PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 88
Informatyka Ekonomiczna 15 2010

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

ZARZĄDZANIE RYZYKIEM JAKO ELEMENT ZAPEWNIENIA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W ORGANIZACJI

Streszczenie: Ryzyko związane z funkcjonowaniem systemów informatycznych staje się coraz bardziej powszechne i przybiera różnorodne formy. Postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i liczby czynników ryzyka. W tym kontekście bardzo istotnym procesem jest zarządzanie ryzykiem, służące minimalizacji strat związanych z zagrożeniami. Proces ten polega głównie na identyfikacji zagrożeń i podatności, szacowaniu ryzyka oraz rekomendowaniu dodatkowych środków zabezpieczeń. W artykule przedstawiono zagadnienia zarządzania ryzykiem, zaprezentowano uproszczony model tego procesu na bazie normy ISO/IEC TR 13335. Dokonano również przeglądu i charakterystyki wybranych standardów i zaleceń w tym obszarze oraz wskazano komputerowe narzędzia wspierające ten proces w organizacjach.

Słowa kluczowe: zarządzanie ryzykiem, bezpieczeństwo systemów informatycznych, analiza ryzyka, model zarządzania ryzykiem, standardy i normy zarządzania ryzykiem.

1. Wstęp

Nowoczesne technologie informacyjne warunkują funkcjonowanie obiektów gospodarczych, których działalność w coraz większym stopniu uzależniona jest od najnowszych, lecz jednocześnie bezpiecznych narzędzi teleinformatycznych. Postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i ilości czynników ryzyka. Współczesne systemy informatyczne (SI) wykreowały nowe rodzaje ryzyka, a ich bezpieczeństwo nabrało wymiaru globalnego.

Rosnąca współcześnie wartość informacji powoduje wzrost zagrożeń systemów informatycznych, stąd niezwykłej wagi problemem staje się zagadnienie ich bezpieczeństwa. Z jednej strony przedsiębiorstwa dążą do otwartości i szerokiego dostępu do informacji, z drugiej – chcą, aby ich systemy informatyczne zachowywały poufność, integralność i stałą aktualność. Gdy kluczowe zasoby informacyjne utracą te cechy, może to w znacznym stopniu zagrozić funkcjonowaniu organizacji. Bezpie-

czeństwo SI może więc decydować nie tylko o pozycji na rynku i wizerunku zewnętrznym firmy, ale często również o jej dalszym istnieniu.

Problematyka bezpieczeństwa systemów informatycznych ma charakter złożony, interdyscyplinarny i jest obecnie niezwykle aktualna ze względu na pojawiające się nowe formy zagrożeń tych systemów, ciągły postęp w zakresie technologii informacyjnych, jak i metod, technik oraz narzędzi ich zabezpieczania. Ponadto każde naruszenie bezpieczeństwa może stać się przyczyną wymiernych strat finansowych, a liczba incydentów związanych z bezpieczeństwem systemów informatycznych w organizacjach rośnie z roku na rok. Obecnie istnieje trend, zauważalny zarówno w badaniach naukowych, jak i w praktyce, postrzegania różnych aspektów działalności biznesowej firm przez pryzmat ryzyka. Ma to odzwierciedlenie również w problematyce bezpieczeństwa systemów informatycznych, niezmiernie istotnej dla współczesnych organizacji. Celem niniejszego artykułu jest wprowadzenie do problematyki zarządzania ryzykiem bezpieczeństwa systemów informatycznych ze szczególnym uwzględnieniem tematyki analizy ryzyka. W artykule dokonany zostanie także przegląd i charakterystyka wybranych standardów i zaleceń w tym obszarze oraz syntetyczna prezentacja wybranych komputerowych narzędzi wspierających ten proces w organizacjach.

2. Ryzyko w obszarze bezpieczeństwa systemów informatycznych

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 nieodłącznie towarzyszy podejmowaniu decyzji gospodarczych. Globalizacja gospodarki powoduje, iż dotychczasowe warunki funkcjonowania organizacji diametralnie się zmieniają. Otoczenie, w którym działa współczesne przedsiębiorstwo, jest nie tylko zmienne, ale często wręcz nieprzewidywalne. W miarę postępu technologicznego, a w szczególności gwałtownego rozwoju Internetu, jak i wzrostu znaczenia informacji dla funkcjonowania przedsiębiorstw, ryzyko związane z funkcjonowaniem systemów informatycznych staje się coraz bardziej powszechne i przybiera różnorodne formy. Przy tak dynamicznym rozwoju technologii informatycznych skraca się zdecydowanie czas wymagany na odpowiednią reakcję wobec ryzyka. Brak odpowiedniego przygotowania może prowadzić przedsiębiorstwa do upadku, dlatego właściwa reakcja na ryzyko stanowi o możliwościach przetrwania i rozwoju firmy.

Termin ryzyko bezpieczeństwa systemów informatycznych nie jest definiowany w sposób jednoznaczny, podobnie, jak pojęcie samego ryzyka, które ma wiele odcieni znaczeniowych. W większości jednak jest ono 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 obszarze bezpieczeństwa syste-

mów informatycznych, gdzie jest rozpatrywana możliwość wykorzystania podatności na zagrożenie w celu spowodowania następstw niekorzystnych dla systemów informatycznych, a co się z tym wiąże, także organizacji [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.

Na potrzeby bezpieczeństwa systemów informatycznych można przytoczyć następującą definicję ryzyka 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].

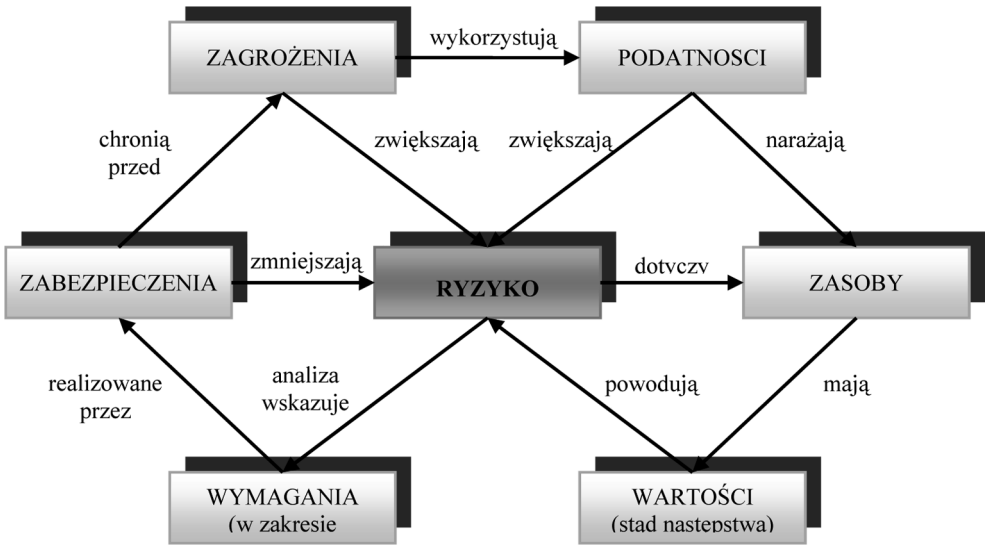
Istnieje szereg innych standardów, próbujących regulować niniejszą problematykę. Na przykład międzynarodowy standard ISO/IEC TR 13335 zawiera pewne wskazówki, od czego zależy wielkość ryzyka związanego z bezpieczeństwem systemów informatycznych: „Ryzyko jest funkcją wartości zasobów objętych ryzykiem, możliwości wystąpienia zagrożeń, łatwości wykorzystania podatności na zagrożenia oraz istniejących (lub planowanych, gdy szacuje się ryzyko dla projektowanych systemów bezpieczeństwa) zabezpieczeń mogących zredukować ryzyko" (PN-ISO-13335) [Liderman 2008, s. 70]. Wybrane standardy odnoszące się do tej tematyki zostaną syntetycznie scharakteryzowane w dalszej części artykułu.

3. Proces zarządzania ryzykiem bezpieczeństwa systemu informatycznego

Zarządzanie ryzykiem jest procesem osiągania i utrzymywania stanu równowagi między zidentyfikowanymi zagrożeniami a działaniami podjętymi w celu zabezpieczenia SI. Odgrywa ono obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji, polega na identyfikacji zagrożeń i podatności, szacowaniu ryzyka oraz wyborze określonych środków bezpieczeństwa. Proces ten to identyfikacja, mierzenie i kontrolowanie ryzyka w celu jego maksymalnego ograniczenia oraz zabezpieczenie przed jego skutkami. Zarządzanie ryzykiem ma na celu m.in. [Liderman 2006]:

– wykazanie, których rodzajów ryzyka i jak można uniknąć, stosując rozwiązania organizacyjne i techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji w SI,
– zapewnienie optymalnego, ze względu na koszty i ograniczenia, stanu bezpieczeństwa SI,
– zminimalizowanie ryzyka szczątkowego, aby stało sie ryzykiem akceptowalnym.

Związki pomiędzy poszczególnymi elementami w procesie zarządzania ryzykiem prezentuje rys. 1.



Rys. 1. Związki w zarządzaniu ryzykiem

Źródło: [Grzywak 2000, s. 291].

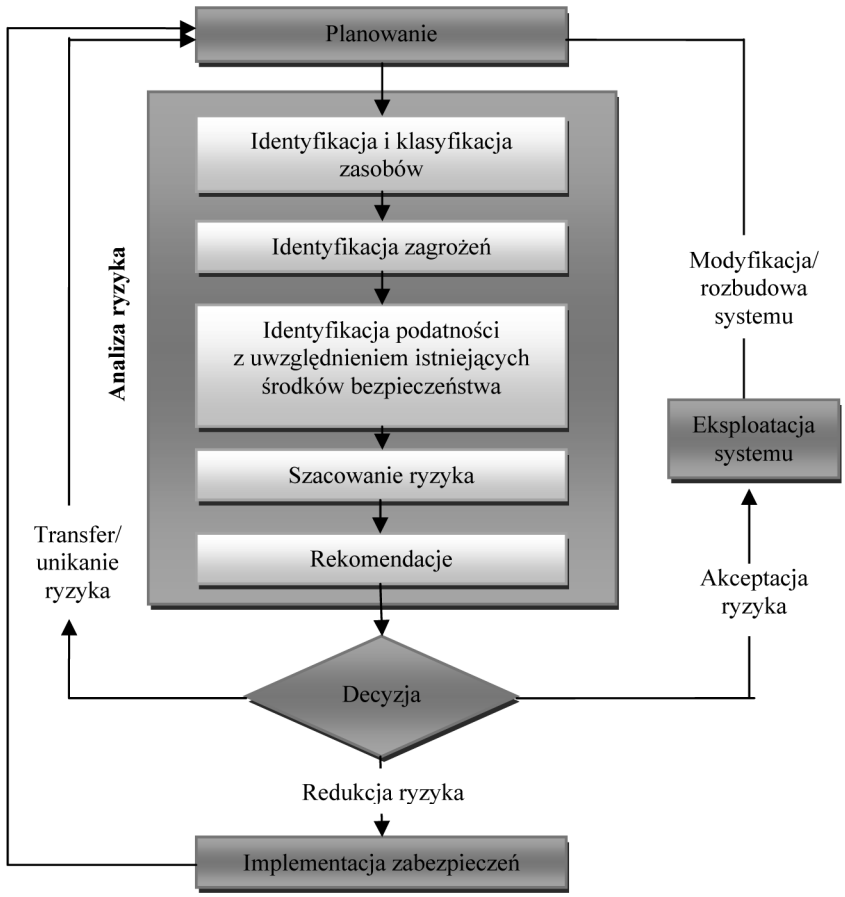
W pracy M. Pańkowskiej [2002, s. 289], biorącej pod uwagę klasyfikację M. Portera, wyróżniono trzy zasadnicze warianty strategii zarządzania ryzykiem w organizacjach:

– strategię koncentracji (innowacji), oznaczającą implementację nowoczesnych rozwiązań zabezpieczających,
– strategię dywersyfikacji, oznaczającą różne systemy i sposoby zabezpieczeń,
– strategię minimalnych kosztów zabezpieczeń, oznaczającą 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 bezpieczeństwa SI,
– podkreślenie kluczowego znaczenia ludzi i procesów,
– ewoluowanie ze zmieniającym się prawem, zagrożeniami oraz mechanizmami kontroli,
– umożliwienie szybkiej reakcji na zagrożenia i przeprowadzanie udoskonaleń.

Jak już wskazano w artykule, identyfikacja zagrożeń i podatności, szacowanie ryzyka oraz rekomendowanie określonych środków zabezpieczeń to podstawowe elementy procesu zarządzania ryzykiem. Uproszczony schemat modelu tego procesu, bazujący na przytoczonej już normie ISO/IEC TR 13335-3, został zaprezentowany na rys. 2.



Rys. 2. Uproszczony model zarządzania ryzykiem według standardu ISO/IEC TR 13335

Źródło: [Piotrowski 2008].

Jak wynika z zaprezentowanego modelu, kluczowy element procesu zarządzania ryzykiem bezpieczeństwa systemów informatycznych stanowi analiza ryzyka, pozwalająca na identyfikację zasobów systemu, zlokalizowanie odpowiadających im podatności i zagrożeń oraz oszacowanie prawdopodobieństwa ich wystąpienia i wielkości potencjalnych strat. Analiza ryzyka obejmuje ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, autentyczności i niezawodności. Analizę ryzyka można traktować także jako usystematyzowanie zagrożeń, w postaci podziału na kategorie, wraz ze środkami im przeciwdziałającymi. W wyniku takiej klasyfikacji jesteśmy w stanie opracować plan działania, który ułatwi skierowanie większości środków na przeciwdziałanie najbardziej prawdopodobnym zagrożeniom, a więc podjąć określone decyzje [Młynarski, Piechota 2001].

Analiza ryzyka powinna być przeprowadzana w różnych fazach cyklu życia systemu bezpieczeństwa, dlatego też pełny cykl analizy ryzyka może być stosowany dla nowych, jak i eksploatowanych systemów, podczas okresowych przeglądów i kontroli wdrożenia zabezpieczeń, podczas projektowania systemu, a także przy planowaniu znaczących zmian w systemie. Analiza ryzyka koncentruje się na wykonaniu 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 SI – analiza zagrożeń powinna ustalać prawdopodobieństwo ich wystąpienia i możliwość zniszczenia zasobów SI,
– analizy zabezpieczeń w aspekcie efektywności istniejących środków zabezpieczeń,
– analizy podatności poszczególnych zasobów SI,
– oceny prawdopodobieństwa, czyli częstotliwości wystąpienia zagrożenia – ocena ta powinna uwzględniać identyfikację, czas trwania i siłę zagrożenia, jak też efektywność zabezpieczeń.

Formularz analizy ryzyka powinien zatem zawierać m.in. opis ryzyka, potencjalny skutek, szacunkowy koszt eliminacji skutków, prawdopodobieństwo wystąpienia zagrożenia, względne priorytety, opis działań zapobiegawczych oraz przewidywany koszt zabezpieczeń [Młynarski, Piechota 2001]. Tego typu informacje zawsze będą miały charakter szacunkowy, jednak dokładne, bazujące m.in. na doświadczeniach innych firm, wykonanie analizy ryzyka może być bardzo pomocne w realizacji kolejnych procesów związanych z zarządzaniem ryzykiem. Prawidłowe oszacowanie ryzyka i ocena prawdopodobieństwa jego wystąpienia dają jasny obraz jego wpływu na funkcjonowanie całego systemu. Do analizy i oszacowania ryzyka, na jakie są narażone SI, stosuje się dwie grupy metod [Szczepankiewicz 2006]:

– metody ilościowe, gdzie oszacowanie wartości ryzyka wiąże się z wykorzystaniem miar liczbowych – wartość zasobów jest określana kwotowo, częstotliwość wystąpienia zagrożenia – liczbą przypadków, a podatność – wartością prawdopodobieństwa ich utraty; metody te prezentują wyniki w postaci wskaźników;
– jakościowe, które nie operują na danych liczbowych, przedstawiając wyniki w postaci opisów, zaleceń, gdzie oszacowanie ryzyka wiąże się z opisem jakościowym wartości aktywów, określeniem skal jakościowych dla częstotliwości wystąpienia zagrożeń i podatności na dane zagrożenie, albo z opisem tzw. scenariuszy zagrożeń poprzez przewidywanie głównych czynników ryzyka.

W tabeli 1 przedstawiono najważniejsze zalety oraz wady ilościowych i jakościowych metod analizy ryzyka.

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

Analiza ryzyka	Metody ilościowe	Metody jakościowe
Wybrane zalety	• Pozwalają określać konsekwencje wystąpienia incydentów w sposób ilościowy, co ułatwia przeprowadzenie analizy kosztów i korzyści podczas wyboru zabezpieczeń. • Dają dokładniejszy obraz ryzyka.	• Pozwalają uszeregować ryzyka według priorytetu. • Pozwalają wyznaczyć w krótkim czasie i bez większych nakładów obszary zwiększonego ryzyka. • Analiza jest stosunkowo łatwa i tania.
Wybrane wady	• Zależą od zakresu i dokładności zdefiniowanej skali pomiarowej. • Wyniki analizy mogą być nieprecyzyjne. • Zwykle muszą być wzbogacone o opis jakościowy (w postaci komentarza). • Analiza jest na ogół droższa, wymaga doświadczenia i zaawansowanych narzędzi.	• Nie pozwalają wyznaczyć prawdopodobieństw i skutków następstw za pomocą miar liczbowych. • Trudniejsza jest analiza kosztów-korzyści podczas doboru zabezpieczeń. • Uzyskane wyniki mają charakter ogólny, przybliżony itp.

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

W zależności od wagi danego zagrożenia można stosować różne miary ryzyka, od bardzo prostych ocen, określających ryzyko jako wysokie, średnie lub niskie, do dokładnych wskaźników, wyrażonych jako prawdopodobieństwo wystąpienia danego zdarzenia.

Norma ISO/IEC 17799 wyróżnia cztery strategie analizy ryzyka. Ich charakterystykę przedstawiono w tab. 2. Wybór strategii analizy jest istotnym elementem zarządzania ryzykiem, wpływa on bowiem znacząco na koszty przeprowadzenia tego procesu.

Jak już wspomniano, podstawowym celem analizy ryzyka jest dostarczenie informacji niezbędnej w podejmowaniu decyzji o zastosowaniu określonych środków bezpieczeństwa w organizacji. Istnieje kilka sposobów radzenia sobie z ryzykiem, będących istotnym elementem procesu zarządzania ryzykiem. Są to przede wszystkim: unikanie, transfer, redukcja oraz akceptacja ryzyka. Unikanie ryzyka polega na zarządzaniu technologiami informatycznymi w taki sposób, aby nie podejmować działań mogących zwiększać ryzyko. Taki sposób zarządzania ryzykiem jest bardzo ograniczony, gdyż na większość czynników po prostu nie mamy wpływu. Transfer ryzyka polega na przeniesieniu konsekwencji wystąpienia szkody lub jej skutków finansowych na inny podmiot. Najczęstszym rozwiązaniem są tutaj różnego rodzaju ubezpieczenia. Redukcja ryzyka polega na wprowadzaniu określonych środków bezpieczeństwa. Natomiast akceptacja ryzyka to pogodzenie się z ewentualnymi konsekwencjami i zaniechanie dalszych działań [Piotrowski 2008].

Usystematyzowany i dobrze realizowany proces zarządzania ryzykiem przyczynia się do zidentyfikowania ryzyka utraty bezpieczeństwa systemu informatycznego w prowadzonej działalności. Zidentyfikowane rodzaje ryzyka zostają ocenione pod

Tabela 2. Cztery strategie korporacyjnej analizy ryzyka dla zabezpieczenia SI

Nazwa strategii korporacyjnej analizy ryzyka	Charakterystyka strategii
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 wykorzystywanych w innych organizacjach. • Czas i nakład pracy poświęcony na wybór zabezpieczeń jest zredukowany. • Identyfikacja odpowiednich zabezpieczeń podstawowego poziomu nie wymaga dużych 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.
Strategia nieformalnej analizy ryzyka	• Polega na przeprowadzeniu nieformalnej, ale pragmatycznej analizy ryzyka SI. • Nie opiera się na metodach strukturalnych, lecz na wiedzy i doświadczeniu pracowników lub konsultantów zewnętrznych. • Nie wymaga wielu zasobów i czasu, jest efektywna pod względem kosztów. • Jest odpowiednia dla mniejszych organizacji. • Podstawowe wady strategii: – duże prawdopodobieństwo pominięcia niektórych rodzajów ryzyka, – na jej rezultaty wpływ mają subiektywne oceny osoby dokonującej analizy, – trudności w uzasadnieniu wyboru konkretnych zabezpieczeń i poniesionych na nie kosztów.
Strategia szczegółowej analizy ryzyka	• Wymaga głębokiego rozpoznania i oceny zasobów, oszacowania zagrożeń. • Jest podstawą do wyboru i określenia zabezpieczeń uzasadnionych zidentyfikowanym ryzykiem oraz do ograniczenia tego ryzyka do akceptowalnego poziomu. • W jej wyniku określone zostają właściwe zabezpieczenia dla wszystkich SI. • Podstawowe wady strategii: – wymaga czasu, nakładu pracy, wiedzy i doświadczenia, – możliwość zbyt późnego określenia potrzeb bezpieczeństwa SI, gdyż systemy są badane szczegółowo, co wymaga 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 (podejście zalecane dla większości firm). • Zasoby i finanse można skierować tam, gdzie przyniosą najwięcej korzyści. • Podstawowa wada strategii: niedokładność wstępnych wyników identyfikacji doprowadzić może do pominięcia niektórych SI, wymagających szczegółowej analizy ryzyka.

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

kątem konsekwencji biznesowych oraz zostaje określone prawdopodobieństwo ich wystąpienia. W ramach tego procesu definiuje się zasady w zakresie postępowania z ryzykiem i określa priorytety podejmowanych działań, których celem jest ograniczanie ryzyka; monitorowana jest także efektywność tych działań. Dzięki informowaniu o istniejącym ryzyku oraz szkoleniom dotyczącym zasad ich ograniczania rośnie bezpieczeństwo SI w organizacji.

4. Zarządzanie ryzykiem według wybranych norm, standardów i zaleceń

Metody i techniki zabezpieczeń systemów informatycznych są przedmiotem standaryzacji, zarówno przez międzynarodowe, jak i krajowe instytucje standaryzacyjne. Instytucje te poświęcają coraz więcej uwagi problematyce związanej z zarządzaniem ryzykiem, a w szczególności ryzykiem związanym z funkcjonowaniem SI w organizacjach. Widoczna jest również pewna tendencja, objawiająca się tym, iż kwestie dotyczące bezpieczeństwa SI, które jeszcze niedawno były traktowane niezależnie, rozpatrywane są coraz częściej w kontekście kompleksowego procesu zarządzania ryzykiem [Szczepankiewicz 2006]. Celem instytucji standaryzacyjnych jest tworzenie i promowanie norm międzynarodowych w różnorodnych dziedzinach działalności technicznej, ekonomicznej i naukowej. Niektóre z nich dostarczają wskazówek i wytycznych dla osób zarządzających ryzykiem bezpieczeństwa systemów informatycznych. Wybrane normy, ważniejsze z punktu widzenia zarządzania ryzykiem, zaprezentowano w tab. 3.

W obszarze zarządzania ryzykiem IT istotny jest raport techniczny – ISO/IEC TR 13335, określany mianem *Guidelines for the Management of IT Security*, składający się z pięciu zasadniczych części. Ich syntetyczną charakterystykę zawarto w tab. 4.

W odniesieniu do systemów informatycznych proces zarządzania ryzykiem najpełniej opisany jest we wspomnianym raporcie technicznym ISO/IEC TR 13335–3 *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*. Dokument zawiera szczegółowe informacje dotyczące trójpoziomowej polityki bezpieczeństwa, omawia metody analizy ryzyka, implementację zabezpieczeń oraz sposobów reagowania na różne incydenty. W raporcie tym wiele miejsca poświęcono technikom i metodom analizy ryzyka oraz postępowania z nim.

Według tego dokumentu punktem wyjścia do efektywnego zarządzania ryzykiem związanym z systemami informatycznymi jest określenie celów bezpieczeństwa instytucji w zakresie ochrony informacji [Szczepankiewicz 2006]. Pierwszym etapem w procesie zarządzania ryzykiem powinno być postawienie pytania, jaki poziom ryzyka jest akceptowalny dla organizacji. Kolejny krok to wyznaczenie celów bezpieczeństwa SI. Jednocześnie należy także rozważyć ważne cele biznesowe oraz ich związek z bezpieczeństwem. W zależności od celów należy uzgodnić strategię

Tabela 3. Zarządzanie ryzykiem bezpieczeństwa SI w wybranych standardach ISO/IEC

Standard międzynarodowy	Polska Norma	Syntetyczna charakterystyka standardu
ISO/IEC TR 13335–1	PN-I-13335–1 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem SI. Część 1: Pojęcia i modele bezpieczeństwa SI	Precyzuje terminologię i związki między pojęciami używanymi w informatyce i zarządzaniu bezpieczeństwem SI. Proponuje podstawowe modele zarządzania bezpieczeństwem.
ISO/IEC TR 13335–2	Raport techniczny ISO/IEC TR 13335–2 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Część 2: Zarządzanie i planowanie bezpieczeństwa SI	Zawiera opis różnych sposobów podejścia do prowadzenia analizy ryzyka, planów zabezpieczeń, roli szkoleń i działań uświadamiających, opis struktur organizacyjnych i stanowisk pracy związanych z bezpieczeństwem SI.
ISO/IEC TR 13335–3	Raport techniczny ISO/IEC TR 13335–3 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem SI. Część 3: Techniki zarządzania bezpieczeństwem SI	Zawiera: model trójpoziomowej polityki bezpieczeństwa, rozwinięcie problematyki analizy ryzyka i implementacji planu zabezpieczeń, zasady reagowania na incydenty.
ISO/IEC TR 15408–1	PN-ISO/IEC 15408–1 Technika informatyczna. Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych. Część 1: Wprowadzenie i model ogólny	Definiuje tzw. wspólne kryteria oceny zabezpieczeń SI (*common criteria*), które mogą być używane jako podstawa do oceny właściwości SI. Odnosi się także do modelu zarządzania ryzykiem.
ISO/IEC TR 15408–3	PN-ISO/IEC 15408–3 Technika informatyczna. Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych. Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń	Omawia techniki zabezpieczeń oraz kryteria oceny zabezpieczeń informatycznych. Definiuje także poziomy uzasadnienia zaufania i warunki, jakie muszą spełniać elementy systemu zabezpieczeń.
ISO/IEC 17799	PN-ISO/IEC 17799 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informatycznym	Ma formę wytycznych i zaleceń. Definiuje 36 celów oraz 127 regulacji bezpieczeństwa podzielonych na 10 obszarów.
ISO/IEC 17799-2	PN ISO/IEC 17799-2 Systemy zarządzania bezpieczeństwem informacji. Część 2: Specyfikacja i wytyczne do stosowania	Zawiera wymagania dotyczące wdrażania, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji w kontekście ryzyka biznesowego.

Źródło: opracowanie własne na podstawie [Szczepankiewicz 2006].

Tabela 4. Syntetyczna charakterystyka standardu ISO/IEC TR 13335

Symbol części raportu	Nazwa części raportu	Syntetyczna charakterystyka części raportu
ISO/IEC TR 13335-1	Wytyczne do zarządzania bezpieczeństwem SI	– terminologia, związki między pojęciami, – podstawowe modele, – trzy podprocesy: zarządzanie ryzykiem, zmianami i konfiguracją
ISO/IEC TR 13335-2	Technika informatyczna – Planowanie i zarządzanie bezpieczeństwem SI	– określenie celów, strategii, polityki bezpieczeństwa, – określenie wymagań w zakresie bezpieczeństwa, – różne podejścia do analizy ryzyka, – plany zabezpieczeń – dobór właściwych zabezpieczeń oraz monitorowanie procesu ich wdrażania i funkcjonowania, – organizacja służb odpowiedzialnych za bezpieczeństwo, – znaczenie szkoleń i działań uświadamiających, – role i stanowiska pracy w instytucji związane z bezpieczeństwem, – wykrywanie i reagowanie na incydenty
ISO/IEC TR 13335-3	Techniki zarządzania bezpieczeństwem systemów informatycznych	– przedstawienie procesów zarządzania, – formułowanie trójpoziomowej polityki bezpieczeństwa, – rozwinięcie problematyki analizy ryzyka i implementacji planu zabezpieczeń, – czynności powdrożeniowe: utrzymanie, monitorowanie i reagowanie na incydenty
ISO/IEC TR 13335-4	Wybór zabezpieczeń	– klasyfikacja i charakterystyka różnych form zabezpieczeń, – sposoby doboru zabezpieczeń ze względu na rodzaj zagrożenia lub specyfikację systemu, – prezentacja zaleceń wynikających z norm ISO/IEC i opracowanych przez różne organizacje, – podejście do analizy ryzyka polegające na wyróżnieniu obszarów wymagających szczegółowej lub podstawowej analizy ryzyka
ISO/IEC TR 13335-5	Zabezpieczenie dla połączeń z sieciami zewnętrznymi	– dobór zabezpieczeń stosowanych do ochrony styku systemów instytucji z siecią zewnętrzną

Źródło: opracowanie własne na podstawie [www.centrumbezpieczenstwa.pl].

konieczną do ich osiągnięcia. Po określeniu strategii bezpieczeństwa i zagadnień wchodzących w jej skład, powinna stać się ona podstawą polityki bezpieczeństwa organizacji [Szczepankiewicz 2006].

Jedną z podstawowych norm związanych z zarządzaniem bezpieczeństwem SI jest standard ISO/IEC 17799 o nazwie *Praktyczne zasady zarządzania bezpieczeństwem informacji*. Zastosowanie wytycznych powyższej normy daje możliwość zmniejszenia do minimum ryzyka zafałszowania, a nawet utraty informacji, co na obecnym etapie rozwoju w zakresie technologii informacyjnych jest niemalże koniecznością. Zastosowanie normy ISO/IEC 17799 pozwala także określić wymagania przedsiębiorstwa pod względem bezpieczeństwa, sformułować politykę ochrony i bezpieczeństwa SI oraz wybrać środki, dzięki którym jego bezpieczeństwo zostanie zapewnione. Norma wspomaga więc procesy organizacyjne w sposób umożliwiający racjonalne podwyższenie bezpieczeństwa systemu, koncentrując się na sferze organizacyjnej oraz kontrolując obszary zwiększonego ryzyka [Jakubowski 2002]. W dokumencie tym wyróżniono takie obszary tematyczne, jak:

1) polityka bezpieczeństwa,
2) organizacja systemu zarządzania bezpieczeństwem w firmie,
3) inwentaryzacja i klasyfikacja posiadanych zasobów,
4) edukacja pracowników,
5) bezpieczeństwo fizyczne i środowiskowe,
6) zarządzanie komunikacją i bieżącą obsługą polityki bezpieczeństwa,
7) kontrola dostępu do zasobów,
8) utrzymanie i rozbudowa SI zgodnie z polityką bezpieczeństwa,
9) zarządzanie ciągłością pracy firmy,
10) zgodność polityki bezpieczeństwa z regulacjami i normami.

Cobit (*control objectives for information and related technology*) jest zestawieniem dobrych praktyk do zarządzania IT, utworzonym przez stowarzyszenie ISACA. Metodyka Cobit służy jako pomoc w zarządzaniu, kontroli i audycie systemów informatycznych. Cobit szczegółowo określa wytyczne w zakresie zarządzania technologiami informatycznymi w firmie, także w ramach procesów analizy ryzyka bezpieczeństwa informatycznego. W standardzie wyróżniono 34 procesy, które są związane z zarządzanymi zasobami oraz tak zwanymi wymogami (kryteriami) informacyjnymi. Każdy wymóg biznesowy jest opisany przez siedem biznesowych wymogów informacyjnych, stanowiących kryteria kontrolne. Są to: skuteczność (zapewnienie, że informacja w procesach biznesowych jest dla nich odpowiednia i adekwatna, dostarczona na czas w sposób prawidłowy), wydajność (zapewnienie, że dostarczenie informacji odbywa się w ramach optymalnego zużycia zasobów), poufność (zapewnienie, że dostęp do informacji mają tylko osoby uprawnione), integralność (zapewnienie, że informacja pozostaje dokładna i kompletna), dostępność (zapewnienie, że dostęp do informacji jest możliwy wtedy, gdy jest to wymagane w procesie biznesowym), zgodność (zapewnienie, że każdy element systemu pozostaje zgodny z przepisami prawa), wiarygodność (zapewnienie właściwych informacji dla

zarządzania organizacją). Szczególnie istotne, z punktu widzenia problematyki zarządzania ryzykiem bezpieczeństwa SI są następujące kryteria: poufność, integralność i dostępność.

Spośród 34 procesów zdefiniowanych w standardzie Cobit szczególnie ważny i interesujący z punktu widzenia ryzyka jest proces oznaczony jako PO9, czyli szacowanie ryzyka. W ramach tego procesu zaleca się szacowanie ryzyka do celów biznesowych. Ma ono stanowić wsparcie dla decyzji kierownictwa w zakresie zarządzania ryzykiem [Szczepankiewicz 2006]. W ramach szacowania ryzyka Cobit definiuje następujące podprocesy [Korytowski 2002; Szczepankiewicz 2006]: ocena ryzyka biznesowego (PO-9.1), przyjęcie podejścia do oceny ryzyka (PO-9.2), identyfikacja ryzyka (PO-9.3), pomiar ryzyka (PO-9.4), plan działania w zakresie ryzyka (PO-9.5), akceptacja ryzyka (PO-9.6), wybór środków bezpieczeństwa (PO-9.7), poparcie dla zarządzania ryzykiem (PO-9.8).

Standard podaje szereg kolejnych wytycznych dotyczących ryzyka i jego szacowania. Można do nich zaliczyć następujące zalecenia:

– ryzyko informatyczne powinno być regularnie szacowane,
– kierownictwo powinno być powiadamiane o istotnych, mogących wpłynąć na scenariusze ryzyka, zmianach w środowisku IT,
– organizacja powinna określić poziom akceptowanego ryzyka i wdrożyć procedury postępowania z ryzykiem nieakceptowanym,
– kierownictwo musi monitorować wielkość ryzyka i podejmować działania w razie przekroczenia jego akceptowanego poziomu [Szczepankiewicz 2006].

Cobit, jak również i inne wskazane normy i zalecenia mogą stanowić bardzo cenne źródło informacji dla osób odpowiedzialnych za zarządzanie, kontrolę i audyt IT w organizacji, w tym również w obszarze zarządzania ryzykiem informatycznym.

5. Komputerowe wsparcie zarządzania ryzykiem

Większość popularnych metodyk zarządzania ryzykiem doczekała się komputerowego wsparcia, a aplikacje te zostały stworzone na bazie norm, standardów czy dobrych praktyk. Przykładami takich systemów są następujące programy i pakiety informatyczne: CRAMM, Marion, CORA, COBRA, MEHARI-Risk, RiskPAC.

System CRAMM bazuje na popularnej metodyce CRAMM, która została przyjęta przez CCTA (U.K. Government Central Computer and Telecommunications Agency) jako rządowy standard podejścia do analizy ryzyka i zarządzania bezpieczeństwem. Zarządzanie ryzykiem według CRAMM składa się z następujących po sobie procesów: identyfikacji i wyceny zasobów, oceny zagrożeń i podatności, wyboru oraz rekomendacji mechanizmów kontrolnych i zabezpieczających [Ryba 2006, s. 44]. Jest to pakiet służący do analizy i zarządzania ryzykiem, składający się z trzech części, a dodatkowo wspierany dużą biblioteką ankiet, kwestionariuszy i zaleceń. Istnieją dwie podstawowe wersje tego systemu: uproszczona – „Express" oraz zaawansowana dla profesjonalistów – „Expert".

Marion jest pakietem opracowanym w Wielkiej Brytanii przez firmę Coopers & Lybrand i służy do analizy ryzyka w organizacjach komercyjnych. Opiera się na bibliotece znanych incydentów, a zawiera wiele ankiet i kwestionariuszy stosowanych do oceny rozwiązań w zakresie bezpieczeństwa. W analizie ryzyka zastosowano metodę obejmującą elementy analizy jakościowej i ilościowej. Oprogramowanie wylicza wyniki analizy dla 27 kategorii zasobów i zagrożeń. Umożliwia także prowadzenie analizy porównawczej wyników oraz utworzenie cenowej bazy danych dla elementów mających wpływ na bezpieczeństwo. Umożliwia to programowe oszacowanie kosztów ponoszonych w związku z poprawą systemu zabezpieczeń [Białas 2006, s. 158; *Analiza ryzyka*... 2009].

CORA (Cost-of-Risk-Analysis System) jest systemem opracowanym przez International Security Technology Inc. Współpracuje ze stosowanymi w organizacjach systemami zarządzania ryzykiem, importując z nich dane. Specjaliści od ryzyka definiują i przechowują parametry ryzyka jako pliki z zasadami ryzyka. Te zasady stanowią podstawę pracy dla personelu operacyjnego. Eksperci używają tego systemu do wykrycia i przechowywania danych na temat podatności dla wszystkich zagrożeń [*Analiza ryzyka*... 2009].

System COBRA (Consultative, Objective & Bifunctional Risk Analysis) służy do jakościowej i ilościowej analizy ryzyka oraz do oceny zgodności zastosowanych rozwiązań z omówionym wcześniej w artykule międzynarodowym standardem ISO/IEC 17996. Oprogramowanie dedykowane jest dla profesjonalistów w tej dziedzinie, a jego głównym elementem jest zestaw automatycznie generowanych wzorcowych formularzy i baza wiedzy. Podstawowe moduły systemu to moduł tworzenia kwestionariuszy, moduł przeglądu ryzyka/zgodności oraz generator raportów z przeprowadzonych analiz. System ten składa się z pięciu narzędzi: do analizy ryzyka (Risk Consultant), do oceny ryzyka (PC Security Consultant), do oceny zgodności zastosowanych rozwiązań z normą BS 7799 (BS 7799 Security Consultant), do analizy zgodności funkcjonowania organizacji z przyjętą w niej polityką bezpieczeństwa (Policy Compliance Analyst) oraz moduł wspomagający tworzenie i ocenę planu ciągłości działania (Continuity Consultant) [Białas 2006, s. 151-152].

Pakiet specjalistycznego oprogramowania MEHARI-Risk służy do przeprowadzenia szczegółowej analizy ryzyka SI. Spełnia on też wiele innych funkcji wspierających zarządzanie ryzykiem w organizacji, w tym planowanie kosztów oraz zapewnienie zgodności z przepisami. Metodą uzyskania kompletnych danych o systemie informatycznym, niezbędnych do wyznaczenia ryzyka dla tego systemu, jest audyt wewnętrzny. Wykonuje się go poprzez przygotowanie kwestionariuszy z pytaniami do odpowiednich osób. System automatycznie generuje kwestionariusze audytowe. Po wprowadzeniu do systemu wyników ankiet oprogramowanie automatycznie wyznacza ryzyko dla wszystkich wybranych dla danego systemu scenariuszy zagrożeń. Wynikiem działania programu jest m.in. kompleksowy raport, zawierający informacje zbiorcze, mogący stanowić dla kierownictwa podstawę do podejmowania decyzji w zakresie ograniczania ryzyka związanego z bezpieczeństwem systemów informatycznych [*MEHARI-Risk – Wielozadaniowy*... 2009].

Opracowany w Stanach Zjednoczonych przez firmę CSCI (Computer Security Consultants Inc.) pakiet RiskPAC służy do przeprowadzenia analizy ryzyka oraz określenia wpływu tego ryzyka na procesy biznesowe. Zastosowano w nim metodę ilościową i jakościową analizy ryzyka. Oprogramowanie zawiera narzędzie do projektowania kwestionariuszy (moduł Designer) oraz narzędzie do zarządzania przeglądem ryzyka z wykorzystaniem tych kwestionariuszy (moduł Survey Manager). Podstawą funkcjonowania programu jest proces udzielenia odpowiedzi na pytania sformułowane w kwestionariuszach, dotyczące organizacji, jej systemów informatycznych, sieci, sprzętu, oprogramowania, procesów biznesowych, zarządzania. Uzyskane informacje mogą zostać zaprezentowane w formie raportów, których wzorce znajdują się w bibliotece raportów. W systemie zawarto osobny moduł korekcji, przedstawiający na podstawie przeprowadzonej analizy zalecenia, których celem jest poprawienie poziomu bezpieczeństwa systemów informatycznych w organizacji [*Analiza ryzyka*... 2009].

6. Zakończenie

Podsumowując, należy podkreślić, iż korzyści wynikające z właściwego przeprowadzenia procesu zarządzania ryzykiem bezpieczeństwa systemów informatycznych w organizacji mogą być wielopłaszczyznowe. Odpowiednie podejście do problematyki zarządzania ryzykiem, polegające na wdrożeniu odpowiednich standardów, implementacji właściwych funkcji, mechanizmów zabezpieczających i kontrolnych, oraz komputerowe wsparcie tego procesu mogą znacznie zmniejszyć prawdopodobieństwo wystąpienia incydentów, które mogłyby negatywnie wpłynąć na organizację, a także mogą doprowadzić do obniżenia kosztów i przyczynić się do uzyskania przewagi nad konkurencją.

Literatura

Analiza ryzyka w zarządzaniu bezpieczeństwem informacji, Wyższa Szkoła Bezpieczeństwa i Ochrony, http://www.wsbio.waw.pl/attachments/063_analiza_ryzyka_informacji.ppt, 11.02.2009.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006.

CRAMM.com – Risk Assessment Tool /The total information security toolkit, http://www.cramm.com/, 22.05.2008.

Grzywak A., *Bezpieczeństwo systemów komputerowych*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.

ISO/IEC TR 13335, *Information Technology - Security Techniques - Guidelines for the management of IT Security*, Raport techniczny ISO 13335, 2005.

Jakubowski R., *Bezpieczeństwo w standardzie*, Raport ComputerWorld „Bezpieczeństwo danych w sieci", „ComputerWorld" 24.06.2002.

Korytowski J., *Praktyki kontrolne w zakresie zarządzania ryzykiem*, Materiały konferencyjne ISACA Kontrola'02, Bielsko-Biała 2002.

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

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

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

MEHARI-Risk – Wielozadaniowy System Analizy Ryzyka i Zarządzania Bezpieczeństwem Informacji, http://www.mehari-risk.pl, 10.02.2009.

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:] B. Kubiak, A. Korowicki (red.), *Zastosowanie informatyki w rachunkowości i finansach*, Polskie Towarzystwo Ekonomiczne, Gdańsk 2002.

Pańkowska M., *Zarządzanie zasobami informatycznymi*, Difin, Warszawa 2001.

Piotrowski M., *Zarządzanie ryzykiem*, cz. I. *Panowanie nad niepewnością*, http://www.e-ochronadanych.pl/a,184,zarzadzanie-ryzykiem-cz-i-.html, 17.06.2008.

Ryba M., *Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M*, rozprawa doktorska, Akademia Górniczo-Hutnicza w Krakowie, Kraków 2006.

Szczepankiewicz E., Szczepankiewicz P., *Zarządzanie ryzykiem informatycznym według międzynarodowych norm i standardów*, „Monitor Rachunkowości i Finansów" 2006, nr 11, http://www.mrf.pl/index.php?mod=m_artykuly&cid=89&id=36, 06.11.2008.

www.centrumbezpieczenstwa.pl, 28.06.2008.

RISK MANAGEMENT AS AN ELEMENT OF PROVIDING INFORMATION SYSTEMS SECURITY IN ORGANIZATIONS

Summary: The risks associated with the information systems security are becoming more common and have a variety of different forms. A technological change generates dependencies that cause an increase in diversity, complexity and quantity risk factors. In this context, information system security risk management is a very important process, which minimizes the probability of losses connected with threats. Information systems security risk management plays a very important role in almost all areas of modern organizations. It relies mainly on the identification of hazards and vulnerability, risk estimation and recommending additional security measures. The most important process in risk management is risk analysis, which main goal is to identify the system resources, to indicate the threats and risks and to estimate the probability of their occurrence and the losses. The article presents the issue of information systems security risk management, shows the simplified general model of this process according to the ISO/IEC TR 13335 standard. It focuses also on the revision and presentation of different standards and recommendations in this area. Different tools, computer programmes and packages supporting this process in organizations is also discussed.