INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 20 • 2011

ISSN 1507-3858

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

KWANTYFIKATYWNE I KWALIFIKATYWNE METODY ANALIZY RYZYKA NA POTRZEBY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W ORGANIZACJI

Streszczenie: Zarządzanie ryzykiem informatycznym odgrywa obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji. Wymaga ono rzetelnego i cyklicznego przeprowadzania kluczowego dla niego zadania, czyli analizy ryzyka. Celem niniejszego artykułu jest przedstawienie problematyki jednego z najistotniejszych etapów procesu zarządzania ryzykiem, jakim jest analiza ryzyka, zaprezentowanie zarówno ilościowego, jak i jakościowego podejścia do tego zagadnienia. Jako przykład metody kwantyfikatywnej w artykule zaprezentowano analizę ryzyka według metody Courtneya. Omówionym w artykule przykładem podejścia kwalifikatywnego jest analiza ryzyka na potrzeby bezpieczeństwa systemów informatycznych w organizacji według metodyki opracowanej przez NIST (National Institute of Standards and Technology).

Słowa kluczowe: bezpieczeństwo systemów informatycznych, zarządzanie ryzykiem, analiza ryzyka, metoda Courtneya, metodyka NIST.

1. Wstęp

Stosowanie technologii informacyjnych do realizacji zadań biznesowych zawsze jest obarczone ryzykiem. Ryzyko związane z szerokim zastosowaniem tych technologii w biznesie rośnie wraz ze zwiększaniem się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Dlatego też należy optymalnie dobierać różnorodne środki i metody zabezpieczeń, właściwie je stosować i wreszcie odpowiednio nimi zarządzać. Podstawą budowy i utrzymania systemu bezpieczeństwa w organizacji jest właściwie przeprowadzany proces zarządzania ryzykiem, którego głównym elementem jest analiza ryzyka. Analiza ryzyka obejmuje ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, autentyczności i niezawodności zasobów systemu informatycznego (SI). Metody analizy ryzyka wspierają dobór środków zmierzających do ograniczenia i kontroli ryzyka.

Celem niniejszego artykułu jest wprowadzenie do problematyki analizy ryzyka, przedstawienie zarówno idei ilościowych, jak i jakościowych metod realizacji

tego procesu. Jako przykład metody kwantyfikatywnej w artykule zaprezentowano analizę ryzyka według metody Courtneya. Omówionym w artykule przykładem podejścia kwalifikatywnego jest metodyka opracowana przez National Institute of Standards and Technology.

2. System pojęciowy ryzyka i 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. Termin „ryzyko" nie jest definiowany w sposób jednoznaczny, pojęcie to 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. W kontekście bezpieczeństwa SI ryzyko jest traktowane najczęściej 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. Ryzyko, definiowane przez normę PN-I-02000, to możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych. Jedną z najprostszych, a jednocześnie najlepiej oddających istotę tego terminu, jest definicja stowarzyszenia ISACA (Information Systems Audit and Control Association): „Ryzyko jest możliwością wystąpienia zdarzenia, które będzie miało niepożądany wpływ na organizację i jej systemy informatyczne" [ISACA – Standard 050.050.030… 2000].

W pracy [Stokłosa i in. 2001, s. 17] zdefiniowano, że bezpieczeństwo informacji „polega na ich ochronie, czyli zabezpieczeniu przed nieuprawnionym lub nieprawidłowym, przypadkowym bądź umyślnym ujawnieniem, modyfikacją lub zniszczeniem". Przez pojęcie „system bezpieczeństwa" należy rozumieć ogół środków, metod i procedur, mających na celu niedopuszczenie do zniszczenia, utraty, kopiowania, modyfikacji lub zdradzenia zasobów SI.

Bezpieczeństwo SI polega na takim jego zabezpieczeniu, aby dostępność, poufność, integralność, autentyczność i niezawodność jego zasobów osiągnęły optymalny poziom (por. [PN-I-02000]). Bezpieczeństwo jest zatem rozumiane w terminach następujących atrybutów:

- dostępność (*availability*) – oznacza niczym nieograniczoną możliwość korzystania z danych przez uprawnionych do tego użytkowników. Informacja powinna być zatem dostępna dla osób upoważnionych, w określonym miejscu, czasie i postaci (por. [Stokłosa i in. 2001, s. 18]);
- poufność (*security*) – oznacza niedostępność treści zawartej w danych dla wszystkich podmiotów nieuprawnionych do jej odczytania;

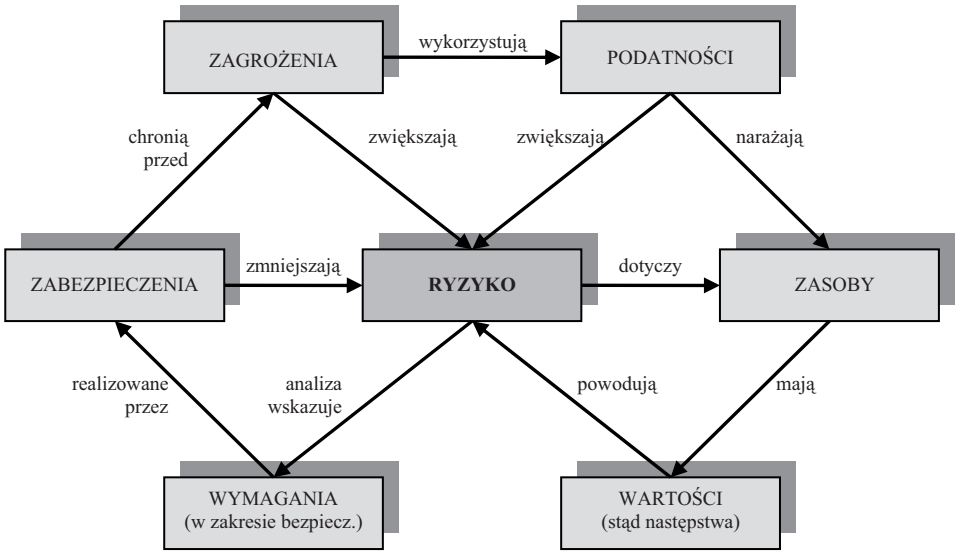
- integralność (*integrity*) – informacja w systemie nie może zostać zmieniona lub zniszczona przez osoby do tego nieupoważnione, a tym samym jej stan pozostanie zgodny z wymaganiami i oczekiwanym stanem właściwym.

Biorąc pod uwagę powyższe definicje, ryzyko w aspekcie bezpieczeństwa SI można rozpatrywać z punktu widzenia następujących kategorii [Ryba 2006, s. 13-14]:

- użyteczności (*relevance risk*) – w kategorii tej wyróżnia się ryzyko, że zebrane informacje nie są wykorzystywane lub okazują się nieprzydatne bądź aktualność otrzymanej i opracowanej informacji jest niewystarczająca;
- integralności (*integrity risk*) – ryzyko, że wykorzystywane dane i programy nie są wolne od błędów, nie zapewniają poprawności i kompletności informacji lub nie przedstawiają wiernie zdarzeń gospodarczych;
- poufności (*confidentiality risk*) – ryzyko dotyczy niedostępność treści zawartej w danych dla wszystkich podmiotów nieuprawnionych do jej odczytania;
- dostępności (*availability risk*) – ryzyko dotyczy ograniczenia możliwości korzystania z systemów i danych przez uprawnionych do tego użytkowników lub zachwiana zostanie zdolność systemów do przetwarzania danych na potrzeby kluczowych procesów w organizacji;
- adekwatność infrastruktury (*infrastructure risk*) – ryzyko, że kluczowe procesy informatyczne (zapewnienie działania systemów i sieci, zarządzanie bazami danych, zarządzanie bezpieczeństwem informacji itp.) nie zapewniają w sposób efektywny odpowiedniego wsparcia dla kluczowych potrzeb organizacji.

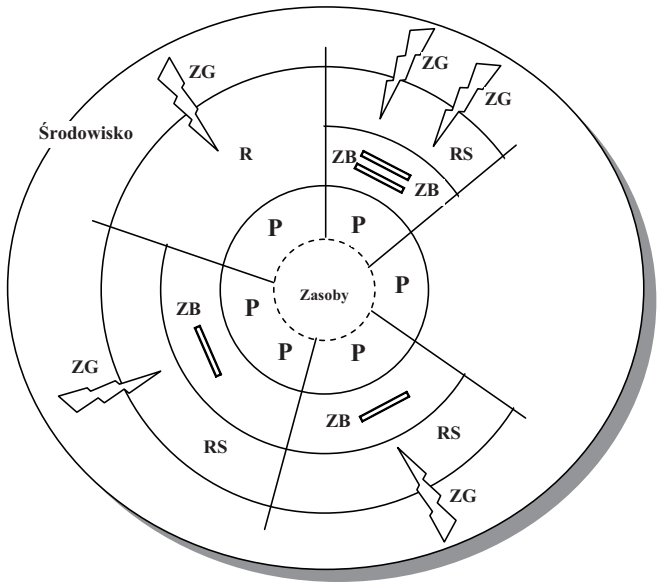
Wyżej wymienione kategorie ryzyka są rozszerzeniem o elementy biznesowe (właściwości użyteczności i adekwatności infrastruktury) atrybutów bezpieczeństwa informacji zdefiniowanych w standardzie BS 7799, opracowanym przez Brytyjski Instytut Normalizacyjny. Zalecenia te, opublikowane w „Code of Practice for Information Security Management", zostały poddane normalizacji przez ISO (Międzynarodowa Organizacja Normalizacyjna) oraz IEC (Międzynarodowa Komisja Elektrotechniczna), czego wynikiem jest norma o nazwie „Praktyczne zasady zarządzania bezpieczeństwem informacji" [PN ISO/IEC 17799], obecnie stopniowo zastępowana przez normy z serii ISO/IEC 27000. Istnieje też wiele innych standardów próbujących regulować tę problematykę. Międzynarodowy standard ISO/IEC TR 13335 zawiera wskazówki, od czego zależy wielkość ryzyka związanego z bezpieczeństwem SI: „(…) 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" [PN-ISO-13335; Liderman 2008, s. 70]. Powiązania między pojęciami z normy ISO/IEC TR 13335 zostały przedstawione na rys. 1 i 2.

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 2001 r. przez Bazylejski Komitet ds. Nadzoru Bankowego. Ryzyko to definiuje



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

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



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

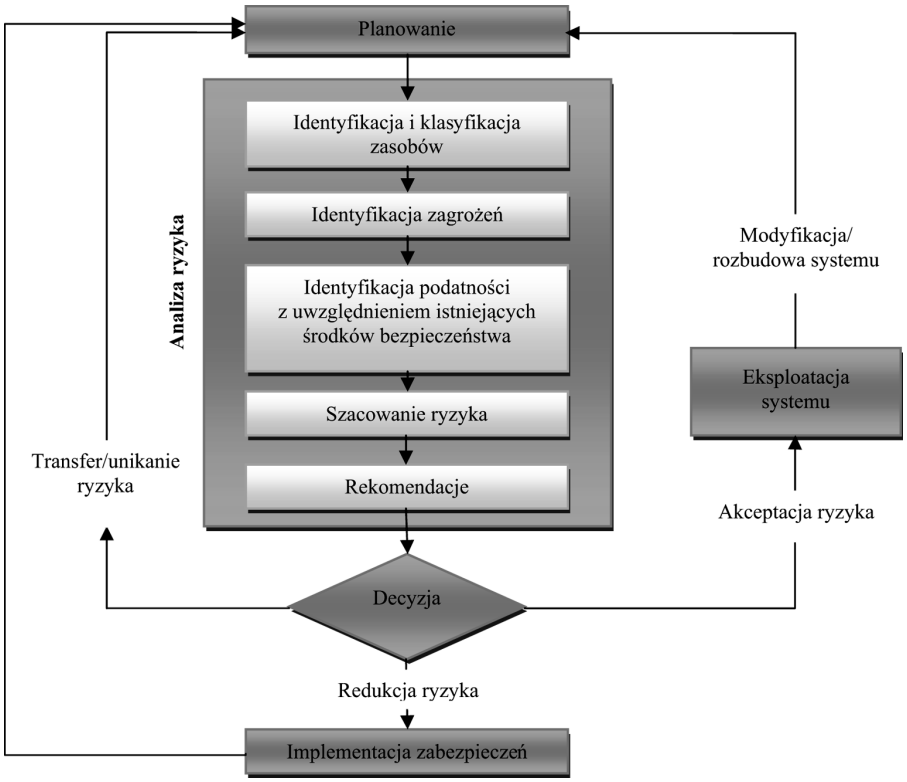
Rys. 2. Ryzyko, zasoby, ryzyko szczątkowe, zagrożenia i podatności w ujęciu standardu ISO/IEC TR 13335-1

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

się jako „ryzyko straty wynikającej z niewłaściwych lub zawodnych procesów, ludzi i systemów lub ze zdarzeń zewnętrznych". Do rodzajów ryzyka operacyjnego, które mogą wywoływać straty materialne, można zaliczy 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, co może wynikać z problemów z infrastrukturą sprzętową, programową czy telekomunikacyjną [Lewandowski 2004].

3. Zarządzanie ryzykiem w aspekcie bezpieczeństwa systemów informatycznych

Proces identyfikacji zagrożeń dla systemu, podatności jego zasobów, szacowania ryzyka oraz rekomendowania dodatkowych środków ochrony nazywa się zarządzaniem ryzykiem (*risk management*). Według polskiej normy PN-I-13335-1 zarządzanie ryzykiem jest jednym z kluczowych elementów procesu zarządzania bezpie-



Rys. 3. Uproszczony model zarządzania ryzykiem według standardu ISO/IEC TR 13335-3

Źródło: [PN ISO/IEC TR 13335-3].

czeństwem systemów informatycznych. Jego zasadniczym celem jest zmniejszenie ryzyka występującego w systemie. 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]:

- wskazanie, jak można uniknąć ryzyka, stosując rozwiązania organizacyjne techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji,
- utrzymanie optymalnego, ze względu na koszty i ograniczenia, stanu bezpieczeństwa,
- zminimalizowanie ryzyka szczątkowego, aby stało się ryzykiem akceptowalnym.

Uproszczony schemat modelu tego procesu, bazujący na przytoczonej już normie ISO/IEC TR 13335-3, został zaprezentowany na rys. 3.

Jak wynika z zaprezentowanego modelu, kluczowy element procesu zarządzania ryzykiem bezpieczeństwa SI stanowi analiza ryzyka, która pozwala na identyfikację zasobów systemu, zlokalizowanie odpowiadających im podatności i zagrożeń oraz oszacowanie prawdopodobieństwa ich wystąpienia i wielkości potencjalnych strat.

4. Analiza ryzyka

Analiza ryzyka to niewątpliwie kluczowy element procesu zarządzania bezpieczeństwem SI, a zatem i zarządzania ryzykiem. Głównym celem analizy ryzyka jest identyfikacja wszystkich elementów mających wpływ na bezpieczeństwo zasobów majątkowych, finansowych i informacyjnych instytucji, określenie ich podatności na zagrożenia, oszacowanie prawdopodobieństwa ich wystąpienia oraz wielkości potencjalnych strat. W wyniku przeprowadzonej analizy powinny zostać zaproponowane odpowiednie środki redukujące istniejące w danym środowisku informatycznym ryzyko do akceptowalnego poziomu [GIODO… 2009]. Typowy proces szczegółowej analizy ryzyka bezpieczeństwa informacji składa się z sześciu podstawowych etapów: identyfikacja i wycena zasobów, identyfikacja i ocena zagrożeń, identyfikacja i ocena podatności z uwzględnieniem istniejących zabezpieczeń, szacowanie ryzyka oraz opracowanie rekomendacji.

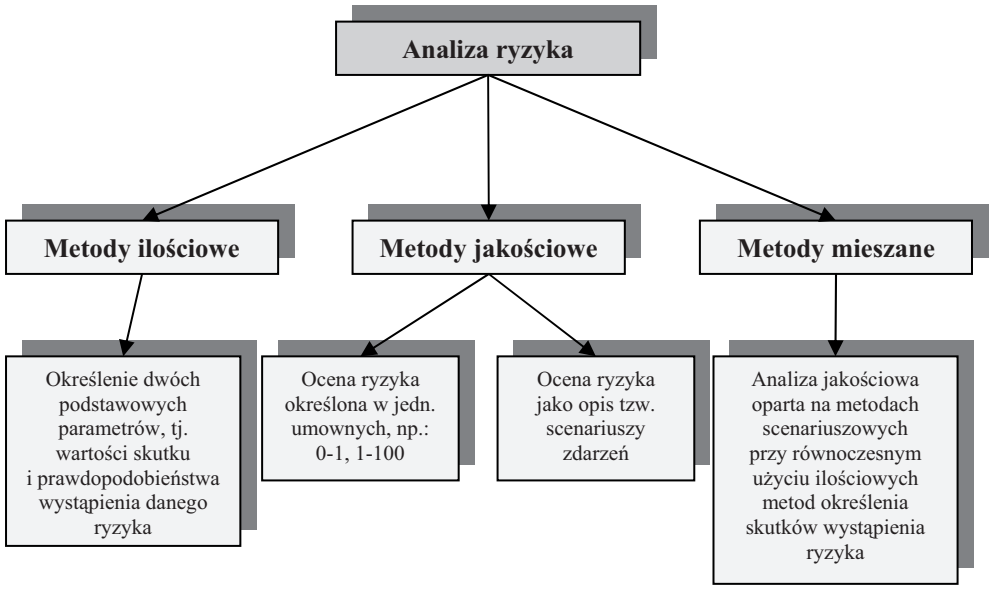
Analiza ryzyka skłania do wykonania prac w następujących obszarach [Pańkowska 2002, s. 283-284]:

- 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 – analiza zagrożeń powinna ustalać prawdopodobieństwo ich wystąpienia i możliwość zniszczenia zasobu,
- 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, jak też efektywność zabezpieczeń.

W teorii i praktyce stosowanych jest wiele metod analizy ryzyka na potrzeby bezpieczeństwa SI. Ogólnie można je podzielić na trzy grupy (rys. 4):

- metody kwantyfikatywne (ilościowe),
- metody kwalifikatywne (jakościowe),
- metody mieszane (ilościowo-jakościowe).



Rys. 4. Podział metod analizy ryzyka

Źródło: opracowanie własne na podstawie [Szczepankiewicz 2006; Łuczak 2009].

Metody kwantyfikatywne (ilościowe) opierają się na matematycznych obliczeniach wpływu zagrożenia na bezpieczeństwo systemu oraz prawdopodobieństwa jego wystąpienia. Operują wyłącznie na danych numerycznych, opracowanych na podstawie analizy danych statystycznych i historycznych. Oszacowanie wartości ryzyka wiąże się z wykorzystaniem miar liczbowych – wartość zasobów jest okre-

ślana kwotowo, częstotliwość wystąpienia zagrożenia – liczbą przypadków, a podatność – wartością prawdopodobieństwa ich utraty. Metody tego typu prezentują wyniki w postaci wskaźników. W metodach tych przy analizie ryzyka najważniejsze jest określenie dwóch podstawowych parametrów, tj. wartości skutku i prawdopodobieństwa wystąpienia danego zdarzenia. Skutki mogą być określone przez ocenę wyników zdarzeń lub przez ekstrapolację na podstawie danych z przeszłości [Łuczak 2009]. Przykładem ilościowych metod analizy ryzyka są metody: Courtneya, Fishera oraz Parkera. W dalszej części artykułu zostanie omówiona metoda Courtneya jako przykład ilościowej analizy ryzyka na potrzeby bezpieczeństwa systemów informatycznych.

Metody kwalifikatywne (jakościowe) są znacznie bardziej subiektywne, gdyż bazują na wiedzy i ocenie ekspertów. Wykorzystuje się w nich miary opisowe, które mogą mieć liczbowe odpowiedniki (np. 1 – ryzyko małe, 2 – ryzyko średnie itd.). Nie operują one na danych liczbowych, przedstawiając wyniki jedynie w postaci opisów, zaleceń. Oszacowanie ryzyka w takich przypadkach wiąże się z:

- opisem jakościowym wartości aktywów, określeniem skal jakościowych dla częstotliwości wystąpienia zagrożeń i podatności na dane zagrożenie,
- opisem tzw. scenariuszy zagrożeń poprzez przewidywanie czynników ryzyka.

Metody tego typu są często bardzo elastyczne i otwarte na wszelkiego typu modyfikacje. W analizie jakościowej wszelkie ryzyko i potencjalne skutki jego wystąpienia prezentowane są w sposób opisowy. Polega to na użyciu scenariuszy zdarzeń i określeniu skutków potencjalnych realizacji ryzyka. Mogą zawierać bardzo dużo szczegółów pomocnych do podjęcia konkretnych działań i wyboru odpowiednich zabezpieczeń. Powszechnie używane są różne skale utworzone do opisu konkretnych sytuacji i wszelkich wyjątków [Łuczak 2009]. Przykładem jakościowych metod analizy ryzyka są metody: CRAMM – CCTA *Risk Analysis and Management Metod*, STIR – *Simple Technique for Illustrating Risk*, RMF – *Risk Management Framework* firmy Microsoft, FRAP – *Facilitated Risk Analysis Process* oraz MEHARI – *Method for Harmonized Risk Analysis*. Analiza ryzyka realizowana przy zastosowaniu metod jakościowych wspomagana jest często przez narzędzia informatyczne [GIODO… 2009]. Zarówno metody ilościowe, jak i jakościowe mają swoje słabe strony i ograniczenia, które przedstawiono w tab. 1. Z uwagi na te liczne ograniczenia większość organizacji wykorzystuje kombinację dwóch powyższych podejść. Wobec tego stosowane są analizy jakościowe oparte na metodach scenariuszowych do identyfikowania wszystkich obszarów ryzyka i skutków, przy równoczesnym użyciu ilościowej analizy do określenia kosztów skutków wystąpienia ryzyka. **Metody mieszane** (ilościowo-jakościowe) wydają się być najbardziej efektywne, wymagają jednak dużej wiedzy i doświadczenia.

Prawidłowo przeprowadzony proces analizy ryzyka, a zwłaszcza poprawne oszacowanie ryzyka i ocena prawdopodobieństwa jego wystąpienia, daje jasny obraz jego wpływu na funkcjonowanie całego systemu informacyjnego w organizacji.

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 • Wyniki szacowania ryzyka mają swój wymiar finansowy i procentowy • Dają dokładniejszy obraz ryzyka • Szacowanie i wyniki są obiektywne i przez to mogą być porównywalne • Wartość informacji (dostępność, integralność, poufność) wyrażana jest w jednostkach pieniężnych	• Pozwalają uszeregować ryzyka według priorytetu • Pozwalają wyznaczyć w krótkim czasie i bez dużych środków obszary zwiększonego ryzyka • Analiza jest stosunkowo łatwa i tania, a kalkulacje i obliczenia (jeżeli występują) są proste i zrozumiałe • W większości przypadków nie jest konieczna wycena informacji (jej dostępności, poufności, integralności) • Nie jest konieczne ilościowe określenie skutków i częstotliwości wystąpienia zagrożeń • Nie jest konieczne, aby szacować koszt rekomendowanych sposobów postępowania z ryzykiem i wyliczać potencjalny zysk (stratę) • Ogólne wskazanie znaczących obszarów ryzyka, na które koniecznie trzeba zwrócić uwagę • Możliwość rozpatrywania i uwzględnienia przy szacowaniu takich aspektów, jak np. wizerunek firmy, kultura organizacyjna itp. • Możliwość zastosowania przy braku konkretnych informacji i danych ilościowych lub zasobów, które mogłyby być potrzebne przy metodach ilościowych
Wybrane wady i ograniczenia	• 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 • Kalkulacje są wykonywane całościowo, jeżeli nie zostały zrozumiane i wytłumaczone, kierownictwo może nie ufać wynikom etapu szacowania ryzyka • Stosowanie metod ilościowych jest niepraktyczne i nieefektywne, kiedy nie są używane zautomatyzowane narzędzia czy aplikacje informatyczne • Konieczne jest gromadzenie wymiernych informacji na temat środowiska IT, zabezpieczeń, zasobów	• 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; Łuczak 2009; Ozier 2004; ENISA… 2006].

5. Metoda Courtneya jako przykład ilościowej analizy ryzyka

Wśród metod ilościowych analizy ryzyka warto zwrócić uwagę na metodę Courtneya, opracowaną przez R. Courtneya z firmy IBM, opierającą się na szacowaniu potencjalnej straty jako iloczynu wartości strat związanych z wystąpieniem zagrożenia oraz wskaźnika określającego prawdopodobieństwo jego wystąpienia. Bazująca na pracach R. Courtneya metoda analizy ryzyka została zaprezentowana w publikacji Federal Information Processing Standards Publication – "*FIPS 65 – Guideline for Automatic Data Processing Risk Analysis*", w której ryzyko systemów informatycznych rozpatrywane jest w kontekście omówionych wcześniej w niniejszym artykule atrybutów bezpieczeństwa, takich jak: integralność, poufność i dostępność. Metoda ta została zaakceptowana przez instytucje państwowe Stanów Zjednoczonych jako oficjalna metoda analizy ryzyka.

W celu wyznaczenia wielkości ryzyka dla danego SI proponowany jest wzór na roczną oczekiwaną stratę ALE (*Annual Loss Exposure*), czyli wartość przewidywanych średnich rocznych strat wynikłych z wykorzystania podatności danego SI. Wartość ta jest wyrażaną w walucie wielkością wyznaczaną ze wzoru [Ryba 2006, s. 37]:

$$ALE = SLE \times ARO,$$

gdzie: *ARO* – roczny wskaźnik wystąpienia zdarzenia (*Annualized Rate of Occurance*) jest szacowaną częstotliwością wystąpienia zdarzenia powodującego daną stratę,

SLE – spodziewana jednorazowa strata (*Single Loss Expectancy*) jest wyrażoną w walucie wielkością przewidywanej straty wynikłej z jednokrotnego wystąpienia zdarzenia powodującego daną stratę – wielkość ta wyznaczana jest ze wzoru [Ryba 2006, s. 38]:

$$SLE = AV \times EF,$$

gdzie: *AV* – wartość zasobu (*Asset Value*) jest wyrażoną w walucie wartością zasobu, do którego odnosi się analizowane zdarzenie powodujące daną stratę,

EF – wskaźnik ekspozycji (*Exposure Factor*) określa procent wartości zasobu *AV*, jaka zostaje utracona w wyniku pojedynczego zdarzenia powodującego daną stratę.

Natomiast oczekiwana roczna strata wyraża się wzorem [Ryba 2005]:

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

gdzie: *f* – indeks określający szacowaną częstotliwość wystąpienia zdarzenia powodującego stratę,

i – indeks określający szacowaną wysokość straty spowodowanej wystąpieniem zdarzenia powodującego tę stratę.

W przedstawionym powyżej wzorze występują parametry *f* i *i*. Sposób ich wyznaczenia w metodzie Courtneya zaprezentowany został w tab. 2.

Tabela 2. Sposób wyznaczania parametrów *f* i *i* według metody Courtneya

Prawdopodobieństwo wystąpienia zdarzenia	Wartość parametru *f*	Rząd wielkości szacowanej straty	Wartość parametru *i*
Raz na 300 lat	1	10 PLN	1
Raz na 30 lat	2	100 PLN	2
Raz na 3 lata	3	1 000 PLN	3
Raz na 100 dni	4	10 000 PLN	4
Raz na 10 dni	5	100 000 PLN	5
Raz na dzień	6	1 000 000 PLN	6
10 razy dziennie	7	10 000 000 PLN	7
100 razy dziennie	8	100 000 000 PLN	8
1000 razy dziennie	9	1 000 000 000 PLN	9

Źródło: [Ryba 2005].

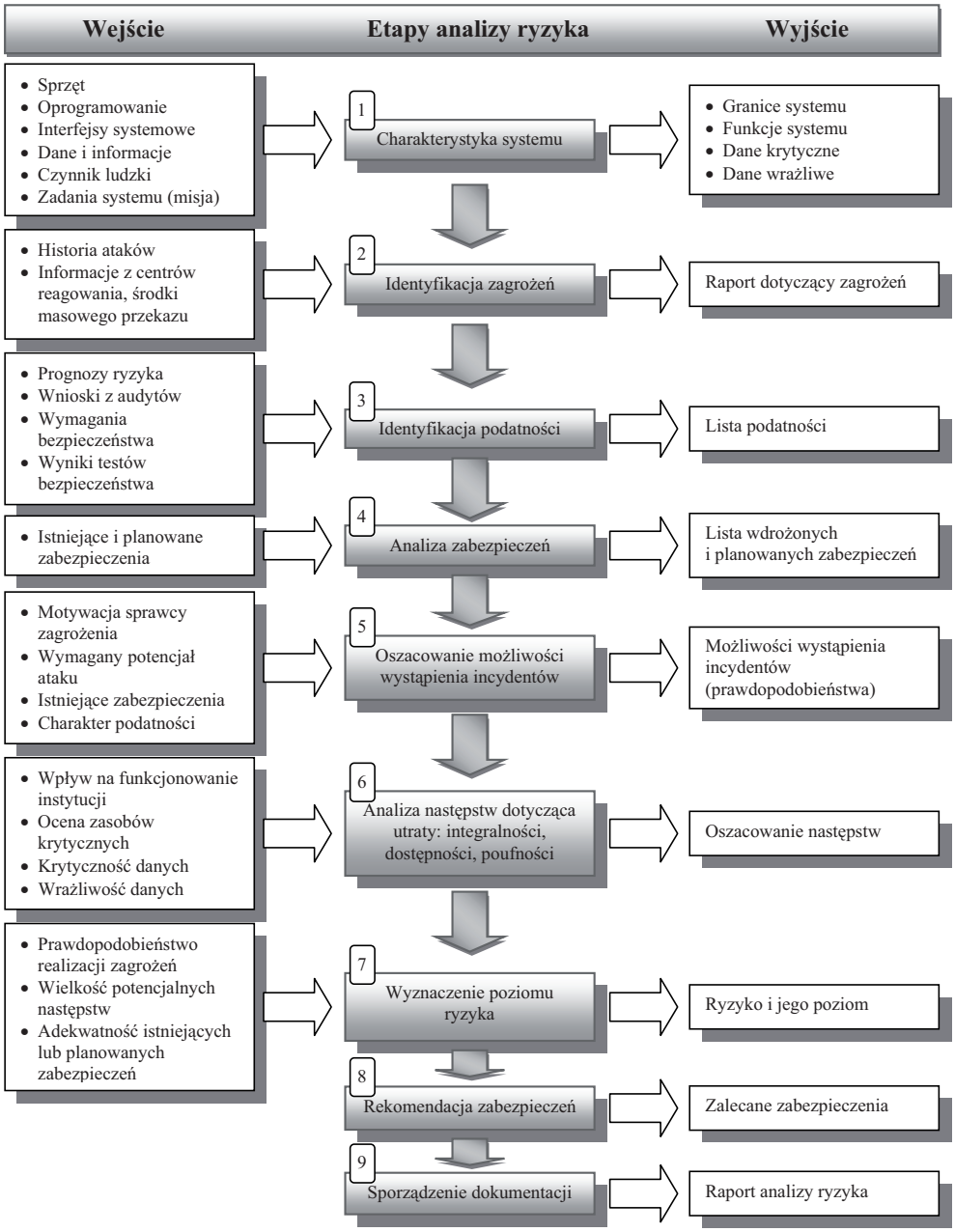
Przedstawiana metoda wyróżnia sześć zasadniczych grup zagrożeń: przypadkowe ujawnienie danych, przypadkowa modyfikacja danych, przypadkowe usunięcie danych, celowe ujawnienie danych, celowa modyfikacja danych, celowe usunięcie danych. Powszechność analizy ryzyka na podstawie metody Courtneya wynika z prostoty zastosowanego podejścia oraz łatwości i intuicyjności wyliczania wielkości *ALE*, a także z faktu, że było to jedno z pierwszych sformalizowanych podejść do analizy ryzyka, przyjęte jako standard rządowy w USA. Wadą metody jest znaczny subiektywizm wyznaczania wartości parametrów *f* i *i*.

6. Metodyka NIST jako przykład jakościowej analizy ryzyka

NIST (National Institute of Standards and Technology) opracował wytyczne dotyczące zarządzania ryzykiem na potrzeby bezpieczeństwa SI. Metodyka definiuje proces zarządzania ryzykiem w odniesieniu do całego cyklu życia systemu SDLC (*System Development Life Cycle*). Metodyka obejmuje trzy zasadnicze elementy: etap analizy ryzyka składający się z podstawowych 9 kroków, etap redukcji ryzyka oraz wskazanie wzorcowych praktyk działania.

Etap analizy ryzyka przedstawiono na rys. 5. Jak już wspomniano, składa się on z następujących 9 zasadniczych kroków [Ryba 2006, s. 41-42; Białas 2006, s. 110-117]:

1. Wybór systemów objętych oceną, określenie zakresu oceny, opracowanie charakterystyki wybranych systemów, gromadzenie informacji dotyczących środowiska



Rys. 5. Proces analizy ryzyka według metodyki NIST

Źródło: [Stoneburner i in 2002; Białas 2006, s. 111].

eksploatacji systemów. Identyfikacja podstawowych elementów mających wpływ na wielkość ryzyka.

2. Identyfikacja i stworzenie kompletnej listy zagrożeń odnoszących się do systemów informatycznych objętych przeprowadzaną oceną ryzyka.

3. Identyfikacja i stworzenie kompletnej listy podatności w objętych oceną systemach informatycznych, które mogą zostać wykorzystane przez zidentyfikowane uprzednio zagrożenia.

4. Analiza istniejących i planowanych mechanizmów kontrolnych i zabezpieczających, mających na celu minimalizację istotności potencjalnych zidentyfikowanych zagrożeń bądź ich całkowitą eliminację. Zabezpieczenia obejmują środki techniczne i pozatechniczne.

5. Określenie prawdopodobieństw wykorzystania podatności przez zidentyfikowane źródła zagrożeń. Może być stosowana skala o kilku poziomach, jak np.: wysoki, średni, niski.

6. Analiza następstw, określająca wpływ rozważanych potencjalnych zdarzeń na systemy, dane i organizację. Wielkość tego wpływu określona jest w trzystopniowej skali jako: wysoki (100), średni (50), niski (10).

7. Wyznaczenie ryzyka za pomocą macierzy ryzyka (*Risk-Level Matrix*) – zob. tab. 3. Na podstawie tej macierzy określany jest poziom całkowitego ryzyka dla każdego ze zidentyfikowanych zagrożeń jako: wysokie – dla iloczynu z przedziału (50, 100], średnie – (10, 50], niskie – [1, 10].

Tabela 3. Przykład macierzy ryzyka według metodyki NIST

Prawdopodobieństwo wystąpienia incydentu	Następstwa		
	niskie (10)	średnie (50)	wysokie (100)
Wysokie (1,0)	niskie $10 \times 1{,}0 = 10$	średnie $50 \times 1{,}0 = 50$	wysokie $100 \times 1{,}0 = 100$
Średnie (0,5)	niskie $10 \times 0{,}5 = 5$	średnie $50 \times 0{,}5 = 25$	średnie $100 \times 0{,}5 = 50$
Niskie (0,1)	niskie $10 \times 0{,}1 = 1$	niskie $50 \times 0{,}1 = 5$	niskie $100 \times 0{,}1 = 10$

Źródło: [Białas 2006, s. 115].

8. Opracowanie, z uwzględnieniem takich czynników, jak ograniczenia prawne, postanowienia polityki bezpieczeństwa, istniejące ograniczenia technologiczne, organizacyjne i finansowe, rekomendacji w zakresie zabezpieczeń oraz innych rozwiązań mających na celu minimalizację ryzyka systemów informatycznych do poziomu akceptowalnego przez organizację.

9. Przygotowanie dokumentacji zawierającej rezultaty przeprowadzonej analizy ryzyka systemów informatycznych w postaci raportu. Dokumentacja ta stanowi podstawę kolejnych decyzji podejmowanych w celu minimalizacji ryzyka.

7. Zakończenie

Problematyka bezpieczeństwa systemów informatycznych ma charakter złożony i interdyscyplinarny i jest obecnie niezwykle aktualna ze względu na pojawiające się nowe formy zagrożeń SI, ciągły postęp w zakresie nowoczesnych technologii informacyjnych, jak i metod, technik oraz narzędzi ich zabezpieczania. Ponadto każde naruszenie bezpieczeństwa może się stać przyczyną wymiernych strat finansowych, liczba zaś tego rodzaju zjawisk rośnie z roku na rok. Najważniejsze w skutecznym zarządzaniu systemem bezpieczeństwa powinno być odpowiednie zarządzanie ryzykiem. Analiza ryzyka, kluczowy etap procesu zarządzania ryzykiem, jest całościową identyfikacją zagrożeń i podatności aktywów systemu informatycznego oraz określeniem potrzeby ich kontrolowania lub akceptacji wyznaczonych mierników na wcześniej ustalonym poziomie. Celem analizy ryzyka jest dostarczenie informacji niezbędnej w podejmowaniu decyzji o zastosowaniu określonych metod, środków bezpieczeństwa w przedsiębiorstwie. Jak wskazano w artykule, w praktyce istnieją zarówno ilościowe, jakościowe, jak i mieszane metody przeprowadzania tego procesu w organizacjach. Korzyści wynikające z odpowiednio przeprowadzonej analizy ryzyka są wielopłaszczyznowe, gdyż mogą pomóc w utrzymaniu równowagi między stratami a kosztami zaimplementowanych zabezpieczeń, pomagają w planowaniu wydatków, wskazują zasadność lub brak podstaw do dodatkowych inwestycji w bezpieczeństwo systemów informatycznych, wskazują także na trendy w obszarze bezpieczeństwa.

Literatura

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

ENISA: *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, 2006, www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf.

GIODO – Generalny Inspektor Ochrony Danych Osobowych, *ABC przetwarzania danych osobowych w sektorze bankowym*, Warszawa 2009, www.giodo.gov.pl/plik/id_p/1430/j/pl/.

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.*

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 WAT 2006, nr 23.

Łuczak J., *Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001*, Zeszyty Naukowe Akademii Morskiej w Szczecinie nr 19(91), Szczecin 2009, http://www.wsm.szczecin.pl/userfiles/File/wydawnictwo/ZN_19/ZN_AM_19_91_Luczak.pdf.

Ozier W., *Risk Analysis and Assessment*, CRC Press LLC, 2004.

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.

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*, Polski Komitet Normalizacyjny 2007.

PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Polski Komitet Normalizacyjny 2007.

Ryba M., *Analiza i zarządzanie ryzykiem systemów informatycznych*, Ernst&Young 2005 http://www.mimuw.edu.pl/~sroka/archiwalne/2005ey/materialy/.

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

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

Stoneburner G., Goguen A., Feringa A., *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST), Computer Security Division, Information Technology Laboratory, 2002.

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

U.S. Department of Commerce, National Bureau of Standards, *Federal Information Processing Standards Publication 65: Guideline For Automatic Data Processing Risk Analysis*, 1 sierpnia 1979.

QUALITATIVE AND QUANTITATIVE INFORMATION SYSTEMS SECURITY RISK ANALYSIS METHODS IN AN ORGANIZATION

Summary: Risk management plays a very important role in almost all areas of contemporary organizations. It requires to carry out risk analysis in a reliable and recurring way. The purpose of this article is to present one of the most important steps in the process of risk management that is risk analysis. The article also presents both quantitative and qualitative approaches to this issue. As an example of quantitative method, the paper presents risk analysis according to the Courtney method. The method developed by NIST (National Institute of Standards and Technology) is presented as an example of qualitative approach to information systems security risk analysis.

Key words: Information systems security, risk management, risk analysis, Courtney method, NIST methodology.