ODOLNOST KRITICKÉ INFRASTRUKTURY

Richter Rostislav[1], Kovářík František[2]

ABSTRAKT
Odolnost kritické infrastruktury se týká zajištění dodávek základních druhů zboží a služeb nehledě na to jaké mimořádné události se mohou objevit. Odolnost infrastruktury lze pojímat jako schopnost redukovat rozsah a délku mimořádné události. Efektivnost odolnosti infrastruktury nebo firem spočívá v jejich schopnosti anticipovat, absorbovat, adaptovat se a/nebo ve schopnosti rychlé obnovy z mimořádných událostí. Ochrana a odolnost kritické infrastruktury nejsou protichůdné koncepty; představují doplňující se a nezbytné prvky komplexní strategie řízení rizik. Silný základ vyvinutý pro ochranu a odolnost kritické infrastruktury nadále zůstává základní a rozhodující součástí managementu rizik ve všech sektorech kritické infrastruktury.

Klíčová slova:
kritická infrastruktura, odolnost, ochrana, prvek kritické infrastruktury

ABSTRACT
Critical infrastructure resilience is about delivering essential sorts the goods or services regardless of disruptive events that may occur. Infrastructure resilience it is possible to see as the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. Protection and resilience critical infrastructure are not opposing concepts; they represent complementary and necessary elements of a comprehensive risk management strategy. The strong foundation developed for critical infrastructure protection continues to be an essential and vital part of risk management in all critical infrastructure sectors.

Key words:
critical infrastructure, resilience, element of critical infrastructure

[1] Ing. Mgr. Rostislav Richter, Institut ochrany obyvatelstva, Lázně Bohdaneč, rostislav.ricter@ioolb.izscr.cz
[2] Ing. František Kovářík, Institut ochrany obyvatelstva, Lázně Bohdaneč, frantisek.kovarik@ioolb.izscr.cz

1 PRVKY KRITICKÉ INFRASTRUKTURY

Systém určování prvků kritické infrastruktury a jejich ochrany je v České republice upraven zákonem č. 240/2000, o krizovém řízení (krizový zákon), ve znění pozdějších předpisů a příslušným nařízeními vlády ČR. Je vhodné poznamenat, že zmíněný krizový zákon zapracovává Směrnici Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

1.1 VÝCHODISKA URČOVÁNÍ PRVKŮ

Objasnění pojmů

Krizovým zákonem byly definovány mimo jiné pojmy prvek kritické infrastruktury a subjekt kritické infrastruktury.

Prvek kritické infrastruktury

Prvkem kritické infrastruktury může být zejména stavba, zařízení, prostředek nebo veřejná infrastruktura.

Veřejnou infrastrukturou mohou být např. dle stavebního zákona pozemky, stavby, zařízení, a to:

1. **dopravní infrastruktura**, například stavby pozemních komunikací, drah, vodních cest, letišť a s nimi souvisejících zařízení;
2. **technická infrastruktura**, kterou jsou vedení a stavby a s nimi provozně související zařízení technického vybavení, například vodovody, vodojemy, kanalizace, čistírny odpadních vod, stavby a zařízení pro nakládání s odpady, trafostanice, energetické vedení, komunikační vedení veřejné komunikační sítě a elektronické komunikační zařízení veřejné komunikační sítě, produktovody;
3. **občanské vybavení, kterým jsou stavby, zařízení a pozemky sloužící** například pro vzdělávání a výchovu, sociální služby a péči o rodiny, zdravotní služby, kulturu, veřejnou správu, **ochranu obyvatelstva**;
4. veřejné prostranství, zřizované nebo užívané ve veřejném zájmu.

Subjekt kritické infrastruktury

Subjektem kritické infrastruktury se rozumí provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury.

Subjekt kritické infrastruktury odpovídá za ochranu prvku kritické infrastruktury. Za tímto účelem je povinen vypracovat tzv. **plán krizové připravenosti subjektu kritické infrastruktury**. Ministerstvo vnitra – Generální ředitelství Hasičského záchranného sboru ČR vypracovalo pro subjekty kritické infrastruktury Metodiku zpracování plánů krizové připravenosti.

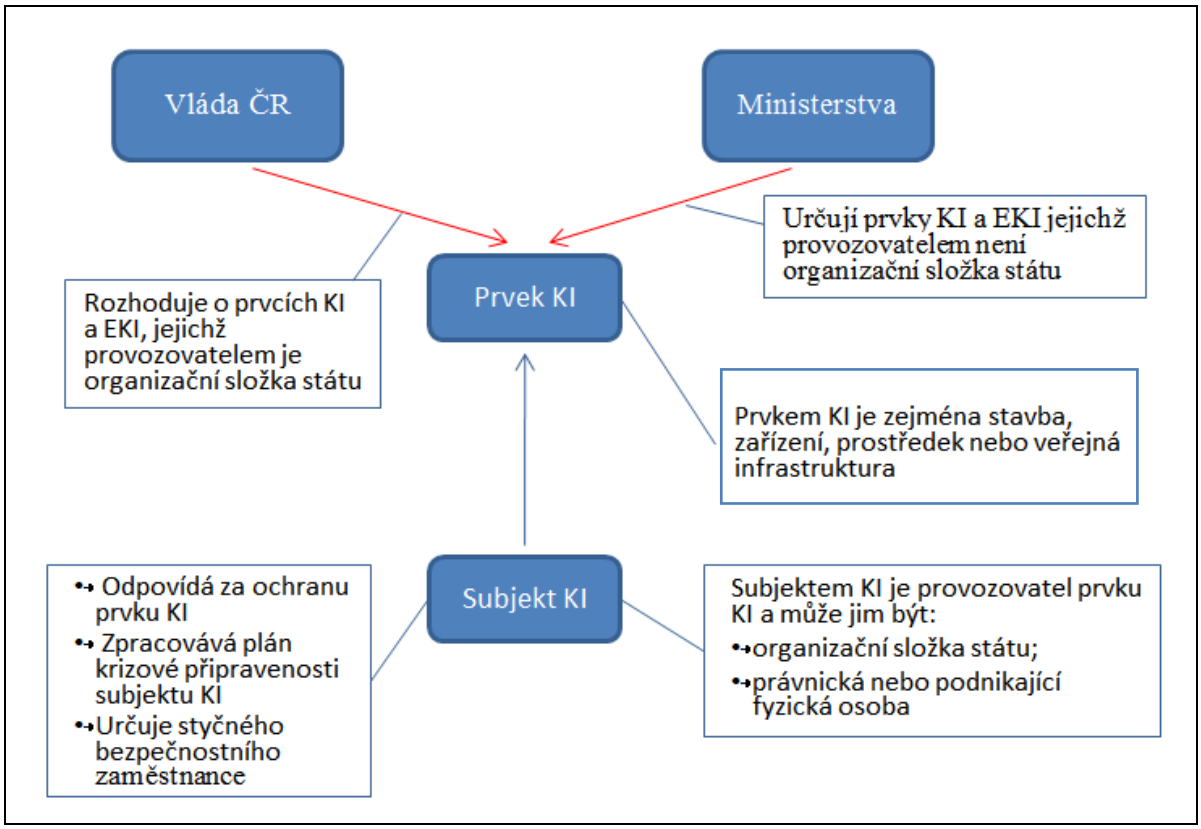
V ČR, pro řešení problematiky kritické infrastruktury, byl zvolen národní přístup, to znamená, že problematikou kritické infrastruktury se zabývá ústřední

úroveň státní správy tj. vláda a příslušná ministerstva a další ústřední orgány státní správy (dále jen ministerstva). Tato kompetence dle krizového zákona nepřísluší krajům a dalším samosprávným územním celkům.

Prvky kritické infrastruktury určuje:

- vláda ČR - v případě, že jde o prvky, jejichž provozovatelem je organizační složka státu;
- ministerstva - v případě, že jde o prvky, jejichž provozovatelem není organizační složka státu.

Schematicky je znázorněno určování prvků kritické infrastruktury na obrázku 1: Určování prvků kritické infrastruktury.



Obrázek 1: Určování prvků kritické infrastruktury

Legenda:

- KI – kritická infrastruktura
- EKI – evropská kritická infrastruktura
- Styčný bezpečnostní zaměstnanec – poskytuje součinnost za subjekt kritické infrastruktury za účelem plnění úkolů podle zákona upravujícího ochranu kritické infrastruktury (tj. dle krizového zákona)

1.2 URČOVÁNÍ PRVKŮ KRITICKÉ INFRASTRUKTURY

Krizovým zákonem bylo stanoveno, že prvky kritické infrastruktury budou určovány v těchto devíti odvětvích: energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa.

V praxi tak Vláda ČR rozhodla na základě seznamu předloženého Ministerstvem vnitra **o prvcích kritické infrastruktury, jejichž provozovatelem je organizační složka státu** a svým usnesením ze dne 14. prosince 2011 schválila seznam prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu.

Celkem bylo vládou určeno 103 prvků ve třech odvětvích:

- odvětví veřejné správy - určeno 64 prvků (31 prvků má charakter organizace tj. ministerstva, 6 prvků má charakter datové centrum a 27 prvků má charakter datová infrastruktura);
- odvětví komunikačních a informačních systémů – určeny 4 prvky (např. Národní centrum kybernetické bezpečnosti, Informační systém Vega-D atd.)
- odvětví nouzové služby – určeno 35 prvků (např. Operační středisko operačního odboru Policejního prezidia České republiky a jednotlivých krajů, Operační a informační středisko Ministerstvo vnitra – Generální ředitelství Hasičského záchranného sboru ČR a jednotlivých krajů atd.)

Ministerstva v praxi naplňují příslušná ustanovení krizového zákona o určování prvků kritické infrastruktury. Pro názornost lze uvést příklad určení prvků kritické infrastruktury Ministerstvem průmyslu a obchodu a Správou státních hmotných rezerv.

- **Ministerstvo průmyslu a obchodu**, jako příslušný správní orgán, opatřením obecné povahy ze dne 17. 2. 2011, určilo prvky evropské kritické infrastruktury na území ČR v energetice:

a) v pododvětví elektřina:

- přenosová soustava:
  1. hlavní technický dispečink;
  2. záložní technický dispečink;
  3. elektrická stanice přenosové soustavy Sokolnice;
  4. elektrická stanice přenosové soustavy Slavětice;
  5. elektrická stanice přenosové soustavy Nošovice;

b) v pododvětví zemní plyn:

- přepravní soustava:
  1. technický dispečink;
  2. hraniční předávací stanice Lanžhot;
  3. hraniční předávací stanice Hora Svaté Kateřiny.

Správa státních hmotných rezerv jako příslušný správní orgán, určila v dubnu 2012 opatřením obecné povahy prvky kritické infrastruktury v odvětvích ropa a ropné

produkty. Jedná se o vybrané subjekty přepravní soustavy, distribuční soustavy, skladování ropy a pohonných hmot a výroby pohonných hmot.

2. ODOLNOST KRITICKÉ INFRASTRUKTURY

Odolnost kritické infrastruktury (dále jen OKI) je ukazatel, který vypovídá o schopnosti zajistit fungování systému/prvku v podmínkách působení vnějších i vnitřních činitelů. Odolný prvek zajišťuje svoji cílovou funkci i v podmínkách, které na něj působí degradujícím účinkem.

2.1 PŘÍSTUPY V POJÍMÁNÍ ODOLNOSTI

Pojem odolnost (resilience) pochází z **reologie.** Jedná se o vědní obor zabývající se studiem vnitřní reakce látek (pevných i tekutých) na působení vnějších sil resp. jejich deformovatelností a tokovými vlastnostmi.

Obecně však lze vyvodit resp. využít pro potřeby tématiky odolnosti kritické infrastruktury dvě základní reologické vlastnosti, které v určitém slova smyslu determinují tzv. reologické chování. Jde o **elasticitu** - schopnost pružné reakce na změny a zaměřené k návratu do původní funkce **a plasticitu** [také viskozitu resp. kríp (creep) neboli tečení] – odolnost založená zejména v robustnosti, které přísluší udržení funkčnosti a dle síly změny následuje trvalá deformace.

Robustnost

Z pohledu technické kybernetiky se pod robustností skrývá představa velmi stabilního systému, který není ve své funkčností a konstituci dotčen ani závažnými změnami své struktury nebo působením vlivů okolí.

Zcela jinou představu o robustnosti má matematická statistika nebo teorie řízení. Obecný požadavek však zůstává. Působíme-li na robustní systém vnějšími podněty, pak očekáváme, že vliv těchto podnětů systém vůbec nebo jen velmi málo ovlivní. Jeho hlavní vlastnosti zůstanou neporušeny. Robustnost také chápat jako malou citlivost změny.

Robustnost je klíčovou vlastností systémů. Dimenzováním moderních konstrukcí směrem k robustnosti lze rozumět nastavení takových schopností systému, aby jejich odezva byla přiměřená situaci/zatížení resp. mimořádné události.

Elasticita

Obecně může být elasticita vnímána jako jedna z možných funkcí robustnosti. Elasticita v kontextu OKI je schopnost pružné (flexibilní) a adekvátní reakce organizace zabezpečit kontinuitu činností, funkcí a procesů. Jde o schopnost reakce jak v podmínkách mimořádné události resp. krizové situace tak v podmínkách běžných. Tedy období managementu rizik, které mimo jiné zahrnuje vnitřní a vnější monitorování organizace, identifikaci rizika, jeho analýzu a hodnocení.

Hodnocení rizik pomáhá při rozhodování o **ošetření rizik** (tj**. p**roces pro modifikování **rizika).** Ošetření rizika může zahrnovat:

- vyhnutí se riziku rozhodnutím nezačínat nebo nepokračovat v činnosti, která způsobuje riziko;
- převzetí nebo zvýšení rizika ve snaze chopit se příležitosti;
- odstranění zdroje rizika;
- změnu možnosti výskytu;
- změnu následků;
- sdílení rizik s jinou stranou nebo stranami (včetně smluv a financování rizika); a
- uchování rizika na základě informované volby.

2.2 KONCEPT ODOLNOSTI

Odolnost je schopnost systému odolávat naplněným hrozbám při udržení své funkčnosti. Souvisí s životností (trvalostí) a výkonem, kdy dochází k očekávanému, standardním problémům. Odolnost je také schopnost systému neztratit svou funkčnost – to jest vykonávat očekávané standardy – navzdory hrozbám. Je nejlépe objasnitelná v rámci představy o trvanlivosti, trvalosti, stálosti a udržitelnosti výkonu apod.

OKI je schopnost redukovat rozsah (závažnost) anebo dobu trvání destruktivní události. Efektivita/účinnost OKI nebo podniku spočívá v jejich schopnostech anticipovat, absorbovat, adaptovat se anebo ve schopnosti rychlé obnovy z potenciální destruktivní události.

Koncept odolnosti zahrnuje snižování rizika pro komunity, zvýšení schopnosti obnovy a zajištění kontinuity základních služeb a činností. Byly stanoveny dva základní (jádrové) cíle odolnosti:

- **zajistit širokou základnu odolnosti:** zvýšit schopnosti rodin, komunit, privátních organizací a všech úrovní státní správy a samosprávy pro udržení základních služeb a činností.
- **zajistit odolnost infrastruktury**: zvýšit schopnost systémů, sítí a činností kritické infrastruktury v zájmu udržení její funkčnosti, schopnosti rychlé obnovy škod a narušení a schopnosti se adaptovat ke změnám podmínek.

Odolnost komunity je spojována se schopností vrátit obyvatelstvo do práce, obnovit podnikání a obnovit základní služby a ekonomickou stabilitu komunity nebo provázaných uskupení postižených komunit.

Odolnost společnost není pojímána jako konečný výsledek či konec nějakého procesu, ale jeden z prvků všestranného (komplexního) spektra připravenosti a reakcí.

Na odolnost lze nahlížet také jako dlouhodobou schopnost systému vypořádat se změnami a pokračovat ve funkčnosti. Zde vystupuje do popředí aspekt flexibility (elasticity). Pro ekosystém jako les, odolnost znamená vypořádání se s bouřemi, požáry a znečištěním, zatímco pro společnost zahrnuje schopnost vypořádat s politickou nejistotou nebo s živelnými pohromami způsobem, který je udržitelný v dlouhodobém hledisku.

Přístup k odolnosti se zaměřuje na dynamické interakce mezi obdobími postupné a náhlé změny a jak se přizpůsobit a formovat změny.

Odolnost kritické infrastruktury zpravidla obsahuje:

- absorpční kapacity (schopnost odolávat)
- adaptivní kapacity (schopnost absorbovat)
- obnovovací kapacity (schopnost obnovovat)

Národní poradní výbor USA pro infrastrukturu uvádí ještě čtvrtou kapacitu resp. první z hlediska časové osy, a to kapacitu anticipační, tj. schopnost předjímat, předpokládat, předvídat.

Co se myslí, když mluvíme o odolnosti, jaké akce, jaké činnosti mohou být realizovány, aby se zvýšila odolnost?

Ve zprávě o vnitřní bezpečnosti USA jsou identifikovány čtyři strategické cíle odolnosti:

1. zvýšit připravenost;
2. efektivní účinná reakce (záchranná, pohotovostní, nouzová či bezpečnostní – dle charakteru událost se jedná);
3. rychlá obnova;
4. zmírňování a snižování rizik.

Odolnost není pojímána jako něco navíc, ale jako součástí zvyšování bezpečnosti. Např. Strategický rámec vnitřní bezpečnosti USA pojímá odolnost jako jeden ze tří základních prvků v pojetí komplexního přístupu k vnitřní bezpečnosti:

- **Bezpečnost** (security): ochrana USA a jejího obyvatelstvo, životních zájmů a způsobu života
- **Odolnost**: podporovat individuální, komunitní a systémovou robustnost, adaptabilitu a schopnost rychlé obnovy.
- Cla a devizy (Customs and Exchange): urychlit a prosadit obchod, cestování a imigraci dle zákona

Tento přístup k odolnosti zahrnuje nejen oblast životních infrastruktur, ale také odolnost společnost, území, jednotlivce atp.

2.3 ŘÍZENÍ ODOLNOSTI

Velmi zajímavým přístupem k řešení OKI je řízení odolnosti systémů, respektive systému systémů ve vztahu k odvětvovým kritériím kritické infrastruktury. Příbuzným přístupem je tzv. řízení rizik, jehož cílem je predikce v návaznosti na analytické nástroje o poznání systému, možnostmi jeho nerovnováhy. Řešení nápravných opatření (korekcí) se pak odehrává preventivně.

U řízení odolnosti je postup velmi podobný. Ve sledovaném systému provedeme analýzu systému a tím popíšeme monitoring možných hrozeb. Následně stanovíme kritéria sledovatelnosti nerovnovážných stavů škálovým hodnocením. Protože je kritická infrastruktura provázaný systém, je nutné poznat i možné dominoefekty. Poznání dominoefektů je velice užitečné v tom smyslu, že jedním ze základních smyslů řízení odolnosti je udržení kontinuity funkčnosti celého systému. Kontinuita je především manažerskou záležitostí a proto je nutné vytvořit jakési organizační workflow, ve kterém vyměníme efektivní automatizaci oběhu dokumentů

za automatizaci informačních gesčních manažerských toků po správních rezortních liniích. Jedná se tedy o kontinuitu řízení prostřednictvím systému kompetentních lidí.

2.4 ODOLNOST A EFEKTIVITA

Pokud se zabýváme odolností, je nezbytné se zmínit o problému efektivity např. v kontextu závislostí na dodavatelích – na dodavatelském řetězci. Například bezpečnost dodávek ropy se podle přístupu Evropské unie měří na základě posouzení dodatečného přínosu nové kapacity vzniklé na základě daného projektu z hlediska krátkodobé a dlouhodobé odolnosti systému a zbývající flexibility systému umožňující vyrovnat se s přerušením dodávek podle různých scénářů.

Dodavatelský řetězec lze charakterizovat jako jednoduchý a kompaktní nebo jako mnohostranný, rozvětvený až nadměrný. Každý z nich má silné a slabé stránky – viz obrázek 2.

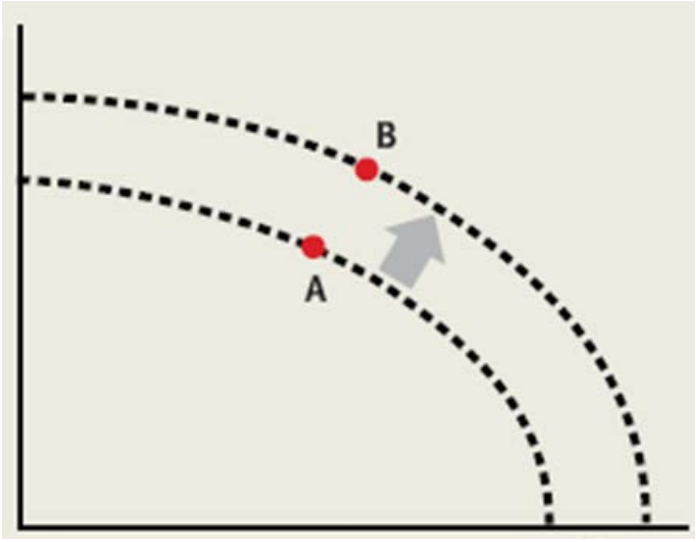
Jednoduchý/kompaktní
Více zranitelný
Menší administrativa
Menší transakční náklady
Více úsporný
Hůře zákaznicky modifikovaný

Mnohostranný/dispersní
Méně zranitelný
Vyšší administrativa
Vyšší transakční náklady
Méně úsporný
Snáze zákaznicky modifikovaný

Obrázek 2: Jednoduchý veru. mnohostranný model

Otázkou je vyváženost (balance) mezi efektivností a odolností. Vyváženost je klíčovým aspektem před kterým stojí manažeři řídící dodavatelský řetězec.
Například Whirlpool byl schopen posílit jak efektivitu, tak odolnost a to konsolidací svých výrobků a zvýšením v používání standardizovaných komponentů. Whirlpool zjednodušil dodavatelský řetězec používáním standardizovaných komponentů ve více výrobcích – pro myčky, pračky atp. Dříve měl například ve 20 typech praček 20 typů kontrolních/řídících jednotek, které zredukoval čtyři kontrolní/ řídících jednotky pro 20 typů praček. Tím se zvyšuje jak efektivita, tak odolnost.

Způsob jak by měli manažeři přistupovat k řešení vztahu efektivity a odolnosti je znázorněn na grafu 1.



Graf 1: Zvyšování efektivity a odolnosti

Komentář

- Jednostranně zaměřená snaha se zaměřit na efektivitu vede ke křehkému zásobovacímu řetězci.
- Na druhé straně, vysoký stupeň redundance (mnohočetnosti) dodavatelských řetězců ve svém výsledku vede k menší efektivitě.
- Jako ideální strategie posunuje oblouk směrem ven, zvyšuje se jak efektivita, tak odolnost, např. z bodu A do bodu B.

3. ZÁVĚR

Odolná infrastruktura znamená, že systémy a jejich prvky budou schopny přežít a dobře fungovat ve stále více nejisté budoucnosti. Odolnost kritické infrastruktury může také vystupovat jako vlastní primární mechanismus k budování přístupu spolupráce firem a státu pro ochranu kritické infrastruktury.

Zvýšení odolnosti kritické infrastruktury spočívá také v **kultivaci partnerských vztahů**, které podněcují spolupráci a sdílení informací mezi všemi úrovněmi státní správy a privátním sektorem vlastnícím či provozujícím prvky kritické infrastruktury.

Odolnost kritické infrastruktury obsahuje absorpční kapacity (schopnost odolávat), adaptivní kapacity (schopnost absorbovat) a obnovovací kapacity (schopnost zvovuobnovy).

LITERATURA

[1] What is Resilience? Institute for Resilient Infrastructure. Přístup: http://www. engineering. leeds.ac.uk/resilience/downloads

[2] Návrh nařízení Evropského parlamentu a Rady o hlavních směrech transevropské energetické infrastruktury a o zrušení rozhodnutí č. 1364/2006/ES. KOM/2011/0658. CELEX: 52011PC0658.

[3] Strategie odolnosti kritické infrastruktury a odolnost kritické infrastruktury. Přístup: http://tisn.gov.au/www/tisn/rwpattach.nsf/VAP/
[4] CRITICAL INFRASTRUCTURE RESILIENCE FINAL REPORT AND RECOMMENDATIONS NATIONAL INFRASTRUCTURE ADVISORY COUNCIL SEPTEMBER 8, 2009. Přístup:http://www.dhs.gov/xlibrary/ assets/niac/ niac_critical_ infrastructure_resilience.pdf
[5] QUADRENNIAL HOMELAND SECURITY REVIEW. REPORT (FEBRUARY 2010). Přístup:HTTP://WWW.DHS.GOV/XABOUT/GC_1208534155450.SHTM
[6] Guidelines for trans-European energy infrastructure and repealing Decision No 1364/2006/EC. COM(2011) 658.
[7] Optimization of Resources for Mitigating Infrastructure Disruptions Study. National Infrastructure Advisory Council. October 19, 2010. Přístup:http://www.dhs.gov/files/committees/editorial_0353.shtm
[8] ASTHURIRANGAN, G., SRINIVAS, P., Sustainable and Resilient Critical Infrastructure Systems, Simulation, Modeling and Intelligent Engineering, Springer, USA, p. 265, ISBN 978-3-642-11405-2,
[9] What is resilience? Stockholm Resilience Centre. Přístup: http://www. stockholmresilience.org/ research/whatisresilience. 4.aeea46911 a3127427980004249.html
[10] Zákon č. 240/2000, o krizovém řízení (krizový zákon)
[11] Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon)

Článok recenzoval:
doc. Ing. Jozef Klučka PhD.