*Piotr Adamczewski*

# Ryzyko w realizacji złożonych przedsięwzięć informatycznych

Praktyka zastosowań informatyki wspomagających procesy zarządzania nader często wskazuje, że wiele zamierzeń w tym zakresie kończy się połowicznym sukcesem. Zagraniczne doświadczenia wskazują (a krajowe przykłady to w pełni potwierdzają), że finalizacja blisko 70% przedsięwzięć informatycznych jest opóźniana, przekracza przewidziane nakłady lub nie spełnia oczekiwań użytkowników. Dotyczy to zarówno zamierzeń realizowanych na szczeblu rządowym (np. POLTAX), jak i na poziomie poszczególnych przedsiębiorstw czy instytucji.

Poniższe rozważania są wynikiem wieloletnich doświadczeń autora, który z pozycji konsultanta nadzoruje wiele złożonych przedsięwzięć informatycznych tak krajowych, jak i zagranicznych w zakresie kompleksowej informatyzacji dużych i średnich przedsiębiorstw, banków komercyjnych, urzędów administracji publicznej i samorządowej.

Złożone przedsięwzięcie informatyczne (ZPI), stanowiące praktyczną realizację zintegrowanego systemu informatycznego zarządzania (ZSIZ), dokonuje się przy zaangażowaniu względnie dużych zasobów finansowo-czasowych określonego użytkownika, przy czym:

- przyszły użytkownik ZSIZ przykłada doń wagę strategiczną,
- dostrzegalny jest kompleksowy zakres proponowanego rozwiązania,
- przedsięwzięcie obejmuje cały cykl życia ZSIZ – od momentu powstania potrzeby rozwiązania problemu za pomocą systemu informatycznego, aż do jego eksploatacji użytkowej,
- wymagana jest pomoc specjalistów-konsultantów z zakresu informatyki.

W uproszczeniu można przyjąć, że choć ZSIZ jest tylko zbiorem urządzeń i programów, to jednak wdrożenie takiego systemu oznacza nowy sposób funkcjonowania przedsiębiorstwa czy instytucji. Praktycznie, takie rozwiązanie obejmuje zarząd i kierownictwo średniego szczebla, a także poziom operacyjny (bezpośrednich wykonawców). Naturalne konsekwencje takiego rozumienia wdrożenia są następujące:

- głównym czynnikiem sukcesu wdrażania ZSIZ są ludzie, a nie sprzęt i oprogramowanie,
- decyzja o wdrażaniu jest strategiczną decyzją (inwestycją) użytkownika, oznaczającą zmianę stylu działania instytucji czy przedsiębiorstwa.

W przedsięwzięciu informatycznym miarą ryzyka jest prawdopodobieństwo, że wdrożony ZSIZ nie przyniesie spodziewanych korzyści, nie będzie posiadać wymaganych właściwości użytkowych, nie zostanie wdrożony zgodnie z planem, lub że przekroczone zostaną przewidywane koszty przedsięwzięcia. W większości przypadków ZPI, szacunek ryzyka możliwy jest jedynie w odniesieniu do czasu i kosztów przedsięwzięcia. Ogólne ryzyko tego przedsięwzięcia wynika z przybliżonej oceny poziomu wielu cząstkowych czynników, zgrupowanych w trzy kategorie: zakresu, struktury i technologii przedsięwzięcia.

Kategoria czynników ryzyka związanych z zakresem przedsięwzięcia obejmuje pracochłonność prac, czas realizacji przedsięwzięcia, wielkość zespołu wdrożeniowego, sprzężenia z innymi systemami, liczbę instalacji systemu oraz liczbę komórek organizacyjnych w zasięgu ZSIZ.

Kategoria czynników ryzyka związanych ze strukturą przedsięwzięcia obejmuje podkategorie definicji przedsięwzięcia, poparcia zamierzenia informatyzacji (atmosfery wokół ZPI), wpływu systemu na instytucję, składu zespołu wdrożeniowego oraz zarządzania przedsięwzięciem.

Kategoria czynników ryzyka związanych z technologią systemu obejmuje szereg czynników, dotyczących sprzętu i oprogramowania użytkowego, systemowego oraz narzędziowego.

Rzeczywistym i złożonym zagrożeniem dla powodzenia ZPI jest ograniczenie jego widzenia do zagadnień czysto technicznych. Każde przedsięwzięcie wiąże się z ryzykiem, przez które rozumie się wystawienie instytucji na zagrożenia, takie jak:

- brak lub tylko częściowe uzyskiwanie oczekiwanych korzyści z powodu trudności wdrożeniowych,
- przekroczenie zakładanych kosztów wdrożenia,
- przekroczenie przewidywanego czasu wdrożenia,
- rozbieżność parametrów rozwiązania finalnego – osiągniętych i zakładanych.

Czynniki zagrażające zamierzeniom informatycznym są bardziej złożone i jest ich więcej, niż zwykle sądzą ich twórcy i użytkownicy. Zagrożenia tkwią

w otoczeniu organizacyjnym, w zachowaniach ludzi, dostępnych zasobach i wyposażeniu oraz w samym zespole tworzącym zastosowania. W szczególności, należy wymienić następujące zagrożenia (por. [4]):

- brak zdolności instytucji do zmiany lub niechęć do jej wprowadzenia i zamiar wykorzystania technologii informatycznej jako jej substytutu,
- niezdolność do przyswajania nowej technologii przetwarzania danych,
- brak poczucia celu, niedostateczna znajomość możliwości i ograniczeń informatyki oraz brak zaangażowania kierownictwa,
- brak motywacji i uczestnictwa użytkowników,
- ograniczone zasoby i wyposażenie w sprzęt i oprogramowanie,
- niedostateczne umiejętności i doświadczenie twórców systemu,
- niesprawna organizacja zespołu tworzącego ZSIZ,
- wykorzystywanie nieodpowiednich metod, technik i narzędzi tworzenia systemu,
- brak lub nieskuteczność systemu sterowania i kontroli tworzenia ZSIZ,
- pojawienie się nowych, nieprzewidzianych czynników w otoczeniu.

Analizując pojęcie ryzyka ZPI, można wskazać dwa obszary, w których powstaje ryzyko niepowodzeń (por. 5):

- faza tworzenia ZSIZ:
  - ▲ określenie celów przez użytkownika,
  - ▲ nieumiejętność wybrania odpowiedniej technologii i jej zmiany,
  - ▲ niezdolność przewidzenia ekonomicznych skutków (oszacowania) i określenia mechanizmu (oddziaływania) wprowadzania nowego ZSIZ,
  - ▲ niepełne widzenie organizacji i wynikająca z tego ograniczona zdolność przewidzenia psychologicznych i behawioralnych oddziaływań wprowadzanego ZSIZ,
  - ▲ niezadowalający przebieg procesu tworzenia ZSIZ: brak uczestnictwa użytkowników, zakłócenia komunikacji, nieskuteczność sterowania i oceny jakości rozwiązań przez użytkowników,
  - ▲ niezdolność zrozumienia i przewidywania wszystkich aspektów tworzenia ZSIZ;
- faza eksploatacji ZSIZ:
  - ▲ niezdolność stworzenia i/lub wykorzystywania rozwiązania technicznego odpowiednio szybkiego, łatwego w użytkowaniu i niezawodnego,
  - ▲ niezdolność utrzymania kompletnej i aktualnej bazy danych, nieumiejętność rozwiązania problemów przy wykorzystaniu technologii informatycznej,
  - ▲ niezdolność stworzenia rozwiązania wolnego od negatywnych wpływów na warunki pracy, zmianę władzy czy zmianę wymagań, kwalifikacji i zakres pracy,
  - ▲ nieumiejętność stworzenia rozwiązań złożonych – możliwych do zrozumienia, sterowania, utrzymania i dokonywania zmian.

Literatura dostarcza wiele ujęć problematyki zagrożeń dla wprowadzania ZSIZ oraz związanego z tym ryzyka [5, 6]. Różnorodność doświadczeń przedstawionych w literaturze pozwala uwzględnić wszystkie istotne aspekty ryzyka i jego źródeł w ocenie, eliminowaniu przyczyn i zapobieganiu skutkom.

Analiza zagrożeń i ryzyka jest jedną stroną identyfikacji i przygotowania rozwiązań problemów związanych z przeprowadzeniem zamierzenia. Drugą – znacznie ważniejszą ze względu na pozytywne oddziaływanie na uczestników oraz znaczenie dla organizacji – jest analiza czynników powodzenia (sukcesu). Ma ona na celu wskazanie okoliczności i czynników sprzyjających pożądanemu przebiegowi prac i osiąganiu wyznaczonych rezultatów. Taka ze wszech miar potrzebna analiza nie znajduje jednak należytego zainteresowania. Przyczyną tego jest przekonanie o „uzdrawiających właściwościach" ZSIZ i pełne zaufanie do informatyków oraz generalnie niechęć do analizy potrzeb ze strony informatyków. Ponadto ważniejsze w przygotowaniu wielkiego zamierzenia w sposób naturalny okazuje się eliminowanie zagrożeń bądź zaniechanie prac, jeśli są one zbyt duże. Dopiero w następnym kroku szuka się sposobów zwiększenia efektów zamierzenia, które będzie podjęte, jeśli nie stwierdzi się zagrożeń. Trzeba nadto pamiętać, że wobec powszechnego zakładania możliwości „doskonalenia istniejącej organizacji" poprzez wprowadzenie ZSIZ zamiast jej zmiany nie określa się nawet celów „komputeryzacji". Trudno zatem byłoby oczekiwać analizy czynników powodzenia w osiąganiu celów, których nie sprecyzowano.

Omówione wyżej czynniki ryzyka w realizacji ZPI występują niezależnie od zaawansowania instytucji w stosowaniu rozwiązań informatycznych. W miarę uzyskiwania doświadczeń, zwiększa się jej zdolność do zmniejszania ryzyka. W szczególności, umiejętność przewidywania zagrożeń i podejmowania koniecznych działań pozwala zmniejszać ryzyko niepowodzenia ZPI.

Prace nad ZSIZ zawsze przebiegają w warunkach niepewności, charakterystycznej dla każdej zmiany wprowadzanej bez możliwości zawieszenia działalności. Dynamika zmian wprowadzanych w rzeczywistych warunkach działania jest sama w sobie zagrożeniem i dlatego nie można dopuszczać dodatkowych zagrożeń. Są one tymczasem bardzo liczne, a mogą wynikać z nie rozpoznanych postaw użytkowników, niedostatecznego doświadczenia insty-

| Lp. | Grupa czynników | Wyszczególnienie | Ocena | Waga |
|---|---|---|---|---|
| 1 | wielkość ZPI | ● pracochłonność (roboczogodziny):<br>a) 100–3000 b) 3001–15000 c) 15001–30000 d) > 30000<br>● czas wdrożenia (miesiące):<br>a) < 12 b) 13–24 c) > 24 | 1–4<br><br>1–3 | 0.09<br><br>0.08 |
| 2 | struktura rozwiązania | ● zakres modyfikacji rozwiązania (%):<br>a) < 25 b) 26–50 c) > 50<br>● zakres zmian w strukturze organizacji:<br>a) minimalny b) widoczny c) istotny | 1–3<br><br>1–3 | 0.08<br><br>0.08 |
| 3 | technologia | ● novum w wyposażeniu użytkownika:<br>a) komputer centralny b) terminale<br>c) mikrokomputery d) nic<br>● novum dla twórców rozwiązania:<br>a) baza danych b) telekomunikacja<br>c) język programowania/CASE d) nic | 3–0<br><br>3–0 | 0.09<br><br>0.09 |
| 4 | organizacja ZPI | ● przeprowadzono studium wykonalności:<br>a) pełen zakres (z udziałem użytkownika)<br>b) główne aspekty (bez użytkownika) c) nie przeprowadzono<br>● ustalono plan realizacji ZPI z priorytetami:<br>a) przez zespół mieszany<br>b) przez wykonawców wg swojego rozeznania<br>c) tworzony jest na bieżąco | 1–3<br><br>1–3 | 0.08<br><br>0.08 |
| 5 | metodyka ZPI | ● wykorzystywana metoda realizacji ZPI:<br>a) standardowa w pełnym zakresie<br>b) własna c) nieokreślona<br>● analiza potrzeb i specyfikacja rozwiązania zajmie ogólnej czasochłonności prac (%):<br>a) < 10 b) 10–30 c) > 40 | 1–3<br><br>3–1 | 0.08<br><br>0.09 |
| 6 | rola użytkownika | ● ogólna postawa użytkownika:<br>a) pełne zaangażowanie i współpraca<br>b) bierne zaangażowanie c) niechęć<br>● udział użytkownika w zespole mieszanym:<br>a) specjaliści wyznaczeni przez użytkownika<br>b) specjaliści wskazani przez wykonawców<br>c) nie uczestniczy | 1–3<br><br>1–3 | 0.08<br><br>0.08 |

Źródło: Opr. własne z wykorzystaniem [4].

tucji w stosowaniu technologii informatycznej, konieczności współpracy z firmami handlowymi i usługowymi (dostawcami, wykonawcami), które nie dają pełnej gwarancji wykonania słabo zdefiniowanego zadania, zmienności warunków działania, braku możliwości przewidywania zmian, powodowanego doraźnością działań, braku poczucia ich celowości i obaw przed zmianą organizacyjną.

Czynniki ryzyka nie są trafnie rozpoznawane tak przez informatyków, jak i użytkowników ZSIZ. Uważa się powszechnie, iż główne zagrożenia są związane z czynnikami technicznymi oraz użytkownikami. W rzeczywistości najczęściej powodami niepowodzenia są czynniki związane z wykorzystaniem metod, podejmowaniem decyzji oraz oddziaływaniem otoczenia [1, 2, 4]. W fazie eksploatacji ZSIZ niepowodzenie jest najczęściej związane z brakiem definicji celów lub ich nietrafnością oraz charakterystykami procesu. Na etapie tym niepowodzenie jest kojarzone z problemami złożoności, problemami pojęciowymi oraz reakcjami użytkowników ZSIZ.

Celem analizy ryzyka powinno być określenie zagrożeń i ich źródeł oraz wskazanie sposobów:
- eliminowania zagrożeń i ich przyczyn,
- zmniejszenia zagrożenia w przypadku niemożności wyeliminowania źródeł zagrożeń poprzez wprowadzenie stosownych form sterowania ZPI,
- eliminowania lub ograniczenia wywołanych negatywnych skutków,
- działania w razie wystąpienia negatywnych skutków zamierzenia, których nie można wyeliminować bądź zmniejszyć.

Analiza ryzyka ma dać realizatorom ZPI pod-

stawy do podejmowania wszystkich decyzji dotyczących zamierzenia – od podjęcia prac przygotowawczych, aż po pełne wdrożenie i rozwój ZSIZ. Wstępna analiza ryzyka jest szczególnie istotna w przypadku użytkowników, którzy nie mają wystarczającego doświadczenia w zastosowaniach informatyki, a podejmują wielkie zamierzenia o dużym stopniu ryzyka. Sama analiza pozwala na zapoznanie się ze złożonością zamierzenia i związanego z nim ryzyka. Uświadomienie sobie skali zagrożeń, ich źródeł i wielkości ryzyka powinno doprowadzić do weryfikacji wstępnych decyzji o zakresie prac, sposobie ich prowadzenia, zaangażowaniu pracowników i kontrahentów, zakresie prac wstępnych oraz zasadach sterowania zamierzeniem. Szczególnie ten ostatni czynnik – mający zasadniczy wpływ na powodzenie ZPI, a lekceważony tak przez użytkowników, jak i twórców ZSIZ – może ulec znacznym modyfikacjom w wyniku analizy.

Liczne zamierzenia mogą przynieść rezultaty zbliżone do oczekiwanych, jeśli w początkowej fazie prac przeprowadzi się analizę warunków, w jakich prowadzone będą prace projektowo-wdrożeniowe. Na podstawie analizy można określić wymagania, jakie powinny być spełnione w celu zapewnienia pełnej realizacji. Opierać się ona może na pytaniach, podzielonych na sześć grup, a dotyczących następujących aspektów:

- wielkości ZPI wyrażonej w liczbie roboczogodzin, oczekiwanym czasie wdrożenia, wartości kontraktu, liczbie zaangażowanych jednostek organizacyjnych;
- struktury systemu, czyli udziału modyfikowanych czynności, związanych z nimi zmian struktur, postaw użytkowników, zakresu funkcjonalnego, znaczenia zmian organizacyjnych w jednostkach;
- technologii, czyli zakresu zmian technologii przetwarzania danych (sprzętu i oprogramowania), znajomości technologii przez użytkowników, sposobu zaopatrywania się; znajomości dziedzin zastosowań przez twórców ZSIZ;
- organizacji projektu, obejmujących zakres prac wstępnych: studium wykonalności, plan projektu, organizacyjne formy sterowania i kontroli, rozłożenie odpowiedzialności za przebieg prac, podstawy ustalenia celów ZPI, istnienie kryteriów oceny rezultatów;
- metod tworzenia systemu, czyli doboru metod, technik i narzędzi, zakresu analizy potrzeb, zakresu uczestnictwa użytkowników;
- roli użytkowników, czyli dominujących postaw użytkowników, doświadczenia w wykorzystaniu technologii, zaangażowania wyższego kierownictwa.

Uzyskane odpowiedzi mają dać podstawy oceny warunków, w jakich prowadzone jest zamierzenie przygotowania do prac projektowych i ich organizacji oraz zasad sterowania i kontroli realizacji ZPI. Na podstawie odpowiedzi udzielonych przez przyszłych użytkowników ZSIZ oraz jego twórców tworzone są podstawowe charakterystyki, umożliwiające szacowanie ryzyka. Ryzyko jest określane jako wielkości procentowe wyrażające udział stwierdzonych zagrożeń w całości oraz w poszczególnych aspektach. Znaczenie wskaźników procentowych jest mniej istotne niż uświadomienie sobie skutków, a w szczególności zagrożeń, jakie wiążą się z przebiegiem procesu tworzenia, wdrażania i eksploatacji ZSIZ. Wskaźnik całkowitego ryzyka zamierzenia ma sygnalizować skalę występujących zagrożeń. Wskaźniki cząstkowe pozwalają zwrócić uwagę na szczególne zagrożenie związane z poszczególnymi aspektami ZPI.

O potrzebie analizy ryzyka związanego z realizacją ZPI przekonało się już wiele zespołów wdrożeniowych. Identyfikacja zagrożeń i ich oceny pozwalają zmniejszyć ryzyko i zapobiec błędom, a w konsekwencji podjąć działania służące usprawnieniu przygotowania całości prac (por. [1, 2]). Na zakończenie należy stwierdzić, że system jakości prac projektowych, wynikający z zalecanych norm ISO 9001 (z wytycznymi w normie ISO 9000-3) może w tym względzie wymusić daleko idące zmiany. Jest to jednak w naszych krajowych warunkach jeszcze perspektywa paru lat. Certyfikaty normy ISO 9000 w zakresie produkowanego w Polsce sprzętu komputerowego dokonują istotnych zmian jakościowych w tym sektorze rynku — czas na podobne zmiany w obszarze usług informatycznych.

*Piotr Adamczewski*

BIBLIOGRAFIA

[1] ADAMCZEWSKI P., *Praktyczne uwagi konsultanta złożonych przedsięwzięć informatycznych*, Mat. konf. INFOGRYF '94, TNOiK, Szczecin 1994, s. 299–306.

[2] ADAMCZEWSKI P., *Uwarunkowania realizacyjne złożonych przedsięwzięć informatycznych*, maszynopis powielony, PTE, Poznań 1994.

[3] FRENZEL C.W., *Management of Information Technology*, Boyd & Fraser, Boston 1992.

[4] KURAŚ M., *Analiza ryzyka przedsięwzięć informatycznych*, Mat. konf. INFOGRYF '94, TNOiK, Szczecin 1994, s. 217–228.

[5] LYYTINEN K., *Expectation Failure Concept and Systems Analysts' View of Information System Failures: Result of an Exploratory Study*, „Information and Management", No. 14, 1988.

[6] WALSHAM A., *Interpreting Information Systems in Organizations*, John Wiley & Sons, Chichester, New York 1992.

Autor jest pracownikiem naukowym w stopniu doktora Katedry Systemów Logistycznych Akademii Ekonomicznej w Poznaniu