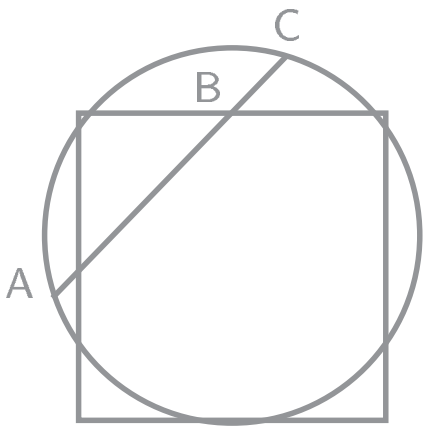
Inżynieria oprogramowania

Radosław Klimek

2015-23



http://home.agh.edu.pl/rklimek

1 Analiza i zarządzanie ryzykiem

Analiza i zarządzanie ryzykiem

Joseph M. William TURNER: *Parowiec w burzy śnieżnej*

Ryzyko

Definicja

Ryzyko to możliwość zaistnienia sytuacji niepożądanej (ocenianej negatywnie), zawsze jako skutek pewnego zdarzenia. ⌟

Definicja [Woodward i in.]

Ryzyko jest zobiektywizowaną niepewnością wystąpienia niepożądanego zdarzenia. ⌟

Definicja [Górski]

Ryzyko oznacza możliwość obniżenia poziomu sukcesu przedsięwzięcia (do całkowitego braku sukcesu włącznie). ⌟

Ryzyko (cd.)

Ryzyko jest scharakteryzowane przez (przynajmniej) dwie wielkości:

1. **prawdopodobieństwo** wystąpienia pewnego zdarzenia,
2. (potencjalnie) **negatywne skutki** tego zdarzenia.

Ryzyko (cd.)

Ryzyko jest scharakteryzowane przez (przynajmniej) dwie wielkości:

1. **prawdopodobieństwo** wystąpienia pewnego zdarzenia,
2. (potencjalnie) **negatywne skutki** tego zdarzenia.

Uwagi:

- Jeżeli **prawdopodobieństwo** pewnego zdarzenia jest równe lub bliskie zera, to albo zdarzenie to nigdy nie wystąpi – wówczas jednak mamy doczynienia z sytuacją braku zagrożenia, albo występuje pewność – wtedy jednak należy wiązać to raczej z istnieniem pewnego problemu wymagającego rozwiązania, ale już nie z samym ryzykiem.
- Zdarzenie związane z ryzykiem musi mieć także potencjalnie **negatywne skutki** – gdyby miało tylko skutki pozytywne, to wówczas nie byłaby to sytuacja istotna z punktu widzenia istnienia zagrożenia.

Ryzyko a strony projektu

Ryzyko wynikające z niepożądanej sytuacji może zmniejszyć satysfakcję poszczególnych stron projektu, np.:

- klient – przekroczony budżet, przekroczony harmonogram;
- wykonawca – odmowa klienta uznania systemu za ukończony, nieuznanie umowy za zakończoną;
- użytkownik – niewystarczająca lub błędna funkcjonalność, nieprzyjazny interfejs użytkownika, nieefektywność i zawodność systemu;
- instalator – trudność w dopasowaniu systemu do środowiska użytkowego;
- a także inne przypadki braku satysfakcji uczestników-stron.

Powyższy wykaz należy traktować jako przykładowy.

Źródła ryzyka – działania i wydarzenia

Ryzyko jest związane z **podejmowaniem decyzji**. Przykładowe powody powstawania **niepewności** i w konsekwencji pojawienia się ryzyka:

- złożone struktury (dane, funkcjonalność);
- długi cykl życia projektu;
- zmieniające się technologie informatyczne;
- zmienność wymagań.

Źródła ryzyka – działania i wydarzenia (cd.)

Źródła ryzyka (charakterystyka wykonawcza):

- działania które zamierzamy podjąć;
- działania które inni zamierzają podjąć; oraz
- wydarzenia zewnętrzne będące poza naszą bezpośrednią kontrolą.

Inny podział (umiejscowienie w stosunku do projektu):

- wewnętrzne – wynikające z właściwości procesu;
- zewnętrzne – wynikające z uwarunkowań realizacyjnych; a także
- wprowadzone – skutek niedostatecznej wiedzy lub zaniedbań.

Źródła ryzyka – obszary występowania

Podstawowe obszary występowania ryzyka:

- polityka;
- zasoby ludzkie;
- uwarunkowania finansowe;
- uwarunkowania prawne;
- terminarz;
- wymagania jakościowe;
- oprogramowanie (software);
- sprzęt (hardware);
- techniczne.

Źródła ryzyka – obszary występowania (cd.)

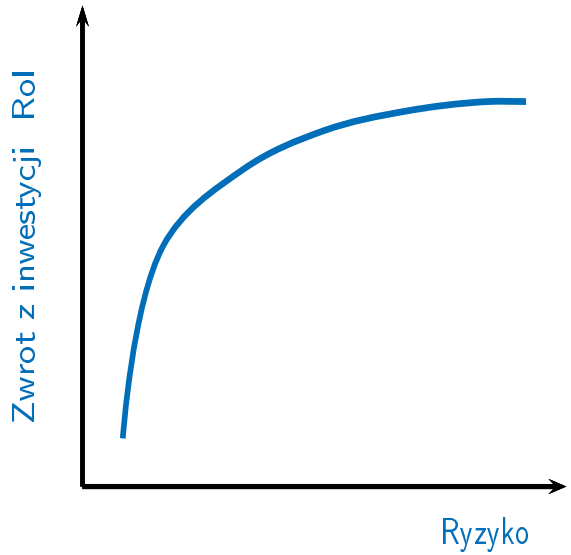
Ale np. **European Space Agency** definiuje ryzyko techniczne w odniesieniu do następujących aspektów:

- jakość i stabilność wymagań użytkownika;
- poziom zdefiniowania i stabilność interfejsów zewnętrznych;
- odpowiedniość i dostępność zasobów;
- dostępność i jakość narzędzi;
- doświadczenie i wyszkolenie zespołu;
- przypisanie odpowiedzialności;
- czas realizacji;
- innowacyjność projektu.

Kontekst ryzyka

- Ważnym kontekstem każdego projektu i ryzyka z nim związanego jest zwrot z inwestycji.
- Na osi pionowej odkładane są potencjalne zyski. Zyski w dużej mierze są uzależnione od podejmowanego ryzyka (np. nowe technologie) – działania nowatorskie umożliwiają uzyskanie przewagi nad konkurencją.
- Zadaniem kierownika projektu jest znalezienie właściwego punktu na krzywej, przy uwzględnieniu ryzyka i kosztów z tym związanych.
- Uwaga: wykresu na slajdzie nie należy traktować zbyt ściśle – jest to raczej informacja o tendencjach w procesach projektowych – wykres dla każdego projektu może być inny, uzależniony od jego specyfiki.

Kontekst ryzyka – interpretacja



Zwrot z inwestycji *RoI* (ang. **Return on Investment**) umożliwia pomiar finansowych korzyści wynikających z pewnej aktywności w stosunku do kosztów z nią związanych:

$$RoI = \frac{Zyski}{Zainwestowany\ \ kapital} \times 100\%$$

Charakterystyka ryzyka – podsumowanie

W ramach pełnego opisu ryzyka wskazane jest przedstawienie informacji o następujących elementach:

- **zakres** – opis przedsięwzięcia w kontekście którego definiowane jest ryzyko;
- **zagrożenie** – opis niepożądanej sytuacji;
- **skutki** – opis negatywnych konsekwencji materializacji zagrożenia;
- **czynniki ryzyka** – opis sytuacji wyjściowej względem której istnieje szansa wystąpienia ryzyka;
- **szansa wystąpienia** – oszacowanie szansy materializacji zagrożenia (w szczególności prawdopodobieństwo materializacji);

Charakterystyka ryzyka – podsumowanie (cd.)

- **umiejscowienie w czasie** – określenie przedziału czasowego wystąpienia zagrożenia;
- **powiązania** – określenie efektu jaki będzie miało wystąpienie danego zagrożenia na zagrożenie inne;
- **niepewność** – określenie stopnia pewności odnośnie informacji przedstawionych powyżej.

Opcje decyzyjne postępowania z ryzykiem

W stosunku do zidentyfikowanego ryzyka należy rozważać następujące strategie postępowania:

- **uniknięcie ryzyka** – wyeliminowanie możliwości materializacji zagrożenia (np. wybór drogi alternatywnej), klauzule wyłączające;
- **redukcja ryzyka** – zmniejszenie prawdopodobieństwa i/lub skutków zagrożenia;
- **kompensacja ryzyka** – jeden rodzaj ryzyka jest równoważony przez inny, a całość ulega redukcji;
- **transfer ryzyka** – przejęcie ryzyka przez innego uczestnika projektu lub inny podmiot (także firma ubezpieczeniowa);

Opcje decyzyjne postępowania z ryzykiem (cd.)

- **retencja ryzyka** – zatrzymanie ryzyka, np. decyzja o oczekiwaniu na wystąpienie innego zdarzenia;
- **podział ryzyka** – poszukiwanie wspólnika, segmentacja;
- **zaakceptowanie i racjonalizacja ryzyka** – przyjęcie ryzyka i zaplanowanie działań awaryjnych, a także śledzenie rozwoju sytuacji i ewentualne wdrożenie planu awaryjnego, aktywne zarządzanie.

Proces postępowania z ryzykiem

Dwie podstawowe fazy:

1. **analiza** (identyfikowanie, rozpoznanie i wymodelowanie ryzyka, interpretacja rezultatów);
2. **zarządzanie** (przeciwdziałanie, ograniczanie, eliminowanie).

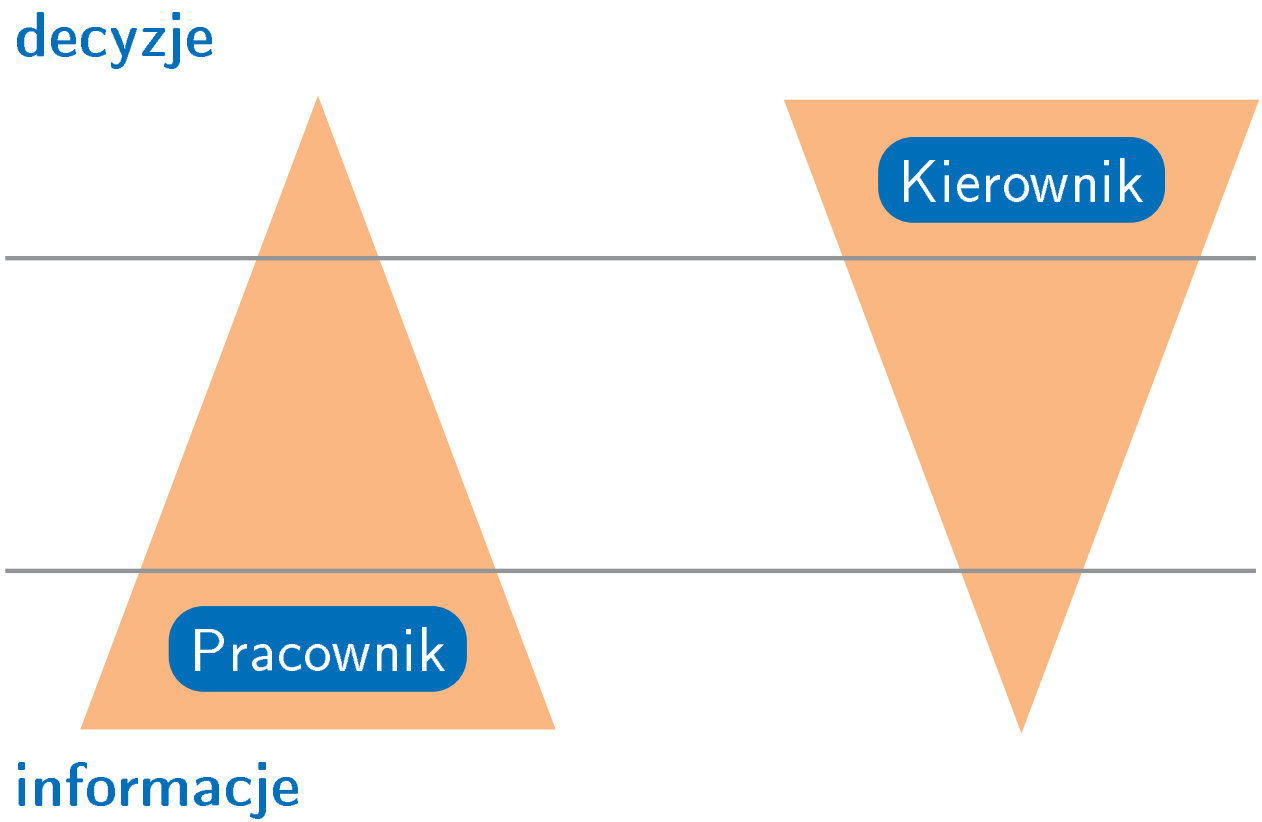
Analiza i zarządzanie ryzykiem są raczej domeną kierowników projektów, to jednak powinni w tym uczestniczyć także członkowie zespołu projektującego – stąd oczekiwanie właściwej wzajemnej komunikacji, łącznie z dobraniem adekwatnych ku temu środków i narzędzi.

Proces postępowania z ryzykiem (cd.)

Aczkolwiek analiza i zarządzanie ryzykiem są domeną raczej kierowników projektów, to jednak w obu tych procesach powinni uczestniczyć także, stosownie do swoich możliwości:

1. (wszyscy) członkowie zespołu projektującego i wykonawczego (np. tzw. burza mózgów);
2. grupy eksperckie (wewnętrzne lub zewnętrzne);
3. a nawet klienci i użytkownicy.

Asymetria informacji



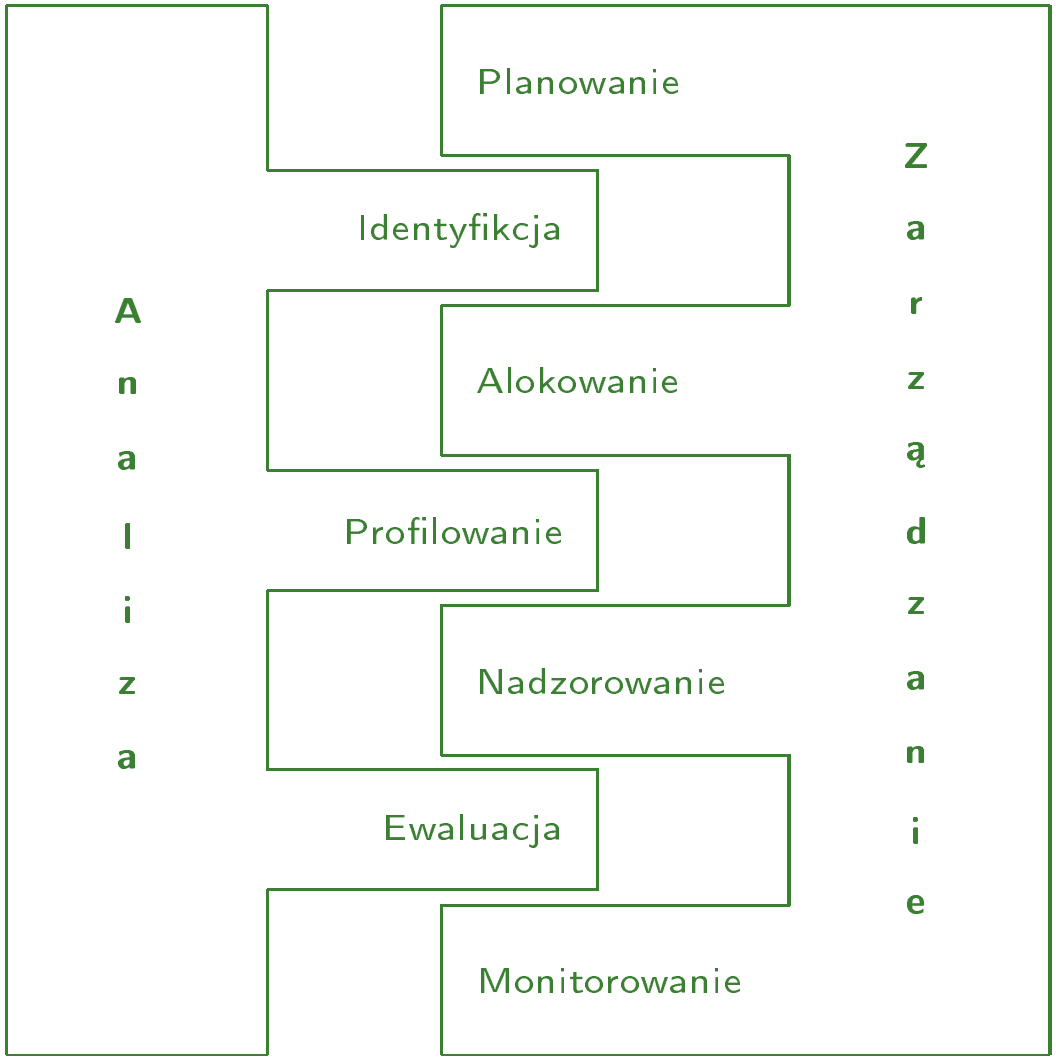
Asymetria informacji (cd.)

Możliwe skutki asymetrii infomacji:

1. formułowanie niepoprawnych wniosków;
2. niespójność działania;
3. zagrożenie interesu drugiej strony (uczestników);
4. przeoczenie pojawiających się informacji (niewykorzystanie informacji).

Oczywiście z faktu możliwej pewnej asymetrii informacji nie należy wyciągać wniosków, że taka sytuacja zawsze musi mieć miejsce, oraz że informacje „leżą” tylko i wyłącznie po stronie pracowników.

Analiza i zarządzanie ryzykiem (wg R. Charette'a)



Analiza i zarządzanie ryzykiem (wg R. Charette'a) – uwagi

- Ludzka aktywność, w odniesieniu do ryzyka występującego w procesie wytwarzania oprogramowania, można podzielić zasadniczo na dwie różne, wzajemnie jednak na siebie oddziaływujące fazy: **analizę** i **zarządzanie**.
- Niezależność obu faz, tworzących zamkniętą całość, choć poszczególne elementy (analiza, zarządzanie), oddziaływują na siebie wzajemnie.
- Iteracyjny proces uściślania obu faz.
- Całość stanowi układ komplementarny.

Proces analizy ryzyka

Przynajmniej trzy etapy:

1. **Identyfikacja** – czynność krytyczna w całej analizie i zarządzaniu ryzykiem, cel: wykrycie i zidentyfikowanie wszystkich rodzajów ryzyka, narzędzia: głównie specjalistyczne kwestionariusze ułatwiające rozpoznanie źródeł ryzyka, bardzo przydatne także doświadczenie analityków i projektantów;
2. **Profilowanie** – ocena każdego zidentyfikowanego ryzyka, wartościowanie/profilowanie: prawdopodobieństwo zdarzenia (z negatywnymi konsekwencjami), zależności/nezależności pomiędzy poszczególnymi rodzajami ryzyka, uwarunkowania czasowe, priorytety ryzyka;

Proces analizy ryzyka (cd.)

3. **Ewaluacja** – pytanie o akceptację/nieakceptację ryzyka (akceptacja – brak zmian w projekcie, nieakceptacja – określenie działań alternatywnych i obronnych), wyznaczenie progu akceptowalności ryzyka, narzędzia etapu: drzewa lub tablice decyzyjne.

Proces zarządzania ryzykiem

Cztery kolejne etapy:

1. **Planowanie** – planowanie postępowania, np. zmniejszanie prawdopodobieństwa ryzyka, albo też przyjmowanie ryzyka przy ograniczaniu jego negatywnych konsekwencji (lub połączenie obu podejść);
2. **Alokowanie** – przydzielenie dostępnych zasobów do tych miejsc projektu, które, np. ze względu na priorytety poszczególnych ryzyk, wymagają tego w pierwszej kolejności, charakterystczne jest tu balansowanie zasobami w stosunku do wcześniejszego planu (kryterium optymalizacyjne: czas, koszty, itp.);

Proces zarządzania ryzykiem (cd.)

3. **Nadzorowanie** – zgodność realizacji zarządzania z przyjętymi założeniami, odstępstwa implikują zmianami w zarządzaniu, a w szczególności mogą wymagać ponownej analizy ryzyka (identyfikacja);
4. **Monitorowanie** – śledzenie i gromadzenie informacji na temat efektywności stosowanych procedur, dokonywanie odpowiednich pomiarów (metryki), dane wykorzystywane zarówno w bieżącym zarządzaniu ryzykiem, jak i w przyszłej analizie, możliwość zidentyfikowania nowych źródeł ryzyka (jakby wprowadzenie do kolejnej analizy ryzyka).

Proces zarządzania ryzykiem – uwagi

- Planowanie – należy unikać sytuacji aby skutkami działań doprowadzić do pogorszenia sytuacji istniejącej (np. poprzez wprowadzenie nowego, trudniejszego przypadku ryzyka).
- Alokowanie – jest konsekwencją zaplanowanego postępowania z ryzykiem, może także obejmować punkty czasowe związane ze zwiększonym prawdopodobieństwem ryzyka.

Identyfikowanie ryzyka – strategie

Założenia odnośnie trzech kategorii występującego ryzyka:

1. ryzyko **znane** – jest tym czego w sposoób naturalny obawiają się wykonawcy projektu – wymaga właściwej klasyfikacji i opisania;
2. ryzyko **nieznane** – powinno być zidentyfikowane, tak aby móc skutecznie przeciwdziałać jego skutkom;
3. ryzyko **niepoznawalne** – jest poza zasięgiem metod identyfikacji i najczęściej określane jest w trakcie realizacji przedsięwzięcia jako tzw. okoliczności nieprzewidywalne.

Przyjmuje się także, że nawet ryzyko zaklasyfikowane jako znane jest jeszcze niedostatecznie opisane i uświadomione, co jest skutkiem niedostatków wzajemnej komunikacji uczestników projektu.

Identyfikowanie ryzyka – strategie (cd.)

Dwie podstawowe strategie identyfikowania ryzyka:

1. **analiza zstępująca** – np. przeglądanie list kontrolnych z wykazem potencjalnych zagrożeń i odnoszenie do sytuacji obecnej;
2. **analiza wstępująca** – ocena sytuacji obecnej i wskazanie jej możliwych skutków negatywnych.

Analiza zstępująca może prowadzić u niedoświadczonych analityków do nadmiernego rozrostu zagrożeń.

Analiza wstępująca może prowadzić do zbytniego skoncentrowania się na sytuacji bieżącej i możliwość przeoczeń.

Identyfikowanie ryzyka – metody

Możliwych jest wiele metod identyfikowania ryzyka, a jako przykładową warto wymienić tzw. burzę mózgów czy analizę subiektywną (intuicja, doświadczenie). Jednak podstawowe znaczenie mają metody oparte na tzw. **kwestionariuszach identyfikacyjnych**, zawierających listy kontrolne z wykazem potencjalnych zagrożeń do rozważenia.

Identyfikowanie ryzyka – metody (SEI CMU)

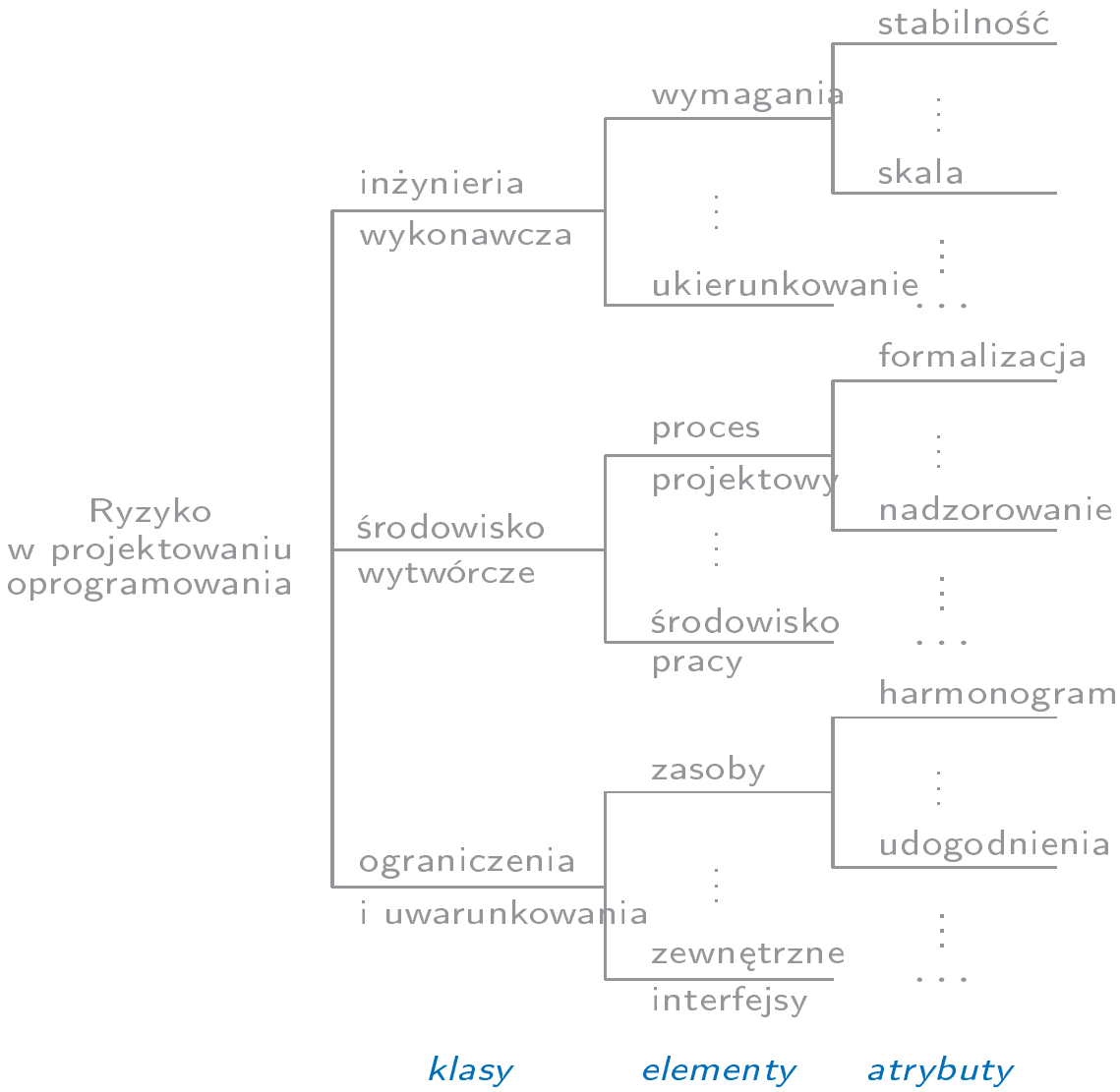
Postulaty odnośnie postępowania z identyfikowaniem ryzyka, uwzględnione w znanej metodzie zaproponowanej przez

Software Engineering Institute Carnegie Mellon Univeristy:

- strukturalizacja,
- powtarzalność,
- jednoznaczność,
- obiektywność.

M. J. Carr, S. L. Konda, I. Monarch, F. C. Ulrich, C. F. Walker. *Taxonomy-Based Risk Identification*. Technical Report CMU/SEI-93-RT-6. Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Pennsylvania, 1993.

Systematyka identyfikowania (wg. SEI CMU)



Systematyka identyfikowania (wg. SEI CMU) – uwagi

- Podział problemów tworzenia oprogramowania na **klasy**, **elementy** i **atrybuty**.
- Odnośnie klas mamy:
  1. **inżynieria wykonawcza** – techniczne aspekty wykonywanego przedsięwzięcia, np.: aktywność zarówno intelektualna jak i fizyczna realizatorów, dostępny sprzęt, oprogramowanie i dokumentacja.
  2. **środowisko wytwórcze**, tj. metody i narzędzia wykorzystywane w wytwarzaniu oprogramowania, oraz
  3. **ograniczenia i uwarunkowania**, tj. ograniczenia wynikające z uwarunkowań organizacyjnych, wykonawczych, kontrakt informatyczny – na ograniczenia te wykonawcy nie mają praktycznie żadnego wpływu.
- Na bazie powyższej systematyki, jako narzędzie identyfikacji, buduje się następnie tzw. **kwestionariusze identyfikacyjne**.

Kwestionariusz SEI CMU – przykład (1)

A. Inżynieria wykonawcza

1. Wymagania

a. Stabilność

[*Czy wymagania zmieniają się w trakcie wytwarzania oprogramowania?*]

[1] Czy wymagania są stabilne?

(nie) [1.a] Jak wpływa to na system?

- jakość
- funkcjonalność
- terminarz
- integrację
- projekt
- testowanie

[2] Czy interfejsy ulegają zmianie?

⋮

Kwestionariusz SEI CMU – przykład (2)

A. Inżynieria wykonawcza

1. Wymagania

⋮

f. Wykonalność

[*Czy istnieją wymagania nierealizowalne z analitycznego punktu widzenia?*]

[11] Czy jakieś wymagania są trudne do implementacji?

(tak) [11.a] Jakie są to wymagania?

(tak) [11.b] Dlaczego są one trudne do implementacji?

(nie) [11.c] Czy podjęto studia nad wykonalnością?

(tak) [11.c.1] Czy nie ma wątpliwości odnośnie przyjętych założeń?

⋮

Kwestionariusz SEI CMU – itd.

W całym formularzu są 194 podstawowe pytania.

Kwestionariusz SEI CMU – itd.

W całym formularzu są 194 podstawowe pytania.

Plik: **i24-ryzyko-ext-Taxonomy-BasedRiskIdentyfication**

Zmiana prawdopodobieństwa ryzyka

Należy zawsze upewnić się czy zmiany opisu danego zagrożenia są przez nas dobrze rozumiane (i udokumentowane). Przykładowo zmiany samego prawdopodobieństwa ryzyka powinny spowodować rozważenie pytań:

- czy rzeczywiście sytuacja związana z ryzykiem uległa zmianie, czy też po prostu lepiej ją teraz rozumiemy?
- jeśli coś się zmieniło, jakie atrybuty ryzyka uległy zmianie?
- czy stało się tak na skutek działań celowych, czy też z innych powodów?
- jaka będzie tendencja tych zmian w dłuższym okresie czasu?

Definiowanie ryzyka

Definiowanie ryzyka może się odbywać poprzez więcej niż jedną zmienną, np. poprzez kategorie przedstawiające konsekwencje (wpływ) ryzyka:

- katastrofalne
- poważne
- znaczące
- marginalne
- nieistotne

oraz stopnie prawdopodobieństwa zdarzenia:

- bardzo prawdopodobne
- prawdopodobne
- dość prawdopodobne
- mało prawdopodobne
- bardzo mało prawdopodobne
- niezwykle mało prawdopodobne

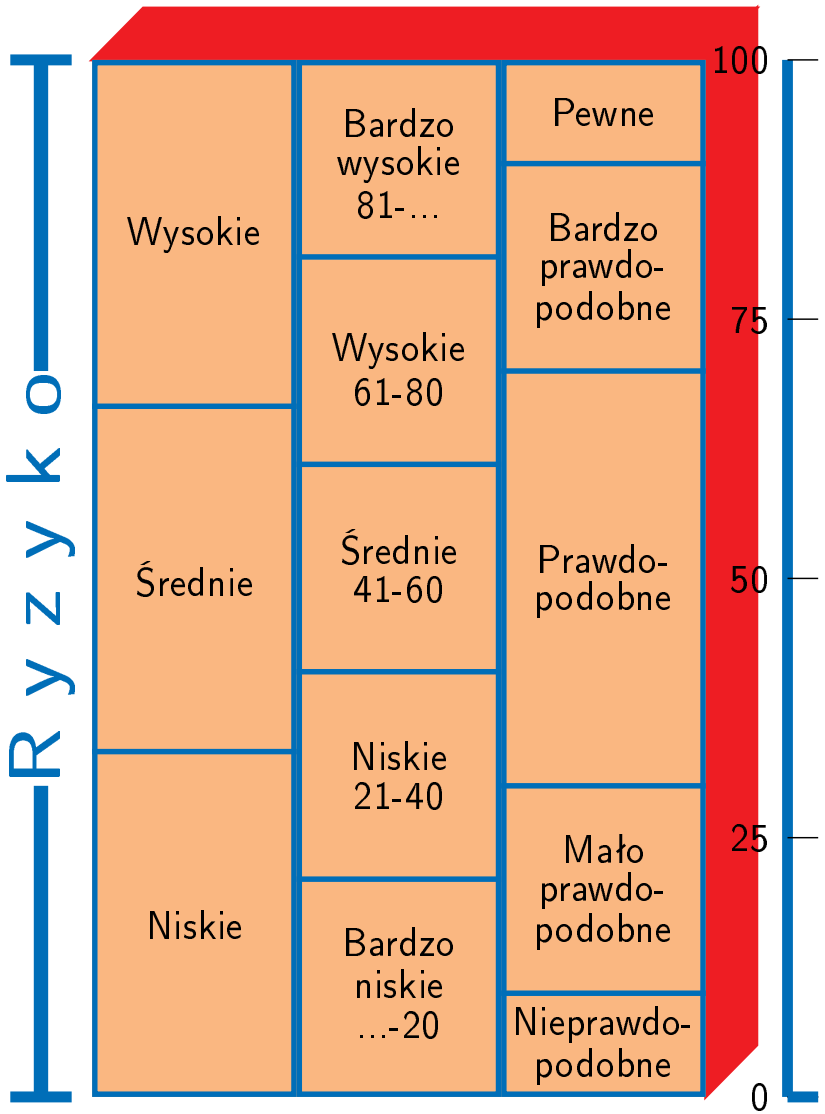
Wg. **RAMP – Risk Analysis and Management of Projects**. Institute of Civil Engineers oraz Institute of Actuaries (W. Brytania) 1998.

Definiowanie ryzyka (cd.)

Pozwala to na wypracowanie odpowiednich działań wobec wpływu analizowanego ryzyka:

Wpływ ryzyka	Wskazane działanie wobec ryzyka
Nie do przyjęcia	Eliminowanie lub przeniesienie
Niepożądany	Próba uniknięcia lub przeniesienia
Do przyjęcia	Utrzymać na tym poziomie i próbować nim kierować
Nieistotny	Pominąć

Miary oceny ryzyka



Macierz ryzyka – ryzyko ogólne

Prawdopodobieństwo ryzyka	Starty: wysokie	Starty: średnie	Starty: niskie
b. wysokie	b. wysokie	wysokie	średnie
wysokie	wysokie	wysokie	średnie
średnie	wysokie	średnie	średnie
niskie	średnie	średnie	niskie
b. niskie	średnie	średnie	niskie

Macierz ryzyka – ryzyko ogólne – uwagi

- Znajomość prawdopodobieństwa wystąpienia zdarzenia negatywnego oraz znajomość strat jakie mogą pojawić się w systemie stanowi także punkt wyjścia do oceny ogólnego ryzyka powodzenia całego projektu.
- Pokazana macierz pozwala także wyznaczyć hierarchię ważności poszczególnych rodzajów ryzyka, istotnych przy ustalaniu strategii postępowania z ryzykami zidentyfikowanymi w systemie (projekcie).
- Zarówno w tej macierzy, jak i następnej, można przyjmować inne miary poziomu ryzyka.

Macierz ryzyka – poziom strat

Poniżej pokazano macierz – wg. **US Air Force System Command** – wyznaczania poziomu strat na podstawie wpływu pewnego czynnika i prawdopodobieństwa jego wystąpienia.

	Prawdopodobieństwo				
Wpływ	bardzo wysokie	wysokie	średnie	niskie	bardzo niskie
katastroficzny	wysokie	wysokie	średnie	średnie	niskie
krytyczny	wysokie	wysokie	średnie	niskie	żadne
marginalny	średnie	średnie	niskie	żadne	żadne
zaniedbywalny	średnie	niskie	niskie	żadne	żadne

Zakres zapobiegania ryzyku

Działania zapobiegawcze w stosunku do ryzyka polegają – zasadniczo – na dwóch kierunkach działań:

1. zmniejszeniu prawdopodobieństwa wystąpienia ryzyka;
2. minimalizacji strat związanych z negatywnym zdarzeniem.

Zakres zapobiegania ryzyku

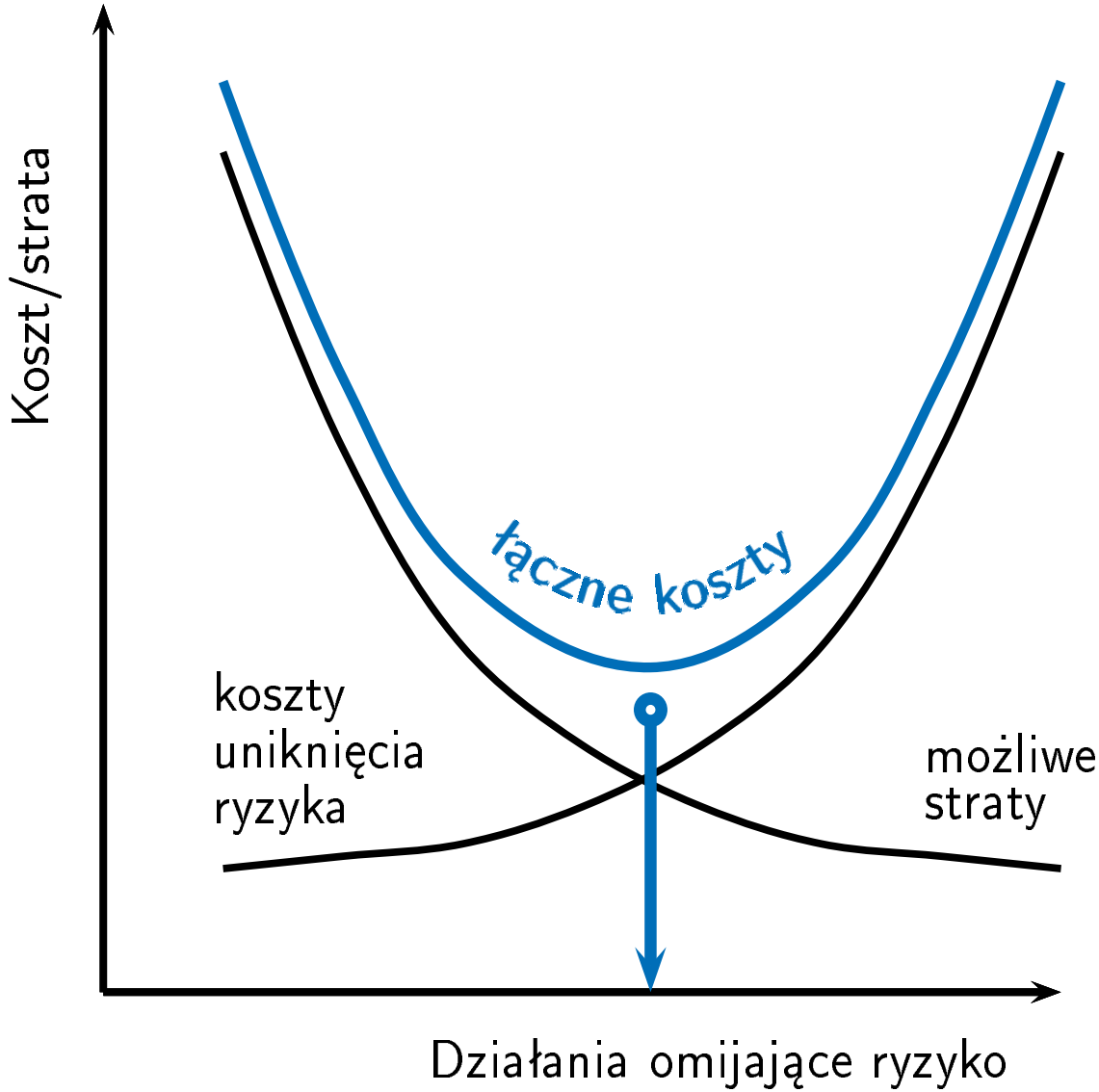
Działania zapobiegawcze w stosunku do ryzyka polegają – zasadniczo – na dwóch kierunkach działań:

1. zmniejszeniu prawdopodobieństwa wystąpienia ryzyka;
2. minimalizacji strat związanych z negatywnym zdarzeniem.

Działania zapobiegawcze powinny ograniczać potencjalne straty. Jednakże ponoszenie zbyt wysokich kosztów minimalizowania strat może być ekonomicznie nieuzasadnione – od pewnego momentu koszty minimalizacji mogą przewyższać wartość samych strat.

Optymalnym rozwiązaniem jest wyznaczenie momentu/miejsca (poprzez koszty łączne) do którego warto podejmować działania minimalizacyjne – ogólnie jest to typowe działanie zarządcze.

Zakres zapobiegania ryzyku – interpretacja



Model kosztowy – ekspozycja ryzyka

Szacowanie poziomu ryzyka może uwzględniać tzw. model kosztowy poprzez uwzględnienie wielkości ewentualnych strat. Wyniki mogą być przydatne przy ustalaniu hierarchii ważności zagrożeń. I tak, **ekspozycja ryzyka** RE:

$$RE = P(z) \cdot L(z)$$

gdzie:

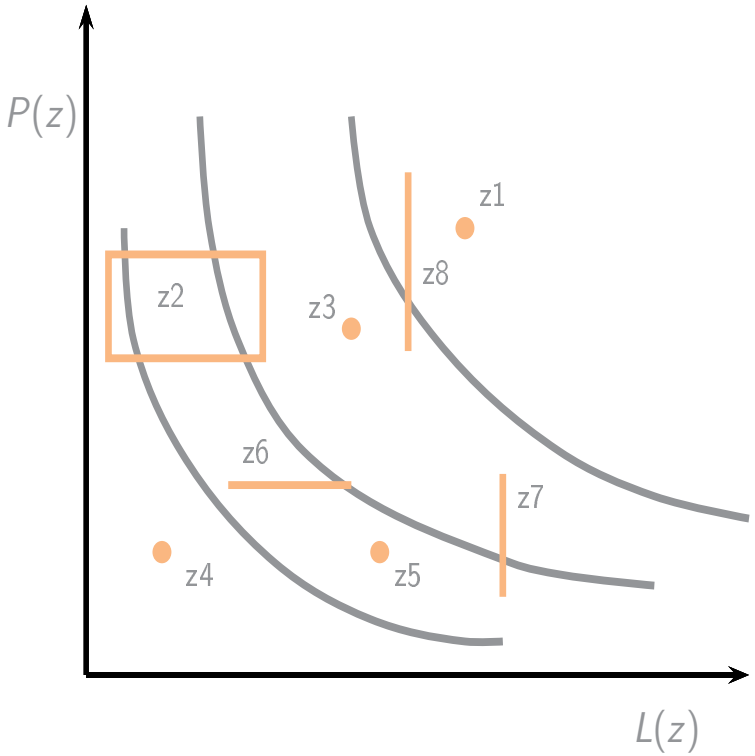
z – niepożądana sytuacja/zdarzenie (ozn. także UO);
P – prawdopodobieństwo niepożądanej sytuacji;
L – koszty jako skutek zaistnienia sytuacji niepożądanej.

Model kosztowy – ekspozycja ryzyka (cd.)

Pozostaje jednak problem szacowania ryzyka łącznego dla projektu, co można czynić poprzez np.:

- analizę sieciową;
- drzewa zdarzeń;
- metody eksperckie;
- inne metody.

Ekspozycja ryzyka – reprezentacja graficzna



Niektóre wielkości, zarówno prawdopodobieństwo, jak i koszty mogą być szacowane zarówno punktowo, jak i przedziałowo.

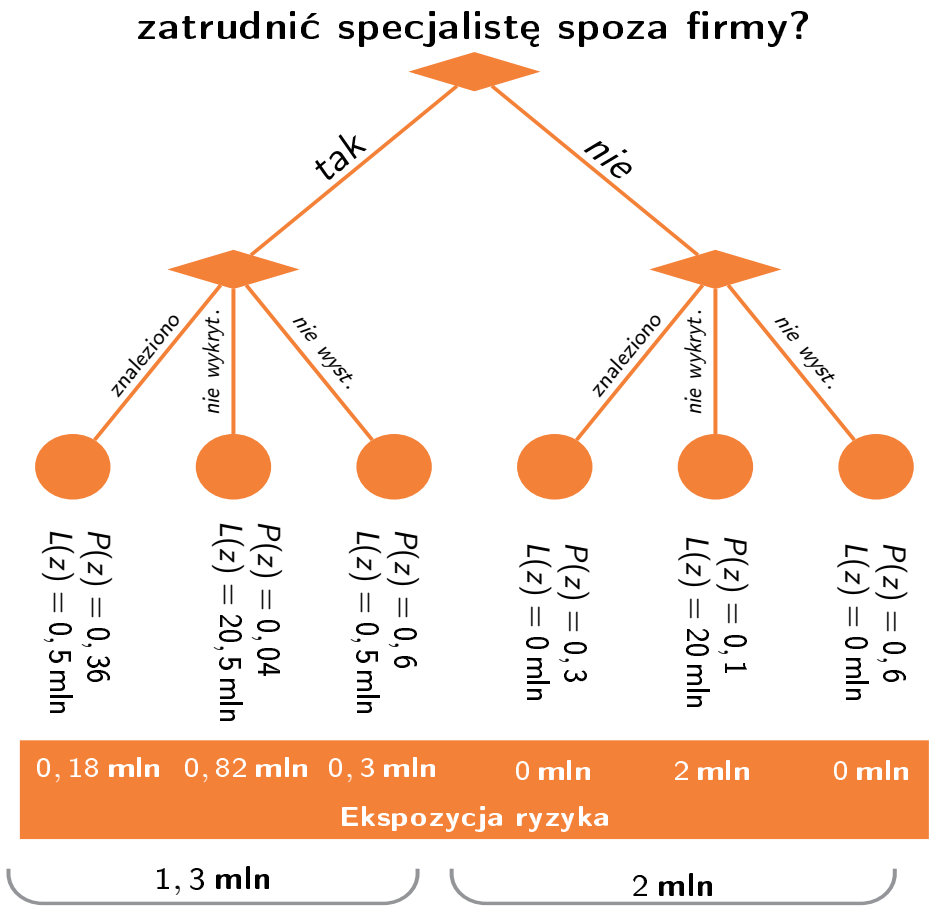
Szacowanie przedziałowe może odbywać się przedziałowo na jednej lub drugiej skali, albo na obu jednocześnie.

Ekspozycja ryzyka – reprezentacja graficzna – uwagi

- Reprezentacja graficzna lepiej pozwala zanalizować ryzyko, pozwalając uniknąć skupienia się tylko na jednym rodzaju ryzyka.
- Krzywe reprezentują pewną stałą wartość ryzyka.
- Szacowanie przedziałowe ma zaletę, że może lepiej może oddawać rzeczywistość.
- Zagrożenia $z1$ oraz $z8$ należą do grupy najpoważniejszych, z tym, że $z8$ jest oszacowane z pewną niepewnością.

Analiza ryzyka – drzewo decyzyjne

Dość popularny przykład odnośnie drzew decyzyjnych i ryzyka: zagrożenie wynikające z możliwości wystąpienia błędu krytycznego w oprogramowaniu.



Poziom redukcji ryzyka

Działania i efekty zmierzające do ograniczenia ryzyka mogą być ukazane poprzez obliczenie tzw. **poziomu redukcji ryzyka** (**dźwignia**) *RRL*:

$$RRL = \frac{(RE_b - RE_a)}{RRC} = \frac{L(z) \cdot (P_b(z) - P_a(z))}{RRC}$$

gdzie:

RE_b – ekspozycja ryzyka „przed”;
RE_a – ekspozycja ryzyka „po”;
P_b – prawdopodobieństwo „przed”;
P_a – prawdopodobieństwo „po”;
RRC – koszty redukcji ryzyka.

Odmienne podejścia odnośnie problemu ryzyka

Znanych jest kilka taksonomii w odniesieniu do problemu analizy i zarządzania ryzykiem w projekcie informatycznym:

R. Charette	dwufazowa analiza-zarządzanie ryzykiem;
B. W. Boehm	hierarchiczna systematyka zarządzania ryzykiem;
R. Fairley	siedmiopunktowa analiza i zarządzanie ryzykiem.

Odmienne podejścia odnośnie problemu ryzyka

Znanych jest kilka taksonomii w odniesieniu do problemu analizy i zarządzania ryzykiem w projekcie informatycznym:

R. Charette	dwufazowa analiza-zarządzanie ryzykiem;
B. W. Boehm	hierarchiczna systematyka zarządzania ryzykiem;
R. Fairley	siedmiopunktowa analiza i zarządzanie ryzykiem.

- **R. Charette** – dwie fazy, faza „statyczna" oraz faza „dynamiczna". Podział bardzo klarowny.
- **B. W. Boehma** – klasyczna, hierarchiczna taksonomia, mianem zarządzania określa się tu całość postępowania z ryzykiem. Dzieli się ono na dwie części, a mianowicie na szacowanie oraz nadzorowanie. Brak progów (jak u Charette'a).
- **R. Fairley** – siedmiopunktowa metoda analizy i zarządzania ryzykiem. Nakierowanie na sytuacje kryzysowe, jako efektu zmaterializowania się ryzyka.

Opanowanie kryzysu

Elementy zarządzania kryzysem:

- ogłoszenie kryzysu oraz przedstawienie i nagłośnienie problemu;
- przypisanie odpowiedzialności i uprawnień do działań kryzysowych (np. zwolnienie z innych obowiązków);
- wzmożenie kontroli stanu (w razie konieczności nawet kilka razy dziennie);
- zagwarantowanie zasobów i rozluźnienie ograniczeń dotyczących zużycia zasobów przez grupę kryzysową;
- ustanowienie trybu pracy specjalnej dla grupy kryzysowej (godziny ponadwymiarowe, nocleg w firmie), wsparcie logistyczne;

Opanowanie kryzysu (cd.)

- ustanowienie granic strefy kryzysowej (np. czy pozostały personel pracuje normalnie);
- ustanowienie nieprzekraczalnego terminu po którym sprawa jest przejmowana przez wyższe szczeble zarządzania.

Wznowienie po kryzysie

Po opanowaniu kryzysu niezbędne są działania podsumowujące:

- analiza przyczyn kryzysu i udokumentowanie wszystkich wniosków wynikających z kryzysu;
- obliczenie kosztów dodatkowych (obiektywne straty) spowodowanych kryzysem i koniecznością jego przezwyciężenia;
- obliczenie kosztu i czasu koniecznego na dokończenie projektu;
- uaktualnienie planów i harmonogramów oraz nowe alokacje zadań;
- „ukaranie winnych” oraz „nagrodzenie bohaterów”.

Ryzyko – „mądrości ludowe”

Jeśli nie zajmiesz aktywnej postawy względem problemu ryzyka, to ryzyko „zajmie” aktywną postawę względem twojego projektu.

Należy dzielić się swoją wiedzą na temat ryzyka, w szczególności należy dzielić się nią z decydentami.

Zapobieganie ryzyku jest w odniesieniu do kosztów bardziej efektywne niż samo jego wykrywanie.

Jeśli nie szukasz informacji na temat ryzyka, to szukasz kłopotów.