ANALÝZA A HODNOTENIE RIZÍK

Žák Miroslav, Kredatus Ondrej *)

ABSTRAKT

Rozsah opatrení na zaistenie bezpečnosti v akomkoľvek systéme by mal byť úmerný veľkosti rizík a ohrození, ktorým je alebo môže byť tento systém vystavený. Riziko (možnosť, nebezpečenstvo straty, neúspechu, škody) býva definované ako určitý druh neistoty, ktorý je možné prostredníctvom štatistických metód kvantifikovať, a tak predpovedať vznik nepriaznivých skutočností. Stupeň miery bezpečnosti (rizika) je možné merať. I keď vždy ide o vyjadrenie kvality je vhodné, keď je tato kvalita nejakým spôsobom kvantifikovaná. Tento článok pojednáva o možnosti využitia kvantitatívnej analýzy ako prevod slovného kvalitatívneho hodnotenia na kvantitatívne.

Kľúčové slová:
bezpečnostné prostredie, riziko, manažérstvo rizika, subjektívne pravdepodobnosti.

ABSTRACT

The range of measures to ensure safety in any system should be proportional to the size of the risks and threats, which is or may be exposed to this system. Risk (the possibility of risk of loss, failure, damage) is usually defined up as a kind of uncertainty that can be quantified by statistical methods, and to predict the emergence of adverse facts. Grade level of safety (risk) can be measured. Although each is an expression of quality is appropriate when the quality is somehow quantified. This article discusses the possibility of using quantitative analysis of how the transfer of verbal qualitative to quantitative assessment.

Keywords:
security environment, risk, management risk, subjective probability.

*)

[1] Miroslav ŽÁK, Dr. h. c. prof. Ing. DrSc., Akadémia ozbrojených síl generála Milana Rastislava Štefánika Demänová 393, 031 06 Liptovský Mikuláš 6, 0960422792, e-mail miroslav.zak@aos.sk

[2] Ondrej KREDATUS, Ing. PhD., Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Demänová 393, 031 06 Liptovský Mikuláš 6, 0960423199, e-mail ondrej.kredatus@aos.sk

ÚVOD

V posledných rokoch došlo v politicko-bezpečnostnej situácii vo svete, Európe k výrazným zmenám, na ktoré musíme reflektovať aj pri riešení krízových situácií v podmienkach Slovenskej republiky. Súčasný svet je vystavený konfrontácií s protivníkom, ktorý je rozptýlený po celom svete a ktorý nahradzuje nedostatok konvenčných vojenských prostriedkov bezohľadným terorizmom. Pripravenosť teroristických skupín kedykoľvek prevziať iniciatívu, umierať na následky svojich vlastných operácií, zabíjať čo najviac ľudí a čo možno najokázalejším spôsobom, vyvolať paniku a rozložiť infraštruktúru, to všetko je dôvod na hľadanie spôsobov, ako sa vyrovnať s týmto fenoménom súčasnosti. V súčasnosti sa zabezpečenie efektívneho velenia a riadenia v prostredí asymetrického bojiska považuje za jeden z rozhodujúcich faktorov, ktoré vedú k splneniu cieľov a úloh postavených na veliteľov. Cieľom je dosiahnuť prevahu v rozhodovaní, podmienenú informačnou prevahou, keď je prenesená do využiteľných poznatkov umožňujúcich rýchlejšie plánovanie, lepšie rozhodovanie a rozhodnejšie účinky operácií.

1 ROZHODOVANIE A MANAŽÉRSTVO RIZÍK

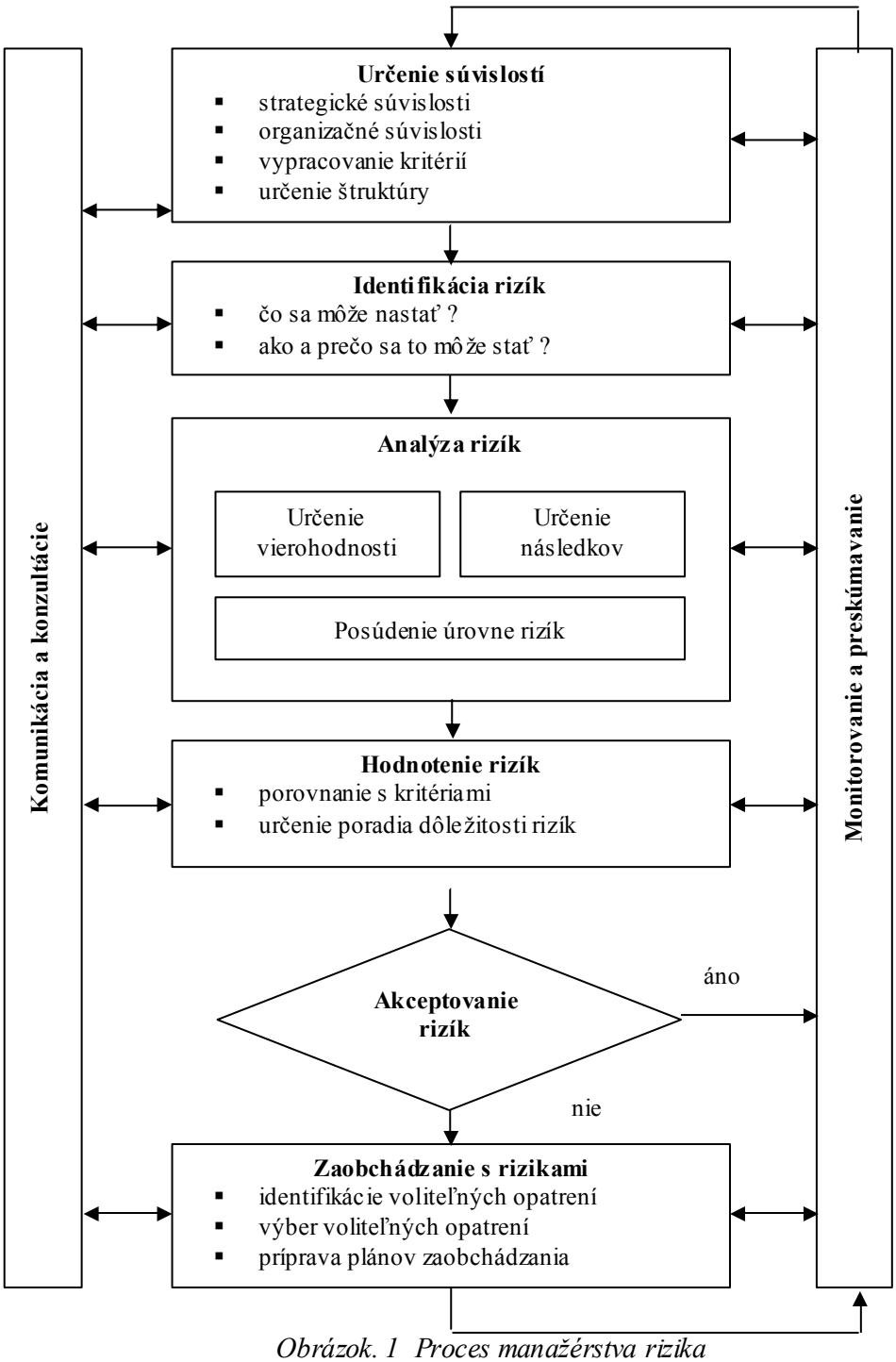
Pre asymetrické operácie je charakteristický moment prekvapenia pri ich vzniku a to aj v prípade, že sme sledovali nárast rizikových faktorov. Táto skutočnosť je ďalej zvýrazňovaná aj tým, že spravidla nemáme dostatok podrobných informácií o tom, kde a kedy môže k rizikovej situácii dôjsť. K týmto faktorom ďalej pristupuje obrovský nárast rozsahu činnosti a ich veľká rôznorodosť, ohrozenie existenčne dôležitých záujmov spoločnosti priamo alebo sprostredkovane, činnosť v strese a v časovej tiesni, narušenie zaužívaných pracovných postupov a rozhodovacích procesov a ich nútený prechod na zvláštny režim činnosti, rozhodovanie bez možnosti podrobnej analýzy a rad ďalších.

Podmienkou dosiahnutia prevahy v rozhodovaní je koncepcia rozvoja a implementácie informačných sietí, znalostných databáz a systémov na podporu rozhodovania a velenia. Táto koncepcia umožní vedenie operácií prostredníctvom komplexného, spoločného a cieľavedomého používania systémov velenia, riadenia, spojenia, počítačového spracovania, spravodajstva a prieskumu formou digitalizácie a zasieťovania nasadených síl na maximalizovanie účinku operácií v reálnom čase.

V navrhovaných systémoch na podporu rozhodovania sa predpokladá aj rozsiahle využitie postupov manažérstva rizík. Manažérstvo rizika poskytuje všeobecný návod na určovanie súvislostí, identifikáciu, analýzu, vyhodnocovanie, zaobchádzanie, komunikáciu a trvalé monitorovanie rizík. Manažérstvo rizika treba chápe ako integrálna súčasť dobrej veliteľskej a riadiacej praxe, ako iteratívny proces, ktorý svojou postupnosťou umožňujú trvalé zlepšovanie pri rozhodovaní. Hlavné prvky procesu manažérstva rizika sú znázornené na obrázku (Obrázok 1).

Posudzovaniu rizík predchádza určovanie súvislostí a identifikácia rizík. Pri určovaní súvislostí treba určiť a definovať základné parametre, v rámci ktorých sa riziká musia riadiť, aby sa poskytol aj návod na rozhodovanie. Posúdia sa kritériá, v porovnaní s ktorými sa bude hodnotiť riziko. Rozhodnutia týkajúce sa prijateľnosti rizika a zaobchádzania s rizikom sa môžu zakladať na bezpečnostných, bojových,

technických, ekonomických, legislatívnych, sociálnych, humanitných alebo iných kritériách. Hoci kritériá rizika sa najskôr vypracúvajú ako súčasť určenia súvislostí s manažérstvom rizika, môžu sa ďalej rozpracúvať a spresňovať po identifikácii konkrétnych rizík a výbere techniky analýzy rizika.



Obrázok. 1 Proces manažérstva rizika

Identifikácia rizík sa zameriava na identifikáciu rizík, ktoré sa majú riadiť. Obsažná identifikácia ako výsledok dobre štruktúrovaného systematického procesu je kritická, pretože potenciálne riziko, ktoré sa v tejto etape neidentifikuje, sa z ďalšej analýzy vylučuje. Identifikácia má zahŕňať všetky riziká bez ohľadu na to, či sú alebo

nie sú pod kontrolou. Cieľom je vytvoriť obsažný zoznam udalostí, ktoré by mohli ovplyvniť každú činnosť v operácii. Tieto udalosti sa potom rozoberajú podrobnejšie s cieľom zistiť, čo sa môže stať.

Pri analýze rizík sa posudzujú jestvujúce bezpečnostné opatrenia a analyzujú sa riziká v termínoch následkov a možností súvisiacich s týmito opatreniami. Analýza má brať do úvahy množinu potenciálnych následkov a možností, že tieto následky nastanú. Následok a možnosť možno kombinovať, čím sa získa vierohodnosť rizika. Hodnotenie samotnej úrovne rizika je možné merať.

Zaobchádzanie s rizikom zahŕňa identifikáciu rozsahu voliteľných opatrení na zaobchádzanie s rizikom, ich posúdenie, prípravu plánov zaobchádzania s rizikom a ich zavedenie. Voliteľné opatrenia, ktoré sa navzájom nemusia vylučovať alebo nemusia byť vhodné vo všetkých prípadoch. Ide o také opatrenia ako vyvarovanie sa rizika rozhodnutím nepokračovať s činnosťou, ktorá pravdepodobne vyvolá riziko, zníženie vierohodnosti výskytu rizika, obmedzenie následkov rizika, prenos rizika, a zachovanie rizika.

2 ANALÝZA A HODNOTENIE RIZÍK

Analýza a hodnotenie rizík patria k najdôležitejším a najzložitejším etapám manažérstva rizika. Pri analýze rizík sa posudzujú jestvujúce bezpečnostné opatrenia a analyzujú sa riziká v termínoch následkov a možností súvisiacich s týmito opatreniami. Analýza má brať do úvahy množinu potenciálnych následkov a možností, že tieto následky nastanú. Následok a možnosť možno kombinovať, čím sa získa vierohodnosť rizika (Obrázok 2).

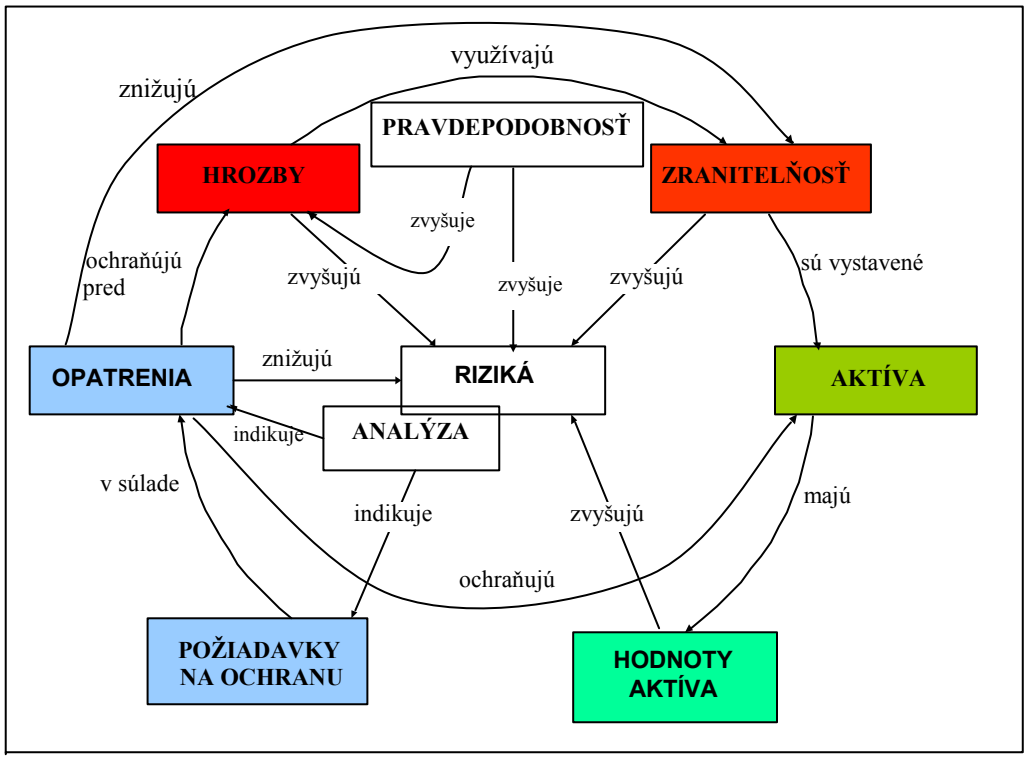
Pri rozhodovaní a plánovaní v podmienkach vedenia asymetrických operácií to znamená, že je potrebné identifikovať možné hrozby v priestore operácie, vyhodnotiť, ktoré z nich predstavujú riziko pre vedenie operácie a prípadne prijať opatrenia na zvýšenie ochrany vojsk. Výsledné riziko je potrebné chápať ako funkciu veľkosti hrozby, dôležitosti a ochrany objektu (živej sily, techniky a podobne).

Hodnotenie samotnej úrovne rizika je možné merať. I keď vždy ide o vyjadrenie kvality je vhodné, keď je tato kvalita nejakým spôsobom kvantifikovaná. Môžeme k tomu pristúpiť aj tak, že vyjadríme vzťah hrozby a možnej straty. Takýto prístup je dobre rozpracovaný napríklad v oboru bezpečnosti informačných technológii. Hodnotenie spravidla spočíva v tom, že sa špecifikuje povaha vzťahu hrozby a rizika a ďalších faktorov (hodnota, zraniteľnosť, protiopatrenia).

Pri rozhodovaní a plánovaní v podmienkach vedenia asymetrických operácií to znamená, že je potrebné identifikovať možné hrozby v priestore operácie, vyhodnotiť, ktoré z nich predstavujú riziko pre vedenie operácie a prípadne prijať opatrenia na zvýšenie ochrany vojsk. Výsledné riziko je potrebné chápať ako funkciu veľkosti hrozby, dôležitosti a ochrany objektu (živej sily, techniky a podobne).

Hodnotenie samotnej úrovne rizika je možné merať. I keď vždy ide o vyjadrenie kvality je vhodné, keď je tato kvalita nejakým spôsobom kvantifikovaná. Môžeme k tomu pristúpiť aj tak, že vyjadríme vzťah hrozby a možnej straty. Takýto prístup je dobre rozpracovaný napríklad v oboru bezpečnosti informačných

technológii. Hodnotenie spravidla spočíva v tom, že sa špecifikuje povaha vzťahu hrozby a rizika a ďalších faktorov (hodnota, zraniteľnosť, protiopatrenia).



Obrázok 2 Analýza a verifikácia rizík

Analýzu a hodnotenie rizika možno robiť s rozličným stupňom podrobností v závislosti od informácií o riziku a od dostupných údajov. Ak nie sú k dispozícii nijaké údaje z minulosti, možno alternatívne urobiť subjektívny odhad, ktorý vyjadruje stupeň presvedčenia jednotlivca alebo skupiny, že nastane konkrétna udalosť alebo výsledok. Aby sme sa vyvarovali subjektívnych názorov, mali by sa pri analýze následkov a ich vierohodnosti využiť najlepšie dostupné informačné zdroje. Pri analýze rizík sa môže použiť kvalitatívny alebo kvantitatívny prístup, prípadne ich kombinácia.

Kvalitatívna analýza sa spravidla používa ako úvodná hodnotiaca etapa, tam, kde číselné údaje sú nedostatočné na vykonanie kvantitatívnej analýzy. Kvalitatívne metódy využívajú najmä expertné ohodnocovanie. Tieto sa využívajú v prípadoch, ak chýbajú alebo sú ťažko vyjadriteľné číselné hodnoty (údaje) pre kvantitatívne ohodnotenie rizika. Pomocou týchto metód sa dá hodnotiť riziko napr. ako prijateľné alebo neprijateľné, malé, nízke, stredné a podobne. Kvantitatívna analýza využíva na následky a odhad pravdepodobnosti číselné hodnoty získavané z údajov uvedených v rozličných zdrojoch. Kvalita analýzy závisí od presnosti a úplnosti použitých číselných hodnôt. Vierohodnosť sa zvyčajne vyjadruje ako pravdepodobnosť, frekvencia alebo ako kombinácia výskytu a pravdepodobnosti. Pri kombinácii predchádzajúcich prístupov (semikvantitatívnej analýze) sa kvalitatívnym mierkam priraďujú číselné hodnoty. Pri semikvantitatívnej analýze sa pre meranie úrovne rizika (verifikáciu úrovne rizika) môžu využiť subjektívne pravdepodobnosti, ktoré vyjadrujú osobné

presvedčenie manažéra (experta) vo výskyt určitého javu alebo udalosti. Medzi číselnými hodnotami a slovnými popisy subjektívnych pravdepodobností existuje určitý vzťah.

V systémoch na podporu rozhodovania môže byť v znalostnej databáze uložený prehľad o možných hrozbách o možných ohrozeniach v priestore pôsobenia expedičnej jednotky i o pravdepodobnosti ich výskytu. To umožní zatriedenie rizík a ďalej identifikáciu priorít pre príslušné stupne velenia a riadenia. Ak výsledné riziká patria do kategórie malé riziko alebo prijateľné riziko, možno ich akceptovať s minimálnou ďalšou pozornosťou. Malé riziká a prijateľné riziká treba monitorovať a periodicky preskúmavať s cieľom presvedčiť sa, že zostávajú prijateľné. Ak riziká nepatria do kategórie malé riziko alebo prijateľné riziko, treba sa nimi zaoberať a použiť jedno alebo viacero voliteľných odvetných opatrení. Prijaté opatrenia musia podporovať zvýšenie bezpečnosti vojsk pri presunoch, pri plnení úloh na kontrolných stanovištiach a podobne.

ZÁVER

Znalosť potenciálnych rizík je dôležitým faktorom pre prijímanie optimálnych rozhodnutí. K identifikácii a analýze rizík je nutné pristupovať metodicky, posúdiť všetky možné i nemožné situácie, aby sa zaistilo rozpoznanie všetkých dôležitých činností v organizácii a definovanie všetkých z nich vyplývajúcich rizík. Z uvedeného dôvodu bude vhodné využívať metódy manažérstva rizík pri plánovaní a vedení operácií v podmienkach asymetrického operačného prostredia

LITERATÚRA:

[1] SAATY, T. L.: *The Analytic Hiearchy Process*. Mc. Graw-Hill Publising, New York 1980.

[2] SMEJKAL, V. – RAIS, K.: *Řízení rizík*. Grada Publishing a.s. Praha 2003.

[3] ŽÁK, M. - RAČKO, J: *Informations and Crisis Manageent.* In: Zborník z medzinárodnej vedeckej konferencie – THE INTERNET, COMPETITIVENESS AND THE ORGANIZATIONAL SECURITY – Information and Data Security, Crisis Manageent and Strategic Decision-making in Knowledge Society. X Annual International Conference, Univerzita Tomáše Bati ve Zlíne, Fakulta managementu a ekonomiky, Zlín 26. marec 2008.

[4] Slovenská technická norma STN 01 0380 Manažérstvo rizika (AS/NZS 4360:1999). Slovenský ústav technickej normalizácie, Bratislava 2003.

[5] ŽÁK, M. - BUČKA, P.: *Podpora riešenia vojenských rozhodovacích problémov*. Medzinárodná konferencia „Spoločné operace a vzdušné sily, PVO 2008. Universita obrany Brno, Česká republika, 23.–24.5.2008, 12 s. ISBN 978-80-7231-582-4

Článok recenzoval:
prof. Ing. Ladislav Šimák, PhD.