PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 82
Informatyka Ekonomiczna 14 2009

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

KOMPUTEROWE NARZĘDZIA WSPOMAGANIA ANALIZY RYZYKA W ŚRODOWISKU INFORMATYCZNYM

Streszczenie: Zarządzanie ryzykiem informatycznym jest dyscypliną integrującą wiele różnorodnych technologii, metod i technik służących identyfikacji, analizie, ocenie incydentów i zagrożeń, a także wdrażania środków zwiększających bezpieczeństwo. Problematyka ta ma charakter złożony, interdyscyplinarny i jest obecnie niezwykle aktualna ze względu na pojawiające się nowe formy zagrożeń systemów informatycznych, ciągły postęp w zakresie technologii informacyjnych, jak również metod, technik oraz narzędzi ich zabezpieczania. Celem niniejszego artykułu jest wprowadzenie do problematyki zarządzania ryzykiem informatycznym, a szczególnie dokonanie przeglądu i charakterystyki wybranych komputerowych narzędzi wspierających ten proces w organizacjach.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, analiza ryzyka, zarządzanie ryzykiem, metodyki zarządzania ryzykiem.

1. Wstęp

Technologie informacyjne pozwalają osiągnąć organizacjom nową jakość funkcjonowania, jednocześnie rośnie stopień zdeterminowania sprawnego zarządzania nowoczesnymi, lecz bezpiecznymi rozwiązaniami teleinformatycznymi. W miarę postępu technologicznego, a szczególnie gwałtownego rozwoju Internetu, jak również wzrostu znaczenia informacji dla funkcjonowania przedsiębiorstw, ryzyko związane z funkcjonowaniem systemów informatycznych staje się coraz bardziej powszechne i przybiera różnorodne formy. Współczesne systemy informatyczne wykreowały nowe rodzaje ryzyka, a ich bezpieczeństwo nabrało wymiaru globalnego. Ryzyko związane z szerokim zastosowaniem technologii informatycznych w biznesie rośnie w miarę zwiększania się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Obecny postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i liczby czynników ryzyka. Brak odpowiedniego przygotowania na ryzyko może doprowadzić firmę do upadku, stąd też właściwe reagowanie na nie stanowi o możliwościach przetrwania i rozwoju przedsiębiorstwa. W tym kontekście bardzo istot-

nym procesem jest analiza ryzyka, służąca optymalizacji, a właściwie minimalizacji strat związanych z ryzykiem. Aby ułatwić i podnieść efektywność działań w tym zakresie, stworzono wiele metodyk i standardów wspomagających proces analizy i zarządzania ryzykiem informatycznym. Niejednokrotnie na bazie tych standardów i stworzonych na ich podstawie metodyk analizy ryzyka opracowano komputerowe narzędzia wspomagające. Służą one głównie do analizy ryzyka i zarządzania nim oraz do bieżącego utrzymywania określonego poziomu bezpieczeństwa w organizacjach. Celem niniejszego artykułu jest wprowadzenie do zagadnień ryzyka informatycznego, a szczególnie jego analizy, oraz zaprezentowanie wybranych narzędzi, programów i pakietów komputerowych wspomagających proces analizy ryzyka w przedsiębiorstwach.

2. Podstawy ryzyka systemów informatycznych

Potrzeba prowadzenia badań naukowych nad ryzykiem narodziła się w czasach nowożytnych, ale profesjonalnym pomiarem i kontrolą ryzyka zaczęto się zajmować dopiero w połowie ubiegłego wieku [Kaczmarek 2008, s. 23]. Ryzyko jest związane z każdą formą działalności człowieka. Ze względu na to, iż jest to zjawisko powszechne i bardzo złożone, stanowi trudną do definiowania i klasyfikacji kategorię [Krasodomska 2008, s. 13]. W związku z wszechobecnością jego występowania 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. Należy jednak pamiętać o tym, iż w różnych dziedzinach naukowych ryzyko jest postrzegane inaczej. Etymologia ryzyka nie została dotychczas jednoznacznie wyjaśniona. Według różnych źródeł słowo wywodzi się z języka łacińskiego, gdzie czasownik *risicare* znaczy omijać coś. Greckie „*riza*", podobnie jak włoskie „*ris(i)co*", oznacza rafę, którą statek powinien ominąć, a więc niebezpieczeństwo, którego powinien uniknąć [Kaczmarek 2008, s. 11-12; Krasodomska 2008, s. 13-14]. Termin ryzyka systemów informatycznych, określany często w literaturze przedmiotu jako ryzyko informatyczne, nie jest definiowany w sposób jednoznaczny, podobnie jak definicja samego ryzyka. Jak wskazano, termin „ryzyko" ma wiele odcieni znaczeniowych. W większości z nich jednak jest związany z pojęciem straty, co jest zgodne również z intuicyjnym rozumieniem tego pojęcia. Najogólniej jest to możliwość lub prawdopodobieństwo wystąpienia niekorzystnego w skutkach zdarzenia. Takie ujęcie ryzyka odpowiada jego znaczeniu w obszarze technologii informatycznych, gdzie jest rozpatrywana możliwość wykorzystania podatności przez zagrożenie w celu spowodowania niekorzystnych następstw dla systemów informatycznych, a co się z tym wiąże – także instytucji [Białas 2006, s. 75]. W kontekście bezpieczeństwa systemów informatycznych ryzyko systemów informatycznych najczęściej jest traktowane jako zbiorcza miara prawdopodobieństwa i wagi sytuacji, w której dane za-

grożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu, a zatem pośrednią lub bezpośrednią szkodę dla organizacji.

Dla potrzeb bezpieczeństwa systemów informatycznych można przytoczyć następującą definicję podaną w normie IEC 61508: „Ryzyko oznacza miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażoną jako iloczyn prawdopodobieństwa (lub możliwości) wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat)" [Liderman 2001]. Z kolei ryzyko informatyczne definiowane przez Polską Normę PN-I-02000 to możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych [Polska Norma PN-I-02000... 1998].

Jedną z najprostszych, a jednocześnie najlepiej oddającą istotę ryzyka systemów informatycznych jest definicja podana przez stowarzyszenie ISACA (Information Systems Audit and Control Association): „Ryzyko jest możliwością wystąpienia zdarzenia, które będzie miało niepożądany wpływ na organizację i jej systemy informatyczne" [ISACA… 2000].

Istnieje wiele innych standardów próbujących regulować tę problematykę. Na przykład międzynarodowy standard ISO/IEC TR 13335 zawiera pewne wskazówki, od czego zależy wielkość ryzyka związana z funkcjonowaniem systemów informatycznych: „… ryzyko jest funkcją wartości zasobów objętych ryzykiem, możliwości wystąpienia zagrożeń, łatwości wykorzystania podatności przez zagrożenia oraz istniejących (lub planowanych, gdy szacuje się ryzyko dla projektowanych systemów bezpieczeństwa) zabezpieczeń mogących zredukować ryzyko" [Polska Norma PN-I-13335… 1999; Liderman 2008, s. 70].

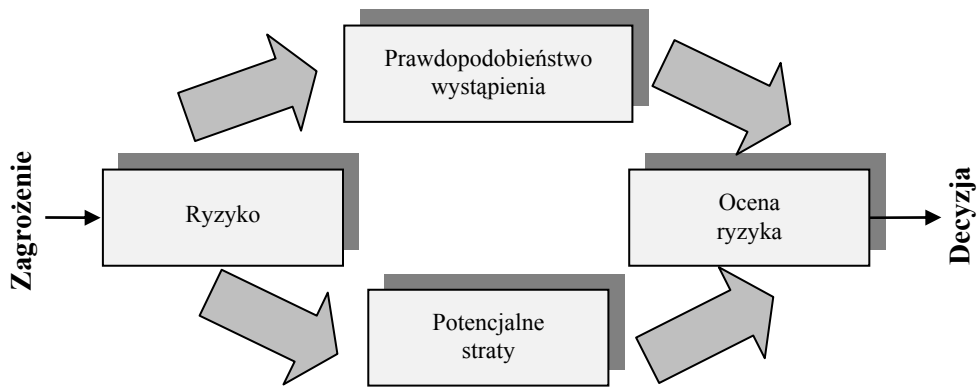
3. Analiza ryzyka informatycznego jako element zarządzania ryzykiem

Zarządzanie ryzykiem informatycznym odgrywa obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania współczesnych organizacji. Polega ono głównie na identyfikacji zagrożeń i podatności, szacowaniu ryzyka oraz wyborze określonych środków bezpieczeństwa.

Termin „analiza ryzyka" (*risk analysis*) w literaturze przedmiotu jest używany bardzo często, przy czym różni autorzy podają różny zakres przedsięwzięć składających się na proces analizy ryzyka. Generalnie analiza ryzyka polega na ocenie wszystkich negatywnych skutków badanego przedsięwzięcia i odpowiadających im prawdopodobieństw (częstości występowania) [Liderman 2001]. K. Liderman podaje najbardziej ogólną definicję analizy ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, formułując ją następująco: „Analiza ryzyka (dla potrzeb bezpieczeństwa teleinformatycznego) jest procesem identyfikacji (jakościowej i ilościowej) ryzyka utraty bezpieczeństwa teleinformatycznego" [Liderman 2001].

Analiza ryzyka to niewątpliwie kluczowy element procesu zarządzania ryzykiem. Publikacje związane z tą problematyką – zarówno krajowe, jak i zagraniczne

– wydają się jednak traktować ją w sposób dość dowolny. Przejawia się to w wielości definicji analizy ryzyka, a także w tym, iż często błędnie utożsamia się analizę ryzyka z zagadnieniem zarządzania ryzykiem. Analiza ryzyka jest głównym procesem zarządzania ryzykiem, identyfikuje i ocenia ryzyko, które ma być kontrolowane lub akceptowane. Analiza ryzyka obejmuje także ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, autentyczności i niezawodności zasobów systemu informacyjnego. Na rysunku 1 przedstawiony został ogólny model analizy ryzyka zaprezentowany w pracy [Szyjewski 2004, s. 232].



Rys. 1. Model analizy ryzyka

Źródło: [Szyjewski 2004, s. 232].

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 pomoże podjąć określone decyzje [Młynarski, Piechota 2001].

Analiza ryzyka dotyczy przeprowadzenia prac w następujących obszarach [Pańkowska 2001, 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, jak też efektywność zabezpieczeń.

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

– opis ryzyka (np. zniszczenie sprzętu, utrata danych, kradzież poufnych informacji),
– potencjalny skutek,
– szacunkowy koszt eliminacji skutków,
– prawdopodobieństwo wystąpienia zagrożenia,
– względne priorytety,
– 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. 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].

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 znacznych zmian w systemie.

Istnieje wiele metodyk analizy ryzyka. Wybór odpowiedniej z nich zależy od charakteru badanego obszaru, a także od obszaru dotyczącego zarządzania ryzykiem, tj. systemu bezpieczeństwa informacji. Do istotnych narzędzi identyfikujących ryzyko można zaliczyć [Wójcik 2009]:

- analizę środowiskową – ocenę wpływu zmian środowiska zewnętrznego na procesy zarządzania i kontroli w organizacji,
- scenariusze zagrożeń – symulowanie awarii i słabości systemu kontroli wewnętrznej,
- analizę potencjalnych strat – ocenę z punktu widzenia zasobów organizacji,
- identyfikację systemową – ocenę wpływów wszystkich możliwych do zidentyfikowania czynników ryzyka.

Podsumowując, można stwierdzić, iż zadaniem procesu analizy ryzyka jest wskazanie aktywów najbardziej zagrożonych w firmie (miejsc o relatywnie wyso-

kim prawdopodobieństwie wystąpienia zagrożenia), dzięki czemu wiemy, którymi aktywami należy się zająć w pierwszej kolejności i wdrożyć dla nich odpowiednie zabezpieczenia (fizyczne, techniczne, sprzętowe, programowe, kryptograficzne lub organizacyjne). Zatem analiza ryzyka jest zasadniczo głównym procesem zarządzania ryzykiem, identyfikuje ryzyko, które ma być kontrolowane, minimalizowane lub też akceptowane, i dokonuje jego oceny. Podstawowym celem analizy ryzyka jest dostarczenie informacji niezbędnej w podejmowaniu decyzji o zastosowaniu określonych metod, środków, narzędzi bezpieczeństwa w organizacji.

4. Wybrane systemy informatyczne we wspomaganiu procesu analizy ryzyka

Zarządzanie bezpieczeństwem systemów informacyjnych, szczególnie w dużych przedsiębiorstwach, jest niewątpliwie złożonym zadaniem, niosącym wiele trudności. Aby ułatwić i podnieść efektywność działań w tym zakresie, stworzono wiele metodyk i standardów wspomagających proces analizy i zarządzania ryzykiem informatycznym. Niejednokrotnie na bazie tych standardów i stworzonych na ich podstawie metodyk analizy ryzyka opracowywano komputerowe narzędzia wspomagające. Stopień skomplikowania współczesnych systemów informacyjnych wykonanie kompleksowej i zgodnej z odpowiednimi normami i przepisami analizy ryzyka czyni zadaniem niezwykle trudnym do realizacji, szczególnie bez wsparcia specjalistycznego oprogramowania. Systemy te dają niejednokrotnie możliwość automatyzacji procesu analizy ryzyka w systemach informacyjnych przedsiębiorstwa oraz przystępnej prezentacji jej wyników dla osób odpowiedzialnych za bezpieczeństwo informacji oraz dla kierownictwa organizacji. Służą one głównie do analizy i zarządzania ryzykiem oraz do bieżącego utrzymywania określonego poziomu bezpieczeństwa w organizacjach. Wśród tego typu rozwiązań znajdują się m.in. [Białas 2006, s. 106]:

- kwestionariusze, formularze, zestawienia,
- aplikacje biurowe,
- proste aplikacje użytkowe,
- zaawansowane, rozbudowane i kompleksowe oprogramowanie służące analizom, testom w obszarze systemu bezpieczeństwa,
- systemy ekspertowe,
- specjalistyczne oprogramowanie do modelowania i symulacji.

Jak już wspomniano, narzędzia te stanowią najczęściej implementację wybranych standardów i metodyk. Bardzo istotną grupę narzędzi informatycznych stanowią systemy do analizy ryzyka, służące do badania niebezpiecznych, hipotetycznych incydentów, a także systemy monitorowania bieżących zdarzeń w obszarze bezpieczeństwa informacji w organizacji, do których zaliczyć można np. skanery i testery bezpieczeństwa [Białas 2006, s. 106].

Do popularnych wśród profesjonalistów narzędzi analizy ryzyka należą m.in. następujące metodyki, na podstawie większości których powstały zautomatyzowane systemy wspomagania analizy ryzyka [Wójcik 2009; Pejaś 2009]:

1. CRAMM (*CCTA's Risk Analysis and Management Method*) – metoda realizująca wymagania norm przez analizę luk i opracowywanie programu poprawy bezpieczeństwa dzięki tworzeniu rejestru zasobów informacji, definiowaniu zakresu zarządzania bezpieczeństwem informacji oraz przez tworzenie dokumentacji wdrożonych środków zaradczych;

2. COBRA (*Control Objectives for Risk Analysis*) – pełna metodyka analizy ryzyka, zaprojektowana dla zarządu i kierownictwa organizacji do całościowej oceny profilu ryzyka związanego z prowadzoną działalnością, ze szczególnym uwzględnieniem bezpieczeństwa wizerunku jednostki, zgodności z obowiązującymi regulacjami prawnymi i ustawodawczymi, oraz do wewnętrznych mechanizmów kontrolnych;

3. MARION (*Mission Analysis and Risk Impact on Operations Net-work-tool*) – metodologia analizy ryzyka i oceny jego wpływu na funkcjonowanie instytucji, opracowana głównie dla środowisk bankowych i instytucji finansowych;

4. MEHARI (*Method for Harmonized Risk Analysis*) – metodyka realizująca zalecenia norm BS 7799 i ISO/IEC 13335 przy użyciu jednolitego systemu oszacowania ryzyka, prawidłowo dobranych zabezpieczeniach i właściwej lokalizacji zasobów;

5. EBIOS (*Expression des Besoins et Identification des Objectifs de Securite*) – to nie tylko metoda szacowania ryzyka, lecz również narzędzie wspomagające zarząd (służące do określania wymagań, definiowania zakresu badania).

6. COBIT (*Control Objectives for Information and related Technology*) – standard opracowany przez stowarzyszenie ISACA oraz IT Governance Institute. Stanowi zbiór dobrych praktyk z zakresu IT Governance, które mogą być wykorzystywane przede wszystkim przez audytorów systemów informatycznych; IT Governance to koncepcja dotycząca takiej organizacji strategii IT przedsiębiorstwa, która współgra ze strategią biznesową, zapewniając firmie osiągnięcie jej celów oraz wprowadzając dobre praktyki w zarządzaniu ryzykiem, a także w pomiarze wydajności technologii informatycznych. IT Governance koncentruje się na tym, aby procesy biznesowe przynosiły wymierne korzyści oraz aby funkcjonowanie technologii informatycznych odbywało się zgodnie z zasadą minimalizowania ryzyka.

7. PN – ISO/IEC 17799 (27005) – Polska norma opracowana na bazie międzynarodowego standardu dotyczącego praktycznych zasad zarządzania bezpieczeństwem informacji.

Tak jak wskazano powyżej, większość z tych popularnych metodyk doczekała się komputerowego wsparcia, a aplikacje te zostały stworzone na bazie tych właśnie norm, standardów czy dobrych praktyk. Przykładem takich systemów są następujące programy i pakiety informatyczne: CRAMM, Marion, CORA, Buddy System, COBRA, MEHARI-Risk, RiskPAC, VIR'94, MAGERIT czy system RISK Watch.

System CRAMM bazuje na wspomnianej wcześniej 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 systemów informatycznych według CRAMM składa się z następujących po sobie procesów [Ryba 2006, s. 44]:

- identyfikacja i wycena zasobów – w ramach których określany jest szczegółowy zakres analizy systemów informatycznych w odniesieniu do sprzętu, oprogramowania i danych przetwarzanych w tych systemach, dla każdego z objętych analizą zasobów następuje jego wycena, a także ocena istotności wpływu nieprawidłowości w funkcjonowaniu danego zasobu na organizację (określona w dziesięciostopniowej skali),
- ocena zagrożeń i podatności – jej celem jest określenie prawdopodobieństwa zajścia zdarzeń zakłócających prawidłowe funkcjonowanie zasobów, gdzie zidentyfikowane zasoby przydzielane są do grup zasobów (*asset groups*), dla których generowane są wykazy zagrożeń mogących dotyczyć danej grupy zasobów i wyznaczany jest w pięciostopniowej skali poziom ryzyka dla każdej z grup,
- wybór oraz rekomendacja mechanizmów kontrolnych i zabezpieczających – proces polegający na przygotowywaniu zestawienia zalecanych mechanizmów, których wdrożenie powinno zapewnić ograniczenie zidentyfikowanych uprzednio rodzajów ryzyka.

Największą różnicą CRAMM w stosunku do wielu innych metodyk analizy i zarządzania ryzykiem systemów informatycznych jest wykorzystanie dedykowanego oprogramowania, które jest integralnym elementem metodyki odpowiedzialnym za wsparcie wszystkich przedstawionych powyżej etapów i które to oprogramowanie podlega ciągłemu rozwojowi [http://www.cramm.com].

Obecna wersja systemu CRAMM jest oferowana i rozwijana przez firmę Insight. Jest to pakiet służący do analizy ryzyka i zarządzania nim , składający się z 3 części, a dodatkowo jest wspierany dużą biblioteką ankiet, kwestionariuszy i zaleceń. Pakiet powstał przy współpracy brytyjskich specjalistów rządowych i firmy BIS Applied System Limited. Jest zabezpieczony przed nieuprawnionym dostępem oraz utratą poufności baz danych, które są tworzone w trakcie realizacji zadań [*Analiza ryzyka w zarządzaniu…*]. .

Istnieją dwie podstawowe wersje tego systemu: uproszczona – „Express" oraz zaawansowana dla profesjonalistów – „Expert". Wersja „Express" funkcjonuje według następującego schematu [Białas 2006, s. 142-143]:

- użytkownik przypisuje wartości w przedziale 1-10 dla zidentyfikowanych zasobów, mając na względzie koszt ich odtworzenia w przypadku ich utraty,
- następuje wybór zagrożeń dotyczących organizacji z dostępnej biblioteki zagrożeń,
- wszystkim wybranym zagrożeniom oraz związanej z nimi podatności zasobów przypisuje się określone miary jakościowe, określające ich ważność,

- następuje automatyczne uruchomienie procesu generującego listę zalecanych środków bezpieczeństwa,
- użytkownik systemu otrzymuje trzy typy raportów: miar ryzyka, podsumowujący oraz szczegółowy,
- następuje zdefiniowanie bieżących statusów dla poszczególnych zabezpieczeń, wybór z dostępnych opcji statusu: zainstalowany, niezainstalowany, dyskutowany, niemożliwy do zastosowania itp.

Wersja „Expert", która w zasadzie dedykowana jest dla profesjonalistów, a szczególnie dla inspektorów bezpieczeństwa teleinformatycznego, jest rozszerzona w stosunku do omówionej powyżej wersji „Express" i zawiera analizator ryzyka, narzędzie wspomagające wdrożenie standardu BS 7799, bibliotekę zabezpieczeń, kreator raportów oraz narzędzie wspomagające proces opracowania planów awaryjnych. Praca z wersją „Expert" systemu CRAMM przebiega według następującego schematu: przygotowanie, analiza zasobów, analiza ryzyka, zarządzanie ryzykiem [Białas 2006, s. 143].

MARION jest pakietem opracowanym w Wielkiej Brytanii przez firmę Coopers & Lybrand i służy do analizy ryzyka w organizacjach komercyjnych. Pakiet opiera się na bibliotece aktualnie znanych incydentów, zawiera wiele ankiet i kwestionariuszy stosowanych do oceny rozwiązań w zakresie bezpieczeństwa. W analizie ryzyka zastosowano metodę zawierającą 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. Prezentacja wyników możliwa jest w formie zarówno numerycznej, jak i graficznej [Białas 2006, s. 158; *Analiza ryzyka w zarządzaniu…*].

CORA (*Cost-of-Risk-Analysis System*) jest systemem opracowanym ponad 30 lat temu przez International Security Technology, Inc. System ten współpracuje ze stosowanymi w organizacjach systemami zarządzania ryzyka, importując z nich dane. Specjaliści od ryzyka definiują i przechowują parametry ryzyka jako pliki z zasadami ryzyka (*risk rules*). Te zasady stanowią później podstawę pracy dla personelu operacyjnego. System CORA dostarcza strukturę umożliwiającą przechowywanie tych informacji. Oddzielnie przygotowuje się oszacowania potencjalnej straty dla wszystkich elementów organizacji oraz używa się systemu CORA do oszacowań. Eksperci używają tego systemu do wykrycia i przechowywania danych na temat podatności dla wszystkich zagrożeń [*Analiza ryzyka w zarządzaniu…*].

Buddy System używa w pełni automatycznego podejścia do zbierania informacji na temat stacji roboczych, serwerów, aplikacji, poszczególnych komputerów, dla których należy przeprowadzić analizę ryzyka. Centralnie zlokalizowany moduł służący do badań przeprowadza analizę podatności, tworzy scenariusze *what-if* – „co się stanie, jeżeli", analizę ryzyka oraz zarządza ryzykiem. Moduł generuje raporty – zawiera przygotowanych ponad 50 własnych wzorów zawierających informacje,

które można zastosować w wielu różnych sytuacjach, jak również pozwala tworzyć własne raporty dostosowane do konkretnych potrzeb przedsiębiorstwa. System zawiera analizę kosztów i spodziewanych strat, używając przede wszystkim metody ROI (*Return on Investments*). Od 1987 r. jest stosowany do oceny ryzyka w sieciach komputerowych, systemach oraz projektach o różnym poziomie złożoności [*Analiza ryzyka w zarządzaniu…*].

System COBRA (*Consultative, Objective & Bifunctional Risk Analysis*) służy zarówno do jakościowej, jak i ilościowej analizy ryzyka oraz do oceny zgodności zastosowanych rozwiązań z międzynarodowym standardem w zakresie zarządzania bezpieczeństwem informacji ISO/IEC 17996. Oprogramowanie dedykowane jest w zasadzie dla profesjonalistów w tej dziedzinie, a jego głównym elementem jest zestaw automatycznie generowanych wzorcowych formularzy i baza wiedzy. Podstawowe moduły systemu COBRA to moduł tworzenia kwestionariuszy, moduł przeglądu ryzyka/zgodności oraz generator raportów z przeprowadzonych analiz. System ten składa się z pięciu zasadniczych narzędzi [Białas 2006, s. 151-152]:

- narzędzie do analizy ryzyka (*risk consultant*),
- program do oceny ryzyka informatycznego (*PC security consultant*),
- moduł do oceny zgodności zastosowanych rozwiązań z normą brytyjską BS 7799 (*BS 7799 security consultant*),
- narzędzie do analizy zgodności funkcjonowania organizacji z przyjętą w niej polityką bezpieczeństwa (*policy compliance analyst*),
- moduł wspomagający tworzenie i ocenę planu ciągłości działania (*continuity consultant*).

Kolejny system to pakiet specjalistycznego oprogramowania o nazwie MEHARI-Risk, służący do przeprowadzenia szczegółowej analizy ryzyka systemu informacyjnego, bazujący na przytoczonej już metodologii analizy ryzyka w systemach informacyjnych MEHARI. MEHARI-Risk spełnia też wiele innych funkcji wspierających zarządzanie bezpieczeństwem informacji w przedsiębiorstwie, w tym planowanie kosztów oraz zapewnienie zgodności z przepisami. Metodą uzyskania kompletnych danych o systemie informacyjnym, niezbędnych do wyznaczenia ryzyka dla tego systemu, jest audyt wewnętrzny, czyli zbadanie tego systemu pozwalające na wyznaczenie jakości usług zabezpieczających. Wykonuje się go przez przygotowanie kwestionariuszy z pytaniami do odpowiednich osób mających styczność z badanym systemem informacyjnym [*MEHARI-Risk*…].

Metodologia MEHARI, zaimplementowana w oprogramowaniu MEHARI-Risk, pozwala na automatyzację procesu doboru pytań do ankiet. Dzięki odpowiedniemu i kompletnemu opisowi systemu informacyjnego, skorelowaniu funkcji i informacji tego systemu z zasobami oraz wskazaniu scenariuszy zagrożeń i wykorzystaniu odpowiednich macierzy korelacyjnych dobór pytań jest w tej metodologii automatyczny. System automatycznie generuje kwestionariusze audytowe. Po wprowadzeniu do systemu MEHARI-Risk wyników ankiet system automatycznie wyznacza ryzyko dla wszystkich wybranych dla danego systemu informacyjnego scenariuszy zagro-

żeń. Ostatecznym wynikiem działania systemu MEHARI-Risk w zakresie analizy ryzyka informacyjnego jest kompleksowy raport, który zawiera m.in. następujące informacje zbiorcze [*MEHARI-Risk*…]:

- relacje między informacjami a zasobami oraz między funkcjami a zasobami zachodzące w analizowanym systemie informacyjnym przedsiębiorstwa,
- wyniki audytu,
- graficzne prezentacje wyników analizy ryzyka (słupkowe, radarowe – mapy ryzyka),
- wyznaczenie ryzyka szczątkowego (*residual risk*), czyli takiego, które pozostaje po wprowadzeniu mechanizmów zabezpieczających.

Raport taki może stanowić dla kierownictwa przedsiębiorstwa podstawę do podejmowania decyzji w zakresie ograniczania ryzyka związanego z systemem informacyjnym, co stanowi klucz do prawidłowego zarządzania bezpieczeństwem informacji w przedsiębiorstwie. Jest też dokumentem wyjściowym do budowania systemu zarządzania bezpieczeństwem informacji zgodnego z międzynarodową normą ISO/IEC 27001. System MEHARI-Risk wspiera również i automatyzuje inne zadania związane z zarządzaniem bezpieczeństwem informacji, gdyż [*MEHARI-Risk*…].

- umożliwia badanie zgodności systemu informacyjnego z ISO/IEC 17799 – niezbędne do prawidłowego, zgodnego ze współcześnie obowiązującymi standardami międzynarodowymi zarządzania bezpieczeństwem informacji oraz do certyfikacji zgodności z normą ISO/IEC 27001,
- umożliwia badanie zgodności systemu informacyjnego np. z ustawą o ochronie danych osobowych oraz ustawą o ochronie informacji niejawnych itp.

Wśród innych ważnych i popularnych systemów wspomagających proces analizy ryzyka warto wymienić pakiet RISKPAC, VIR'94, MAGERIT czy system RISK Watch.

Opracowany w Stanach Zjednoczonych przez firmę CSCI (Computer Security Consultants Inc.) pakiet RiskPAC przygotowany jest do prowadzenia analizy ryzyka i określenia wpływu tego ryzyka na procesy biznesowe. Zastosowano w nim metodę ilościową i jakościową analizy ryzyka. Oprogramowanie RiskPAC zawiera:

- narzędzie do projektowania kwestionariuszy (moduł *Designer*),
- 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. Zestawy ankiet i kwestionariuszy pogrupowane są w cztery kategorie. Każda z nich tworzy oddzielny zbiór aktywów i zagrożeń podlegających szczegółowej ocenie. Poziomy ryzyka przedstawiane są i monitorowane dla każdej kategorii oddzielnie. W systemie zawarto osobny moduł korekcji, który na podstawie przeprowadzonej analizy przedstawia zalecenia, któ-

rych celem jest poprawienie poziomu bezpieczeństwa w organizacji [*Analiza ryzyka w zarządzaniu*].

Metodologia VIR'94 (niderl. *Voorschrift Infomatiebeyeiliging Rijkdienst*), łącznie z właściwym oprogramowaniem, zalecana jest przez oficjalne służby ochrony informacji Holandii jako dyrektywa działania. Stosować ją można na wszystkich szczeblach zarządzania, od jednostek administracji publicznej, przez różnego rodzaju instytucje, aż do przedsiębiorstw. Program ten stosuje metodę D&V (*Dependency & Vulnerability*), polegającą na podziale procesu analizy ryzyka na dwa zasadnicze etapy: etap D (*dependency*) – analiza stopnia uzależnienia organizacji od technologii informatycznych, oraz etap V (*vulnerability*) – analiza podatności [Białas 2006, s. 158].

MAGERIT (*Methodology of Risk Analysis and Management of Information Systems of Public Administrations*) to metodologia zalecana dla instytucji administracji publicznej. Zajmuje się ona następującymi trzema podstawowymi obszarami [Białas 2006, s. 159]:

- opisem metodologii analizy i zarządzania ryzykiem,
- przygotowaniem możliwie pełnej informacji i zgrupowaniem jej w bazie danych stanowiącej produkt wyjściowy do właściwej oceny ryzyka,
- programowaniem narzędziowym wspomagającym implementację metody.

Produkt obejmuje wszystkie fazy przetwarzania, przesyłania i przechowywania informacji w systemach informacyjnych.

Ostatnim omawianym systemem jest RISK WATCH, zalecany do stosowania w agencjach rządowych Stanów Zjednoczonych. W pakiecie zastosowano metodologię ilościowo-jakościową. Jest jednym z najbardziej rozbudowanych pakietów.

Zalety omówionych powyżej, a także innych informatycznych systemów wspomagania procesu analizy ryzyka w środowisku informatycznym to m.in. [*Analiza ryzyka w zarządzaniu*]:

- ustalone sposoby wprowadzania danych, łatwość dostępu i posługiwania się informacjami zapisanymi w bazie danych utworzonej do przeprowadzenia analizy,
- możliwość manipulowania danymi w celu zobrazowania wpływu i efektów różnych kombinacji zastosowania środków zabezpieczających i symulacji strat,
- możliwość szybkiego wprowadzania zmian do rozpoznawanego środowiska (aktywa i zasoby) oraz rozpoznanie wielkości ryzyka w instytucji.

5. Zakończenie

Problematyka analizy ryzyka w kontekście zarządzania bezpieczeństwem systemu informacyjnego w przedsiębiorstwie jest trudnym, złożonym oraz wciąż nierozpoznanym do końca zagadnieniem. Istnieje wiele podejść i metodyk mających na celu zidentyfikowanie i ocenę rodzajów ryzyka występujących w funkcjonowaniu systemu informacyjnego w organizacji. Jak wskazano w artykule, istnieje również wiele aplikacji, programów i pakietów wspomagających proces analizy ryzyka w środowi-

sku informatycznym. Wiele z nich opracowanych zostało na bazie popularnych, szeroko stosowanych międzynarodowych standardów i norm w zakresie zarządzania ryzykiem czy konkretnie jego analizy. Należy również podkreślić, iż z racji istnienia wielu standardów, a także rozwiązań informatycznych w omawianym obszarze, wybór konkretnego systemu nie jest zadaniem prostym i powinien odbyć się po zdefiniowaniu kryteriów wymagań, wybraniu zespołu do oceny narzędzi, przygotowaniu listy ocenianych punktów, przedstawieniu propozycji oprogramowania wykorzystywanego w analizie ryzyka oraz ocenie aplikacji.

Literatura

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

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

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

ISACA – Information Systems Audit and Control Association – *Standard 050.050.030 – IS Auditing Guideline – Use of Risk Assessment in Audit Planning*, ISACA, 2000.

ISO/IEC TR 13335-1 *Information Technology – Security Techniques – Guidelines for the management of IT Security – Part 1: Concepts and models of IT Security.*

ISO/IEC TR 13335-3 *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security.*

Kaczmarek T.T., *Zarządzanie zdywersyfikowanym ryzykiem w świetle badań interdyscyplinarnych*, Wydawnictwo Wyższej Szkoły Zarządzania i Marketingu, Warszawa 2008

Krasodomska J., *Zarządzanie ryzykiem operacyjnym w bankach,* Polskie Wydawnictwo Ekonomiczne, Warszawa 2008.

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

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

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

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

Pejaś J., *Wprowadzenie do zabezpieczeń: rola zabezpieczeń, typy zabezpieczeń, pojęcia i definicje*, 2009, http://kio.wi.zut.edu.pl/pobierz-pliki/doc_download/46-oi-wprowadzeniedozabezpieczen.pdf .

Polska Norma PN-I-02000 – *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*, Polski Komitet Normalizacyjny, 1998.

Polska Norma PN-I-13335 – *Zarządzanie zabezpieczeniami systemów informatycznych*, Polski Komitet Normalizacyjny, 1999.

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

Szyjewski Z., *Metodyki zarządzania projektami informatycznymi*, Wydawnictwo Placet, Warszawa 2004.
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001*, http://www.zabezpieczenia.com.pl/20080717664/artykuly/ochrona_informacji/, 2009.

COMPUTER TOOLS SUPPORTING RISK ANALYSIS IN INFORMATION TECHNOLOGY ENVIRONMENT

Summary: Information technologies allow organizations to achieve new performance, but these technologies increase also the degree of dependence of the proper management on modern but secure ICT solutions. The risks associated with the functioning of information systems are becoming more common and have a variety of different forms. The risk connected with a wide application of information technologies in business is increasing with increasing interdependency of the organization from its customers, business partners and outsourcing operations. Technological change generates dependencies that cause an increase in diversity, complexity and quantity risk factors. The lack of adequate preparation for risks may lead to the collapse of the company and therefore appropriate preparation for the risks gives opportunities for the survival and development of an enterprise. In this context, risk analysis is a very important process, which minimizes the probability of losses. To facilitate and improve the effectiveness of risk analysis process, a number of methodologies and standards of risk analysis and management have been elaborated. Many different computer tools have been developed on the basis of these risk analysis methodologies and standards. They are used primarily for risk analysis and management and to maintain the current level of security in specific organizations. The article presents the issue of one of the most significant stages of risk management which is IT risk analysis, especially focusing on the presentation of different tools, computer programmes and packages supporting the risk analysis process in enterprises.