Ing. David Řehák, Ph.D.

Katalog rizik: softwarový nástroj pro podporu řízení rizik v rezortu obrany

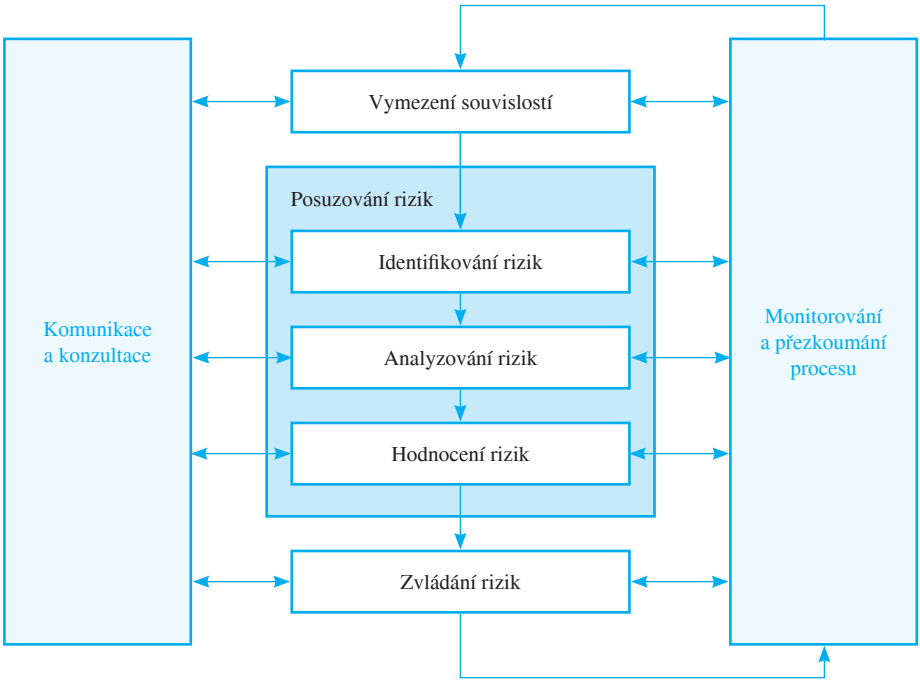
Řízení rizik, zvládání rizik, ovlivňování rizik či minimalizace rizik a další podobné pojmy jsou v současné době stále více používány a skloňovány v nejrůznějších podobách a souvislostech. Každá organizace nebo podnik čelí v rámci svého působení nebo v oblasti svého podnikání rizikům, které mohou vést ke snížení hodnoty organizace, případně až k jejímu ochromení nebo úplnému zničení. Proto se každý manažer snaží negativnímu působení těchto rizik předcházet a v případě, že již došlo k jejich působení, tak alespoň snížit jejich dopad na nejnižší možnou míru. V případě strategické úrovně naplňování cílů organizace se pak řízení rizik jeví existenční nutností a životním zájmem každé organizace. Proto můžeme říci, že řízení rizik v současné době zažívá oprávněný rozvoj a přitahuje pozornost všech významných manažerů, neboť s jeho využitím je možné předcházet ztrátám a škodám velkého rozsahu, které mohou mít pro organizaci až fatální následky.

Jinak tomu není ani v rezortu Ministerstva obrany České republiky, který se zabývá implementací vhodného systému řízení rizik již několik let. Vzhledem k tomu, že rezort obrany čelí značnému množství rizik nejrůznějších druhů (k tomuto faktu výrazně přispívá účast AČR v zahraničních misích), představuje optimální nastavení takovéhoto systému časově a zdrojově velmi náročný proces. Proto se jeví jako vhodné řešení postupné zavádění procesu řízení rizik (od jednotlivých sekcí MO ČR až po útvary a zařízení rezortu obrany) s využitím vhodných a dostupných softwarových nástrojů, jejichž aplikací bude celý proces značně zjednodušen, zpřesněn a urychlen.

Proces řízení rizik

Hned zpočátku je nutné si uvědomit, že **řízení rizik** (risk management) je proces, při němž se organizace nebo subjekt snaží zamezit působení existujících nebo předpokládaných hrozeb a navrhuje řešení, která mají prostřednictvím vhodných opatření minimalizovat závažnost dopadu a/nebo pravděpodobnost výskytu nežádoucích událostí. Aby byl proces řízení rizik efektivní, musí být nedílnou součástí řízení organizace, musí být zakotven v kultuře a praxi organizace a musí být uzpůsoben jejím procesům. Proces řízení rizik sestává z pěti základních subprocesů (viz obr. 1), kterými jsou komunikace a konzultace, vymezení souvislostí, posuzování rizik (zahrnuje identifikování, analyzování a hodnocení rizik), zvládání rizik a monitorování a přezkoumání procesu.

Stěžejním a nejnáročnějším subprocesem procesu řízení rizik je **posuzování rizik** (risk assessment), které zahrnuje tři stěžejní činnosti, a to identifikování, analyzování a hodnocení rizik. Počáteční činností subprocesu posuzování rizik je **identifikování rizik** (risk identification). V rámci této činnosti jsou prováděny dva úkony, a to identifikaci, stanovení hodnoty a seskupování aktiv a identifikaci konkrétních hrozeb a možných příčin jejich působení, tj. zdrojů hrozeb. Cílem tohoto kroku je vytvořit komplexní seznam



Obr. 1: Proces řízení rizika (upraveno podle ISO/IEC 31000:2009, s. 8)

rizik založený na takových událostech, které by mohly zamezit, snížit nebo zpomalit dosažení cílů. Rovněž je důležité identifikovat rizika související s nevyužitím příležitosti. Nezbytným krokem identifikování rizik je však zvážení všech možných příčin. Komplexní identifikace je totiž rozhodující, protože rizika, která nejsou identifikována na tomto stupni, nebudou zahrnuta do následující analýzy. Proto jsou při identifikování rizik důležité aktuální informace, které by měly obsahovat vhodná a podrobná data. Identifikace tak zahrnuje veškerá rizika bez ohledu na to ať jejich zdroj již je pod kontrolou organizace, nebo ještě není.

Druhou činností po identifikaci rizik je **analyzování rizik** (risk analysis), které je založeno na zdokonalování pochopení rizik. Poskytuje vstupy pro hodnocení rizik a pro rozhodnutí o tom, zda je potřeba identifikovaná rizika zvládnout a jaké jsou nejvhodnější strategie a metody zvládání rizik. Analýza rizik bere zřetel na příčiny a zdroje hrozeb, jejich pozitivní a negativní dopady (následky) a pravděpodobnost, že tyto dopady mohou nastat. Faktory, které ovlivňují závažnost dopadu a pravděpodobnost výskytu události by měly být rovněž identifikovány. Výsledkem analýzy rizik je stanovení neboli odhad úrovní jednotlivých rizik.

Závěrečnou činností subprocesu posuzování rizik je **hodnocení rizik** (risk evaluation). Smyslem této činnosti je napomáhat při rozhodování (založeném na výsledcích analýzy rizik) o tom, která rizika musí být přednostně zvládána. Hodnocení rizik zahrnuje dva úkony, a to komparaci úrovní rizik stanovených během analýzy s kritérii pro hodnocení rizik stanovenými při vymezení souvislostí a následné stanovení přijatelnosti

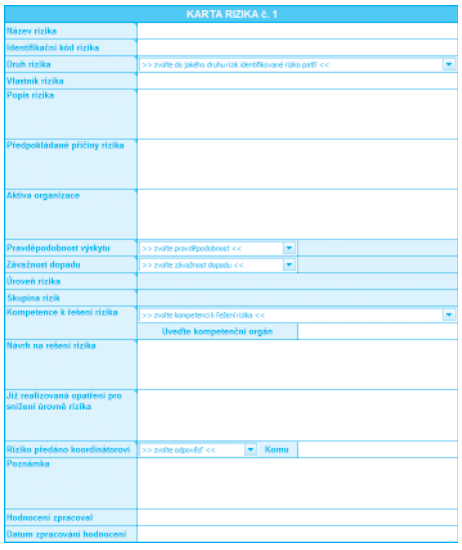
rizik a jejich prioritizaci. Jestliže úroveň rizika nesplňuje stanovená kritéria, riziko musí být zvládáno. Při rozhodování o zahájení subprocesu zvládání rizik je nezbytné počítat se širší souvislostí rizika a brát zřetel na přípustnou odchylku u rizik vznikajících ve vnějším prostředí organizace. Rozhodnutí by pak mělo být učiněno v souladu se zákonnými či jinými přijatými požadavky. Za některých okolností může hodnocení rizik vést k rozhodnutí o provedení další analýzy nebo k rozhodnutí neřešit zvládání rizika jakýmkoli jiným způsobem než udržováním stávající regulace rizika. Toto rozhodnutí je zpravidla ovlivňováno zájmem nebo postojem organizace k rizikům a rizikovými kritérii, která byla stanovena.

Katalog rizik

Jak již bylo řečeno, posuzování rizik je nejnáročnějším subprocesem procesu řízení rizik. Při jeho realizaci jednotlivé součásti rezortu obrany operují s velkým množstvím informací, které musí v relativně krátkém čase zaevidovat, vyhodnotit a navrhnout adekvátní řešení. Proto za účelem podpory tohoto subprocesu, tj. posuzování rizik, byl autorem článku vytvořen softwarový nástroj **Katalog rizik** (viz obr. 2), který slouží k evidenci identifikovaných rizik, jejich hodnocení a následné prioritizaci za účelem jejich dalšího zvládání.

Obr. 2: Softwarový nástroj „Katalog rizik“

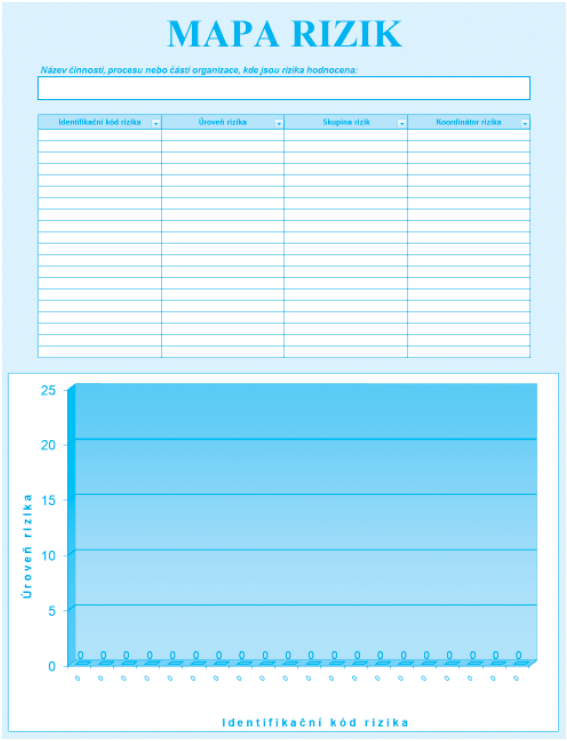
Tento softwarový nástroj sestává z úvodní stránky, dvaceti karet pro evidenci identifikovaných rizik a mapy rizik. Na úvodní stránce katalogu je nutné nejprve zadat název činnosti, procesu nebo konkrétní součásti rezortu obrany, kde budou rizika hodnocena. Tím dochází k vymezení okruhu aktiv, [1] která budou dále hodnocena. Následně je zapotřebí prostřednictvím podpůrných metod a technik [2] identifikovat jednotlivá rizika a zaznamenat o nich veškeré potřebné informace do jednotlivých karet (viz obr. 3).



Obr. 3: Karta rizika

Nejprve je nutné každému identifikovanému riziku přiřadit název a identifikační kód, pod kterým bude zaevidováno. Dále zařadit do jakého druhu rizik patří, čímž pracovníci rezortu obrany získávají přehled o tom, která rizika jsou druhově nejpočetnější, a mohou se lépe orientovat při identifikaci příčin působení těchto rizik. Následuje stanovení vlastníka rizika, což je odpovědný správce, který bude mít na starosti sledování dalšího vývoje rizika. Zcela zásadními informacemi, které musí být do karty rizika zaneseny, jsou popis daného rizika, předpokládané příčiny vzniku a působení rizika na hodnocenou část rezortu obrany a konkrétní aktiva nacházející se v hodnocené oblasti dopadu rizika. Na základě těchto informací může vlastník rizika přistoupit k jeho analýze a stanovení úrovně rizika. Prvním krokem analýzy je stanovení pravděpodobnosti výskytu potenciální nežádoucí události, k níž může dojít v důsledku působení daného rizika na hodnocená aktiva rezortu obrany. V rámci druhého kroku analýzy stanovuje potenciální závažnost dopadu nežádoucí události na hodnocená aktiva rezortu obrany. Samotná úroveň rizika je pak automaticky vypočtena součinem bodových hodnot odpovídajících zvolené pravděpodobnosti výskytu a závažnosti dopadu potenciální nežádoucí události. Na základě výsledné úrovně rizika je riziko zařazeno do příslušné skupiny rizik (běžná, významná a klíčová rizika), čímž je zřejmé jak velké nebezpečí pro rezort obrany představuje.

V druhé polovině vyplňování karty rizika je pozornost zaměřena na řešení neboli zvládání rizika. Nejprve je nutné zaznamenat informace týkající se kompetence řešení daného rizika, tzn. zda řešení rizika je či není v kompetenci konkrétní součásti rezortu obrany, a který kompetenční orgán se jím bude dále zabývat (např. ministerstvo, sekce, odbor či pracoviště). V případě, že řešení daného rizika je v kompetenci rezortu obrany, následuje uvedení konkrétních návrhů na jeho řešení a uvedení opatření, která již byla realizována pro snížení úrovně rizika. Dále je zaznamenáno, zda riziko bylo předáno konkrétnímu koordinátorovi a je uvedeno jeho jméno. V závěru vyplňování karty rizika je možné uvést doplňující informace a musí být vyplněno jméno zpracovatele a datum, kdy hodnocení rizika bylo provedeno.



Obr. 4: Mapa rizik

Po ukončení analýzy a evidence všech identifikovaných rizik následuje přesun na záložku „Mapa rizik“ (viz obrázek 4), kde je k dispozici soupis všech analyzovaných rizik, který zahrnuje identifikační kódy rizik, úroveň rizik,

skupiny, do kterých byla rizika zařazena a jména koordinátorů rizik. Tyto údaje mohou být jakýmkoli způsobem filtrovány či řazeny, takže např. může být provedena prioritizace rizik dle jejich závažnosti. Veškerá rizika jsou pak znázorněna graficky na mapě rizik a je u nich uveden identifikační kód a úroveň rizika.

Závěr

Smyslem softwarového nástroje „Katalog rizik" je usnadnění činnosti pracovníků rezortu obrany při identifikování, analyzování, hodnocení a prioritizaci rizik za účelem jejich dalšího zvládání. Zavedením tohoto softwarového nástroje lze předpokládat, že v rezortu obrany dojde nejen ke zrychlení činností v oblasti řízení rizik, ale především ke zkvalitnění celého procesu. Rovněž budou moci být veškerá data o identifikovaných rizicích snadněji sdílena, což povede ke zvýšení vzájemné spolupráce mezi jednotlivými součástmi rezortu obrany.

V současné době byl „Katalog rizik" předán k praktickému využití sekci rozvoje druhů sil – operační sekce Ministerstva obrany ČR, pro kterou byl vytvořen v rámci expertizního úkolu zadaného ředitelem sekce. Prozatím bude pracovníky sekce využíván k evidenci a prioritizaci rizik spojených s dosahováním operačních schopností Armády České republiky. Jeho další využití je v současné době projednáváno také s odborem interního auditu Ministerstva obrany ČR.

Poznámky k textu:

[1] Blíže viz ŘEHÁK, GRASSEOVÁ (2009, s. 13).
[2] Blíže viz GRASSEOVÁ, DUBEC, ŘEHÁK (2009), SMEJKAL, RAIS (2006) nebo BARTLOVÁ, BALOG (2007).

Literatura:

BARTLOVÁ, Ivana, BALOG, Karol. *Analýza nebezpečí a prevence průmyslových havárií.* 2. vyd. Ostrava: SPBI, 2007, sv. 7, 191 s. ISBN 978-80-7385-005-0.

CHJ-6. *Pokyn k jednotnému uplatňování závazných pravidel a doporučení pro systém řízení rizik v orgánech veřejné správy*, 2004. 37 s.

GRASSEOVÁ, Monika, DUBEC, Radek, HORÁK, Roman. *Procesní řízení ve veřejném i soukromém sektoru*. 1. vyd. Brno: Computer Press, 2008. 266 s. ISBN 978-80-251-1905-1.

GRASSEOVÁ, Monika, DUBEC, Radek, ŘEHÁK, David. *Analyzování při strategickém řízení - praktické nástroje, metody a postupy.* 1. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2621-9.

ISO/IEC 31000. *Risk management – Principles and guidelines on implementation,* [Draft International Standard], 2008, 18 p.

ISO/IEC Guide 73. *Risk management - Vocabulary*, 2002.

ŘEHÁK, David, GRASSEOVÁ, Monika. Vymezení souvislostí jako součást procesu řízení rizik u organizací ústřední státní správy. *Vojenské rozhledy*, Praha, 2009, roč. 18(50), č. 3, s. 12-18. ISSN 1210-3292.

SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích.* 2. vyd. Praha: Grada Publishing, 2006. 296 s. ISBN 80-247-1667-4.

TICHÝ, Milík. *Ovládání rizika. Analýza a management.* 1. vyd. Praha: C. H. Beck, 2006. 396 s. ISBN 80-7179-415-5.