Tomasz Parys

Ryzyko w projektach wdrożeniowych zintegrowanych systemów informatycznych : próba klasyfikacji pod kątem barier i działań nim obarczonych

Problemy Zarządzania 10/3, 41-53

2012

Problemy Zarządzania, vol. 10, nr 3 (38): 41–53
ISSN 1644-9584, © Wydział Zarządzania UW
DOI 10.7172.1644-9584.38.3

Ryzyko w projektach wdrożeniowych zintegrowanych systemów informatycznych – próba klasyfikacji pod kątem barier i działań nim obarczonych

Tomasz Parys

Zasadniczym celem niniejszego opracowania jest ukazanie miejsca, jakie zajmuje ryzyko w projekcie wdrożeniowym zintegrowanego systemu informatycznego. Przybliżono podstawowe zagadnienia związane ze specyfiką projektu wdrożeniowego, podano definicję ryzyka oraz omówiono jego podział i obszary występowania, a także kluczowe jego czynniki. Zasadniczą część artykułu stanowi prezentacja autorskiej koncepcji klasyfikacji ryzyka oraz opis poszczególnych kategorii w kontekście działań nim obarczonych.

1. Wprowadzenie

Decyzja o informatyzacji jest wielkim wydarzeniem w działalności każdego przedsiębiorstwa. Związana jest zazwyczaj z wielkimi nadziejami, którym towarzyszą nie mniejsze obawy. Informatyzacja to z jednej strony ogromne koszty, z drugiej zaś konieczność przeprowadzenia wielu zmian zarówno w sferze organizacji działania, jak i metod działalności biznesowej. Każde wdrożenie, jako przedsięwzięcie informatyczne wywołujące zmiany w przedsiębiorstwie, jest obarczone ryzykiem niepowodzenia. W niniejszym opracowaniu po syntetycznym przedstawieniu zagadnień związanych w definicją ryzyka oraz jego cechami podjęto próbę klasyfikacji działań wdrożeniowych i związanego z nimi ryzyka wraz zakresem oddziaływania na projekt wdrożeniowy.

2. Specyfika projektu wdrożeniowego

Projekt informatyczny można zdefiniować jako „przedsięwzięcie o charakterze tymczasowym, nastawione na stworzenie unikalnego produktu lub usług, (...) które wykorzystując narzędzia informatyczne bazujące na technologii komputerowej, przyczynią się do poprawy funkcjonowania organizacji w zakresie ich zastosowania" (Szyjewski 2001b). Rozwijając powyższą definicję, należy zauważyć, że projekt jest zdarzeniem jednorazowym, realizowanym w przedsiębiorstwie po raz pierwszy i jest nastawiony na określony cel. Cel

ten bardzo często wynika z ogólnej koncepcji funkcjonowania organizacji. Jest zatem sformułowany albo w strategii, albo też stanowi część definicji celów przedsięwzięcia informatycznego. Każdy projekt ma wewnętrzną organizację, która jest dla niego specyficzna i nie jest ujęta w strukturach organizacyjnych firmy. Projekt jest złożony, co oznacza, iż składa się on z elementów, które można wyodrębnić, a które wzajemnie tworzą jedną całość. Działania w nim wykonywane są wyraźnie wyodrębnione spośród innych. Oznacza to, że projekt nie jest powiązany z żadnym (ani rutynowym, ani bieżącym, tj. operacyjnym) działaniem przedsiębiorstwa. Jest on także ograniczony, co głównie związane jest z ograniczeniami zasobów, jakie są niezbędne do jego przeprowadzenia (finanse, czas, specjaliści). Każdy projekt jest także przedsięwzięciem ryzykownym, ponieważ podczas całego czasu swojego trwania jest narażony na ryzyko niepowodzenia. Projekt wdrożeniowy realizowany jest na wielu płaszczyznach i swoim zakresem obejmuje zazwyczaj kilka obszarów jednocześnie. Działania wykonywane w ramach projektu poza kwestiami czysto technicznymi dotykają także sfery aktywności biznesowej, oddziałują na pracowników oraz na otoczenie socjologiczne przedsięwzięcia.

Ze względu na fakt, iż wiele działań w projekcie wykonywanych jest po raz pierwszy lub w nowych, nieznanych warunkach, pojawia się niepewność. Dotyczy ona zarówno wykonywania działań, jak i ich skutków. W takiej sytuacji pojawia się ryzyko, że podejmowane działania mogą zakończyć się niepowodzeniem lub ich wykonanie zostanie zakłócone. W praktyce niepewność i ryzyko są ze sobą ściśle powiązane (Szyjewski 2004). Dzieje się tak dlatego, ponieważ działania obarczone ryzykiem dotyczą nieprzewidywalnej przyszłości (Pritchard 2002).

Niestety, tylko nieliczne projekty wdrożeniowe kończą się sukcesem. Sukces projektu wdrożeniowego pozostaje w ścisłej zależności z wielkością systemu, który objęty jest danym przedsięwzięciem. Im większy projekt, tym mniejsze prawdopodobieństwo, że zakończy się sukcesem, natomiast znacznie większe, iż projekt taki zostanie przerwany (Stanik i Szewczuk 2001). Prawdopodobieństwo niepowodzenia projektu wdrożeniowego wzrasta wraz z rozmiarem systemu, co jest związane ze specyfiką przebiegu przedsięwzięć informatycznych. Szczególny wpływ ma tutaj stosunkowo duża trudność określenia sytuacji niekorzystnych, które mogą zakłócać przebieg prac. Nieodłącznym elementem każdego przedsięwzięcia informatycznego są niepewność, pojawiające się bariery i wynikające z nich zagrożenia, które określane są wspólnym mianem ryzyka przedsięwzięcia.

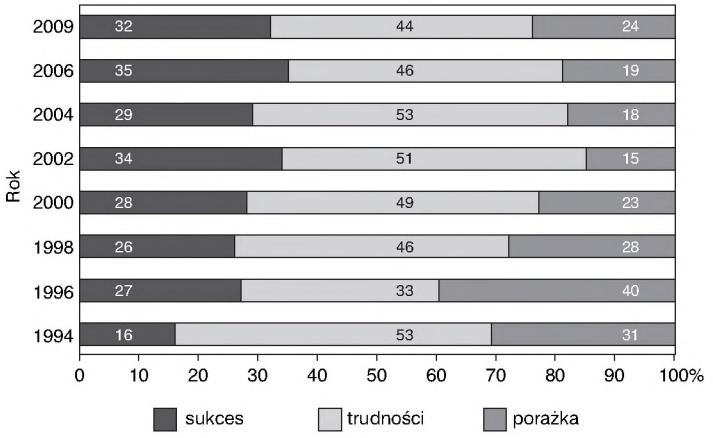
Rysunek 1 przedstawia, jak rozkładał się odsetek projektów wdrożeniowych zakończonych sukcesem w odniesieniu do tych stwarzających problemy oraz zakończonych porażką na przestrzeni lat 1994–2009.

Analizując zobrazowane na wykresie dane, można sformułować dwa następujące wnioski:

– na przestrzeni wielu lat objętych zakresem analizy (1994–2009) zdecydowana większość projektów generowała problemy lub zakończyła się porażką;

- odsetek projektów zakończonych sukcesem pozostawał na poziomie poniżej 35% (jedynie w 2006 r. osiągnął ten poziom);
- zależności pomiędzy wymienionymi kategoriami projektów pozostawały w bardzo podobnych relacjach – zmiany zazwyczaj nie przekraczały 5%;
- pomimo stosowania coraz doskonalszych metod i narzędzi zarządzania projektami, odsetek projektów generujących problemy w ich realizacji lub zakończonych porażką pozostaje bardzo duży (68% w 2009 r.).

Wynika z tego, że ryzyko niepowodzenia projektu wdrożeniowego (lub zakłóceń w jego przebiegu) jest wysokie i należy podejmować próby zidentyfikowania go, określenia jego rozmiaru, sklasyfikowania i zarządzania nim.



Rys. 1. Odsetek projektów zakończonych sukcesem, porażką oraz sprawiających trudności. Źródło: http://www.projectsmart.co.uk/the-curious-case-of-the-chaos-report-2009.html, odczyt: grudzień 2011.

3. Ryzyko – definicja, podział, obszary występowania

Literatura przedmiotu dostarcza wiele definicji ryzyka, z których następujące wydają się najpełniejsze i najlepiej oddające specyfikę zjawiska (Stanik i Szewczuk 2001; Duncan 1996):

1. *Ryzyko* to „możliwość klęski (niepowodzenia) przedsięwzięcia, możliwość wystąpienia niechcianej sytuacji, której urzeczywistnienie wpłynie na obniżenie poziomu sukcesu przedsięwzięcia informatycznego (łącznie z całkowitym brakiem sukcesu czyli klęską)".
2. *Ryzyko* jest „szansą jakiegoś wydarzenia, którego urzeczywistnienie będzie miało wpływ na realizację zamierzonego celu".
3. *Ryzyko* jest „możliwością doświadczenia niepowodzenia".

4. *Ryzyko* jest „zobiektywizowaną niepewnością wystąpienia niepożądanego zdarzenia" (Woodward, Hemel i Hedley 1979)[1].

Literatura przedmiotu podaje wiele klasyfikacji ryzyka oraz metod jego oceny. W zależności od przyjętego kryterium można wskazać wiele klasyfikacji. Jako ilustrację problemu przedstawiono w pracy syntetyczną klasyfikację ryzyka.

Najogólniejszą klasyfikacją ryzyka jest jego podział na podstawie kryterium typu. Według niego podział ryzyka kształtuje się następująco:
- *ryzyko typowe* – występuje przy realizacji każdego projektu informatycznego, niezależnie od dziedziny, jakiej dotyczy; jego wystąpienie wynika ze specyfiki i charakteru przedsięwzięcia informatycznego;
- *ryzyko specyficzne* – ściśle związane ze specyfiką dziedziny, jakiej dotyczy wdrażany w ramach projektu system informatyczny; ryzyko tego typu występuje w przypadku każdego konkretnego przedsięwzięcia realizowanego np. na indywidualne zamówienie, na podstawie specjalnej lub niestandardowej metodyki czy też przy zastosowaniu specjalnych narzędzi; pojawia się ono zawsze wtedy, gdy działanie nacechowane jest indywidualnością.

Stosując kryterium poziomu informacji, można dokonać następującego podziału ryzyka (Kaczmarek 2002; Stanik i Szewczuk 2001):
- *ryzyko znane* (*know risk*) – ryzyko można zaklasyfikować do tej grupy, jeżeli na podstawie analizy projektu, potencjalnych źródeł wystąpienia ryzyka, przeprowadzenia symulacji możliwe jest jego zidentyfikowanie oraz określenie z pewną dokładnością konkretnych zdarzeń, jakie mogą zaistnieć;
- *ryzyko przewidywalne* (*predictable risk*) – ryzyko należy do tej grupy wtedy, gdy na podstawie wiedzy osób zaangażowanych w projekt (kierownik projektu, konsultanci, informatycy) można wyznaczyć źródła wystąpienia potencjalnego ryzyka oraz oszacować poziom zagrożenia dla projektu spowodowanego wystąpieniem tego ryzyka;
- *ryzyko nieprzewidywalne* (*unpredictable risk*) – występuje wtedy, kiedy nie można przewidzieć zarówno wystąpienia niepożądanych zdarzeń, jak i ich skutków; można o nim mówić zawsze wtedy, gdy wdrożenie dotyczy nowego systemu oraz kiedy brak jest doświadczeń wdrożeniowych w danym obszarze; ryzyko takie jest nieodłączną częścią każdego projektu wdrożeniowego.

Skutki związane z występującym ryzykiem mają miejsce praktycznie we wszystkich obszarach związanych z realizowanym projektem. Do takich obszarów należą szczególnie:
- *przygotowany harmonogram przedsięwzięcia*, czyli wszystkie rozłożone w czasie działania podejmowane przy realizacji projektu – skutki w tym obszarze objawiają się najczęściej opóźnieniami w terminach realizacji poszczególnych działań;
- *budżet projektu*, czyli wymiar finansowy całego projektu – skutki w tym obszarze są powiązane z harmonogramem; wszelkie opóźnienia w realiza-

cji projektu znajdują swoje odzwierciedlenie w zwiększonych wydatkach, co jest jednoznaczne ze wzrostem kosztów realizacji całego projektu;
- *zasoby przedsiębiorstwa*, tj. ludzie, materiały, środki techniczne – zakłócenia w realizacji projektu wpływają na zmianę tych zasobów, powodując zmiany w ich wykorzystaniu, czego efektem może być ich niepełne lub niezgodne z planem wykorzystanie;
- *jakość wykonywanych przez dostawcę prac oraz wartość końcową produktu* (wdrożonego rozwiązania), która jest szczególnie ważna dla odbiorców – użytkowników końcowych.

Skutki zaistnienia ryzyka można podzielić według kryterium ich wystąpienia na wewnętrzne oraz zewnętrzne. Skutki wewnętrzne pojawiają się w obszarze związanym bezpośrednio z realizowanym przedsięwzięciem i dotykają głównie firmy klienta (nabywcy). Natomiast skutki zewnętrzne są związane z całym otoczeniem projektu, tj. dotyczą nie tylko nabywcy, lecz także firmy dostawcy (producenta) zaangażowanego w całe przedsięwzięcie (Szyjewski 2004).

Wiedza o samym ryzyku oraz o miejscach (obszarach) wystąpienia jego skutków znacznie ułatwia przeciwdziałanie im, jak również podjęcie kroków mających na celu zminimalizowanie ich rozmiarów. Aby jednak możliwa była pełna identyfikacja ryzyka, należy zwrócić uwagę na dodatkowe jego cechy, które obok niepewności i skutków pozwalają znacznie lepiej je określić. Do cech tych należą (Szyjewski 2004):
- *zakres* – określenie obszaru, zakresu działań, opis czynności projektu, jak również określenie przedziału czasowego, którego dotyczyć będzie ryzyko;
- *zagrożenie* – definicja sytuacji, która może mieć niekorzystny wpływ na wykonywane czynności, zadania i w efekcie na przebieg projektu jako całości; można je wszystkie rozpatrywać oddzielnie, łączyć w grupy w oparciu o różne klasyfikacje i kryteria; wszystkie one pozostają w ścisłym związku z czynnikami ryzyka;
- *czynniki ryzyka* – określone stany wejściowe dla poszczególnych działań czy procesów, które są determinantą wystąpienia w ich trakcie określonych zagrożeń, które mogą być pomocne w ocenie ryzyka;
- *rozłożenie w czasie* – ryzyko wystąpienia konkretnej bariery czy też związanego z nią zagrożenia jest zazwyczaj powiązane z określonym przedziałem czasowym, w którym projekt jest realizowany.

Obecność ryzyka w każdym projekcie jest nieunikniona. Występuje ono w każdym projekcie informatycznym, niezależnie od jego wielkości i zakresu działalności przedsiębiorstwa, jaki obejmuje. Pojawia się ono na wszystkich płaszczyznach realizacji projektu. Projekt wprowadza zmiany w dotychczasowym funkcjonowaniu organizacji. W zależności od ich zmiany i charakteru ryzyko może być mniejsze lub większe, ale ono zawsze występuje (Szyjewski 2001b). Ryzyko dla powodzenia projektu zależy od płaszczyzny wystąpienia określonej bariery i wynikających z niej zagrożeń.

W pewnych obszarach prawdopodobieństwo wystąpienia ryzyka jest tak niskie, że można przyjąć, że ryzyko w tym obszarze nie występuje, w innych zaś jest wysokie, co powoduje, że obszary te nazywane są obszarami ryzyka. *Obszarami ryzyka* nazywamy zatem te płaszczyzny związane z realizacją projektów informatycznych, na które ryzyko ma bezpośredni wpływ lub z którymi jest ono związane. W celu usystematyzowania wiedzy na temat barier i wynikających z nich zagrożeń skutkujących wstąpieniem ryzyka niepowodzenia projektu wdrożeniowego należy zawsze określić obszary ryzyka, w których ono występuje.

Podobnie jak w przypadku samego ryzyka, także obszary związane z jego wystąpieniem można podzielić według wielu różnych klasyfikacji. Najogólniej obszary ryzyka można podzielić w następujący sposób:

- *środowisko wykonawcze* – związane ze stroną techniczną prowadzonego przedsięwzięcia, dotyczy głownie samego projektu, używanych narzędzi, stosowanej metodyki itd.;
- *środowisko użytkownika* – dotyczy przyszłych użytkowników systemu zarówno pracowników funkcyjnych, jak i informatyków firmy klienta odpowiedzialnych za konserwację i utrzymanie systemu w ruchu; zawiera w sobie poziom przygotowania merytorycznego użytkownika, nastawienia do przedsięwzięcia itp.;
- *środowisko przedsięwzięcia* – zakres działań związany z samym projektem, jego wielkością, organizacją, jak również z zespołem wdrożeniowym zaangażowanym w realizację tego przedsięwzięcia.

Literatura przedmiotu przytacza wiele różnych klasyfikacji obszarów ryzyka. Na przykład firma ORACLE® w swojej metodyce o nazwie CDM (*Customer Development Method*) wyróżnia następujące obszary ryzyka[2]:

- *zakres prac projektowych* – wszelkie działania wykonywane w czasie realizacji projektu wdrożeniowego;
- *działania klienta* – całość zachowań firmy klienta, zarówno użytkowników końcowych, jak i członków zespołu wdrożeniowego;
- *aspekty techniczne* – wszystkie zdarzenia, które mają miejsce zarówno w systemie, jak i narzędziach wspomagających prace wdrożeniowe;
- *zasoby firmy wraz z logistyką* – ryzyko związane z dostępnością zasobów, ich właściwym wykorzystaniem oraz możliwościami elastycznego przeplanowania ich użycia;
- *otoczenie rynkowe* – wszystko to, co dzieje się poza stronami umowy, tj. dostawcą (producentem) rozwiązania a klientem – firmą wdrażającą dane rozwiązanie u siebie;
- *partnerzy umowy i przebieg projektu* – ogół działań wykonywanych w ramach podpisanej umowy i wynikających z realizowanego w jej ramach projektu.

4. Podstawowe czynniki ryzyka w projekcie wdrożeniowym

Jak widać na podstawie przytoczonych powyżej klasyfikacji, określenie obszarów ryzyka może być bardzo różne. Poszczególne podziały różnią się od siebie w zasadzie tylko stopniem szczegółowości, przy czym wszystkie one obejmują opisane powyżej obszary realizacji projektu wdrożeniowego. Pojawienie się ryzyka niepowodzenia projektu wdrożeniowego, będące rezultatem wystąpienia określonego zdarzenia, którego genezą jest istnienie określonej bariery, jest uwarunkowane wieloma dodatkowymi elementami – zagrożeniami. Te wynikające z barier zagrożenia, charakteryzujące się określoną prawidłowością występowania, zachodzą w „określonej sytuacji odniesienia, która ma wpływ na wzrost (...) określonego zagrożenia związanego z ryzykiem" (Stanik i Szewczuk 2001). Tak właśnie definiowany jest czynnik ryzyka, którego określenie stanowi kolejny krok w definiowaniu ryzyka niepowodzenia projektu wdrożeniowego. Czynniki ryzyka można – podobnie jak jego obszary – podzielić według wielu różnych kryteriów ułatwiających ich klasyfikację.

Przyjmując jako kryterium miejsce powstawania, czynniki ryzyka można podzielić na zewnętrzne, umiejscowione poza zespołem wdrożeniowym, oraz wewnętrzne, występujące w nim samym. Rozszerzając tę klasyfikację, można wyróżnić następujące, typowe grupy czynników ryzyka:

- czynniki powiązane z istniejącą strukturą organizacyjną przedsiębiorstwa i obowiązującymi procedurami wewnętrznymi;
- czynniki związane z użytkownikami systemu – wszystkimi ludźmi, którzy w dowolnym stopniu będą w swojej pracy wykorzystywać system;
- czynniki powiązane z wiedzą i doświadczeniem osób zaangażowanych w projekt (menedżerów, konsultantów, informatyków itd.);
- czynniki związane z systemem informatycznym, jego specyfiką oraz złożonością;
- czynniki łączące z elementami biznesowymi oraz wewnętrznymi uwarunkowaniami o charakterze formalno-prawnym;
- czynniki związane z przebiegiem samego projektu wdrożeniowego – zwłaszcza zaś z zaplanowanym i przyjętym harmonogramem zarówno w wymiarze czasu jego realizacji, jak i bezpośrednio z tym związanych kosztów jego prowadzenia.

Czynniki ryzyka wpływają na przebieg całego przedsięwzięcia informatycznego. Widać je we wszystkich wymiarach prowadzonych działań – od harmonogramu przez koszt realizacji, aż po ewentualne kary związane z brakiem wypełnienia zapisów kontraktu. Wyznaczenie czynników ryzyka jest zagadnieniem bardzo istotnym głównie ze względu na fakt, iż wystąpienie niektórych z nich może powodować, że zagrożona będzie realizacja całego projektu, a tym samym funkcjonowanie systemu w organizacji z wszelkimi negatywnymi następstwami tego właśnie niepowodzenia.

W przypadku wdrożeń systemów zintegrowanych projekty mają bardzo duży zakres, zaś czynniki ryzyka są następujące (Szyjewski 2001b):
- błędna ocena sytuacji początkowej, prowadząca w późniejszym czasie do zagrożenia powodzenia projektu wdrożeniowego;
- brak ekspertów, których wiedza jest niezbędna w rozwiązywaniu sytuacji kryzysowych – dodatkowo szybki rozwój technologii informatycznych powoduje pojawianie się nowych narzędzi programowych i nowego sprzętu, w których obsłudze i zastosowaniach brakuje doświadczenia;
- napięty lub długi harmonogram, w przypadku którego ryzyko wynika z dynamicznej ewolucji technologii informatycznych i wymuszanych przez nią zmian otoczenia – długie harmonogramy, z natury rzeczy, realizację celu odsuwają w przyszłość, co powoduje niską dynamikę prac (szczególnie na początku);
- niestabilny skład (duża fluktuacja) lub duża liczebność zespołu wdrożeniowego – taka sytuacja powoduje spadek wydajności spowodowany brakiem współpracy oraz opóźnieniami związanymi z koniecznością wprowadzenia nowych osób do pracy w zespole wdrożeniowym;
- korzystanie z usług firm zewnętrznych (np. podwykonawcy) – wsparcie ze strony takich firm jest zjawiskiem jak najbardziej pozytywnym, jednak w przypadku korzystania z tego typu usług nie ma możliwości pełnego nadzoru nad poczynaniami takich firm;
- bardzo wysokie wymagania dotyczące zarówno efektywności (mocy) obliczeniowej systemu, jak i jego niezawodności – jest to obarczone dużym ryzykiem, ponieważ wszelkie założenia odnośnie tych wielkości mają charakter szacunków i przybliżeń; nie można ich przewidzieć przed zakończeniem projektu;
- zmienność wymagań w trakcie trwania projektu – nowe wymagania powstają na skutek zmiany otoczenia lub oczekiwań klienta; nie mogą być one jednak z różnych względów zrealizowane.

5. Klasyfikacja, opis ryzyka, bariery i działania nim obarczone

Podsumowaniem rozważań o ryzyku, jakie występuje podczas każdego przedsięwzięcia informatycznego, i przejściem do jego klasyfikacji jest określenie jego rozmiarów, z którymi należy się liczyć.

Ze względu na przytoczony wcześniej podział na ryzyko typowe i specyficzne, co jest odzwierciedleniem charakterystyki prowadzonych projektów, konieczne jest zwymiarowanie tego właśnie ryzyka oraz jego reprezentacja w określonej skali. Tylko wtedy, kiedy ryzyko zostanie zwymiarowane i przedstawione w wielkościach, które pozwolą na porównanie go w różnych obszarach, będzie można dobrze zanalizować ewentualne skutki jego wystąpienia i zaplanować środki zaradcze. Zwymiarowanie jego wielkości i przedstawienie go w postaci zrozumiałej dla szerokiego grona osób zainteresowanych ryzykiem

jest bardzo istotne, ponieważ ma duże znaczenie dla prawidłowego zrozumienia skali zagrożenia dla powodzenia projektu wdrożeniowego. Z prezentacją rozmiarów ryzyka ściśle związany jest sposób mierzenia ryzyka i określania wartości, która będzie informacją na temat rozmiaru zagrożenia. Identyfikacja ryzyka polega na określeniu, jakie zdarzenia mogą być niekorzystne dla realizowanego projektu. Rozpoznane ryzyko powinno zostać udokumentowane poprzez jego opisanie w rozbiciu na warunki jego zaistnienia, przejawy oraz przewidywane skutki dla realizacji projektu wdrożeniowego.

Ryzyko można przedstawiać na wiele różnych sposobów, przy czym najczęściej stosowane są:

- *opis słowny* – ryzyko opisywane jest przy użyciu powszechnie stosowanych określeń skali występowania w notacji „bardzo małe", „małe", „średnie" itd.;
- *wartość liczbowa* – ryzyko opisywane jest przez nadanie mu określonej wartości liczbowej zawierającej się w danym przedziale; opisane w tej notacji ryzyko jest stosunkowo proste do identyfikacji, gdyż posiłkując się wartością liczbową, można je umieścić na osi liczbowej i w ten sposób porównać jego wielkość z ryzykiem np. z innego obszaru czy też projektu wdrożeniowego; dodatkowym atutem tej reprezentacji jest fakt, iż umożliwia ona rozpatrywanie ryzyka w określonej skali zagrożenia przedsięwzięcia, tj. od pełnego sukcesu po całkowitą katastrofę; zaletą tej metody jest przedstawienie ryzyka za pomocą jednej zrozumiałej liczby, przez co interpretacja skali zjawiska jest bardzo prosta, szczególnie w kontekście dokonywania zestawień i porównań;
- *punkt, obszar, odcinek* umieszczony w układzie współrzędnych opisanych osiami niepewności, na których odłożone są wielkości prawdopodobieństwa wystąpienia zagrożenia i jego skutków – metoda taka daje dużo informacji o samym ryzyku i pozwala je stosunkowo dobrze zinterpretować, nie ułatwia jednak prostego porównywania z innymi wartościami.

Ryzyko w projekcie wdrożeniowym materializuje się w postaci barier wdrożeniowych, które przejawiają się konkretnymi sytuacjami lub działaniami mającymi negatywny wpływ na przebieg wdrożenia. W praktyce zatem należy stworzyć kategorie opisujące rozmiar tego ryzyka oraz przypisać do nich poszczególne działania i grupy działań będące przejawem barier oraz określić prawdopodobieństwo ich wystąpienia.

5.1. Kategorie ryzyka

W wyniku prowadzonych badań zdefiniowano kilka kategorii[3] ryzyka, stosując notację słowną. Przyjęto 9 kategorii ryzyka, do których przyporządkowano szacunkowe wartości liczbowe wyrażone w procentach (tabela 1).

Na takie rozwiązanie zdecydowano się, gdyż :

- pozwoli ono syntetycznie pogrupować występujące działania oraz ryzyko z nimi związane;
- w ramach jednej kategorii umożliwi ono wewnętrznie ustrukturyzowanie poszczególnych działań (tabela 2).

Lp.	Opis słowny rozmiaru ryzyka	Rozmiar wyrażony w procentach
1.	Brak	0
2.	Znikome	10
3.	Bardzo małe	20
4.	Małe	30
5.	Średnie	40
6.	Znaczące	40–60
7.	Duże	60–80
8.	Bardzo duże	80–90
9.	Pewne	90–100

Tab. 1. Klasyfikacja przyjętego ryzyka. Źródło: opracowanie własne.

Lp.	Kategoria ryzyka	Działania zaklasyfikowane do kategorii ryzyka
1.	Brak	Ryzyko nie występuje. Do tej kategorii należą działania najprostsze, o bardzo małym zakresie, nie wymagające zaangażowania dużych zasobów. Przykładem jest zakup oprogramowania lub inna czynność zaopatrzeniowa. Ewentualne opóźnienia wynikające z tych czynności nie mają wpływu na przebieg całego procesu wdrożeniowego.
2.	Znikome	Ryzyko występuje w stopniu minimalnym. Do tej kategorii należą te działania, których poziom trudności jest niski, nie wymagają zaangażowania dużych zasobów, jednak są związane z szerszym zakresem działania (obejmują do 10 stanowisk roboczych). Ewentualne problemy związane z tymi działaniami mają typowy charakter oraz dają się łatwo usunąć. Przykładem może być instalacja prostej aplikacji na kilku stanowiskach. Na poziomie takich czynności nie występuje opór ludzi, ponieważ materia działania jest im dobrze znana, a przyczynami ich złej pracy są zazwyczaj zwykłe błędy i pomyłki.
3.	Bardzo małe	Ryzyko związane z czynnościami zaliczanymi do tej grupy, podobnie jak poprzednio, jest nieduże, jednak wzrasta wraz z zakresem działania (zakres do 30 stanowisk). Przykładem takich działań może być instalacja systemu operacyjnego oraz niezbędnych usług w połączeniu w komunikacją między stanowiskami (np. opierając się na grupach roboczych).

Cd. tab. 2

Lp.	Kategoria ryzyka	Działania zaklasyfikowane do kategorii ryzyka
4.	Małe	Ryzyko w tej grupie jest związane z wielkością przedsięwzięcia. Działania w tej grupie dotyczą przedsięwzięć związanych z technologią sieciową i zapewnieniem komunikacji. Przykładem działań mogą być zarówno budowa infrastruktury, jak i instalacja wymaganego oprogramowania. Dotyczy działań w sieciach o niewielkich rozmiarach (do 100 użytkowników).
5.	Średnie	Do tej grupy zaklasyfikowane zostały wszystkie czynności związane z funkcjonowaniem infrastruktury sieciowej, jeżeli łączy się to z koniecznością dokonywania zmian i związanego z nimi szkolenia użytkowników. Takim ryzykiem obarczone są także działania związane z koniecznymi aktualizacjami oprogramowania w systemach sieciowych do 100 użytkowników.
6.	Znaczące	Ryzykiem tej wielkości obarczone są działania dotyczące zagadnień wychodzących poza jeden obszar funkcjonalny, związane z funkcjonowaniem infrastruktury sieciowej. Takim ryzykiem obarczone są także braki funkcjonalności systemu na poziomie kilku stanowisk roboczych. Do tej kategorii zaklasyfikować można także działania związane z wymianą i/lub rozbudową, względnie z wprowadzeniem nowego narzędzia. Dodatkowo połączone jest to z koniecznością szkoleń oraz zmianami w organizacji. Opór ludzi na poziomie tych działań jest także obarczony takim ryzykiem. Przykładem może być rozbudowa sieci oraz włączenie do systemu nowych działów funkcjonalnych przedsiębiorstwa. Działania te nabierają szczególnego znaczenia w przypadku przedsiębiorstwa wielooddziałowego rozproszonego geograficznie i związanej z tym konieczności integracji.
7.	Duże	Do kategorii tej należą działania wykonywane na płaszczyźnie całego przedsiębiorstwa, tj. kiedy dotyczą (w różnym stopniu) wszystkich działów funkcjonalnych przedsiębiorstwa. Ta kategoria ryzyka dotyczy szczególnie działań związanych z oporem ludzi wobec zmian (np. restrukturyzacja), brakiem komunikacji lub wadliwą komunikacją. Dużym ryzykiem obarczone są także problemy wynikające z braku szkoleń lub niewystarczającej ich liczby oraz poziomu, tj. głównie działania będące wynikiem braku wiedzy oraz niekompetencji. Do tej kategorii należą także błędy działania systemu wynikające z braków funkcjonalności na poziomie firmy (np. w module finansowym czy też raportowania). Dużym ryzykiem obarczone są także działania osób nieposiadających wystarczającej wiedzy merytorycznej (brak ekspertów).
8.	Bardzo duże	Działania podejmowane w ramach zespołu wdrożeniowego (zarówno konsultantów, użytkowników, informatyków, jak też kierujących projektem). Działania tych ludzi mają bezpośredni wpływ na przebieg procesu wdrożeniowego, tj. przestrzeganie harmonogramu, a tym samym przydzielonych zasobów. Wszelkie decyzje, sposób i atmosfera ich podejmowania mają bezpośrednie przełożenie na przebieg wdrożenia oraz jego efekt.

Cd. tab. 2

Lp.	Kategoria ryzyka	Działania zaklasyfikowane do kategorii ryzyka
9.	Pewne	Działania zarządu, kierownictwa i innych decydentów najwyższego szczebla. Jeżeli na tym poziomie wystąpią zakłócenia i bariery, niepowodzenie projektu jest pewne. Od działań z tego zakresu nie ma bowiem odwrotu, a to dlatego, że mają one kluczowy charakter i determinują wszystkie inne. Na tym etapie ciężko jest barierom przeciwdziałać, jako że jest to najwyższy poziom decyzyjny. Przykładem jest brak zgody zarządu na dodatkowe zakupy, np. sprzętu lub licencji systemu. Do tej kategorii zaliczyć należy także zbyt napięty lub zbyt długi harmonogram. W tym drugim przypadku, w dobie dynamicznego rozwoju techniki i technologii, pojawia się ryzyko niedopasowania zastosowanych rozwiązań (zawartych w projekcie) do aktualnych wymogów. Dodatkowo przyjęty na początku cel może z upływem czasu ulec zupełnej zmianie.

Tab. 2. Opis przyjętych kategorii ryzyka. Źródło: opracowanie własne.

Przedstawione kategorie ryzyka oraz obszary działań do nich zaliczone traktować należy w kategorii modelowych wytycznych, które pozwolą opisać i pogrupować konkretne działania. Mogą być one rozbudowywane o konkretne rzeczywiste działania, tak aby dobrze poznać ryzyko i ułatwić zarządzanie nim.

6. Podsumowanie

W czasie prowadzonych badań okazało się, że problemy, jakie występują w czasie wdrożenia pod kątem występowania ryzyka, wykazały pewną prawidłowość. Można je najogólniej zaklasyfikować do trzech grup: techniczne (sprzęt), systemowe (działanie systemu) oraz ludzkie (działania ludzi). Problemy techniczne charakteryzują się największym stopniem powtarzalności oraz stosunkowo wysoką przewidywalnością. Ich wystąpienie jest związane z najmniejszym ryzykiem dla przebiegu projektu wdrożeniowego. Problemy wynikające z funkcjonowania systemu zintegrowanego, jak np. braki funkcjonalności czy źle zdefiniowane interfejsy, także dają się w pewnym stopniu przewidzieć. I choć występują one mniej regularnie niż problemy techniczne, to ich usunięcie następuje zazwyczaj wskutek zastosowania typowych, znanych zabiegów. Ryzyko wystąpienia takich zdarzeń jest jednak wyższe. Problemy, z którymi związane jest największe ryzyko, są generowane przez ludzi (głównie przez użytkowników). Te problemy występują zazwyczaj nieoczekiwanie, natomiast te, które można przewidzieć, pojawiają się bez żadnej regularności i mają najróżniejsze przyczyny. Dodatkowo występują one z różnym natężeniem oraz nie wykazują żadnych, nawet najmniejszych prawidłowości.

Informacje o autorze
Dr Tomasz Parys – Katedra Systemów Informacyjnych Zarządzania, Wydział Zarządzania Uniwersytetu Warszawskiego. E-mail: parys@mail.wz.uw.edu.pl.

Przypisy

1 W literaturze przedmiotu ta definicja ryzyka jest najczęściej stosowana. Por. Szyjewski 2001a.

2 Opracowano na podstawie materiałów dostępnych na stronie http://www.postjobfree.com/resume/yyttq, odczyt: listopad 2011.

3 Kategorie zdefiniowane zostały na potrzeby dużych systemów zintegrowanych. Dla przedsięwzięć mniejszych kategorie należy przedefiniować, choć ich układ będzie podobny.

Bibliografia

Duncan, W.R. 1996. *A Guide to the Project Management Body of Knowledge*, Sylva: Project Management Institute.

Kaczmarek, T. 2002. *Zarządzanie ryzykiem*, Gdańsk: ODDK.

Kubiak, B.F. i A. Korowicki (red) 2001. *Human Computer Interaction 2001*, Gdańsk: Wydawnictwo Akwila – Roman Młodkowski.

Pritchard, C.L. 2002. *Zarządzanie ryzykiem w projektach. Teoria i praktyka*, Warszawa: WIG-PRESS.

Szyjewski, Z. 2001a. *Projektowanie systemów informatycznych*, Warszawa: Wydawnictwo Naukowe PWN.

Szyjewski, Z. 2001b. *Zarządzanie projektami informatycznymi*, Warszawa: Placet.

Szyjewski, Z. 2004. *Metodyki zarządzania projektami informatycznymi*, Warszawa: Placet.

Stanik, J. i J. Szewczuk 2001. Szacowanie ryzyka przedsięwzięć informatycznych cz. I – wprowadzenie do oceny ryzyka przedsięwzięć informatycznych, w: B.F. Kubiak i A. Korowicki (red) *Human Computer Interaction 2001*, Gdańsk: Wydawnictwo Akwila – Roman Młodkowski.

Woodward, M.R., Hemel, M.A. i D. Hedley 1979. A Measure to Control Flow Complexity in Program Text. *IEEE Transactions on Software Engineering*, nr 5.