ZAJIŠTĚNÍ ODOLNOSTI KRITICKÉ INFRASTRUKTURY V KOMPLEXNÍM POJETÍ BUSINESS CONTINUITY MANAGEMENTU

Zdeněk Kopecký[1],
Luděk Benda[2], Petr Půlpán[3], Miroslav Špaček[4], Vítězslav Života[5]

ABSTRAKT (ABSTRACT)

Článek se zabývá východisky využití nástrojů procesního řízení a Business Continuity Managementu v zajištění bezpečnosti, celistvosti a funkčnosti kritické infrastruktury. Daná problematika je předmětem projektu Bezpečnostního výzkumu České Republiky č. VI20152018039. Projekt je postaven na komplexním pojetí odolnosti kritické infrastruktury s ohledem na zabezpečení kontinuity procesů subjektů a objektů kritické infrastruktury v systému krizového a havarijního plánování veřejné správy České republiky.

The article focuses on usage of process management tools and Business Continuity Management in ensuring security, integrity and functionality of critical infrastructure. This issue is subject of the project of the Security research of the Czech Republic No. VI20152018039. The project is based on a complex approach to durability of critical infrastructure in regards to securing continuity of processes of subjects and objects of the critical infrastructure in crisis and emergency planning system of public administration of the Czech Republic**.**

KLÍČOVÁ SLOVA (KEY WORDS)

Managemen kontinuty podnikání, krizový management, kritická infrastruktura.

Business Continuity Management, Crisis Management, critical infrastructure.

ÚVOD

Ochrana kritické infrastruktury patří v současné době k bezpečnostních fenoménů. Je aktuálním předmětem krizového řízení na mezinárodní i národní úrovni. Základní terminologie kritické infrastruktury, která se postupně vyvíjela, vychází především ze

[1] Ing. Zdeněk Kopecký, Ph.D., Vysoká škola ekonomická v Praze – Institut krizového managementu, Ekonomická 957, 148 01 Praha 4, Czech Republic, tel.: +420 224094223, kopecky@vse.cz
[2] Ing. Luděk Benda, WAK Systém, s.r.o., Petržílková 2564/21, 158 00 Praha 5, Czech Republic, tel.: +420 251612552, benda@waksystem.cz,
[3] Ing. Petr Půlpán, WAK Systém, s.r.o., Petržílková 2564/21, 158 00 Praha 5, Czech Republic, tel.: +420 251612552, pulpan@waksystem.cz,
[4] doc. Ing. Miroslav Špaček, Ph.D., MBA, Vysoká škola ekonomická v Praze – Fakulta podnikohospodářská, nám W. Churchilla 4, 130 67 Praha 3, Czech Republic, tel.: +420 224098728, Miroslav spacek@vse,cz
[5] Ing. Vítězslav Života, WAK Systém, s.r.o., Petržílková 2564/21, 158 00 Praha 5, Czech Republic, tel.: +420 251612552, zivota@waksystem.cz,

Směrnice Rady 2008/114/ES (dále jen Směrnice) a ze zákona č. 240/2000 Sb.[6]. Definice uvedená ve Směrnici chápe kritickou infrastrukturu jako: „*Prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel a jejichž narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí.*“

Ochrana kritické infrastruktury má být podle Směrnice zaměřena na zajištění celistvosti a nepřetržité funkčnosti kritické infrastruktury

Jsou identifikováni vlastníci a provozovatelé kritické infrastruktury, na které jsou ze strany exekutivy, v souladu s legislativou, kladeny požadavky na její ochranu. Z hlediska velmi významného postavení podnikové sféry při ochraně kritické infrastruktury je však nutné spojit priority podniků s požadavky státu tak, aby byla na obou stranách naplněna kritéria účelnosti, účinnosti a efektivity. Východiskem je daná legislativa, systémový přístup a procesní řízení ochrany kritické infrastruktury s využitím metod kvantitativního managementu pro optimalizaci procesů zabezpečení její funkčnosti a celistvosti.

Směrnice se odrazila i při novelizaci krizového zákona a v prováděcím nařízení vlády č. 432/2010 kde byla stanovena průřezová a odvětvová kritéria pro určování prvků národní kritické infrastruktury:

Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,

b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo

c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

Odvětvová kritéria jsou stanovena pro níže uvedené oblasti národní kritické infrastruktury České republiky:

- *Energetika* – v národním i evropském rámci
- *Vodní hospodářství* – v národním i evropském rámci.
- *Potravinářství a zemědělství* - v národním i evropském rámci.
- *Zdravotnictví* - v národním i evropském rámci.
- *Doprava* – evropský rámec s ohledem na odlišné reálie počítá i s námořní a příbřežní dopravou.
- *Komunikační a informační systémy* – národní rámec nezmiňuje výslovně ochranu informačních systémů a sítí, evropský rámec nepočítá s poštovními službami.
- *Finanční trh a měna* – národní rámec počítá navíc s pojišťovnictvím.
- *Výroba nebezpečných látek* – evropský rámec nepočítá s biologickými materiály.
- *Nouzové služby* – pouze v národním rámci, evropský rámec s nimi nepočítá.
- *Veřejná správa* – pouze v národním rámci, evropský rámec s ní nepočítá.
- *Vesmír* – s touto problematickou národní rámec nepočítá, ale je v evropském rámci.
- *Věda a výzkum* – s touto problematickou národní rámec nepočítá, ale je v evropském rámci.

[6] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění nařízení vlády č. 36/2003 Sb.

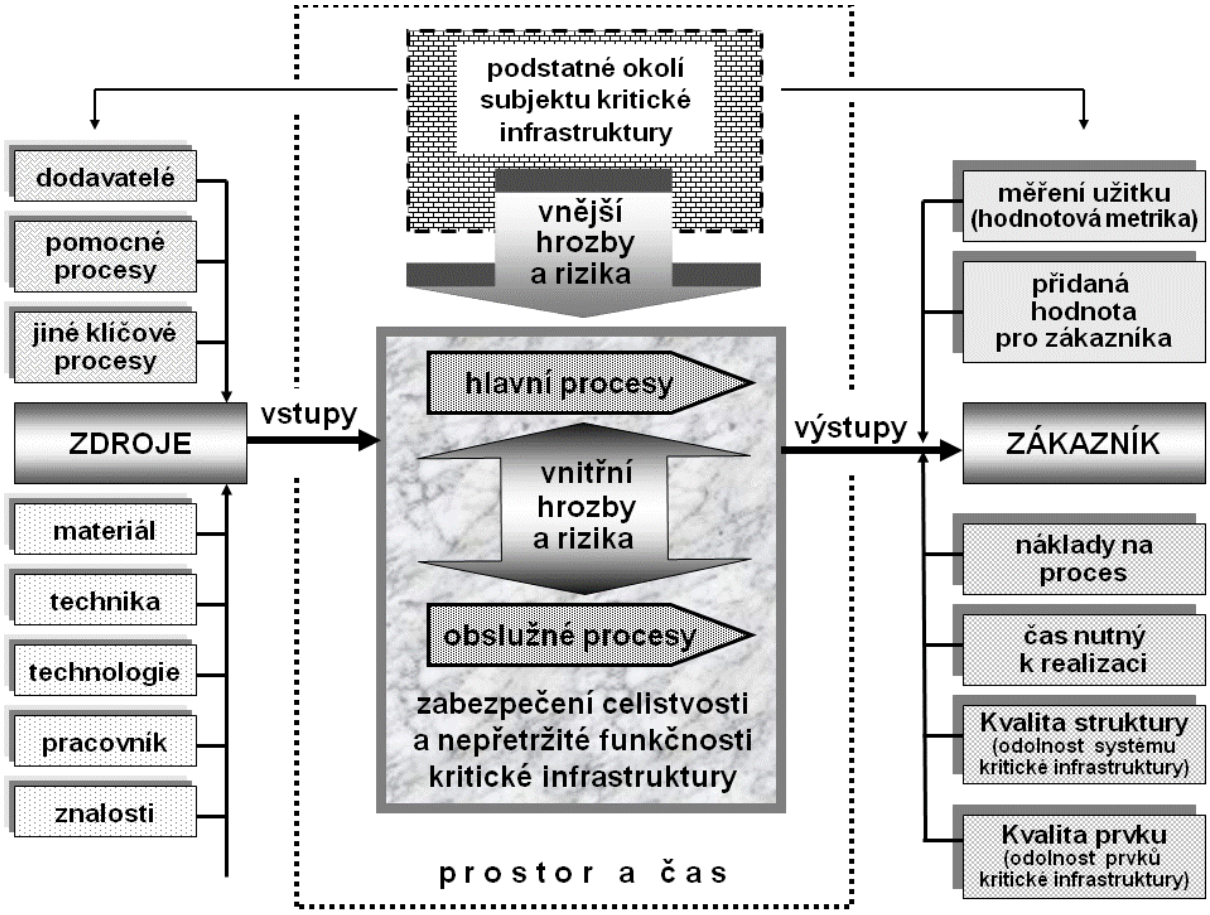
1. PROCESNÍ PŘÍSTUP K ZAJIŠTĚNÍ BEZPEČNOSTI A FUNKČNOSTI KRITICKÉ INFRASTRUKTURY

Zabezpečení celistvosti a nepřetržité funkčnosti a bezpečnosti kritické infrastruktury by mělo vycházet ze systémového pojetí infrastruktury, jako dynamického adaptabilního a otevřeného (vazby na vnější prostředí) systému prvků a vazeb. Zodolnění infrastruktury, jako systému by se potom mělo orientovat na stránku:

- statickou, spočívající v odolnosti jednotlivých prvků a vazeb (především kritických), v redundanci zdrojů (vytváření záloh, zásob, rezerv) a v diverzifikaci rizika (rozložení, popř. přenesení dopadů disfunkčnosti infrastruktury na více subjektů),
- dynamickou, spočívající v případě ztráty funkce některého prvku nebo vazby ve flexibilitě a adaptabilitě (schopnosti rekonfigurace) na nové podmínky pro nouzové zabezpečení funkčnosti infrastruktury jako systému a zpětnou obnovu do nového stabilního stavu.

Zároveň by měla být požadovaná ochrana kritické infrastruktury (zabezpečení její nepřetržité funkčnosti a celistvosti) pojímána jako zdrojově podmíněný proces s přidanou hodnotou pro zákazníka, kterým je v tomto případě stát (i když v konečném pořadí stále občan) tak, jak je schematicky znázorněno na Obrázku 1.

Obrázek 1: Ochrana kritické infrastruktury jako zdrojově podmíněný proces



Zdroj: vlastní

To umožňuje aplikaci procesního řízení (Business Process Management – BPM)[7], které jako manažerská disciplína vychází z jasně specifikovaných cílů organizace a hierarchie procesů k jejich dosažení.

Cíle zabezpečení nepřetržité funkčnosti a celistvosti kritické infrastruktury, které musí vycházet jak z „požadavků státu“[8], tak z podnikatelské strategie organizace, by měly naplňovat atributy obsažené v anglické zkratce SMART[9] ve významu:

- *konkrétní* – Cíle jsou v tomto případě jasně naformulované, ať již v legislativě nebo v související prováděcí dokumentaci.
- *měřitelné* – Měřitelnost (kvantifikace) je důležitý požadavek především z hlediska jednoznačnosti průběžné a konečné kontroly naplňování cílů. Jedinou kvantifikací jsou však nyní pouze kritéria pro určení prvku kritické infrastruktury[10]. Chybí kvantifikace požadované úrovně ochrany (odolnosti) kritické infrastruktury ve vztahu ke kvantifikaci jednotlivých potencionálních hrozeb (rizik).
- *dosažitelné* (přijaté po vzájemné domluvě zainteresovaných stran) – Způsob dosažení by měl být dán krizovými plány a plány připravenosti subjektu kritické infrastruktury, jako racionálními cestami dosažení cílů, dávajícími jednoznačnou odpověď na otázky co a jak (kdy, kde, s jakými zdroji) pro ochranu kritické infrastruktury dělat.
- *realistické* – Stanovené cíle (z hlediska bezpečnosti státu) by měly brát v úvahu i podmiňující a návazné cíle (včetně podnikatelských cílů subjektů kritické infrastruktury). Je to systémové pojetí ochrany kritické infrastruktury ve vztahu ke svému podstatnému okolí.
- *správně načasované* – Měl by být stanoven časový horizont dosažení cílů a procesy jejich dosažení by měly být sledovatelné i v čase, jako základnímu fenoménu jejich průběhů.

Procesy (ochrany kritické infrastruktury) musí být identifikovány, specifikovány a analyzovány jak samy o sobě, tak vzhledem ke svému postavení v hierarchii procesů v organizaci (mapy procesů) ve vztahu k hierarchii cílů i odpovídající úrovni řízení pro jejich napřímení nebo redesign. To by se mělo odrazit i v organizační struktuře[11], informační podpoře a dalších podpůrných procesech.

Procesní řízení, na rozdíl od funkčního přístupu (typického pro veřejnou správu), umožňuje větší flexibilitu organizace při řešení rizikových a složitých problémů a v širší míře jejich zefektivňování a optimalizaci, tak jako v případě udržení funkčnosti a celistvosti kritické infrastruktury. I když na druhé straně implementace BPM do praxe vyžaduje zvýšené nároky na informační podporu a změnu organizační struktury a s tím spojenou problematiku lidského faktoru tyto změny podstupovat.

2 BUSINESS CONTINUITY PLAN A JEHO INTEGRUJÍCÍ ROLE PŘI ZAJIŠTĚNÍ FUNKČNOSTI KRITICKÉ INFRASTRUKTURY

Nejvhodnější formou implementace systémového přístupu a procesního řízení do praxe v ochraně kritické infrastruktury z hlediska podnikohospodářské sféry je Business

[7] Např. Veber, J. a kol. Management, základy moderní manažerské přístupy výkonnost a prosperita. Management Press, 2009. ISBN 978-80-7261-200-0

[8] Bezpečnostní strategie České republiky a s ní související legislativy.

[9] Specific, Measurable, Attainable (Ageed), Realistic, Timed (Trackbale).

[10] Nařízení vlády č 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

[11] Projektová organizační struktura v rámci stávající hierarchie kompetencí (odpovědnosti a pravomoci) nebo v případě potřeby vyšší flexibility interdisciplinární struktura.

Continuity Management (BCM)[12], který lze chápat jako řízení kontinuity podnikatelských procesů (kontinuity funkčnosti kritické infrastruktury) ve vztahu k provozním (operačním) rizikům[13]. Je to systémový a integrovaný přístup k zabezpečení udržení činnosti podniku (zabezpečení celistvosti a funkčnosti kritické infrastruktury) z hlediska řízení provozních rizik, kdy je řízení rizik zaměřené pouze na jednotlivé faktory provozuschopnosti příliš úzké a neúčinné.

Pojem provozního rizika má v podnikové sféře dvojí význam. Setkáváme se s ním ve finanční analýze podniku, kde rozeznáváme[14]:

- finanční riziko - je spojeno s mírou podílu cizích zdrojů financování v celkových zdrojích. Vyplývá ze skladby zdrojů podle nároků na pořadí úhrady,
- provozní riziko - rozsah využívání hmotného investičního majetku a s tím spojených fixních nákladů a jejich poměr k nákladům variabilním.

Pro potřeby BCM (a to i v uplatnění pro oblast ochrany kritické infrastruktury) je ale provozní riziko chápáno jako:

- omezení nebo znemožnění podnikání vnitřními vlivy (provozní havárie, poškození strojů, stávka, úrazy, atd.),
- omezení nebo znemožnění podnikání vnějšími vlivy (živelní pohromy, epidemie, terorismus, energetická omezení, narušená dopravní a energetická infrastruktura, atd.)

Systém zabezpečení kontinuity podnikání je systém organizačních, personálních, materiálních, technických, finančních a dalších opatření k minimalizaci rizik diskontinuity a zabezpečení nezbytných zdrojů (vstupů) a udržení podmínek k realizaci podnikatelských aktivit (např. ve výstavbě, údržbě a provozování kritické infrastruktury) při vzniku mimořádných a následných krizových situací.

Bezprostředním cílem zabezpečení kontinuity je co nejdelší udržení podnikatelského procesu. Přesto i zde se počítá s jeho možným řízeným omezením nebo, z hlediska obnovy (revitalizace), přípustným přerušením v důsledku omezení nezbytných zdrojů z hlediska jejich kvantity, kvality a funkčnosti ve vztahu k prostoru a času, tak aby byly zachovány alespoň v minimální míře požadované funkce.

Základním nástrojem BCM je Business Continuity Plan (BCP), jako výstup první sekvenční manažerské funkce BCM. BCP staví mosty mezi tím, kde jsme (v jakém stavu ochrany funkčnosti infrastruktury) a tím, kam chceme jít (jaké úrovně ochrany chceme dosáhnout.

Krizová legislativa ukládá v oblasti plánování mnohé povinnosti subjektům podnikohospodářské sféry (včetně subjektů kritické infrastruktury) při přípravě na krizové situace a jejich řešení. Jde především o:

- plán krizové připravenosti[15] (plán krizové připravenosti subjektu kritické infrastruktury),
- plán opatření hospodářské mobilizace[16],

---

[12] Původně, ale většinou i nyní, je BCM spojován s udržením a obnovou informačních technologií po jejich zhroucení (Disaster Recovery). V současné době je ale i snaha využít metodologii BCM v oblasti veřejné správy v systému krizového řízení jako Government Continuity Management (GCM).

[13] V BCM se jedná o taková rizika, která nejsou spojena s uplatněním výrobku nebo služby na trhu, ale se zajištěním podmínek a „dostatečností" zdrojů pro jejich produkci. Např. v ERM (Enterprise risk management) je provozní riziko chápáno jako součást organizačního rizika, které z hlediska tvorby hodnoty je ještě v základní kategorizaci doplněno o riziko strategické a tržní.

[14] Např.: Grünwald, R. - Holečková, J. Finanční analýza a plánování podniku. VŠE Praha, 1994

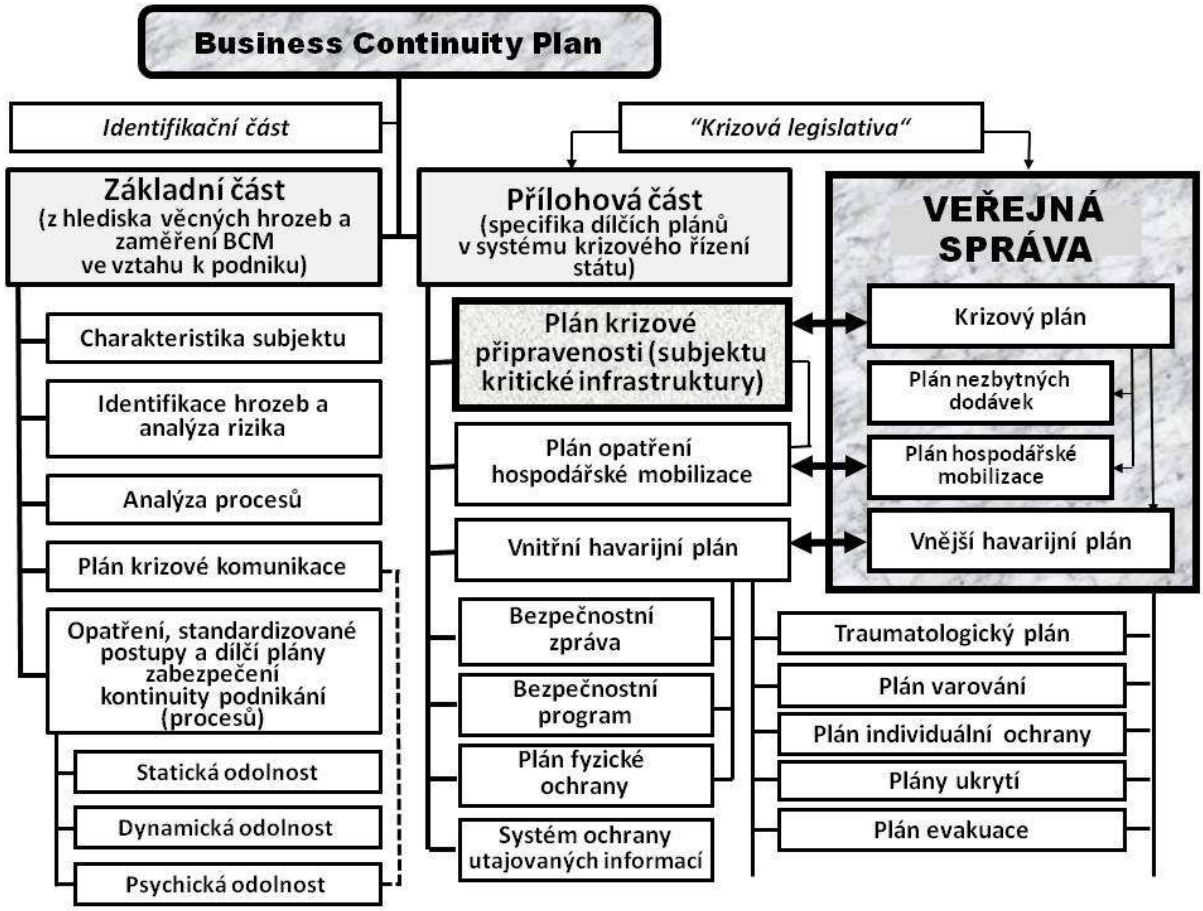
[15] V souladu se zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

[16] Pokud je podnik subjektem hospodářské mobilizace ve smyslu zákona č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy

- vnitřní havarijní plán[17],
- bezpečnostní program prevence závažné havárie obsahující popis systému řízení bezpečnosti v podnikatelském objektu,
- bezpečnostní zpráva (v základním členění podle příslušné vyhlášky),
- plán fyzické ochrany.

Rámcová struktura BCP ve vztahu k systému havarijního a krizového plánování veřejné správy maximálním rozsahu[18] je na Obrázku 2.

Obrázek 2. Struktura BCP ve vztahu ke krizovému a havarijnímu plánovaní v systému veřejné správy České republiky



Zdroj: vlastní

Všechny tyto plány se dotýkají jedné a té samé reality, řešené z různých úhlů pohledu a s tím i souvisejících gesčních a kontrolních orgánů veřejné správy[19]. Ta realita, společná pro všechny plány, je na jedné straně dána hrozbami a riziky a na straně druhé možnostmi konkrétního subjektu (má stále jedny a ty samé zdroje a schopnosti) čelit dopadům těchto

[17] V souladu se zákonem č. 224/2015 Sb., o prevenci závažných havárií způsobených vybranými chemickými látkami nebo chemickými přípravky (zákon o prevenci závažných havárií)

[18] Pokud se zároveň jedná např. o subjekt hospodářské mobilizace podle zákona č. 241/2000 Sb., nebo podnik zařazený do třídy A nebo B v souladu se zákonem č. 224/2015 Sb.

[19] Např. MV ČR, SSHR, MŽP ČR, Krajské úřady, Správní úřady na úseku požární ochrany, ochrany obyvatelstva a Integrovaného záchranného systému, Český inspekce životního prostředí, Státní úřad inspekce práce, krajské hygienické stanice, atd.

hrozeb. Navíc, vše co je na podnikohospodářských subjektech požadováno, je primárně z hlediska potřeb veřejné správy[20]. To, že se tím řeší částečně i zájem podniku, což je pro něj samozřejmě prospěšné, je až druhotné. Oproti tomu BCP řeší primárně zájem a potřeby podniku, i když na základě toho je lépe připraven plnit i úkoly na něj kladené v rámci krizového a havarijního plánování. Proto má smysl do přípustné míry integrovat[21] a tím zracionalizovat systém plánování podnikohospodářského subjektu (subjektu kritické infrastruktury a jeho objektů) ve vztahu k bezpečnostním i provozním hrozbám daného subjektu kritické infrastruktury a jeho objektů kritické infrastruktury.

Základem integrace by měl být, vzhledem k jeho komplexnímu pojetí hrozeb a rizik diskontinuity, BCP, který by integroval společné části (např. identifikace hrozeb, analýza rizik a procesů atd.) a v přílohové části by byla specifika jednotlivých plánů, vyplývajících z požadavků krizového a havarijního plánování. Na možnou racionální integraci již stávající plánovací, organizační nebo technické dokumentace, kterou subjekt kritické infrastruktury v rámci své veřejnoprávní povinnosti zpracovává, je myšleno i v zákoně č. 240/2000 Sb. Při specifikaci plánu krizové připravenosti subjektu kritické infrastruktury.

ZÁVĚR

Zabezpečení ochrany kritické infrastruktury při naplňování základních funkcí státu je vzhledem k současným bezpečnostním hrozbám nezbytné. Pro podnikohospodářské subjekty (subjekty kritické infrastruktury) je nejen nutné podřídit procesy zabezpečení ochrany kritériím účelnosti, účinnosti a efektivity, optimalizovat je z hlediska zdrojů a času ve vztahu ke svým cílům, ale i požadavkům systému krizového řízení státu. Integrující roli zde může vzhledem ke svému komplexnímu pojetí vnějších i vnitřních provozních rizik ve vazbě na faktory a rizika ekonomická sehrát Business Continuity Plan subjektu kritické infrastruktury, jehož primárním předmětem je zabezpečení kontinuity procesů. V tomto případě by šlo o procesy zabezpečení ochrany a udržení nepřetržité funkčnosti a celistvosti kritické infrastruktury pro potřeby dosahování podnikatelských cílů subjektu kritické infrastruktury (majitele nebo provozovatele infrastruktury), zahrnující i požadavky, vyplývající z příslušné legislativy a dokumentace systému krizového a havarijního plánování se zaměřením na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Příspěvek vznikl v rámci řešení projektu Bezpečnostního výzkumu Ministerstva vnitra České Republiky „Nástroje zavedení procesního řízení v zajištění bezpečnosti a funkčnosti kritické infrastruktury s důrazem na odvětví dopravy“ – (BCM), ev. č. VI20152018039.

LITERATURA

1 Benda, L. - Kopecký, Z. - Půlpán, P. et al. *Optimalizace procesů a nákladů při obnově dopravní infrastruktury v rámci systému krizového řízení ČR (TA01030819*) [CD-ROM]. *WAK SYSTEM,* Praha. 2013.

[20] Např. plán krizové připravenosti, řeší připravenost podnikohospodářského subjektu zahrnutého do krizového plánu pouze v rozsahu plnění toho, co je na něm požadováno. Zjednodušeně řečeno, státu je jedno, pokud dojde např. k provozní havárii v podniku, která ohrozí dosahování podnikatelských cílů, ale neohrozí zdraví a životy pracovníků a nedotkne se jeho (z hlediska státu) podstatného okolí.

[21] Jedná se např. o informace, které jsou předmětem zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, nebo mají charakter zvláštních skutečností podle zákona č. 240/2000 Sb., o krizovém řízení.

2 Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

3 Kopecký, Z. Podnik jako subjekt kritické infrastruktury v krizovém řízení státu. In Maajtán, Š. (ed.). *Aktuálne problémy podnikovej sféry 2013.* Bratislava: Ekonóm, s. 265-270. 2013. ISBN 978-80-225-3636-3.

4 Kopecký, Z. et al. Návrh systému informační podpory ochrany kritické dopravní infrastruktury pro potřeby řešení typových plánů krizového řízení veřejné *správy* (KRIZ - *CG941-**055**-030*) [CD-ROM]. 2011. VŠE v Praze.

5 Kopecký, Z. Východiska zvýšení odolnosti subjektů kritické infrastruktury. In *Riešenie krizových situácií v špecifickom prostredí.* Žilina: Fakulta špeciálného inžinierstva Žilinskej univerzity, 2010. s. 375–381. ISBN 978-80-554-0203-1.

6 Nařízení vlády ČR č. 431/2010 Sb., kterým se mění nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně *(§ 17a Náležitosti plánu krizové připravenosti subjektu kritické infrastruktury).*

7 Nařízení vlády ČR č 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

8 Nařízení vlády ČR č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) některých zákonů (krizový zákon), ve znění nařízení vlády č. 36/2003 Sb. – *(§ 18 Způsob zpracování plánu krizové připravenosti a plánu krizové připravenosti subjektu kritické infrastruktury).*

9 Příloha k Nařízení vlády ČR č. 432/2010 Sb. ze dne 22. prosince 2010 o kritériích pro určení prvku kritické infrastruktury

10 Veber, J. a kol. Management, základy moderní manažerské přístupy výkonnost a prosperita. Management Press, ISBN 978-80-7261-200-0

11 Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).

12 Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy.