

# Leonard Rozenberg, Magdalena Kieruzel

---

## Pomiar i kontrola ryzyka projektu informatycznego

---

Ekonomiczne Problemy Usług nr 58, 543-550

---

2010

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

*LEONARD ROZENBERG, MAGDALENA KIERUZEL*

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

lrozenberg@wi.zut.edu.pl, mkieruzel@wi.zut.edu.pl

## POMIAR I KONTROLA RYZYKA PROJEKTU INFORMATYCZNEGO

### Wprowadzenie

W trakcie realizacji każdego projektu napotkać można na szereg zagrożeń, których źródła tkwią zwykle w zasobach ludzkich lub rzeczowych, u nierzetelnych podwykonawców, w wybranej technologii, czy w środowisku. Aby ryzyko minimalizować, należy móc je identyfikować, móc oceniać wielkość i wpływ na projekt, analizować przyczyny i skutki, tworzyć mechanizmy kontroli ryzyka oraz podejmować szybko stosowne działania prewencyjne lub korygujące.

Ryzyko to rodzaj wątpliwości, czy uzyskamy zaplanowany wynik (w ujęciu pozytywnym traktowany jako szansa, albo w ujęciu negatywnym postrzegany jako zagrożenie). Podejmowanie ryzyka jest wpisane w każdy proces biznesowy.

Według P. Wróblewskiego<sup>1</sup> ryzyko jest zdarzeniem, które w trakcie realizacji projektu może doprowadzić do niepożądanego rezultatu. Wróblewski wprowadza pewne uproszczenie w postrzeganiu ryzyka, utożsamiając je tylko z potencjalnym problemem w realizacji projektu.

K. Frączkowski<sup>2</sup> przy określaniu zagrożeń dla projektu posługuje się dwoma określeniami. Definiuje z jednej strony ryzyko jako szansę, że niebezpieczeństwo pojawi się w projekcie, przynosząc skutki określone z pewnym prawdopodobieństwem, podkreślając, że ryzyko jest zjawiskiem permanentnym. Z drugiej strony określa niepewność jako „niemożność uzyskania informacji, charakteryzującą się

---

<sup>1</sup> P. Wróblewski: *Zarządzanie projektami informatycznymi dla praktyków*, Wydawnictwo Helion, 2005.

<sup>2</sup> K. Frączkowski: *Zarządzanie projektem informatycznym*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003.

brakiem wpływu na zmianę sytuacji – niepewność nie podlega ocenie za pomocą prawdopodobieństwa i minimalizacji”.

## 1. Kontrola ryzyka według metodyki PRINCE2

Każdy projekt poddawany jest nieustannym zmianom, zarówno tym występującym w bezpośrednim otoczeniu, jak i w dalszym środowisku.

Zmiany dotyczą również zagrożeń, na które narażony jest projekt. W trakcie postępów prac pojawiają się nowe ryzyka, istotność innych zmienia się, a jeszcze inne tracą na znaczeniu. Dlatego cykl zarządzania ryzykiem w projekcie powinien być kilkakrotnie powtarzany.

W metodyce PRINCE2 cykl zarządzania ryzykiem realizowany jest w kilku głównych etapach.

Pierwszym etapem jest identyfikacja zagrożeń, a metodyka PRINCE2 wyróżnia kilka podstawowych kategorii ryzyka, które mogą stanowić punkt początkowy dla procesu identyfikacji. Główne obszary ryzyka organizacji w odniesieniu do projektów to<sup>3</sup>:

- ryzyka strategiczne, handlowe (np. bankructwo wykonawców, zmienność rynku, niespełnienie przez dostawców zobowiązań wynikających z umowy w aspekcie jakości, ilości, terminów),
- ryzyka techniczne, eksploatacyjne, infrastrukturalne (np. błąd ludzki, niedbalstwo zawodowe, błędy wykonawcze),
- ryzyka ekonomiczne, finansowe, rynkowe (np. inflacja, zmienność kursów walut, niestabilność stóp procentowych),
- ryzyka prawne (np. nowe zmienione prawo, które unieważnia założenia będące podstawą dla działań w projekcie, wymagania licencyjne, zmiany w strukturze podatków),
- ryzyka organizacyjne, zarządcze (np. słabe przywództwo, zła polityka firmy, niekompetentne zarządzanie, niekompletne informacje),
- ryzyka środowiskowe (np. katastrofy naturalne, problemy transportowe).

Ważne jest, aby przy identyfikacji ryzyka nie dokonywać jego oceny. Mogłoby to bowiem doprowadzić do nieuzasadnionych decyzji o wykluczeniu danego ryzyka z listy potencjalnych zagrożeń lub też zmiany jego pozycji w hierarchii ryzyk. Wszystkie ryzyka zostają wpisane do tzw. Rejestru Ryzyka prowadzonego i uzupełnianego w trakcie realizacji projektu.

Drugim etapem zarządzania ryzykiem jest właśnie ocena zagrożeń. W omawianej metodyce przyjmuje się, że ryzyko projektu określają dwie miary tj. praw-

---

<sup>3</sup> *Managing Successful Projects with Prince2*, The Stationery Office Ltd., CCTA, Norwich 2002.

dopodobieństwo wystąpienia ryzyka oraz jego wpływ na projekt. Jest to tożsame z propozycją przedstawioną przez Frączkowskiego, który określa wartość pojędynczego ryzyka, jako:

$$\text{Ryzyko}(i) = S(i) \cdot \text{Prob}(i) \quad (1)$$

gdzie:

$i$  – licznik identyfikowanego ryzyka,

$\text{Prob}(i)$  – oszacowane prawdopodobieństwo wystąpienia  $i$ -tego ryzyka,

$S(i)$  – oszacowany skutek wystąpienia  $i$ -tego ryzyka.

Dokonując oceny ryzyka zajmujemy się więc z jednej strony oszacowaniem faktycznego prawdopodobieństwa wystąpienia określonego ( $i$ -tego) zdarzenia, a z drugiej strony określamy jego stopień oddziaływania (wpływu) na projekt. Wpływ danego zdarzenia może być rozpatrywany pod kątem takich elementów, jak: czas, koszty, jakość, zakres, korzyści czy zachowania ludzkie.

Łączne ryzyko można – korzystając z oznaczeń do poprzedniego wzoru – opisać zależnością:

$$\text{Ryzyko\_Łączne} = \sum_{i=1}^n S(i) \cdot \text{Prob}(i) \quad (2)$$

W przypadku niektórych rodzajów ryzyk dość oczywiste jest przedstawienie ich w postaci danych finansowych, istnieją jednak pewne niemierzalne zagrożenia, które mogą być szacowane subiektywnie przez ekspertów, czyli osoby mające doświadczenie w danych ryzykach projektu. Szacowanie to może polegać na przypisaniu określonych wag prawdopodobieństwu i wpływowi.

Pomimo wprowadzonych w metodyce PRINCE2 sposobów oceny ryzyka przez pryzmat prawdopodobieństwa ich wystąpienia oraz wpływu na projekt nie otrzymujemy miary ryzyka w wymiarze finansowym. Łączny rezultat przeliczenia ryzyka według wzoru (2) w PRINCE2 skutkuje jedynie zakwalifikowaniem danego zagrożenia do klasy ryzyka niskiego, średniego bądź wysokiego, czyli umożliwia realizację oceny ryzyka na przykład metodą indeksów ryzyka operacyjnego. Taki sposób prezentacji ryzyka nie jest zbyt wygodny, szczególnie wtedy, gdy chcemy porównać te same zagrożenia z różnych projektów.

Najbardziej naturalnym sposobem waluacji ryzyka przy projektowaniu i wdrażaniu projektów informatycznych jest pokazanie ryzyka w kategoriach pieniężnych. Służyć temu może choćby użycie metodyki VaR, o czym poniżej.

## 2. Pomiar ryzyka dla projektów informatycznych

Zgodnie z istotą zarządzania ryzykiem należy utrzymać ryzyko na takim poziomie, który będzie akceptowalny, czyli zapewnić takie warunki, w których nie poniesiemy (w wyniku wystąpienia zdarzenia) strat większych niż założono.

Pomocne w realizacji tego założenia może być określenie wartości narażonej na ryzyko, czyli VaR (*Value at Risk*). Miara VaR (w tłumaczeniu: wartość zagrożona, wartość ryzykowana, wartość narażona na ryzyko) była dotąd stosowana głównie w obszarze zarządzania ryzykiem portfela kredytowego banku. Według P. Besta VaR „jest statystyczną miarą ryzyka, która szacuje maksymalną stratę na portfelu, jaka może wystąpić przy założonym poziomie ufności”.

Nieco inną, pełniejszą, definicję przedstawia A. Langner: „*Value at Risk* to maksymalna oczekiwana wartość straty wartości rynkowej, która może wystąpić w normalnych warunkach rynkowych w określonym czasie i z określonym prawdopodobieństwem”. Jak podaje K. Kuziak, VaR jest obecnie „najpopularniejszym rozwiązaniem, jeśli chodzi o pomiar ryzyka rynkowego”, można stosować ten miernik również w przypadku innych niż ryzyko rynkowe rodzajów ryzyka finansowego. Wartość narażona na ryzyko, jako podstawa dla innych miar ryzyka w przedsiębiorstwie, może posłużyć wyznaczeniu wielu różnych miar, z których wymienimy: EaR (*Earnings at Risk*), CFaR (*Cash Flow at Risk*) oraz LaR (*Liquidity at Risk*).

Dla obliczania ryzyka przy pomocy VaR stosowanych jest wiele metod:

- metoda wariancji-kowariancji,
- metoda symulacji historycznej,
- metoda symulacji Monte Carlo i Vegas,
- metoda wyznaczania kwantyla dowolnego rozkładu,
- podejście oparte na teorii wartości ekstremalnych,
- podejście oparte na wykorzystaniu wartości pochodzących z ogona rozkładu.

Ze względu na prosty sposób obliczeń najczęściej stosowana jest metoda wariancji-kowariancji. Wykorzystujemy tutaj współczynnik zmienności w postaci odchylenia standardowego. Jest to możliwe dzięki przyjętemu założeniu, że procentowe zmiany np. cen na rynkach finansowych mają rozkład normalny.

Chcąc wyliczyć potencjalną stratę dla pojedynczego aktywum posłużymy się wzorem<sup>4</sup>:

$$\text{VaR}(i) = V(i) \cdot P(i) \quad (3)$$

gdzie:

V(i) – zmienność (w naszym przypadku wartość odchylenia standardowego dla pojedynczego aktywum),

P(i) – wartość pojedynczego aktywum.

<sup>4</sup> P. Best: *Wartość narażona na ryzyko*, Oficyna Ekonomiczna, Kraków 2000.

Wyznaczając VaR za pomocą wzoru (3) należy przyjąć założenie co do rozkładu prawdopodobieństwa naszych obserwacji. Zakładając, że jest to rozkład normalny, wzór (3) uzupełnimy o wartość dystrybuanty odczytanej z tablic rozkładu normalnego standaryzowanego<sup>5</sup> i w wyniku tego otrzymujemy:

$$\text{VaR}(i) = c \cdot \sigma(i) \cdot P(i) \quad (4)$$

gdzie:

$c$  – percentyl rozkładu normalnego zależny od poziomu ufności,

$\sigma(i)$  – zmienność – wartość odchylenia standardowego,

$P(i)$  – wartość waloru, czyli wielkość ekspozycji na ryzyko.

Prezentowany sposób waluacji ryzyka metodą VaR odnosił się do pojedynczego aktywum. W praktyce możemy wyznaczyć wartość narażoną na ryzyko dla dowolnej ilości aktywów według wzoru:

$$\text{VaR} = \sqrt{\sum_{i=1}^n \mu^2(i) \cdot \sigma^2(i) + 2 \cdot \sum_{i=1}^n \sum_{j=1}^n \mu(i) \cdot \mu(j) \cdot r(i, j)} \quad (5)$$

gdzie:

$\mu(i)$  – udział wartościowy  $i$ -tego aktywum w portfelu,

$r(i, j)$  – współczynnik korelacji między stopami zwrotu aktywów  $i, j$ .

Przedstawione powyżej rozważania znalazły już należne im miejsce w praktyce rynku akcji. Metoda VaR może być jednak z powodzeniem stosowana także do waluacji ryzyka w projektach informatycznych. Biorąc pod uwagę procesowy charakter prac projektowych można w projekcie informatycznym dokonać dekompozycji zestawu działań, a następnie wyliczyć dla poszczególnych czynności odpowiadające im ryzyka. W rezultacie można będzie wyznaczyć VaR dla całego projektu.

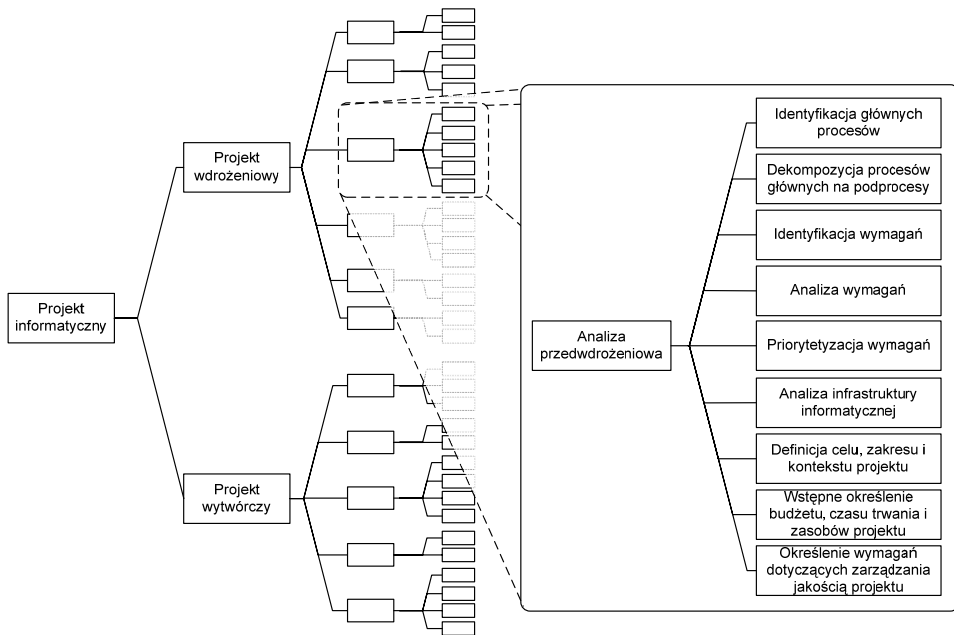
Przystępując do określenia ryzyka projektu, także projektu informatycznego, musimy dokonać identyfikacji poszczególnych działań w projekcie. Przebieg procesów w projekcie informatycznym najlepiej przedstawić w postaci drzewa czynności, na przykład zgodnie z rysunkiem 1.

Na rysunku 1 pokazano dekompozycję czynności dla przykładowego procesu analizy przedwdrożeniowej, gdzie wyznaczono czynności składowe konieczne w jego realizacji. Podobna dekompozycja może być przedstawiona dla dowolnego

---

<sup>5</sup> E. Majerowska: *Wartość narażona na ryzyko a ryzyko inwestowania w akcyjne fundusze inwestycyjne*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 415, Prace Ekonometrii i Statystyki nr 16, 2005.

procesu. Aby określić całkowite ryzyko, z jakim wiąże się realizacja projektu, konieczne jest określenie poszczególnych ryzyk dla każdego procesu. To z kolei może być wyznaczone poprzez wartość ryzyka (VaR) liczoną, jako iloczyn prawdopodobieństwa ryzyka niepowodzenia procesu i wartości narażonej na ryzyko. Przez wartość narażoną na ryzyko będziemy rozumieli wartość realizacji procesu w projekcie.



Rys. 1. Przykładowe drzewo czynności projektu informatycznego

Źródło: opracowanie własne.

Dla zarządzających firmą, a szczególnie dla wydających zgodę na realizację projektu informatycznego istotna jest informacja o ogólnym ryzyku, na jakie narażony jest projekt.

Metoda VaR może wspierać określenie całkowitego ryzyka dla projektu w wymiarze finansowym. Otrzymana wartość jest podstawą do porównania ryzyka w różnych projektach.

## Podsumowanie

Zmiany zachodzące w otoczeniu powodują, że współczesne przedsiębiorstwo staje ciągle wobec realiów, nowych wyzwań i ryzyk. Z każdej strony pojawiają się

naciski na wprowadzanie nowych rozwiązań we wszystkich sferach działalności, czyli produkcji, technologii, marketingu itp. Odpowiedni system informatyczny może okazać się czynnikiem decydującym o sukcesie przedsiębiorstwa w rywalizacji z konkurencją. Tymczasem, według badań Standish Group, niemal 70% firm jest niezadowolonych z efektów nowych wdrożeń IT. Według najnowszego raportu Standish Group<sup>1</sup>, badającego sytuację w firmach amerykańskich, jedynie 32% wszystkich projektów IT kończy się sukcesem.

Jedną z przyczyn tak częstych porażek projektów IT jest wybór źle „wyskalowanego” systemu – zbyt małego lub, co bywa dość częstym zjawiskiem w ostatnich latach, zbyt dużego. Wzrost gospodarczy, jaki poprzedzał obecny kryzys, spowodował, że wiele firm wydawało na swoje funkcjonowanie więcej, niż wskazywałyby na to ich realne potrzeby. Działając w okresie prosperity firmy te zapomniały o ryzyku, rozbudowując niektóre obszary działalności o niepotrzebne struktury, procesy czy komórki organizacyjne.

Jednym z przykładów poluzowania dyscypliny finansowej firm jest właśnie wybór zbyt rozbudowanego systemu informatycznego wykraczającego poza aktualne oraz planowane potrzeby przedsiębiorstwa. Często okazuje się, że koszty implementacji i utrzymania tych efektywnych i bogatych w tzw. nowinki techniczne rozwiązań są znacznie wyższe niż korzyści z nich płynące. Owa nieopłacalność szczególnie uwidacznia się w czasie dekonjunktury gospodarczej, kiedy firmy szukają oszczędności<sup>6</sup>.

Wdrożenie zbyt rozbudowanego systemu informatycznego naraża firmy na dwa rodzaje ryzyk (strat).

Pierwsze powoduje konieczność poniesienia kosztów optymalizacji wdrożonego systemu i dostosowania go do faktycznych potrzeb przedsiębiorstwa. Uporczywe trwanie przy źle dobranym systemie, oprócz znacznego obciążenia dla budżetu firmy, w sposób nieunikniony prowadzi do zwiększania dystansu do firm konkurencyjnych, które w kryzys weszły z odpowiednimi systemami.

Drugi rodzaj ryzyka wynika z czasochłonności i pracochłonności procesów dostosowawczych, niezbędnych w rezultacie wyboru nieoptymalnego lub źle wyskalowanego rozwiązania. Czas i energia potrzebne do przeprowadzenia wymaganych zmian mogłyby zostać wykorzystane przez przedsiębiorstwo na szukanie aktywnych sposobów walki z kryzysem, np. poprzez opracowywanie nowych strategii biznesowych.

Aby zwiększyć szansę powodzenia procesów dostosowawczych i uniknąć skutków ryzyk, które doprowadziły do konieczności modyfikacji systemu, warto skorzystać z metodyki VaR. Trzeźwe spojrzenie pozwala na kontrolowanie działań, jak również racjonalizowanie oczekiwań i potrzeb generowanych przez użytkowni-

---

<sup>6</sup> Monday PR [online]: <http://prportal.pl/2009/05/efektywny-system-it-solidna-podstawa-sukcesu-firmy> [dostęp: 2009].



ków – szczególnie oczekiwań polegających na rozbudowie systemów w kierunku rozwiązań, do których użytkownicy są przyzwyczajeni, tak aby modyfikowany system był w efekcie odpowiednio wyskalowany i dostosowany do potrzeb przedsiębiorstwa. Nie można też zapominać, że zanim rozpoczęty zostanie proces minimalizacji ryzyk systemu, należy poddać analizie procesy biznesowe przedsiębiorstwa i jeśli jest to konieczne, również one powinny zostać zoptymalizowane pod kątem ryzyka.

### Literatura

1. Best P.: *Wartość narażona na ryzyko*, Oficyna Ekonomiczna, Kraków 2000.
2. Frączkowski K.: *Zarządzanie projektem informatycznym*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003.
3. Kalinowski M.: *Zarządzanie ryzykiem walutowym w przedsiębiorstwie*, CeDeWu, Warszawa 2007.
4. Majerowska E.: *Wartość narażona na ryzyko a ryzyko inwestowania w akcyjne fundusze inwestycyjne*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 415, Prace Ekonometrii i Statystyki nr 16, 2005.
5. *Managing Successful Projects with Prince2*, The Stationery Office Ltd., CCTA, Norwich 2002.
6. Monday PR [online]: <http://prportal.pl/2009/05/efektywny-system-it-solidna-podstawa-sukcesu-firmy> [dostęp: 2009].
7. Wróblewski P.: *Zarządzanie projektami informatycznymi dla praktyków*, Wydawnictwo Helion, 2005.

## MEASUREMENT AND CONTROL THE RISK IN AN IT PROJECT

### Summary

Managing of risk is mainly getting along with the situation when the project is exposed on any risk. The aim is to control the degree of this exposing by keeping the risk on the acceptable level in a cost effective way. In this article it is shown how to measure the risk in the IT project, which uses the Value at Risk.

*Translated by Magdalena Kieruzel*