PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 159

Informatyka Ekonomiczna 19 2011

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

ZASTOSOWANIE MODELI DOJRZAŁOŚCI W ZARZĄDZANIU RYZYKIEM NA POTRZEBY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W ORGANIZACJI

Streszczenie: W literaturze pojawia się wiele modeli dojrzałości odnoszących się do różnych dziedzin. Jednym z najbardziej znanych jest model dojrzałości opracowany przez Software Engineering Institute. Początkowo był on opracowywany z myślą o organizacjach tworzących oprogramowanie, jednak ewoluował i znalazł zastosowanie w wielu innych dziedzinach. Współczesna postać tej metody, znana pod nazwą CMMI (*Capability Maturity Model Integration*), jest pewnego rodzaju standardem, znajdującym zastosowanie w wielu obszarach. W artykule przedstawiono koncepcję modeli dojrzałości jako narzędzia umożliwiającego ocenę istniejącego poziomu zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych w organizacji oraz porównano go z wzorcowym rozwiązaniem.

Słowa kluczowe: ryzyko, zarządzanie ryzykiem, bezpieczeństwo systemów informatycznych, modele dojrzałości, CMMI.

1. Wstęp

Ryzyko związane z szerokim zastosowaniem systemów informatycznych (SI) w biznesie rośnie wraz ze zwiększaniem się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Postęp technologiczny generuje zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i ilości czynników ryzyka. Obecnie szczególnego znaczenia nabiera problematyka zarządzania ryzykiem w aspekcie bezpieczeństwa SI, koncentrująca się na poszukiwaniu optymalnego stosunku między zagrożeniami a kosztem zabezpieczeń zasobów informatycznych. Jednym z problemów w odpowiednim przebiegu procesu zarządzania ryzykiem jest sposób jego oceny, który pozwalałby na usprawnienie jego realizacji.

Celem niniejszego artykułu jest charakterystyka modeli dojrzałości (*maturity models*) i propozycja ich zastosowania jako narzędzia umożliwiającego ocenę bieżącego poziomu realizacji procesów zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji oraz pozwalającego na odniesienie aktualnych rozwiązań do systemu wzorcowego. Taka analiza porównawcza może

być podstawą identyfikacji czynników, które wymagają szczególnego usprawnienia, dzięki czemu możliwe byłoby osiągnięcie wyższego poziomu dojrzałości.

2. Etymologia i istota pojęcia ryzyka

Zdefiniowanie ryzyka jest zadaniem bardzo trudnym, a podanie jednoznacznej, precyzyjnej definicji jest wręcz niemożliwe. Ryzyko jest definiowane w różnych naukach i teoriach, m.in. w ekonomii, naukach behawioralnych, naukach prawnych, psychologii, statystyce, ubezpieczeniach, teorii prawdopodobieństwa i wielu innych. Nauka o ryzyku jest praktycznie rozwijana w większości nauk i stosowana we wszystkich technologiach. Obecnie nie istnieje jeszcze jednolita teoria ryzyka, a samo pojęcie możemy rozpatrywać na wielu poziomach i niemalże we wszystkich dziedzinach działalności człowieka.

Etymologia ryzyka nie została dotychczas jednoznacznie wyjaśniona. Według Encyklopedii Brockhausa znaczenie tego słowa wywodzi się z języka łacińskiego, gdzie czasownik *risicare* znaczy omijać coś. Greckie *riza* podobnie jak włoskie *ris(i)co* (lub *rischio*) oznacza rafę, którą statek powinien ominąć, a więc niebezpieczeństwo, którego powinien uniknąć [Kaczmarek 2003, s. 11-12].

W języku angielskim *risk* oznacza sytuację powodującą niebezpieczeństwo lub możliwość, że zdarzy się coś złego. Bliskim pojęciu ryzyka jest słowo *hazard*, będące synonimem niebezpieczeństwa, potencjalnego źródła niebezpieczeństwa, zagrożenia [Kaczmarek 2008, s. 51].

Na rozwój teorii ryzyka znaczący wpływ miało odkrycie rachunku prawdopodobieństwa przez B. Pascala i P. Fermata w XVII wieku. W 1654 r. wprowadzili oni pojęcie wartości oczekiwanej. Ryzyko zaczęto wówczas definiować jako prawdopodobieństwo osiągnięcia założonego celu. Największe osiągnięcia w dziedzinie ryzyka ma nauka amerykańska (m.in.: [Willett 1901; Knight 1921; Arrow 1979; Vaughan 1997]). Początek naukowego zainteresowania ryzykiem wiąże się z opublikowaniem w 1901 roku przez A.H. Willetta pionierskiej pracy *The Economic Theory of Risk and Insurance* (*Ekonomiczna teoria ryzyka i ubezpieczeń*). Znaczący wpływ na myśl ekonomiczną i teorię ryzyka miały prace F.H. Knighta, pochodzące z lat dwudziestych ubiegłego wieku, poruszające zagadnienia ryzyka i niepewności. Od tego momentu ryzyko i niepewność weszły na stałe do ekonomii i znalazły wyraz w nowej teorii wyboru, rozwijanej między innymi przez noblistę Kennetha J. Arrowa [1979]. Na gruncie nauk o finansach ryzyko włączyli do teorii ekonomii trzej inni laureaci Nagrody Nobla: Harry M. Markowitz, Merton H. Miller i William F. Sharpe. Podstawowe założenia teorii ryzyka określili brytyjscy ekonomiści – Alfred Marshall oraz Arthur C. Pigou. Ponadto zagadnienia te były rozpatrywane przez wielu ekonomistów szkoły klasycznej. Obecnie żaden ekonomista nie może w swoich analizach pomijać problemu ryzyka [Staniec, Zawiła-Niedźwiecki 2008].

Niektórzy autorzy twierdzą, że nie można jednoznacznie zdefiniować ryzyka inaczej niż tylko poprzez zbiór opisujących je cech, takich jak [Jedynak, Szydło 1997, s. 14-15; Gładysz 2006]:

- źródło i przedmiot ryzyka, czyli powód, który czyni rozważania nad ryzykiem uzasadnionym oraz sytuację (zjawisko) równoznaczną z przedmiotem analizy ryzyka,
- możliwe następstwa ryzyka, czyli potencjalny charakter skutków podjętych decyzji oraz miary tych skutków w ujęciu podmiotowym i przedmiotowym,
- podjęcie ryzyka, czyli o decyzja podjęciu aktywnych działań związanych z realizacją zadań potrzebnych do uzyskania korzyści i minimalizacji strat,
- realizacja ryzyka, czyli wystąpienie przewidywanych lub nieprzewidywalnych skutków zdarzeń, których źródłem jest przedmiot ryzyka,
- możliwość manipulacji ryzykiem, czyli podatność przedmiotu ryzyka na stosowanie środków i metod ukierunkowujących zachodzące procesy w pożądanym kierunku.

Od czasu owych pierwszych prób włączenia ryzyka do teorii ekonomicznych nastąpił silny rozwój teorii ryzyka oraz zarządzania ryzykiem. W dzisiejszych czasach problematyka ryzyka podejmowana jest w wielu dyscyplinach naukowych, szczególnie ważna jest również dla szeroko rozumianej informatyki oraz bezpieczeństwa SI.

3. Ryzyko w aspekcie bezpieczeństwa systemów informatycznych

Istnieje wiele standardów mających regulować problematykę ryzyka w obszarze bezpieczeństwa SI w organizacji. Na potrzeby bezpieczeństwa SI można przytoczyć następującą definicję ryzyka podaną w normie IEC 61508: „Ryzyko oznacza miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji, wyrażoną jako iloczyn prawdopodobieństwa (lub możliwości) wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat)" [Liderman 2001].

Jedna z najprostszych, a jednocześnie najlepiej oddająca istotę ryzyka systemów informatycznych, to 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]. Biorąc pod uwagę powyższą definicję, ryzyko w obszarze bezpieczeństwa SI rozpatrywane może być z punktu widzenia następujących kategorii [Ryba 2006, s. 13-14]:

- użyteczności (*Relevance Risk*) – w kategorii tej wyróżnia się ryzyko, że zebrane informacje są niewykorzystane lub nieprzydatne, bądź lub także aktualność otrzymanej informacji jest niewystarczająca;
- integralności (*Integrity Risk*) – w kategorii tej wyróżnia się 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*) – w tej kategorii 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 użytkowników lub zachwiana zostanie zdolność systemów do przetwarzania danych na potrzeby kluczowych procesów;
- adekwatności infrastruktury (*Infrastructure Risk*) – ryzyko wiąże się z tym, że kluczowe procesy informatyczne (zapewnienie działania systemów i sieci, zarządzanie bazami danych, zarządzanie bezpieczeństwem, procesy odtworzenia działalności na wypadek awarii itp.) nie zapewniają w sposób efektywny wsparcia kluczowym potrzebom organizacji.

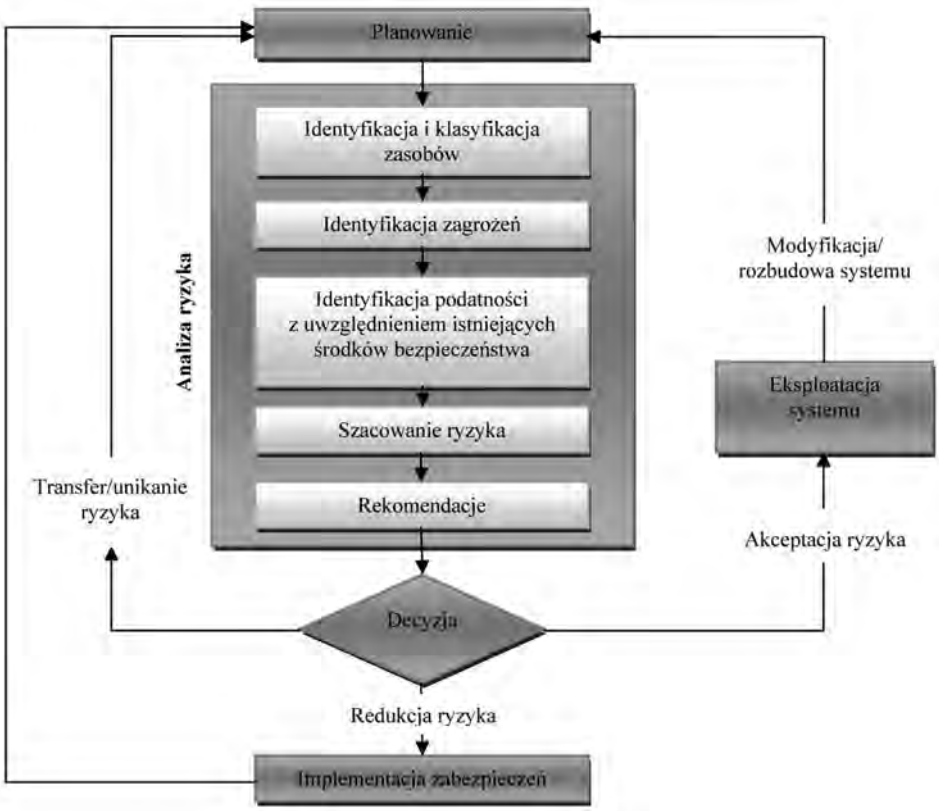
Wymienione kategorie ryzyka są rozszerzeniem o elementy biznesowe (właściwości użyteczności i adekwatności infrastruktury), atrybutów bezpieczeństwa informacji (poufność, integralność, dostępność), zdefiniowanych w standardzie BS 7799 *Code of Practice for Information Security Management*. Termin „ryzyko" ujęto także w normie ISO/IEC TR 13335-1, gdzie traktuje się je jako zbiorczą miarę prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów SI, a zatem pośrednią lub bezpośrednią szkodę dla instytucji [ISO/IEC 13335-1]. Definicja ta nawiązuje do terminu podatności (*vulnerability*), stanowiącej słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie oraz atrakcyjność aktywów informacyjnych [ISO/IEC 13335-3]. Norma zawiera również wskazówki, od czego zależy wielkość ryzyka: „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 [ISO/IEC 13335-1; Liderman 2008, s. 70].

4. Wprowadzenie do zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych w organizacji

Zgodnie ze wspomnianą normą ISO/IEC TR 13335 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 [Molski, Łacheta 2007; ISO/IEC 13335-1]. Zatem jest to proces mający na celu ograniczenie ryzyka do akceptowalnego poziomu. Powinien składać się on z następujących faz: planowania, nabywania, rozwoju, testowania, odpowiedniego rozmieszczenia systemów informatycznych [Molski, Łacheta 2007; Łuczak 2009].

M.E. Whitman zwraca uwagę na wzajemną relację pomiędzy szacowaniem ryzyka a jego osłabieniem – co stanowi istotę zarządzania ryzykiem [Whitman, Mattord 2006]. Na to osłabienie, czyli ograniczanie ryzyka, składają się działania takie, jak wybór odpowiednich mechanizmów zabezpieczeń, wdrożenie, testowanie i monitorowanie mechanizmów zabezpieczeń, akceptacja ryzyka szczątkowego [Wójcik 2008]. M.E. Whitman wymienia następujące etapy zarządzania ryzykiem [Whitman, Mattord 2006]:

- identyfikacja ryzyka,
- oszacowanie wpływu na działalność,
- oszacowanie słabych punktów i zagrożeń,
- oszacowanie bieżących środków osłabienia ryzyka.



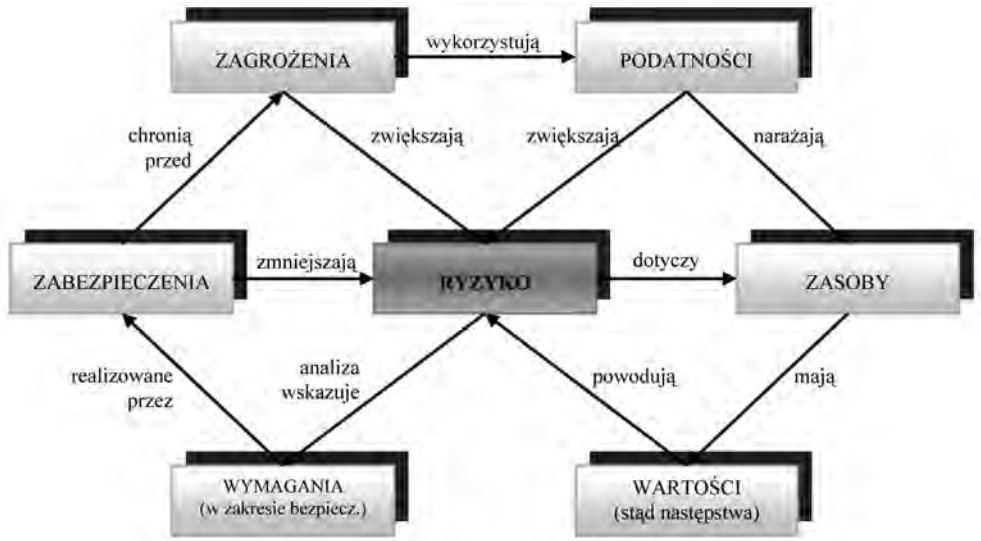
Rys. 1. Uproszczony model zarządzania ryzykiem według standardu ISO/IEC TR 13335

Źródło: [ISO/IEC 13335].

Analizując różne podejścia i definicje zarządzania ryzykiem na potrzeby bezpieczeństwa SI, można stwierdzić, że identyfikacja zagrożeń i podatności, szacowanie

ryzyka oraz rekomendowanie określonych środków zabezpieczeń to podstawowe elementy procesu zarządzania ryzykiem. Uproszczony schemat modelu tego procesu, oparty na przytoczonej już normie ISO/IEC TR 13335, został zaprezentowany na rysunku 1.

Jak wynika z zaprezentowanego uproszczonego modelu, podstawowy element procesu zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji stanowi analiza ryzyka, która pozwala na identyfikację zasobów systemu, zlokalizowanie odpowiadających im podatności i zagrożeń oraz oszacowanie prawdopodobieństwa ich wystąpienia i wielkości potencjalnych strat. Analiza ryzyka obejmuje ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, autentyczności i niezawodności systemu informatycznego. Związki między poszczególnymi istotnymi elementami w procesie zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych zaprezentowano na rysunku 2.



Rys. 2. Związki w zarządzaniu ryzykiem

Źródło: [Grzywak 2000, s. 291].

Efektywny program zarządzania ryzykiem powinien zapewniać osiągnięcie celów biznesowych organizacji przez [Wójcik 2008]:

- skuteczniejsze zabezpieczenie systemów informatycznych, które służą do przechowywania, przetwarzania i przesyłania informacji należących do organizacji,
- wykazanie, których rodzajów ryzyka i w jaki sposób można uniknąć, stosując rozwiązania organizacyjne i techniczne w zakresie przetwarzania, przesyłania i przechowywania informacji w SI,

- umożliwienie kierownictwu uzasadnienia swych decyzji dotyczących wydatków na zarządzanie ryzykiem, zaplanowanych w budżecie.

Zarządzanie ryzykiem jest procesem osiągania i utrzymania 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. Zarządzanie ryzykiem w aspekcie bezpieczeństwa systemów informatycznych w organizacji ma na celu m.in. [Liderman 2006]:

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

Należy podkreślić, że korzyści wynikające z właściwego przeprowadzenia procesu zarządzania ryzykiem bezpieczeństwa systemów informatycznych w organizacji mogą być wielopłaszczyznowe. Odpowiednie podejście do tej problematyki, polegające na wdrożeniu odpowiednich standardów, implementacji właściwych funkcji, mechanizmów zabezpieczających i kontrolnych oraz komputerowe wsparcie tego procesu może zmniejszyć znacząco prawdopodobieństwo wystąpienia incydentów, które mogłyby negatywnie wpłynąć na organizację, a także może doprowadzić do obniżenia kosztów i przyczynić się do uzyskania przewagi nad konkurencją. Brak odpowiedniego zarządzania ryzykiem może mieć poważne konsekwencje dla przedsiębiorstwa, gdyż może prowadzić do utraty klientów, osłabienia pozycji rynkowej, utraty prestiżu, zakłócenia współpracy z partnerami i kontrahentami, a także może generować znaczące koszty.

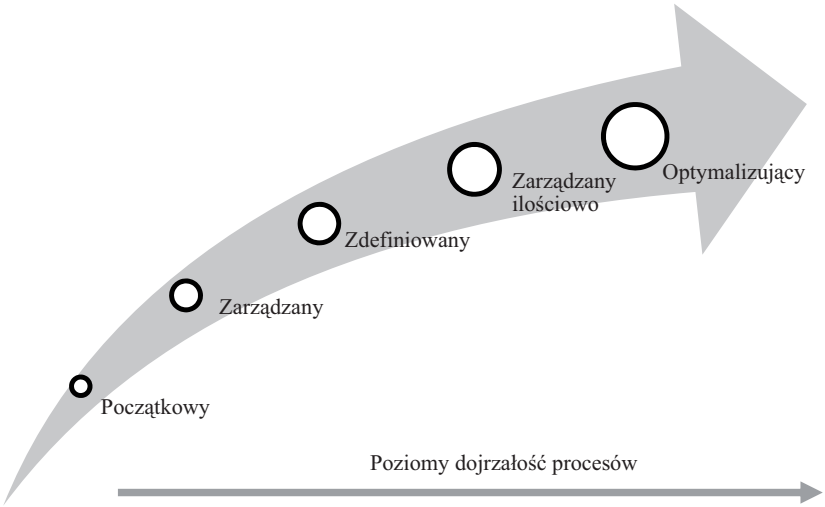
Jednakże istotnym problemem dla kierownictwa organizacji pozostaje możliwość oceny poziomu zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych, co może przełożyć się na usprawnienie i podniesienie efektywności tego procesu. Jednym z rozwiązań pozwalających na ocenę funkcjonującego systemu zarządzania ryzykiem mogą być modele dojrzałości.

5. Istota modeli dojrzałości systemów i procesów

W literaturze przedmiotu można znaleźć wiele modeli dojrzałości odnoszących się do różnych dziedzin, m.in. zarządzania projektami, tworzenia oprogramowania, zarządzania szeroko rozumianą informatyką [Andersen, Jessen 2003]. Do popularnych standardów stosujących koncepcję modeli dojrzałości można zaliczyć CMMI (*Capability Maturity Model Integration*). CMMI został stworzony przez Software Engineering Institute jako model służący zarządzaniu wytwarzaniem oprogramowania, jednak później ewoluował i był rozwijany także w innych dziedzinach. Model ten

jest modelem samodoskonalenia organizacji, a ocena dojrzałości polega w nim na określeniu, czy w organizacji istnieją zaimplementowane procesy należące do określonych grup zdefiniowanych w ramach modelu. Dodatkowo określa się dojrzałość procesów, czyli poziom ich realizacji [Jur 2008].

Omawiany model stworzony został wokół pewnej liczby tak zwanych obszarów procesowych, do których przyporządkowana została lista celów i praktyk. Całość podzielono na dwie reprezentacje: ciągłą (*continous representation*) i stopniowaną (*staged representation*) [Jur 2008]. Reprezentacja ciągła polecana jest z reguły mniejszym firmom, gdzie istnieje skuteczna kontrola nad poszczególnymi mechanizmami działania organizacji. Jednak w większej organizacji, gdzie trudniej jest utrzymać pieczę nad poszczególnymi komórkami, istnieje ryzyko pogubienia się w strukturach CMMI i ocena dojrzałości poszczególnych procesów staje się bardzo trudna, wręcz niemożliwa do zrealizowania. Dlatego większym organizacjom proponuje się tzw. reprezentację stopniowaną, która jest wprawdzie mniej elastyczna, ale dzięki temu, że narzuca kolejność poprawy jakości obszarów procesowych, jest łatwiejsza we wdrażaniu i zapewnia większe prawdopodobieństwo, iż całość przebiegnie bez większych zakłóceń [*Capability*... 2010]. Reprezentację stopniowaną modelu CMMI wyznacza pięć głównych poziomów dojrzałości (*maturity levels*), co obrazuje rysunek 3.



Rys. 3. Poziomy dojrzałości procesów według modelu CMMI

Źródło: opracowanie własne.

Jak przedstawiono to na rysunku 3, model CMMI definiuje następującą pięciostopniową skalę dojrzałości procesów w organizacji (zob. http://www.sei.cmu.edu/) [Zygała 2010; Garczyński 2009]:

- Początkowy (*Initial*) – procesy na tym poziomie dojrzałości charakteryzuje działanie reaktywne, *ad hoc* oraz nieuporządkowane. Na tym poziomie organizacja na ogół nie zapewnia stabilnego środowiska dla zarządzania. Brakuje planowania procesu, przez co tylko jego fragmenty są definiowane przed rozpoczęciem prac.
- Powtarzalny (*Repeatable*) – metody organizacji i zarządzania procesami stają się bardziej przewidywalne. Przebiegi procesów podlegają działaniom doskonalącym, a pracownicy są zorientowani na analizowanie i doskonalenie metod pracy oraz na doskonalenie własnej wiedzy i umiejętności. Zastosowanie w organizacji znajdują metody planowania procesów. Na poziomie tym ustanowiona jest polityka związana z zarządzaniem procesami oraz procedury jej wdrażania.
- Definiowany (*Defined*) – na tym poziomie dojrzałości organizacja posiada zbiór zdefiniowanych najważniejszych procesów, będących podstawą działalności operacyjnej. Procesy są udokumentowane w całej organizacji. W dokumentacji organizacji procesów wykorzystuje się podstawowe zasady zarządzania projektami, najlepsze praktyki i inne regulacje odnoszące się do organizacji procesów w ramach projektu. Występuje okresowe modyfikowanie obowiązujących standardów, procedur narzędzi i metod − stosownie do potrzeb zmieniających się uwarunkowań. W całej organizacji prowadzony jest program szkoleń w celu zapewnienia personelowi odpowiedniego poziomu wiedzy i umiejętności niezbędnych do wykonywania powierzonych im zadań.
- Zarządzany ilościowo (*Quantitatively Managed*) – dla poszczególnych procesów zdefiniowane są zestawy mierników, które zapewniają ocenę tych procesów pod kątem jakości i efektywności. Ustanowione zbiory mierników pozwolą menedżerom dokonać rzetelnej oceny stanu procesów oraz wyznaczyć dla nich cele doskonalenia. Procesy są charakteryzowane za pomocą dobrze zdefiniowanych i spójnych mierników oraz wskaźników.
- Zoptymalizowany (*Optimizing*) – na tym poziomie mamy do czynienia z procesem wzorcowym, bliskim ideału na danym poziomie rozwoju technologii i metod zarządzania. Cała organizacja skupiona jest na ciągłym doskonaleniu procesów. Innowacje, które stosują najlepsze praktyki, są identyfikowane i wdrażane w całej organizacji. W doskonaleniu procesów wykorzystuje się zaawansowane metody i techniki zarządzania informacją, oparte na zaawansowanych technologiach informacyjno-komunikacyjnych.

Każdy poziomom dojrzałości składa się z określonej liczby obszarów procesowych, które organizacja musi zaimplementować, aby znaleźć się na określonym poziomie dojrzałości modelu CMMI. Warto zauważyć, że obszary procesowe w tej reprezentacji zostały tak zaprojektowane, iż nie jest możliwe osiągnięcie poziomu trzeciego, nie spełniwszy wcześniej wymagań poziomu drugiego. Podobnie jest oczywiście w przypadku kolejnych poziomów – czwartego czy piątego. W ten sposób doskonalenie procesów w reprezentacji stałej ma charakter przyrostowy. Organizacja ma niejako gotowy program doskonalenia obecnych w niej procesów. Jest to dobre

rozwiązanie dla tych firm, które nie posiadają wystarczającej wiedzy na temat stopnia zaawansowania swoich procesów, a co za tym idzie – trudno jest im jednoznacznie zdecydować, jak powinien wyglądać ich plan usprawniania i doskonalenia. W takiej sytuacji zastosowanie reprezentacji stałej może się okazać niezwykle przydatne i pomocne [Chrapko]. Z modelu tego skorzystało już wiele firm i instytucji, wśród których wymienić można GE Money Bank, GMC Software Technology czy HP.

6. Model dojrzałości zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych

Koncepcja modeli dojrzałości została rozwinięta przez wspomniany już w artykule Software Engineering Institute jako metoda doskonalenia procesów produkcji oprogramowania. Współczesna postać tej metody, pod nazwą CMMI (*Capability Maturity Model Integration*), stanowi pewien standard, który stał się inspiracją dla rozwoju nowych obszarów zastosowań wspomnianej metody [Zygała 2010]. Zatem może ona znaleźć zastosowanie również w obszarze zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych w organizacji.

Model dojrzałości w zarządzaniu ryzykiem jest powszechnie stosowanym modelem referencyjnym, zbiorem dobrych praktyk, służących ocenie kompetencji organizacji w zakresie zarządzania ryzykiem [*Zarządzanie*… 2007]. Przeznaczeniem takiego modelu jest umożliwienie organizacji dokonania oceny poziomu dojrzałości, na jakim znajduje się ona w obszarze zarządzania ryzykiem, w porównaniu z kryteriami zawartymi w modelu. Za pomocą modelu organizacja jest w stanie określić swój poziom dojrzałości zarządzania ryzykiem, a także na tej podstawie wyznaczyć długofalowe cele w zakresie doskonalenia tego procesu.

Modele dojrzałości mają na ogół pięć poziomów, w ramach których jakość procesów jest oceniana przez porównanie z wcześniej określonymi kryteriami. Poziomy mają za zadanie opisać poszczególne fazy i etapy we wdrażaniu praktyk zarządzania. Syntetycznie scharakteryzowane w tabeli 1 poziomy dojrzałości określają kolejne stopnie doskonalenia aż do osiągnięcia poziomu optymalizowanego, na którym w organizacji funkcjonuje kultura ciągłego doskonalenia zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych [*Capability*... 2007]. W zakresie funkcjonowania systemu zarządzania ryzykiem szczególne znaczenie będą miały m.in. następujące elementy [Jur 2008]:

- świadomość zagrożeń i ryzyk w obszarze bezpieczeństwa systemów informatycznych,
- doświadczenie w użytkowaniu systemów informatycznych,
- zdolność definiowania potrzeb w zakresie bezpieczeństwa systemów informatycznych,
- kompetencje pracowników w zakresie systemów informatycznych i ich bezpieczeństwa (wiedza, świadomość, umiejętności i doświadczenie).

Zatem dojrzała organizacja w sposób przemyślany i rozważny zarządza ryzykiem, przeprowadzając cykliczne szkolenia dla pracowników oraz funkcjonuje w kulturze ciągłego doskonalenia tych procesów. W organizacjach niedojrzałych aktywność w zakresie zarządzania ryzykiem w obszarze bezpieczeństwa to wycinkowa i słabo zorganizowana działalność zabezpieczająca, która nie gwarantuje odpowiednich efektów i często sprowadza się jedynie do usuwania skutków awarii sprzętu i oprogramowania. W tabeli 1 przedstawione zostały poszczególne poziomy modelu dojrzałości zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych.

Tabela 1. Poziomy modelu dojrzałości zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych

Poziom dojrzałości	Syntetyczna charakterystyka poziomu dojrzałości zarządzania ryzykiem
1	2
Początkowy (*Initial*)	• Organizacja nie zapewnia stabilnego środowiska dla zarządzania ryzykiem. • Organizacja nie ma formalnego procesu zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych, przeglądy ryzyka są reakcyjne, a reakcje *ad hoc*. • Skupianie się jedynie na zgodności z obowiązującymi regulacjami. • Brak standardów w zakresie zarządzania ryzykiem na potrzeby bezpieczeństwa SI w organizacji. • Organizacja poświęca minimum uwagi identyfikacji i ocenie ryzyka. • Zagrożenia i ryzyko SI są analizowane raz na rok lub nawet rzadziej. • Źródła potencjalnych zagrożeń SI nie są zarejestrowane, a informacja o nich nie jest rozpowszechniana wśród pracowników organizacji. • Aktywność w zakresie zarządzania ryzykiem i bezpieczeństwa SI to wycinkowa i słabo zorganizowana działalność zabezpieczająca, która nie gwarantuje odpowiednich efektów i często sprowadza się jedynie do usuwania skutków awarii sprzętu i oprogramowania. • Personel często podejmuje w zakresie bezpieczeństwa SI działania na własną rękę, będące często wynikiem jakichś incydentów i naruszeń poufności, integralności lub dostępności informacji i systemów. • Brak szkoleń w zakresie bezpieczeństwa SI i zarządzania ryzykiem.
Powtarzalny (*Repeatable*)	• W organizacji ustalone są ogólne zasady zarządzania ryzykiem, ale nie w pełni zaimplementowane. • Niektóre procesy są zidentyfikowane i opisane. • Zarząd poodejmuje pewne działania oraz środki, aby zarządzać ryzykiem na potrzeby bezpieczeństwa SI. • Działania w obszarze bezpieczeństwa systemów informatycznych mają swój budżet oraz dedykowany personel z określonymi rolami, odpowiedzialnością, a także uprawnieniami. • Pracownicy czasem przechodzą szkolenia i są świadomi większości zagrożeń i ryzyka.
Zdefiniowany (*Defined*)	• Proces zarządzania ryzykiem jest zdefiniowany, sformalizowany i zunifikowany w całej organizacji.

Tabela 1, cd.

1	2
	• Powołane są określone jednostki organizacyjne zajmujące się *stricte* problematyką zarządzania ryzykiem w aspekcie bezpieczeństwa SI w organizacji, zapewniające spójne, skoordynowane i systematyczne podejście do ryzyka. • W organizacji są pracownicy zdolni do planowania reakcji na ryzyko. • W organizacji funkcjonują plany utrzymania ciągłości działania (*Business Continuity Planning*) w zakresie tworzenia, weryfikacji i aktualizacji planów wznawiania działania w obszarze kluczowych procesów organizacji, w przypadku wystąpienia awarii istotnych systemów informatycznych. • Zarząd organizacji przegląda najważniejsze zagrożenia bezpieczeństwa SI, a zarządzanie ryzykiem służy celom biznesowym. • Ustalone są różne poziomy szkoleń dla pracowników. • Przygotowywane są raporty dla pracowników wyższego szczebla, m.in. raporty z audytów bezpieczeństwa SI.
Zarządzany ilościowo (*Quantitatively managed*)	• Wszystkie procesy są opisane, a ich właściciele zostali jasno zdefiniowani. • Kultura zarządzania ryzykiem ma swojego przywódcę. • Zarządzanie ryzykiem jest elementem procesu zarządzania organizacją i integralną częścią jej działalności. • Nacisk kładziony jest przede wszystkim na pomiar, agregację i zarządzanie ryzykiem w całej organizacji. • Miary ilościowe (wskaźniki ryzyka) są zdefiniowane dla poszczególnych systemów i procesów. • Oceny ilościowe prowadzone są przez doświadczoną kadrę. • Stosuje się efektywnie wskaźniki wczesnego ostrzegania. • Podejmuje się próby oceny poziomu zarządzania ryzykiem w organizacji (m.in. poprzez zewnętrznych specjalistów). • Przeprowadzane są dokładniejsze oceny i rygorystyczne analizy ryzyka. Obszary o wysokim ryzyku poddaje się szczegółowej analizie. • Podejmowane są szersze i dobrze zorganizowane działania zmierzające do redukcji ryzyka.
Zoptymalizowany (*Optimizing*)	• Kultura ciągłego doskonalenia systemu zarządzania ryzykiem służy potrzebom bezpieczeństwa systemów informatycznych w organizacji. • Każdy poziom zarządzania w organizacji jest zainteresowany czynnym udziałem w zarządzaniu ryzykiem w aspekcie bezpieczeństwa SI. • Zdefiniowane są koszty i korzyści związane z zarządzaniem ryzykiem. • Organizacja posiada strategię ciągłego doskonalenia systemu zarządzania ryzykiem. • Istnieją programy szkoleń dla wszystkich osób mających dostęp do informacji chronionych w organizacji. • Odpowiedzialność za bezpieczeństwo informacji i systemów jest włączona do opisów zakresów obowiązków, procedur przyjmowania nowych pracowników i ich ocen okresowych. • Najlepsze praktyki w zakresie zarządzania ryzykiem są identyfikowane i rozpowszechniane w całej organizacji.

Źródło: opracowanie własne na podstawie [*Zarządzanie*… 2007; Garczyński 2009].

Na podstawie tabeli 1 dojrzałość zarządzania ryzykiem na potrzeby bezpieczeństwa SI można zdefiniować jako początkową w przypadku, kiedy w organizacji brakuje jakichkolwiek aktywności mających na celu identyfikację, analizę, redukcję i monitorowanie ryzyka w obszarze bezpieczeństwa systemów informatycznych. O wysokiej dojrzałości będziemy mówili wówczas, kiedy w organizacji mamy do czynienia z procesem wzorcowym, bliskim ideału na danym poziomie rozwoju technologii i metod zarządzania [Zygała 2010]. Podstawą tego poziomu jest wykorzystanie idei ciągłego doskonalenia. Usystematyzowany i dobrze realizowany proces zarządzania ryzykiem przyczynia się do zidentyfikowania ryzyka w zakresie utraty bezpieczeństwa systemu informatycznego w kontekście prowadzonej działalności. Zidentyfikowane ryzyka zostają ocenione pod kątem konsekwencji biznesowych oraz określone jest prawdopodobieństwo ich wystąpienia. W ramach tego procesu zdefiniowane zostają zasady w zakresie postępowania z ryzykiem, określone są priorytety podejmowanych działań, celem których celem jest ograniczanie ryzyka. Monitoruje się także efektywności tych działań. Dzięki informowaniu o istniejącym ryzyku oraz szkoleniom dotyczącym zasad ich ograniczania rośnie bezpieczeństwo SI w organizacji.

7. Podsumowanie

Omawiane w artykule koncepcje modeli dojrzałości i opracowane na ich podstawie metody doskonalenia procesów mogą być zastosowane w wielu obszarach dziedzinowych funkcjonowania różnych organizacji. Opisany w niniejszym artykule model CMMI może zostać zastosowany do oceny poziomu zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych w organizacji. Istotne jednak jest, aby w odpowiedni sposób opracować poszczególne kryteria charakteryzujące kolejne poziomy dojrzałości procesu zarządzania ryzykiem. Tak skonstruowany model może się stać cennym narzędziem, które umożliwi identyfikację aktualnego poziomu zarządzania ryzykiem w obszarze bezpieczeństwa systemów informatycznych oraz pozwoli na sprawne porównanie tego poziomu z innym, wzorcowym systemem. Te działania prowadzić mogą również do określenia elementów procesu, które wymagają udoskonalenia w celu osiągnięcia wyższego poziomu dojrzałości zdefiniowanego w modelu CMMI.

Literatura

Andersen E.S., Jessen S.A., *Project maturity in organisations*, „International Journal of Project Management 2003, 21.

Arrow K.J., *Eseje z teorii ryzyka*, Warszawa 1979.

Capability Maturity Model Integration, http://www.bei.org.pl/index.php?Itemid=97&id=44&option=com_content&task=view (5.10.2010).

Chrapko M., *Extreme Programming i CMMI. Kreatywność, czy dyscyplina?* www.hakin9.org/upload/UploadFiles/XP_i_CMMI_cz2.doc (5.10.2010).

Garczyński D., *Modele dojrzałości systemów w zarządzania ryzykiem operacyjnym w banku*, [w:] *Wybrane problem budowy aplikacji dla gospodarki elektronicznej*, red. M. Niedźwiedziński, K. Lange-Sadzińska, Wyd. Marian Niedźwiedziński – CONSULTING, Łódź 2009.

Gładysz M., *Ryzyko w działalności gospodarczej*, Zeszyty Naukowe Ekonomika i Organizacja Gospodarki Żywnościowej nr 59, 2006, http://ekrol.sggw.waw.pl/publikacje/pdf/zneiogz59_2006/gladysz.pdf (5.10.2010).

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

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.*

Jedynak P., Szydło S., *Zarządzanie ryzykiem*, Wydawnictwo Ossolineum, Wrocław 1997.

Jur M. *Wybór systemu informatycznego a dojrzałość informatyczna inwestora*, [w:] *Materiały II Międzynarodowej Konferencji Młodych Naukowców Szkół Wyższych Euroregionu Nysa*, Jelenia Góra 2008, http://www.ae.jgora.pl/p/konferencje/konfernecja_mlodych_naukowcow/IIMK_MNSWEN_do_int_cz2a.pdf (5.10.2010).

Kaczmarek T.T., *Zarządzanie zdywersyfikowanym ryzykiem w świetle badań interdyscyplinarnych*, Wydawnictwo Wyższej Szkoły Zarządzania i Marketingu, Warszawa 2003.

Kaczmarek T.T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Wydawnictwo Difin, Warszawa 2008.

Knight F.H., *Risk, Uncertainty and Profit*, University of Boston Press, Boston 1921.

Liderman K., *Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego*, [w:] *Biuletyn Instytutu Automatyki i Robotyki Wojskowej Akademii Technicznej*, nr 16, Wydawnictwo IAiR, Warszawa 2001.

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

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

Łuczak J., *Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001*, Zeszyty naukowe Akademii Morskiej w Szczecinie, 2009, nr 19 (91), s. 63-70, http://www.wsm.szczecin.pl/userfiles/File/wydawnictwo/ZN_19/ZN_AM_19_91_Luczak.pdf (5.10.2010).

Molski M., Łacheta M., *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007.

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

Staniec I, Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym*, Wyd. C.H. Beck, Warszawa 2008.

Vaughan E.J., *Risk Management*, J. Wiley & Sons Inc., New York 1997.

Whitman M.E., Mattord H.J., *Readings and Cases in the Management of Information Security*, Thomson Course Technology, Boston 2006.

Willett A., *The Economic Theory of Risk and Insurance*, Columbia University Press, New York 1901.

Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001* – cz. 2. http://www.zabezpieczenia.com.pl/ochrona-informacji/system-zarzadzania-bezpieczenstwem-informacji-zgodny-z-iso-iec-27001-cz-2 (17.07.2008).

Zarządzanie ryzykiem. Przewodnik dla praktyków, Great Britain. Office of Government Commerce, Wyd: The Stationery Office, 2007, http://books.google.pl (5.10.2010).

Zygała R., *Zastosowanie modeli dojrzałości w zarządzaniu informatyczną infrastrukturą organizacji*, Informatyka Ekonomiczna. Informatyka w zarządzaniu 15, Prace Naukowe UE we Wrocławiu nr 88, Wydawnictwo Uniwersytetu Ekonomicznego, Wrocław 2010.

APPLICATION OF MATURITY MODELS IN RISK MANAGEMENT FOR SECURITY OF INFORMATION SYSTEMS IN ORGANIZATIONS

Summary: In the literature there are many different maturity models applied in various areas. One of the most famous is the maturity model developed by the Software Engineering Institute. Initially it was developed for software development organizations, but it has evolved and has been applied in other fields. The modern form of this method – CMMI (*Capability Maturity Model Integration*), is standard, applicable in many areas and branches. The article presents the concept of maturity models as a tool for assessing the existing level of information systems security risk management and for comparing it with the model solution. Thus it is also possible to identify the elements of risk management process that require improvements in order to reach the next – higher level of maturity.