Halina Tańska[1], Agnieszka Władzińska[2]

Badanie wpływu wybranych grup ryzyka na projekty informatyczne

1. Wstęp

W języku potocznym ryzyko jest utożsamiane z pewną miarą zagrożenia wynikającego z niezależnych zdarzeń. Stwierdzenie to sugeruje, że z ryzykiem w zasadzie nic nie da się zrobić, bowiem ono po prostu istnieje. Zastanawiające jest, czy w związku z tym pojęcie zarządzania ryzykiem nie jest czasem wyraźnym nadużyciem.

Analiza literatury przedmiotu[3] pozwala przyjąć, że pod pojęciem ryzyka kryje się każda taka przyszła sytuacja lub zdarzenie, które może wywierać negatywny wpływ na projekt, szczególnie projekt informatyczny. Zazwyczaj nie wiadomo, czy niebezpieczna sytuacja wystąpi i jak dotkliwe będą jej skutki. Wieloletnie doświadczenie autorek niniejszego artykułu pozwala zaakceptować praktyczne stanowisko: istnienie ryzyka wnosi do projektu element niepewności. Nie można zatem natychmiast podejmować działań zaradczych, które mogą być kosztowne, trzeba jednak starannie je przygotować i wcielić w życie, jeśli ryzyko zacznie się materializować.

W zarządzaniu projektami ryzyko jest definiowane jako możliwość przypadkowego wystąpienia pewnego zdarzenia, które będzie miało wpływ na realizację projektu, w szczególności może zadecydować o jego sukcesie lub klęsce. W odróżnieniu od potocznego znaczenia słowa „ryzyko" pojęcie ryzyka w zarządzaniu projektami jest przede wszystkim związane z nieprzewidywalnością wystąpienia określonego zdarzenia, podczas gdy samo zdarzenie niekoniecznie musi być

[1] Uniwersytet Warmińsko-Mazurski, Wydział Matematyki i Informatyki.
[2] ZETO Softvare, Olsztyn.

[3] J. Phillips, *Zarządzanie projektami IT*, Helion, Gliwice 2004; K. Sacha, *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 249; T. Starecki, *Zarządzanie projektami dla inżynierów*, Wydawnictwo BTC, Legionowo 2011, s. 74; P. Kosiuczenko, M. Śmiałek, J. Swacha, *Od procesów do oprogramowania: badania i praktyka*, PTI, Warszawa 2015.

szkodliwe dla projektu. Można zatem mówić o ryzyku negatywnym i pozytywnym w kontekście jego oddziaływania na projekt. Praktyka pokazuje, że realizacja każdego projektu jest nieodłącznie związana z ryzykiem i wynika wprost z samej definicji projektu, a dokładniej z jego unikatowości.

W niniejszym opracowaniu autorki, abstrahując od definicyjnej różnorodności pojęć ryzyka[4], skupiają się na identyfikacji jego grup i określeniu ich wpływu na przykładzie wybranych projektów. Zwłaszcza istotne jest dla nich wskazanie i rozpoznanie zachowań zespołów wykonawczych zaangażowanych w realizację projektu oraz prezentacja przesłanek zastosowania metodyki zarządzania ryzykiem i wynikających z tego wniosków.

2. Istota ryzyka i determinanty zarządzania nim

W najbardziej ogólnym ujęciu celem zarządzania ryzykiem w projekcie jest zwiększenie prawdopodobieństwa sukcesu projektu przez zmniejszenie prawdopodobieństwa porażki. Efekt ten osiąga się przez zwiększanie skutków ryzyka pozytywnego i zmniejszanie efektów ryzyka negatywnego. Z punktu widzenia realizacji projektu najistotniejsze są te rodzaje ryzyka, które mają istotny wpływ na podstawowe parametry projektu, czyli jego koszty, czas realizacji, zakres lub jakość wytworzonych produktów (tj. przedmiotów odbioru cząstkowych i końcowego)[5]. W literaturze przedmiotu wielu autorów, m.in. B. Boehm, wskazuje na konieczność uwzględnienia w każdym projekcie rodzajów ryzyka, które występują zarówno po stronie klienta, jak i po stronie wykonawcy; stąd obie strony muszą swoje ryzyko rozważyć. Przyjmuje się, że ryzyko klienta, nazywane ryzykiem biznesowym, polega przede wszystkim na tym, że niepowodzenie projektu, wzrost jego kosztu lub przekroczenie terminu zakończenia mogą pogorszyć rynkową pozycję przedsiębiorstwa, uniemożliwić wykonanie misji lub spowodować zwiększenie kosztów działania. Źródła tego ryzyka mogą być różnorakie i wymagają przygotowania przez klienta alternatywnych wariantów postępowania. Ryzyko wykonawcy, nazywane ryzykiem projektowym, polega z kolei na tym, że różne czynniki mogą uniemożliwiać wykonanie projektu w ustalonym zakresie, w wyznaczonym czasie lub w ramach danego budżetu.

---

[4] Chodzi tu o pojęcia stosowane w inżynierii oprogramowania i zarządzaniu projektami informatycznymi.

[5] T. Starecki, op.cit., s. 74.

W skład działań podejmowanych przez kierownictwo projektu w celu uniknięcia lub zmniejszenia skutków zagrożenia podczas realizacji projektu wchodzą przede wszystkim:

- okresowe przeglądy poszczególnych rodzajów ryzyka w celu kontrolowania i wykrywania symptomów jego materializacji oraz kontrola skuteczności działań zarządczych;
- działania zarządcze przedsiębrane po materializacji ryzyka, zmierzające do uniknięcia lub ograniczenia jego szkodliwych skutków.

Aby zapewnić rzeczywistą ochronę projektu przed skutkami ryzyka, wszystkie podejmowane w tym zakresie działania muszą być zaplanowane i przewidziane w harmonogramie oraz budżecie projektu. Dlatego planowanie zarządzania ryzykiem jest jednym z istotnych (kluczowych) elementów planowania projektu. Wynikiem planowania obsługi ryzyka w projekcie są dwa dokumenty zarządcze, tj. plan zarządzania ryzykiem (*risk management plan*) i rejestr ryzyka (*risk register*). W pierwszym z dokumentów wskazuje się: metody wykrywania ryzyka, oceny podejmowanych działań oraz osoby odpowiedzialne za wykonanie tych zadań. Drugi dokument obejmuje:

- identyfikację ryzyka, czyli określenie tych (wszystkich) przyszłych sytuacji lub zdarzeń, które mogą prowadzić do zagrożenia;
- ocenę stopnia zagrożenia, na którą składa się ocena prawdopodobieństwa wystąpienia ryzyka i szkodliwości jego skutków;
- zaplanowanie sposobów postępowania, które pozwolą uniknąć ryzyka lub ograniczyć jego szkodliwe skutki, jeśli ryzyko wystąpi.

Podczas wykonania projektu rejestr ryzyka staje się dokumentem operacyjnym. Służy bieżącej rejestracji stanu wszystkich zidentyfikowanych rodzajów ryzyka, zapisywaniu podjętych działań i dokumentowaniu postępów w usuwaniu skutków ryzyka[6].

Źródła ryzyka mogą tkwić w zewnętrznym otoczeniu projektu, przyjętych metodach pracy lub sposobie organizacji projektu i zarządzania nim[7]. W czasie identyfikacji ryzyka można posłużyć się prostą klasyfikacją ryzyka, zgodnie

[6] K. Sacha, op.cit., s. 295.

[7] *Managing Successful Project with PRINCE2*, Fourth Edition, The Stationery Office, London 2005.

z którą do podstawowych jego rodzajów jest zaliczane ryzyko: zewnętrzne[8], organizacyjne[9], zarządzania[10] i techniczne[11].

Projekty informatyczne są zaliczane do najbardziej ryzykownych, jeśli chodzi o ich realizację zgodnie z umową. Jest to wypadkowa skomplikowanych działań i różnych czynników. Po pierwsze, instytucje prawa cywilnego i prawa autorskiego dotyczące zamawiania dzieł (utworów, projektów) nie do końca odpowiadają specyfice tworzenia, wdrażania i eksploatacji programów komputerowych. Szczególnie uwidacznia się to na etapie odbiorów jakościowych, w zakresie rękojmi za wady czy świadczeń gwarancyjnych. Po drugie, realizacja projektu IT wymaga ścisłego współdziałania zamawiającego i wykonawcy, a co za tym idzie – precyzyjnego określenia w umowie szeregu zagadnień związanych z tego rodzaju projektem, a, jak wykazuje praktyka, strony nie zawsze odpowiednio ustalają te kwestie w kontrakcie.

Wiele rodzajów ryzyka związanego z realizacją projektów IT da się ograniczyć lub wyeliminować poprzez odpowiednie zapisy umowy. Dobrą praktyką jest zorganizowanie spotkania stron zainteresowanych tą realizacją i omówienie istotnych kwestii w ramach regularnych spotkań lub warsztatów. W pewnych jednak przypadkach pomiędzy stronami dochodzi do sporu odnośnie do

---

[8] Ryzyko zewnętrzne jest istotne z uwagi na fakt, że oprogramowanie tworzone w projekcie informatycznym jest przeznaczone do pracy w określonym środowisku, wyznaczonym przez biznesowe potrzeby użytkowników. Jeżeli to środowisko ulegnie zmianie, to może pojawić się presja na zmianę zakresu projektu. Jeśli umowa nie definiuje wystarczająco dokładnie wymagań i odpowiedzialności za zmiany, to koszty i czas dodatkowych prac związanych z implementacją zmian mogą zachwiać budżetem i harmonogramem projektu. Innego rodzaju ryzykiem może być nagłe wycofanie się jednego z udziałowców projektu.

[9] Ryzyko organizacyjne wynika z konieczności zarządzania zasobami. Wykonanie projektu wymaga współpracy udziałowców oraz współdziałania różnych zespołów roboczych. W każdym z miejsc styku mogą wystąpić problemy o różnym podłożu. Jeżeli przedstawiciele klienta delegowani do kontaktów z wykonawcą nie mają czasu, to mogą wystąpić trudności z uzyskaniem danych i uzgodnieniem wspólnego rozumienia proponowanych rozwiązań. Jeżeli użytkownicy obawiają się zmian wywołanych wdrożeniem projektu, to mogą nie udzielać potrzebnych odpowiedzi. Jeżeli zasoby projektu (ludzie i infrastruktura) są współdzielone z innym projektem, to mogą one nie być dostępne wówczas, gdy będą potrzebne.

[10] Ryzyko zarządzania determinuje jakość procesu wytwarzania i powstałych produktów. Najczęstszym i największym niebezpieczeństwem w tej kategorii jest błędne oszacowanie pracochłonności lub czasu potrzebnego na wykonanie niektórych zadań. Powodem tego może być niedostateczne rozpoznanie innowacyjności projektu. Skutkiem nierealistycznego planowania może być albo przekroczenie zaplanowanych terminów i brak czasu na dalsze zadania, albo pozorne ich wykonanie z licznymi błędami.

[11] Ryzyko techniczne jest utożsamiane z grupą zagrożeń wewnętrznych, które mogą wynikać z: niejednoznaczności specyfikacji wymagań, użycia nieodpowiednich metod, technik lub narzędzi oraz braku umiejętności i doświadczenia personelu.

należytego wykonania zobowiązań. Szczególnego znaczenia nabiera wówczas rola ekspertów z zakresu informatyki, to bowiem ich opinie przeważnie decydują o ocenie, czy świadczenia wykonawcy i zamawiającego zostały wykonane prawidłowo[12].

W niniejszym opracowaniu akcent został położony na: klasyfikację grup rodzajów ryzyka w zrealizowanych już projektach, określenie poziomu ich wpływu na projekt, ustalenie skutków tego oraz wskazanie niezbędnych działań.

3. Badanie poziomów ryzyka na przykładzie wybranych projektów informatycznych

W celu określenia, identyfikacji i diagnozy ryzyka wykorzystano autorską metodykę badania projektów, która została oparta na ogólnodostępnej wiedzy z zakresu zarządzania oprogramowaniem. Niektóre jej elementy dopasowano do indywidualnych potrzeb firmy wytwarzającej oprogramowanie, wynikających z jej wieloletniego doświadczenia w tej dziedzinie. Wszystkie miary (wielkości) uzyskane w trakcie badania wpisane do rejestru zostały sprecyzowane przez zespół złożony z kierowników oraz osób odpowiedzialnych za ich realizację. Wszystkie rodzaje ryzyka zdeterminowane (określone) w wybranych trzech syntetycznie opisanych projektach były na etapie badania akceptowalne z punktu widzenia zarządzających tymi przedsięwzięciami.

W praktyce doprowadziło to do ustalenia przesłanki ryzyka oraz skutków jego wystąpienia. Przesłanka ryzyka została zdefiniowana jako prosta miara, tj. iloczyn dwóch czynników: poziomu ryzyka (P) oraz skutku (S) jego wystąpienia. Dla każdego czynnika przyjęto skalę 1–5 (tabela 1) i określono poziom wystąpienia ryzyka i skutki ryzyka (podejście porządkowe).

W efekcie zastosowania prostej miary otrzymano zestawienie (tabela 2) zawierające przesłankę ryzyka (PR – czyli iloczyn: P i S). W tym przypadku przyjęto skalę 1–4 wraz z odpowiednimi zakresami (1–25).

---

[12] Warto w związku z tym poznać rolę, jaką powinny odgrywać osoby mające wiedzę z zakresu IT, szczególnie zarządzania projektami. Istotne są kryteria, którymi kierują się biegli przy ocenie tego, czy świadczenie wykonawcy zostało prawidłowo wykonane i jak powinien zostać prawidłowo określony przedmiot i zakres opinii biegłego w sprawach cywilnych o niewykonanie umowy IT. *Chaos Report – Q&A with Jennifer Lynch*, Standish Group, 2015, https://www.infoq.com/articles/standish-chaos-2015 [dostęp 21.06.2016].

Tabela 1. Skala ryzyka

Skala	Poziom wystąpienia (P)	Opis	Skutek (S)
1	pomijalne	nie wystąpiło ani razu w ciągu ostatniego roku	nieznaczący
2	niskie	pojedyncze zdarzenie w ciągu ostatniego roku	mały
3	średnie	wystąpiło w ostatnim roku lub zdarza się nieregularnie	poważny
4	wysokie	kilka zdarzeń na rok	krytyczny
5	bardzo wysokie	kilka zdarzeń w miesiącu lub częściej	katastrofalny

Źródło: opracowanie własne.

Tabela 2. Przesłanka ryzyka jako podstawowa miara

Skala	Zakres	Typ i charakterystyka przesłanki ryzyka (PR)
1	1–4	NISKIE RYZYKO: ryzyko akceptowalne, podlegające monitorowaniu podczas cyklu analizy ryzyka
2	5–10	ŚREDNIE RYZYKO: ryzyko może być zaakceptowane przez kierownictwo komórki na podstawie wdrożonych i utrzymywanych działań minimalizujących (niwelujących) skutki
3	12–16	WYSOKIE RYZYKO: ryzyko nieakceptowane, stąd w celu jego ograniczenia konieczne jest podjęcie działań na podstawie decyzji dyrekcji
4	20–25	BARDZO WYSOKIE RYZYKO: ryzyko nieakceptowalne, a zatem natychmiast trzeba podjąć na podstawie decyzji dyrekcji konieczne działania w celu jego obniżenia

Źródło: opracowanie własne.

W celu weryfikacji przyjętej metodyki w badaniu posłużono się trzema różnymi projektami informatycznymi (A, B, C), które zostały w syntetyczny sposób zaprezentowane w tabeli 3. Badanie polegało na analizie tych projektów pod kątem zastosowanej technologii, czasu realizacji, liczebności zespołu itp.

Projekt A – oparty na technologii Delphi, rozłożony w czasie, zespół 42-osobowy, złożony z trzech kierowników, ośmiu analityków, trzech projektantów, 14 programistów, sześciu testerów, czterech specjalistów ds. wdrożeń IT oraz czterech specjalistów ds. obsługi klienta (*Helpdesk*). Projekt skierowany do kilkuset rozproszonych w całej Polsce klientów, o bardzo zróżnicowanym poziomie dojrzałości informatycznej oraz mocno zróżnicowanych wymaganiach ze względu na uwarunkowania prawne w różnych regionach samorządowych. Realizacja projektu polegała na działaniach utrzymaniowych systemu już istniejącego

(naprawa błędów, dostosowywanie do zmian przepisów prawa) oraz pracach rozwojowych wynikających z różnic w realizacji procesów biznesowych poszczególnych użytkowników.

Projekt B – wykorzystano technologię Java, projekt krótkoterminowy, zespół 8-osobowy, złożony z kierownika, analityka, projektanta, trzech programistów oraz dwóch testerów. Projekt indywidualny, na zamówienie klienta, skierowany do ściśle określonej jednostki organizacyjnej. Realizacja projektu polega na zbudowaniu nowego systemu na podstawie wymagań biznesowych klienta.

Projekt C – zastosowano technologię mieszaną (Java, technologie mobilne), zespół 20-osobowy, złożony z dwóch kierowników, czterech analityków, dwóch projektantów, siedmiu programistów oraz trzech testerów. Projekt skierowany do określonej grupy klientów skupionych w jednej organizacji, w której jasno zostały określone zasady funkcjonowania poprzez centralnie narzucone procesy technologiczne. Celem projektu była budowa nowego systemu według wymagań biznesowych klienta.

W tabeli 3 zestawiono dobrane celowo projekty, uwzględniając takie czynniki (kryteria) jak:

- wykorzystana technologia;
- rodzaj klienta (rozproszony, scentralizowany);
- liczebność zespołów zależna od wielkości i indywidualnych potrzeb;
- złożoność merytoryczna systemu;
- czas trwania, określony według szacunków złożoności oprogramowania.

Tabela 3. Zestawienie wybranych projektów

Projekt	Technologia	Czas trwania (lata)	Rodzaj klienta	Złożoność zespołu	Złożoność merytoryczna systemu
A	Delphi	1–10	rozproszony	bardzo duża (42 osoby)	bardzo duża liczba wymagań pochodzących od różnych klientów
B	Java	2–4	centralny	mała (osiem osób)	duża liczba wymagań pochodzących od jednego klienta umiejscowionego w jednej jednostce organizacyjnej
C	Java, technologie mobilne	poniżej roku	rozproszony	średnia (20 osób)	duża liczba wymagań pochodzących od rozproszonej geograficznie organizacji klientów

Źródło: opracowanie własne.

Dla poszczególnych projektów wybrano grupy ryzyka (tabela 4) i przeanalizowano je pod kątem: zespołu realizującego projekt, dokumentacji wykorzystywanej oraz wytwarzanej w projekcie, infrastruktury wykorzystywanej przez zespół, harmonogramu projektu oraz wdrożenia systemu u klienta (analiza dotyczyła 5 grup).

Tabela 4. Wykaz grup ryzyka i działania podjęte w momencie ich materializacji

Kod ryzyka	Grupa ryzyka	Podatność	Przykłady zagrożeń	Działania
1Z	zespół	częste zmiany kadrowe	niestabilny zespół, strata czasu na szkolenie nowych pracowników, brak poczucia bezpieczeństwa	właściwa polityka kadrowa, podejmowanie działań integrujących zespół, wydzielenie stabilnego trzonu zespołu, złożonego z zaufanych pracowników
2Z	zespół	brak kompetencji kadry zarządzającej	niewłaściwe zarządzanie, niewłaściwy nadzór, chaos organizacyjny	szkolenia z zarządzania, stosowanie nowych technik zarządzania, wymiana doświadczeń między kierownikami
3D	dokumentacja	niejasny lub niekompletny opis analityczny lub techniczny	brak opisu dokumentacji lub niekompletny opis	stworzenie standardów przygotowywanej dokumentacji i odpowiednia weryfikacja tworzonych dokumentów
4D	dokumentacja	zmienność wymagań	niewłaściwe zarządzanie wymaganiami, chaos organizacyjny	dokumentowanie realizowanych prac, uwzględnienie w umowie etapu akceptacji wymagań przez klienta
5I	infrastruktura	różnorodność infrastruktury	różny poziom infrastruktury dostępnej u klienta	szczegółowa analiza wpływu poziomu infrastruktury na projekt na każdym etapie realizacji
6I	infrastruktura	awaria infrastruktury	awaria infrastruktury lub sieci podczas realizacji projektu	stworzenie procedur nadzoru nad infrastrukturą oraz systemu powiadamiania o awarii

Kod ryzyka	Grupa ryzyka	Podatność	Przykłady zagrożeń	Działania
7H	harmonogram	czas trwania projektu	krótki czas na realizację założonych zadań	kontrola stanu realizacji prac na każdym etapie projektu, wczesne ostrzeganie o możliwych przekroczeniach budżetu lub czasu
8H	harmonogram	zmiany harmonogramu podczas realizacji projektu	możliwość zmiany poszczególnych terminów wewnętrznych w czasie realizacji całego projektu	monitorowanie wpływu zmian na ostateczny termin i budżet projektu na każdym etapie jego realizacji
9W	wdrożenie	złożony model wdrożenia systemów	trudności podczas wdrożenia systemu wynikające z organizacji pracy klientów	przeprowadzenie szczegółowej analizy przedwdrożeniowej i przedstawienie jej do akceptacji klienta
10W	wdrożenie	czas wdrożenia	wydłużenie czasu wdrożenia	przeprowadzenie szczegółowej analizy przedwdrożeniowej, kontrola stanu wdrożenia przez kierownika projektu

Źródło: opracowanie własne.

W trzech analizowanych projektach metodą ekspercką ustalono odpowiednio poziom[13] (P) i skutek (S), a także przesłankę (PR). Tabela 5 prezentuje otrzymane wyniki, zaś rysunek 1 stanowi graficzną ilustrację istotnych parametrów (w tym przypadku PR).

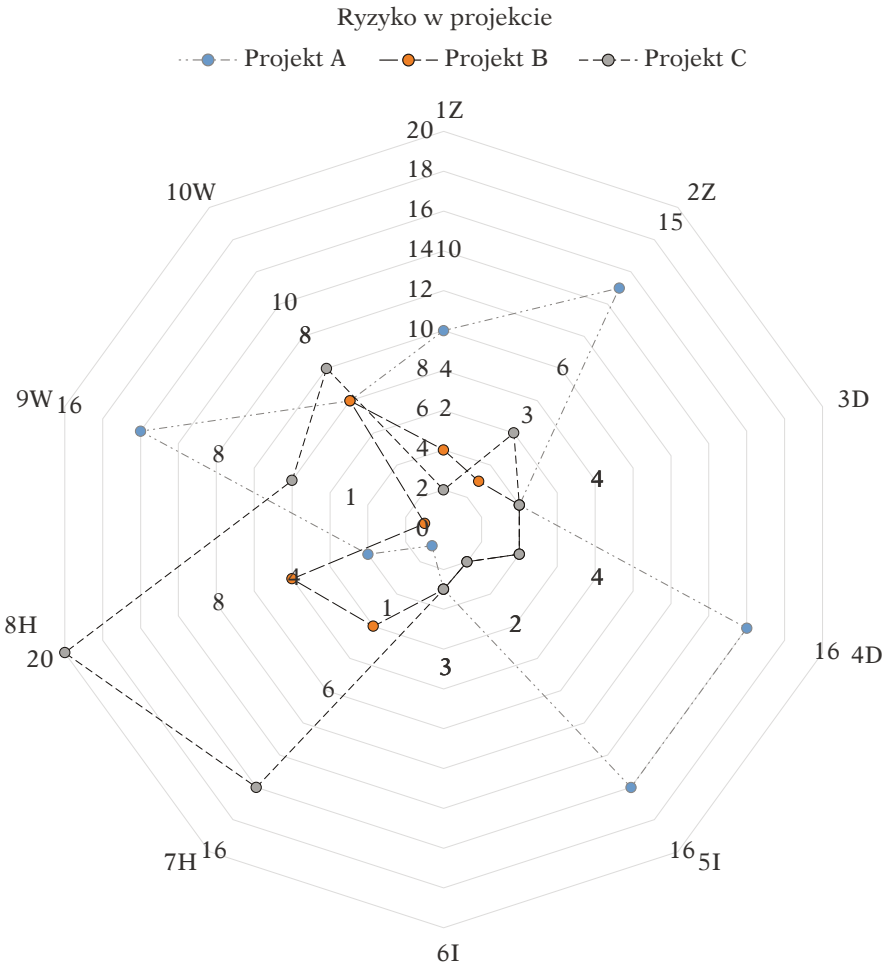
Tabela 5. Zestawienie rodzajów ryzyka w przypadku projektów A, B, C

Ryzyko	Projekt A			Projekt B			Projekt C		
	P	S	PR	P	S	PR	P	S	PR
1Z	5	2	10	2	2	4	1	2	2
2Z	3	5	15	1	3	3	2	3	6
3D	2	2	4	2	2	4	2	2	4
4D	4	4	16	1	4	4	1	4	4
5I	4	4	16	1	2	2	1	2	2

[13] W literaturze przedmiotu każde ryzyko jest oceniane w odniesieniu do prawdopodobieństwa jego wystąpienia i wpływu na realizację projektu. Stosowane są dwa podejścia, tzn. oceny liczbowe i oceny porządkowe. W artykule zastosowano drugie podejście.

Ryzyko	Projekt A			Projekt B			Projekt C		
	P	S	PR	P	S	PR	P	S	PR
6I	1	3	3	1	3	3	1	3	3
7H	1	1	1	3	2	6	4	4	16
8H	4	1	4	4	2	8	4	5	20
9W	4	4	16	1	1	1	2	4	8
10W	4	2	8	2	4	8	2	5	10
Średnia	**3,2**	**2,8**	**9,3**	**1,8**	**2,5**	**4,2**	**2**	**3,4**	**7,5**

Źródło: opracowanie własne.



Rysunek 1. Poziom ryzyka w trzech projektach

Źródło: opracowanie własne.

Analiza otrzymanych wyników upoważnia autorki do sformułowania kilku wniosków (spostrzeżeń):

1. W przypadku żadnego z projektów (A, B, C) nie wystąpił najwyższy poziom ryzyka, co świadczy o wysokiej dojrzałości organizacji realizującej projekty.
2. Najwyższy średni poziom ryzyka (tabela 5) stwierdzono w przypadku projektu A, który cechują: najdłuższy termin, największa liczba klientów i największy zespół realizujący.
3. Najwyższy pionom ryzyka zarejestrowano w przypadku projektu C, dotyczył on ryzyka 8H, projekt ten miał najkrótszy termin realizacji, stąd największy wpływ ryzyka zmian w terminie realizacji.
4. Najwięcej i najmniej ryzyka na poziomie wysokim odnotowano w przypadku projektów A i B.
5. Najmniej ryzyka na poziomie niskim stwierdzono w przypadku projektu A.
6. Najbardziej ryzykowny okazał się projekt A, najmniej projekt B.

4. Podsumowanie

Na temat ryzyka i metod szacowania jego wielkości powstają obszerne publikacje[14]. Wydaje się jednak, że nie ma uniwersalnych metod jego szacowania. Autorki, analizując trzy różnorodne projekty, dokonały oceny ryzyka każdego z nich, uwzględniając takie czynniki, jak: liczebność zespołu, wiedza i kompetencje członków, kompletność dokumentacji, harmonogram. Na podstawie obserwacji wskazują, że jeśli zespół wykonawczy nie godzi się na ryzyko, to musi skupić się na działaniach zapobiegających, ograniczających jego wpływ. Obserwacja i analiza ryzyka na każdym etapie procesu wytwarzania oprogramowania nie eliminują całkowicie jego wystąpienia, ale pozwalają zachować kontrolę w realizowanym projekcie.

Reasumując: bezsporne wydaje się opracowanie i zastosowanie odpowiedniej metody oceny ryzyka w różnych aspektach związanych z procesem wytwarzania oprogramowania, a także w ramach eksploatacji systemów informatycznych. Odpowiednie mechanizmy monitorowania wskazanych miar (wartości) i ich wrażliwości gwarantują prawidłowe działanie w tym zakresie. Należy podkreślić

[14] J. Phillips, op.cit.; A. Koszlajda, *Zarządzanie projektami IT. Przewodnik po metodykach*, Helion, Gliwice 2010; K. Sacha, op.cit.

fakt, że najważniejszy w tych wszystkich przypadkach jest czynnik ludzki, który niestety jest najbardziej zawodny i wymaga nieustannej uwagi.

Bibliografia

Boehm B., *Software Risk Management: Principles and Practices*, IEEE Software, 1991.

Kosiuczenko P., Śmiałek M., Swacha J., *Od procesów do oprogramowania: badania i praktyka*, PTI, Warszawa 2015.

Koszlajda A., *Zarządzanie projektami IT. Przewodnik po metodykach*, Helion, Gliwice 2010.

Managing Successful Project with PRINCE2, Fourth Edition, The Stationery Office, London 2005.

Phillips J., *Zarządzanie projektami IT*, Helion, Gliwice 2004.

Sacha K., *Inżynieria oprogramowania*, Wydawnictwo Naukowe PWN, Warszawa 2010.

Starecki T., *Zarządzanie projektami dla inżynierów*, Wydawnictwo BTC, Legionowo 2011.

Źródła sieciowe

Chaos Report – Q&A with Jennifer Lynch, Standish Group, 2015, https://www.infoq.com/articles/standish-chaos-2015 [dostęp 21.06.2016].

* * *

Study of the Effect of the Selected Groups of Risks on IT Projects

Abstract

There are many methodologies for calculating risk in the implementation of projects. The authors of the article present the chosen method for the estimation, which is tailored to the individual needs of a team performing IT projects and is the resultant of the recommended methods of risk analysis. At the same time, they make an attempt to study how the selected group of risks affect projects, what is the difference between them and what the levels of risk and the effects of risk are, depending on the character of a project, the type of the customer, the type of implementation or complexity of a team.

Keywords: risks, group of risks, risk management plan