

SMEJKAL, Vladimír, RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. 4., aktualizované a rozšířené vydání. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

Josef Melichar^a

Monografie autorské dvojice Vladimír Smejkal a Karel Rais ve svém čtvrtém, aktualizovaném a rozšířeném vydání navazuje na předchozí tři monografie zabývající se riziky a jejich zvládním. Kniha byla napsána v současném prostředí České republiky a přináší aktuální poznatky z oblasti řízení rizik. Kniha je v jednotlivých kapitolách rozčleněna do tří úrovní, což poskytuje dostatečný stupeň podrobnosti a zároveň zamezuje příliš komplikované struktuře textu.

V této knize lze vidět zdroj hodnotných informací a návodů na to, jak ovlivnit úspěšnost organizace pomocí zvládnutí rizik. Problematika rizik a jejich řízení je zde srozumitelně a čtenářsky velmi přijatelně objasněna a i když je tematika knihy zasazena z větší části do civilního prostředí, přímo se nabízí myšlenka jejího využití v prostředí ozbrojených sil. Problematika hodnocení rizik a jejich řízení je využitelná zejména při obranném plánování a při plánování a vyhodnocování operací. Při obranném plánování se rizika vážou na hrozby plynoucí z bezpečnostního prostředí a tudíž je nevyhnutné se jejich identifikací a řízením zabývat a využít potenciálu, který problematika řízení rizik nabízí při plánování obranných schopností tak, jak se tomu děje například v NATO. Kromě toho je hodnocení a řízení rizik standardní a nezbytnou součástí procesu plánování a vyhodnocování operací, není tedy důvod tuto problematiku ponechat pouze civilním firmám. Příklady popisované na civilních firmách je třeba chápat jako použití zásad pro identifikaci a řízení rizik v jejich podmínkách, a tyto zásady využít a aplikovat v prostředí ozbrojených sil.

V první kapitole se autoři zabývají popisem života firmy, příčinami neúspěchu v podnikání, krizemi firem, jejich zdroji, základními příznaky krizí a způsoby, jak jim předcházet. Typické vnitřní zdroje krizí, jakými jsou personální krize nebo krize know-how, uvedené v této kapitole, stejně jako některé kritické momenty rozvoje úspěšné firmy, jakými jsou například získání zaměstnanců, obsazení manažerských funkcí nebo zajištění financování pro další rozvoj, které jsou uváděny jako klíčové pro firmu, jsou stejně klíčové také pro státní organizace. Využití poznatků popisovaných v této kapitole se zdaleka neomezuje pouze na firmy soukromých podnikatelů, ale je přínosem i pro státní organizace, k nimž patří například armáda České republiky.

Armáda České republiky je obdobná firma jako firmy uváděné v knize, potýká se s řadou problémů, které jsou stejné jako problémy civilní firmy. Výše uvedené příklady jsou tak platné jak pro civilní firmy, tak i pro Armádu České republiky (AČR). Stejně tak některé momenty jsou stejně klíčové pro firmy i pro AČR, s problémy získávání zaměstnanců, obsazení manažerských funkcí nebo zajištění financování pro další rozvoj se jistě v průběhu svojí kariéry každý voják setkal.

^a Centre for Security and Military Strategic Studies, University of Defence, Brno, Czech Republic.
josef.melichar@unob.cz

Ve druhé kapitole, pojednávající o charakteristických znacích úspěšné firmy, stojí za zmínku rámec 7S faktorů konzultační firmy McKinsey (struktura, strategie, systémy, schopnosti, spolupracovníci, styl a sdílené hodnoty), která rovněž najde široké využití mimo prostředí civilních firem. V této kapitole se objevují hned dvě klíčové myšlenky - „záruka trvalého úspěchu je v přizpůsobování“ (s. 38) a „dnešní úspěšná firma musí být připravena na trvalý proces změn“ (s. 56). Jakkoliv jednoduché a obecné se mohou tyto myšlenky zdát, představují závěry, které vycházejí z vyhodnocení historického vývoje přírody, kdy rostlinné a živočišné druhy, které se nedokázaly přizpůsobit neustálým změnám ve svém okolí, zanikly. Tyto dvě základní myšlenky tak představují skutečný klíč k úspěchu, který je bohužel v reálném životě často ignorován.

Třetí kapitola je věnována vztahu řízené změny a snižování rizika ve firmě. Čtenář je zde proveden procesem řízených změn ve firmě, je mu představen model řízení změn zakladatele vědy o chování jedinců a skupin ve společnosti Kurta Lewina, vyučovaný na všech manažerských školách. Tento model rozdělující proces změny ve firmě do tří základních kroků, kterými jsou rozmrazení, přechod a znovuzmrazení, je v knize srozumitelně představen jako užitečný nástroj pro pochopení a pro uskutečňování změn ve firmách. V závěru kapitoly popsané chápání změny jako cesty a schopnost přizpůsobení se měnícím se podmínkám stejně jako schopnost improvizace představují informace, které stojí za přečtení a které dotváří rámec této kapitoly.

Ve čtvrté kapitole se autoři zaměřují na pojem riziko, jsou zde popsány základní atributy rizika, možné postoje k rizikům, obecné zákonitosti řízení rizik a postup při řízení podnikatelských rizik. Je zde rovněž uveden postup pro výpočet míry rizik, postup pro hodnocení rizik a základní pravidla pro praktické řízení rizik. Tato kapitola přináší stěžejní část problematiky rizik a jejich řízení, a umožňuje pochopit podstatu pojmu riziko. Spolu s následující pátou kapitolou, pojednávající o metodách snižování rizik, tvoří páteř knihy a jsou absolutním minimem, které by čtenář měl přečíst, pokud chce porozumět problematice rizik a jejich řízení.

V páté kapitole se autoři zaměřují na metody používané ke snižování rizik. Zabývají se zde doporučeními pro jejich výběr k řešení rizik podle základních charakteristik rizika. Jsou zde popsány s uvedením praktických příkladů základní metody ke snižování rizik, tedy redukce rizika, přenesení rizika, vyhnutí se riziku a podstoupení rizika, což přináší solidní informační základ pro řízení rizik. Za jedno z nejzajímavějších témat této kapitoly lze považovat využití prognostických metod a možnosti využití genetických algoritmů a neuronových sítí. Podstata genetických algoritmů je zde popsána pomocí analogie z přírody, která je schopna vyrovnat se s problémy ve složitém a měnícím se prostředí. Tato metoda, vzhledem k tomu, že se zaměřuje na řešení špatně strukturovaných složitých problémů v neustále se měnícím prostředí, vyvolává otázku možnosti jejího využití při řešení způsobu, jak se vyrovnat se současnými a budoucími hrozbami, které vycházejí z dynamicky se měnícího bezpečnostního prostředí. Prognostické metody jsou využitelné při řešení otázek obranného plánování, při kterých je třeba zpracovávat scénáře možného budoucího vývoje bezpečnostního prostředí, což představuje řešení špatně strukturovaných problémů. Možnosti využití genetických algoritmů při prognózování mohou představovat cestu, jak zefektivnit zpracování scénářů. Mohou také usnadnit hledání způsobu, jak se s těmito scénáři vyrovnat při obranném plánování, tedy při definování schopností, které budeme v budoucnu potřebovat k zajištění bezpečnosti státu.

Šestá kapitola se zaměřuje na otázky informačního rizika z pohledu získávání informací a z pohledu ochrany informací. Kapitola přináší čtenáři národní strategii informační bezpečnosti České republiky, hlavní cíle zákona o zabezpečení kybernetické bezpečnosti a objasnění dopadu tohoto zákona na orgány veřejné moci, na soukromoprávní subjekty a na

subjekty spravující kritickou informační infrastrukturu. Autoři se rovněž zabývají možnostmi využití řízených úniků informací, což je velmi zajímavý a účinný nástroj k ovlivnění vlastního úspěchu. V současném komplexním informačním prostředí, ve kterém jsme v mnohém závislí na počítačových sítích a které je zdrojem nepřeborného množství příležitostí a hrozeb, je tato problematika vysoce aktuální a lze ji doporučit jako základní součást informační gramotnosti.

Sedmá kapitola je věnována vztahu investičního rozhodování a rizika, finanční analýze, metodám finanční analýzy a na postupu při finanční analýze. Na dvou praktických příkladech (hydroelektrárna v Mongolsku a parkoviště v Brně) je uveden možný postup při rozhodování o realizaci investice. Společným jmenovatelem obou příkladů je použití genetických algoritmů popsaných v páté kapitole. V závěru kapitoly jsou uvedené možnosti využití umělých neuronových sítí, které jsou zajímavé svou schopností pracovat obdobně jako lidský mozek s přednostmi, kterou představuje schopnost eliminovat omyly běžné u lidského mozku při zpracovávání velkého množství kritérií.

Osmá kapitola je zaměřena na právní rizika a jejich prevenci. Kapitola přibližuje problematiku právních skutečností a právních úkonů, zajímavý pojem dobré mravy, ale také nově problematiku elektronického podpisu, elektronických právních úkonů a konverze dokumentů, tedy převodu dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě. Tato kapitola se také zabývá aktuálními pojmy jako eLegislativa, ePodatelna, ePlatební rozkaz, eTrestní řízení a některými dalšími pojmy souvisejícími s informačním prostředím a elektronizací. Čtenář zde najde souhrn užitečných informací nezbytných pro vyhnutí se rizikům v právním prostředí, soustředěný do jedné kapitoly, což je velmi přijatelný servis.

Devátá kapitola se zaměřuje na rizika ve veřejné správě, zabývá se orgány veřejné moci, riziky spojenými s výkonem veřejné moci a riziky podle zákona o finanční kontrole ve veřejné správě. Nejsou opomenuta ani rizika, jakými jsou politická, kulturní, vojenská rizika, terorismus a další. Smejkal s Reitem zde poukazuje na nesprávný pohled na rizika v případě činnosti orgánů veřejné moci, kdy se mnoho lidí domnívá, že rizika u těchto orgánů není třeba řešit. Takovéto zjištění ukazuje na potřebu porozumět problematice rizik a jejich řízení, ale také na to, že ve znalosti této problematiky existují značné mezery.

Desátá kapitola pojednává o zásadách krizového plánování, podrobněji se zabývá krizovým řízením v České republice, legislativou, která krizové řízení vymezuje, a vývojem v oblasti krizového řízení do budoucnosti. V závěru kapitoly se autoři zaměřují na nedostatky v oblasti prevence krizových událostí, které se projevují například výstavbou stavebních objektů v záplavových oblastech, ale taky tím, že neexistuje zpracovaná komplexní analýza rizik zabývající se státem a jeho majetkem, stejně jako životy, zdravím a majetkem občanů. Za velmi zajímavou část této kapitoly lze považovat pasáž pojednávající o bezpečnostních hrozbách uvedených v *Bezpečnostní strategii České republiky*, schválené vládou v roce 2011. Těmito hrozbami jsou terorismus, šíření zbraní hromadného ničení a jejich nosičů, kybernetické útoky, nestabilita a regionální konflikty v euroatlantickém prostoru a jeho okolí, negativní dopady mezinárodní migrace, organizovaný zločin a korupce, ohrožení funkčnosti kritické infrastruktury, přerušení dodávek strategických surovin nebo energie, pohromy přírodního a antropogenního původu a jiné mimořádné události. Bezpečnostní hrozby představují východisko pro zpracování scénářů možného budoucího vývoje, a na ně navazující požadavky na schopnosti, které Česká republika potřebuje k tomu, aby se vyrovnala s riziky plynoucími z těchto scénářů. Zpracované hrozby z pohledu současného stavu obranného plánování ČR visí částečně ve vzduchoprázdnu, jsou definovány a marně natahují ruku po scénářích, které na ně mají navazovat. Jejich uvedení v kontextu krizového plánování provokuje otázku „co s těmito hrozbami můžeme udělat?“

a mělo by vyprovokovat českou bezpečnostní komunitu k tomu, aby udělala již dlouho potřebný logický následující krok.

Čtvrté, aktualizované a rozšířené vydání knihy *Řízení rizik ve firmách a jiných organizacích* autorů Vladimíra Smejkal a Karla Reise nelze hodnotit jinak než pozitivně. Monografie řeší problematiku rizik a jejich řízení, kterou lze klasifikovat jako klíčovou problematiku pro úspěšnost státních i nestátních subjektů. Na rozdíl od jiných knih jako například *Analýza podniku v rukou manažera* autorů Monika Grasseová, Radek Dubec, David Řehák, která problematiku řízení rizik přináší v jedné kapitole na 37 stránkách, přináší tato kniha komplexním způsobem zpracované informace potřebné pro zvládání rizik zasazené do současného Evropského a světového kontextu. Kniha najde využití mezi čtenáři zabývajícími se strategií.