PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1144 2006
Informatyka Ekonomiczna 9

Adam Nowicki, Artur Rot

ANALIZA RYZYKA JAKO ELEMENT STRATEGII BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO PRZEDSIĘBIORSTWA

1. Wstęp

Strategia bezpieczeństwa jest dokumentem określającym główny cel bezpieczeństwa. Powinna ona w sposób jak najbardziej obiektywny wskazywać cele, potrzeby zabezpieczeń oraz określać umowny poziom bezpieczeństwa systemu informacyjnego (SI) w organizacji. W tym celu, opracowując strategię bezpieczeństwa, należy dokonać wstępnej analizy wartości zasobów oraz zagrożeń i ryzyka. Analizę ryzyka można traktować jako usystematyzowanie w postaci podziału na kategorie zagrożeń wraz ze środkami im przeciwdziałającymi. Wykonanie analizy ryzyka może być bardzo pomocne przy realizacji kolejnych procesów zarządzania bezpieczeństwem systemu informacyjnego w organizacji.

Publikacje związane z problematyką analizy ryzyka – zarówno krajowe, jak i zagraniczne – wydają się jednak traktować ją w sposób dowolny. Przejawia się to w wielości definicji analizy ryzyka, a także w tym, iż często utożsamia się analizę ryzyka z jego zarządzaniem.

Celem niniejszego artykułu jest zaprezentowanie problematyki strategii bezpieczeństwa systemu informacyjnego przedsiębiorstwa oraz analizy ryzyka jako jej podstawowego elementu.

2. Istota i etapy zarządzania bezpieczeństwem systemu informacyjnego

Artykuł A. Nowickiego i A. Rota pt.: *Rola kultury organizacyjnej w zarządzaniu bezpieczeństwem systemu informacyjnego przedsiębiorstw* zamieszczony w niniejszym zeszycie naukowym przybliża istotę, przesłanki i znaczenie zarządzania bezpieczeństwem SI oraz pokazuje jego związki z zarządzaniem organizacją. W artykule tym przedstawiono również definicję zarządzania bezpieczeństwem SI. Definicja ta określała **zarządzanie bezpieczeństwem systemu informacyjnego jako ciągły, cykliczny, złożony i racjonalnie finansowany proces umożliwiający**

bezpieczną realizację misji, do której instytucję powołano. Zarządzanie bezpieczeństwem systemu informacyjnego obejmuje zespół złożonych powtarzalnych procesów zmierzających do osiągnięcia i utrzymywania oczekiwanego poziomu bezpieczeństwa systemu informacyjnego, tzn. poziomu poufności, integralności, dostępności, autentyczności i niezawodności.

Na proces ten składa się wiele etapów, które można pogrupować w trzy zasadnicze fazy:

- fazę prac przygotowawczych,
- fazę prac implementacyjnych,
- fazę prac kontrolnych.

W I fazie – **fazie prac przygotowawczych**, wyróżnić można:

- ustalenie strategii określającej potrzeby w zakresie bezpieczeństwa i cele systemu bezpieczeństwa,
- analizę ryzyka naruszenia bezpieczeństwa zasobów SI,
- planowanie i projektowanie systemu bezpieczeństwa – formułowanie polityki bezpieczeństwa SI;

II faza to **faza prac implementacyjnych**, a składają się na nią:

- organizacja i realizacja przedsięwzięć zabezpieczających,
- szkolenia pracowników;

III faza – **faza prac kontrolnych** składa się z:

- eksploatacji, monitoringu i audytu systemu bezpieczeństwa,
- oceny systemu bezpieczeństwa.

Ponadto ważnym procesem w zarządzaniu bezpieczeństwem systemu informacyjnego będzie **doskonalenie systemu bezpieczeństwa w przedsiębiorstwie**. Każdy z powyższych procesów dotyczy zasobów systemu informacyjnego, związany jest z określonymi metodami zabezpieczeń i zaangażowaniem pracowników. Pierwszy z etapów zarządzania bezpieczeństwem związany jest z ustaleniem **strategii bezpieczeństwa**, określającej przede wszystkim potrzeby w zakresie bezpieczeństwa oraz cele systemu bezpieczeństwa.

3. Strategia bezpieczeństwa

W pracy [Krupski 2003] zwrócono uwagę, iż strategia jest pojęciem wieloznacznym i stosowanym w różnych dziedzinach działalności ludzkiej, a w ostatnich latach zaczął mieć duże znaczenie w teorii organizacji i zarządzania. Szerokiej analizy terminologicznej tego pojęcia dokonał R. Krupski w pracy [Krupski 2005, s. 13-16]. Przytacza on szereg definicji sformułowanych przez różnych autorów. Warto w tym miejscu przytoczyć dwie z nich. Pierwsza podana została przez R.L. Ackoffa [1973], według którego strategia dotyczy długofalowych celów i sposobów ich osiągania, wpływających na system jako całość. Druga, sformułowana przez A.D. Chandlera [1962], mówi, iż strategia to określenie głównych, długofalowych celów i przyjęcie takich kierunków działania oraz taka alokacja zasobów,

które są konieczne do zrealizowania zadań. Autorem innej definicji, na którą w kontekście zarządzania bezpieczeństwem SI warto zwrócić uwagę, jest H. Mintzberg. Według niego, strategia jest wzorcem decyzji, który określa cele, tworzy zasadnicze polityki i plany dla osiągnięcia tych celów, określa rodzaj przedsięwzięć, strukturę organizacji, konieczny wkład inwestorów [Mintzberg, Quinn 1991].

W literaturze przedmiotu strategię bezpieczeństwa definiuje się jako serię specyficznych działań, które należy podjąć, by zwiększyć zakres i intensywność zabezpieczeń. W takim ujęciu strategia bezpieczeństwa ma następujące fazy [Pańkowska 2002, s. 286]:

- **Zrozumienie sytuacji obecnej** – przegląd technologii informacyjnych wykorzystywanych przez organizację, jej polityki bezpieczeństwa i dyrektyw zarządzania oraz ryzyka.
- **Zdefiniowanie środowiska najbardziej pożądanego** – przegląd najlepszej polityki, najlepszych procedur i działań praktycznych, rozmowy i wywiady z jak największą liczbą osób, z uwzględnieniem specjalistów ds. informatyki. Na podstawie analizy wymagań formułuje się architekturę zabezpieczeń.
- **Ocena najbardziej pożądanych rozwiązań alternatywnych i ocena ryzyka** – przegląd przyszłych systemów i aplikacji oraz kierunków rozwoju technik informatycznych.
- **Określenie najlepszej procedury postępowania** – prezentacja rekomendacji dla szczegółowych rozwiązań i procesów działań, analiza kosztów, opracowanie planu taktycznego.
- **Rozpoczęcie** – rozpoczęcie realizacji planu (rozpoczęcie implementacji rekomendowanej technologii, rozwiązań organizacyjnych, administracyjnych).

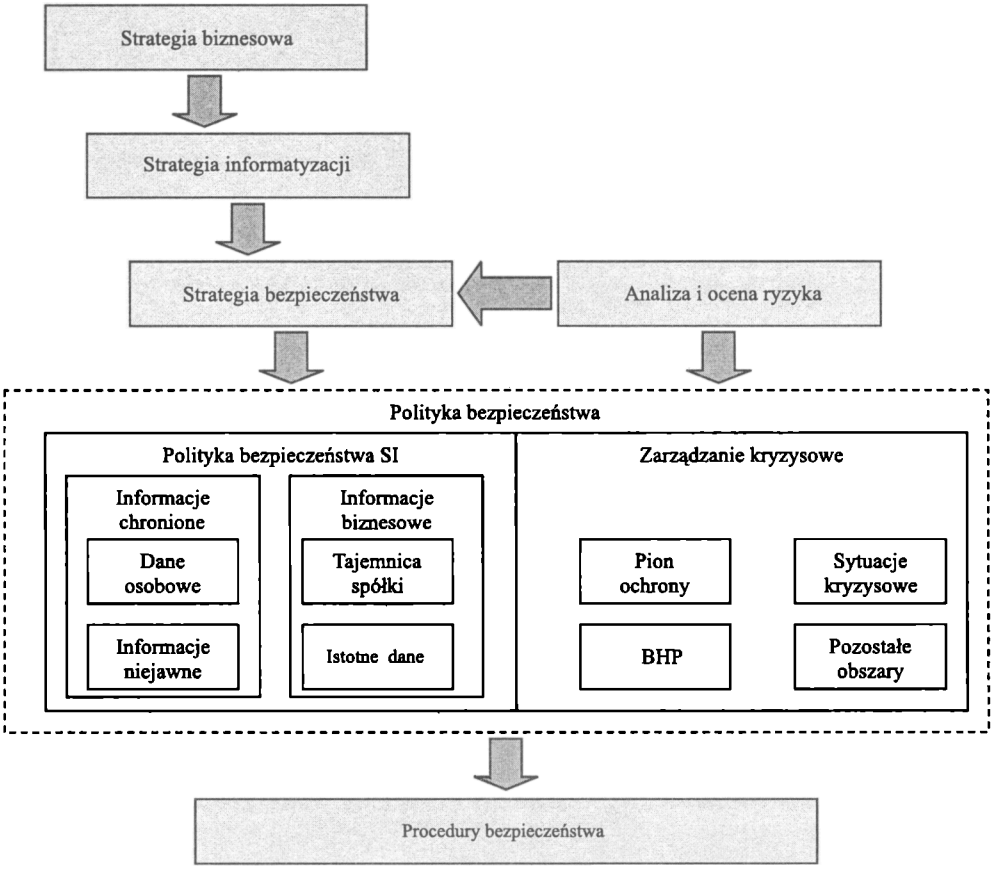
Strategia bezpieczeństwa jest nadrzędnym dokumentem określającym główny cel bezpieczeństwa. Musi być ona zgodna ze strategią biznesową oraz strategią informatyzacji, a także dążyć do osiągnięcia celów biznesowych [Bielec 2005] (zob. rys. 1).

Zwrócenie szczególnej uwagi na wymagania biznesowe przy formułowaniu strategii bezpieczeństwa pozwala na:

- zidentyfikowanie i określenie istotności ryzyka związanego z bezpieczeństwem, mogącego wpłynąć negatywnie na osiągnięcie celów biznesowych,
- doprowadzenie do kompletnego i spójnego wdrożenia systemu zarządzania bezpieczeństwem SI na podstawie istniejących rozwiązań i mechanizmów,
- zwrócenie szczególnej uwagi na ludzi i ich uprawnienia w przedsiębiorstwie,
- monitorowanie i wymuszanie autoryzacji w środowisku informatycznym.

Określenia celów, potrzeb, umownego poziomu bezpieczeństwa dla organizacji dokonuje zarząd wspierany przez kierownictwo działu IT, inspektorów i administratorów bezpieczeństwa oraz konsultantów zewnętrznych. Analizują oni szereg czynników, m.in.:

- znaczenie celów globalnych instytucji dla niej samej i dla społeczeństwa,
- zakres tolerancji zakłóceń w osiąganiu celów globalnych (misji) instytucji związanych z naruszeniem bezpieczeństwa SI,



Rys. 1. Hierarchia dokumentów w przedsiębiorstwie
Źródło: [www.ey.com; Bielec 2005].

- wielkość funduszy przewidzianych na zapewnienie bezpieczeństwa systemu informacyjnego,
- adekwatność zabezpieczeń do wartości chronionych zasobów,
- przyjęcie umownego poziomu bezpieczeństwa (zob. tab. 1).

Strategia bezpieczeństwa powinna także uwzględniać oraz rozważać następujące kwestie i zagadnienia:

- stopień uzależnienia instytucji od narzędzi technologii informacyjnej,
- potrzebę szczególnej ochrony środków i narzędzi technologii informacyjnej używanych do przetwarzania informacji poufnych,
- stopień zależności pomiędzy dokładnością, stosownością i dostępnością informacji przetwarzanych przez środki technologii informacyjnej a najważniejszymi decyzjami w organizacji,
- stopień zależności ważnych funkcji i zadań organizacji od technologii informacyjnej,

- możliwość tolerowania błędów w przetwarzaniu informacji,
- stopień tolerancji na przestoje i zakłócenia w funkcjonowaniu IT,
- aspekty prawne zobowiązujące do ochrony określonych zasobów informacyjnych przedsiębiorstwa.

Tabela 1. Umowne poziomy bezpieczeństwa

	Maksymalny (max – maximum)	Wysoki (h – high)	Umiarkowany (m – moderate)	Niski (l – low)
Charakterystyka ogólna	błędy w obszarze technologii informacyjnych prowadzą do załamania się instytucji oraz grożą konsekwencjami dla wybranych dziedzin gospodarki	zdarzenia szkodliwe prowadzą do załamania głównych obszarów funkcjonowania firmy oraz powodują duże szkody dla niej oraz jej partnerów biznesowych	Wynikiem szkodliwego zdarzenia jest sparaliżowanie instytucji	Wynikiem szkodliwego zdarzenia są zakłócenia w pracy przedsiębiorstwa
Poufność SI	bezpieczeństwo SI zagwarantowane, zgodnie ze ściśle zdefiniowanymi wymaganiami dla obszarów krytycznych	bezpieczeństwo SI zgodne z ustalonymi wymaganiami prawnymi i podwyższone dla obszarów krytycznych	Poufność wymagana jedynie dla informacji przeznaczonych na użytek wewnętrzny instytucji	Poufność SI nie jest wymagana
Poprawność przetwarzania informacji	poprawność informacji na najwyższym możliwym do osiągnięcia poziomie	przetwarzane informacje muszą być poprawne; ważna jest możliwość wykrywania i naprawiania błędów	Drobne błędy mogą być tolerowane. Błędy uniemożliwiające realizację zadań organizacji muszą być wykryte i naprawione	Błędy są tolerowane, przy czym umożliwiają dalszą realizację zadań instytucji
Tolerowanie zakłóceń w funkcjonowaniu IT (dostępność)	zadania podstawowe instytucji nie mogą być realizowane bez środków IT. Błyskawiczny czas reakcji na zdarzenia przy podejmowaniu decyzji wymaga informacji najwyższej jakości. Zakłócenia w funkcjonowaniu systemów informatycznych są niemożliwe	procesy ściśle uzależnione od czasu lub złożone zadania całkowicie uzależnione od środków IT są realizowane bez zakłóceń. Dopuszcza się krótkie przerwy w funkcjonowaniu systemów informatycznych	Dłuższe okresy zakłóceń w funkcjonowaniu IT, prowadzące do naruszenia terminów zobowiązań są niedopuszczalne	Nie dopuszcza się do dłuższych upadków – niezbyt długie upadki są akceptowane

Źródło: [Grzywak 2000, s. 295].

Strategia bezpieczeństwa jest bardzo specyficznym i istotnym elementem systemu zabezpieczeń instytucji. Powstaje zawsze jako pierwszy z wielu dokumentów, z którego treści następują kolejne odwołania do dokumentów polityki bezpieczeństwa czy rozmaitych procedur operacyjnych, również z zakresu zabezpieczeń. Dokument strategii bezpieczeństwa jest również dokumentem najbardziej ogólnym i prezentującym długookresowy trend planowania, wprowadzania i modyfikacji zabezpieczeń systemu informacyjnego. Ze względu na ogólny charakter strategia bezpieczeństwa nie wymaga wprowadzania istotnych zmian w jego treści, a jedynie drobnych korekt wynikających np. ze zmienności standardu używanej technologii informacyjnej.

Treść strategii bezpieczeństwa jest uzależniona od wielu czynników. Jej forma jest związana z przyjętym dla instytucji standardem. Specyficznym elementem odróżniającym strategię bezpieczeństwa systemu informacyjnego od dokumentów strategii biznesowych, rozwoju lub planowania budżetu jest m.in. jej techniczny charakter (ale bez szczegółów technicznych) oraz powiązania z głównymi elementami funkcjonowania instytucji, takimi jak zakupy czy budżet. Strategia bezpieczeństwa ma jeszcze jeden specyficzny element – jest stała i w większości przypadków może być przeniesiona do innej instytucji z tej samej branży. Nie ma jednak możliwości zaadaptowania strategii bezpieczeństwa w firmach o innym profilu działalności. Zupełnie inne cele, wymagania i założenia będą występowały np. w banku, firmie telekomunikacyjnej czy jednostce militarnej. Poza skrajnie różnymi własnościami systemu informacyjnego i zagrożeniami, różnice występują tu także w kulturze organizacyjnej, sposobie zarządzania, uwarunkowaniach technologicznych, ekonomicznych i prawnych. Strategia bezpieczeństwa powinna być formułowana dla każdego przedsiębiorstwa oddzielnie ze względu na odrębną ocenę ryzyka i kondycję finansową.

Strategia bezpieczeństwa powinna mieć przemyślany i spójny układ. Główną częścią strategii bezpieczeństwa jest opisanie potrzeb zabezpieczeń obszarów biznesowych i określenie celu ich ochrony. W sposób szczegółowy należy określić również grupy zabezpieczeń, jakie będą wykorzystywane do ochrony danych i innych zasobów systemu informacyjnego, oraz to, w jakiej kolejności będą implementowane.

Cechy wspólne strategii zabezpieczeń dla różnych instytucji to [Pańkowska 2001, s. 167]:

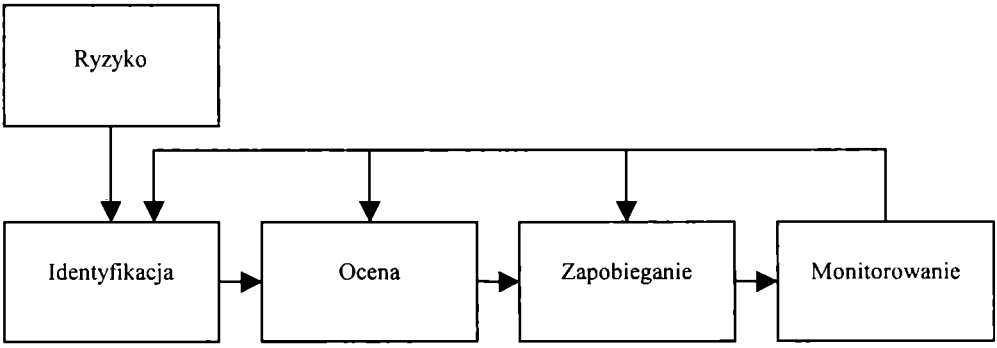
1. Celem strategii jest wygenerowanie modelu systemu zabezpieczeń i ustalenie kierunków rozwoju tego systemu w organizacji, nie zaś znalezienie rozwiązania każdego problemu zgłaszanego przez pracownika. Strategia może rekomendować różnorodne rozwiązania, określać zalecenia, co stwarza konieczność odniesienia się do każdego zagrożenia.
2. Strategia musi pozwolić pogodzić cele ogólne z celami indywidualnymi użytkowników systemu informacyjnego.
3. Nie wszystkie cele są bezpośrednio realizowane, ich duża część zostaje osiągnięta w dalszej perspektywie czasu.
4. Strategia bezpieczeństwa ewoluuje. Strategia powinna być weryfikowana i modyfikowana ze względu na zmiany w celach ekonomicznych i kierunkach funkcjonowania obiektu gospodarczego.

Strategia powinna w sposób jak najbardziej obiektywny wskazywać potrzeby zabezpieczeń. W tym celu należy dokonać wstępnej analizy wartości zasobów oraz analizy zagrożeń i ryzyka. Jeżeli uda się określić realne potrzeby zabezpieczeń poszczególnych systemów informatycznych, to do dopełnienia strategii pozostaje jedynie określenie, w jakiej kolejności zasoby będą zabezpieczane i w jakim czasie zostanie osiągnięty wymierny – określony poziom bezpieczeństwa. Ta część strategii bezpieczeństwa często określana jest jako analiza ryzyka.

4. Analiza ryzyka

Jak wspominano już wielokrotnie, efektywne funkcjonowanie systemów informacyjnych zależy od praktyk w zakresie bezpieczeństwa, a ogólnie od zarządzania bezpieczeństwem SI. Jednym z podstawowych procesów w zarządzaniu bezpieczeństwem jest **zarządzanie ryzykiem**, które powinno być prowadzone podczas całego okresu eksploatacji systemu, gdyż tylko wówczas jest efektywne [Tsoumas, Tryfonas 2004]. **Zarządzanie ryzykiem** jest procesem osiągania i utrzymania stanu równowagi między zidentyfikowanymi zagrożeniami a działaniami podjętymi w celu zabezpieczenia zasobów systemu informacyjnego.

Z. Szyjewski, dokonując w pracach [Szyjewski 2001; Szyjewski 2004] obszernej analizy różnych aspektów związanych z zarządzaniem projektami informatycznymi, dużo miejsca poświęcił problematyce zarządzania ryzykiem. Przedstawione tam wybrane ujęcia tej tematyki zaadaptować można na potrzeby zarządzania ryzykiem związanym z zagrożeniami bezpieczeństwa systemu informacyjnego organizacji. Podkreśla on, iż w praktyce niepewność i ryzyko są ściśle ze sobą związane, a zarządzanie ryzykiem przedstawia jako proces cyklicznie powtarzanych działań (zob. rys. 2 i 3) [Szyjewski 2004, s. 223].



Rys. 2. Model zarządzania ryzykiem

Źródło: [Szyjewski 2004, s. 223].

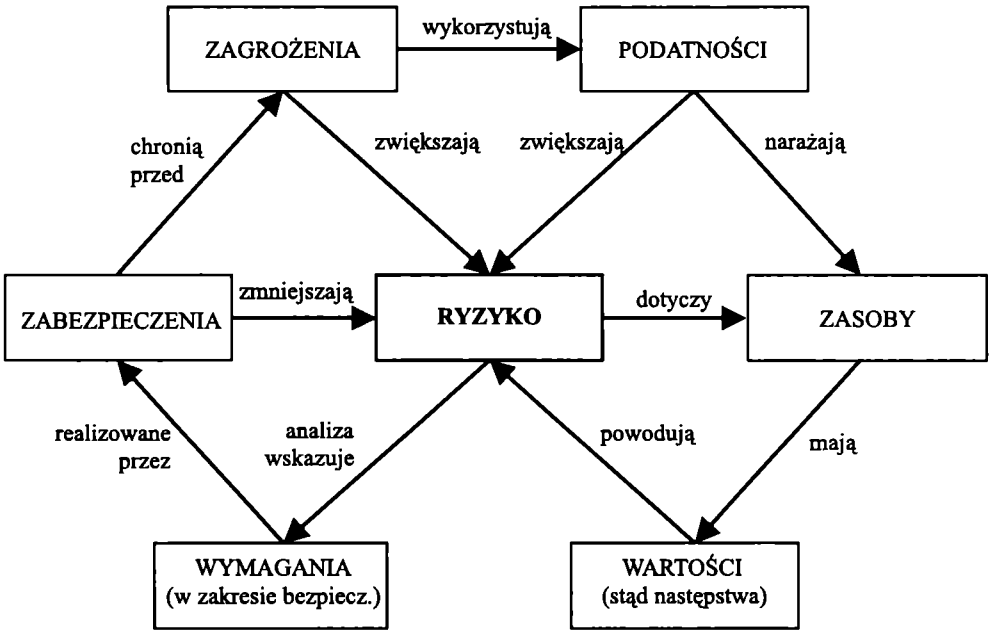
M. Pańkowska, biorąc pod uwagę klasyfikację M. Portera, wyróżnia trzy zasadnicze warianty strategii zarządzania ryzykiem [Pańkowska 2002, s. 289]:

- *strategia koncentracji (innowacji)* oznaczająca implementację nowoczesnych rozwiązań zabezpieczających;
- *strategia dywersyfikacji*, oznaczająca niezawodność, różne systemy i sposoby zabezpieczeń;
- *strategia minimalnych kosztów zabezpieczeń*, oznaczająca minimalizację nakładów finansowych przeznaczonych na bezpieczeństwo SI.

Strategia zarządzania ryzykiem musi ewoluować wraz ze zmieniającymi się celami i strategiami biznesowymi przedsiębiorstwa. Powinna ona wykazywać następujące cechy:

- elastyczność wobec rosnącej złożoności i skali zagrożeń związanych z bezpieczeństwem SI,
- podkreślenie kluczowego znaczenia ludzi i procesów,
- ewoluowanie wraz ze zmieniającym się ustawodawstwem, zagrożeniami oraz mechanizmami kontrolnymi,
- umożliwienie szybkiej reakcji na występujące zagrożenia i przeprowadzanie udoskonaleń.

Analiza ryzyka to niewątpliwie podstawowy element procesu zarządzania bezpieczeństwem SJ. Jest głównym procesem zarządzania ryzykiem, identyfikuje ryzyko, które ma być kontrolowane lub akceptowane. Analiza ryzyka obejmuje ocenę wartości zasobów, podatności i następstw w aspekcie naruszania poufności, integralności, dostępności, autentyczności i niezawodności.



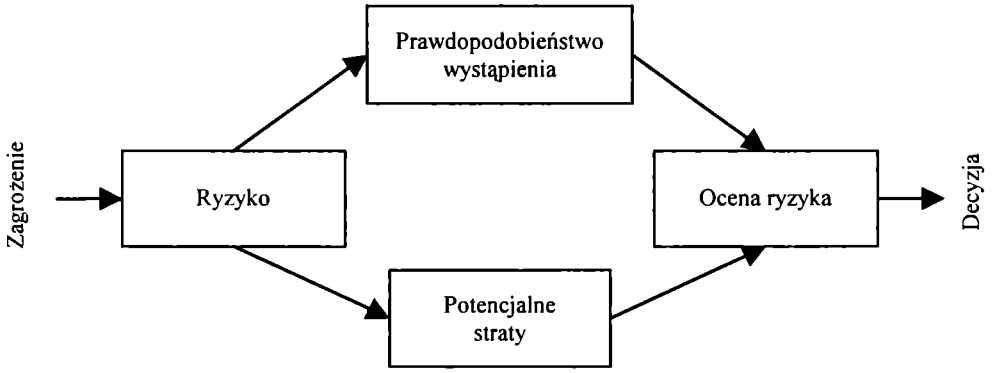
Rys. 3. Związki w zarządzaniu ryzykiem

Źródło: opracowanie własne na podstawie [Grzywak 2000, s. 291].

Analizę ryzyka można traktować także jako usystematyzowanie w postaci podziału na kategorie zagrożeń wraz ze środkami im przeciwdziałającymi. W wyniku takiej klasyfikacji jesteśmy w stanie opracować plan działania, który pozwoli na skierowanie większości środków na przeciwdziałanie najbardziej prawdopodobnym zagrożeniom, a więc podjąć określone decyzje (Młynarski, Piechota 2001). Na rysunku 4 przedstawiony został ogólny model analizy ryzyka zaprezentowany w pracy (Szyjewski 2004, s. 232).

Analiza ryzyka powinna być przeprowadzana w różnych fazach cyklu życia systemu bezpieczeństwa, dlatego też pełny cykl analizy ryzyka może być stosowany:

- dla nowych systemów,
- dla eksploatowanych systemów – w dowolnym momencie życia systemu,
- podczas okresowych przeglądów i kontroli wdrożenia zabezpieczeń,
- podczas projektowania systemu,
- przy planowaniu istotnych zmian w systemie.



Rys. 4. Model analizy ryzyka

Źródło: [Szyjewski 2004, s. 232].

Analiza ryzyka skłania do wykonania prac w następujących obszarach (Pańkowska 2002, s. 283-284):

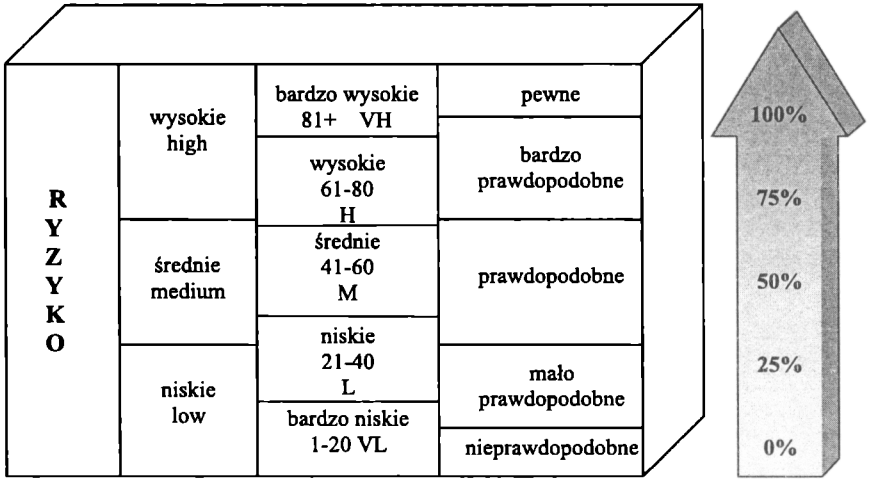
- wartościowania zasobów (informacja, oprogramowanie, sprzęt i zasoby fizyczne) – wartość zasobu to nie tylko wartość jego nabycia, ale również krótkoterminowe efekty i długoterminowe konsekwencje jego zniszczenia,
- oceny konsekwencji – określenie stopnia zniszczenia lub strat, jakie przypuszczalnie mogą wystąpić,
- identyfikacji zagrożeń, czyli obiektów lub zdarzeń, które niszczą zasoby systemu informacyjnego – analiza zagrożeń powinna ustalać prawdopodobieństwo ich wystąpienia i możliwość zniszczenia zasobu SI,
- analizy zabezpieczeń w aspekcie efektywności istniejących środków zabezpieczeń,
- analizy podatności poszczególnych zasobów SI,
- oceny prawdopodobieństwa, czyli częstotliwości wystąpienia zagrożenia – ocena ta powinna obejmować obecność, czas trwania i siłę zagrożenia, a także efektywność zabezpieczeń.

W związku z tym formularz analizy ryzyka powinien zatem zawierać m.in. [Młynarski, Piechota 2001]:

- opis i charakterystykę ryzyka (np. zniszczenie sprzętu, utrata danych, kradzież poufnych informacji),

- potencjalne następstwa,
- szacunkowy koszt eliminacji następstw,
- prawdopodobieństwo wystąpienia zagrożenia,
- opis działań zapobiegawczych,
- koszt zabezpieczeń.

Tego typu informacje zawsze będą miały charakter szacunkowy, jednak dokładne, bazujące m.in. na doświadczeniach innych przedsiębiorstw wykonanie analizy ryzyka może być bardzo pomocne przy realizacji kolejnych procesów zarządzania bezpieczeństwem systemu informacyjnego w organizacji. Pozostaje jednak problem oszacowania ryzyka. 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 [Szyjewski 2004, s. 230]. Zobrazowano to na rys. 5.



Rys. 5. Miary ryzyka

Źródło: [Szyjewski 2004, s. 230].

Do oceny ryzyka zastosować można macierz oceny poziomu ryzyka, służącą oszacowaniu wartości oczekiwanej strat. Prawidłowe oszacowanie ryzyka i ocena prawdopodobieństwa jego wystąpienia dają jasny obraz jego wpływu na funkcjonowanie całego systemu informacyjnego. Tym szacunkom służy wiele metod. Do najpopularniejszych i często prezentowanych w literaturze przedmiotu można zaliczyć następujące [Wawrzyniak 2000]:

- Metoda Courtneya – opiera się na szacowaniu potencjalnej straty jako iloczynu wartości strat pieniężnych związanych z wystąpieniem danego zagrożenia oraz wskaźnika określającego prawdopodobieństwo jego wystąpienia (zob. [Caelli, Longley, Shain 1994]).

- Metoda macierzowa (*Matrix-Method*) – polega na zestawieniu głównych procesów systemowych oraz ich zagrożeń i przypisaniu każdej parze poziomu ryzyka (zob. [Caelli, Longley, Shain 1994]).

Tabela 2. Macierz szacowania ryzyka

Obszary podatności oraz możliwe następstwa ryzyka	Ryzyko strat finansowych			Ryzyko strat produktywności			Ryzyko utraty zaufania klientów		
	H	M	L	H	M	L	H	M	L
Personel	H – high/wysokie, M – medium/średnie, L – low/niskie								
Nieautoryzowane ujawnienie lub zniszczenie informacji									
Nieumyślna modyfikacja lub zniszczenie informacji									
Brak lub błędna usługa									
Odmowa usługi									
Sprzęt									
Nieautoryzowane ujawnienie lub zniszczenie informacji									
Nieumyślna modyfikacja lub zniszczenie informacji									
Brak lub błędna usługa									
Odmowa usługi									
Aplikacje									
Nieautoryzowane ujawnienie lub zniszczenie informacji									
Nieumyślna modyfikacja lub zniszczenie informacji									
Brak lub błędna usługa									
Odmowa usługi									
Komunikacja									
Nieautoryzowane ujawnienie lub zniszczenie informacji									
Nieumyślna modyfikacja lub zniszczenie informacji									
Brak lub błędna usługa									
Odmowa usługi									
Oprogramowanie i systemy operacyjne									
Nieautoryzowane ujawnienie lub zniszczenie informacji									
Nieumyślna modyfikacja lub zniszczenie informacji									
Brak lub błędna usługa									
Odmowa usługi									

Źródło: GAO – Information Security Risk Assessment.

Jedną z przykładowych metod jest szacowanie ryzyka na podstawie macierzy pokazanej w tab. 2 (*Risk Assessment Matrix*). Macierz ta wyszczególnia pięć pod-

stawowych obszarów ryzyka, którymi są: personel, sprzęt, aplikacje, komunikacja, oprogramowanie i systemy operacyjne. Metoda polega na przypisaniu poszczególnym obszarom odpowiednio wysokiego, średniego lub niskiego poziomu ryzyka. Ryzyko to może dotyczyć strat finansowych, strat produktywności oraz utraty zaufania klientów.

Norma PN ISO/IEC 17799 wyróżnia cztery strategie korporacyjnej analizy ryzyka dla zabezpieczenia systemu informacyjnego. Ich krótką charakterystykę przedstawiono w tab. 3. Wybór strategii analizy ryzyka jest istotnym elementem procesu zarządzania bezpieczeństwem systemu informacyjnego, wpływa on bowiem istotnie na koszty przeprowadzenia tej analizy. Można wymienić jeszcze kilka innych rodzajów strategii analizy ryzyka (zob. [Pańkowska 2002, s. 290-291]). Zaliczyć należy do nich ujęcia zawarte w tab. 4.

Tabela 3. Cztery strategie korporacyjnej analizy ryzyka dla zabezpieczenia SI

Nazwa strategii korporacyjnej analizy ryzyka	Charakterystyka strategii
1	2
Strategia podstawowego poziomu bezpieczeństwa	• polega na wyselekcjonowaniu grupy zabezpieczeń, które pozwalałyby na osiągnięcie podstawowego poziomu bezpieczeństwa SI, • po zbadaniu podstawowych potrzeb możliwe jest przystosowanie zabezpieczeń stosowanych w innych przedsiębiorstwach, • nie wymaga angażowania zasobów dla przeprowadzenia szczegółowej analizy ryzyka, • czas i nakład pracy poświęcone na wybór odpowiednich zabezpieczeń są zredukowane, • identyfikacja odpowiednich zabezpieczeń podstawowego poziomu nie wymaga znacznych zasobów, a te same lub podobne zabezpieczenia mogą zostać zaadaptowane do wielu systemów informatycznych, • podstawowe wady strategii: – ustawienie poziomu podstawowego zbyt wysoko może powodować nadmierny poziom ochrony niektórych zasobów SI, – ustawienie poziomu podstawowego zbyt nisko może powodować brak bezpieczeństwa niektórych zasobów i systemów informatycznych, – mogą wystąpić trudności w zarządzaniu istotnymi zmianami bezpieczeństwa
Strategia nieformalnej analizy ryzyka	• polega na przeprowadzeniu nieformalnej, ale pragmatycznej analizy ryzyka wszystkich systemów, • nie opiera się na metodach strukturalnych, lecz na wiedzy i doświadczeniu pracowników lub konsultantów zewnętrznych, • nie wymaga wielu zasobów i czasu, • efektywna pod względem kosztów, • odpowiednia dla mniejszych organizacji, • podstawowe wady strategii: – duże prawdopodobieństwo pominięcia niektórych rodzajów ryzyka i zagrożeń, na jej rezultaty wpływ mają subiektywne poglądy i oceny osoby dokonującej analizy,

tab. 3, cd.

1	2
	– trudności w uzasadnieniu wyboru konkretnych zabezpieczeń i poniesionych na nie kosztów, – mogą wystąpić trudności w zarządzaniu zmianami bezpieczeństwa
Strategia szczegółowej analizy ryzyka	• wymaga głębokiego rozpoznania i oceny zasobów, oszacowania zagrożeń tych zasobów, • jest podstawą do wyboru i określenia zabezpieczeń uzasadnionych zidentyfikowanymi ryzykami oraz do ograniczenia tych rodzajów ryzyka do akceptowalnego poziomu, • w jej wyniku określone zostają właściwe zabezpieczenia dla wszystkich systemów, • wyniki niniejszej analizy mogą zostać użyte do zarządzania zmianami bezpieczeństwa, • podstawowe wady strategii: – wymaga czasu, nakładu pracy, wiedzy i doświadczenia, – istnieje prawdopodobieństwo zbyt późnego określenia potrzeb w zakresie bezpieczeństwa systemu informacyjnego, gdyż systemy są badane bardzo szczegółowo, do czego wymagane jest dużo czasu
Strategia mieszana	• polega na wstępnej identyfikacji z zastosowaniem metody analizy wysokiego poziomu systemów o wysokim ryzyku lub krytycznych z punktu widzenia prowadzonej działalności, • wyniki identyfikacji są podstawą do podziałów systemów na te, dla których będzie przeprowadzana szczegółowa analiza ryzyka, oraz te, dla których podstawowy poziom zabezpieczeń jest wystarczający, • zapewnia równowagę między minimalizacją czasu i nakładu pracy a właściwym wyborem zabezpieczeń, • wspomaga tworzenie natychmiastowego obrazu strategicznego całego bezpieczeństwa, co może być pomocne w planowaniu, • zasoby i środki finansowe można przeznaczyć tam, gdzie przyniosą najwięcej korzyści, • systemy narażone na wysokie ryzyko mogą być w miarę szybko zabezpieczone, • podejście efektywne czasowo i zalecane dla większości przedsiębiorstw, • podstawowe wady strategii: – niedokładność wstępnych wyników identyfikacji doprowadzić może do pominięcia niektórych systemów wymagających szczegółowej analizy ryzyka

Źródło: opracowanie własne na podstawie [Pańkowska 2002, s. 287-289].

Tabela 4. Strategie analizy ryzyka

Nazwa strategii analizy ryzyka	Syntetyczna charakterystyka strategii
Strategia funkcjonalna analizy ryzyka	• dotyczy różnych funkcji i obszarów funkcjonalnych systemu informacyjnego, • składa się ze strategii cząstkowych funkcjonalnych (np. strategii analizy zagrożeń zasobów materialnych, oprogramowania, danych)

	• traktowana jest na równi z innymi strategiami funkcjonalnymi (np. strategią marketingową, produkcji, informatyzacji, finansów), • powinna ona być powiązana bezpośrednio z ogólną strategią przedsiębiorstwa
Strategia systemowa analizy ryzyka	• oznacza przyjęcie orientacji systemowej na strategiczne kształtowanie systemu zabezpieczeń, • traktuje zabezpieczenia jako systemową strategię, • zorientowane funkcjonalnie optymalizacje cząstkowe zostają zastąpione optymalizacją systemową zorientowaną poziomo na cały system zabezpieczeń SI
Strategia integrująca zabezpieczeń (zintegrowana)	• przyjmuje się, że strategia informatyzacji oddziałuje na strategię ogólną przedsiębiorstwa, • zasady myślenia i działania zorientowanego na informatykę modyfikują odpowiednio strategie instytucji, • zabezpieczenie SI i analiza ryzyka nie są traktowane tylko jako procesy obecne we wszystkich obszarach funkcjonalnych firmy, ale jako dziedzina integrująca i stymulująca działania pozostałych sfer funkcjonowania i zarządzania przedsiębiorstwem
Strategia analizy ryzyka według ról	• rola – to, co dana osoba ma do wykonania w przedsiębiorstwie, zarówno w kooperacji z innymi osobami, jak i ze względu na samą organizację, • model ról opisuje wszystkie role i ich pozycje w organizacji, • analiza ryzyka opartego na rolach wymaga wprowadzenia do modelu dwóch zasadniczych elementów: ról i aktorów, • definiuje role i aktorów oraz umożliwia analizę scenariuszy, • analiza ról umożliwia modelowanie dla prowadzenia symulacji ataków i prób naruszeń bezpieczeństwa zasobów SI

Źródło: opracowanie własne na podstawie [Pańkowska 2002, s. 290-291].

W literaturze anglojęzycznej istnieją całe opracowania poświęcone problematyce analizy ryzyka i jej związków ze strategią bezpieczeństwa. Warto zwrócić uwagę na pozycję [Peltier 2001], szeroko omawiającą tę tematykę.

5. Zakończenie

Podstawowym celem opracowania strategii bezpieczeństwa powinno być określenie, w sposób jak najbardziej obiektywny, potrzeb i celów zabezpieczeń oraz wyznaczenie docelowego umownego poziomu bezpieczeństwa. Aby to osiągnąć, należy dokonać wstępnej analizy wartości zasobów oraz analizy zagrożeń i prawdopodobieństwa ich wystąpienia. Ta część strategii bezpieczeństwa często określana jest jako analiza ryzyka. Problematyka analizy ryzyka w kontekście zarządzania bezpieczeństwem systemu informacyjnego jest wciąż zagadnieniem nierozpoznanym do końca. Istnieje wiele podejść i metodyk mających na celu zidentyfikowanie i ocenienie ryzyka występującego w funkcjonowaniu systemu informacyjnego. Jest to jednak proces bardzo istotny i konieczne jest uwzględnienie go przy opracowywaniu strategii bezpieczeństwa systemu informacyjnego.

Literatura

Ackoff R.L., *O system pojęć systemowych*, „Prakseologia" 1973 nr 2.
Bielec J., *Potrzeby informatyczne użytkowników a bezpieczeństwo systemu informatycznego*, Materiały konferencyjne „Od informacji do decyzji" – Konferencja tygodnika „Computerworld" 17 marca 2005.
Caelli W., Longley D., Shain M., *Information Security Handbook*, Macmillan Press Ltd., 1994.
Chandler A.D., *Strategy and Structure*, Cambridge, Massachusetts 1962.
Grzywak A., *Bezpieczeństwo systemów komputerowych*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.
Krupski R. (red.), *Zarządzanie przedsiębiorstwem w turbulentnym otoczeniu*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.
Krupski R. (red.), *Zarządzanie strategiczne. Koncepcje – metody*, AE, Wrocław 2003.
Mintzberg H., Quinn J.B., *The Strategy Process, Concepts, Contexts, Cases*, Prentice Hall, Englewood Cliffs, New Jersey 1991.
Młynarski K., Piechota J., *Polityka bezpieczeństwa jako kluczowy element tworzenia systemu informatycznego*, Materiały konferencyjne VII Konferencji PLOUG 2001 „Systemy informatyczne u progu nowego wieku – wydajność i bezpieczeństwo", 23-27 października, Zakopane, Kościelisko 2001.
Pańkowska M., *Wielowariantowość analizy ryzyka dla zabezpieczania systemów informatycznych zarządzania*, [w:] *Zastosowanie informatyki w rachunkowości i finansach*, red. B. Kubiak, A. Korowicki, Polskie Towarzystwo Ekonomiczne, Gdańsk 2002.
Pańkowska M., *Zarządzanie zasobami informatycznymi*, Wydawnictwo Difin, Warszawa 2001.
Peltier T.R., *Information Security Risk Analysis*, Auerbach Publications 2001.
Szyjewski Z., *Metodyki zarządzania projektami informatycznymi*, Wydawnictwo Placet, Warszawa 2004.
Szyjewski Z., *Zarządzanie projektami informatycznymi*, Wydawnictwo Placet, Warszawa 2001.
Tsoumas V., Tryfonas T., *From Risk Analysis to Effective Security Management: Towards an Automated Approach, Information Management & Computer Security* Vol. 12, Bradford 2004.
United States General Accounting Office (GAO) – Accounting and Information Management Division *Information Security Risk Assessment. Practices of Leasing Organizations*, http://www.gao.gov, 1999.
Wawrzyniak D., *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, AE, Wrocław 2002.
www.ey.com.

RISK ANALYSIS AS THE ELEMENT OF INFORMATION SYSTEM SECURITY MANAGEMENT IN THE ENTERPRISE

Summary

Security strategy is a document, which defines the main security aim. It should show in objective way the aims, needs in security area and define the conventional security level. To elaborate the strategy one should conduct initial resources value analysis as well as threats and risk analysis. The risk analysis subject in area of information system management is still an unexamined problem. There are many different approaches, methods, whose aim is to identify and estimate the risk in information systems performance. It is very important process and it is necessary to include it in a process of building IS security strategy in enterprise. The purpose of the article is to present the subject of IS security strategy in a company and to discuss risk analysis as its main component.

Adam Nowicki – prof. dr hab., kierownik Katedry Inżynierii Systemów Informatycznych Zarządzania Akademii Ekonomicznej we Wrocławiu.

Artur Rot – dr, asystent w Katedrze Inżynierii Systemów Informatycznych Zarządzania Akademii Ekonomicznej we Wrocławiu.