Piotr Ziobrowski

Bezpieczeństwo informacji we współczesnej firmie

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 1, 77-84

2009

Piotr ZIOBROWSKI
Gnieźnieńska Wyższa Szkoła Humanistyczno-Menedżerska „Milenium”

BEZPIECZEŃSTWO INFORMACJI WE WSPÓŁCZESNEJ FIRMIE

Technika informatyczna jest procesem sterowania (jak również może służyć kontroli) za pomocą mikroprocesorów (lub innych układów komputerowych). W przedsiębiorstwach wykorzystuje się z reguły dwa systemy komputerowe: pierwszy z nich ma służyć przechowywaniu (i przetwarzaniu) danych, drugi ma być drogą szybkiej (i sprawnej) komunikacji. Istotne jest, aby stosowane techniki informacyjne były dopasowane do potrzeb konkretnej firmy. Ponadto właściwy wybór systemów informatycznych powinien być wykorzystywany w sposób podnoszący efektywność komunikacji i sprawność procesów gospodarczych firmy. Informatyczne systemy zarządzania mają za zadanie realizować cele stawiane sobie przez organizacje, firmy, czy korporacje. Aby jednak było to możliwe należy spełnić kilka warunków.

Bezpieczeństwo informacji

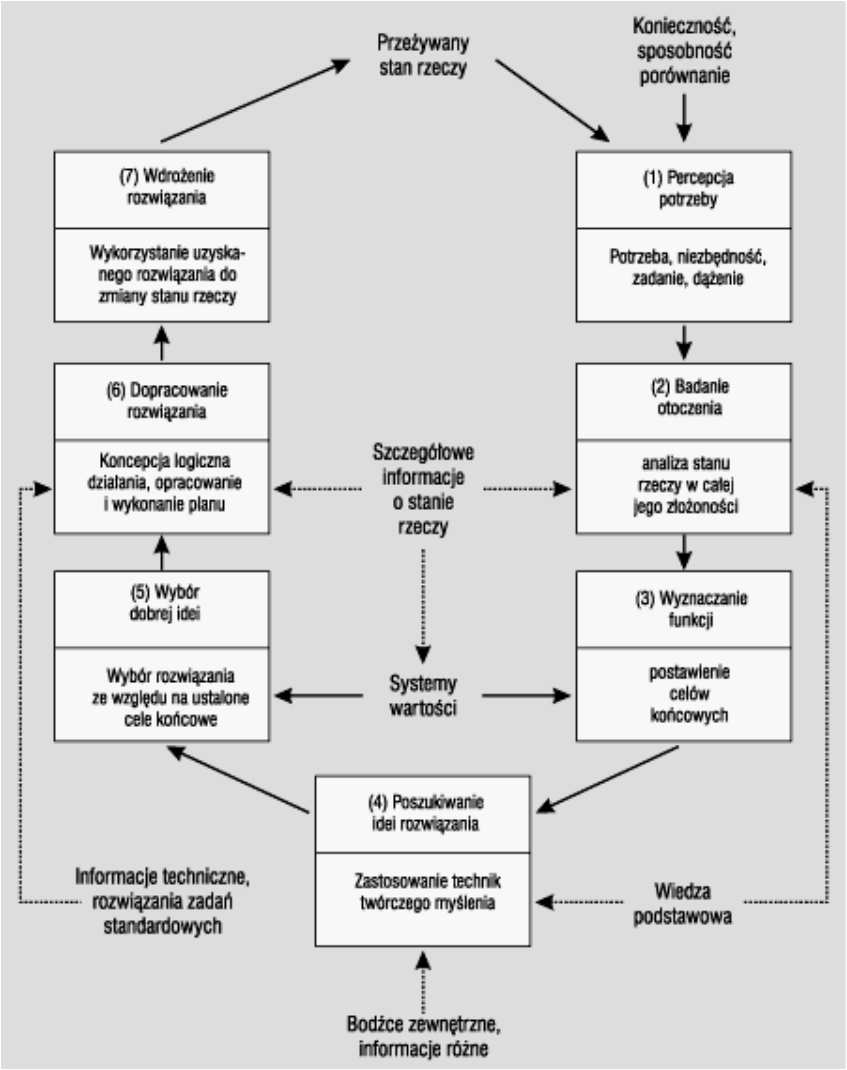
Zarządzanie firmą, korporacją, czy instytucją jest możliwe dzięki informacji. Niedużym ryzykiem będzie stwierdzenie, że funkcjonowanie każdego przedsiębiorstwa zależy od dostępu do informacji. *Informacją jest każda wiadomość, powodująca jakąś reakcję i inicjująca określone działania: w samym systemie zarządzania- lub w jego otoczeniu – wśród kierownictwa albo w elementach wykonawczych organizacji, firmy lub korporacji – produkcyjnych, usługowych, itp.*[1] Informacja jest istotna z uwagi na to, że to właśnie ona zapoczątkowuje łańcuch w postaci decyzji, dalej działania powodującego konkretne rezultaty.

Żyjemy w społeczeństwie opartym na informacji, niejednokrotnie mamy do czynienia z jej nadmiarem. Istotne jest wyłonienie informacji, z którymi konieczne należy się zapoznać, informacji, z którymi według uznania można się zapoznać, informacji, które mogą pomóc pozytywnie się wyróżnić i informacji, które nie są nam potrzebne. Do cech dobrej informacji zaliczamy: wiarygodność i dokładność, kompletność, jasność i zrozumiałość, dostępność, szybkość (terminowość) dostarczenia. Warto również wspomnieć o klasyfikacji ze względu na kryterium tajemnicy, podział obejmuje informacje: jawne, poufne i tajne.[2] Można zaryzykować stwierdzenie, że funkcjonowanie firmy zależy od dostępu do informacji. Powszechnym staje się w tym celu instalowanie w firmach odpowiednich systemów do gromadzenia oraz wymiany informacji.

Trudno nie zgodzić się z Markiem Blim, który w swoich analizach podaje, że „inżynieria bezpieczeństwa informacji to przede wszystkim umiejętność analizowania otoczenia pod względem zbierania i wykorzystywania każdej z wielu dostępnych danych na potrzeby bieżące bezpieczeństwa instytucji/organizacji/grupy społecznej”. Systemowa metoda analizy funkcjonalnej „charakteryzuje się wyjątkową prostotą pętli podstawowego algorytmu postępowania w prowadzonym procesie analizy problemu i w podejściu do generacji praktycznie sprawdzalnego rozwiąza-

[1] A. Barczak, T. Sidoruk: *Bezpieczeństwo systemów informatycznych zarządzania.* Warszawa 2003, s. 13
[2] Ibidem, s. 15-16

nia, którego warunkowe przyjęcie jest przede wszystkim zobligowane możliwościami pomyślnego wdrożenia. Takie postępowanie ma zarazem zachowane wszelkie pierwiastki rozwiązań *a posteriori*, tych ujawnionych w trakcie analizy, a zarazem z różnych względów (organizacyjnych, materialnych, osobowych itp.) niezbyt możliwych do bezpośredniego włączenia we wdrażane rozwiązanie (mimo ich słuszności zgodności z wybraną dobrą ideą). Analiza funkcjonalna składa się z siedmiu etapów: 1. percepcji potrzeby; 2. badania otoczenia; 3. wyznaczenia funkcji; 4. poszukiwania idei rozwiązania; 5. wyboru dobrej idei; 6. dopracowania rozwiązania; 7. wdrożenia rozwiązania".[3]



Rysunek nr 1. Analiza funkcjonalna
Źródło: M. Blim: *Teoria ochrony informacji (cz. 1).* „Zabezpieczenia" 28.02.2009.

[3] M. Blim: *Teoria ochrony informacji (cz. 1).* „Zabezpieczenia" 28.02.2009

Wchodząc w interakcje z informacją, przechodzimy w fazę komunikacji. Komunikacja jest niezwykle ważnym elementem w budowaniu systemów informacyjnych zarządzania. Cele organizacji, firmy lub korporacji, które wyznaczają ich zadania, także – bezpośrednio lub pośrednio – wyznaczają zadania systemów informatycznych zarządzania. Jednym z takich zadań jest regulowanie dopływu informacji do szczebli kierowniczych w taki sposób, aby osoby funkcyjne na poszczególnych stanowiskach pracy otrzymywały informacje konieczne i wystarczające do realizacji zadań.[4] Przy czym pamiętać należy, że do podjęcia prawidłowych decyzji niezbędne jest pewne minimum informacyjne. Wielość i złożoność informacji niezbędnych w podejmowaniu decyzji zarządczych powoduje, że współcześnie trudno sobie wyobrazić dobre funkcjonowanie nawet stosunkowo małej firmy i biura, a tym bardziej - korporacji lub instytucji bez zastosowania w nich nowoczesnych technologii informacyjnych, w tym zwłaszcza w ich systemach zarządzania. Przekonanie o tym powoduje, że technika komputerowa, będąca podstawą tych technologii, jest wykorzystywana w systemach zarządzania bardzo szeroko już od wielu lat.[5] Informatyczny system zarządzania jest „tylko" (bądź – „aż") systemem wspomagającym zarządzanie (i tak powinniśmy go wykorzystywać!).

System informacyjny organizacji, firmy lub korporacji może być określony jako wielopoziomowa struktura, która pozwala użytkownikowi tego systemu na transformowanie określonych informacji wejściowych na pożądane informacje wyjściowe za pomocą odpowiednich procedur i modeli. W wyniku uzyskania tych informacji mogą być podejmowane określone decyzje. Biorąc pod uwagę powyższą definicję, konkretny system informacyjny – w zależności od potrzeb - można analizować albo jako wielopoziomową strukturę, albo jako element lub zbiór elementów łańcucha decyzyjnego funkcjonującego w systemie zarządzania organizacji, firmy lub korporacji.[6]

Do podstawowych elementów systemu informacyjnego dowolnej organizacji można zaliczyć: zbiór użytkowników systemu, zbiór informacji charakteryzujących stan sfery realnej oraz zachodzące w niej zmiany (stanowiących „zasoby informacyjne" systemu informacyjnego), zbiór elementów narzędzi technicznych służących gromadzeniu, przetwarzaniu, przesyłaniu i udostępnianiu informacji (w trybie obligatoryjnym i na żądanie), zbiór rozwiązań systemowych stosowanych w danej organizacji, stanowiących o stosowanej formule zarządzania, zbiór metainformacji opisujących system informacyjny i jego zasoby, relacje pomiędzy poszczególnymi zbiorami.

Jeśli którykolwiek z wyżej wymienionych elementów systemu informacyjnego zarządzania jest realizowany przy udziale techniki komputerowej, wówczas przyjmuje się, że system taki nosi nazwę *systemu informatycznego zarządzania*. Jest to więc najbardziej uproszczona, a jednocześnie najbardziej ogólna definicja systemu informatycznego zarządzania, wskazująca zarazem na różnice pomiędzy systemem informacyjnym i systemem informatycznym. Można także na podstawie powyższej definicji stwierdzić, że systemy informatyczne są pewną klasą – obecnie dominującą – systemów informacyjnych zarządzania. Biorąc jednak pod uwagę nieprecyzyjność, a tym samym – wątpliwą jednoznaczność takiej definicji, w dziedzinie systemów zarządzania często przyjmuje się, że system informatyczny jest to

[4] A. Barczak, T. Sidoruk, op. cit., s. 17
[5] Ibidem, s. 25
[6] Ibidem, s. 28

wyodrębniona część systemu informacyjnego, która – z punktu widzenia przyjętych celów działania – jest skomputeryzowana. Systemem informatyzowanym nazywa się system, którego funkcjonowanie jest usprawniane poprzez wprowadzenie lub udoskonalenie systemów komputerowych oraz dzięki odpowiednim zmianom w obiegu, prezentacji (udostępnianiu), przetwarzaniu i przechowywaniu informacji.

Informatyzacja systemu informacyjnego powinna prowadzić m.in. do poprawy funkcjonalności interfejsów służących kontaktom z użytkownikami oraz wymianie informacji z otoczeniem, a także zwiększeniu bezpieczeństwa danych i informacji. Na tle powyższej definicji, możliwa jest do przyjęcia nieco zawężona definicja systemu informatycznego. Pojęcie to obejmuje sprzęt komputerowy i oprogramowanie, umożliwiające udoskonalenie funkcji, szybkości i precyzji działania algorytmów w całości lub w części systemu informacyjnego oraz zwiększenie możliwości przetwarzania, zabezpieczania i udostępniania (prezentacji) informacji w informatyzowanym systemie.[7]

Bezpieczeństwo informatycznych systemów zarządzania

Ze względu na przydatność w odniesieniu do różnych kategorii decyzji, a także poziomów zastosowania w strukturze organizacji, stosowane obecnie systemy informatyczne, wspierające zarządzanie można podzielić na następujące kategorie: systemy transakcyjne TPS (Transaction Processing Systems), systemy nowoczesnego biura OAS (Office Automation Systems), systemy informacyjne zarządzania MIS (Management Information Systems), systemy wspomagania zarządzania produkcją MRP II (Manufacturing Resource Planning) lub ERP (Enterprise Resource Planning), systemy sterowania i zarządzania produkcją MES (Manufacturing Executing Systems), zintegrowane systemy zarządzania CIM (Computer Integrated Manufacturing), systemy wspomagania zarządzania MSS (Management Support Systems), systemy wspomagania decyzji DSS (Decision Support Systems), systemy informacyjne kierownictwa EIS (Executive Information Systems), systemy wspomagające kierownictwo ESS (Executive Support Systems), systemy eksperckie ES (Expert Systems).[8] W różnych obszarach zarządzania wykorzystywane są ponadto różne, mniej lub bardziej wyspecjalizowane systemy wspomagające funkcje zarządzania lub kierowania. Mogą one występować zarówno jako samodzielne systemy, jak i pod kontrolą zintegrowanego systemu zarządzania. Należą do nich, m.in. systemy wspomagające prace projektowe: CAD (Computer Aided Design), CADD (Computer Aided Design and Drafting), CAE (Computer Aided Engineering), CASE (Computer Aided System Engineering), systemy wspomagające planowanie i harmonogramowanie, np. CAP (Computer Aided Planning), systemy wspierające kontrolę jakości, np. CAQ (Computer Aided Quality Assurance), systemy treningowe i edukacyjno-szkoleniowe (podnoszenie kwalifikacji), np. CAL (Computer Assisted Learning) lub CAT (Computer Assisted Training), systemy wspomagające sterowanie procesami wytwórczymi, np. CAM (Computer Assisted Manufacturing).[9]

Rozwijająca się technologia informatyczna powoduje powstanie nowych produktów i usług. Jednocześnie powoduje to dynamiczną ekspansję nowych zagro-

[7] Ibidem, s. 20
[8] Ibidem, s. 25-26
[9] Ibidem, s. 27

żeń. Wymaga to wprowadzenia zorganizowanego zapewnienia bezpieczeństwa informacji oraz stwarza potrzebę wypracowania jednolitego podejścia do zagadnień związanych z zarządzaniem i kontrolą nad technologiami informatycznymi.

Na podkreślenie zasługuje fakt, że zarządzanie bezpieczeństwem systemów informatycznych oznacza ciągły proces składający się z pewnej liczby innych procesów (subprocesów). Brak ciągłości zaburza, czy wręcz uniemożliwia skuteczne zarządzanie bezpieczeństwem systemów informatycznych. Dla przeprowadzenia procesu certyfikacji w zakresie zarządzania bezpieczeństwem informacji opracowano szereg norm związanych z bezpieczeństwem i audytem systemów informatycznych. Jednym z nowszych standardów zarządzania bezpieczeństwem informacji jest ISO/IEC 27001 (jej polski odpowiednik to PN-ISO/IEC 27001: 2007). Norma ta umożliwia przeprowadzenie procesu certyfikacji w zakresie zarządzania bezpieczeństwem informacji.

Anna Bielawa,[10] analizując zagadnienie podaje, że Norma ISO 27001 jest oparta na brytyjskiej normie BS-7799-2. Zgodnie ze zmienionymi zasadami akredytacji, certyfikaty BS-7799 nie są przyznawane od 24 lipca 2006 roku, a wszystkie nowe systemy bezpieczeństwa są certyfikowane na zgodność z wymaganiami standardu ISO 27001. W instytucjach posiadających certyfikat BS-7799 powinno podczas audytu lub recertyfikacji nastąpić przejście do nowej normy.

Standard ISO 27001 składa się z części podstawowej i załączników. W części podstawowej normy zdefiniowano wymagania związane z ustanowieniem i zarządzaniem systemem zarządzania bezpieczeństwem informacji, dokumentacją, odpowiedzialnością kierownictwa, wewnętrznymi audytami, przeglądami i ciągłym doskonaleniem systemu. Warto podkreślić, że obecnie, norma wymaga udokumentowania metodyki analizy ryzyka, a także zapewnienia jej powtarzalności i porównywalności wyników. Załącznik A normy ISO/IEC 27001 został zmieniony. Obecnie, zarządzanie incydentami bezpieczeństwa stało się jednym z głównych obszarów normy. Załącznik A tej normy wyróżnia zabezpieczenia 11 obszarów wpływających na bezpieczeństwo informacji w organizacji. Należą do nich: polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie aktywami, bezpieczeństwo zasobów ludzkich, bezpieczeństwo fizyczne i środowiskowe, zarządzanie systemami i sieciami, kontrola dostępu, pozyskiwanie, rozwój i utrzymanie systemów informatycznych, zarządzanie incydentami związanymi z bezpieczeństwem informacji, zarządzanie ciągłością działania, zgodność. Istotną zaletą normy jest kompleksowe podejście do bezpieczeństwa informacji. Wymieniono w niej obszary bezpieczeństwa fizycznego, osobowego, teleinformatycznego i prawnego. Nie określono szczegółowych technicznych wymagań, lecz wskazano na zagadnienia, które należy uregulować. Sposób zabezpieczenia tych obszarów, zależny od przedsiębiorstw, powinien być oparty na przeprowadzonej analizie ryzyka.

M. Blim, podaje, że ochrona informacji w przypadku systemu informacyjnego opartego w całości na technice informatycznej jest przedsięwzięciem systemowym, a więc programowo-sprzętowym. Jako działania zabezpieczające wymienia: stosowanie określonych bezpiecznych procedur przy projektowaniu i produkcji sprzętu teleinformatycznego, stosowanie określonych bezpiecznych procedur przy projektowaniu, kodowaniu, produkcji i dystrybucji oprogramowania, stosowanie odpo-

[10] A. Bielawa: *System zarządzania bezpieczeństwem informacji według normy ISO/IEC 27001:2005*. „Studia i prace wydziału Nauk ekonomicznych i Zarządzania" nr 1, ss. 172-173

wiednich programów operacyjnych, wykonywanie bezpiecznych instalacji sprzętowych, stosowanie urządzeń i procedur do odtwarzania STI kodowanie i szyfrowanie informacji jak i nośników z jej zbiorami.

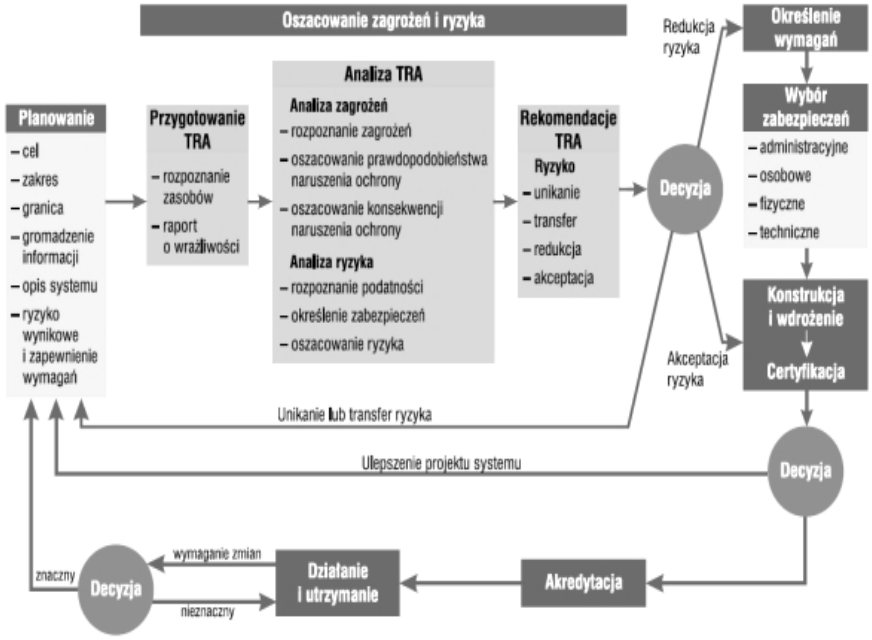
Ważnym elementem jest, podkreśla dalej Marek Blim, przewidywalność potencjalnych zagrożeń dla bezpieczeństwa systemu informacyjnego realizowanego przy wykorzystaniu projektowanego systemu teleinformatycznego. Za główne należy jednak uznać działanie na korzyść ochrony wewnętrznych i zewnętrznych połączeń komunikacyjnych STI. Systemy teleinformatyczne charakteryzują się bowiem pod względem swego wykorzystania w procesach informacyjnych dwoma elementarnymi procesami: przetwarzaniem informacji w samym systemie, przesyłaniem informacji między systemami, co wiąże się z odpowiednimi funkcjami obsługi i usługami systemowymi, a zarazem wymaga odpowiednich uprawnień w zakresie dostępu i czynności wobec zbiorów/zasobów informacyjnych, bo nawet wiadomości przekazywane w obrębie firmy są narażone na rozmaite niepożądane oddziaływania, stąd konieczne są funkcje ochrony dla systemu ich przemieszczania.[11]

Do najistotniejszych procesów wchodzących w skład procesu zarządzania bezpieczeństwem systemów informatycznych zalicza się: zarządzanie konfiguracją, zarządzanie zmianami, zarządzanie ryzykiem. Bardzo obrazowo owe subprocesory charakteryzuje A. Wójcik,[12] według którego *zarządzanie konfiguracją jest procesem weryfikacji zmian w systemie.* Słusznie podkreśla, że *celem bezpieczeństwa w tym zakresie jest wiedza i świadomość wprowadzonych zmian*. Uważa, że *zarządzanie konfiguracją ma gwarantować: wprowadzanie zmian, które nie obniżą efektywności funkcjonowania systemu, skuteczności mechanizmów zabezpieczających oraz ogólnego bezpieczeństwa organizacji, wprowadzanie stosownych zmian dotyczących planowania ciągłości działania i odtwarzania po awarii.* Sam proces zarządzania konfiguracją nie dotyczy tylko zmian konfiguracji, lecz obejmuje również tak istotne elementy, jak: weryfikacja legalności oprogramowania, sprawdzenie mechanizmów kontrolnych przechowywania oprogramowania, czy wreszcie inwentaryzację zasobów organizacji. Kolejny ważny element skutecznego procesu zarządzania bezpieczeństwem informatycznych systemów zarządzania jest „zarządzanie zmianami". Proces ten polega na *identyfikowaniu nowych wymagań w zakresie bezpieczeństwa, gdy wprowadzane są zmiany w systemie informatycznym*. Ów subprocesor jest bardzo ważny z uwagi na niezwykle szybki rozwój technologii i usług, a wraz z nimi nowych zagrożeń, co powoduje nieustanne zmiany systemów informatycznych. Zmiany mogą dotyczyć: nowych procedur i funkcji systemu, aktualizacji oprogramowania, zmian sprzętowych, wprowadzenia dodatkowych połączeń sieciowych i międzysieciowych, pojawienia się nowych użytkowników. Planowaną zmianę w systemie informatycznym należy poddać analizie pod kątem jej wpływu na bezpieczeństwo. *Poważne zmiany w systemie wymagają dokładnej oceny ryzyka w celu określenia nowych wymagań bezpieczeństwa*. Podkreślić trzeba, że *skuteczny proces zarządzania zmianami zapewnia spójność infrastruktury informatycznej, odpowiedni poziom bezpieczeństwa informacji przy projektowaniu nowych rozwiązań oraz wdrożenie komponentów o wysokiej jakości.* I wreszcie ostatni subprocesor – „zarządzanie ryzykiem", jak sama nazwa obrazo-

[11] M. Blim: Teoria ochrony informacji (cz. 2). „Zabezpieczenia" 28.02.2009

[12] Por. A. Wójcik: *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001*, „Zabezpieczenia" 2008, nr 2, s. 68-73.

wo wskazuje jest procesem szacowania ryzyka mającym na celu ograniczenie go do akceptowalnego poziomu. Norma PN-I-13335-1:1999 wskazuje, że *zarządzanie ryzykiem to całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego. Efektywny program zarządzania ryzykiem powinien zapewniać osiągnięcie celów biznesowych organizacji przez: skuteczniejsze zabezpieczenie systemów informatycznych, które służą do przechowywania, przetwarzania i przesyłania informacji należących do organizacji, umożliwienie kierownictwu uzasadnienia swych decyzji dotyczących wydatków na zarządzanie ryzykiem zaplanowanych w budżecie. W ramach „starego modelu" zarządzania ryzykiem można wyróżnić dwa procesy główne: szacowanie ryzyka, ograniczanie ryzyka. Szacowanie ryzyka obejmuje: zidentyfikowanie i określenie wartości aktywów organizacji – można wykorzystać tu metodę jakościową lub ilościową, zidentyfikowanie zagrożeń i określenie prawdopodobieństwa ich wystąpienia, analizę ryzyka – ocenę podatności systemów lub aktywów na wystąpienie czynników ryzyka (czynniki ryzyka sprzyjające wystąpieniu strat). Na ograniczanie ryzyka składają się następujące działania: wybór odpowiednich mechanizmów zabezpieczeń, wdrożenie, testowanie i monitorowanie mechanizmów zabezpieczeń, akceptacja ryzyka szczątkowego*.



Rysunek nr 2. Model zarządzania ryzykiem
Źródło: M. Bieniak: *Teoria ochrony informacji (cz.2).* „Zabezpieczenia" 28.02.2009.

Ryzyko szczątkowe *(residual risk)* to ryzyko, które pozostaje mimo wprowadzenia mechanizmów zabezpieczających. Na proces szacowania ryzyka składa się identyfikacja informacji lub aktywów informatycznych, które są podatne (wrażliwe)

na naruszenie bezpieczeństwa. Przykładowo aktywem informatycznym są: oprogramowanie i sprzęt komputerowy, zasoby informacyjne, a także i usługi, dokumenty organizacji, a nawet pracownicy, zasoby intelektualne, środki finansowe, czy wyposażenie. Kolejnym, nie mniej ważnym, etapem procesu szacowania ryzyka jest zdefiniowanie zagrożeń związanych z aktywami (czyli wszystkim, co przedstawia wartość dla danej organizacji) oraz określenie prawdopodobieństwa wystąpienia podatności. Podatność wskazuje na słabość mechanizmów kontroli wewnętrznej, która może być wykorzystana na przykład do uzyskania nieautoryzowanego dostępu do systemu. Zagrożenie oznacza niebezpieczeństwo dla systemów informatycznych. Rezultatem wykorzystania podatności przez zagrożenie jest następstwo (np. strata aktywów informatycznych). Może mieć ono charakter ilościowy, np. w postaci bezpośredniej straty pieniędzy lub jakościowy, np. w postaci zniszczenia reputacji, jak również może oznaczać pośrednie lub bezpośrednie straty dla organizacji. Po identyfikacji aktywów, zagrożeń, jak i podatności, dana firma czy przedsiębiorstwo muszą określić akceptowalny dla własnych potrzeb poziom ryzyka. Dla wszystkich nieakceptowanych rodzajów ryzyka audytor powinien wskazać i ocenić istniejące mechanizmy kontrolne. Niestety, po wdrożeniu mechanizmów kontrolnych, w jednostce zawsze jednak pozostaje jeszcze pewne ryzyko szczątkowe. Do powyżej opisanego modelu zarządzania ryzykiem dochodzi nowy model, którego celem jest ograniczenie ryzyka do akceptowalnego poziomu przez opracowanie odpowiedniego schematu postępowania z ryzykiem. W modelu tym, za istotne podkreśla się ciągłość i systematyczność. Do ważnych narzędzi identyfikujących ryzyko można zaliczyć: analizę środowiskową – ocenę wpływu zmian środowiska zewnętrznego na procesy zarządzania i kontroliw 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. Wśród profesjonalistów do popularnych narzędzi analizy ryzyka zalicza się: CRAMM *(CCTA Risk Analysis and Management Method)* – metodę realizującą wymagania norm poprzez analizę luki opracowywanie programu poprawy bezpieczeństwa, tworzenie rejestru zasobów informacji, definiowanie zakresu zarządzania bezpieczeństwem informacji oraz tworzenie dokumentacji wdrożonych środków zaradczych. 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. MARION *(Mission Analysis and Risk Impact on Operations Net-work-tool).* MEHARI *(Methode Harmonisee d'Analyse de Risques)* – realizuje zalecenia norm BS 7799 i ISO/IEC 13335 przy użyciu jednolitego systemu oszacowania ryzyka, prawidłowo dobranych zabezpieczeń i lokalizacji zasobów. 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). W powiązaniu z Common Criteria oraz ciągłym rozwojem w zakresie zarządzania bezpieczeństwem informacji (seria ISO 27000) EBIOS staje się techniką całościowego zarządzania ryzykiem.