

O FORMALNYCH I PRAKTYCZNYCH ZASADACH ZARZĄDZANIA RYZYKIEM PROJEKTÓW INFORMATYCZNYCH

GRZEGORZ HOŁOWIŃSKI □ □ □ □ KRZYSZTOF MAŁECKI

Streszczenie

Autorzy przedstawili zagadnienie zarządzania ryzykiem projektów informatycznych w ujęciu formalnym jak i praktycznym. Formalne aspekty związane są z zaleceniami i wymaganiami stosowanych na całym świecie metodologii PMI i PMBook. Zalecenia praktyczne zostały opracowane na podstawie doświadczeń autorów, zdobytych w ciągu ostatniej dekady w projektach informatycznych krajowych i międzynarodowych.

Słowa kluczowe: zarządzanie projektami, zarządzanie ryzykiem w projektach, inżynieria oprogramowania

1. Wstęp

Kluczowym czynnikiem projektów informatycznych jest zapewnienie deklarowanego czasu dostarczenia produktu na rynek. Każdy projekt jest ograniczony poprzez czas, koszty i zakres, a zmiana któregokolwiek z tych czynników wpływa na pozostałe.

Prowadzenie projektów informatycznych przy minimalizowaniu czasu i kosztów prowadzi do pojawiania się nowych, dodatkowych czynników ryzyka, niezależących tylko od złożoności projektu. Wybór technologii, dostępność odpowiednich zasobów – np. specjalistów, ekspertów, urzędów – tylko w określonych oknach czasowych powoduje, że wzrasta ryzyko niedostarczenia poszczególnych produktów w czasie. Prowadzić to może do zaniechania lub kosztownych zmian w projektach (patrz Tabela 1).

Zarządzanie ryzykiem jest zagadnieniem, któremu poświęcono liczne książki i publikacje¹²³⁴. Zarządzanie ryzykiem pozwala zapanować nad problemami z tym związanymi. Dynamiczny rozwój metod zarządzania projektami i zarządzania ryzykiem rozwija się w dwóch wspierających się wzajemnie obszarach – w teorii i w praktyce. Wnioski z praktyki (ang. *lessons learned*) zarządzania projektami informatycznymi zostały przedstawione między innymi w pracach Kwak i in. i Roberta⁵⁶.

¹ Buttrick R., *The Project Workout: 4th edition, Financial Times/ Prentice Hall, 2009, s. 560.*

² Heldman K., *Project Manager's Spotlight on Risk Management, Jossey-Bass, 2005, s. 224.*

³ Hillson D., *Practical Project Risk Management: The Atom Methodolog, Management Concepts, 2007, s. 224.*

⁴ Kendrick T., *Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project, AMA-COM/American Management Association, 2003, s. 358.*

⁵ Roberts B.B., *Lessons-learned: round 2, INCOSE Proceedings of a Symposium on Risk Management, 2001 (<http://www.futron.com/pdf/ROBERTSFinal.pdf>).*

⁶ Kwak Y.H., Stoddard J., *Project risk management: lessons learned from software development environment, Technova-*

Roberts wskazuje na następujące zagadnienia⁷:

- najpoważniejsze czynniki ryzyka zostają bardzo często przeoczone przez zarządzających projektami,
- menadżerowie nieodpowiednio kategoryzują czynniki ryzyka i poświęcają nim nieodpowiednie zasoby,
- urzeczywistnienie ryzyka uderza w wiele parametrów projektu – czas, harmonogram, aspekty techniczne realizacji – łączne oddziaływanie nie jest poprawnie oszacowane na etapie planowania obsługi materializacji ryzyka,
- identyfikacja ryzyka jest krytycznym etapem w procesie zarządzania ryzykiem jednak pomimo tego jest często traktowana po macoszemu,
- podejście typu „szybciej, lepiej, taniej” zwiększa ryzyko w projekcie,
- kierownik projektu musi zajmować mocną pozycję, aby trzymać w ryzach proces zarządzania ryzykiem.

Kwak i Stoddard uzupełniają te wnioski o inne istotne kwestie⁸:

- kierownicy projektów nie zawsze mają czas na wdrażanie formalnego procesu zarządzania ryzykiem,
- zarządzanie ryzykiem jest wartością dodaną do projektu w ramach produktów zarządczych, pomimo tej powszechnej wiedzy tylko zbiurokratyzowane instytucje (w Stanach Zjednoczonych) pozwalają sobie na korzystanie z usług konsultantów zajmujących się tą tematyką,
- projekty wymagają, aby uczestniczący w nich ludzie rozwijali swoje umiejętności i byli zmotywowani także do zmian swoich zachowań,
- rzeczywista pozytywna zmiana w zarządzaniu ryzykiem musi zaistnieć nie tylko na poziomie zarządzających przedsiębiorstwem i projektami, ale także na poziomie pracowników – niestety zmiany często są deklarowane wyłącznie na papierze, co powoduje, że wszyscy, których zmiana powinna dotyczyć zachowują dobre samopoczucie.

Celem niniejszej pracy jest przedstawienie wybranych formalnych reguł zarządzania ryzykiem proponowanych przez metodologię PRINCE2⁹ i PMI/PMBook¹⁰ oraz praktycznych zasad zarządzania ryzykiem w projektach informatycznych. Analiza, komentarze i propozycje praktycznych zasad zostały poparte ponad dziesięcioletnim doświadczeniem autorów z uczestnictwa w realizacji projektów informatycznych w zespołach krajowych i międzynarodowych.

tion, Elsevier, Nov., 2003, s. 915–920.

⁷ Roberts B.B., *Lessons-learned: round 2, INCOSE Proceedings of a Symposium on Risk Management, 2001* (<http://www.futron.com/pdf/ROBERTSFinal.pdf>).

⁸ Kwak Y.H., Stoddard J., *Project risk management: lessons learned from software development environment, Technovation, Elsevier, Nov., 2003, s. 915–920.*

⁹ PRINCE2, *Managing Successful Projects with PRINCE2, Her Majesty's Stationery Office, 2005, s. 484.*

¹⁰ PMI, *A Guide to the Project Management Body of Knowledge, Fourth Edition, p. 510, 2008, str 510.*

Tabela 1. Przykłady nieudanych projektów informatycznych w pierwszej dekadzie XXI wieku

Przedsiębiorstwo	Strata [mln USD]	Opis system informatycznego, którego rozwój lub wdrożenie nie powiodło się
Hudson Bay (Stany Zjednoczone)	33,3	Problemy z systemem magazynowym
Avis Europe PLC (Wielka Brytania)	54,5	Nieudane wdrożenie (zaniechano prac wdrożeniowych) systemu ERP
Ford Motor Co. (Stany Zjednoczone)	400,0	Nieudane wdrożenie systemu do zarządzania zakupami
J Sainsbury PLC (Wielka Brytania)	527,0	Porzucenie systemu zarządzania łańcuchem dostaw
Hewlett-Packard Co. (Stany Zjednoczone)	160,0	Problemy z systemem ERP
AT&T Wireless (Stany Zjednoczone)	100,0	Problemy z przejściem do nowej wersji systemu CRM
McDonald's Corp. (Stany Zjednoczone)	170,0	Zaprzestanie rozwoju prac nad innowacyjnym systemem informacyjnym do obsługi zakupów
Nike Inc. (Stany Zjednoczone)	100,0	Problemy z systemem zarządzania łańcuchem dostaw
Kmart Corp. (Stany Zjednoczone)	130,0	Nieudane wdrożenie (zaniechane) systemu zarządzania łańcuchem dostaw

Źródło: Opracowanie własne.

2. Czynniki ryzyka w projektach informatycznych

Ryzyko projektu to skumulowany efekt prawdopodobieństwa wystąpienia niepewnych zdarzeń, które mogą korzystnie lub niekorzystnie wpływać na realizację projektu i osiągnięcie jego celów¹¹.

Zarządzanie ryzykiem wg strukturalnej metodyki zarządzania projektem PRINCE2¹² to „[...] radzenie sobie z sytuacją narażenia projektu na ryzyko (tzn. prawdopodobieństwo wystąpienia określonych zagrożeń oraz gdy się one urzeczywistnią, ich potencjalnych skutków). Celem jest planowanie nad stopniem tego narażenia poprzez podejmowanie działań utrzymujących ryzyko na akceptowalnym poziomie w sposób efektywny kosztowo”.

W praktyce w organizacjach często marginalizuje się zarządzanie ryzykiem mając nadzieję, że będą one w stanie poradzić sobie z problemami, które się pojawiają.

Jones sprowadził czynniki ryzyka w projekcie informatycznym do trzech grup¹³:

- ryzyka związanego z niewłaściwym szacowaniem czasu realizacji projektu,
- ryzyka wynikającego z błędnych lub optymistycznych raportów okresowych,
- ryzyka związanego z naciskami wywieranymi na projekt, kierownika i zespół projektowy.

Boehm wskazał ryzyka związane z realizacją projektów przez firmy informatyczne¹⁴, tj.:

¹¹ PRINCE2, *Managing Successful Projects with PRINCE2*, Her Majesty's Stationery Office, 2005, s. 484.

¹² Tamże.

¹³ Jones, C., *Minimizing the risks of software development*, Cutter IT Journal 11 (6), s. 13–21, 1998.

- brak odpowiedniego zespołu (problemy kadrowe) – problemy z doбором członków zespołu, z możliwościami pozyskania specjalistów na rynku pracy, ubytki w czasie realizacji projektu,
- nierealny budżet i harmonogram – sytuacja oczekiwany czas i koszt realizacji projektu nie pozwala na realizację projektu a projekt mimo to jest rozpoczynany; sytuacja taka ma miejsce, gdy mamy do czynienia z naciskami na podjęcie projektu (np. wewnątrz firmy, aby podjąć ryzyko i spróbować zdobyć nowy rynek lub klienta) lub błędnie oszacowano koszt i czas realizacji projektu,
- implementacja funkcjonalności niezgodnych z wymaganiami (strata czasu i innych zasobów) na skutek błędnej komunikacji, niezrozumienia lub niejasności czy niejednoznaczności wymagań,
- implementacja złych i niefunkcjonalnych interfejsów użytkownika wynikająca np. z braku komunikacji z klientem lub przyszłym użytkownikiem,
- zbytne „dążenie do doskonałości” powodujące implementację nadmiarowych i nieoczekiwanych przez nikogo funkcjonalności – mamy z tym do czynienia, gdy programiści chcą oddać najlepszy produkt poświęcając zasoby na jego wykańczanie, podczas gdy wymagane jest oddanie produktu spełniającego podstawowe wymagania,
- nieskończone – ciągłe zmiany w wymaganiach (ang. CR, change request), które mogą doprowadzić każdy projekt do porażki, związane z problemami z komunikacją lub jednoznacznym określeniem wymagań, braku determinacji w ograniczaniu liczby zmian w szczególności w końcówce projektu (zamrażanie zmian),
- problemy ze komponentami pozyskiwanymi poza zespołem (zakup, zlecenie wykonania komponentów) – dostarczonymi po terminie, z ich jakością, itp.,
- problemy z zewnętrznymi zadaniami zlecanymi, z ich jakością, terminami – zadania i produkty zlecane do wykonania na zewnątrz należy rozpatrywać jako projekty obciążone swoimi ryzykami wpływającymi na ryzyka realizacji projektu głównego,
- problemy z rzeczywistą wydajnością w projekcie – bywa ona różna i zależy od wielu czynników, np. zmęczenia pracowników (którzy nie powinni pracować w nadgodzinach) czy realnym czasie pracy (dzień pracy jest równoważnikiem 8 godzin, jednakże w praktyce przyjmuje się go za równoważnik 5–6 godzin).

Wiele z wyżej wymienionych czynników ryzyka zależy bezpośrednio od ludzi biorących bezpośrednio lub pośrednio udział w realizowanym projekcie informatycznym.

¹⁴ Boehm, B.W., *Software risk management principles and practices*, IEEE Software 8 (1), 1991, s. 32–41.

3. Ryzyko w projekcie a czynnik ludzki

W celu rozpoczęcia pracy nad analizowaniem ryzyka w projekcie informatycznym należy postawić sobie kilka podstawowych pytań: jakie jest ryzyko niepowodzenia poszczególnych zadań?

- jaki jest wpływ tego ryzyka na projekt?
- co można zrobić?
- co powinniśmy zrobić?
- czy koszt działań związanych z zarządzaniem ryzykiem nie jest zbyt duży?
- czy czas działań związanych z zarządzaniem ryzykiem nie jest zbyt długi?

Odpowiedzi na powyższe pytania zależą od wiedzy, doświadczenia i odpowiedzialności uczestniczących w realizacji projektu. Podejście do ryzyka przez osoby odpowiedzialne i zarządzające projektem wpływa istotnie na proces zarządzania ryzykiem. Powszechnie znana jest klasyfikacja osób ze względu na różne podejście do ryzyka: (i) ludzie unikający ryzyka to osoby charakteryzujące się postawą zachowawczą, (ii) ludzie skłonni do podejmowania ryzyka – w ten sposób można scharakteryzować aktywnych inwestorów, (iii) ludzie świadomi ryzyka traktujący je jako normalny element codziennego życia oraz (iv) ludzie lekceważący ryzyko, często nieświadomi tego ryzyka. Nie tylko sponsor czy kierownik projektu są osobami, dla których sposób postrzegania ryzyka jest ważny – znaczenie ma także charakter innych osób, które różnie klasyfikują oraz oceniają postrzegane ryzyka i eskalują je bądź nie do swoich przełożonych.

Niezmierznie istotnym czynnikiem w realizacji projektu jest komunikacja pomiędzy uczestnikami projektu. Istotne jest jednoznaczne określenie zasad komunikacji (zakres, częstotliwość, odpowiedzialność) przed rozpoczęciem lub na samym początku projektu.

Jasne i jednoznaczne zasady komunikacji i odpowiedzialności ułatwiają pracę i pozwalają na odpowiednie reagowanie w sytuacjach zagrożenia projektu lub jego poszczególnych zadań.

Przykładem informacji niezmiernie ważnej dla zarządzania ryzykiem jest informacja o dopuszczalnych tolerancjach lub też inaczej mówiąc dopuszczalnym poziomem akceptacji ryzyka. Należy pamiętać, że osoby zarządzające ryzykiem muszą za każdym razem rozważyć i oszacować akceptowalny poziom ryzyka, który będzie się zmieniać w zależności od osobniczego podejścia do ryzyka a przede wszystkim do wag przypisywanych poszczególnym zagrożeniom.

Podobnie każdy z członków zespołu będzie analizował poszczególne ryzyka. Także i zespół projektowy będzie akceptował duże ryzyko w pewnych dziedzinach, podczas gdy w innych nie (np. tam gdzie będzie chodzić o zagrożenie dla zdrowia i życia, kwestie prawne, itp.).

Niezmierznie ważne są cechy osobowe poszczególnych członków zespołu projektowego, które mogą być załączkiem problemów natury społecznej w grupie. Ponadto przed kierownikiem zespołu stoją wyzwania związane z zatrudnianiem bądź wymianianiem członków zespołu co ma wpływ (negatywny lub pozytywny) na efektywność pracy i możliwości dotrzymania terminów.

4. Formalne zasady zarządzanie ryzykiem w projekcie informatycznym

Zarządzanie ryzykiem projektu to wszelkie działania podejmowane w zarządzaniu projektem w celu¹⁵:

- identyfikacji ryzyka (zdarzenia w projekcie),
- sklasyfikowania lub pomiaru poszczególnych rodzajów ryzyka (prawdopodobieństwa wystąpienia oraz ocena wpływu materializacji ryzyka),
- neutralizacja lub zapobiegania ryzyka (ograniczenie dotkliwości materializacji ryzyka).

Identyfikacja ryzyka polega na wytypowaniu i opisanu zdarzeń, które mogą mieć potencjalnie negatywny wpływ na realizowany projekt. Częstym problemem jest zapominanie o ryzyku które istnieje już na etapie eksploatacji produktów projektu. Pod koniec realizacji projektu zdarza się identyfikować zagrożenia, które mogą wpływać na produkt projektu w okresie jego eksploatacji – informacje te powinny być jawne dla użytkowników produktu.

W celu identyfikacji ryzyka stosuje się m.in.: przegląd specyfikacji/dokumentacji, techniki gromadzenia informacji formalnej i nieformalnej, listy kontrolne, techniki diagramowe (szacowanie i monitorowanie czasu realizacji zadań oraz dostępnych zasobów), analizę SWOT, itp.

Oprócz zastosowania w/w metod istotne znaczenie ma własne doświadczenie, które pozwala na urealnienie oceny sytuacji. Ponadto często stosuje się wspólne – z zespołem, ekspertami zewnętrznymi – identyfikowanie i szacowanie ryzyk, np. z zastosowaniem metody delfickiej. W takim przypadku można zaprosić do współpracy ekspertów zewnętrznych spoza firmy, w szczególności gdy w grę wchodzi nowe obszary merytoryczne w projekcie lub technologie niestosowane dotychczas w firmie.

Tabela 1. Analiza jakościowa z zastosowaniem wag dla szacunków prawdopodobieństwa i skutków materializacji ryzyka (szarym kolorem zaznaczono tolerowane ryzyka)

		Prawdopodobieństwo materializacji ryzyka		
		Niskie [1]	Średnie [2]	Wysokie [3]
Skutki materializacji ryzyka	Łagodne [1]	1 (1 x 1)	2 (1 x 2)	3 (1 x 3)
	Umiarkowane [3]	3 (3 x 1)	6 (3 x 2)	9 (3 x 3)
	Dotkliwe [6]	6 (6 x 1)	12 (6 x 2)	18 (6 x 3)

Źródło: Na podstawie [10].

W przypadku organizacji lub osób istotne znaczenie ma prowadzenie bazy wiedzy na temat wcześniej realizowanych projektów, zarówno tych udanych jak i nieudanych. Rejestr taki może zawierać informacje na temat zaistniałych, rozpoznanych lub niezidentyfikowanych w porę ryzyk, ich zapobieganiu oraz obsłudze w wypadku zmaterializowania. Wiedza ta jest znacząco pomocna w procesie identyfikacji ryzyka w bieżącym projekcie informatycznym.

Do identyfikacji i dalszej klasyfikacji ryzyka stosuje się także symulowanie przyszłych zdarzeń przy uwzględnieniu różnych scenariuszy rozwoju przyszłej sytuacji.

¹⁵ PMI, *A Guid to the Project Management Body of Knowledge, Fourth Edition*, p. 510, 2008, s. 510.

Klasyfikacja ryzyka polega na dokonaniu oceny ryzyka z zastosowaniem metod opisowych – nienumerycznych. Analiza jakościowa może korzystać z metod szacunkowych z wykorzystaniem określonych wag aby łatwiej klasyfikować ryzyka. Przykładowe zestawienia wag przedstawiono w tabelach (Tabela 1).

Analiza jakościowa pozwala nie tylko na doprecyzowanie ryzyk oraz prawdopodobieństwa i skutków ich materializacji ale pozwala na wygenerowanie takich produktów zarządczych jak: rejestr ryzyka, ranking ryzyk projektu informatycznego, trendów w jakościowej analizie ryzyk. Ponadto pozwala na sklasyfikowanie ryzyk na: (i) wymagające dalszej szczegółowej analizy, (ii) podlegające bieżącej obserwacji (wysokie prawdopodobieństwo wystąpienia a w szczególności wysokie koszty w przypadku materializacji ryzyka), (iii) wymagające reakcji w najbliższym czasie.

Pomiar ryzyka jest realizowany poprzez ocenę prawdopodobieństwa oraz skutków najważniejszych rodzajów ryzyka za pomocą wskaźników liczbowych. Podczas tego etapu wykonuje się analizę ilościową, która polega na przypisaniu wartości liczbowych zarówno do ryzyka projektu jako całości oraz do istotnych rodzajów ryzyka z zastosowaniem rachunku prawdopodobieństwa. Analizy ilościowej nie wykonuje się dla ryzyk sklasyfikowanych w analizie jakościowej jako nieistotnych z małym wpływem na realizację projektu informatycznego.

Do pomiaru ryzyka można zastosować metodę Monte Carlo opracowaną przez polskiego naukowca, pracującego nad amerykańską bombą termojądrową, Stanisława Ulama. Na tym etapie stosuje się także drzewa decyzyjne do kwantyfikacji wyników projektu, oceny prawdopodobieństwa osiągnięcia celu projektu czy też identyfikacji najlepszych decyzji kierowania projektem informatycznym. Innymi stosowanymi metodami są analiza wrażliwości i oczekiwana wartość pieniężna. Jednym z rezultatów analizy ilościowej jest określenie prawdopodobieństwa osiągnięcia celów kosztowych i terminowych projektu, co pozwala stwierdzić, że np. mamy X% szans na zakończenie projektu w terminie Y oraz V% szans na zamknięcie się w kosztach projektu Z PLN.

Planowanie sposobów reagowania na ryzyko sprowadza się do tworzenia strategii neutralizowania lub zapobiegania ryzyku. Istotnym wynikiem planu sposobu reagowania na ryzyko jest określenie działań, które pomogą rozwiązać problemy związane z poszczególnymi rodzajami ryzyka rozpoznanymi w procesie identyfikacji ryzyka.

Reagowanie na ryzyko sprowadza się do następujących metod: (i) unikania ryzyka, (ii) łagodzenia ryzyka, (iii) przeniesienia ryzyka, (iv) akceptacji ryzyka, (v) tworzenie rezerw na obsługę urzeczywistnionego ryzyka.

Unikanie ryzyka w praktyce może być zastosowane poprzez wybranie innej – znanej technologii informatycznej, wyboru innego partnera lub podwykonawcy do realizacji projektu, czy też na podjęciu decyzji o nie przystępowaniu do realizacji projektu. Łagodzenie ryzyka polega na jego redukcji poprzez podejmowanie działań w celu ograniczenia stopnia narażenia na nie. Przeniesienie ryzyka może polegać na np. zaproszeniu innych partnerów lub podwykonawców, ubezpieczenie się od odpowiedzialności lub zapewnieniu odpowiednich zapisów w umowie, aby przenieść koszty materializacji ryzyka na inne strony umowy. Akceptacja ryzyka jest ostatnią z metod reagowania na ryzyko i wiąże się z akceptacją poniesienia kosztów materializacji ryzyka. Firma informatyczna przygotowuje się do akceptacji ryzyka wzmacniając własną pozycję, aby znieść jego skutki. Zazwyczaj dzieje się to w sposób aktywny (tworzenie rezerw na poniesienie ewentualnych kosztów) lub pasywny (przyjęcie ryzyka).

Nadzorowania i kontrola ryzyka (monitorowanie) jest etapem, w którym następuje faktyczne wdrożenie zarządzania ryzykiem w realizacji projektu między innymi poprzez kroczącą aktualizację spisów, rejestrów ryzyk i planowanych sposobów reagowania na ryzyko. Sprowadza się to do nieustannej, bieżącej obserwacji poszczególnych rodzajów ryzyka oraz warunków przy zastosowaniu narzędzi zdefiniowanych na etapie planowania.

Na tym etapie niezwykle pomocne są działania zapobiegawcze mające na celu eliminację ryzyka zanim ono wystąpi. W przypadku materializacji ryzyka istotną rolę pełni plan awaryjny oraz plan zapasowy, mający na celu zdefiniowanie akcji i działań występujących, gdy plan awaryjny okazuje się nieskuteczny.

Należy pamiętać, że zawsze realnym właścicielem i odpowiadającym za ryzyko jest osoba zlecająca projekt w firmie – może to być właściciel firmy, przewodniczący komitetu sterującego projektem¹⁶, itp. Dotyczy to także sytuacji, gdy kierownikiem projektu nie jest żadna z wymienionych osób – a tak niemal wygląda norma w praktyce, gdzie menadżer projektu jest tylko wynajęty do prowadzenia konkretnego projektu.

Planowanie zarządzania ryzykiem sprowadza się do zapewnienia infrastruktury oraz opracowania planu zarządzania ryzykiem w projekcie informatycznym. W praktyce projekt nie jest samodzielnym bytem, ale zależy od wymogów sponsora projektu a co za tym idzie od szerszego środowiska organizacji. Zatem uwarunkowania zarządzania ryzykiem zależą od strategii zarządzania ryzykiem w organizacji realizującej projekt oraz tolerancji grup interesu wobec ryzyka.

Praktyczne podejście do zarządzania ryzykiem wymaga rejestrowania informacji o ryzyku w dokumentacji projektowej. Zakres informacji i częstotliwość raportowania może być ściśle określona lub tylko zalecana przez konkretną metodologię. W praktyce powinno się raportować informacje „w wystarczającej ilości i w odpowiednim czasie”.

Na każdym etapie zarządzania ryzykiem powinna być prowadzona dokumentacja, choćby w formie informacji cząstkowych – jeśli nie możemy podać bardziej szczegółowych danych.

Minimalne zestawienia informacyjne dotyczące procesu ryzyka są wymagane przez metodyki. Klasycznym przykładem takiego dokumentu jest **rejestr ryzyka**^{17,18}.

Rejestr ryzyka praktycznie powinien zawierać następujące informacje na temat każdego ze zidentyfikowanych ryzyk (oczywiście nie wszystkie będą od początku znane):

- nazwa ryzyka – definiowana jednoznacznie i unikalnie w celu komunikacji i odwołań,
- identyfikator ryzyka, przyjmujący stany: otwarty, zamknięty, w procesie analizie,
- właściciel ryzyka – którym jest osoba najlepiej mogąca monitorować zjawisko związane z ryzykiem – może to być menadżer projektu lub inne osoby (członkowie zespołu, nadzorujący projekt, inne osoby z organizacji realizującej lub w której realizowany jest projekt, itp.),
- wynik analizy: opis zdarzenia, prawdopodobieństwo wystąpienia P i jego wpływ W (na czas, jakość, zakres, koszt), iloczyn $P \times W$, symptomy materializacji ryzyka, sposób zarządzania ryzykiem w postaci planu awaryjnego i planu zapasowego,
- historia wpisu,
- ranking ryzyka (opcjonalny).

¹⁶ PRINCE2, *Managing Successful Projects with PRINCE2*, Her Majesty's Stationery Office, 2005, s. 484.

¹⁷ PRINCE2, *Managing Successful Projects with PRINCE2*, Her Majesty's Stationery Office, 2005, s. 484.

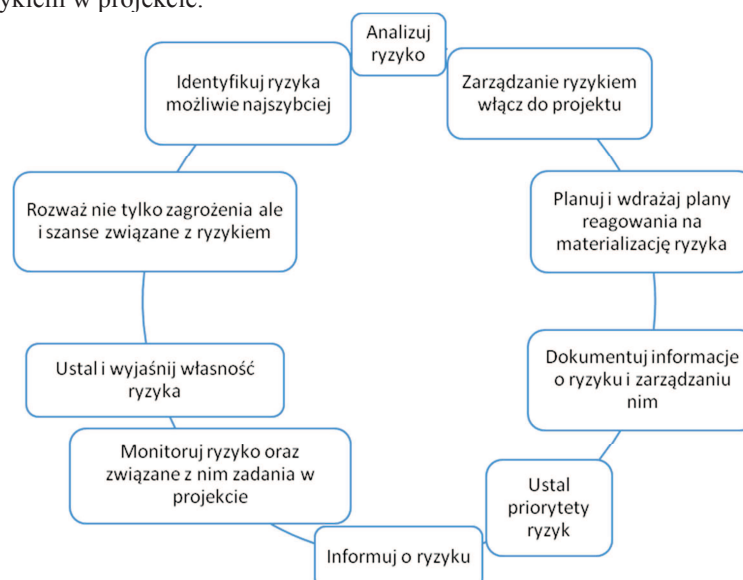
¹⁸ PMI, *A Guide to the Project Management Body of Knowledge, Fourth Edition*, p. 510, 2008, s. 510.

W procesie zarządzania ryzykiem pojawić się może wiele błędów powodujących, że nie można zdefiniować wszystkich istotnych ryzyk, które pojawiają się, materializują bądź stają nieaktualne w cyklu życia projektu informatycznego.

5. Praktyczne zasady minimalizacji ryzyka podczas prowadzenia projektów informatycznych

Bart Jutte proponuje 10 zasad zarządzania ryzykiem w projekcie¹⁹ (patrz Rysunek).

Zarządzanie ryzykiem jest częścią projektu i tak powinno być traktowane, należy przeznaczyć na nie odpowiednie zasoby (nakłady czasu, koszt). Nie uwzględnienie kosztów i czasu pracy osób zaangażowanych w zarządzanie ryzykiem powoduje, że praca ta będzie nieoszacowana i wykonywana w nieformalnym nadliczbowym czasie, bądź pomijana co doprowadzi do załamania zarządzania ryzykiem w projekcie.



Rysunek 1. Zasady zarządzania ryzykiem w projekcie wg Barta Jutte

Źródło: Opracowanie własne na podstawie [7].

Ryzyko w projekcie powinno być identyfikowane możliwie najszybciej, tak aby możliwe było uniknięcie jego urzeczywistnienia lub możliwie najlepsze przygotowanie się do zmierzenia się z wynikiem jego materializacji. Dokumentacja projektowa, często bardzo obszerna i dostępna w pełni tylko w wersji elektronicznej, nie zawsze zawiera informację o możliwych ryzykach. Jednak uważne jej czytanie (często wielokrotne i przez różne osoby) pozwala na znalezienie „między wierszami” informacji o ryzykach, które mogą się w projekcie pojawić lub są już obecne. Praca z klientem i zespołem projektowym, podwykonawcami, itd., często w formie spotkań cyklicznych, jest doskonałym źródłem informacji o ryzykach, które rozpoznawane są z czasem,

¹⁹ Jutte B., 10 Golden Rules of Project Risk Management, <http://www.projectfuture.net>.

kiedy przechodzi się na coraz niższy poziom szczegółów w projekcie (na poziom konkretnych zadań projektowych).

Informacja o zidentyfikowanych ryzykach oraz planowanych metodach reagowania na nie, może być sekretem członka lub zespołu projektowego. Informacja ta powinna trafić do zespołu – aby rozważyć możliwe działania – oraz do sponsora projektu, który, jako jego właściciel, powinien mieć wiedzę o istniejących ryzykach. Od kierownika projektu zależy, czy o konkretnym ryzyku powinien poinformować natychmiast (ryzyka o dużym prawdopodobieństwie materializacji i wpływie na projekt) czy umieścić tę informację dopiero w okresowym raporcie nt. realizacji projektu, co dzieje się w przypadku większości tego typu zdarzeń.

Bardzo często ryzyko kojarzone jest tylko z negatywnymi zjawiskami. Wynika to zazwyczaj z optymalizowania zasobów (czasu) i skupieniu się na tym aby projekt zakończył się pozytywnie. Powoduje to, że identyfikuje się zazwyczaj tylko te ryzyka, które generują negatywny wpływ na realizację projektu. Jednakże identyfikując nowe ryzyko należy rozpatrzyć nie tylko jego negatywny wpływ ale i możliwe pozytywne skutki. Ponadto ryzyka o wyłącznie pozytywnym wpływie należy traktować analogicznie do tych, których materializacja przynosi skutki negatywne. Daje to szansę na wykorzystanie możliwości, które mogą się pojawić w projekcie. Zatem wszystkie ryzyka należy analizować pod kątem wpływów pozytywnych i negatywnych, gdyż materializacja ryzyka może być szansą zaistnienia sytuacji możliwych do wykorzystania w projekcie lub szeroko pojmowanej działalności firmy.

Sama identyfikacja i przyjęcie planu działania dla obsługi ryzyka i jego materializacji nie wystarcza. Konieczne jest ustalenie właściciela ryzyka. Może nim być sponsor, kierownik projektu lub członek zespołu projektowego. Prostem i skutecznym mechanizmem jest formalne przypisanie każdego ryzyka właścicielowi, którego zadaniem będzie monitorowanie i optymalizacja ryzyka (np. poprzez zapobieganie lub przygotowanie się do jego materializacji).

Optymalne zarządzanie ryzykiem wymaga – jako warunku koniecznego choć niewystarczającego – ustalenia priorytetów dla zidentyfikowanych ryzyk. Pozwala to na zajęcie się ryzykami o najwyższych priorytetach, tych, których materializacja może stanowić największy problem.

Zidentyfikowane ryzyka wymagają dokładnej analizy, której celem jest zrozumienie ich natury, co z kolei pozwala na przyjęcie odpowiedniego sposobu reagowania. Bart Jutte rozważa analizę ryzyka na następujących poziomach²⁰:

- indywidualna analiza każdego ryzyka – jako dobry sposób na przemyślenie wyników urzeczywistnienia ryzyka,
- analiza efektów materializacji ryzyka – pozwala opisać efekty, które wystąpią w momencie urzeczywistnienia ryzyka oraz ich efekty pochodne,
- szczegółowa analiza wpływu materializacji ryzyka na parametry projektu, takie jak: koszt, czas dostarczenia produktów projektu, jakość produktów,
- analiza zjawisk poprzedzających materializację ryzyka na potrzeby monitorowania ryzyka oraz lekcji na przyszłość,
- ogólna analiza całego projektu w świetle ryzyk już zidentyfikowanych.

Planowanie i wdrażanie planów reagowania na materializację ryzyka jest wartością dodaną projektu, która pozwala na zażegnanie zagrożenia lub zminimalizowanie negatywnego wpływu urzeczywistnienia ryzyka. W przypadku, gdy mamy do czynienia z pozytywnym wpływem wystą-

²⁰ Jutte B., *10 Golden Rules of Project Risk Management*, <http://www.projectfuture.net>.

pienia jakiegoś zjawiska (ryzyko „pozytywne”) to celem właściciela ryzyka jest dążenie do materializacji ryzyka lub też zaniechanie działania – jeśli szanse na urzeczywistnienie lub ich wpływ pozytywny są małe.

Zarządzanie ryzykiem powinno być dobrze udokumentowane. Dokumentacja w postaci rejestru ryzyka pozwala nie tylko na śledzenie historii i stanu bieżącego ryzyka w projekcie ale minimalizuje szanse zapomnienia o wcześniej zidentyfikowanym ryzyku. Rejestr taki jest świetnym narzędziem do komunikacji (informowania) członków zespołu, komitetu sterującego, sponsora i innych osób, w zależności od potrzeb. W przypadku niepowodzenia projektu pozwala także bronić kierownika, który możliwie najlepiej zarządzał ryzykiem identyfikując je i planując optymalizację urzeczywistnienia ryzyka. Pomimo tego, w praktyce można jednak spotkać kierowników projektów, którzy nie chcą dokumentować zarządzania ryzykiem obawiając się, że dokumentacja ta zostanie użyta przeciwko nim.

Istotnym elementem procesu zarządzania ryzykiem jest śledzenie ryzyka oraz realizacji związanych z nim zadań projektowych. Śledzenie ryzyka dotyczy obserwacji szans jego wystąpienia, zmiany wpływu i konieczności przyjmowania innych strategii wobec jego materializacji. Śledzenie zadań powiązanych z ryzykami określonymi w rejestrze ryzyka sprowadza się do monitorowania zadań – przesunięć w harmonogramie, zmiany warunków koniecznych do rozpoczęcia, realizacji i zakończenia zadania – oraz czynników z tym powiązanych.

Opisane powyżej zasady prowadzenia projektu są, w opinii autorów, dobrymi wzorcami do zarządzania ryzykiem przez kierownika projektu. Należy je uzupełnić o zarządzanie ryzykiem na poziomie zespołu projektowego.

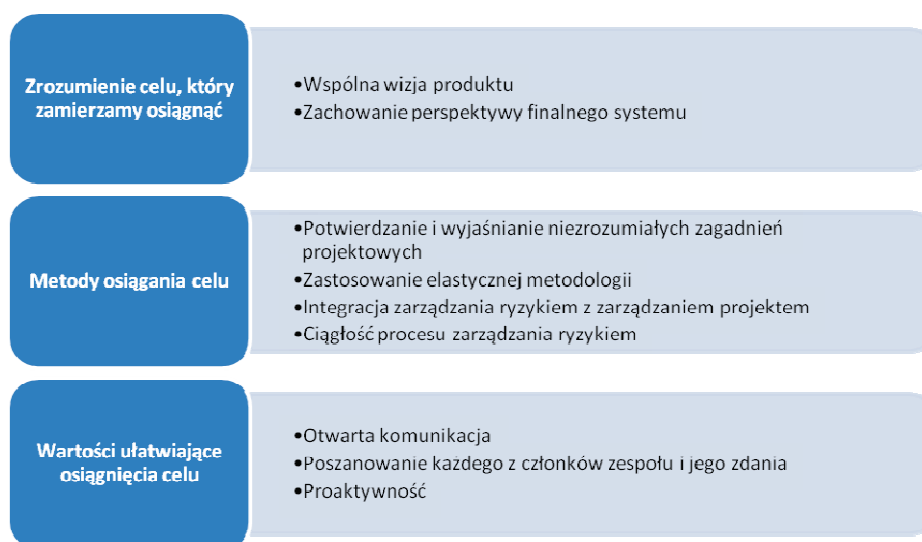
Zarządzanie ryzykiem w projekcie powinno obejmować zespół projektowy a członkowie zespołu powinni rozumieć istniejące ryzyko, brać aktywny udział w identyfikowaniu i zapobieganiu ryzyku. Pomyślna realizacja projektu może być ułatwiona jeśli zespół jest pro aktywny i realizuje zadania rozumiejąc ich celowość.

Szereg zasad zarządzania ryzykiem w pracy zespołowej został zaproponowany przez Higuera i in. W niniejszym opracowaniu podzielono te zasady na trzy grupy²¹:

- zasady zapewniające zrozumienie celu projektu,
- reguły związane z metodami realizacji projektu,
- wartości ułatwiające osiągnięcie celu przez zespół.

Każdy członek zespołu powinien rozumieć cel projektu i zakres zadań zespołu. Wymaga to wypracowania możliwie najwcześniej wizji produktu jednakowo rozumianej przez wszystkich członków zespołu. Naczelną zasadą powinno być także stałe pamiętanie i odnoszenie się do finalnego celu projektu i produktów mających powstać (lub inaczej wizji całego systemu).

²¹ Higuera R.P., Gluch D.P., i inni, *An introduction to team risk management, Special Report, CMU/SIE-94-SR-1, Software engineering Institute, 1994, s. 534.*



Rysunek 2. Podstawowe zasady minimalizacji ryzyka w pracy zespołowej

Źródło: Opracowanie własne na podstawie [4].

Drugą grupę stanowi dobór odpowiednich narzędzi w zakresie elastycznych technologii informatycznych i metodologii zarządzania projektem, zintegrowanie ciągłego zarządzania ryzykiem z projektem (jako część projektu – ciągle zadanie zarządcze) oraz jasna i czytelna komunikacja. To właśnie komunikacja stanowi największy problem w realizowaniu projektów, gdyż percepcja i zrozumienie języka, zwrotów oraz domniemania mogą powodować całkowite niezrozumienie pod przykrywką jasności zakresu i celu zadań. Sytuację szczególnie utrudniają żądania zmiany w projekcie na tle niesprecyzowanych dokładnie i mierzalnie wymogów dotyczących produktów finalnych. Stąd też proces komunikacji i wyjaśniania wszystkich niejasności powinien być ciągły i dobrze zrozumiany przez wszystkich uczestników projektu.

Ostatnia grupa zasad powiązana jest z wartościami, które powinien reprezentować zespół oraz cechami osobowymi pożądanymi u jego członków, są to:

- otwarta komunikacja pomiędzy członkami zespołu,
- proaktywność – każdy z członków zespołu powinien dążyć do inicjowania zmian i kontrolowania sytuacji, a nie jedynie reagować na nią,
- szacunek dla każdego członka zespołu i liczenie się z jego zdaniem – co pozwala na aktywny udział wszystkich w zgłaszaniu problemów, propozycji rozwiązań, itp.

Powyższe reguły dla zarządzania ryzykiem mają charakter praktyczny zweryfikowany pozytywnie przez autorów podczas uczestnictwa w projektach (krajowych i międzynarodowych) w ostatnich 10 latach. Należy je uzupełnić o konieczność ciągłej weryfikacji i wzrostu efektywności, chociażby z japońskim podejściem Kaizen, które każe pamiętać, że ulepszanie procesu zarządzania ryzykiem w projektach jest ciągłe i nie ma końca.

6. Podsumowanie

Zarządzanie ryzykiem powinno być częścią zarządzania projektem informatycznym. Nie zawsze ma to jednak miejsce w praktyce. Wpływa to na zaniechanie lub zwiększenie kosztów wielu projektów informatycznych z powodu złej komunikacji. Niezrozumienie pomiędzy klientem a producentem (zespołem projektowym) jest przyczyną 66% projektów informatycznych wg Forrester Research.

Należy pamiętać jednak, że dziedzina jaką jest zarządzanie projektami a w szczególności jego część – zarządzanie ryzykiem – dynamicznie się rozwija a praktyka wciąż zaskakuje studiami przypadków.

Autorzy przedstawili czynniki ryzyka w projekcie informatycznym ze szczególnym uwzględnieniem czynnika ludzkiego. Przedstawiono formalne, ogólne zasady zarządzania ryzykiem zebrane na podstawie metodologii zarządzania projektami PRINCE2 i PMI/PMBook. Następnie zebrano praktyczne zasady zarządzania ryzykiem w projektach, które zostały opatrzone komentarzem. Komentarz ten powstał na bazie wieloletniego doświadczenia w realizacji projektów w zespołach polskich i międzynarodowych.

Bibliografia

- [1] Boehm, B.W., *Software risk management principles and practices*, IEEE Software 8 (1), 1991, s. 32–41.
- [2] Buttrick R., *The Project Workout: 4th edition*, Financial Times/ Prentice Hall, 2009, s. 560.
- [3] Heldman K., *Project Manager's Spotlight on Risk Management*, Jossey-Bass, 2005, s. 224.
- [4] Higuera R.P., Gluch D.P., i inni, *An introduction to team risk management*, Special Report, CMU/SIE-94-SR-1, Software engineering Institute, 1994, s. 534.
- [5] Hillson D., *Practical Project Risk Management: The Atom Methodolog*, Management Concepts, 2007, s. 224.
- [6] Jones, C., *Minimizing the risks of software development*, Cutter IT Journal 11 (6), s. 13–21, 1998.
- [7] Jutte B., *10 Golden Rules of Project Risk Management*, <http://www.projectfuture.net>.
- [8] Kendrick T., *Identifying and Managing Project Risk: Essential Tools for Failure-Proofing Your Project*, AMACOM/American Management Association, 2003, s. 358.
- [9] Kwak Y.H., Stoddard J., *Project risk management: lessons learned from software development environment*, Technovation, Elsevier, Nov., 2003, s. 915–920.
- [10] PMI, *A Guid to the Project Management Body of Knowledge*, Fourth Edition, p. 510, 2008, s. 510.
- [11] PRINCE2, *Managing Successful Projects with PRINCE2*, Her Majesty's Stationery Office, 2005, s. 484.
- [12] Roberts B.B., *Lessons-learned: round 2*, INCOSE Proceedings of a Symposium on Risk Management, 2001 (<http://www.futron.com/pdf/ROBERTSFinal.pdf>).

ABOUT BOTH FORMAL AND INFORMAL RULES OF THE RISK MANAGEMENT IN IT PROJECTS

Summary

Authors presents both formal and informel aspects of risk management in IT projects. The formal ones are related to requirements of world-wide used methodologies like American PMI or British PMBook. The authors' 10 years of personal experience in software engineering gained in both national and international projects stands behind presented practical rules.

Keywords: project management, risk management, software engineering

Grzegorz Hołowiński
Zakład Logistyki i Informatyki
Wydział Inżynieryjno-Ekonomiczny Transportu
Akademia Morska w Szczecinie
ul. Henryka Pobożnego 11
e-mail: g.holowinski@am.szczecin.pl

Krzysztof Małecki
Zakład Systemów Komputerowych
Instytut Techniczny
Państwowa Wyższa Szkoła Zawodowa w Gorzowie Wlkp.
ul. Myśliborska 34
e-mail: kmalecki@wi.zut.edu.pl