Koncepcja metody oceny ryzyka w przedsięwzięciach informatycznych

Wojciech Machała
Wojskowa Akademia Techniczna Wydział Cybernetyki Instytut Systemów Informatycznych

e–mail: wmachala@isi.wat.waw.pl

Streszczenie

W artykule przedstawiono sposób konstruowania i wyznaczania wartości miary powodzenia realizacji przedsięwzięcia informatycznego zwanej wskaźnikiem zagrożenia przedsięwzięcia informatycznego. Wartość tego wskaźnika jest obliczana na podstawie tzw. sprawczych i wykonawczych czynników zagrożenia, które stanowią agregację różnych ryzyk, identyfikowanych i ocenianych z wykorzystaniem tradycyjnych metod.

1. Wprowadzenie w problematykę ryzyka w przedsięwzięciach informatycznych

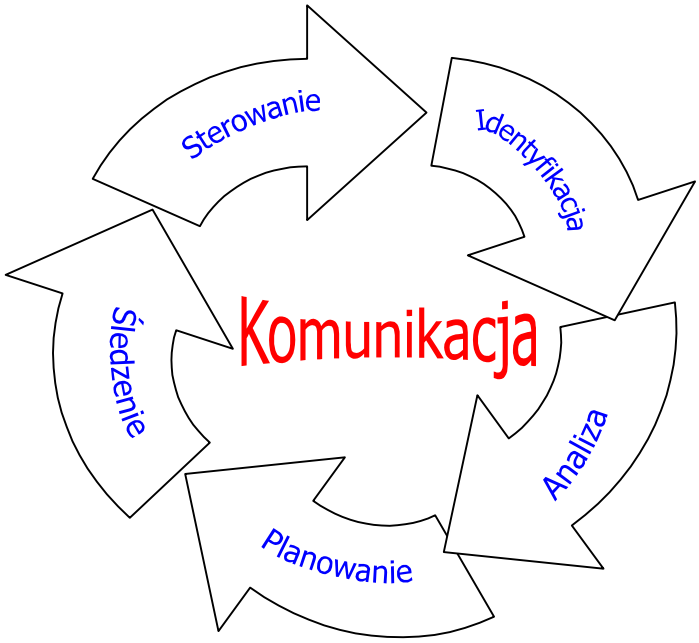
W literaturze dotyczącej ryzyka w przedsięwzięciach informatycznych można znaleźć wiele dyskusji dotyczących definicji pojęcia ryzyka. Wszyscy autorzy tych dyskusji są jednak zgodni co do faktu, że ryzyko zawsze charakteryzowane jest przez dwa elementy:

- Niepewność – zdarzenie, które powoduje urzeczywistnienie ryzyka może lecz nie musi wystąpić. Ryzyko, którego urzeczywistnienie jest pewne w 100 % powinno być klasyfikowane jako ograniczenie realizacji przedsięwzięcia informatycznego.
- Skutki – urzeczywistnienie się ryzyka powoduje wystąpienie negatywnych konsekwencji lub strat.

Dobra definicja ryzyka została przedstawiona w dokumencie „Australian Standard on Risk Management" (AS/NZS 4360:1995) w którym ryzyko jest definiowane jako „szansa jakiegoś wydarzenia, które będzie miało wpływ na realizację zamierzonego celu".

Ryzyko jest nieodłącznym elementem realizacji każdego przedsięwzięcia informatycznego, dlatego profesjonalne podejście do przedsięwzięć informatycznych wymaga stosowania przez kierownika projektu skutecznej metody zarządzania ryzykiem. Jednym z bardziej znanych paradygmatów zarządzania ryzykiem w przedsięwzięciach informatycznych jest paradygmat opracowany przez Software Engineering Institute (SEI) na Carnegie Mellon University (rys. 1).

Przedstawiony paradygmat reprezentowany jest symbolicznie przez okrąg dla podkreślenia ciągłości procesu zarządzania ryzykiem a łuki wskazują logiczne i czasowe następstwo przepływu informacji między poszczególnymi czynnościami realizowanymi w procesie zarządzania ryzykiem. Centralnym elementem w modelu zarządzania ryzykiem jest komunikacja, ponieważ bez efektywnych metod komunikowania żadne podejście do zarządzania ryzykiem nie umożliwi osiągnięcia sukcesu. Wymiana informacji o ryzyku na różnych poziomach organizacji, istotnych dla efektywnego wykonywania działań w ramach zarządzania ryzykiem jest niezwykle istotna z punktu widzenia powodzenia całości przedsięwzięcia informatycznego.



Rys. 1. Model zarządzania ryzykiem proponowany przez Software Engineering Institute

Identyfikacja ryzyka jest „inwentaryzacją” potencjalnych zagrożeń, zanim będą one wywierać wpływ na realizację przedsięwzięcia informatycznego. Rezultatem tej czynności jest lista specyficznych dla danego przedsięwzięcia elementów ryzyka.

Analiza ryzyka polega na dokładnym zbadaniu wszystkich zidentyfikowanych ryzyk w celu przekształcenia informacji o potencjalnych ryzykach w informację decyzyjną. Dla każdego zidentyfikowanego ryzyka oceniane jest prawdopodobieństwo jego wystąpienia i rozmiar potencjalnych start. Rozważa się również skutki jednoczesnego urzeczywistnienia się kilku elementów ryzyka.

Planowanie ryzyka polega na wykorzystaniu informacji o ryzykach w różnych decyzjach i działaniach mających na celu złagodzenie skutków urzeczywistnienia się ryzyk. Dla każdego elementu ryzyka powinien być określony sposób postępowania np.: łagodzenie, unikanie, akceptacja, transfer, pogłębiona analiza ryzyka.

Śledzenie ryzyka realizowane jest poprzez monitorowanie statusu ryzyk oraz działań rozpoczętych w celu łagodzenia lub unikania ryzyka.

Sterowanie ryzykiem jest czynnością polegającą na korygowaniu odchyleń od przewidywanych rezultatów działań podjętych w celu łagodzenia lub unikania ryzyka.

Dwie pierwsze czynności (identyfikacja i analiza) można określić jako działania zmierzające do oceny ryzyka a wykonywanie pozostałych czynności (planowanie, śledzenie i sterowanie) zmierza do obniżania ryzyka.

W dalszej części artykułu przedstawiono koncepcję metody oceny ryzyka co w kontekście opisanego wyżej modelu zarządzania ryzykiem oznacza koncepcję identyfikacji i analizy ryzyka.

2. Identyfikacja i analiza ryzyka

Stosowane w praktyce metody identyfikacji ryzyka są w swojej istocie bardzo podobne do siebie – polegają one na utworzeniu listy źródeł potencjalnych ryzyk dla konkretnego przedsięwzięcia informatycznego. Lista taka często jest przekształcana do pewnej struktury hierarchicznej. Poniżej przedstawiono fragment takiej struktury.

1. Środowisko wytwarzania:
    1.1. Proces wytwarzania:
        1.1.1. ....

1.2. Proces zarządzania przedsięwzięciem:

1.2.1. Planowanie

1.2.2. Organizacja projektu

1.2.3. ....

Do każdego elementarnego źródła ryzyka należy dołączyć pytanie lub listę pytań, które umożliwią identyfikację ryzyk związanych z danym źródłem. Ryzyka związane z planowaniem (1.2.1) oraz organizacją projektu (1.2.2) mogą być zidentyfikowane na podstawie następującej listy pytań:

1.2.1. <u>Planowanie:</u>

1.2.1.1. Czy przedsięwzięcie jest zarządzane zgodnie z planem ?

1.2.1.2. Czy plan przedsięwzięcia podlega reorganizacji stosownie do okoliczności ?

1.2.1.3. Czy każdy poziom zespołu wykonawczego jest uwzględniany w planowaniu zadań ?

1.2.1.4. Czy dla znanych ryzyk zostały utworzone plany awaryjne ?

1.2.2. <u>Organizacja projektu:</u>

1.2.2.1. Czy organizacja przedsięwzięcia informatycznego jest efektywna ?

1.2.2.2. Czy wszyscy członkowie zespołu wykonawczego dobrze rozumieją swoje role i role innych członków ?

1.2.2.3. Czy wszyscy członkowie zespołu wykonawczego dobrze rozumieją zakres odpowiedzialności swojej oraz innych członków zespołu ?

Przygotowanie wyczerpującego kwestionariusza umożliwiającego identyfikację wszystkich potencjalnych ryzyk nie jest trywialne. W literaturze można znaleźć wiele różnych szablonów kwestionariuszy służących identyfikacji ryzyka, które w razie potrzeby mogą być rozszerzona o szczególne pytania wynikające z specyfiki danego przedsięwzięcia informatycznego. Mimo że przygotowanie właściwego kwestionariusza oraz uzyskanie wyczerpujących odpowiedzi na zawarte w nim pytania jest bardzo pracochłonne (np. kwestionariusz identyfikacji ryzyka przygotowany przez SEI zawiera ok. 200 szczegółowych pytań), to trudno sobie wyobrazić inny sposób identyfikacji wszystkich ryzyk.

Czynnością następującą po identyfikacja ryzyka jest jego analiza, czyli przekształcenie informacji o zidentyfikowanych ryzykach w informację decyzyjną (określenie prawdopodobieństwa wystąpienia i ocena rozmiaru strat). W tym miejscu można postawić pytanie: czy kierownik projektu jest w stanie śledzić tak dużą ilość czynników wpływających na powodzenie przedsięwzięcia informatycznego ? Nawet jeśli odpowiedź na to pytanie jest pozytywna, to z pewnością każdy kierownik projektu chciałbym posiadać bardziej syntetyczną informację dotyczącą szansy powodzenia przedsięwzięcia informatycznego.

3. Wskaźnik zagrożenia przedsięwzięcia informatycznego

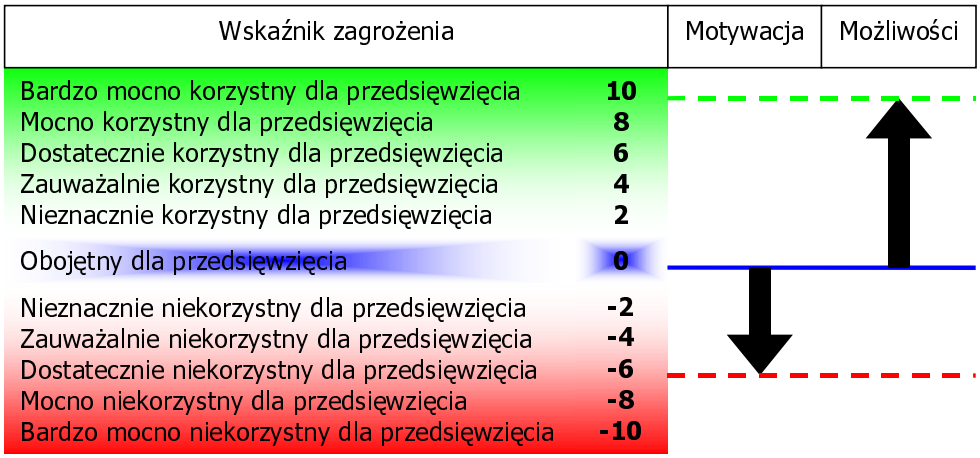
Każde przedsięwzięcie informatyczne jest realizowane w ustalonej konfiguracji klient – wykonawca. Przedstawiciele wysokiego szczebla obu stron takiej konfiguracji są zainteresowani aktualnymi szansami powodzenia realizowanego przedsięwzięcia informatycznego. Konieczna jest zatem syntetyczna miara takiej szansy, którą można określić jako wskaźnik zagrożenia przedsięwzięcia informatycznego. Wskaźnik taki powinien mieć dwie składowe reprezentujące odpowiednio:

- stan motywacji konfiguracji klient – wykonawca do pomyślnego zakończenia przedsięwzięcia informatycznego;
- stan możliwości wykonawczych konfiguracji klient – wykonawca pomyślnego zakończenia przedsięwzięcia informatycznego.

Rysunek 2 przedstawia propozycję zobrazowania wskaźnika zagrożenia wraz z interpretacją wartości jego składowych (przy założeniu, że wartość każdej składowej da się wyrazić w postaci liczby z zakresu [-10..10]).

Wyznaczenie wartości wskaźnika zagrożenia bezpośrednio na podstawie listy zidentyfikowanych ryzyk raczej nie jest możliwe, należy zatem wprowadzić pośredni poziom miar opisujących szansę powodzenia przedsięwzięcia informatycznego. Wartość składowych wskaźnika zagrożenia (motywacja i możliwości) może być wyznaczona na podstawie wartości tzw. sprawczych i wykonawczych czynników zagrożenia przedsięwzięcia informatycznego. Czynniki sprawcze zagrożenia przedsięwzięcia informatycznego opisują te elementy działalności konfiguracji klient – wykonawca oraz te właściwości (cechy) tej konfiguracji, które generują przyczyny upadku (lub powodzenia) przedsięwzięcia informatycznego. Czynniki wykonawcze zagrożenia przedsięwzięcia informatycznego opisują te elementy działalności konfiguracji klient – wykonawca oraz te właściwości (cechy) tej konfiguracji, które określają fizyczną realizowalność przedsięwzięcia informatycznego. Ilość czynników sprawczych i wykonawczych powinna być tak dobrana, aby zbiór wartości tych czynników ustalony dla określonej chwili był równie dobrą informacją decyzyjną dla kierownika projektu jak wartość wskaźnika zagrożenia, ale jednocześnie nie

powinien zwierać zbyt dużo informacji szczegółowych – ilość czynników sprawczych i wykonawczych powinna zwierać się w przedziale od ok. 10 do ok. 20.



Rys. 2. Zobrazowanie wskaźnika zagrożenia przedsięwzięcia informatycznego

Przy tak określonej semantyce sprawczych i wykonawczych czynników zagrożenia przedsięwzięcia informatycznego, oczywistym wydaje się fakt obliczenia wartości stanu motywacji konfiguracji klient – wykonawca na podstawie zbioru wartości czynników sprawczych zagrożenia przedsięwzięcia informatycznego, a wartości stanu możliwości wykonawczych konfiguracji klient – wykonawca na podstawie zbioru wartości czynników wykonawczych zagrożenia przedsięwzięcia informatycznego. Z kolei wartości czynników sprawczych i wykonawczych mogą być wyznaczone na podstawie listy zidentyfikowanych ryzyk, które będziemy nazywać czynnikami pierwotnymi zagrożenia przedsięwzięcia informatycznego. W tym celu dla każdego zidentyfikowanego ryzyka / czynnika pierwotnego należy określić:

- czy dany czynnik pierwotny wpływa na określony czynnik sprawczy czy wykonawczy ?
- liczbę określającą bieżący stopień urzeczywistnienia się danego ryzyka;
- jak dany czynnik pierwotny wpływa na określony czynnik sprawczy / wykonawczy – powoduje jego wzrost czy spadek ?

4. Sposób obliczania wartości czynników sprawczych i wykonawczych oraz wskaźnika zagrożenia

Jak pokazano w poprzednim rozdziale, czynniki pierwotne zagrożenia przedsięwzięcia informatycznego mogą być określone na podstawie kwestionariuszy identyfikacji ryzyka. Zatem ilość czynników pierwotnych może być w przybliżeniu równa ilości pytań zawartych w kwestionariuszu identyfikacji ryzyka. Zatem przedstawienie analizy każdego czynnika pierwotnego oraz sposobu przekształcenia wszystkich czynników pierwotnych w czynniki sprawcze i wykonawcze nie jest możliwe w niniejszym opracowaniu.

Niewątpliwie jednym z czynników wpływających na powodzenie przedsięwzięcia informatycznego są dobrze sformułowane i udokumentowane wymagania. Generalnie wymagania nie stanowią o fizycznych możliwościach realizacji przedsięwzięcia informatycznego, ale raczej są potencjałem wpływającym na powodzenie przedsięwzięcia informatycznego. Tak więc jednym z czynników sprawczych zagrożenia przedsięwzięcia informatycznego będzie „jakość wymagań".

Każda specyfikacja wymagań może być oceniona np. z punktu widzenia: stabilności, pełności, jasności i sprzeczności wymagań. Wymienione atrybuty wymagań stanowią zatem czynniki pierwotne zagrożenia przedsięwzięcia informatycznego. Przybliżona ocena tych atrybutów może być zrealizowana przy użyciu następującego kwestionariusza:

- Stabilność wymagań (StaW):
  - 4 - wymagania bardzo stabilne, gwarantowane dokumentami uzgodnionymi i podpisanymi przez przedstawicieli wysokiego szczebla ze strony klienta i wykonawcy;
  - 3 - wymagania stabilne, zdefiniowane w analitycznych dokumentach roboczych;
  - 2 - mała stabilność wymagań – nieformalne uzgodnienia między zespołem wykonawczym a użytkownikiem końcowym;
  - 1 – duża zmienność wymagań, brak pełnej koncepcji systemu ze strony klienta.
- Pełność wymagań (PełW):
  - 4 - wymagania pełne dla każdego fragmentu systemu, zdefiniowane na wszystkich poziomach ogólności;
  - 3 - brak drugorzędnych wymagań dla wybranych elementów systemu;
  - 2 - brak istotnych wymagań dla niektórych kluczowych elementów systemu;

- 1 - brak zasadniczych wymagań, uniemożliwiających rozpoczęcie prac.

- Jasność wymagań (JasW):
  - 4 - wymagania jasne, zrozumiałe dla wszystkich zainteresowanych członków zespołu wykonawczego;
  - 3 - niejasne sformułowanie drugorzędnych wymagań dla wybranych elementów systemu;
  - 2 - niejasne sformułowanie istotnych wymagań dla niektórych kluczowych elementów systemu;
  - 1 - niejasne sformułowanie zasadniczych wymagań, uniemożliwiające rozpoczęcie prac.
- Sprzeczność wymagań (SprW):
  - 4 - sprzeczność zasadniczych wymagań, uniemożliwiająca realizację systemu;
  - 3 - sprzeczność istotnych wymagań, wymagająca dokładnego sprecyzowania wymagań użytkownika;
  - 2 - sprzeczność wymagań drugorzędnych, które nie mają większego wpływu na realizację systemu;
  - 1 - brak sprzecznych wymagań.

Zakładając, że stabilność, pełność, jasność i sprzeczność wymagań w pełni określa jakość zdefiniowanych wymagań, można skonstruować formułę reprezentującą wartość czynnika sprawczego „jakość wymagań" (JakWym):

$$JakWym = (StaW \times PełW \times JasW) / SprW \qquad a = 0{,}25 \leq JakWym \leq 64 = b$$

Ponieważ inne czynniki sprawcze i wykonawcze mogą mieć inny zakres wartości dopuszczalnych ($JakWym \in [0{,}25..64]$), należy dokonać takiej transformacji formuł dla wszystkich czynników, aby uzyskać zakres wartości dopuszczalnych [-10..10]. Ułatwi to porównywanie wartości poszczególnych czynników między sobą oraz zapewni pożądany zakres zmienności wyliczanego wskaźnika zagrożenia (czyli [-10..10]).

Dla czynnika JakWym formuła transformująca będzie miała następującą postać:

$$JakWym' = JakWym - 10{,}25 + [(JakWym - 0{,}25) / 63{,}75] \times (-43{,}75)$$

W ogólnym przypadku, formuła transformująca jest następująca:

$$C' = C - 10 - a + [(C - a) / (b - a)] \times (20 - b + a)$$

gdzie:

- C' – wartość określonego czynnika sprawczego lub wykonawczego po transformacji;
- C – wartość określonego czynnika sprawczego lub wykonawczego przed transformacją;
- a – minimalna dopuszczalna wartość czynnika;
- b – maksymalna dopuszczalna wartość czynnika.

Przedstawienie sposobu obliczania wartości wszystkich czynników sprawczych i wykonawczych wykracza poza możliwości niniejszego artykułu, dlatego dalsze rozważania będą prowadzone przy następujących założeniach:

- zdefiniowany został zbiór czynników pierwotnych zagrożenia $P = (p_1, p_2,...,p_k)$;
- dla każdego czynnika pierwotnego skonstruowany został kwestionariusz oceny wartości danego czynnika, umożliwiający ustalenie jego bieżącej wartości należącej do przedziału $[a..b]$, gdzie $a = 1$, b – dowolna liczba naturalna większa od 1;
- zdefiniowany został zbiór czynników sprawczych zagrożenia $C = (c_1, c_2,...,c_n)$;
- dla każdego czynnika sprawczego zdefiniowana została formuła przedstawiająca zależność między wybranymi czynnikami pierwotnymi zagrożenia a danym czynnikiem sprawczym;
- zdefiniowany został zbiór czynników wykonawczych zagrożenia $E = (e_1, e_2,...,e_m)$;
- dla każdego czynnika sprawczego zdefiniowana została formuła przedstawiająca zależność między wybranymi czynnikami pierwotnymi zagrożenia a danym czynnikiem wykonawczym.

Niech $R = (M, P)$ oznacza wskaźnik zagrożenia przedsięwzięcia informatycznego, gdzie:

- $M \in [-10..10]$ – oznacza stan motywacji do pomyślnego zakończenia przedsięwzięcia informatycznego;
- $P \in [-10..10]$ – oznacza stan możliwości wykonawczych pomyślnego zakończenia przedsięwzięcia informatycznego.

Najprostszym sposobem ustalenia wartości stanu motywacji oraz stanu możliwości jest wyznaczenie wartości „wypadkowej: odpowiednio czynników

sprawczych oraz czynników wykonawczych zagrożenia przedsięwzięcia informatycznego:

$$M = \sum_{i=1}^{n} \left(w_i^c \times c_i \right) \qquad P = \sum_{i=1}^{m} \left(w_i^e \times e_i \right)$$

gdzie:

w_i^c - oznacza wagę i-tego czynnika sprawczego

w_i^e - oznacza wagę i-tego czynnika wykonawczego

Skonstruowany w ten sposób wskaźnik zagrożenia przedsięwzięcia informatycznego jest dobrą miarą szansy powodzenia przedsięwzięcia informatycznego. Niewątpliwie żaden wskaźnik nie zastąpi zdrowego rozsądku kierownika projektu, który często intuicyjnie podejmuje pewne działania naprawcze w czasie realizacji przedsięwzięcia, ale z pewnością może być przydatny w różnych sytuacjach decyzyjnych.

Bibliografia

[1]. Carr M., Konda S., Monarch I., Ulrich F., Walker C. – Tacxonomy Based Risk Identification, Carnegie Mellon University Software Engineering Institute, Technical Report 1993

[2]. Gallagher B. – Software Acquisition Risk Management Key Process Area (KPA) A Guidebook, Carnegie Mellon University Software Engineering Institute, 1999

[3]. Austarlian Standard on Risk Management, AS/NZS 4360:1995

[4]. Nowicki T., Najgebauer A., Ulicki M., Machała W. – Opracowanie bazy danych dla potrzeb komputerowego wspomagania systemu wczesnego ostrzegania, Wojskowa Akademia Techniczna Wydział Cybernetyki Instytut Systemów Informatycznych, 1997