 2000 te zalecenia brytyjskie opublikowane w *Code of Practice for Information Security Management* zostały poddane normalizacji przez ISO (Międzynarodowa Organizacja Normalizacyjna) oraz IEC (Międzynarodowa Komisja Elektrotechniczna). Wynikiem tych prac jest norma o nazwie „Praktyczne zasady zarządzania bezpieczeństwem informacji" (ISO/IEC 17799) (zob. [PN-ISO/IEC 17799:2007…]), obecnie stopniowo zastępowana przez normy z serii ISO/IEC 27000 (zob. [PN-ISO/IEC 27001:2007…]). Atrybuty bezpieczeństwa ujęte w tej normie to: poufność (*confidentiality*), integralność (*integrity*), dostępność (*availability*).

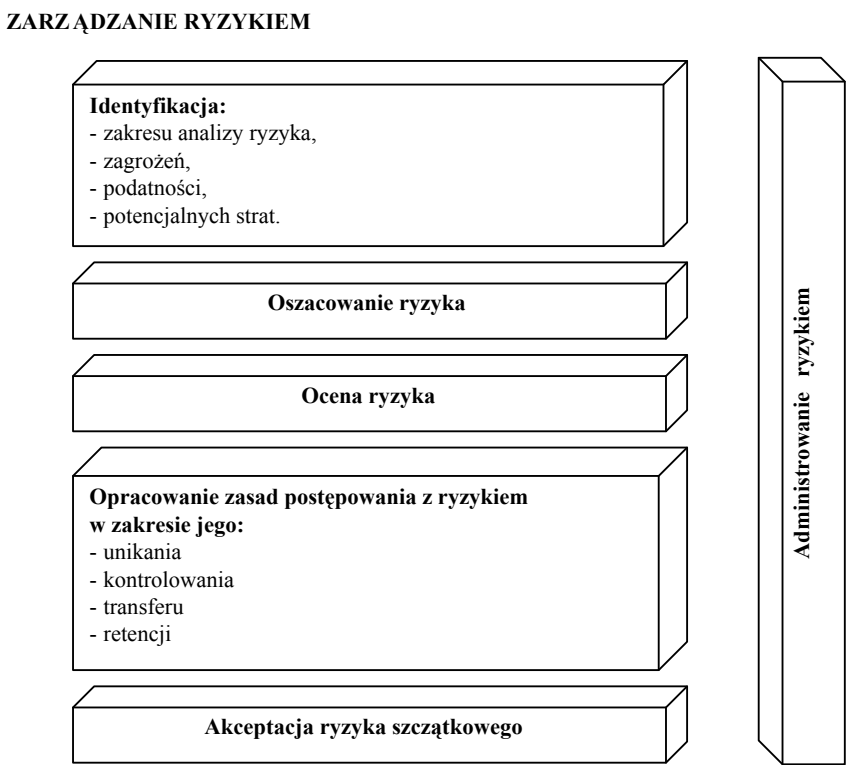
Nieco odmiennie termin ryzyka systemów informatycznych ujęto w normie ISO/IEC TR 13335-1, gdzie traktuje się je jako zbiorczą miarę prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu informacyjnego, a zatem pośrednią lub bezpośrednią szkodę dla instytucji [ISO/IEC TR 13335-1]. Definicja ta nawiązuje do terminu podatności (*vulnerability*), która według normy ISO/IEC TR 13335-3 obejmuje 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" [ISO/IEC TR 13335-1; Liderman 2008].

W praktyce, a szczególnie w instytucjach finansowych, stosowane jest często także pojęcie ryzyka operacyjnego. Jego definicja została przedstawiona w dokumencie konsultacyjnym Nowa bazylejska umowa kapitałowa, opracowanym w styczniu 2001 r. przez Bazylejski Komitet ds. Nadzoru Bankowego. Ryzyko operacyjne definiuje się jako „ryzyko straty wynikającej z niewłaściwych lub zawodnych procesów, ludzi i systemów lub ze zdarzeń zewnętrznych". Do rodzajów ryzyka operacyjnego,

które mogą wywoływać znaczne straty materialne, można zaliczyć wiele czynników, wśród których ważną rolę odgrywa ryzyko związane ze sferą funkcjonowania technologii informacyjnych, a szczególnie z brakiem ciągłości pracy instytucji, przerwaniem pracy systemów informatycznych, załamaniem ich pracy, co wynikać może z problemów ze sprzętem, z oprogramowaniem lub problemów telekomunikacyjnymi [Lewandowski 2004].

4. Proces zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych

Zarządzanie ryzykiem, zgodnie z definicjami ISO/IEC Guide 73:2005, to „skoordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka". Celem zarządzania ryzykiem nie jest więc całkowita likwidacja zagrożeń czy wyeliminowanie ryzyka, ale jego zmniejszenie do akceptowalnych rozmiarów (tzw. ryzyka szczątkowego) i ograniczenie następstwa potencjalnego zagrożenia do założonego z góry poziomu [Staniec, Zawiła-Niedźwiecki 2008, s. 204].



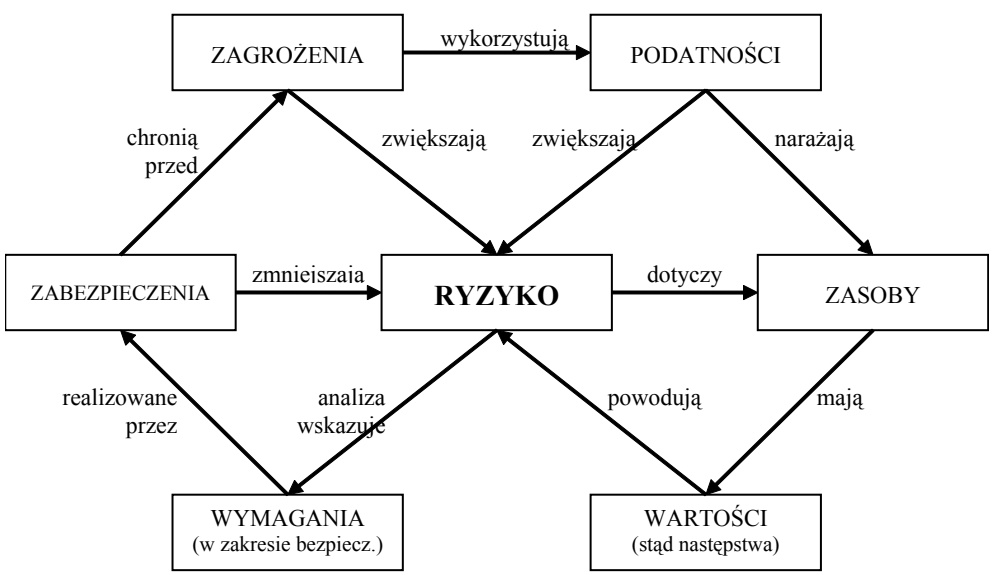
Rys. 1. Podstawowe elementy procesu zarządzania ryzykiem

Źródło: [Liderman 2006].

Ogólnie mówiąc, zarządzanie ryzykiem na potrzeby bezpieczeństwa systemów informatycznych jest procesem osiągania i utrzymania stanu równowagi między zidentyfikowanymi zagrożeniami a działaniami podjętymi w celu zabezpieczenia zasobów informatycznych. Odgrywa ono obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji, polega głównie na identyfikacji zagrożeń i podatności, szacowaniu ryzyka oraz wyborze określonych środków bezpieczeństwa. Zarządzanie ryzykiem to identyfikacja, mierzenie i kontrolowanie ryzyka w celu jego maksymalnego ograniczenia oraz zabezpieczenie przed skutkami ryzyka. Ogólny schemat tego procesu został przedstawiony na rys. 1.

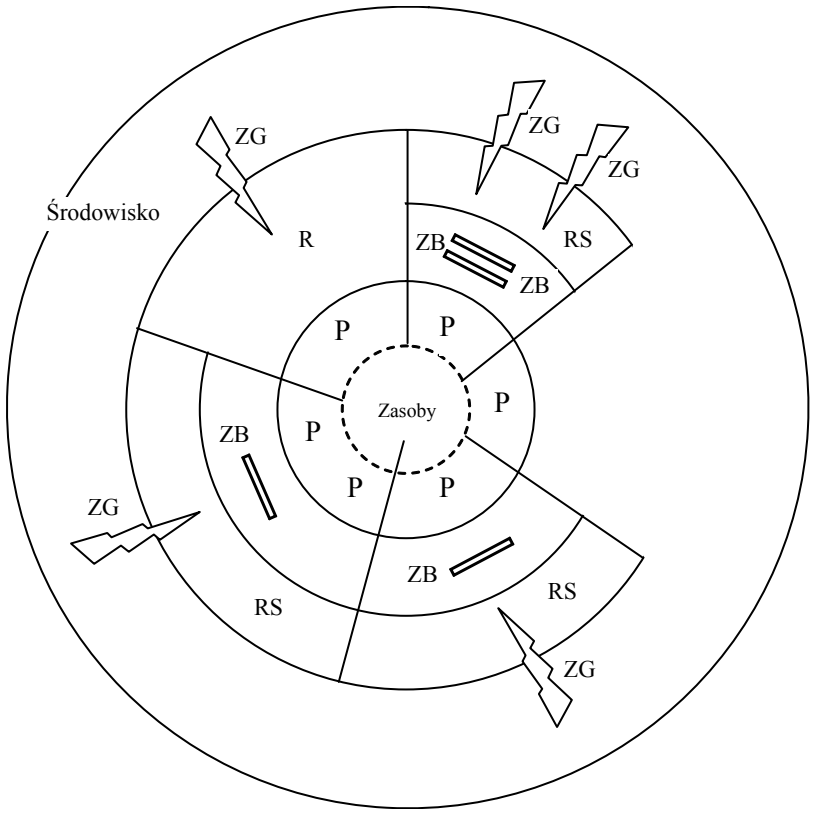
Zarządzanie ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji ma na celu [Liderman 2006]:

- wykazanie, których rodzajów ryzyka i jak można uniknąć, stosując rozwiązania organizacyjne i techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji w firmowych systemach IT,
- zapewnienie optymalnego, ze względu na koszty i znane/zadane ograniczenia, stanu ochrony informacji przetwarzanej w systemach informatycznych,
- zminimalizowanie ryzyka szczątkowego tak, aby stało sie ryzykiem akceptowalnym.



Rys. 2. Związki w zarządzaniu ryzykiem według normy ISO/IEC TR 13335-1

Źródło: opracowanie własne na podstawie [ISO/IEC TR 13335-1].



Legenda: R – ryzyko, RS – ryzyko szczątkowe, ZB – zabezpieczenie, ZG – zagrożenie, P – podatność.

Rys. 3. Ryzyko, zasoby, ryzyko szczątkowe, zagrożenia i podatności w ujęciu normy ISO/IEC TR 13335-1

Źródło: opracowanie własne na podstawie [ISO/IEC TR 13335-1].

Należy pamiętać o tym, że ryzyko możemy jedynie zmniejszyć, nigdy zlikwidować w całości. Ryzyko, które pomimo zastosowania różnorodnych fizycznych, sprzętowych, programowych, kryptograficznych i organizacyjnych środków zabezpieczeń, pozostanie w naszym systemie, określane jest jako ryzyko szczątkowe (*residual risk*).

Jak już podkreślono, zarządzanie ryzykiem na potrzeby bezpieczeństwa systemów informatycznych to proces identyfikacji zagrożeń dla systemu, podatności jego zasobów, szacowania ryzyka oraz rekomendowania dodatkowych środków bezpieczeństwa. Według polskiej normy PN-I-13335-1 zarządzanie ryzykiem jest jednym z kluczowych elementów procesu zarządzania bezpieczeństwem systemów IT. Wzajemne powiązania między podstawowymi pojęciami z normy PN-ISO 13335-1 zostały przedstawione rys. 2 i 3.

W zarządzaniu ryzykiem niezwykle istotna jest odpowiedź na pytanie, do jakiego poziomu należy ryzyko obniżać, gdyż okazuje się, że w pewnym momencie implementacja nowych zabezpieczeń jest znacznie bardziej kosztowna niż potencjalne korzyści z niej płynące. Podstawowa zasada mówi, że ryzyko należy obniżać do takiego poziomu, w którym organizacja będzie zdolna ponieść ciężar potencjalnych strat, spowodowanych przez zrealizowane zagrożenia, i kontynuować swoją działalność [Piotrowski 2008].

5. Postępowanie z ryzykiem

Istotnym etapem procesu zarządzania ryzykiem jest wybór postępowania z ryzykiem. W ramach wyboru postępowania z ryzykiem należy dokonać [Szczepankiewicz, Szczepankiewicz 2006]:

- identyfikacji metod, narzędzi i środków redukcji lub transferu ryzyka oraz oszacowania ich kosztów i skuteczności,
- wdrożenia metod i środków redukcji lub transferu ryzyka,
- ustalenia poziomu akceptowalnego ryzyka,
- ustalenia metod unikania ryzyka.

W ramach różnych koncepcji i standardów stosowane są różne metody postępowania z ryzykiem. W literaturze przedmiotu wymieniane są takie działania, jak unikanie ryzyka, kontrolowanie ryzyka, transfer ryzyka, redukcja ryzyka oraz akceptacja ryzyka.

Unikanie ryzyka polega na takim zarządzaniu systemami informatycznymi, aby nie podejmować działań mogących zwiększać ryzyko – oczywiście taka strategia działania jest bardzo ograniczona, gdyż na większość czynników po prostu nie można mieć wpływu. Zatem unikanie ryzyka oznacza kierowanie samą działalnością (bez implementacji nowych zabezpieczeń) w taki sposób, aby ryzyko związane z tą działalnością było możliwie najmniejsze, lub też wręcz niepodejmowanie określonej działalności [Wołowski 2006].

Kolejną formą reagowania na ryzyko jest jego redukcja (ograniczanie). Ryzyko może być zredukowane przez wdrożenie architektury bezpieczeństwa, składającej się z zabezpieczeń, procedur, regulaminów itp. [Wołowski 2006]. Zatem redukcja to nic innego jak wprowadzanie zabezpieczeń do systemu, mających na celu zwiększenie jego bezpieczeństwa. Redukcja ryzyka jest podstawową strategią postępowania dla ryzyka przekraczającego wyznaczony poziom istotności dla danej organizacji. Podjęte działanie może prowadzić do likwidacji ryzyka lub do jego ograniczenia do akceptowalnego poziomu. Działania zmierzające do redukcji ryzyka mogą zmierzać w dwóch zasadniczych kierunkach [Liderman 2006; Szczepankiewicz, Szczepankiewicz 2006]:

- prewencja, czyli zapobieganie, oddziaływanie przez kontrolowanie podatności na możliwość realizacji zagrożenia;

- minimalizacja (redukcja) strat, czyli oddziaływanie na skutek realizacji zagrożenia, mające na celu zmniejszanie wielkości strat w przypadku wykorzystania podatności przez zagrożenie.

Do grupy działań o charakterze prewencyjnym, zmniejszających prawdopodobieństwo wystąpienia negatywnych zdarzeń w zakresie ryzyka informatycznego, należą m.in. [Szczepankiewicz, Szczepankiewicz 2006]:

- polityka ochrony dostępu do sprzętu, danych i funkcji systemowych,
- polityka dostępu do Internetu i innych sieci zewnętrznych,
- określanie standardów w zakresie jakości sprzętu, oprogramowania i usług IT,
- planowanie wydajności i pojemności systemów informatycznych,
- systemy wykrywania i usuwania szkodliwego oprogramowania,
- mechanizmy kontroli wewnętrznej oraz audyt,
- dobór i szkolenie personelu.

Szczególnie istotnym elementem jest ostatnia z wymienionych grup działań, a mianowicie szkolenia użytkowników systemu. Ich przeprowadzanie powinno być podporządkowane dwóm zasadniczym celom, a mianowicie zapoznaniu pracowników z nowymi rozwiązaniami technicznymi i organizacyjnymi oraz wzrastaniu świadomości pracowników w zakresie bezpieczeństwa SI. Szkolenia powinny być prowadzone przez osoby o dużej wiedzy merytorycznej z zakresu bezpieczeństwa oraz o dużym doświadczeniu praktycznym.

Do grupy działań zmniejszających skutki wystąpienia negatywnych zdarzeń w obszarze systemów informatycznych należą m.in. [Szczepankiewicz, Szczepankiewicz 2006]:

- plany awaryjne w zakresie utrzymania i odtworzenia ciągłości działania,
- architektura techniczna uwzględniająca redundantne elementy, systemy i centra przetwarzania,
- procedury reakcji na incydenty,
- procedury zarządzania problemem,
- urządzenia zapasowe.

Redukcja ryzyka jest rozwiązaniem stosowanym najczęściej, przynosi jednak właściwe i pożądane efekty tylko wtedy, gdy poprzedza ją rzetelnie i odpowiednio przeprowadzony proces analizy ryzyka. Kolejne działanie to transfer ryzyka, który polega na przeniesieniu konsekwencji wystąpienia szkody lub jej skutków finansowych na inny podmiot – najczęściej są to różnego rodzaju ubezpieczenia. Podstawową zasadą transferu jest dokonywanie go na podmiot, który potrafi ryzykiem zarządzać lepiej niż podmiot, który chce się ryzyka pozbyć lub je ograniczyć. Istnieje kilka form transferu ryzyka w organizacjach, a przede wszystkim:

- outsourcing tych funkcji firmy, które są obarczone szczególnie wysokim ryzykiem,
- ubezpieczenie ryzyka,
- korzystanie z wyspecjalizowanych usług zewnętrznych.

Ostatnia z wymienionych form transferu ryzyka to korzystanie z wyspecjalizowanych usług zewnętrznych. Jest to rozwiązanie uzasadnione w przypadku, gdy usługi zewnętrzne są tańsze, mają wyższą jakość i są lepiej zarządzane, niż miałoby to miejsce, gdyby były wykonywane przez wewnętrzny personel organizacji. Usługi takie w przypadku ryzyka informatycznego mogą dotyczyć serwisu sprzętu komputerowego i oprogramowania, dostarczenia i uruchomienia sprzętu zastępczego na wypadek awarii, przechowywania rezerwowych kopii danych, usuwania szkodliwego oprogramowania [Szczepankiewicz, Szczepankiewicz 2006]. Warunkiem realności takiego rozwiązania jest brak sprzężenia zwrotnego. Jeżeli bowiem skutki incydentu w obszarze bezpieczeństwa mogą wtórnie dotknąć instytucji lub organizacji dokonującej transferu ryzyka, to można mówić co najwyżej o wewnętrznym przesunięciu lub zmianie charakteru ryzyka wewnątrz organizacji [Wołowski 2006].

Transfer ryzyka powinien być efektywny kosztowo, zapewniać doprowadzenie ryzyka do akceptowalnego poziomu [Liderman 2006].

Akceptacja ryzyka to pogodzenie się z ewentualnymi konsekwencjami i zaniechanie dalszych działań – niestety, jak pokazuje praktyka, jest to bardzo często stosowane rozwiązanie. Po dokonaniu wyboru środków redukcji ryzyka lub ustaleniu warunków jego transferu oraz określeniu, jakie ograniczenie ryzyka zostanie osiągnięte, zawsze pozostanie ryzyko szczątkowe. Jednak w pewnych sytuacjach pomimo wysokiego poziomu ryzyka szczątkowego uzasadniona jest jego akceptacja. Uzależnione jest to od spodziewanych korzyści, które przynosi organizacji proces, do którego odnosi się rozpatrywane ryzyko. Akceptacja poziomu ryzyka szczątkowego powinna dotyczyć nie bezwzględnej wartości spodziewanych strat związanych z ryzykiem, ale spodziewanych strat odniesionych do spodziewanych korzyści [Szczepankiewicz, Szczepankiewicz 2006; Liderman 2006]. Decyzja o akceptacji ryzyka szczątkowego powinna należeć do zarządu przedsiębiorstwa. Akceptacja ryzyka nie powinna być stosowana dla ryzyka, które nie spełnia wszystkich następujących warunków [Wołowski 2006]:

- łatwe do przewidzenia skutki i wysokość potencjalnej szkody,
- relatywnie niska wysokość pojedynczej szkody,
- niskie prawdopodobieństwo znacznej kumulacji szkód.

W działaniach związanych z reakcją na ryzyko szczególnie istotne jest regularne monitorowanie ryzyka i jego raportowanie. Stanowią one podstawę do szybkiej identyfikacji i oceny słabości występujących w systemie zarządzania ryzykiem. Procesom tym powinny być poddane wszystkie incydenty naruszające własności zasobów chronionych. Dane uzyskane w procesie monitorowania oraz wyniki audytów stanowią podstawę do raportowania na temat stanu zarządzania ryzykiem. Raporty powinny być tworzone według ustalonego wzoru i przekazywane systematycznie do organów odpowiedzialnych za zarządzanie ryzykiem w organizacji [Szczepankiewicz, Szczepankiewicz 2006].

Literatura

Arrow K.J., *Eseje z teorii ryzyka*, Warszawa 1979.

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.

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.*

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., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2008.

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

Klimczak K.M., *Dylematy ujęcia ryzyka w teorii ekonomii*, Acta Universitatis Lodziensis, Łódź 2007.

Knight F.H., *Risk, Uncertainty and Profit,* University of Boston Press, Boston 1921.

Krupa M., *Ryzyko i niepewność w zarządzaniu firmą*, Wyd. Antykwa, Kraków 2002.

Lewandowski D., *Ryzyko operacyjne w bankach – zarządzanie i audyt w świetle wymagań Bazylejskiego Komitetu ds. Nadzoru Bankowego*, „Bank i Kredyt", kwiecień 2004.

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.

Liderman K., *Zarządzanie ryzykiem jako element zapewnienia odpowiedniego poziomu bezpieczeństwa teleinformatycznego*, Biuletyn Instytutu Automatyki i Robotyki 2006 nr 23, WAT, Warszawa 2006.

Nahotko S., *Ryzyko ekonomiczne w działalności gospodarczej*, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 2001.

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

Piotrowski M., *Zarządzanie ryzykiem cz. I. Panowanie nad niepewnością*, http://www.e-ochronadanych.eu/a,297,zarzadzanie-ryzykiem-cz-i-.html, 2008.

PN-I-02000, *Technika informatyczna – zabezpieczenia w SI – terminologia*, Polski Komitet Normalizacyjny, 1998.

PN-ISO/IEC 17799:2007, *Technika informatyczna – praktyczne zasady zarządzania bezpieczeństwem informacji.*

PN-ISO/IEC 27001:2007, *Technika informatyczna – techniki bezpieczeństwa –systemy zarządzania bezpieczeństwem informacji – wymagania.*

Ronka-Chmielowiec W. (red.), *Zastosowanie metod ekonometryczno-statystycznych w zarządzaniu finansami w zakładach ubezpieczeń*, AE, Wrocław 2004.

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

Staniec I., Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym*, Wyd. C.H. Beck, Warszawa 2008.

Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa 2001.

Szczepankiewicz E.I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym. Część 3 – Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów" 2006 nr 8.

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.
Szmit M., *Informatyka w zarządzaniu*, Difin, Warszawa 2003.
Vaughan E.J., *Risk Management*, J. Wiley & Sons Inc., New York 1997.
Willett A., *The Economic Theory of Risk and Insurance,* Columbia University Press, New York 1901.
Williams C.A. Jr., Heins R.M., *Risk Management and Insurance*, Mc Graw-Hill Book Company, New York 1989.
Wołowski F., *Zarządzanie ryzykiem systemów informacyjnych*, [w:]. *Bezpieczeństwo systemów informatycznych*, red. A. Niemiec, J.S. Nowak, J.K. Grabara, Polskie Towarzystwo Informatyczne – Oddział Górnośląski, Katowice 2006.

INFORMATION SYSTEMS SECURITY RISK MANAGEMENT – STRATEGIES FOR DEALING WITH RISK

Summary: Risk management is a discipline which integrates a variety of technologies for the identification, analysis, assessment of incidents and threats, and implementation of measures to enhance safety. It plays now a very important role in almost all areas of modern organizations. One of the essential elements of this complex process is the selection of a strategy for dealing with risk. The article provides an overview of the subject of information systems security risk management in organizations with particular emphasis on possible responses to the identified risks in this area.