

RIZIKÁ MANAŽMENTU RIZÍK

Optimista je len neinformovaný pesimista.

Jakub Ukrop

Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava
jukrop[zavináč]gmail[.]com

Abstrakt. *Napriek veľkému počtu podporných nástrojov v sebe vývoj softvéru stále zahŕňa riziká, ktorých zvládnutie je nevyhnutné pre úspešné dokončenie projektu. Oblasť riadenia rizík dnes disponuje množstvom rozdielnych postupov na ich identifikáciu a riešenie. V tejto eseji stručne zhrnieme spôsoby delenia rizík a relatívne dôležitosti jednotlivých typov v procese vzniku softvéru. Zameriame sa na holistický pohľad, ktorý neposudzuje jednotlivé kategórie rizík nezávisle, ale zaoberá sa aj ich vzájomnými podobnosťami a vzťahmi. Ďalej sa budeme venovať najčastejším problémom, ktoré sa v súvislosti s riadením rizík vyskytujú, hlavne v spojení s ľudským faktorom.*

Kľúčové slová: *manažment rizík, riziká vývoja softvéru, averzia k riziku*

Úvod

Riziká hrozia projektom každého druhu, výnimkou nie sú ani tie softvérové. Prieskum v IT sektore z roku 2002 ukázal, že len 29% všetkých projektov, bez ohľadu na rozsah a veľkosť, bolo úspešne dokončených, 53% sa stretlo s problémami a 18% bolo zrušených [7]. Medzi najčastejšie ťažkosti patrí tradične dodržanie funkčnej, časovej a finančnej stránky projektu, čo v praxi znamená vytvorenie produktu v súlade s požiadavkami zákazníka, v dohodnutom termíne a bez prekročenia zdrojov na to určených. Práve systematické riadenie rizík pomáha potenciálne nebezpečenstvá úspešne riešiť alebo im predchádzať.

Existuje viac spôsobov ako definovať pojem rizika. Zhodujú sa v tom, že riziko je za každých okolností spojené s neistotou a stratou [6]. Preto platí, že ak dopredu vieme s istotou predpovedať budúce problémy, nejedná sa o riziko. Ak nastane riziková situácia, dochádza spravidla k určitým nechceným následkom, ktoré projekt viac či menej ohrozia.

To ale neznamená, že risk sám o sebe je zlý. Zlé sú iba hlúpe riziká, ktorým sa dalo jednoducho (a lacno) vyhnúť.

Metodológia manažmentu rizík poskytuje ucelený súbor techník na identifikáciu, analýzu a monitorovanie rizík, ako aj prostriedky zmierňovania ich negatívnych následkov. V prvom kroku sa pomocou doterajších znalostí, tvorby scenárov, brainstormingu a iných techník pokúšame identifikovať všetky riziká pre daný projekt. Analýza objavených rizík spočíva hlavne v ich ohodnotení, ktoré vychádza z pravdepodobnosti, že k nim dôjde a z veľkosti hrozacej straty. Z výsledkov analýzy sa vypracuje plán potenciálnych reakcií na hlavné riziká. Ako projekt postupuje, je nutné riziká pravidelne monitorovať a upravovať pripravené plány podľa meniacich sa priorit.

Úspešné zvládnutie tohto procesu umožní vyhnúť sa niektorým rizikám a zmierniť následky ostatných na prípustnú úroveň.

(Ne)delenie rizík

Existuje viac spôsobov delenia rizík. Z pohľadu kvality produktu rozlišujeme riziko nákladov (cena), riziko rozvrhu (čas) a riziko použiteľnosti výrobku (splnenie požiadaviek). Je známe, že veľká väčšina projektov je odovzdaná neskoro, a ak nie, tak len vďaka zredukovaní plánovanej funkcionality.

Zmysel má aj rozdelenie založené na životnom cykle softvéru, keďže závažnosť rizika vyplýva aj z etapy, v ktorej sa vyskytne. Plán riešenia náhle zmeny požiadaviek zákazníka je iný vo fáze špecifikácie, kde sa zmeny integrujú, ako vo fáze testovania, kde radšej presvedčíme zákazníka, aby si to rozmyslel.

Dôležité kategórie rizík odvodíme aj z „večného“ projektového trojuholníka: ľudia, procesy, technológie. Ide o interné riziká, ktorým venujú manažéri zvyčajne najväčšiu pozornosť, lebo ich na rozdiel od externých môžu priamo ovplyvňovať.

V tejto eseji sa ďalej zameriame na rozčlenenie rizík podľa faktorov, ktoré ich spôsobujú, na 4 skupiny: technické, obmedzenia zdrojov, organizačné a iné [7].

Technické riziká

Technické riziká vyplývajú najmä z chýb a nedostatkov hardvéru a softvéru a boli ako dôležité identifikované už dávno. Spájajú sa so zastaranými technológiami rovnako ako aj s prechodom na nové technológie. Ohrozené sú nimi hlavne prenosnosť, rozširiteľnosť, udržiavateľnosť, interoperabilita a ďalšie vlastnosti softvéru. Možno im predchádzať pravidelnými školeniami pracovníkov a dobrou informovanosťou všetkých členov tímu. Práca s dôverne známymi vývojovými nástrojmi tiež znižuje šance vzniku nečakaných rizík. Väčšinou sú to interné riziká, ale môžu byť aj externé (krach dodávateľa hardvéru, útok vírusu).

Riziká spojené s obmedzeniami zdrojov

Jedná sa predovšetkým o správne rozdeľovanie troch kritických zdrojov – ľudí, peňazí a času – počas priebehu projektu. Presné analýzy nákladov a prínosov pomôžu znížiť pravdepodobnosti takýchto rizík. Existujú aj externé vplyvy, ale z podstaty ide o vnútorné záležitosti firmy.

Organizačné riziká

Organizačné riziká sú dnes považované na najdôležitejšie. Nedávny výskum ukázal, že dôvodom zlyhania väčšiny projektov nebol nedostatok peňazí ani technológií, ale nedostatok kvalifikovaných manažérov a výkonných pracovníkov [7]. Patria sem napríklad otázky dôvery a komunikácie, rozhodovania, plánovania a spolupráce so zákazníkom. Majú svoj pôvod v organizačnej kultúre, štruktúre a biznis procesoch. Napriek rozsahu tejto skupiny rizík sú v praxi často zanedbávané alebo riešené nevhodne.

Iné riziká

V tejto kategórii sa nachádzajú riziká spôsobené legálnymi, etickými, environmentálnymi, politickými a kultúrnymi faktormi, teda vo všeobecnosti externé riziká.

Všetko pod jednou strechou

Rozdiely medzi uvedenými kategóriami sú na prvý pohľad zrejmé, no musíme si uvedomiť, že zaradenie rizika závisí do veľkej miery aj od kontextu. To, čo sa na prvý pohľad javí ako jedno riziko, býva kombináciou viacerých. Napríklad, ak sa ukáže, že tím nemá dostatočné skúsenosti v problémovej oblasti, môže to byť spôsobené nedostatkom vhodných technológií (technické riziko), nedostatkom prostriedkov na prijatie kvalifikovanejších ľudí (obmedzenia zdrojov) alebo nevhodným priradením projektu (organizačné riziko). Samotný nedostatok potrebných technológií (technické) potom môže súvisieť s chýbajúcimi financiami (obmedzenie zdrojov) zavinenými v konečnom dôsledku zlým plánovaním a rozdelením zdrojov (organizačné).

Pre úspešný manažment rizík je potrebný všetko zahŕňajúci, holistický pohľad na organizačné riziká. Skúsení profesionáli považujú všetky interné riziká za spojené s organizačnými faktormi [7], čo poukazuje na dôležitosť kvalitného manažmentu (nielen rizík) a vyspelej podnikovej kultúry.

Ľudský faktor

Pri hodnotení rizika si musíme uvedomiť, že nie je riziko absolútne. Nie je možné jednoducho nazrieť do tabuliek a priradiť rizikám čísla podľa ich závažnosti. Pri dosahovaní cieľov manažmentu rizík hrá preto nevyhnutne dôležitú úlohu človek a jeho subjektívny pohľad.

Vnímanie rizika

Väčšina ľudí vníma riziká intuitívne a rôznymi spôsobmi. Pri identifikácii rizík človek vo všeobecnosti uprednostňuje riziká, ktoré pozná alebo sa ho osobne týkajú. Príliš veľa pozornosti je venovanej hľadaniu skrytých, neznámych rizík, ktoré sú menej pravdepodobné. Bežné riziká sú na druhej strane podceňované. Veľmi nebezpečná je aj prehnaná dôvera v zabehané vnútorné a spoľahlivé vonkajšie systémy [3]. Práve tam, kde nevidíme žiadne riziko, vzniká slabé miesto a môže dôjsť napríklad k porušeniu bezpečnosti. Ak sa pri vyhodnocovaní rizík neoprieme o systematickú analýzu, je

pravdepodobné, že miníme príliš mnoho času a peňazí na znižovanie nedôležitého rizika a naopak.

Pre vnímanie rizika musíme brať do úvahy aj faktory ako stupeň zodpovednosti, ciele, čas, schopnosti, vedomosti a podobne. Perspektíva jednotlivca a tímu sa líši od pohľadu manažmentu a investorov, aj keď sa zdroje rizika pre tieto štyri skupiny prekrývajú a navzájom na seba vplývajú. Na prácu jednotlivca a tímu vplývajú hlavne [3]:

- osobné schopnosti práce s vývojovými metódami a nástrojmi
- skúsenosti vedúceho tímu a jeho schopnosť viesť
- výkon tímu
- dostupnosť školeného personálu
- oddanosť projektu
- lojalita personálu voči organizácii
- zručnosť pri identifikácii a analýze príčin rizík, atď.

Manažment a investori majú na riziká iný pohľad. Zisk, dodržanie plánov a kvalita sú jedny z cieľov manažmentu. Používateľom a zákazníkom záleží napríklad na návratnosti investície, bezpečnosti a použiteľnosti produktu. Rizikové faktory pre túto skupinu sú najmä [3]:

- schopnosti manažérov
- prijímanie vhodných zamestnancov
- spolupráca s externými organizáciami
- zmluvy s poskytovateľmi služieb
- zdroje na školenia
- podpora nasadzovania vylepšených metodológií
- pravidelný prieskum bezpečnostných postupov
- pravidelné monitorovanie a identifikácia rizík, atď.

V procese manažmentu rizík je dôležité venovať sa explicitne pohľadom všetkých zainteresovaných strán.

Averzia k riziku

Priznanie si rizika býva v súčasnej spoločnosti často spájané s nedostatkom sebadôvery. Horlivý manažér postavený pred nesplniteľné požiadavky môže jednať kontraproduktívne. Nestane sa to pri malých rizikách, ale paradoxne práve v situáciách, ktoré sú mimo možností zmierenia následkov rizík na prípustnú úroveň. Ukáže sa napríklad, že termín odovzdania produktu nie je možné stihnúť. Vedúci pracovník postavený pred takýto problém sa rozhodne riziko zámerne ignorovať alebo rýchlo doplní projekt o ďalších ľudí, čo nakoniec iba predĺži dobu potrebnú na dokončenie a zvýši stratu spôsobenú rizikom. Riziká nie sú výzvy.

Ešte horšie je, keď je firemná kultúra poznačená silnou averziou k riziku. Prejaví sa to zameriavaním sa na riešenie kríz a potláčaním analýzy problémov. Hrdinovia riešiaci situáciu, ktorej by sa dalo predísť, sú oceňovaní, poslovia zlých správ trestaní [1]. Ak majú riadiaci pracovníci antipatiu k riziku, podriadení určite nebudú mať veľkú chuť upozorňovať na potenciálne problémy, ktoré potom ostávajú neriešené. Obvykle potom

platí, že čím vyššie postupujeme v hierarchii organizácie, tým menej pozornosti sa rizikám venuje.

Manažment rizík nie je to isté ako vyhýbanie sa im. Nie je to to isté ako riadenie kríz ani riešenie problémov. Práve z takýchto mylných predstáv vyplýva pocit zbytočnosti a spomínaný negatívny postoj. Hľadanie rizík sa musí podporovať (napríklad poukázaním na fakt, že každé objavené riziko je pridanou hodnotou pre klienta [6]), rovnako ako učenie sa z minulých chýb.

Tajomstvo

Mnohé organizácie úspešne aplikujú metodológie manažmentu rizík, ale nechávajú si to pre seba, takže celkové povedomie je nízke a chýba motivácia pre ďalších manažérov. Hovoriť o tom totiž prináša isté nevýhody. „Ak softvérový produkt zlyhá, existencia formálneho plánu, ktorý takéto zlyhanie pripúšťa, by mohla skomplikovať či dokonca skompromitovať legálnu pozíciu výrobcu“ [1]. Tento neodškriepiteľný fakt ešte spomaľuje zavádzanie riadenia rizík v softvérových projektoch.

Reakcia a prevencia

Ako sme spomenuli v úvode, väčšina softvérových projektov nesplní buď termín dodania alebo nedosahuje požadovanú kvalitu. Bez manažmentu rizík sa ich plány zaoberajú iba činnosťou spojenou priamo s vývojom produktu a nemajú alokované záložné zdroje na vyrovnanie sa z rizikami, ktoré sa môžu alebo nemusia prejaviť ako skutočné problémy [4]. Žiadny projekt ale nikdy nejde presne podľa plánu.

Manažment rizík sa často stáva jednorazovou aktivitou vykonávanou vtedy, keď má projekt príliš veľa ťažkostí a je jasné, že niečo sa robiť musí. V takom prípade sa dá hovoriť skôr o riešení problémov než o skutočnej analýze rizík.

Ani systematická a detailná analýza na začiatku vývoja však nezabezpečuje ideálny priebeh prác. Mnoho firiem používa tzv. preskriptívne (reaktívne) metódy. Akcie na zmiernenie rizika sa nasadia až po tom, ako nastali problémy. Manažment sa o nich dozvie, až keď tím minie dôležitý míľnik alebo zákazníci hlásia chyby softvéru, a aplikuje drastickú liečbu (výmena vedúceho, skreslenie projektu, najatie drahých externistov), ktorá môže byť taká nákladná, že projekt zahubí [5].

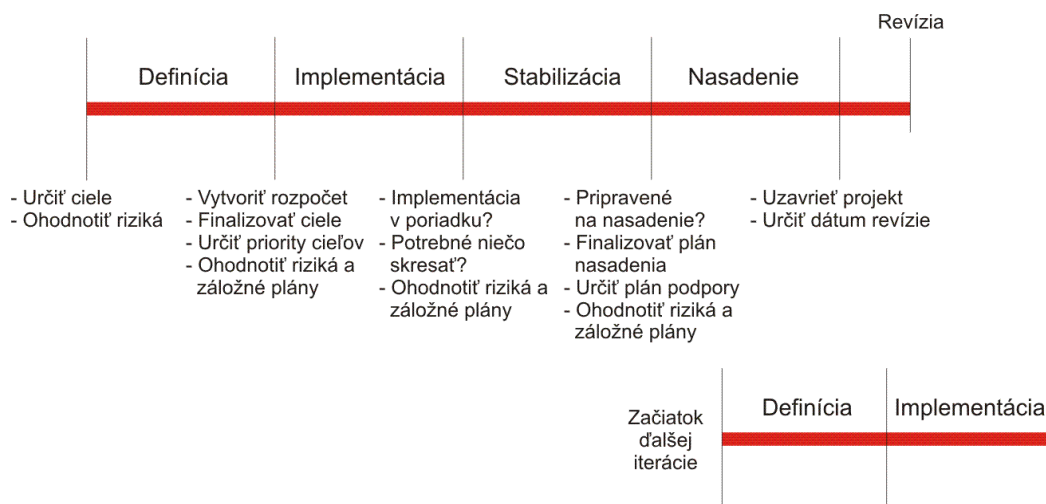
Lepšou alternatívou sú preventívne (proaktívne) metódy. Ak sa riziká priebežne monitorujú, je možné podniknúť kroky k náprave ešte predtým, ako reálne dôjde k ťažkostiam. Flexibilitu podporuje aj použitie agilných metód, modularizácia a rozdelenie na podprojekty. Pri vývoji veľkých systémov sa môže manažment rizík stať príliš komplikovaným nato, aby bol efektívny a použiteľný. Obr.1. zobrazuje schému iteratívneho modelu, v ktorom sa berie ohľad aj na riadenie rizík.

Ďalšie ťažkosti

Každý projekt je v niečom jedinečný a práve veci, ktoré ho odlišujú od iných, sú pre plánovanie rizík dôležité. Unikátna množina okolností, špecifické riešenia. Manažment rizík sa vždy zameriava na konkrétne nie na všeobecné, a preto nie je kompletne

štandardizovateľný [4]. Žiadne univerzálne riešenie, ktoré nevychádza priamo z vlastností daného projektu, nemôže byť dostatočné.

Manažment rizík je nákladný, časovo náročný a mal by byť nasadzovaný už v prvých fázach softvérového vývoja. Aj preto najmä menšie firmy váhajú s jeho nasadením. Častým argumentom je aj tvrdenie, že riziká sú zohľadnené aj v manažmente projektu, a teda nie je dôvod na jeho zavedenie [6]. Ako už bolo povedané, riziká nie sú to isté, čo problémy a vyžadujú si svoj vlastný prístup.



Obr.1. Štyri etapy jednej iterácie softvérového projektu [5].

Zhodnotenie

Riziká v softvérových projektoch si zasluhujú pozornosť všetkých, ktorí sa týchto projektov zúčastňujú. Nie je až také prekvapivé, že takmer každé členenie v softvérovom inžinierstve dokážeme aplikovať aj na manažment rizík - riziká existujú pri činnostiach spojenej prakticky s akoukoľvek časťou softvérového projektu (a tiež pri každej ľudskej činnosti v akejkoľvek inej oblasti).

Manažment rizík je spojený s množstvom chybných predstáv a vo veľkej miere býva aplikovaný len intuitívne. Napriek tomu ide o významnú súčasť projektu, ktorá by nemala byť zanedbávaná. Kľúčová je vyspelá podniková kultúra, ktorá nepodporuje averziu k riziku a dobre zvláda organizačné záležitosti. Rovnako je dôležitá systematická prevencia rizík, ktorá vyžaduje zapojenie všetkých zainteresovaných, od vývojárov po používateľov.

Takže ako povedal Tim Lister: „Veľa šťastia pri vašom projekte – len ho neočakávajte“ [4].

Použitá literatúra

1. Boehm, B.W., DeMarco, T.: Software Risk Management. *IEEE Software*, Vol. 14, No. 3 (1997), 17-19.
2. Carr, M.J.: Counterpoint: Risk Management May Not Be for Everyone. *IEEE Software*, Vol. 14, No. 3 (1997), 21,24.
3. Islam, S., Dong, W.: Human factors in software security risk management. In: *Proc. of the First international Workshop on Leadership and Management in Software Architecture*, ACM, New York (2008), 13-16.
4. Lister, T.: Point: Risk Management Is Project Management for Adults. *IEEE Software*, Vol. 14, No. 3 (1997), 20,22.
5. Murthi, S.: Preventive Risk Management for Software Projects. *IT Professional*, Vol. 4, No. 5 (2002), 9-15.
6. Padayachee, K.: An interpretive study of software risk management perspectives. In: *Proceedings of the 2002 Annual Research Conference of the South African institute of Computer Scientists and information Technologists on Enablement Through Technology*, 2002, 118-127.
7. Warkentin, M., Moore, R.S., Bekkering, E., Johnston, A.C.: Analysis of systems development project risks: an integrative framework. *SIGMIS Database*, Vol. 40, No. 2 (2009), 8-27.

Annotation

Risks of risk management

In spite of a great number of software development tools, there are still risks to be dealt with in order to successfully finish a project. Nowadays, the field of risk management encapsulates many different procedures for risk identification and mitigation. In this essay we briefly summarize some risk categorizations and relative importance of various risk factors in software development process. We focus on holistic viewpoint that deals with relationships and similarities of risks rather than putting them into discrete categories. We also address the most common problems of risk management linked to human and organizational factors.