Scientific Journals
Maritime University of Szczecin

Zeszyty Naukowe
Akademia Morska w Szczecinie

2009, 19(91) pp. 63–70

2009, 19(91) s. 63–70

Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001

Risk assesment methods – ISO/IEC 27001 information security managament system's key element

Jacek Łuczak

Uniwersytet Ekonomiczny w Poznaniu, Katedra Znormalizowanych Systemów Zarządzania, 61-875 Poznań, al. Niepodległości 10, e-mail: jacek.luczak@ue.poznan.pl

Słowa kluczowe: SZBI, ISO / IEC 27001, szacowanie ryzyka, zarządzanie ryzykiem

Abstrakt
Artykuł podejmuje temat systemowego zarządzania bezpieczeństwem informacji (SZBI), skupia się na jego kluczowym aspekcie – metodach szacowania ryzyka. W pierwszej części zdefiniowane zostało ryzyko, szacowanie ryzyka oraz zarządzanie ryzykiem w ISMS, a następnie dokonano przeglądu metod szacowania ryzyka. Praktycznym problemem projektowania i implementacji ISMS jest dobór metody, która będzie adekwatna do danej organizacji, a w efekcie da najlepsze podstawy dla ustanowienia rozwiązań systemowych, w szczególności pozwoli na dobór najbardziej odpowiednich zabezpieczeń.

Key words: ISMS, ISO / IEC 27001, risk assesment, risk management

Abstract
The article presents the subject of the information security management system (ISMS) and it concentrates on the key aspect – the methods of estimating the risk. There are the risk, assessing the risk and risk management definitions in the first part; The review of the methods of estimating the risk was executed then. The selection of the method, to find the most adequate to the organization is the main problem in practical aspect of designing and implementing ISMS. It is really basis to designing solutions and controls to protect information in a system way.

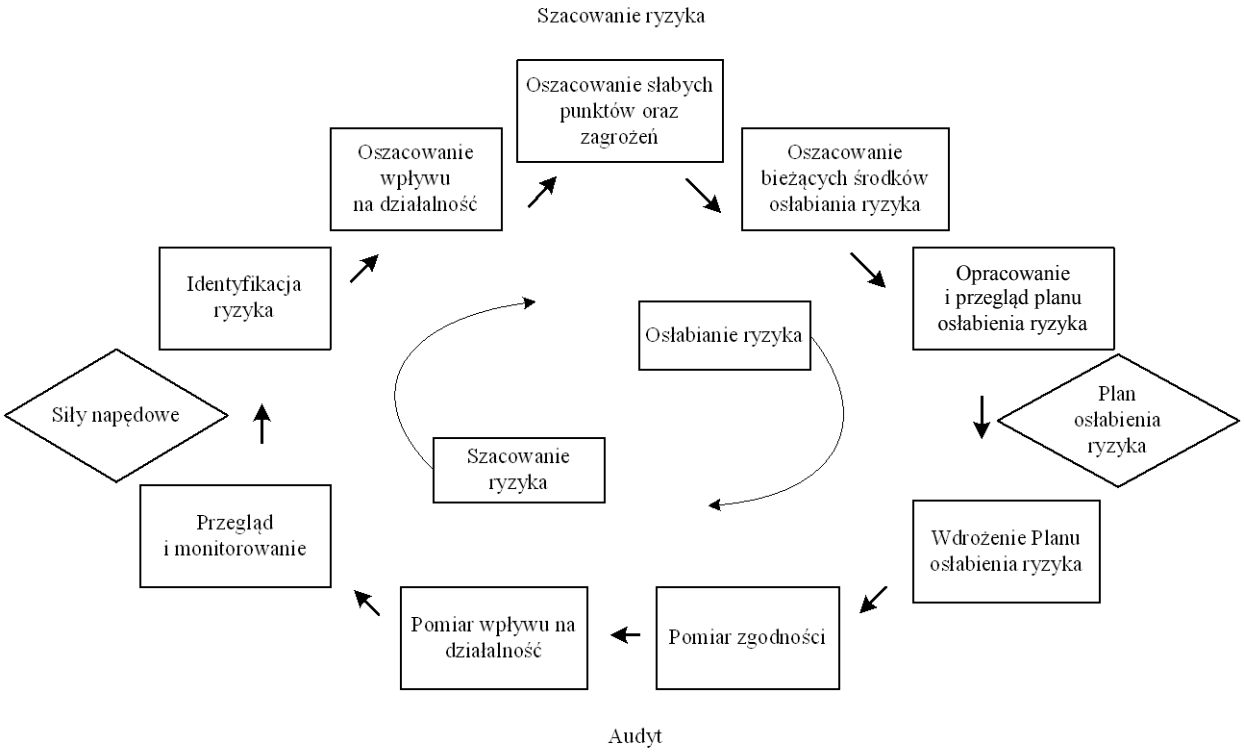
Wstęp

Artykuł dotyczy zarządzania ryzykiem bezpieczeństwa informacji w ujęciu systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001:2005[1]. Jest to przegląd i próba kompleksowego ukazania złożoności współcześnie występujących zagadnień odnośnie bezpieczeństwa informacji w ujęciu organizacji i procedur. Podstawowym celem pracy jest przegląd aktualnie stosowanych metod, koncepcji w ramach systemowego zarządzania bezpieczeństwem informacji według najbardziej powszechnego standardu ISO/IEC 27001: 2005[2] w oparciu o proces szacowania ryzyka bezpieczeństwa informacji.

W praktyce gospodarczej kompleksowa dbałość o bezpieczeństwo informacji jest zagadnieniem nowym, jednak skala i zakres problemów powstających w wyniku nieuwzględniania ryzyk wynikających m.in. z utraty aktywów informacyjnych nie może zostać niezauważona.

[1] ISO (Międzynarodowa Organizacja Normalizacyjna) i IEC (Międzynarodowa Komisja Elektrotechniczna) tworzą system normalizacji międzynarodowej.

[2] Por. także: Information Security Forum's (ISF) – The Standard of Good Practice for Information Security; ISO/IEC 27002 Information Technology – Security Techniques – Code of practice for information security management, ISO, 2005.



Rys. 1. Ogólna struktura zarządzania ryzykiem w ISMS [3, s. 50]
Fig. 1. The general structure of the risk management in ISMS [3, p. 50]

Liczba przeprowadzonych dotychczas w Polsce akredytowanych certyfikacji systemu zarządzania bezpieczeństwem informacji jest jeszcze stosunkowo niewielka w porównaniu np. do innych wiodących znormalizowanych systemów zarządzania[3]. Wynika to przede wszystkim ze złożoności samego zagadnienia systemowego zarządzania bezpieczeństwem informacji, nakładów jakie trzeba ponieść, ale także z niedostatecznej świadomości menedżerów. Na świecie zaobserwować można jednak dynamiczny wzrost liczby wydanych certyfikatów w tym zakresie. W naszym kraju jednostki certyfikujące ciągle jeszcze zbierają doświadczenia, kształcą asesorów i audytorów wiodących. Uczą się tak przedsiębiorstwa, jak również jednostki doradcze i certyfikujące.

Artykuł koncentruje się wokół procesu szacowania ryzyka – osnowy zarządzania bezpieczeństwem informacji; ma za zadanie ukazać całe spektrum teoretycznych koncepcji, praktycznych metod i podejść do szacowania ryzyka bezpieczeństwa informacji. Scharakteryzowane zostały w nim metody mające zastosowanie w procesie szacowania ryzyka (ISO TR 13335-3, ISO 31000, CRAMM, FMEA, MEHARI, OCTAVE).

[3] Wg The ISO Survey Certifications 2007, ISO, 2008 – certyfikaty ISO 9001 – 9184; ISO 14001 – 1089; ISO/TS 16949 — 392; ISO/IEC 27001 – 45.

Zarządzanie ryzykiem bezpieczeństwa informacji

Zarządzanie ryzykiem to proces szacowania ryzyka, mający na celu ograniczenie go do akceptowalnego poziomu. Powinien składać się z następujących faz: planowania, nabywania, rozwoju, testowania, odpowiedniego rozmieszczenia systemów informatycznych [1].

Według A. Zoła [2] zarządzanie ryzykiem (*risk management*) to całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego. Natomiast analiza ryzyka (*risk analysis*) to proces identyfikacji ryzyka, określania jego wielkości i identyfikowania obszarów wymagających zabezpieczeń.

M.E. Whitman zwraca uwagę na wzajemną relację pomiędzy szacowaniem ryzyka a jego osłabieniem – co stanowi istotę zarządzania ryzykiem [3].

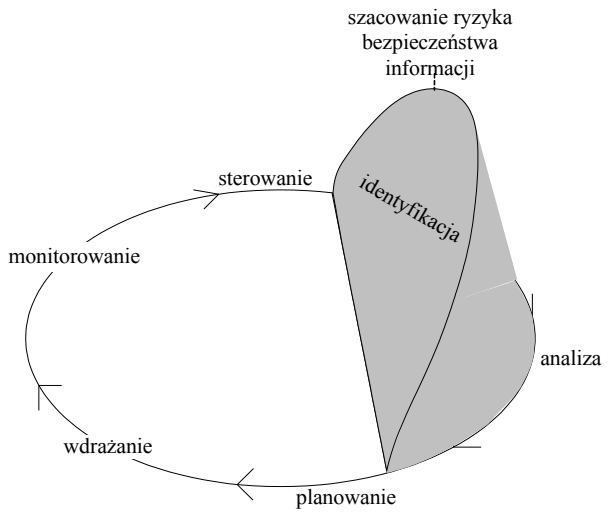
M.E. Whitman [3] wymienia następujące etapy zarządzania ryzykiem:

1) identyfikacja ryzyka,
2) oszacowanie wpływu na działalność,
3) oszacowanie słabych punktów i zagrożeń,
4) oszacowanie bieżących środków osłabienia ryzyka,

5) opracowanie i przegląd planu osłabienia ryzyka,
6) wdrożenie planu osłabienia ryzyka,
7) pomiar zgodności,
8) pomiar wpływu na działalność,
9) przegląd i monitorowanie.

Zgodnie z PN-I-13335-1:1999[4] zarządzanie ryzykiem jest rozumiane jako całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego [4].

Takie podejście ilustruje także Ch. Alberts oraz A. Dorofee [5], wykorzystując zmodyfikowaną spiralę jakości (PDCA).



Rys. 2. Ocena ryzyka w procesie zarządzania ryzykiem bezpieczeństwa informacji [5, s. 11]
Fig. 2. The risk assesment in the information security risk management process [5, p. 11]

W ujęciu modelowym celem procesu zarządzania ryzykiem jest ograniczenie ryzyka do akceptowalnego poziomu przez opracowanie odpowiedniego planu postępowania z nim. Założeniem wpisanym w ten model jest to, że działania realizowane za pomocą planu są skuteczne i wykonywane w sposób ciągły i systematyczny (monitoring, przeglądy).

Ogólna charakterystyka metod szacowania ryzyka bezpieczeństwa informacji

W teorii i praktyce stosowanych jest kilkadziesiąt metod szacowania i oceny ryzyka bezpieczeństwa informacji. Ogólnie można je podzielić na 3 grupy:

1) metody ilościowe,
2) metody jakościowe,
3) metody mieszane.

Podejście jakościowe

Jakościowe szacowanie ryzyka jest najczęściej subiektywną oceną, opartą na dobrych praktykach i doświadczeniu. Wynikiem takiego szacowania są listy zagrożeń wraz z relatywnym rankingowaniem ryzyka (niskie, średnie, wysokie). Metody te są bardzo elastyczne i otwarte na wszelkiego typu modyfikacje. Umożliwiają dzięki temu dostarczenie organizacji szybko i kosztowo efektywne wyniki w zakresie identyfikacji zagrożeń i stosowania zabezpieczeń. Jednak dzięki właśnie tej elastyczności, zakres i koszt szacowania może się bardzo różnić. Dlatego w zależności od dostępnych środków przewidzianych w budżecie, zakres szacowania ryzyka może się zmieniać w czasie.

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.

Korzyści z użycia metod jakościowych:

kalkulacje i obliczenia (jeżeli występują) są proste i zrozumiałe;

- w większości 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 konieczne jest zwrócenie uwagi [6];
- 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 [7].

Metody ilościowe

W podejściu ilościowym przy szacowaniu ryzyka najważniejsze jest określenie dwóch podstawowych parametrów, tj. wartości skutku i prawdopodobieństwa wystąpienia danego ryzyka.

[4] PN-I-13335-1:1999 jest polskim tłumaczeniem standardu wydanego przez Międzynarodową Organizację Normalizacyjną (*International Standard Organization*) oraz Międzynarodową Komisję Elektrotechniczną (*International Electrotechnical Commission*) pod nazwą ISO/IEC TR 13335-1.

Skutki mogą być określone przez ocenę wyników zdarzeń lub przez ekstrapolację na podstawie danych z przeszłości. Konsekwencje mogą być wyrażone w różnych kategoriach (pieniężnie, technicznie, operacyjnie, zasoby ludzkie).

Jakość całej analizy zależy od dokładności wskazanych wartości i statystycznej walidacji użytego modelu [7].

Korzyści z użycia metod ilościowych:

- szacowanie i wyniki są obiektywne i przez to mogą być porównywalne;
- wartość informacji (dostępność, integralność, poufność) wyrażana jest w pieniądzu;
- wyniki szacowania ryzyka są określane w języku zarządu, mają swój wymiar finansowy i procentowy.

Ograniczenia metod ilościowych:

- kalkulacje są wykonywane całościowo, jeżeli nie zostały zrozumiane i wytłumaczone kierownictwo może nie ufać wynikom z szacowania ryzyka, traktując je jako rezultat tzw. czarnej skrzynki;
- stosowanie metod ilościowych jest niepraktyczne i nieefektywne, kiedy nie używane są zautomatyzowane narzędzia czy aplikacje informatyczne;
- konieczne jest gromadzenie wymiernych informacji na temat środowiska IT, zabezpieczeń, zasobów [6].

Metody mieszane

Zarówno metody ilościowe, jak i metody jakościowe mają swoje słabe strony: są zbyt ogólne, niedokładnie identyfikują wszelkie potrzeby w zakresie bezpieczeństwa informacji, nie dostarczają informacji na temat analizy kosztowej w zakresie wprowadzenia nowych zabezpieczeń. Z tego względu większość przedsiębiorstw wykorzystuje kombinację tych dwóch podejść. 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.

Wytyczne do szacowania ryzyka określone w ISO/IEC 27001:2005

Opisany w poprzednim rozdziale model procesu szacowania ryzyka bezpieczeństwa informacji jest wzorcowym ujęciem omawianego zagadnienia, propagowanym i opisanym przez standard ISO/IEC 27001:2005. Opisane są w nim elementy, które powinny się znaleźć przy konstruowaniu metody szacowania ryzyka, natomiast nie jest wyjaśnione jaki konkretny kształt ma przyjąć ostatecznie metoda. Podejście to jest korzystne z tego względu, że norma bezpieczeństwa nie narzuca organizacji stosowania konkretnej jednej metody, dając w ten sposób swobodę wyboru. Jest to uzasadnione przede wszystkim różną wielkością zatrudnienia w organizacji, specyfiką prowadzonej działalności, obszarem działania, strukturą zatrudnienia itp.

Norma nakazuje jednak wskazanie konkretnej metody szacowania ryzyka[5]. Ma to przede wszystkim zagwarantować, że metodyczne podejście do szacowania ryzyka pozwoli na porównywanie wyników w czasie, jak również na powtarzalność rezultatów. Konieczne jest, aby dodatkowo opracować kryteria akceptacji ryzyka i określić akceptowalne poziomy ryzyk. Obecnie istnieją różne metody szacowania ryzyka, które zostały opublikowane i są powszechnie wykorzystywane przez organizacje. Oczywiście możliwe jest stosowanie też metod indywidualnych opracowanych na podstawie własnych doświadczeń. W niniejszym rozdziale zostaną zaprezentowane najbardziej znane metody szacowania ryzyka bezpieczeństwa informacji.

Szacowanie ryzyka wg ISO/IEC TR 13335-3[6]

Norma ISO/IEC 27001 nie określa dokładnie, z jakiej metody najlepiej skorzystać, choć przykładowo podaje w uwadze metody szacowania ryzyka omówione w ISO/IEC TR 13335-3, Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security[7].

[5] W dalszej części opisane zostały kluczowe metody szacowania ryzyka, które są stosowane w wersji podstawowej, a często zmodyfikowanej dla potrzeb danej organizacji. Poza wymienionymi autor zwraca także uwagę na: TRIKE (Treat modeling framework with simulaties to the Microsoft threat modeling processes), AS/N2S 4360:2004 Risk Management (Australian / New Zeland Standard), CVSS (Common Vulnerability Scoring System).

[6] ISO/IEC TR 13335 Technika informatyczna – wytyczne do zarządzania bezpieczeństwem systemów informatycznych, ISO, 1999.

[7] ISO/IEC TR 13335, zwana skrótowo GMITS (*Guidelines for the Management of IT Security*), jest raportem technicznym o istotnym znaczeniu dla funkcjonowania ISMS. Raport ten składa się z pięciu części.

ISO/IEC TR 13335-1 (PN-I-13335-1:1999) – zawiera wytyczne zarządzania bezpieczeństwem systemów informatycznych. Omawia terminologię, związki między pojęciami oraz podstawowe modele.

ISO/IEC TR 13335-2 (PN-I-13335-2:2003) – stanowi szczegółowy opis planowania i zarządzania bezpie-

Standard ISO/IEC 13335-3[8] wydany w roku 1998 jest częścią 5-arkuszowej normy poświęconej technice informatycznej i jest zbiorem wytycznych (wskazówek) dla osób zajmujących się zarządzaniem bezpieczeństwem systemów informatycznych. W arkuszu trzecim można znaleźć sposoby formułowania trójpoziomowej polityki bezpieczeństwa, rozwinięcie problematyki analizy ryzyka, implementacji planu zabezpieczeń i reagowania na incydenty, a także przedstawienie metod szacowania ryzyka bezpieczeństwa informacji.

Metoda OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), czyli ocena luk i zasobów krytycznych dla działania, to wytyczne powstałe w roku 2001 na Uniwersytecie Carnegie-Mellon [5]. Metoda stosowana jest m.in. przez armię USA i zdobywa popularność w wielu innych, najczęściej dużych organizacjach.

Metoda OCTAVE określa ryzyko oparte na strategicznym szacowaniu i planowaniu technik bezpieczeństwa. Kierowana jest do wszystkich typów organizacji. Metoda opiera się na założeniu, że pracownicy organizacji ponoszą odpowiedzialność za ustanawianie organizacyjnej strategii bezpieczeństwa. Wdrażanie jej założeń powinno odbywać się poprzez nieduży, interdyscyplinarny zespół ludzi (3–5 pracowników organizacji), którzy będą zbierać i analizować informacje, wyznaczać strategię stosowania zabezpieczeń i plany postępowania oparte na organizacyjnym ryzyku bezpieczeństwa. Aby wdrożyć metodę OCTAVE efektywnie, zespół musi mieć szeroką wiedzę na temat działalności biznesowej organizacji i procesów bezpieczeństwa [7].

Metoda realizowana jest w trzech etapach. Etap pierwszy polega na całościowej analizie zasobów organizacji, identyfikacji aktualnych praktyk, przeglądzie wymogów dotyczących bezpieczeństwa, diagnozie luk organizacyjnych i istniejących zagrożeń. Etap drugi ma na celu zidentyfikowanie luk technologicznych. Etap trzeci oparty jest na wypracowaniu strategii ochrony i planu postępowania z ryzykiem.

Analiza skutków potencjalnych błędów – FMEA

Failure Mode and Effect Analysis (FMEA) jest metodą wspierającą zarządzanie jakością, jednak koncepcja i zasady szacowania ryzyka (organizacyjnego i technicznego) mogą być z powodzeniem przeniesione na grunt szacowania ryzyka bezpieczeństwa informacji.

W początkowym okresie FMEA miała zastosowanie w Stanach Zjednoczonych w latach 60 do produkcji na potrzeby astronautyki i motoryzacji[9]. Metoda weryfikowała projekty różnych elementów statków kosmicznych i miała przede wszystkim zapewnić bezpieczeństwo uczestnikom wyprawy. Sukces tej metody w NASA spowodował, że znalazła ona zastosowanie w innych branżach. W latach 70 i 80 metoda ta zadomowiła się w Europie i znalazła nowe zastosowania w przemyśle chemicznym, elektronicznym, a także samochodowym, gdzie zaobserwowano największą dynamikę jej zastosowania. W latach 90 została zaadaptowana w ramach

czeństwem systemów informatycznych. Część ta omawia zagadnienia dotyczące:
- określenia celów, strategii i polityki bezpieczeństwa,
- określenia wymagań w zakresie bezpieczeństwa,
- różnych podejść do przeprowadzania analizy ryzyka,
- omówienia różnego rodzaju planów zabezpieczeń,
- sposobów organizacji służb bezpieczeństwa,
- znaczenia szkoleń i działań uświadamiających,
- wykrywania i reagowania na incydenty.

ISO/IEC TR 13335-3 – jest opisem technik zarządzania bezpieczeństwem systemów informatycznych. Zawiera szczegółowe informacje dotyczące trójpoziomowej polityki bezpieczeństwa, omówienie metod analizy ryzyka, implementacji zabezpieczeń oraz sposobów reagowania na różne incydenty zagrażające bezpieczeństwu informacji.

ISO/IEC TR 13335-4 – przedstawia zagadnienia związane z wyborem właściwych zabezpieczeń. Omówiono tu klasyfikacje i charakterystykę różnych form zabezpieczeń, sposoby doboru zabezpieczeń ze względu na rodzaj zagrożenia lub systemu, a także szczegółowe zalecenia wynikające z innych norm oraz branżowych opracowań.

ISO/IEC TR 13335-5 – ostatnia część normy charakteryzuje metody zabezpieczeń dla połączeń z sieciami zewnętrznymi. Omówiono w niej metody zabezpieczenia połączenia sieci wewnętrznej z zewnętrzną.

[8] Krajowe jednostki organizacyjne (należące do ISO lub IEC) opracowują normy międzynarodowe za pośrednictwem komitetów technicznych, prowadzących prace w ramach określonych obszarów. W zakresie techniki informatycznej ISO i IEC utworzyły Wspólny Komitet Techniczny ISO/IEC JTC 1. Podstawowym zadaniem komitetów technicznych jest opracowywanie norm międzynarodowych. Zdarza się jednak, że komitet techniczny publikuje raport techniczny oznaczany symbolem TR.

[9] Stosowanie FMEA jest obowiązkowe dla dostawców w ramach dostaw na pierwszy montaż (OE – *original equipment*, OES – *original equipment services*) – patrz ISO/TS 16949:2009 FMEA MANUAL, AIAG, 2008, [8].

normy ISO 9000, a w szczególności w QS 9000 (ISO/TS 16949) przeznaczonej dla przemysłu samochodowego.

Metoda polega na analitycznym ustalaniu związków przyczynowo-skutkowych powstawania potencjalnych wad produktu oraz uwzględnieniu w analizie czynnika krytyczności (ryzyka). Jej celem jest konsekwentne i systematyczne identyfikowanie potencjalnych wad produktu / procesu, a następnie ich eliminowanie lub minimalizowanie ryzyka z nimi związanego [8].

Szacowanie ryzyka według tej metody oparte jest na oszacowaniu czynników ryzyka. FMEA wymienia trzy kryteria, które wartościowane są punktami od 1 do 10. W przypadku szacowania ryzyka bezpieczeństwa, określić je można w następujący sposób:

- znaczenie dla firmy / lub Klienta;
- prawdopodobieństwo utraty integralności, dostępności i poufności;
- skutki utraty jakiejś z cech bezpieczeństwa informacji (poufność, integralność, dostępność).

W odniesieniu do umownie zdefiniowanej granicy (liczby punktów), konieczne jest przygotowanie i wykonanie planu postępowania z ryzykiem. Powinien on obejmować zadania, czas realizacji, osobę odpowiedzialną oraz szacunek ryzyka – zakładający skuteczność wykonania wskazanych działań.

Metoda CRAMM

CCTA Risk Analysis and Management Method (CRAMM) jest metodą analizy ryzyka rozwiniętą przez brytyjską organizację rządową CCTA (*Central Communication and Telecommunication Agency*), która obecnie zmieniła nazwę na OGC (*Office of Government Commerce*). Integralną częścią metody jest specjalne narzędzie informatyczne do szacowania ryzyka (CRAMM). Korzystanie z metody bez oprogramowania jest utrudnione.

Pierwsze wydanie CRAMM (metody i narzędzia) opierało się na dobrych praktykach organizacji brytyjskiego rządu. Obecnie CRAMM jest preferowaną metodą do szacowania ryzyka przez rząd brytyjski, ale również jest wykorzystywane przez organizacje z innych państw. Metoda jest szczególnie przydatna dla dużych organizacji, takich jak organizacje rządowe czy przemysłu [7].

CRAMM to metoda realizująca wymagania norm poprzez: analizę luk i opracowywanie programu poprawy bezpieczeństwa, tworzenie rejestru zasobów informacji, definiowanie zakresu zarządzania bezpieczeństwem informacji oraz poprzez tworzenie dokumentacji wdrożonych środków zabezpieczeń. Spośród jej zalet można wymienić:

- obszerną bazę szczegółowych pytań;
- generator różnych szablonów raportów, rodzajów wykresów i schematów, dokumentów;
- zgodność z wymaganiami pierwszego i drugiego arkusza ISO/IEC 27001;
- jest użyteczna dla dużych organizacji o różnych profilach;
- jest narzędziem poleconym przez największe korporacje w Anglii, tworzonym przy współudziale inspektorów i administratorów bezpieczeństwa dużych banków i korporacji.

Praktycy jej stosowania zwracają też uwagę na słabe strony:

- nie ma możliwości analizowania poprawności zastosowanego algorytmu obliczeniowego,
- z wyjątkiem CRAMM Expres (prosty moduł służący do analizy konkretnej aplikacji) CRAMM V5 nie jest ogólnie dostępny i jest trudny w użytkowaniu,
- licencja jednostanowiskowa plus obowiązkowe szkolenia CRAMM V5 są bardzo kosztowne [1].

Metoda COBRA

Control Objectives for Risk Analysis (COBRA) to pełna metoda 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.

Struktura metody COBRA składa się z 6 podstawowych obszarów:

1. *Ingerent Risk* (ryzyko wrodzone);
2. *Control Activities & Procedures* (czynności i procedury kontrolne);
3. *Human Resources Risk* (ryzyko związane z działalnością człowieka);
4. *Security Risk* (zagrożenie);
5. Financial Statement Compliance (zgodność bilansu finansowego);
6. *Disaster Readiness* (przgotowanie do katastrofy).

Poza tym wyróżnia się tu 33 podkategorie oraz 429 pytań kontrolnych [1].

Metoda MARION

Methodology of Analysis of Computer Risks Directed by Levels (MARION) została opracowana

i ostatnio zaktualizowana w 1998 r. przez CLUSIF (*Club de la Sécurité de l'Information Français*). Obecnie CLUSIF już nie finansuje rozwoju i nie promuje metody, ponieważ środki zostały przesunięte na korzyść nowo rozwijanej innej metody – MEHARI. Jednakże MARION jest nadal używana przez wiele organizacji.

Podejście to wykorzystuje metodę prowadzenia audytu. Prowadzi ona do oceny stopnia ryzyka zabezpieczeń IT poprzez odpowiednio do tego skonstruowany kwestionariusz ankietowy dający wskazówki w postaci zapisów na tematy związane z bezpieczeństwem. Celem metody jest ustalenie stopnia bezpieczeństwa, który określany jest w oparciu o 27 zagadnień (pytań) pogrupowanych w 6 tematów. Każde zagadnienie jest oceniane w skali od 0 do 4. Ocena na poziomie 3 dla danego zagadnienia oznacza, że procedury / zabezpieczenia funkcjonujące w organizacji są wystarczające i akceptowalne [7].

Metoda MEHARI

Methode Harmonisee d'Analyse de Risque (MEHARI) została opracowana przez ekspertów bezpieczeństwa z CLUSIF. Podejście to oparte jest na definiowaniu mierników redukcji ryzyka odpowiednich dla celów organizacji. Metoda dostarcza:

- modelu szacowania ryzyka,
- ujęcia modułowego modelu (jego komponentów i procesów),
- narzędzi do analizowania incydentów,
- podejścia do identyfikowania podatności poprzez narzędzie audytu,
- podejścia do identyfikacji zagrożeń i charakterystyki podatności,
- zasady optymalnego wyboru działań korekcyjnych [7].

MEHARI realizuje zalecenia norm ISO/IEC 27001:2005 i ISO/IEC TR 13335 przy użyciu jednolitego systemu oszacowania ryzyka, prawidłowo dobranych zabezpieczeń i lokalizacji zasobów.

Można wymienić jej zalety:

- jest nieskomplikowana i prosta w użyciu;
- odpowiednia dla małych i średnich organizacji wykorzystujących technologie informatyczne;
- algorytm obliczeniowy, baza pytań i scenariuszy ryzyka są ogólnie dostępne;
- istnieje możliwość rozbudowania tej metody o pytania, scenariusze itp.

Wymieniane są także jej wady:

- ubogi generator szablonów raportów i rodzajów wykresów;
- nie jest w pełni zgodna z ISO/IEC 27001:2005;
- analiza kosztów nie uwzględnia związków z innymi scenariuszami [1].

Standardy ISACA

Standardy Information Systems Audit and Control Association (ISACA)[10] dotyczące audytu systemów informatycznych podają kilka metod oceny ryzyka systemów informatycznych.

Jedną z nich jest wykorzystanie ośmiu kluczowych zmiennych przy zastosowaniu liczbowych wartości ryzyka z przedziału od 1 (niski) do 5 (wysoki). Rezultaty takiego rankingu są następnie mnożone przez wagi z przedziału od 1 (niski) do 10 (wysoki), dając wartość zwiększoną. Wartość łączną otrzymuje się po dodaniu do siebie wszystkich wartości zwiększonych. Wartość łączna pozwala uszeregować poszczególne obszary audytu według ryzyka [1].

Metody autorskie

Norma ISO/IEC 27001 nie określa dokładnie, z jakiej metody najlepiej skorzystać, dlatego też możliwe jest stosowanie przez organizacje również własnych metod opracowanych na postawie wiedzy branżowej i doświadczenia. Takie podejście jest właściwe dla dużych organizacji, które posiadają odpowiednie struktury organizacyjne do tego, aby tę metodę opracować i zwalidować. Niewątpliwą korzyścią takiego podejścia jest świadomość metody, jak i całego procesu szacowania ryzyka przez wszystkich uczestników biorących udział przy jej wykorzystaniu w procesie szacowania ryzyka bezpieczeństwa informacji. Oczywiście istnieje zagrożenie, że wypracowana metoda okaże się nieskuteczna, a firma nie dostanie rekomendacji przy audycie certyfikacyjnym, co tym samym może skutkować nieprzyznaniem certyfikatu. Dlatego też, małe firmy ze względu na brak przede wszystkim zasobów personalnych, nie decydują się na opracowywanie własnych metod i wolą wybrać jedną z wielu już dostępnych, pozytywnie zaaprobowa-

[10] Stowarzyszenie ISACA (Information Systems Audit and Control Association) jest największą organizacją zajmującą się problemami audytu, kontroli i zarządzania w środowisku informatycznym. Wraz z powołanym Komitetem Standaryzacyjnym opracowało szereg standardów audytowania i kontroli systemów informatycznych. Mają one na celu informować audytorów systemów informatycznych o minimalnym akceptowalnym poziomie świadczonych przez nich usług oraz informować zarządy firm i inne zainteresowane strony o poziomie oczekiwań w stosunku do pracy audytorów systemów informatycznych.

nych przez audytorów podczas audytów certyfikacyjnych.

Zakończenie

Bezpieczeństwo informacji jest ważne, środkiem do jego zapewnienia jest skuteczny system zarządzania bezpieczeństwem informacji, a jego „motorem" musi być zarządzanie ryzykiem – to generalna konkluzja.

Wybór podstawy ISMS, jest jednak istotny, nie musi to być w każdym przypadku ISO/IEC 27001 (a certyfikacja nie ma w żadnym razie kluczowego znaczenia) – to jednak warto skorzystać z międzynarodowego standardu, który jest zbiorem dobrych praktyk zarządzania. Niezależnie od wielkości organizacji i specyfiki jej procesów, zdecydowanie korzystne jest uwzględnienie także ISO/IEC 27002, COBIT, ITIL, ISO 20000 oraz innych norm, szczególnie związanych z metodami szacowania ryzyka. W tym względzie konieczne jest duże oczytanie, wiedza i praktyka dotycząca aspektów organizacyjnych ISMS i każdorazowe zwracanie uwagi, że rozwiązania w ramach systemu muszą być skalowane – dostosowane do rzeczywistych potrzeb.

Bibliografia

1. MOLSKI M., ŁACHOTA M.: Przewodnik audytora systemów informatycznych. Helion, Gliwice 2007, 90, 98–99, 99–100, 1, 97.
2. http://kni.kul.lublin.pl/~andy/ref/other/risk.pdf, 3.
3. WHITMAN M.E., MATTORD H.J.: Readings and Cases in the Management of Information Security. Thomson Course Technology. Boston 2006, 50, 53.
4. PN-I-13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych. PKN, 1999, 9.
5. ALBERTS CH., DOROFEE A.: Managing Information Security Risks. The OCTAVE Approach. Addison-Wesley, Boston 2003.
6. OZIER W.: 67 Risk analysis and assessment. CRC Press LLC, 2004.
7. ENISA: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, 2006, 22, 22–23, 36, 31, 35, 36; ze strony www: http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf.
8. ŁUCZAK J.: System zarządzania jakością dostawców w branży motoryzacyjnej. Wydawnictwo AE, Poznań 2008, 164–174.

Recenzent:
dr hab. inż. Ruta Leśmian-Kordas
profesor Akademii Morskiej w Szczecinie