

MANAŽMENT RIZIKA V PROCESĚ OCHRANY PRVKOV KRITICKEJ INFRAŠTRUKTÚRY

RISK MANAGEMENT TO PROTECT CRITICAL INFRASTRUCTURE

Mária HUDÁKOVÁ
maria.hudakova@fbi.uniza.sk

Abstract

The infrastructure is an essential part of every developed country. Every day we are all dependent on the availability and trouble-free use of infrastructure. Nevertheless, the infrastructure may be seriously damaged, whether natural disasters, technical failures, human errors or terrorism. Therefore, it is important to know the elements of critical infrastructure, identify, assess their risks and propose actions to reduce them and ensure the protection of critical infrastructure. The essence of this paper is to point out the method of risk management of operators of the elements of critical infrastructure in Germany, and pick up the design process of risk management of critical infrastructure in Slovakia.

Key words

Critical Infrastructure, Risks, Crisis, Risk Management, Protecting.

ÚVOD

V posledných rokoch sa situácia z pohľadu bezpečnosti obyvateľstva výrazne zmenila. Rastúci trend mimoriadnych udalostí vytvára nové výzvy a potrebu na zabezpečenie vyššej bezpečnosti jednotlivých krajín. Rovnako ako stav bezpečnosti obyvateľstva, tak aj stav zraniteľnosti infraštruktúry sa mení. Väčšina sektorov a prvkov infraštruktúry je v súčasnosti spojená rozličnými spôsobmi, ktoré sú od seba závislé. Zlyhanie jednej časti infraštruktúry sa veľmi rýchlo rozšíri do iných častí infraštruktúr, miest alebo oblastí podnikania s ďalekosiahlymi dopadmi poškodenia. Infraštruktúra môže byť vážne poškodená, resp. ohrozená prírodnými katastrofami, technickými poruchami, ľudskými chybami alebo úmyselnými činmi teroristického alebo iného trestného charakteru.

Vláda každej krajiny sa snaží investovať množstvo peňazí do bezpečnosti. Avšak pozitívne účinky bezpečnostných opatrení často nie sú merateľné objektívnymi podmienkami. Namiesto toho organizácie alebo orgány štátnej správy považujú dlhšie obdobie bez kríz ako potvrdenie účinnosti prijatých opatrení, ktoré môžu smerovať k tomu, že sa veľmi ľahko prehliadajú potenciálne hrozby a zraniteľné oblasti. Identifikované riziká sú často v praxi tie, ktoré sa zdajú byť zvládnuteľné alebo ovládateľné a pri ktorých sú zjavné príčiny a následky [1]. Ďalšie riziká sú veľmi často ignorované vedome či nevedome a ich možné dopady nie sú zohľadnené pri realizácii preventívnych opatrení. Preto je dôležité, aby manažment rizika bol uplatňovaný nielen v podnikateľských subjektoch, v podmienkach inštitúcií verejnej správy, ale aj pri zvyšovaní komplexnej bezpečnosti organizácií na úseku ochrany kritickéj infraštruktúry [2].

Význam **manažmentu rizika** je v súčasnosti zvýraznený aj tým, že v posudzovanom priestore býva veľmi často veľká koncentrácia obyvateľov, občianskej vybavenosti, dopravných objektov, priemyselných komplexov a tým aj potenciálnych veľkých škôd. Podľa Šimáka sa manažment rizika považuje za nástroj identifikovania, hodnotenia, ale aj znižovania rizik,

pomocou ktorého je možné zvyšovať mieru bezpečnosti rôznych procesov a konkrétnych činností [3].

Kritickú infraštruktúru (KI) môžeme chápať ako časť infraštruktúry (vybrané organizácie a inštitúcie, objekty, sústavy, zariadenia, služby a systémy), ktorej zničenie alebo znefunkčnenie spôsobí ohrozenie alebo narušenie politického a hospodárskeho chodu štátu, alebo ohrozenie života a zdravia obyvateľstva [4]. **Ochrana kritickej infraštruktúry** zahŕňa opatrenia, resp. bezpečnostné riešenia, ktoré znižujú pravdepodobnosť a rozsah poškodenia či porúch zničenia kritickej infraštruktúry. Ide o činnosti (bezpečnostné riešenia), ktorých cieľom je zabezpečiť funkčnosť, integritu a kontinuitu činnosti prvku kritickej infraštruktúry s cieľom predísť, odvrátiť alebo zmierniť hrozbu jeho narušenia alebo zničenia [5, 6].

Podľa zákona o kritickej infraštruktúre v SR je prevádzkovateľom kritickej infraštruktúry považovaná právnická osoba, fyzická osoba, ktorá je vlastníkom prvku alebo z iného právneho dôvodu prevádzkuje prvok [7]. Tento zákon ukladá prevádzkovateľom za povinnosť ochraňovať prvok pred narušením alebo zničením. Na ten účel prevádzkovateľ je povinný poskytnúť príslušnému ústrednému orgánu údaje, doklady a vysvetlenia potrebné aj na **vypracovanie analýzy rizík sektora** (Zákon č. 45/2011, 9§, 1g) [7]. Lenže finančné prostriedky prevádzkovateľov prvkov kritickej infraštruktúry sú na ochranu svojich systémov infraštruktúry obmedzené, keďže neprinášajú priame zisky [8]. Prevádzkovatelia by si mali byť vedomí hrozieb, či rizík a stanoviť ich význam podľa priority závažnosti. **Cieľom príspevku** je poukázať na koncepciu manažmentu rizík a krízového manažmentu prevádzkovateľov prvkov kritickej infraštruktúry v Nemecku a vyzdvihnúť proces tvorby manažmentu rizika kritickej infraštruktúry na Slovensku. Ucelená koncepcia manažmentu rizika na Slovensku, by pomohla prevádzkovateľom prvkov kritickej infraštruktúry ľahšie spracovať hodnotenie rizík, ktoré by im slúžilo ako základ pre vykonávanie cieľených opatrení na ochranu kritickej infraštruktúry.

1 KRITICKÁ INFRAŠTRUKTÚRA V EURÓPE

V podmienkach Európy sa problematika ochrany prvkov kritickej infraštruktúry dostáva do popredia záujmu celej spoločnosti. Európska únia so svojim svetovým postavením a veľkým množstvom obyvateľov musí taktiež dbať na ochranu najdôležitejších infraštruktúr jednotlivých štátov. Spoločným cieľom Európskej rady a Európskej komisie bolo vypracovanie Európskeho programu na ochranu kritickej infraštruktúry (European Programme for Critical Infrastructure Protection) a Výstražnej informačnej siete kritickej infraštruktúry (Critical Infrastructure Warning Information Network). Výsledkom spolupráce členských štátov bolo vypracovanie Zelenej knihy o európskom programe na ochranu kritickej infraštruktúry.

Ochrana najdôležitejšej infraštruktúry proti terorizmu 2005 (Critical Infrastructure Protection in the fight against terrorism) je prvý ucelený dokument Európskej únie na ochranu kritickej infraštruktúry. Má charakter celkovej stratégie a okrem vymenovania sektorov a kritérií na určovanie prvkov obsahuje i návrhy na zlepšenie prevencie, pripravenosti a reakcie na teroristické útoky [9].

V decembri roku 2008 prijala Európska únia (EÚ) Smernicu Rady o identifikácii a označení európskych kritických infraštruktúr a zhodnotenia potreby zlepšiť ich ochranu. (2008/114 ES z 8. Decembra 2008) [10]. Smernica ukladá primárnu a konečnú zodpovednosť za ochranu európskej kritickej infraštruktúry členským štátom a vlastníkom/prevádzkovateľom tejto infraštruktúry. Smernica upravuje povinnosti a postup pre každý členský štát pri identifikácii európskej kritickej infraštruktúry, ktoré spĺňajú tri prierezové a sektorovo špecifické kritéria. Súčasne stanovuje prierezové kritériá a podsektory energetiky a dopravy, na

ktoré sa smernica osobitne vzťahuje. Nevylučuje sa však jej aplikácia aj na ostatné identifikované sektory členskými štátmi [11].

Medzi prierezové kritéria patria [10]:

- kritérium straty na životoch (posudzované v zmysle možného počtu mŕtvych alebo zranených osôb),
- kritérium hospodárskeho vplyvu (posudzované v zmysle závažnosti hospodárskych strát a /alebo zhoršenia výrobkov alebo služieb, zahŕňa aj potenciálny vplyv na životné prostredie),
- kritérium vplyvu na verejnosť (posudzované v zmysle vplyvu na dôveru obyvateľstva, fyzického utrpenia a narušenia každodenného života, zahŕňa aj stratu základných služieb).

Jednotlivé štáty v Európe sú pri budovaní kompletného systému kritickej infraštruktúry rozlične ďaleko. Každý štát si uvedomuje, že zavedenie a ochrana kritickej infraštruktúry je nevyhnutná. V niektorých krajinách EÚ existujú rôzne formy spolupráce z pohľadu štátu, kde jednotlivé ministerstvá alebo iné orgány štátnej správy nesú zodpovednosť za príslušnú oblasť kritickej infraštruktúry a taktiež existujú rôzne formy spolupráce štátneho a súkromného sektora.

2 KONCEPCIA MANAŽMENTU RIZIKA A KRÍZOVÉHO MANAŽMENTU V PROCESE OCHRANY PRVKOV KRITICKEJ INFRAŠTRUKTÚRY V NEMECKU

V Nemecku celá spoločnosť, ako aj vláda preukazuje záujem o bezpečnosť infraštruktúry. Podľa nemeckej ústavy je úlohou štátu zaručiť verejnú bezpečnosť a poriadok a zaistiť, aby populácia bola zabezpečená základnými potrebami. Kritickými sú označované organizácie a zariadenia dôležitého významu pre štát a pri ich výpadku alebo narušení môže nastať buď trvalé narušenie zásobovania, vážne narušenie verejnej bezpečnosti, alebo vzniknú iné dramatické následky. Celková zodpovednosť za aktivity v oblasti ochrany kritickej infraštruktúry leží na Spolkovom ministerstve vnútra, ktoré je spoločne s niekoľkými štátnymi úradmi zodpovedné za zaistenie vnútornej bezpečnosti Nemecka [12].

V Nemecku bola vytvorená príručka „Ochrana kritickej infraštruktúry – Riziko a krízový manažment“ (Schutz Kritischer Infrastrukturen – Risiko und Krisenmanagement) ako spoločný produkt účastníkov z oblasti podnikania, štátnej správy a akademických inštitúcií. Príručka predstavuje koncept manažmentu rizika a krízového manažmentu a je navrhnutá ako nástroj samohodnotenia (sebaanalýza) pre prevádzkovateľov prvkov KI či vládne inštitúcie. Hlavný význam príručky spočíva v tom, aby organizácie a vládne inštitúcie dokázali samostatne efektívne a účinne riadiť riziká, v snahe znížiť vplyvy externých faktorov na prvky kritickej infraštruktúry a tým zlepšiť pripravenosť na potenciálnu krízu pomocou preventívnych opatrení [13].

Pre prevádzkovateľov prvkov kritickej infraštruktúry je dôležité, aby si uvedomovali potenciálne riziká a taktiež príčiny, ktoré ich vyvolávajú. To znamená, mali by identifikovať a znižovať riziká s dostatočným predstihom a byť pripravení na potenciálnu krízu. Včasná identifikácia rizík dáva väčšiu pripravenosť prevádzkovateľom prvkov KI na mimoriadne udalosti a zvládanie krízových situácií. Organizáciám to pomáha zabezpečiť stabilnú prevádzku, zvýšiť tvorbu hodnôt a vládny inštitúciám plniť svoje poslanie poskytovať životne dôležité služby. V príručke „Ochrana kritickej infraštruktúry – Riziko a krízový manažment“ sa koncepcia manažmentu rizika a krízového manažmentu pre prevádzkovateľov KI skladá z piatich fáz [13]:

Fáza 1: Plánovanie (predbežné plánovanie) v organizácii.

Dôkladná príprava plánovania vytvára nevyhnutné podmienky pre úspešné vykonávanie manažmentu rizika v organizácii a aplikovanie stanovených pokynov v príručke. Táto fáza pozostáva z nasledujúcich krokov:

- stanovenie úloh manažmentu rizika a krízového manažmentu v organizácii,
- určenie zodpovednosti za realizáciu manažmentu rizika,
- vyčlenenie zdrojov na realizáciu,
- objasnenie právnych povinností pri zavedení manažmentu rizika a krízového manažmentu,
- definovanie strategických cieľov ochrany prvkov prevádzkovateľov kritickej infraštruktúry,
- zabezpečiť komunikáciu o rizikách v rámci celej organizácie.

Fáza 2: Analýza rizík.

Analýza rizík predstavuje štruktúrovaný prehľad jednotlivých procesov, potenciálnych hrozieb a zraniteľnosti procesov. Kombináciou týchto informácií poskytuje analýza rizík podklady pre všetky kritické procesy v jednotlivých scenároch. Výsledky analýzy rizík sa môžu porovnať s vopred stanovenými strategickými cieľmi na ochranu kritickej infraštruktúry a príslušne ich hodnotiť, aby bolo možné ľahšie vyzdvihnúť význam a dôležitosť rizík. Ak nie je možné dosiahnuť väčšinu strategických cieľov ochrany kritickej infraštruktúry, musia sa prijať konkrétne opatrenia na zníženie existujúcich rizík, čo uľahčí samostatný proces riešenia krízy. Táto fáza pozostáva z nasledujúcich krokov:

- analýza kritickosti,
- identifikácia rizík – analýza hrozieb a tvorba scenárov, analýza zraniteľnosti, kvantifikácia rizík, porovnanie a hodnotenie rizík.

Fáza 3: Preventívne opatrenia a stratégie.

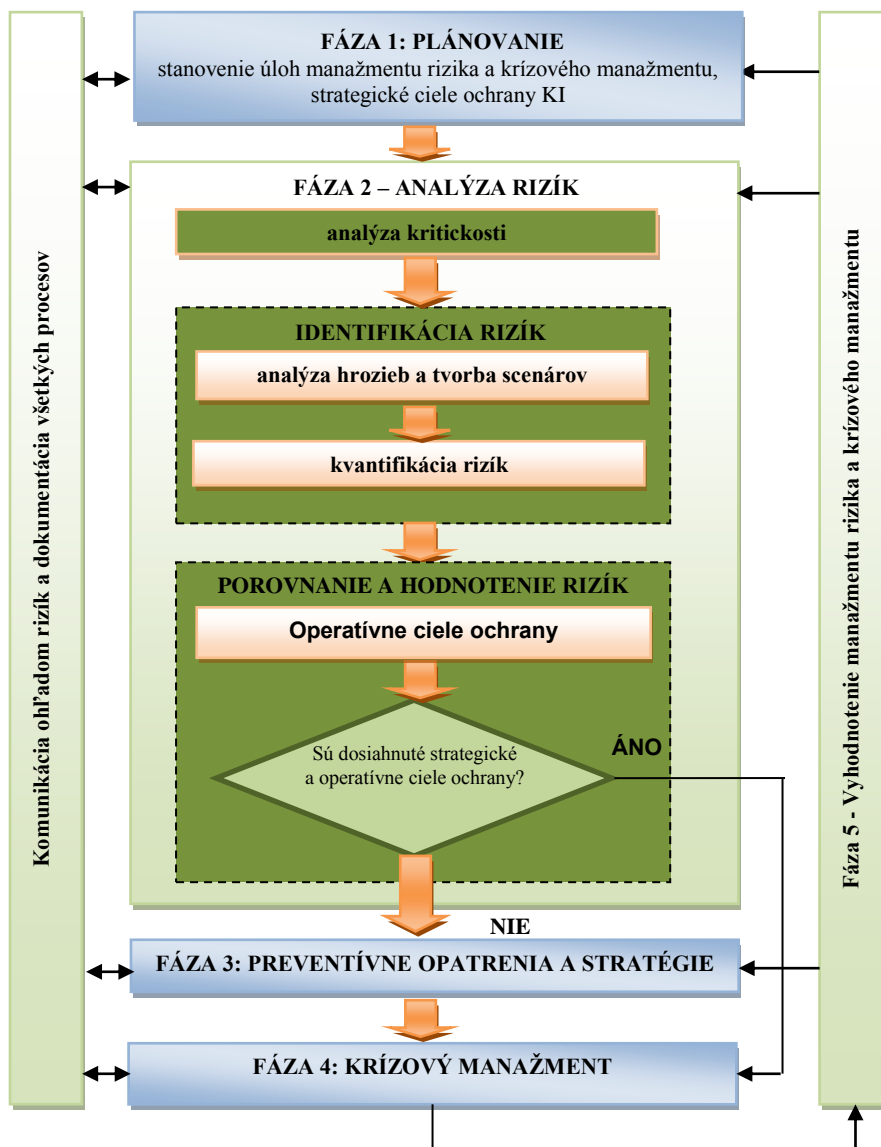
Organizácie, ktoré sa snažia byť viac odolné voči krízam, by mali vytvárať preventívne opatrenia prispievajúce k zníženiu rizík procesov a tým aj produktov. Preventívne opatrenia by mali byť zamerané hlavne na aktívnu ochranu dôležitých zložiek v rámci celej organizácie. Potrebné je si uvedomiť, že vyhýbaniu sa nebezpečenstvu zvyčajne so sebou nesie určitý nedostatok flexibility pre organizáciu alebo štátny orgán. Prenos rizika neznižuje ohrozenie zdravia, ale zabezpečí len finančnú náhradu, aj keď to môže byť podstatne nižšie ako skutočné vzniknuté škody spôsobené v jednotlivých prípadoch. Táto fáza pozostáva z nasledujúcich krokov:

- zníženie rizika,
- vyhýbanie sa riziku (averzia k riziku),
- presun rizika (transfer rizika),
- prijatie rizika (akceptovateľné riziká).

Fáza 4: Krízový manažment.

Ak v organizácii dôjde k vážnemu poškodeniu akéhokoľvek druhu, napriek uskutočneným preventívnym opatreniam, krízový manažment by mal stanoviť štruktúru pre riešenie krízovej situácie. Krízový manažment zahŕňa špeciálne štruktúry a postupy, ktoré sa líšia od bežnej prevádzky v organizácii. Počas krízy je rozhodovací orgán centralizovaný a schopný rýchlo reagovať vhodným spôsobom na vzniknutú situáciu. To umožňuje znížiť dopady krízy a skrátiť čas potrebný na obnovenie bežnej prevádzky.

**KONCEPCIA:
OCHRANA KRITICKEJ INFRAŠTRUKTÚRY – RIZIKO A KRÍZOVÝ MANAŽMENT**



Obr. 1

Koncepcia: Ochrana kritickej infraštruktúry – Riziko a krízový manažment
(upravené podľa zdrojového dokumentu) [13]

Táto fáza pozostáva z nasledujúcich krokov:

- 1 *Stanovenie štruktúry krízového manažmentu:*
 - krízový plán,
 - organizačná štruktúra pre krízový manažment: krízový štáb, krízový manažér štábu, členovia krízového štábu, odborný poradca krízového štábu,
 - postupy, varovanie, krízová komunikácia,
 - priestory pre krízový štáb.
- 2 *Proces krízového riadenia a zvládnutie krízy:*
 - zber informácií a hodnotenie,
 - posúdenie situácie, rozhodovanie a realizácia opatrení,
 - kontrola – monitoring,
 - zabezpečenie nepretržitej prevádzky,
 - návrat k normálnej prevádzke,
 - dokumentácia o činnostiach krízového riadenia.
- 3 *Následné preventívne opatrenia.*

Fáza 5: Vyhodnotenie manažmentu rizika a krízového manažmentu.

Hodnotenie sa vzťahuje na všetky fázy manažmentu rizika a krízového manažmentu. Vychádza z opatrení stanovených v strategických cieľoch ochrany prvkov prevádzkovateľov kritickej infraštruktúry v prvom kroku prípravy plánovania. Hodnotí sa význam stanoveného rizikového profilu organizácie a overuje sa účinnosť realizovaných preventívnych opatrení rovnako ako aj krízového manažmentu v organizácii. Takéto hodnotenia by mali byť pravidelne vykonávané. Ďalšie hodnotenia môžu byť potrebné:

- po realizácii opatrení,
- po rozšírení organizácie alebo zmene organizácie (reštrukturalizácii),
- v prípade zmeny stavu ohrozenia (zmena v bezpečnostnej situácii).

V Nemecku je väčšia časť infraštruktúry súkromne prevádzkovaná a spolu s vládou sa snažia zabezpečiť účinnú ochranu prvkov kritickej infraštruktúry. V rámci tejto spolupráce pomáhajú súkromným firmám rôzne bezpečnostné orgány v oblasti poradenstva, poskytujú špecifické odporúčania na stanovenie preventívnych opatrení. Na druhej strane súkromný sektor prispieva svojimi odbornými znalosťami a praktickými skúsenosťami.

3 KONCEPCIA MANAŽMENTU RIZIKA V PROCESSE OCHRANY PRVKOV KRITICKEJ INFRAŠTRUKTÚRY NA SLOVENSKU

Aj v slovenských podmienkach musia prevádzkovatelia prvkov kritickej infraštruktúry hodnotiť riziká a pripraviť súbor opatrení, čím si vytvoria základné predpoklady na úspešné riadenie rizika v celej organizácii. V procese aplikovania manažmentu rizika pri ochrane prvkov kritickej infraštruktúry je nevyhnutné rešpektovať hlavné zásady a postupnosť krokov. Na Slovensku je možné koncepciu manažmentu rizika v procese ochrany prvkov kritickej infraštruktúry realizovať podľa nasledujúcich krokov:

1. Zabezpečiť podporu štátu pri realizácii manažmentu rizika v procese ochrany kritickej infraštruktúry.

Pri aplikovaní manažmentu rizika na Slovensku je nevyhnutné, aby Európska komisia a Európsky parlament, vláda SR a jednotlivé ministerstvá, ako aj vrcholový manažment dotknutých podnikateľských subjektov podporovali proces uplatňovania zásad manažmentu

rizik na úseku ochrany kritickéj infraštruktúry. Dôležitá je aktívna trvalá podpora štatutárnych zástupcov dotknutých organizácií [3, 6].

2. Zabezpečiť podporu vrcholového manažmentu v procese ochrany kritickéj infraštruktúry.

Na úrovni vrcholového manažmentu je nevyhnutné vypracovať filozofiu znižovania rizik narušenia prevádzkyschopnosti prvkov kritickéj infraštruktúry a zvyšovania úrovne ich ochrany. Zároveň musí byť vo vedení organizácií dosiahnutý konsenzus a všetci vedúci zamestnanci musia zásady manažmentu rizik v problematike ochrany kritickéj infraštruktúry plne podporovať. Na ich uskutočnenie je potrebné vyčleniť nevyhnutné finančné zdroje a zabezpečiť nevyhnutnú prípravu zamestnancov.

Predpokladom pre úspešné zavedenie manažmentu rizika v procese ochrany prvkov kritickéj infraštruktúry je potrebné [3, 14]:

- informovať všetkých manažérov i výkonných zamestnancov s vypracovanou koncepciou ochrany prvkov KI,
- prepojiť manažment rizika s podnikovou kultúrou prevádzkovateľa prvkov KI,
- vytvoriť tím, ktorého členom bude člen vrcholového manažmentu zodpovedný za internú komunikáciu v otázkach uplatňovania politiky manažmentu rizika,
- zvyšovať povedomie o nevyhnutnosti manažmentu rizika a vytvoriť podmienky na komunikáciu v celej organizácii o riadení rizik,
- získať zručnosti zamestnancov v manažmente rizika buď prostredníctvom konzultantov, alebo vzdelávaním a špeciálnou odbornou prípravou,
- zabezpečiť primerané motivačné nástroje, medzi ktoré je možné zaradiť možnosti uznania, rôzne druhy ocenení, ale aj sankcií.

3. Vytvoriť koncepciu manažmentu rizika v procese ochrany kritickéj infraštruktúry.

Každý prevádzkovateľ prvkov kritickéj infraštruktúry musí jednoznačne definovať vzťah medzi zameraním a obsahom manažmentu rizika v procese ochrany prvkov kritickéj infraštruktúry a strategickým plánom organizácie, ako aj rozsah problémov, na ktoré je táto činnosť zameraná. Dôležité je tiež vytvoriť zásady a procesy posudzovania výkonnosti organizácie v nadväznosti na účinnosť riadenia rizik. V rámci plnenia týchto úloh je potrebné integrovať proces manažmentu rizik s plánovacími činnosťami a zdokumentovať realizovaný proces, prijaté rozhodnutia a plánované činnosti [15].

Pri aplikácii manažmentu rizika v procese ochrany prvkov kritickéj infraštruktúry na konkrétne podmienky je dôležité [3]:

- stanoviť ciele, ktoré sa majú dosiahnuť a zdôvodniť význam manažmentu rizika v organizácii,
- definovať akceptovateľné riziká v konkrétnych podmienkach organizácie,
- určiť postupy realizácie manažmentu rizika pre každý prvok kritickéj infraštruktúry, ale aj pre každý úsek činnosti organizácie, každý program, projekt alebo každý postup realizačného tímu,
- stanoviť osobnú zodpovednosť za manažment rizika,
- stanoviť štruktúru a obsah nevyhnutnej dokumentácie na podporu opatrení krízového manažmentu,
- vytvoriť účinné kontrolné mechanizmy, nástroje monitorovania pri preskúmaní rizik, aby bolo možné priebežne hodnotiť zmeny priebehu posudzovaných rizik a tým aj účinnosť procesu manažmentu rizika,
- zabezpečiť aktuálnosť politiky zavádzania manažmentu rizika v neprestajne sa meniacich podmienkach. To umožňuje preskúmanie predchádzajúcich rozhodnutí, ako aj monitorovaných rizik.

V súčasnosti na Slovensku neexistuje všeobecne záväzný predpis, ktorý by sa komplexne zaoberal problematikou ochrany prvkov kritickej infraštruktúry. Pri realizácii manažmentu rizika môžu prevádzkovatelia prvkov v rámci procesu ochrany kritickej infraštruktúry vychádzať zo všeobecných zásad stanovených normou - Manažérstvo rizika STN ISO 31 000: 2011. V tejto norme sú fázy procesu manažmentu rizika nasledujúce [16]:

- posúdenie súvislosti v procesoch a ich významu pre daný subjekt,
- identifikovanie rizík,
- analyzovanie rizík,
- hodnotenie rizík,
- minimalizovanie (zníženie, prípadne odstraňovanie) rizík,
- oboznámenie dotknutých osôb a subjektov so zostatkovými rizikami,
- priebežné kontrolovanie (monitorovanie) úrovne rizík.

Pre prevádzkovateľov prvkov kritickej infraštruktúry by mal byť manažment rizika súčasťou celého manažmentu organizácie, ktorého cieľom je zabezpečiť bezpečnosť a stabilitu riadeného systému, analýzu možných ohrození a hľadanie vhodných korekčných opatrení na minimalizáciu negatívnych vplyvov. Manažment rizika by mali prevádzkovatelia chápať ako systematický prístup k práci s rizikom pri využití rôznych nástrojov a metód manažmentu rizika.

Ochrana prvkov kritickej infraštruktúry na Slovensku je zložitá úloha, ktorá nie je zatiaľ komplexne riešená a uspokojivo zabezpečená. Táto problematika je postupne riešená legislatívnymi opatreniami, ako aj skúmaním a prehlbovaním ich teoretickej podstaty. Samotné bezproblémové fungovanie a plnenie stanovených funkcií prvkami kritickej infraštruktúry je dané ich stabilitou, ktorá je založená na odolnosti, spoľahlivosti, pružnosti reakcie na krízové situácie a schopnosťou obnovy. Okrem toho si to vyžaduje zabezpečenie ich komplexnej ochrany [3].

ZÁVER

Manažment rizika na úrovni prevádzkovateľov prvkov kritickej infraštruktúry musí byť integrovaný so strategickým plánovaním a manažérskymi procesmi v organizáciách. V rámci toho je nevyhnutné určiť postup manažmentu rizika na úrovni prevádzkovateľa vzhľadom na jeho osobitosti. Uvedený postup manažmentu rizika či už v Nemecku alebo na Slovensku by mal byť zameraný na mieru uplatňovania zásad manažmentu rizík v rámci daného prvku KI, t.j.: na identifikáciu rizík aktuálnych pre organizáciu, analýzu a hodnotenie týchto rizík, tvorbu opatrení na zníženie prípadne odstránenie posúdených rizík a priebežné kontrolovanie úrovne rizík. Efektívne monitorovanie a preskúmavanie procesov manažmentu rizika je nevyhnutné vykonávať priebežne, pretože riziká, ktoré ohrozujú bezpečnosť prvkov KI, nie sú statické veličiny.

V Nemecku je koncepcia manažmentu rizika a krízového manažmentu v procese ochrany prvkov kritickej infraštruktúry postavená nielen na manažment rizika, ale zahŕňa aj kroky krízového manažmentu. Ide o širšie rozpracovaný dokument, ktorý presne definuje postupnosť krokov prevádzkovateľov ako aplikovať manažment rizika v procese ochrany prvkov kritickej infraštruktúry a v prípade väčšieho rozsahu zraniteľnosti ako aplikovať krízový manažment v organizácii. Na Slovensku je zatiaľ čiastočne rozpracovaná iba koncepcia manažmentu rizika v procese ochrany prvkov kritickej infraštruktúry na úrovni rôznych verejných publikácií autorov, ktorí sa tejto problematike venujú. Prínosom článku je vyzdvihnúť koncepciu manažmentu rizík a krízového manažmentu prevádzkovateľov prvkov kritickej infraštruktúry vytvorenú v Nemecku, ktorá môže poslúžiť odborníkom pre kritickú

infraštruktúru na Slovensku ako podklad pre tvorbu širšieho rozpracovania koncepcie manažmentu rizika a krízového manažmentu v procese ochrany prvkov kritickej infraštruktúry.

Résumé

Risk management on the level of operators of the elements of critical infrastructure must be integrated with strategic planning and management processes in organizations. It is necessary to determine the risk management process at the level of the operator with respect to its peculiarities. This procedure of risk management in Germany or Slovakia should be focused with mentioned by of the principles of risk management within the element of critical infrastructure i.e. to identify the current respect of organization and assess evaluate these risk, take measured actions to reduce or eliminate the risk assessment and continuous control of risk. It is necessary to monitor and review the risk management process because risks that threaten the safety elements of critical infrastructure are not static variables.

The concept of risk management and crisis management in the process of protection of critical infrastructure elements in Germany is not constructed on risk management but also includes the steps of crisis management. In Slovakia is only partially elaborated the concept of risk management in the process of protection of critical infrastructure elements. This issue is in process by authors at various government publications. The objective of this article is to point out the method of risk management and crisis management of operators of the elements of critical infrastructure in Germany, and underline the design process of risk management of critical infrastructure in Slovakia.

Článok bol spracovaný v rámci projektu APVV-0471-10, Ochrana kritickej infraštruktúry v sektore doprave, riešený na Fakulte bezpečnostného manažmentu Žilinskej univerzity v Žiline.

Literatúra

- [1] NEDELIÁKOVÁ, E., J. SEKULOVÁ a I. NEDELIÁK. Reduction of transport risks at rail level crossings. In: *Transport means 2015: proceedings of the 19th international scientific conference*. Kaunas: Kaunas University of Technology, 2015, s. 236–239. ISSN 1822-296X.
- [2] LEITNER, B., Z. DVOŘÁK a E. SVENTEKOVÁ. Nový študijný program „Bezpečnosť a ochrana kritickej infraštruktúry“ – charakteristika programu a aktuálne výzvy. In: *Riešenie krízových situácií v špecifickom prostredí*. Žilina: Žilinská univerzita, 2015, s. 313–320. ISBN 978-80-554-1022-7.
- [3] ŠIMÁK, L. a kol. *Ochrana kritickej infraštruktúry v sektore dopravy*. Žilina: Žilinská univerzita v Žiline/ EDIS – vydavateľstvo ŽU v Žiline, 2012. ISBN 978-80-554-0625-1.
- [4] MINISTERSTVO VNÚTRA SR. *Ochrana kritickej infraštruktúry* [online]. [cit. 2015-08-12]. Dostupne na: <http://www.minv.sk/?ochrana-kritickej-infrastruktury>
- [5] MINISTERSTVO VNÚTRA SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [online]. [cit. 2015-09-08]. Dostupne na: www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691
- [6] MINISTERSTVO VNÚTRA SR. *Národný program pre ochranu a obranu kritickej infraštruktúry* [online]. [cit. 2015-17-07]. Dostupne na: www.minv.sk/?ochrana-kritickejinfrastruktury&subor=10692
- [7] Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v Slovenskej republike.

- [8] HUDÁKOVÁ, M. a K. BUGANOVÁ. Analýza súčasného systému financovania ochrany kritickej infraštruktúry v SR. *Podniková ekonomika a manažment*. 2012, č. 3, s. 155–163. ISSN 1336-5878.
- [9] EUROPEAN COMMISSION 1. *Communication from the commission to the council and the European parliament – Critical Infrastructure Protection in the fight against terrorism* [online]. Brusel, 2004 [cit. 2015-09-12]. Dostupné na: <http://eurlex.europa.eu>
- [10] EUROPEAN COMMISSION 2. *Council decision on a Critical Infrastructure Warning Information Network* [online]. [cit. 2015-09-12]. Dostupné na: <http://eurlex.europa.eu/>
- [11] VIDRIKOVÁ, D. a K. BOC. *Ochrana kritickej infraštruktúry 1. časť*. Žilina: Žilinská univerzita v Žiline/ EDIS – vydavateľstvo ŽU v Žiline, 2013. ISBN 978-80-554-0654-1.
- [12] VIDRIKOVÁ, D., K. BOC a K. ŠKATULIAKOVÁ. Possible approach to protection of critical infrastructure element in transport sector. *MEST journal*. 2014, Vol. 2, no. 1, s. 103–115. ISSN 2334-7058.
- [13] *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement* [online]. [cit. 2015-09-09]. Dostupné na: http://www.verfassungsschutz.brandenburg.de/media_fast/4055/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf
- [14] LEITNER, B. a L. JANUŠOVÁ. Postup na identifikáciu potenciálnych prvkov kritickej infraštruktúry v podsektore železničná doprava. In: *Krízový manažment*. Žilina: Fakulta bezpečnostného inžinierstva Žilinskej univerzity v Žiline. 2015, roč. 14, č. 2, s. 5–13. ISSN 1336-0019.
- [15] NOVÁK, L. Úvod do krízového plánovania. In: *Riešenie regionálnych disparít a nerovnovážnych stavov v prírodnom a hospodárskom prostredí*. Odbor krízového manažmentu a bezpečnosti štátu Úradu vlády SR, Bratislava: MERKURY, 2007, s. 350–355. ISBN 978-80-89143-55-9.
- [16] STN ISO 31000: 2011. *Manažérstvo rizika. Zásady a návod*. Bratislava: Slovenský ústav technickej normalizácie, 2011.