ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA ŠPECIÁLNEHO INŽINIERSTVA

KRÍZOVÝ MANAŽMENT - 2/2013

KRITICKÁ ANALÝZA PRÍSTUPOV K PROBLEMATIKE OCHRANY KRITICKEJ INFRAŠTRUKTÚRY V SLOVENSKEJ REPUBLIKE

CRITICAL ANALYSIS APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION IN THE SLOVAK REPUBLIC

Dagmar VIDRIKOVÁ[1], Kamil BOC[2]

SUMMARY:

The aim of this article is analyze the current state of critical infrastructure protection in the Slovak Republic. This article also contains a proposal how to design a security plan for protection of critical infrastructure element that has national significance. It is designed the procedure of the security environment analysis, which is an important part of the security plan. It also respects and applies existing scientific knowledge in this area and also the requirements of the Act on Critical Infrastructure. The authors also designed this procedure of the security environment analysis on the basis of broad spectrum of opinion academia and experience of central government.

KEYWORDS: *critical infrastructure, critical infrastructure protection, sector, critical infrastructure element, security plan, security environment, analysis, security, Act on Critical Infrastructure*

ÚVOD

Kritická infraštruktúra – pojem, ktorý v ostatnom období rezultuje na pôde akademickej či ústredných orgánov štátnej správy na národnej i nadnárodnej (Európskej) úrovni. Jej ochrana sa často spája s terorizmom či inými spoločensky nežiaducimi javmi alebo aktivitami, ktoré môžu mať za následok narušenie alebo zničenie jej prvku alebo jeho zariadenia. V súčasnosti sa v Slovenskej republike (ďalej len „SR“) často stretávame s vedením polemiky medzi ústrednými orgánmi štátnej správy či členmi akademickej obce dotýkajúcej sa najmä identifikácie prvku systému kritickej infraštruktúry. Aj napriek tomu, že zákon č. 45/2011 Z. z. o kritickej infraštruktúre jednoznačne takýto prvok identifikuje (spĺňa sektorové a prierezové kritériá), napriek tomu významnejší posun v tejto oblasti SR nedosiahla. Stojí za úvahu hľadať príčiny tejto stagnácie. Veď tejto oblasti sa s prestávkami venujú dotknuté ústredné orgány štátnej správy pod koordináciou Ministerstva vnútra SR už od roku 1999 (zriadené „*Koordinačné centrum pre bezpečnosť národnej infraštruktúry*“, angl. CPNI - *Centre for the Protection of National Infrastructure*, ktorého základnou úlohou bolo rozvíjať a koordinovať činnosti potrebné na ochranu kritickej infraštruktúry), príp. od roku 2002 kedy zákonom č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov boli identifikované objekty osobitnej dôležitosti (*strategické objekty obrannej infraštruktúry, ktorých poškodenie alebo zničenie obmedzí zabezpečenie obrany štátu*) a ďalšie dôležité objekty (*objekty obrannej infraštruktúry, ktorých poškodenie alebo zničenie obmedzí činnosť ozbrojených síl alebo chod hospodárstva Slovenskej republiky*). Síce identifikované boli len objekty dôležité pre obranu, ale aj tieto svojím významom patria medzi prvky systému kritickej infraštruktúry. V čom teda spočívajú alebo čo je zdrojom retardačných faktorov, ktoré bránia SR významnejšiemu pokroku v tejto oblasti? Máme za to, že jedným z možných dôvodov môže byť aj otázka reálneho určenia prvku kritickej infraštruktúry a jeho ochrana. Objekty osobitnej dôležitosti i ďalšie dôležité objekty zaradené do obrannej infraštruktúry majú praktickú identifikáciu vyriešenú. Aj keď sú

[1] Dagmar Vidriková, Ing., PhD., Katedra technických vied a informatiky Fakulty špeciálneho inžinierstva Žilinskej univerzity v Žiline, Ul. 1. mája č. 32, 01026 Žilina, tel.: 041513-6860, e-mail: Dagmar.Vidrikova@fsi.uniza.sk.
[2] Kamil Boc, Ing., PhD., Katedra bezpečnostného manažmentu Fakulty špeciálneho inžinierstva Žilinskej univerzity v Žiline, Ul. 1. mája č. 32, 01026 Žilina, tel.: 041513-6660, e-mail: Kamil.Boc@fsi.uniza.sk.

súčasťou systému kritickej infraštruktúry, riadia sa osobitným právnym predpisom, a teda zákon o kritickej infraštruktúre sa ich dotýka len okrajovo. Identifikácii ostatných prvkov kritickej infraštruktúre mali napomôcť zákonom o kritickej infraštruktúre stanovené sektory v pôsobnosti ústredných orgánov štátnej správy SR. Ich ochrana by mala byť zameraná najmä na štátom stanovené bezpečnostné hrozby. Pre ilustráciu je vhodné posúdiť prístup k ich identifikácii v niektorých štátoch Európskej únie.

1. OCHRANA KRITICKEJ INFRAŠTRUKTÚRY V ZAHRANIČÍ

Pre ilustráciu prístupu k ochrane prvkov kritickej infraštruktúry boli zvolené výberovo len niektoré štáty. Medzi ne patrí USA, ktorých praktické i teoretické skúsenosti sa stali prameňom epistemiologického prístupu tvorby európskych i národných právnych aktov. Vybrané boli aj niektoré štáty Európskej únie, ktorých historický či spoločenský vývoj bol obdobný ako v SR, alebo na ktoré je ekonomicky naviazaná. Predovšetkým ide o Českú republiku, Spolkovú republiku Nemecko a Maďarskú republiku. Mohli byť skúmané prístupy aj ostatných štátov, ale pre účel sledovaný týmto článkom by mali postačovať aj tieto štáty.

1.1. SPOJENÉ ŠTÁTY AMERICKÉ (USA)

Kritická infraštruktúra v Spojených štátoch amerických a Austrálii[3] patrí k jednej z najprepracovanejších kritických infraštruktúr sveta. Rovnako tak, USA a Austrália sú prvými štátmi, ktoré začali pracovať na tvorbe kritickej infraštruktúry a vnímať jej dôležitosť pre fungujúcu spoločnosť. V USA už v roku 1996 bolo vydané Vládne nariadenie č. 13010 (Executive Order 13010). Ním sa ustanovuje Prezidentská komisia na ochranu kritickej infraštruktúry (PCCIP - President s Commission on Critical Infrastructure Protection). Jej úlohou bolo radiť a informovať prezidenta o rozsahu a povahe zraniteľnosti a hrozieb kritickej infraštruktúry so zameraním na fyzické a kybernetické hrozby) [1].

Základným dokumentom, ktorý ako prvý ustanovil kritickú infraštruktúru v USA je Smernica č. 63 *(Presidential decision directive No.63*) [2], ktorá stanovila sektory kritickej infraštruktúry

- informácie a komunikácia,
- bankovníctvo a financie,
- zásobovanie vodou,
- doprava (letectvo, diaľnice, potrubná preprava, železničnej, vodná a pod.),
- verejná správa,
- záchranné služby,
- zdravotníctvo,
- energetika.

Po teroristickom útoku na Svetové obchodné centrum v New Yorku dňa 11. septembra 2001 prezident Bush prijal v októbri roku 2001 ďalšie Vládne nariadenie č. 13228 *(Executive Order 13228)* [3], ktoré svojím obsahom nadväzovalo na teroristické útoky. V roku 2002 bol vydaný „Zákon o národnej bezpečnosti“ (*Homeland Security Act*) [4], ktorý ustanovil ministerstvo národnej bezpečnosti (DHS - Department of Homeland Security). V tom istom roku bol vydaný dokument „Národná stratégia vnútornej bezpečnosti“ (*NSHS-National Strategy for Homeland Security*). V tejto stratégii je preformulovaná definícia kritickej infraštruktúry, ktorá bola pôvodne definovaná v „USA Patriot Act of 2001“ (*Title VII: Increased information sharing for critical infrastructure protection) a súčasne* rozširuje sektory kritickej infraštruktúry o poľnohospodárstvo a potraviny, o chemický priemysel a nebezpečné látky, obranný priemysel, o poštové služby a lodnú dopravu. Následné vládne nariadenia spresňujú jednotlivé podsektory identifikovanej kritickej infraštruktúry. Napríklad:

- Prezidentská smernica č. 7 z roku 2003 (*HSPDA - Homeland Security Presidential Directive*) [5].
- Národná stratégia pre ochranu kritickej infraštruktúry a kľúčových aktív (*NSPP - The National Strategy for The Physical Protection of Critical Infrastructure and Key Assets*) [6], definuje aj 3 kľúčové aktíva, ktorými sú národné a kultúrne pamiatky a monumenty národnej hrdosti, budovy a objekty nesúce národné bohatstvo a ekonomickú silu štátu, vládne budovy a verejná správa.
- Národný plán ochrany kritickej infraštruktúry (*NIPPO - National Infrastructure Protection Plan*), vydaný v roku 2006, člení systém kritickej infraštruktúry na 17 sektorov [7],
- Stratégia na ochranu kyberpriestoru (*The National Strategy to Secure Cyberspace, NIPPO s Cyber Security Plan*) [8].
- Národný plán ochrany kritickej infraštruktúry z roku 2009 (*National Infrastructure Protection Plan – NIPP 2009*) upravuje počet sektorov kritickej infraštruktúry na 18. [9].

[3] V tomto kontexte je pre ilustráciu uvádzaná aj Austrália, ktorá zaujíma v ochrane prvkov KI prioritné postavenie.

NIPP 2009 stanovuje zodpovednosť jednotlivých ústredných orgánov štátnej správy za obranu sektorov. Napríklad:

- ministerstvo poľnohospodárstva je zodpovedné za poľnohospodárstvo, potraviny a iné produkty ako je mäso, hydina, vajcia a pod.
- ministerstvo zdravia a sociálnych služieb je zodpovedné za všeobecné zdravie,
- ministerstvo obrany je zodpovedné aj za ochranu velenia ozbrojeným silám a riadenie obranných procedúr,
- ministerstvo energetiky zodpovedá za ochranu výroby, rafinácie, skladovanie a distribúciu ropy, plynu a elektrickej energie, s výnimkou ochrany komerčných jadrových elektrární,
- ministerstvo školstva je zodpovedné za ochranu podsektora školských zariadení v sektore verejnej správy a pod. (tabuľka 1).

Z vyššie uvedeného vyplýva, že zo strany zodpovedných orgánov je venovaná zvýšená pozornosť za ochranu kritickej infraštruktúry. Jej ochrana je pod priamym riadením prezidenta USA. Svedčí o tom napríklad aj obsah rozhovorov počas návštevy prezidenta Číny v USA (napr. otázka bezpečnosti kyberpriestoru, kyberterorizmus, činnosť čínskych hackerov proti spoločnostiam USA) začiatkom júna 2013.

Tabuľka 1

Sektory a kľúčové prvky kritickej infraštruktúry v USA

Sektory a kľúčové prvky kritickej infraštruktúry v USA		
	Poľnohospodárstvo a potravinárstvo	Agriculture and Food
	Obranný priemysel a vojenské základne	Defense Industrial Base
	Energie	Energy
	Verejné zdravie a starostlivosť o zdravie	Public Health and Healthcare
	Národné a kultúrne pamiatky a monumenty	National Monuments and Icons
	Finančné služby	Financial Services
	Pitná voda a čističky odpadových vôd	Drinking Water and Water Treatment Systems
	Chemický priemysel	Chemical
	Komerčný priemysel	Commercial Facilities
	Vodné priehrady	Dams
	Záchranné a pohotovostné služby	Emergency Services
	Jadrové reaktory, materiály a odpady,	Nuclear Reactors, Materials, and Waste
	Informačné technológie	Information Technology
	Telekomunikácie	Communications
	Pošta a preprava zásielok (poštové služby)	Postal and Shipping
	Dopravné systémy	Transportation Systems
	Vládne zariadenia	Government Facilities

Zdroj: autori podľa [10].

1.2. VÝVOJ KRITICKEJ INFRAŠTRUKTÚRY V NIEKTORÝCH ŠTÁTOCH EURÓPY

Spomedzi európskych štátov sa ako prvá zaoberala otázkami týkajúcimi sa ochrany kritickej infraštruktúry Veľká Británia. V roku 1999 zriadila Koordinačné centrum pre bezpečnosť národnej infraštruktúry (CPNI-Centre for the Protection of National Infrastructure). Základnou úlohou CPNI bolo rozvíjať a koordinovať činnosti potrebné na ochranu kritickej infraštruktúry.

Európska únia so svojim svetovým postavením a počtom obyvateľov dbá na ochranu najdôležitejších infraštruktúr jednotlivých štátov. Teroristické útoky na Madrid a Londýn

zdôraznili hrozbu terorizmu. Reakciou zo strany Európskej únie bolo vypracovanie niekoľkých dokumentov. V nich bola riešená prevencia, pripravenosť a reakcie na hrozby ohrozujúce kritickú infraštruktúru so zameraním najmä na hrozbu terorizmu. Medzi rozhodujúce patrí vypracovanie Európskeho programu na ochranu kritickej infraštruktúry *(European Programme for Critical Infrastructure Protection, ďalej len „EPCIP“*) a Varovnej informačnej siete kritickej infraštruktúry (*Critical Infrastructure Warning Information Network*, ďalej len „CIWIN“). Po pripomienkach členských štátov Európskej únie (ďalej len „EÚ“) i dotknutých priemyselných združení bola v roku 2005 Komisiou Európskych spoločenstiev (ďalej len „Komisia“) vypracovaná Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry (ďalej len „Zelená kniha“).

Obsahom Zelenej knihy sú alternatívne možnosti, ktoré môže Komisia využiť na zavedenie EPCIP a CIWIN. Spresňuje, že cieľom EPCIP je zaistiť, aby v celej EÚ existovali rovnaké úrovne ochranného zabezpečenia najdôležitejšej infraštruktúry, ktorá by obsahovala čo najmenej slabých miest a rýchle a overené mechanizmy obnovy. Úroveň ochrany by pritom nemala byť pre všetky prvky rovnaká, ale odvodená od možného dopadu, ktorý by mohol spôsobiť zlyhanie. EPCIP by mal zabezpečovať:

a) úplná ochrana pred nebezpečenstvami každého druhu,
b) ochrana pred nebezpečenstvami každého druhu so zameraním na terorizmus,
c) ochrana pred nebezpečenstvom terorizmu.

Poškodenie alebo zničenie časti infraštruktúry v jednom členskom štáte môže mať nepriaznivý vplyv na niekoľko ďalších členských štátov i na európsku ekonomiku ako celok. Toto je čoraz pravdepodobnejšie, nakoľko informačno-komunikačné technológie a liberalizácia trhu (napr. pri dodávkach elektrickej energie a plynu) spôsobujú, že mnoho typov infraštruktúry sú súčasťou väčšej siete. Pri takýchto situáciách sú ochranné opatrenia silné len natoľko, ako ich najslabší článok. To znamená, že potrebu jednotnej úrovne ochrany EPCIP navrhol spoločný rámec opatrení na horizontálnej úrovni dopĺňajúci existujúce sektorové kritériá a zoznam definícií a sektorov najdôležitejšej infraštruktúry. Prvkami spoločného rámca sa stali:

- spoločné zásady ochrany najdôležitejšej infraštruktúry,
- spoločne dohodnuté kódy/normy,
- spoločné definície, na základe ktorých možno dohodnúť špecifické definície pre jednotlivé sektory,
- spoločný zoznam sektorov najdôležitejšej infraštruktúry,
- prioritné oblasti ochrany najdôležitejšej infraštruktúry,
- opis zodpovedností príslušných zainteresovaných subjektov,
- dohodnuté referenčné kritériá,
- metodika pre porovnanie infraštruktúry v rôznych sektoroch a stanovenie priorít.

Osobitný význam má Smernica Rady 2008/114/ES (ďalej len „Smernica Rady“), ktorá upravuje povinnosti a postup pre každý členský štát pri identifikácii prvkov Európskej kritickej infraštruktúre (ďalej len „EKI“), ktoré spĺňajú tri prierezové a sektorovo špecifické kritériá. Súčasne stanovila prierezové kritériá a podsektory energetiky a dopravy. Nevylučuje aplikáciu aj na ostatné členskými štátmi identifikované sektory. Prierezovými kritériami sa stali:

- *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).

Súčasne každému členskému štátu, na území ktorého sa nachádza potenciálna EKI, bola uložená najmä povinnosť:

a) zapojiť do dvojstranných a/alebo viacstranných rokovaní ostatné členské štáty, ktoré môžu byť výrazne ovplyvnené potenciálnou EKI,
b) zabezpečiť ich ochranu formou bezpečnostných riešení, ktorých cieľom je zaručiť funkčnosť, kontinuitu a integritu kritickej infraštruktúry za účelom odvrátiť, zmierniť a neutralizovať hrozbu, riziko alebo zraniteľné miesto.

Zavedené bezpečnostné riešenia na ochranu EKI musia byť obsiahnuté v bezpečnostnom pláne alebo v jeho ekvivalente. Postup vypracovania a obsah bezpečnostného plánu pre EKI (*The operator security plan*, ďalej len „OSP“) je smernicou taxatívne

upravený. Každý členský štát disponujúci EKI má:

1. Identifikovať zložky kritickej infraštruktúry EKI a bezpečnostné riešenia, ktoré existujú alebo sa zavádzajú na ich ochranu.
2. Posúdiť, či každá označená EKI, ktorá sa nachádza na území členského štátu, má OSP alebo či sú pre ňu zavedené rovnocenné opatrenia.
3. Ak sa zistí, že takýto OSP alebo jeho ekvivalent existuje a pravidelne sa aktualizuje, žiadne ďalšie vykonávacie opatrenia nie sú potrebné.
4. Ak sa zistí, že sa takýto OSP alebo jeho ekvivalent nevypracoval, prostredníctvom akýchkoľvek opatrení, ktoré považuje za vhodné zabezpečí, aby sa OSP alebo jeho ekvivalent vypracoval.
5. Zabezpečiť, aby sa OSP alebo jeho ekvivalent zaviedol do jedného roka od označenia kritickej infraštruktúry za EKI a následne pravidelne prehodnocoval [13].

EÚ boli v strategických dokumentoch identifikované nasledujúce kľúčové hrozby:

1. Terorizmus.
2. Šírenie zbraní hromadného ničenia.
3. Regionálne konflikty.
4. Zlyhanie fungovania štátu.
5. Organizovaná trestná činnosť.

Uvedené hrozby sa viac-menej dotýkajú každého členského štátu EÚ a teda aj jeho kritickej infraštruktúry. Smernica nevylučuje identifikáciu a zaradenie národných hrozieb a bezpečnostných rizík dotýkajúcich sa prvkov systému EKI či národných prvkov kritickej infraštruktúry. Súčasne vytvára štátom EÚ dostatočné právne prostredie na vypracovanie vlastných všeobecne záväzných právnych predpisov upravujúcich identifikáciu a ochranu sektorov a prvkov kritickej infraštruktúry.

Právna záväznosť sa dotýka určovania a ochrany prvkov EKI. Jednotlivé štáty EÚ na smernicu reagovali rôzne. Niektoré prijali osobitné zákony, niektoré zatiaľ smernicu hlbšie nerozpracovali. Pre ilustráciu uvádzame len niektoré štáty EÚ a ich prístup k naplneniu smernice.

Fínsko

Vo Fínsku sú sektory a politika ochrany kritickej infraštruktúry definované v dokumentoch s názvom „Security of Supply Act" a v "Decree of the National Emergency Supply Agency of 1992". Ide o vládne dokumenty determinujúce oficiálne ciele pre rozvoj spoľahlivosti dodávok, ktoré sú každých 5 až 6 rokov novelizované. Od roku 2008 je kritická infraštruktúra definovaná podrobnejšie.

V súčasnosti kritickú infraštruktúru tvorí:

- energetická sieť a zásobovanie,
- elektronické informačné a komunikačné systémy, vrátane komunikačných sietí, informačné technológie, systémy elektronických masmédií, platobných režimov bánk a poisťovní,
- doprava, logistické systémy,
- zásobovanie vodou a iné miestne zariadenia,
- výstavba infraštruktúry a zariadení,
- finančná služba,
- zásobovanie potravinami,
- zdravotná služba,
- médiá [14].

Vláda Fínska sa zameriava na tú časť kritickej infraštruktúry, ktorá ochraňuje spoločnosť. Vo Fínsku existuje päť kľúčových úradov zaoberajúcich sa kritickou infraštruktúrou. Ide o:

- The Finnish Communications Regulatory Authority (FICORA) zaradené pod ministerstvom dopravy a spojov, ktoré zaisťuje informačné náležitosti, rovnako ako technologické regulácie a štandardizácie.
- The National Emergency Supply Agency (NESA) pracujúce pod dohľadom ministerstva obchodu a priemyslu, ktoré analyzuje hrozby a riziká vo vzťahu k prvkom kritickej infraštruktúry.
- NESA – administratívno – operatívny úrad pre zaistenie spoľahlivosti dodávok do Fínska. Slúži pre rozvoj spolupráce medzi verejným a súkromným sektorom v oblasti ekonomickej pripravenosti, koordinácie prípravy so štátnou správou a pre rozvíjanie a udržiavanie spoľahlivosti dodávok.
- The Steering Committee for Data Security in State Administration (VAHTI) je skupina expertov pracujúcich pod ministerstvom financií, ktorá vytvára politiku a zaisťuje praktických sprievodcov pre zaistenie bezpečnosti informačných systémov.
- National Emergency Supply Council (NESC) bola založená v roku 1955; pracuje pod dohľadom ministerstva zamestnanosti a ekonomiky. Jej úlohou je plánovať a koordinovať činnosti v prípade vzniku mimoriadnych udalostí. Súčasne analyzuje hrozby v oblasti zaistenia bezpečnosti dodávok a plánuje opatrenia v prípade ich vzniku.

Francúzsko

Vo Francúzsku sú za kritické považované všetky sektory, ktoré slúžia na zaistenie základných sociálnych a ekonomických procesov. Medzi tieto kritické sektory patria:

- financie,
- priemysel,
- energetika,
- súdnictvo,
- verejné zdravotníctvo,
- práca národných civilných autorít,
- elektronické komunikačné, audiovizuálne médiá a informačné technológie,
- dopravné systémy,
- zásobovanie vodou,
- potraviny,
- vesmír a výskum,
- ozbrojené sily.

Francúzsky regulačný rámec týkajúci sa kritickej infraštruktúry je pravidelne aktualizovaný. Jeho prístup je založený na riadení rizík, plánov prevencií a odozvy. Do procesu zdieľania informácií je zapojený národný výbor, medzirezortná komisia a zástupcovia obrany a bezpečnosti. Zástupcovia sektorov kritickej infraštruktúry (je ich 12) museli vypracovať národnú bezpečnostnú smernicu. Pre každý prvok kritickej infraštruktúry boli operačné bezpečnostné plány rozpracované do jednotlivých ochranných plánov.

Taliansko

V Taliansku bolo vydaných množstvo stratégií, v ktorých sú definované sektory kritickej infraštruktúry. Sú považované za kritické, aj keď nikde neexistuje žiadny oficiálny zoznam. Ide o tieto sektory:

- bankovníctvo a financie,
- verejná bezpečnosť a poriadok,
- telekomunikácie,
- pohotovostné služby,
- výroba energie, doprava a distribúcia,
- verejná správa,
- systém zdravotnej starostlivosti,
- doprava a logistika,
- voda,
- informačné služby a médiá,
- zásobovanie potravinami.

Kľúčovými ministerstvami zaoberajúcimi sa ochranou kritickej infraštruktúry sú ministerstvo vnútra a ministerstvo pre inovácie a technológie. Rovnako ministerstvo pre komunikácie vyvíja aktivity pre zlepšenie ochrany informačných a komunikačných sietí. Pre zlepšenie ochrany kritickej infraštruktúry (ďalej len „KI“) na všetkých úrovniach spolupracujú verejné organizácie so súkromným sektorom. Najdôležitejšou organizáciou v oblasti ochrany kritickej infraštruktúry je Spoločnosť talianskych expertov pre kritickú infraštruktúru (*Association of Italian Experts for Critical Infrastructures- AIIC*).

Maďarsko

Maďarsko sa zapojilo do Európskeho programu na ochranu kritickej infraštruktúry v roku 2005. Definícia ochrany kritickej infraštruktúry v Maďarsku sa zhoduje s definíciou kritickej infraštruktúry v EÚ, tak ako je formulovaná v Zelenej knihe. Sektory ochrany KI zahŕňajú:

- informačné a komunikačné systémy,
- energetiku,
- zásobovanie vodou,
- dopravu,
- verejné zdravotníctvo,
- zásobovanie potravinami,
- bankovníctvo a finančný sektor,
- priemysel,
- vládne inštitúcie,
- verejnú bezpečnosť a ochranu štátu.

Nemecko

V Nemecku vláda, ako aj celá spoločnosť preukazuje svojím konaním, že sú závislé na bezpečnej infraštruktúre. Za kritické prvky infraštruktúry sú zadefinované tie organizácie a zariadenia, ktoré by v prípade zlyhania alebo poškodenia spôsobili významné narušenie verejného poriadku alebo iné nepriaznivé následky pre veľkú časť populácie. 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. Za kritické sektory v Nemecku sú považované:

- energetika,
- zásobovanie (voda, potraviny, zdravotná starostlivosť, núdzové a záchranné služby),
- telekomunikačné a informačné technológie,
- doprava a obchod,
- nebezpečné materiály,
- bankovníctvo a financie, vládne agentúry,
- štátna správa a súdnictvo,

- médiá, výskumné inštitúcie a kultúrne hodnoty.

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.

Poľsko

Poľsko považuje za kritickú infraštruktúru také hmotné a kybernetické systémy, ktoré sú podstatné na zaistenie nutného minima pre operácie v ekonomike a vláde. V Poľsku je kritická infraštruktúra definovaná nasledovne „*Ide o systémy a s nimi spojené funkčné objekty, objekty stavebné, zariadenia, inštalácie, kľúčové služby pre bezpečnosť štátu a občanov slúžiace k zaisteniu fungovania orgánov štátnej správy, inštitúcií a podnikateľov*“. Kritická infraštruktúra je upravená Národným programom ochrany KI z roku 2013 [36]. Zahŕňa:

- informačno-komunikačné technológie,
- bankový a finančný sektor,
- zdravotnícky sektor,
- dopravu,
- záchranné služby – núdzové služby,
- zaistenie funkčnosti verejnej správy,
- zásobovanie vodou a potravinami,
- dodávky energie a palív,
- skladovanie chemických a rádioaktívnych látok,
- produktovody nebezpečných látok.

Za sektory kritickej infraštruktúry zodpovednosť dve ministerstvá – ministerstvo pre vedu a vyššie vzdelanie a ministerstvo vnútra [14].

Česká republika

Počiatočné činnosti, ktoré boli vykonávané v Českej republike (ďalej len „ČR“), v rámci kritickej infraštruktúry, sa predovšetkým orientovali na ochranu počítačových sietí, a to aj v súvislosti s uznesením Bezpečnostnej rady štátu č. 123 z roku 2000 (ďalej len „BRS“). Nasledovali ďalšie dokumenty nelegislatívneho charakteru ako napríklad:

- Správa o riešení problematiky kritickej infraštruktúry v Českej republike (schválená uznesením Bezpečnostnej rady štátu z 3. júla 2007 č. 30),
- Harmonogram ďalšieho postupu spracovania dokumentov „Komplexná stratégia Českej republiky na riešenie problematiky kritickej infraštruktúry a Národného programu ochrany kritickej infraštruktúry“ (schválený uznesením vlády z 25. februára 2008 č. 170 v znení uznesenia vlády z 2. marca 2009 č. 222) a
- Komplexná stratégia Českej republiky na riešenie problematiky kritickej infraštruktúry a Národný program ochrany kritickej infraštruktúry (schválené uznesením vlády z 22. februára 2010 č. 140) [15].

Analýzou problematiky ochrany prvkov kritickej infraštruktúry a jej väzieb s krízovým riadením, so súčasnou nadväznosťou na Smernicu Rady Česko pristúpilo k legislatívnej úprave ochrany kritickej infraštruktúry. Ňou bolo prijatie novelizácie zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. [16] Prierezové a sektorové kritériá boli upravené nariadením vlády č. 432/2010 Sb. [17].

Podľa nariadenia prierezovým kritériom na určenie prvku kritickej infraštruktúry je hľadisko:

a) obetí s limitnou hodnotou viac ako 250 mŕtvych alebo viac ako 2.500 osôb s následnou hospitalizáciou po dobu dlhšiu ako 24 hodín,
b) ekonomického vplyvu s limitnou hodnotou hospodárskej straty štátu vyššia ako 0,5% hrubého domáceho produktu, alebo
c) vplyvu na verejnosť s limitnou hodnotou rozsiahleho obmedzenia poskytovania nevyhnutných služieb alebo iného závažného zásahu do každodenného života postihujúceho viac ako 125.000 osôb.

Odvetvové kritériá sú konkretizované v Prílohe uvedeného nariadenia pre jednotlivé sektory. ČR identifikovala 9 sektorov kritickej infraštruktúry a 19 podsektorov. Ide o nasledujúce sektory a podsektory:

- Energetika (elektrina, zemný plyn, ropa a ropné produkty).
- Vodné hospodárstvo.
- Potravinárstvo a poľnohospodárstvo (rastlinná, živočíšna a potravinárska výroba).
- Zdravotníctvo.
- Doprava (cestná, železničná, letecká a vnútroštátna vodná doprava).
- Komunikačné a informačné systémy (technologické prvky pevnej a mobilnej siete elektronickej komunikácie a siete pre rozhlasové a televízne vysielanie; technologické prvky pre satelitnú

komunikáciu, pre poštové služby a prvky informačných systémov).
- Finančný trh a mena.
- Núdzové služby (Integrovaný záchranný systém, radiačné monitorovanie, predpovedná, varovná a hlásna služba).
- Verejná správa (verejné financie, sociálna ochrana a zamestnanosť, ostatná štátna správa, spravodajské služby) [17].

Dôvodom konkretizácie sektorov a podsektorov kritickej infraštruktúry identifikovanej v ČR je ilustrácia prístupu ústredných orgánov štátnej správy k tejto problematike. Výkon štátnej správy v oblasti ochrany kritickej infraštruktúry ako súčasti krízového riadenia zohráva Ministerstvo vnútra a Česká národní banka. [16] Zaujímavé je, že Česko bez výraznejších administratívnych prieťahov dokázalo jednoznačne identifikovať prvky kritickej infraštruktúry a jej ochranu ako súčasť krízového riadenia.

V rámci naplnenia právnych predpisov upravujúcich kritickú infraštruktúru v roku 2011 boli vykonané bilaterálne rokovania medzi vládou Česka a susednými štátmi za účelom identifikovania prvkov EKI. Určených bolo 8 prvkov v sektore energetiky. V ostatných sektoroch nebol určený žiadny prvok EKI. Uznesením vlády č. 934 zo dňa 14.12.2011 bol schválený zoznam 103 prvkov kritickej infraštruktúry ktorých prevádzkovateľom je organizačná zložka štátu. [18]. Zaujímavo a inšpirujúco pôsobí, že zoznam prvkov kritickej infraštruktúry bol podľa dislokácie odovzdaný dotknutým hasičským záchranným zborom jednotlivých krajov. Vyplýva to aj z ich postavenia spracovateľov krízových plánov krajov a krízových plánov obcí s rozšírenou pôsobnosťou. V súčasnej dobe v súlade s uvedením uznesením vlády je vykonávaná aktualizácia prvkov kritickej infraštruktúry, ktoré patria pod gesciu organizačnej zložky štátu. Okrem týchto prvkov, Česko vyčlenilo ďalšie prvky kritickej infraštruktúry, ktoré nepatria pod štátnu správu. Označuje ich ako prvky kritickej infraštruktúry, ktorých prevádzkovateľom nie je organizačná zložka štátu. Umožňuje to platný krízový zákon. V súčasnej dobe je evidovaných 1277 prvkov kritickej infraštruktúry, ktorých prevádzkovateľom nie je organizačná zložka štátu. Podľa pripravovanej aktualizácie je možné predpokladať, že v Česku bude celkom 88 prvkov kritickej infraštruktúry, ktorých prevádzkovateľom je organizačná zložka štátu a uvádzaných 1277, ktorých prevádzkovateľom nie je organizačná zložka štátu [15].

Pre ilustráciu uvádzame počet prvkov kritickej infraštruktúry vo vyčlenených sektoroch
a) Energetika 0/295 (elektrina - 0/202,zemný plyn 0/0, ropa a ropné produkty 0/93).
b) Voda (0/11).
c) Doprava (0/13) (cestná – 0/2, železničná 0/8, letecká 0/3).
d) Komunikačné a informačné systémy 4/865 (elektronická komunikácia - 0/710, technologické prvky pre poštové služby – 0/155, technologické prvky k IS – 0/4).
e) Finančný trh a mena 0/74.
f) Núdzové služby 35/19 (IZS -33/19, radiačné monitorovanie 1/0, predpovedná, varovná a hlásna služba 1/0).
g) Verejná správa 64/0 (verejné financie – 5/0, sociálna ochrana a zamestnanosť – 33/0,po úprave 18/0, ostatná štátna správa – 24/0, spravodajské služby 2/0).[4]

V sektoroch potravinárstvo a zdravotníctvo nebol určený žiadny prvok kritickej infraštruktúry.

Z uvedeného vyplýva, že počet prvkov kritickej infraštruktúry, ktorých prevádzkovateľom nie je organizačná zložka štátu je až 94,1740%. Inšpirujúco pôsobia prierezové kritériá, ktoré významným spôsobom umožnili určovanie prvkov kritickej infraštruktúry.

2. OCHRANA KRITICKEJ INFRAŠTRUKTÚRY V SLOVENSKEJ REPUBLIKE

V SR je problematike ochrany kritickej infraštruktúre venovaná pozornosť, ako bolo v úvode konštatované, už od roku 1999. Do súčasnej doby je to takmer 14 rokov. Výsledok toľko ročného úsilia je však mizivý. Prijaté vládne dokumenty vyvrcholili len zákonom o kritickej infraštruktúre z roku 2011. Zákon veľmi dôsledne a podrobne implementoval Smernicu Rady. Aj keď svojím spôsobom má nedostatky, stal sa všeobecne záväzným predpisom pre všetky dotknuté subjekty. Jeho realizácia v praxi však naráža na rôzne problémy. Pozitívne je možné hodnotiť aspoň určenie sektorov kritickej infraštruktúry a návod na určenie prvku kritickej infraštruktúry, určenie zodpovednosti prevádzkovateľa, ako aj návod na spracovanie bezpečnostného plánu. Jeho realizácii však bráni absencia vykonávacej vyhlášky. Určitú nejasnosť vyvoláva určenie sektorov kritickej infraštruktúry. Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike (ďalej len „Národný program“) [33]

[4] 0/2 - znamená počet prevádzkovateľov OZŠ/počet prevádzkovateľov, ktorí nie sú OZŠ. (OZŠ – organizačná zložka štátu).

prijatý v roku 2007 určil nasledujúcich deväť sektorov kritickej infraštruktúry: *Voda, Potraviny, Zdravie, Energetika, Informačné a komunikačné technológie, Doprava, Verejný poriadok a vnútorná bezpečnosť, Priemysel, Finančný sektor.* Zákon o kritickej infraštruktúre [32] prijal osem modifikovaných sektorov. Z Národného programu prevzal takmer všetky sektory okrem sektorov *Verejný poriadok a vnútorná bezpečnosť, Potraviny a Finančný sektor.* Zoznam rozšíril o sektory *Elektronické komunikácie a Pošta.*

Za účelom overenia si praktického spôsobu chápania citlivých KI a jej sektorov vyššie uvedených štátov a SR bola vykonaná ich komparácia. Cieľom komparácie bolo zistiť či jednotlivé uvádzané štáty, ktorých bezpečnostné ohrozenia a sociálno-ekonomické podmienky sú v porovnaní so SR si podobné. Súčasne sme chceli identifikovať rovnaké alebo blízke sektory KI ako identifikovala SR. Porovnanie sektorov kritickej infraštruktúry vyplýva z tabuľky 2.

Tabuľka 2

Sektory kritickej infraštruktúry v niektorých štátoch EÚ

P.č.	Sektory KI	*Fínsko*	*Francúzsko*	*Taliansko*	*Maďarsko*	*Nemecko*	*Poľsko*	*Česko*	*Slovensko*
1.	Bankovníctvo a finančný sektor	👍	👍	👍	👍	👍	👍	👍	👍
2.	Priemysel	👍	👍		👍				👍
3.	Energetika	👍	👍	👍	👍	👍	👍	👍	👍
4.	Verejné zdravotníctvo	👍	👍	👍	👍	👍	👍	👍	👍
5.	Vládne inštitúcie, bezpečnosť a ochrana štátu	👍	👍	👍	👍	👍	👍	👍	
6.	IKT a telekomunikačné systémy	👍	👍		👍	👍	👍	👍	👍
7.	Dopravné a logistické systémy	👍	👍	👍	👍	👍	👍	👍	👍
8.	Zásobovanie vodou	👍	👍	👍	👍	👍	👍	👍	👍
9.	Potraviny	👍	👍	👍	👍	👍	👍	👍	
10.	Veda a výskum		👍			👍			
11.	Výstavba infraštruktúry a zariadení		👍						
12.	Informačné služby, médiá kult. pamiatky	👍	👍	👍		👍	👍		
13.	Záchranné a pohotovostné služby		👍			👍	👍	👍	
14.	Skladovanie nebezpečných látok					👍	👍		
15.	Pošta poštové služby								👍

Poznámka: V tabuľke nie sú uvedené všetky sektory KI štátov, ktorých porovnávanie bolo vykonané. Cieľom bolo poukázať najmä na tie sektory KI, ktoré vybrané štáty EÚ považujú na národnej úrovni za významné. Dôvodom je komparácia SR s vybranými štátmi EÚ v oblasti sektorov KI. Zámerom nebolo vymenovať všetky a presné názvy sektorov KI jednotlivých štátov.

Zdroj: autori

Z tabuľky 2 vyplýva, že prienikom sektorov vybraných štátov EÚ sú sektory týkajúce sa dopravy, bankovníctva a finančníctva, energetiky a verejného zdravotníctva. Môžeme vziať do úvahy, že prienikom je aj sektor IKT. (Taliansko nemá tento sektor výraznejšie – samostatne uvádzaný, ale je modifikovaný v iných sektoroch) a sektor Voda. Najbližším spoločným sektorom je aj Bezpečnosť štátu, tiež označovaný aj ako Verejný poriadok a vnútorná bezpečnosť. Okrem SR ostatné uvádzané štáty EÚ ho považujú za sektor kritickej infraštruktúry. Prečo zákon o kritickej infraštruktúre tento sektor vylúčil nie je známe. I keď v Národnom programe bol identifikovaný. Z analýzy bezpečnostnej situácie v priebehu štyroch rokov (od prijatia Národného programu a prijatia zákona o kritickej infraštruktúre) nevyplynuli žiadne zmeny dotýkajúce sa bezpečnostných záujmov SR či bezpečnostného prostredia SR alebo bezpečnostných hrozieb, ktoré boli identifikované v Bezpečnostnej stratégii, ktorá bola schválená Národnou radou SR 27.septembra 2005. Dá sa na základe tohto konštatovania usudzovať, že zmeny v určení sektorov neboli podmienené týmto dokumentom. Domnievame sa, že práve východiskom pri určovaní sektorov kritickej infraštruktúry nemali byť len odporúčania Smernice Rady, ale aj otázky riešené v bezpečnostnej stratégii. Za účelom zistenia možných motívov pri určovaní sektorov kritickej infraštruktúry sme hľadali kauzálne vzťahy. Jednou z možností skúmania je aj použitie zhlukovej hierarchickej aglomeratívnej analýzy metódou najbližšieho suseda. Touto metódou sme vykonali analýzu sociálno-ekonomických dát vybraných štátov EÚ v rokoch 2006-2012 (podľa aktuálnosti a dostupnosti údajov). V rámci vybraných štátov boli hodnotené dáta týkajúce sa populácie, HDP na jedného obyvateľa, účasť v Eurozóne, výška verejného dlhu, výška

ročnej inflácie, tempo rastu HDP, miera nezamestnanosti, ročná miera rastu v priemysle, spotreba elektrickej energie na obyvateľa a modálne rozdelenie nákladnej dopravy. Sme si vedomí, že nielen tieto štatistické dáta mohli ovplyvniť výber sektorov v jednotlivých štátoch. [26] Za účelom zistenia podobnosti jednotlivých štátov (s využitím uvedených sociálno-ekonomických údajov) sme zisťovali euklidovské vzdialenosti vyjadrujúce rozsah príbuznosti alebo podobnosti.

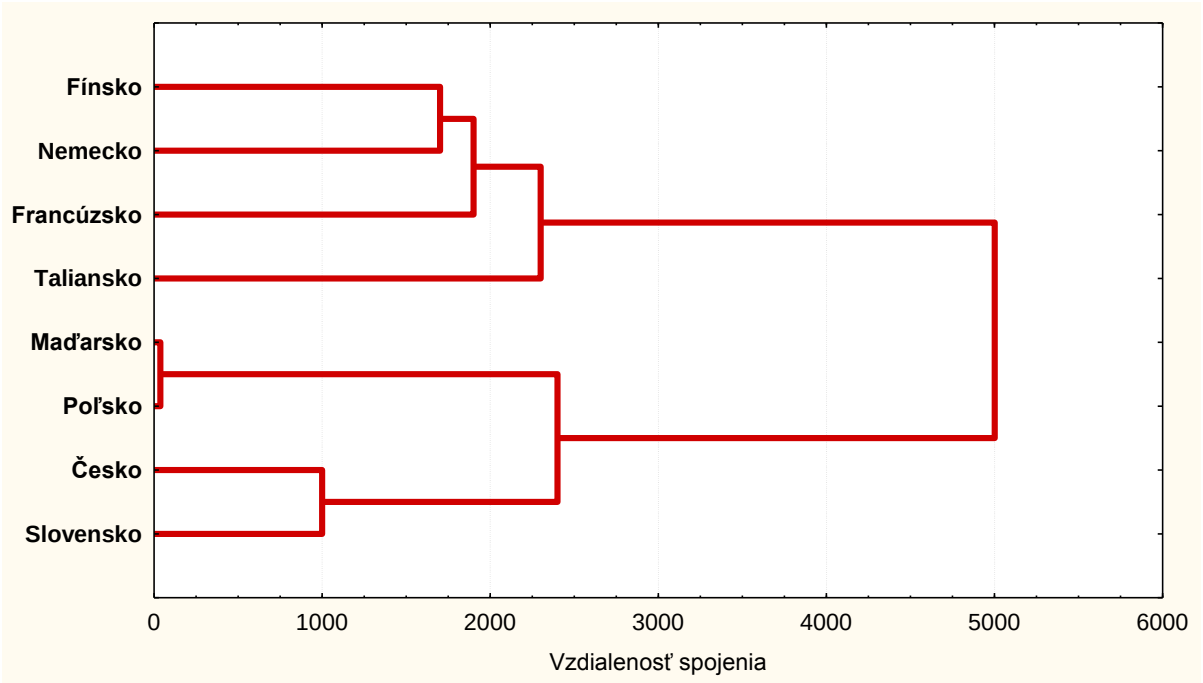
Dáta sú uvedené v tabuľke 3.

Tabuľka 3

Sociálnoekonomické dáta vybraných štátov Európskej únie

Aktualizované v r.		2012							2013-04	2011	2006/2008	2010	
Por. číslo	Štát	Populácia [v mil.]	HDP/obyv [€]	HDP/obyv (PPP) EU27=100%	Eurozóna áno/nie	Verejný dlh [% HDP]	Inflácia ročná [% HDP]	Tempo rastu HDP	Miera nezamestnanosti [%]	Ročná miera rastu v priemysle	Spotreba elektriny/obyv. [kWh]	Modálne rozdelenie nákladnej dopravy	
												cestná	železničná
1.	Fínsko	5,3	29400	115%	áno	53,0	3,2	-0,2	8,3	1,3	16,635.686	75,0	24,8
2.	Francúzsko	63,3	27500	108%	áno	90,2	2,2	0,0	11,0	1,9	7,328.281	82,2	13,5
3.	Maďarsko	10,0	16800	66%	nie	79,2	5,7	-1,7	10,6	5,5	3,690.242	75,1	19,6
4.	Taliansko	61,5	25200	98%	áno	127,0	3,3	-2,4	12,0	0,1	5,417.236	90,4	9,6
5.	Nemecko	81,4	31100	121%	áno	81,9	2,1	0,7	5,4	1,9	6,641.91	64,9	22,2
6.	Poľsko	38,2	16800	66%	nie	55,6	3,7	1,9	10,8	7,2	3,356.851	80,6	19,4
7.	Česko	10,5	20200	79%	nie	45,8	3,5	-1,3	7,2	6,4	6,020.494	79,0	21,0
8.	Slovensko	5,4	19200	75%	áno	52,1	3,7	2,0	14,5	7,2	4,828.587	74,8	22,0
9.	EÚ=27 štátov	501,0	25600	100%		85.3	2.6	-0,2	11,0	3,2		76,4	17,1

Zdroj: autori podľa [19-25]



Obrázok 1. **Zobrazenie výsledkov zhlukovej analýzy sociálno-ekonomických údajov vybraných štátov Európskej únie**

Analýza sociálnoekonomických údajov vybraných štátov EÚ a určenie euklidovských vzdialeností príbuznosti vykonaná pomocou hierarchickej zhlukovej analýzy, pozri obr.1, ukazuje, že vybraté štáty EÚ sa delia do troch základných skupín. Prvú skupinu tvoria štáty

Fínsko, Nemecko, Francúzsko a Taliansko, druhú skupinu Maďarsko a Poľsko a tretiu skupinu Česko a Slovensko. Pritom euklidovské vzdialenosti medzi druhou a treťou skupinou nie sú tak veľké. Znamená to, že Slovensko na základe vytypovaných sociálnoekonomických charakteristík má najbližšie k Česku a následne k Maďarsku a Poľsku. Z toho by sa dalo odvodiť, že aj sektory kritickej infraštruktúry by mali byť obdobné. Z tabuľky 2 však jednoznačne tento záver nevyplýva. Príčiny rozdielov je možné hľadať pravdepodobne v rozdielnej metodike prístupu určovania sektorov KI dotknutými štátnymi orgánmi. Na niektoré nedostatky upozornil aj pán P. Petrovič hlavný odborník ochrany KI z Ministerstva vnútra SR vo svojom vystúpení na 18. konferencii Riešenie špecifických situácií v špecifickom prostredí. Vo svojom vystúpení na tému „Aktuálne problémy ochrany kritickej infraštruktúry“, okrem iného, konštatoval nedostatky zákona č. 45/2011 Z. z. i na snahu rozšírenia existujúcich sektorov o vnútornú bezpečnosť, jadrové zariadenia, potraviny a financie. Teda o tie sektory, ktoré boli ostatnými k SR blízkymi štátmi identifikované.

Odhliadnuc od týchto rozdielov dôležité je nielen objektívne identifikovať sektory KI, ale aj určiť ich prvky. Avšak doteraz nie sú známe jednotlivé prierezové kritériá, podľa ktorých by sa mohli určiť prvky KI po jednotlivých sektoroch a teda ani počet prvkov KI. Je možné predpokladať, že aj napriek zatiaľ nejednoznačnému prístupu SR k ochrane KI sa v krátkej budúcnosti tento stav zlepší. Podľa Plánu práce Bezpečnostnej rady SR na rok 2013 [27] mal byť v na 51. zasadnutí dňa 20. marca prerokovaný dokument pod názvom „Hodnotenie zabezpečenia ochrany prvkov kritickej infraštruktúry“. Pred samotným prerokovaním bol podpredsedom vlády SR a ministrom vnútra SR stiahnutý. Dôvody je možné hľadať v jeho obsahu. Napríklad v materiáli za sektor dopravy je, okrem iného, konštatované, že v oblasti cestnej dopravy neboli určené žiadne prvky kritickej infraštruktúry. Podľa názoru spracovateľov sa pri posudzovaní následkov rozrušenia existujúcich cestných objektov preukázalo, že hustota cestnej siete SR umožňuje variantný výber obchádzkových trás prípadných miest rozrušenia. V prípade zničenia niektorého z nich budú prepravné potreby s časovým zdržaním zabezpečené a závažnejšie negatívne neobmedzia život občanov SR a chod hospodárstva. Takéto konštatovanie je neprijateľné a je aj v rozpore s doterajším naším skúmaním či poznaním prístupu napríklad Českej republiky pri ochrane tohto sektora. Pravdepodobným dôvodom uvedeného konštatovania bolo, že by prípadná snaha o zvýšenie úrovne bezpečnosti objektov na cestnej sieti (napr. mostov, tunelov, estakád) s využitím technických prostriedkov alebo fyzickej ochrany, tak ako sa v dokumente uvádza:„...mohla byť považovaná za neefektívne vynakladanie finančných prostriedkov...“ Obdobné stanoviská a prístup k určovaniu prvkov KI v sektore doprava sa týkal aj železničnej, vodnej či leteckej dopravy. V oblasti bezpečnosti alebo ochrany leteckej dopravy sa spracovatelia odvolávali na letecký zákon [28], či na zákony upravujúce činnosť na dráhach [29-31]. Uvedené zákony však upravujú najmä technologickú bezpečnosť a bezpečnosť riadenia železničnej prepravy. Identifikujú bezpečnostné indikátory nehôd a mimoriadnych udalostí či požiadavky na systém riadenia bezpečnosti (Príloha č. 8 a č. 10 k [29]). Poňatie ochrany tak, ako vyplýva z ducha zákona o kritickej infraštruktúry, v nich absentuje. Inými slovami, nie je akceptovateľné odvolávanie sa na existujúce špeciálne zákony upravujúce prevádzkovú bezpečnosť napríklad dráh, a pritom nerešpektovať požiadavky zákona o kritickej infraštruktúre, ktorý nastoľuje nové bezpečnostné štandardy ochrany prvkov KI v identifikovaných sektoroch. Rozdielne poznanie o existencii prvkov KI v sektore doprava má Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiliny. Na základe riešenia vedeckého projektu APVV - 0471-10 s názvom „Ochrana kritickej infraštruktúry v sektore doprava“ bola vedeckými metódami preukázaná existencia týchto prvkov ako aj potreba ich ochrany.

Z riadených rozhovorov s dotknutými osobami zodpovednými za niektoré sektory KI vyplynulo, že nemajú predstavu ako vypracovať bezpečnostný plán ochrany určeného prvku KI. V Prílohe č. 2 k [32] je síce naznačený obsah plánu, ale jeho vypracovanie si vyžaduje hlbšie odborné vedomosti. V tomto smere vidíme významný priestor pre našu akademickú pôdu.

3. ANALÝZA BEZPEČNOSTNÉHO PROSTREDIA PRVKU KRITICKEJ INFRAŠTRUKTÚRY

Spracovaniu bezpečnostného plánu ochrany prvku KI predchádza analýza bezpečnostného prostredia (bezpečnostná analýza). Jej význam spočíva v zistení reálneho stavu ochrany prvku KI (objektu) a existencie negatívnych javov, ktoré majú alebo

potenciálne môžu mať bezpečnostný význam pre jeho ochranu alebo jej časti. Vytvára potrebné predpoklady pre identifikáciu chráneného záujmu, bezpečnostných rizík, či návrhu komplexu opatrení na dosiahnutie požadovanej úrovne jeho ochrany predchádzajúcej alebo zamedzujúcej jeho narušeniu alebo zničeniu.

Obsahom bezpečnostného plánu prvku KI je:
1. Bezpečnostná analýza obsahujúca, okrem iného, určenie dôležitých zariadení prvku (aktíva), popis a vyhodnotenie možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku.
2. Výber trvalých a mimoriadnych bezpečnostných opatrení na jeho ochranu.
3. Určenie hlavných bezpečnostných opatrení.

Nevylučuje sa, že výber a určenie hlavných bezpečnostných opatrení môžu tvoriť jednu súčasť plánu.

3.1 BEZPEČNOSTNÁ ANALÝZA

Cieľom bezpečnostnej analýzy je vyhodnotenie podmienok a vplyvov vonkajšieho i vnútorného prostredia majúcich bezpečnostný význam pre ochranu prvku KI (chránený záujem). Ňou sa identifikuje existencia relevantných bezpečnostných rizík vonkajšieho i vnútorného prostredia chráneného záujmu, ich príčiny alebo zdroje. Posudzuje sa významnosť, pravdepodobnosť vzniku (aktivizácie) bezpečnostného rizika, jeho dôsledky, ako aj úroveň dostatočnosti realizovaných opatrení na predchádzanie alebo zníženie dôsledkov aktivizovaných bezpečnostných rizík. Pred vykonaním vlastnej analýzy je potrebné stanoviť si limitujúce kritériá vymedzujúce stav, ktorý bude považovaný za stav zabezpečujúci ochranu a stav, kedy bude ochrana narušená alebo nedostatočná.

Bezpečnostná analýza má písomnú formu. Obsahovo je možné ju členiť na 4 časti:
1. Analýza prvku KI.
2. Analýza vonkajšieho bezpečnostného prostredia.
3. Analýza vnútorného bezpečnostného prostredia.
4. Analýza bezpečnostných rizík.

– **Analýza prvku KI** sa vykonáva za účelom identifikácie chránených záujmov (aktív) a úrovne ich ochrany. Chráneným záujmom je tá časť prvku (entity), ktorej narušenie alebo zničenie by malo podľa európskych alebo národných sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia. Chráneným záujmom (chránené aktíva) môžu byť ľudské zdroje, technické a technologické procesy, technológie, osobné a iné citlivé informácie, informačno-komunikačné systémy alebo ich prvky, databázy, špecifický softvér, produkty alebo ich komponenty, nebezpečné látky, špecifické služby alebo činnosti a pod.

Podkladmi pre analýzu je najmä:
a) Opis objektu, ktorého obsahom sú najmä základné údaje o spoločnosti, jej sídle a ostatných používateľoch objektu, predmete podnikateľskej činnosti, riadiacej a organizačnej štruktúre (organizačný poriadok), počte a postavení osôb (zamestnanci, manažment a pod.), o chránenom záujme, urbanistickom, architektonickom a stavebno-technickom riešení stavieb chráneného objektu, ich konštrukčných častiach a použitých stavebných materiálov, prevádzkových, výrobných alebo technických alebo technologických zariadeniach, o koncepcii skladovania, riešení vnútornej dopravy a plôch pre obsluhu, organizácii údržby a opravách technických a technologických zariadeniach, pracovnej prevádzke (pracovný poriadok) a pod.
b) Charakteristika chráneného záujmu, s preukázaním splnenia európskych alebo národných sektorových a prierezových kritérií.
c) Kritériá posudzovania závažnosti dôsledkov pri ohrození chráneného záujmu, ktorými sú napríklad škody na životoch a zdraví osôb, zlyhanie manažérskych funkcií, narušenie, zastavenie alebo obmedzenie alebo zničenie chráneného záujmu alebo jeho časti, únik citlivých informácií. Správne stanovenie kritérií umožní vytvorenie poradia dôležitosti jednotlivých prvkov chráneného záujmu.
d) Hodnotenie a priorizácia chráneného záujmu. Cieľom je posúdiť a stanoviť poradie významnosti jednotlivých chránených aktív podľa ich dôležitosti v nadväznosti na závažnosť dôsledkov na uskutočňovanie hospodárskej a sociálnej funkcie štátu, na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia. Pre hodnotenie je možné využiť hodnotovú maticu za účelom zníženia subjektivity prístupu. Skúma sa ňou relácia

medzi prvkami chráneného záujmu a zvolenými kritériami. Každý prvok chráneného záujmu je hodnotený osobitne napríklad bodovou metódou (s možným využitím expertného ohodnotenia určenými odborníkmi a pod.). Obdobne, každému z kritérií sa priradí váhový koeficient v rozsahu určeného počtu relevantných kritérií. Vhodné je tiež použiť napríklad metódu Fullerovho trojuholníka. Kritérium s najvyšším počtom bodov má najvyššiu dôležitosť. V prípade rovnosti váhového koeficientu, sa dotknuté kritériá zlúčia do jedného kritéria a zaradia podľa poradia od najvyššieho váhového koeficientu k najnižšiemu. Pre prehľadnosť je vhodné výsledky spracovať graficky s využitím napríklad Paretovho diagramu. Spolu s Lorentzovou krivkou sa dá dosiahnuť prehľadné usporiadanie chráneného záujmu podľa priority či rozdeliť podľa významnosti. Dôležitosť rozdelenia chráneného záujmu podľa dosiahnutej významnosti a priority umožňuje správne identifikovať bezpečnostné riziká a vytýčiť zodpovedajúce bezpečnostné opatrenia.

– **Analýza vonkajšieho bezpečnostného prostredia** objektu ochrany má umožniť identifikáciu zdrojov bezpečnostných rizík a hrozieb, ktoré sa v prostredí nachádzajú. Osobitne sa vykonáva analýza vonkajšieho a vnútorného prostredia. Vždy sa skúma spojitosť s chráneným záujmom.

Pri analýze vonkajšieho bezpečnostného sa skúma najmä:

a) Geografická charakteristika – jej význam spočíva najmä v jednoznačnom určení zemepisnej polohy chráneného objektu, pozície k ostatným objektom (napr. intravilán, extravilán, horská oblasť, prihraničná oblasť s štátmi, ktoré nie sú v Európskom hospodárskom priestore [34]).
b) Hydrometeorologická charakteristika - z jej výsledkov sa môžu identifikovať potenciálne riziká (záplavy, snehové kalamity, požiare a pod.).
c) Demografická charakteristika, ktorá je tvorená štatistickými údajmi, získame informácie o stave (počte) a štruktúre (pohlavie, priemerný vek, národnosť, rodinný stav, prírastky, úmrtia, migrácia) obyvateľstva sídla dislokácie chráneného objektu. Môže byť doplnená aj o ukazovatele ekonomického vývoja (zamestnanosť, nezamestnanosť, mesačná mzda, priemysel, doprava, produkčné ekonomické aktivity a pod.).
d) Charakteristika protispoločenskej činnosti je tvorená sociálnymi štatistickými údajmi kriminality a priestupkov. Údaje o kriminalite sa získavajú zo štatistického systému kriminality vedeného Policajným zborom alebo z údajov poskytovaných Štatistickým úradom SR. Obsahujú údaje o trestných činoch a údaje o známych páchateľoch. Pre bezpečnostnú analýzu je potrebné vyhodnotiť údaje o jednotlivých druhoch kriminality a počte napadnutí v danom vonkajšom prostredí.

– **Cieľom analýzy vnútorného bezpečnostného prostredia** je získanie základného prehľadu o existujúcom stave a štruktúre ochrany predmetu chráneného záujmu. Štruktúra ochrany je daná zabezpečením chráneného záujmu:

a) fyzickou ochranou (ďalej len „FO"),
b) technickými bezpečnostnými prostriedkami, najmä:
   - mechanickými zábrannými prostriedkami,
   - poplachovými systémami, ktorých prvkami sú najmä:
     - elektrický zabezpečovací systém (ďalej len „EZS"),
     - kamerový bezpečnostný systém (CCTV),
     - systém kontroly a riadenia vstupov a pod.,
c) režimovými a organizačnými opatreniami.

Súčasne obsahom analýzy vnútorného bezpečnostného prostredia by mala byť aj analýza všetkých incidentov a nežiaducich udalostí, ktoré nemali charakter protispoločenského ani protiprávneho konania avšak mohli ohroziť určenie daného prvku.

Niektorý z uvedených prvkov môže absentovať. Za účelom dosiahnutia cieľa nie je dôležité či ochrana chráneného záujmu je zabezpečovaná všetkými uvedenými prvkami. Podstatné je oboznámiť sa, aké prvky sú na ochranu chráneného záujmu využívané, za akým účelom a v akej kvalite či kvantite.

Obsahom analýzy fyzickej ochrany je ustanovenie napríklad počtu vstupov /výstupov do objektu a ich charakter (osobný, pre motorové vozidlá, kombinovaný a pod.), forma a intenzita kontroly objektu (stála fyzická ochrana v pracovnej dobe, po pracovnej dobe a počas dní pracovného pokoja, kontrolovanie priebežne v rámci pochôdzkovej činnosti pracovníkom FO alebo prostriedkami CCTV).

Analýza technických bezpečnostných prostriedkov pozostáva s čiastkových analýz stavu a účinnosti:

- mechanických zábranných prostriedkov, použitých na obvodovú, plášťovú, priestorovú (vonkajšiu a vnútornú) a predmetovú ochranu,
- EZS,
- kamerového bezpečnostného systému,
- systému kontroly a riadenia vstupov.

Cieľom analýzy je posúdiť existujúci stav použitých prostriedkov a ich prielomovú odolnosť určenú podľa všeobecne záväzných právnych predpisov alebo platných STN.[5]

Výstupom analýzy technických bezpečnostných prostriedkoch by malo byť zhodnotenie ich (ne)dostatočnosti (stupňa spôsobilosti) chrániť predmet záujmu v poňatí účinnosti mechanických zábran a včasnosti signalizácie odhalenia nežiaducich alebo neočakávaných javov.

Analýza organizačných a režimových opatrení spočíva v posúdení rozsahu, obsahu a účinnosti prijatých interných normatívnych aktov upravujúcich personálnu alebo informačnú alebo požiarnu alebo administratívnu bezpečnosť, BOZP, ochranu osobných údajov, ochranu utajovaných skutočností, krízové a havarijné plány, kľúčový režim, systém fyzickej ochrany a pod. Posudzuje sa najmä úroveň dosiahnutia bezpečnostného štandardu stanoveného všeobecne právnymi predpismi[6].

Analýza nežiaducich javov a udalostí má za cieľ identifikovať všetky relevantné skutočnosti, ktoré by mohli ovplyvniť funkčnosť prvku. Analýza sa vykonáva najmenej za obdobie posledných 10 rokov alebo od vzniku prvku KI. Jedná sa o analýzu tých prípadov, ktorých vznik, príčiny a podmienky neboli úplne alebo objektívne objasnené.

Z jednotlivých analýz vonkajšieho a vnútorného bezpečnostného prostredia by mali byť identifikované a do úvahy prichádzajúce bezpečnostné riziká, voči ktorým prvok KI nemá dostatočnú ochranu, príp. vytvára podmienky alebo umožňuje nežiaducu činnosť, ktorá môže potenciálne ohroziť chránený záujem.

– Podstatou **analýzy bezpečnostných rizík** je ich identifikácia, hodnotenie a priorizácia.

Identifikácia a hodnotenie bezpečnostných rizík je predpokladom a východiskom na ich efektívne riadenie. Účelom riadenia bezpečnostných rizík je zníženie vzniku nežiaduceho javu alebo udalosti na akceptovateľnú mieru. Akceptovateľnou mierou sa rozumie nulová alebo nízka pravdepodobnosť ich nastania (napr. pravdepodobnosť vzniku požiaru vyvolaného bleskom je najviac jedenkrát za desať rokov; teda pravdepodobnosť jeho vzniku za jeden rok je priemere 0,10 %; búrková činnosť je však typická pre jarné až jesenné mesiace v roku, t. j. počas 9 mesiacov, čo predstavuje 0,75 % roka; potom pravdepodobnosť vzniku požiaru za jeden rok v dôsledku blesku je 0,10*0,75 = 0,075%).

Cieľom identifikácie bezpečnostných rizík je zistenie

- všetkých významných typov a zdrojov bezpečnostných rizík a hrozieb vo vzťahu k chráneného objektu alebo záujmu a bezpečnostnému prostrediu,
- predpokladov vzniku každého bezpečnostného rizika.

Obsahom identifikácie bezpečnostných rizík je vypracovanie *registra rizík*. V registri sa uvádzajú všetky do úvahy prichádzajúce riziká, ktoré majú alebo môžu mať príčinný vzťah k ochrane posudzovaného chráneného objektu (záujmu). Pri identifikácii bezpečnostných rizík sa vychádza z analýzy chráneného objektu a jeho bezpečnostného prostredia, ktoré ich existenciu objektívne preukazujú. Mali by byť identifikované len tie riziká, ktorých existencia bola preukázaná nastaním nežiaduceho javu alebo udalosti, alebo sa dá reálne predpokladať. Identifikácia bezpečnostných rizík musí byť procesne orientovaná a členená do rôznych oblastí

---

[5] Napríklad:
- Vyhláška NBÚ č. 479/2011 Z, z. ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení vyhlášky Národného bezpečnostného úradu č. 314/2006 Z. z.,
- STN EN 1143-1+A1 (937704) Bezpečnostné úschovné objekty. Požiadavky, klasifikácia a metódy skúšania odolnosti proti vlámaniu. Časť 1: Skriňové trezory, skriňové trezory pre peňažné automaty, trezorové dvere a komorové trezory,
- STN EN 50131- Poplachové systémy. Elektrické zabezpečovacie a tiesňové poplachové systémy.

[6] Napríklad:
- Zákon č.215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení neskorších predpisov,
- Zákon č. 122/2013 Z. z. o ochrane osobných údajov,
- Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci,
- Zákon č. 314/2001 Z. z. o ochrane pred požiarmi.

zdrojov možných bezpečnostných rizík. Bezpečnostné riziká, ktoré nie sú identifikované, nemôžu byť ani riadené, ani inak ovplyvňované. Každému identifikovanému riziku je potrebné priradiť *váhu*, ktorá zodpovedá jeho významnosti (kritickosti). Proces určenia významnosti označujeme ako *hodnotenie bezpečnostných rizík*.

Hodnotenie (veľkosť) bezpečnostného rizika je vyjadrenie jeho veľkosti. Tá je daná pravdepodobnosťou nastania nežiaduceho javu. Okrem toho, veľkosť rizika určujú aj *následky (niekedy označované aj ako „dôsledky")* spôsobené nastaním nežiaduceho javu alebo udalosti. Pri hodnotení rizika je potrebné brať do úvahy ich charakter. Následky môžu byť priame alebo nepriame. *Priame následky* „D_{pr}" sa týkajú bezprostredne chráneného záujmu. Počet priamych následkov $D_{pr} > 1$ (môžeme ich teda označiť ako D_{pr1}, D_{pr2} ,... D_{prm}). *Nepriame následky* (sekundárne, terciárne) „D_{nepr}" znamenajú vystavenie bezprostrednému nebezpečenstvu vonkajšie bezpečnostné prostredie, environment, plnenie obchodných záväzkov a pod. Teda počet nepriamych následkov $D_{nepr} > 1$ (môžeme ich taktiež označiť ako D_{nepr1}, D_{nepr2} ,... D_{neprn}). Napríklad výron dusivého plynu z chemickej spoločnosti nemá priame negatívne následky na chránený objekt a jeho aktíva, ale môže spôsobiť škody na životoch, zdraví a majetku osôb, ktoré sa nachádzajú aj niekoľko desiatok kilometrov v smere pohybu oblaku dusivého plynu (podľa stávajúcej miestnej meteorologickej situácie). Táto sa stanovuje znásobením nenulovej pravdepodobnosti vzniku potenciálneho nebezpečenstva (označované písmenom „P") a veľkosti jeho negatívnych (škodlivých) následkov - „D" (napr. výška škôd na životoch a zdraví osôb, majetku, environmentu, strata obchodného mena, odberateľov, klientov a pod.). Veľkosť bezpečnostného rizika *R* je možné vyjadriť ako násobok pravdepodobnosti *P* a následku *D*:

$$R = P \times D \quad (1)$$

kde

$$D = D_{pr} + D_{nepr} \quad (2)$$

potom

$$R = P \times (D_{pr} + D_{nepr}) \quad (3)$$

Ak

$$D_{pr} = \sum_{j=1}^{m} D_{prj} \quad (4)$$

a

$$D_{nepr} = \sum_{k=1}^{n} D_{neprk} \quad (5)$$

potom

$$D = \sum_{j'1}^{m} \sum_{k=1}^{n} D_{prj} D_{neprk} \quad (6)$$

a následne

$$R = P \times \sum_{j'1}^{m} \sum_{k=1}^{n} D_{prj} D_{neprk} \quad (7)$$

Spôsob vyjadrenia veľkosti bezpečnostného rizika môže byť slovnou deskripciou (tzv. nominálnou stupnicou), abstraktnou číselnou hodnotou (tzv. ordinálnou stupnicou) alebo percentuálnou (tzv. kardinálnou stupnicou). Na hodnotenie bezpečnostných rizík môžu byť použité:

- pravdepodobnostné modely,
- expertné odhady.

Výsledkom identifikácie a následného hodnotenia bezpečnostných rizík by mala byť ich *priorizácia* (poradie dôležitosti). Teda rozhodnutie o potenciálne najpravdepodobnejšom nebezpečenstve, ktorému je chránený záujem vystavený, ak budú naplnené podmienky (spúšťače) vzniku spoločensky nežiaducej udalosti alebo javu (napr. požiar, protispoločenská činnosť, elektrický výboj – blesk, prírodné katastrofy, mimoriadne udalosti).

Podľa priority budú k jednotlivým rizikám prijímané opatrenia na zníženie ich veľkosti tak, aby bola dosiahnutá, pokiaľ to bude možné, ich akceptovateľnosť.

Bezpečnostné riziká majúce neakceptovateľnú úroveň je potrebné zodpovedajúcimi opatreniami korigovať na akceptovateľnú úroveň. Spôsob ich korekcie i použité nástroje a opatrenia sú ďalšou časťou bezpečnostného plánu ochrany prvku KI. Kvalita opatrení na zníženie vyhodnotených bezpečnostných rizík je pozitívne korelovaná jeho kvalitou. Tá je ovplyvňovaná použitou metodikou, spektrom

(1)

či komplexnosťou navrhovaných bezpečnostných opatrení a ich synergiou, ako aj efektívnosťou a účelovosťou. S ohľadom na význam prvku KI (regionálny, národný, európsky) je nevyhnutné čo najviac znížiť rizikovosť prvku danú potenciálne pôsobiacimi bezpečnostnými rizikami. Efektívne zníženie bezpečnostných rizík je možné dosiahnuť komplexom opatrení preventívne a zároveň zabraňujúco pôsobiacich. Podstata spočíva v súčasnom použití technických bezpečnostných prostriedkov, nasadením osôb poverených výkonom fyzickej ochrany a organizačno-režimovými opatreniami.

ZÁVER

Cieľom príspevku bolo na jednej strane poukázať na súčasný prístup SR a niektorých dotknutých ústredných orgánov štátnej správy k ochrane KI a na strane druhej navrhnúť možný obsah bezpečnostnej analýzy ako neoddeliteľnej súčasti bezpečnostného plánu. Zámerom bolo aj vyvolať diskusiu ako na akademickej pôde, tak aj na pôde odbornej verejnosti k otázkam týkajúcim sa ochrany prvkov KI či spôsobu ich určovania.

Sme si vedomí, že niektoré členské štáty EÚ s obmedzeniami a výhradami prijali Smernicu Rady 2008/114/ES, príp. sústavne polemizujú o jej význame, avšak domnievame sa, či práve realizácia bezpečnostných opatrení na ochranu objektov dôležitých pre obranu a hospodárstvo nemala preventívny účinok, ktorým sa aspoň z časti predišlo k ich zničeniu či zlyhaniu.

LITERATÚRA

[1] *PCCIP - President s Commission on Critical Infrastructure Protection*. [on line]. [cit. 2013. 06. 15].Dostupné na: http://itlaw.wikia.com/wiki/President's_Commission_on_Critical_Infrastructure_Protection.

[2] *Presidential decision directive No.63*.[on line]. [cit. 2013. 06. 15].Dostupné na: http://www.securityfocus.com/news/164.

[3] *Executive Order 13228.* [on line]. [cit. 2013. 06. 15].Dostupné na: https://www.fas.org/irp/offdocs/eo/eo-13228.htm.

[4] *Homeland Security Act*.[on line]. [cit. 2013. 06. 15].Dostupné na: http://www.dhs.gov/creation-department-homeland-security.

[5] *NSHS-National Strategy for Homeland Security*.[on line]. [cit. 2013. 06. 15].Dostupné na: http://www.gpo.gov/fdsys/pkg/CPRT-110HPRT39618/pdf/CPRT-110HPRT39618.pdf.

[6] *NSPP - The National Strategy for The Physical Protection of Critical Infrastructure and Key Assets*.[on line]. [cit. 2013. 06. 16].Dostupné na: http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

[7] *NIPPO - National Infrastructure Protection Plan.* [on line]. [cit. 2013. 06. 15].Dostupné na: *http://www.dhs.gov/xlibrary/assets/NIPP_Overview.pdf*.

[8] *The National Strategy to Secure Cyberspace, NIPPO s Cyber Security Plan.* [on line]. [cit. 2013. 06. 15].Dostupné na: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[9] *National Infrastructure Protection Plan – NIPP 2009.* [on line]. [cit. 2013. 06. 15].Dostupné na: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[10] ŠENOVSKÝ, P. 2002. *Stav řešení kritické infrastruktúry na území USA*. [on line]. [cit. 2013. 6. 16]. Dostupné na: http://homel.vsb.cz/~sen76/inform/ki.pdf.

[11] KOMISIA EURÓPSKYCH SPOLOČENSTIEV. 2005.*Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry*. Brusel, 17.11.2005, KOM(2005) 576 v konečnom znení. [on line]. [cit. 2013. 6. 16]. Dostupné na: *http://eur-lex.europa.eu/LexUriServ/site/sk/com/2005/com2005_0576sk01.pdf.*

[12] EUROPEAN COMMISSION: *European Programme for Critical Infrastructure Protection (EPCIP),* 2006, [on line]. [cit. 28.12.2012]. Dostupné na: http://eurlex.europa.eu/Result.do?arg0=EPCIP&arg1=&arg2=&titre=titre&chlang=sk&RechType=RECH_mot&Submit=Search.

[13] EUROPEAN COMMISSION: Council decision on a Critical Infrastructure Warning Information Network. [on line]. [cit. 27.12.2012]. Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:058:0001:01:EN:HTML.

[14] VIDRIKOVÁ,D., BOC, K. 2013.*Ochrana kritickej infraštruktúry-1.časť.* Žilina: Žilinská univerzita, 2013.- 164 s..

[15] KOLEŇÁK, I. 2013. *Krizové řízení a kritická infrastuktura v podmínkach České republiky.* In: Riešenie krízových situácií v špecifickom prostredí : 18. medzinárodná vedecká konferencia: 5. - 6. jún 2013, Žilina. - Žilina: Žilinská univerzita, 2013. - s. 273-282.

[16] Zákon č.240/2000 ze dne 28. června 2000 o krizovém řízení a o změně některých zákonů (krizový zákon) v znení pozdějších předpisů.

[17] Nařízení vlády č. 432/2010 Sb. ze dne 22. prosince 2010 o kritériích pro určení prvku kritické infrastruktury, zveřejněné v Sbírce zákonu částka 149, s. 5623-5630.

[18] Usnesení Vlády České republiky č. 934 ze dne 14. prosince. 2011 k určení prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu. [on line]. [cit. 23.6.2013]. Dostupné na: http://kormoran.vlada.cz/usneseni/usneseni_webtest.nsf/search.cs?SearchView&Query=usnesen%C3%AD%20%C4%8D.%20934.

[19] Eurostat. Databaza.[on line]. [cit. 28.6.2013]. Dostupné na: http://epp.eurostat.ec.europa.eu/tgm/table.do%3Ftab%3Dtable%26language%3Den%26pcode%3Dteilm020%26tableSelection%3D1%26plugin%3D1&usg=ALkJrhiR9FzajzTx63knEF1IXUCacCOZpA.
[20] Eurostat. Databaza. Purchasing Power Standard per capita at current prices. [on line]. [cit. 28.6.2013]. Dostupné na:http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do%3Ftab%3Dtable%26plugin%3D1%26pcode%3Dtec00001%26language%3Den&usg=ALkJrhi5fyuH-PCt_PH96jjM3o-s2KfgdQ.
[21] Eurostat. Databaza.The annual growth rate in industry.[on line]. [cit. 28.6.2013]. Dostupné na: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Industry_and_construction_statistics_-_short-term_developments&usg=ALkJrhjXHgrFZRKenzTNMnqFTs12Et6o0A
[22] Eurostat. Databaza. Energia. [on line]. [cit. 28.6.2013]. Dostupné na: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php%3Ftitle%3DFile:Net_electricity_generation,_2000-2010_(1_000_GWh).png%26filetimestamp%3D20121012130727&usg=ALkJrhjced3yJZUlA2WUwXUE4LLRAq2cWw.
[23] Eurostat. Elelectricity generation 2000-2010. [on line]. [cit. 28.6.2013]. Dostupné na: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php?title=File:Net_electricity_generation,_2000-2010_(1_000_GWh).png&filetimestamp=20121012130727.
[24] Eurostat. Elelectricity generation 2000-2010. [on line]. [cit. 28.6.2013]. Dostupné na: http://epp.eurostat.ec.europa.eu/statistics_explained/images/f/fb/Modal_split_of_inland_freight_transport%2C_2000_and_2010_%281%29_%28%25_of_total_inland_tkm%29.png.
[25] Modal distribution of freight transport. [on line]. [cit. 28.6.2013]. Dostupné na: http://epp.eurostat.ec.europa.eu/statistics_explained/images/f/fb/Modal_split_of_inland_freight_transport%2C_2000_and_2010_%281%29_%28%25_of_total_inland_tkm%29.png.
[26] HENDL J. 2009. *Přehled statistických metod. Analýza a metaanalýza dat.* Praha: Portá, 2009.-696 s.
[27] Úrad vlády SR. Kancelária Bezpečnostnej rady Slovenskej republiky. 2012. *Plán práce Bezpečnostnej rady Slovenskej republiky na rok 2013*. Č.:9233-37942/2012/KBR.Schválený uznesením vlády č. 709/2012 zo dňa 19. decembra 2012. [on line]. [cit. 28.6.2013]. Dostupné na: http://www.vlada.gov.sk/data/files/3314_plan-br-sr-na-2013.pdf.
[28] Zákon č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov).
[29] Zákon č. 513/2009 Z. z. o dráhach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[30] Zákon č. 514/2009 Z. z. o doprave na dráhach v znení neskorších predpisov.
[31] Zákon NR SR č. 258/1993 Z. z. o Železniciach Slovenskej republiky v znení neskorších predpisov.
[32] Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.
[33] *Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike.* [on line]. [cit. 28.6.2013]. Dostupné na: http://www.minv.sk/?ochrana-kritickej-infrastruktury.
[34] § 11 ods.1 písm. a) zákona č.473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) v znení neskorších predpisov.
[35] NOVÁK, L.*: Možnosti testovania výkonnosti prvkov kritickej dopravnej infraštruktúry v železničnej doprave.* In: Bezpečnostní a krizový management na regionální úrovni [elektronický zdroj] : 5.-6.9.2012 Uherské Hradiště : sborník mezinárodní konference. - Zlín: UTB, 2012, s. 156-165.
[36] Narodowy Program Ochrony Infrastruktury Krytycznej, 2013.