Bezpečnostní plány jako významný aspekt ochrany kritické infrastruktury

Security plans as an important aspect of critical infrastructure protection

Lukáš Mach

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš MACH**
Osobní číslo:	**A07615**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní plány jako významný aspekt ochrany kritické infrastruktury**

Zásady pro vypracování:

1. **Zhodnocení významu kritické infrastruktury a její ochrany pro společnost.**
2. **Analýza současných trendů ochrany kritické infrastruktury.**
3. **Specifikace požadavků na bezpečnostní plány prvků kritické infrastruktury.**
4. **Rozbor dostupných metodik zpracování bezpečnostních plánů použitelných i ve vztahu k ochraně kritické infrastruktury.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Vstažná legislativa, příslušné evropské, vnitrostátní, resotní a další normy.**
2. **Mozga J., Vítek M., Kovařík F., Kritická infrastruktura společnosti, Univerzita Hradec Králové, Filozofická fakulta, Gaudeamus, 2008.**
3. **Federal Ministry of the Interior, Protecting Critical Infrastructures Risk and Crisis Management, A guide for companies and government authorities, Berlin, 2008.**
4. **KRULIK O., FYZICKÁ OCHRANA KRITICKÉ INFRASTRUKTURY A KLÍČOVÝCH AKTIV, 2003.**
5. **MURRAY T. A., GRUBESIC H. T., Critical Infrastructure, Reliability and Vulnerability, Springer, 2007.**
6. **BAECHER B.G., FROLOV V. K., Protection of Civilian Infrastructure from Acts of Terrorism, Springer, 2006.**
7. **LINKOV I., WENNING J. R., KIKER A. G., Managing Critical Infrastructure Risks, Decision Tools and Applications for Port Security, Springer, 2006.**

Vedoucí bakalářské práce: **Ing. Martin Hromada**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem této práce je vytvořit ucelený seznam dostupných metodik k vypracování bezpečnostních plánů které jsou používané v současné době, a které mohou být ekvivalentem operačního plánu pro bezpečnost.

Klíčová slova: kritická infrastruktura, bezpečnostní plány, provozovatel, ochrana, bezpečnost

ABSTRACT

The aim of this work is to create a comprehensive list of available methodologies for elaborating security plans that are currently in use, and which may be equivalent to the operational security plan.

Keywords: critical infrastructure, security plans, service, protection, security

Rád bych na tomto místě vyjádřil poděkování svému vedoucímu práce Ing. Martinu Hromadovi nejen za vhodné rady při postupu své práce, ale za celkový přístup a vstřícnost.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Současná společnost je charakteristická svojí složitostí a závislostí na technických technologických systémech, které svojí provázaností a vlivem asymetrického prostředí vytvořily potřebu identifikovat takové složky infrastruktur, které ovlivňují a jsou nevyhnutelné v souvislosti s funkční kontinuitou společnosti. Bezpečnostní prostředí vytváří potřebu optimalizace a aktualizace postupů zajištění bezpečnosti a mezi takovými postupy je jednak implementace směrnice 2008/114/ES a s tím spojené vypracování bezpečnostních plánů.. Cílem mé práce je pojednat o požadavcích na bezpečnostní plány provozovatele kritické infrastruktury a analyzovat další možné přístupy k vypracování ekvivalentů bezpečnostních plánů.

1 VÝVOJ KRITICKÉ INFRASTRUKTURY

Bezpečnostní rizika, jako jsou katastrofy způsobené živelnými pohromami, technologické a chemické havárie, lidská nedbalost, organizovaná trestná činnost, vniknutí do počítačových systémů a v neposlední řadě zvyšující se hrozby teroristických útoků, mely za následek potřebu definovat kritickou infrastrukturu (dále KI) a to jako takovou oblast infrastruktury, kdy její narušení či zničení vyvolá závažné hospodářské a politické následky.

1.1 USA a NATO

Jedním z prvních ucelených dokumentů, který se věnoval problematice KI byla tzv. „Bílá kniha“[1]. Toto rozhodnutí prezidenta Billa Clintona bylo vydáno 22. května 1998. Tato Bílá kniha objasňuje klíčové prvky Clintonovy administrativní politiky pro ochranu KI a je určena pro šíření mezi všechny zúčastněné strany v soukromém i veřejném sektoru. Vnímá KI jako „základní systémy, které mají určitou hmotnou nebo kybernetickou základnu a mají vliv na funkci ekonomiky státu“[1].

Největší historickou událostí ovlivňující vývoj KI a její obrany a ochrany se stal 11. září 2001 útok na Světové obchodní centrum (WTC) v New Yorku. Tento čin přispěl k přehodnocení potřeby chránit a chránit důležité prvky národní infrastruktury. Po útoku vydal 16 října 2001 prezident George W. Bush „Vládní nařízení na ochranu kritické infrastruktury“[2], za účelem zabezpečit ochranu informačních systému KI a hmotných zařízení, které zabezpečovaly funkci ekonomiky, činnosti státu a vedení národní obrany.

V roce 2002 je v USA vydán dokument „Národní strategie vnitřní bezpečnosti“[3], který vnímá kritickou infrastrukturu jako „systémy a zařízení hmotné i virtuální, které jsou životně důležité pro USA a zničení nebo vyřazení z činnosti těchto systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, veřejného zdraví nebo bezpečí, nebo jakákoli jejich kombinace.“[3] Na tento dokument navázaly v roce 2003 „Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení“ a „Národní strategie zabezpečení kybernetického prostoru.“ V roce 2002 přišla s definicí KI i Severoatlantická aliance v rámci Euroatlantické rady partnerství (EAPC) a to: „Kritická infrastruktura zahrnuje fyzické a kybernetické systémy pro zajištění důležitých a nevyhnutelných činností ekonomiky a státní správy“. Zahrnuje hlavně telekomunikační,

energetické, bankovní, finanční, dopravní, vodohospodářské systémy a nouzové služby a to státní i soukromé.

Z těchto mnoha přijatých dokumentů vyplývá, že se přehodnotilo množství investovaných prostředků do bezpečnostního výzkumu, což by mělo přispět k zvýšení ochrany. Výraznou část celkových výdajů investuje USA do výzkumu po útocích na WTC z 11. září 2001. Tato událost ukázala, že hlavní prioritou pro život, stát a jeho subjekty je bezpečné území, bezpečný objekt, bezpečná budova a zachování společenského rastu a kontinuity.

1.2 EU

„V EU se prosazuje, že jednou ze základních rolí vlád států je zajistit pocit jistoty obyvatel státu, tj. zajistit bezpečnost. Důraz na tuto zásadu zesílil po útocích dne 11. září 2001 v USA a zvláště pak po útocích v Madridu dne 11.3. 2004.

Na konci r. 2003 čelní představitelé evropského průmyslu a zákonodárci EU požádali předsedu Evropské Komise pana R. Prodiho o rozpočet na podporu bezpečnostního výzkumu s názvem „Research for Secure Europe“ (Výzkum pro bezpečnou Evropu).[4] Tato zpráva popisuje základní prvky Evropského programu pro výzkum v otázkách bezpečnosti a jeho přínos k řešení nových bezpečnostních úkolů měnícího se světa. Materiál obsahuje 12 doporučení pro budoucnost a žádost o minimální roční rozpočet 1 miliardu EUR na rozvoj technologií v předmětné oblasti. Předseda Evropské komise přijal návrh a po událostech v Madridu dne 11.3.2004 rozhodl o projektu na léta 2007 - 2013. Výše finančních prostředků je předmětem jednání o rozpočtu Evropské komise na léta 2007 - 2013, ale již nyní lze říci, že rámec, ve kterém jednání probíhají je s ČR nesrovnatelný.

V roce 2003 byla zahájena iniciativa „European industrial potential in the field of security research“[20], která si klade za cíl rozvoj bezpečnostního výzkumu. V rámci této iniciativy je definována řada prioritních vědních oborů, mezi něž například patří:

- Shromažďování informací
- Analýza informací
- Analýza kritické infrastruktury

- Energetické materiály
- Risk management
- Krizový management
- Komunikační technologie
- Informační technologie“[5]

„Technologie sama nemůže garantovat pocit bezpečí, ale jeho zabezpečení není možné bez technologie.“ Pod tímto heslem je veden program na výzkum bezpečnosti a na jeho přípravu bylo vyčleněno 65 milionů EUR. Cílem tohoto programu je posílit bezpečí v EU, oživit evropskou konkurenceschopnost a mezi civilním a obranným výzkumem vytvořit určitý sjednocující most. Při tvorbě takového výzkumu je nutné vycházet z jasného faktu, že kybernetika zahrnující elektronické informace, informační technologie a telekomunikace je jádrem řešení dnešních bezpečnostních těžkých úkolů.[5]

20. října 2004 přijala Evropská komise první koncept ucelené kritické infrastruktury a její ochrany a obrany, a to: „Ochrana kritické infrastruktury v boji proti terorismu“[6], kde byly předloženy návrhy pro zlepšení prevence, připravenosti a schopnosti reakce na evropské úrovni na teroristické útoky zasahující KI. Cílem tohoto dokumentu je vytvořit optimální úroveň připravenosti a prevence. Dále definuje KI jako „zařízení, služby a informační systémy, které jsou pro státy životně důležité a jejich zničení nebo vyřazení s činnosti způsobí oslabení národní společnosti, národního hospodářství, veřejného zdraví, bezpečnosti a efektivního fungování vládního systému.“[5]

Dokumentem, který konkrétně řešil problematiku KI se stala „Zelená kniha o Evropském programu na ochranu kritické infrastruktury“[7], vydaná komisí evropských společenství 17. 11. 2005 v Bruselu. „Definice, která vymezuje evropskou kritickou infrastrukturu, by měla vycházet z přeshraničního charakteru, který bude mít pouze taková událost, která způsobí vážné důsledky i za hranicemi členského státu, ve kterém se infrastruktura nachází. Dalším prvkem, který by měla brát v úvahu, je skutečnost, že bilaterální režim spolupráce v oblasti ochrany kritické infrastruktury (OKI) mezi členskými státy představuje dobře zavedený a účinný prostředek nakládání s KI přes hranice dvou členských států. Spolupráce tohoto typu by měla doplňovat EPCIP.“[7] Definice tedy zní: „ECI by měla zahrnovat takové materiální zdroje, služby, zařízení informačních

technologií, sítě a majetek, které mají v případě narušení nebo zničení vážný dopad na zdraví, bezpečnost, zabezpečení, hospodářský nebo sociální blahobyt ve:

- dvou a více členských státech – včetně některé kritické infrastruktury bilaterální povahy (podle potřeby)
- třech a více členských státech – kromě veškeré kritické infrastruktury bilaterální povahy.“[7]

„Hlavním cílem zelené knihy je zapojit velké množství subjektů a získat tak od nich konkrétní informace o politikách vhodných pro Evropský program na ochranu kritické infrastruktury (EPCIP). V EPCIP se uvádí „Účinná ochrana kritické infrastruktury vyžaduje komunikaci, koordinaci a spolupráci jak na národní, tak na evropské úrovni, a to mezi všemi zainteresovanými subjekty – vlastníky a provozovateli infrastruktur, regulačními orgány, profesními organizacemi a odvětvovými sdruženími, stejně jako všech úrovní státní a veřejné správy a také veřejnosti.“[7] „Cílem EPCIP by bylo zajistit, aby v rámci celé Evropské unie existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritické infrastruktury, co nejméně možností selhání a rychlá, vyzkoušená nápravná opatření. Úroveň ochrany by neměla být stejná pro všechny CI, ale měla by být odvozená od dopadu, jenž by mohlo způsobit jejich možné selhání..“ „EPCIP by měl co nejvíce minimalizovat veškeré negativní dopady, které zvýšené investice na ochranu mohou mít na konkurenceschopnost příslušného odvětví. Při výpočtu přiměřenosti nákladů nesmíme opomíjet potřebu udržovat stabilitu trhů, která je rozhodující zejména u dlouhodobého investování, ani vliv, jenž taková ochrana má na vývoj akciových trhů a na makroekonomické prostředí.“[7]

Na zelenou knihu navázala 8. prosince 2008 „Směrnice rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.“[8]

1.2.1 Směrnice 2008/114/ES

„Tato směrnice představuje první etapu přístupu krok za krokem, jehož cílem je určit a označit Evropskou kritickou infrastrukturu (EKI) a posoudit potřebu zvýšit jejich ochranu. Směrnice se proto soustředí na odvětví energetiky a dopravy a měla by být přezkoumána s ohledem na posouzení jejího dopadu a nutnost zahrnout do její oblasti

působnosti další odvětví, mimo jiné odvětví informačních a komunikačních technologií.“[8] Dále nám tento dokument definuje KI 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“ a evropskou kritickou infrastrukturu jako: „kritická infrastruktura nacházející se v členských státech, jejíž narušení nebo zničení by mělo závažný dopad pro nejméně dva členské státy. Závažnost dopadu se posuzuje podle průřezových kritérií. To se vztahuje i na účinky způsobené meziodvětvovými závislostmi na jiných typech infrastruktury“[8]

1.3 Česká republika

„Zpráva o národní kritické infrastruktuře“ z 24. 9. 2002 byla prvním dokumentem v rámci Výboru pro civilní a nouzové plánování (VCNP). Zajímal se především vymezením a definováním pojmů jednotlivých oblasti KI. Dále bylo v tomto dokumentu stanoveno zaměření na tyto oblasti:

- systém dodávky energií
- systém dodávky vody
- systém odpadového hospodářství
- přepravní síť
- komunikační a informační systémy
- bankovní a finanční sektor
- nouzové služby (policie, hasičské záchranné sbory, zdravotnictví)
- veřejné služby (zásobování potravin, sociální služby, pohřební služby)

Problematika KI je mezirezortní a dotýká se více subjektů státní či soukromé správy. Jedním ze subjektů státní správy ČR kterého se daná problematika týká je i Bezpečnostní rada státu. Ta pověřila v roce 2003 Ministerstvo vnitra vypracovat aktuální seznam objektů kritické infrastruktury a Ministrovi informatiky, vnitra a NBU předložit návrh zabezpečení informačních systémů nevyhnutelných pro chod KI. V tomtéž roce připravilo Ministerstvo

vnitra po schůzi VCNP materiál s názvem „Projekt Analýza zabezpečení základních funkcí státu včetně ochrany životně důležité infrastruktury v případě krizových situací“. Byl to první ucelený a souhrnný přehled situace v jednotlivých odvětvích KI, včetně právních předpisů a první definice základních funkcí státu při krizových situacích a kritické infrastruktury. Navzdory tomu není žádný legislativní nástroj, který by konkrétně definoval problematiku KI a proto se v současné době zpracovává „Komplexní strategie k řešení problematiky KI“ a následně na to „Národní program ochrany kritické infrastruktury“ které by měly být zpracovány podle „Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie ČR k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury“ Zpracování a přijetí těchto dokumentů se předpokládá do konce roku 2010.

1.4 Oblasti a produkty KI

Kritická infrastruktura je složitý systém a pro jeho lepší ochranu a přehled je i na základě evropského přístupu možné kritickou infrastrukturu rozdělit na:

- úroveň oblastí (sektorů),
- úroveň produktů a služeb(prvků).

Vzhledem k směrnici 2008/114/ES a potřebu její implementace se i národní sektory a prvky budou určovat podobným způsobem jako EKI, tedy s využitím průřezových kritérií.

Oblasti	Produkty a služby
Energie	Produkce ropy a plynu, rafinace, zpracování a skladování, včetně potrubí, výroba elektřiny, přenos elektřiny, plynu a ropy, rozvod elektřiny, plynu a ropy
Informační a komunikační technologie	Informační systémy a ochrana sítí, automatizace přístrojů a kontrolních systémů, internet, poskytování pevných a mobilních telekomunikačních sítí, radiová komunikace a navigace, satelitní komunikace, vysílání

Voda	Zásobování pitnou vodou, kontrola kvality vody, Těsnění a kontrola množství vody
Potrava	Zásobování potravinami a zajištění jejich bezpečnosti
Zdraví	Lékařské a nemocniční péče, léky, séra, očkovací látky a léčiva, bio-laboratoře a bio-látky
Finanční sektor	Platební služby / platební struktury, vládní finanční přiřazení
Státní správa	Zachování veřejného & právního řádu a bezpečnosti, soudní a vězeňská správa
Civilní správa	Funkce vlády, ozbrojené síly, civilní správa služeb, pohotovostní služby, poštovní a kurýrní služby
Doprava	Silniční, železniční, letecká, vnitrozemská vodní a námořní doprava
Chemický a jaderný průmysl	Výroba, skladování a zpracování chemických a jaderných látek, potrubí pro přepravu nebezpečných látek
Vesmír a výzkum	Vesmír a výzkum

Tabulka 1: seznam sektorů a prvků evropské kritické infrastruktury

„Z hlediska náročnosti na zabezpečení ochrany objektů kritické infrastruktury a zásad řešení jejich narušení se předpokládá diferenciace objektů kritické infrastruktury:

a) podle rozsahu postiženého území

Kategorie objektů národního významu, jejichž narušení by mělo dopad na zajištění bezpečnosti státu, ekonomiky, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva na území státu, resp. dvou a více krajů. Následky nefunkčnosti objektů této kategorie řeší subjekty, které je vlastní nebo provozují samostatně nebo ve spolupráci s ministerstvy a ústředními správními úřady, které odpovídají za oblasti a podoblasti, do kterých činnost příslušného subjektu spadá.

Kategorie objektů krajského významu, jejichž narušení by mělo dopad na zajištění základních funkcí území kraje nebo jeho části. Následky nefunkčnosti objektů této kategorie řeší subjekty, který je vlastní nebo provozují samostatně nebo ve spolupráci s krajem, v jehož správním obvodu se objekt nachází nebo ve spolupráci s hasičským záchranným sborem kraje.

b) podle rozsahu dopadů narušení kritické infrastruktury

Kategorie prioritních oblastí či objektů, jejichž narušení ovlivní jiné oblasti kritické infrastruktury a jejich fungování je nenahraditelné nebo obtížně nahraditelné. Následky nefunkčnosti např. dodávek elektřiny, komunikačních a informačních sítí, vybraných dopravních systémů (dálniční síť, dálková železniční přeprava, dopravní systémy velkých aglomerací) nebo jedinečných objektů kritické infrastruktury má dopad na zajištění společenských potřeb přímo i nepřímo tím, že ovlivní fungování dalších oblastí či objektů kritické infrastruktury. Vzhledem k exkluzivitě těchto prioritních systémů a objektů bude nutné zejména k jejich ochraně přijmout zásadní opatření ke zmírnění dopadů jejich narušení. Jde zejména o takové systémy, které mohou být nefunkční narušením jednoho prvku (objektu), např. přenosová energetická soustava. Kategorie ostatních oblastí nebo objektů, jejichž narušení ovlivní společenský život. Jejich fungování lze za přijetí zvláštních organizačních opatření nahradit nebo provizorně řešit s využitím nouzových služeb. Následky nefunkčnosti např. dodávek ropy, zásobování vodou a potravinami, poskytování zdravotní péče, dopravní obslužnosti, bankovních a finančních služeb nebo veřejné správy lze zmírnit opatřeními k eliminaci rizik, a to jak rizik mimořádných událostí, tak i rizik vyplývajících z nefunkčnosti prioritních oblastí či objektů. Jde zejména o náhradní zdroje elektrické energie, zajištění spolupráce s nouzovými službami, organizační opatření k poskytování výrobků a služeb u fungujících objektů kritické infrastruktury a jiná alternativní řešení. Kategorie zvláštních oblastí nebo objektů, jejichž narušení ovlivní společenský život pouze při specifických událostech, tj. při krizových stavech nevojenského a vojenského charakteru.“[9]

2 ANALÝZA SOUČASNÝCH TRENDŮ OCHRANY KI

V této kapitole pojmu ochranu kritické infrastruktury jako rozbor aktuálních dokumentů, které aktuálně ovlivňují danou problematiku ochrany KI a to ne jen v evropském kontextu.

2.1 Bezpečnostní plán provozovatele

Ochrana kritické infrastruktury obecně patří mezi priority zajištění funkční kontinuity společnosti z ekonomického a sociálního hlediska, proto by tato problematika měla být chápána i v souvislostí s národní bezpečností. Je zřejmé, že za udržení funkčností takových infrastruktur by tedy měl nést zodpovědnost stát a jeho výkonné orgány. Ne jen v souvislosti s touto problematikou se však stát zbavuje zodpovědnosti a přenechává ji provozovatelům, kterým z toho titulu vyplývají spíše povinnosti než práva.[10]

Mezi významné aspekty evropských kritických infrastruktur a zároveň mezi nejdůležitější povinnosti jejich provozovatelů je vypracování bezpečnostního plánu provozovatele (OSP – operator security plan), kde se identifikují složky prvků kritické infrastruktury, bezpečnostní řešení a jiné opatření spojené s ochranou. Další povinností je jmenování styčného úředníka pro bezpečnost (SLO – Security Liaison Officer), který je vnímán jako určitá komunikační entita mezi provozovatelem a státem, respektive kontaktním bodem na ochranu ECI (kontaktním bodem se rozumí ministerstvo vnitra, respektive jiný zodpovědný a na koordinaci činnosti v rámci ECI pověřený státní orgán). Vzhledem k tématu práce se budu věnovat této problematice v další kapitole.

2.1.1 Partnerství soukromého a veřejného sektoru

Vytvoření takového partnerství vytváří rámec pro efektivní komunikaci mezi státním a soukromým sektorem, teda mezi zodpovědným a státem určeným ministerstvem provozovatele, respektive majitelem prvku kritické infrastruktury. Vzhledem na to, že v tomto rozsahu vystupuje ministerstvo jako tvůrce legislativních, politických, normalizačních a jiných nástrojů je vytvoření tohoto vztahu jednou z priorit zabezpečení ochrany kritických infrastruktur v rámci celého společenství a není jen na národní úrovni. Výstupem tohoto partnerství je vytvoření komunikačního kanálu, který umožňuje sdílení relevantních informací.

Typickými příklady realizace formou Private public partnership (PPP) jsou projekty v následujících oborech:

- dopravní infrastruktura – dálnice, tunely, mosty, rychlodráhy,
- zdravotnictví – nemocnice,
- školství – univerzitní komplexy, studentské koleje, školy,
- obrana – výzbroj, speciální infrastruktura. [14]

2.2 Bezpečnostní opatření na ochranu prvků KI

Využívání bezpečnostních opatření patří mezi nejdůležitější aspekty ochrany kritické infrastruktury. Rozmanitost těchto opatření, možnost jejich využití a kombinace má stejně pokrokový charakter jako zvyšující se složitost zařízení a systémů a právě tato složitost vyžaduje jejich efektivní využití. Evidentní je v dané problematice i přínos průmyslu komerční bezpečnosti, který svým působením jednoznačně snižuje zranitelnost objektů KI. Součástí bezpečnostní dokumentace jsou také technické prostředky bezpečnostního průmyslu, jejichž použití je kdykoli opodstatněné. Tyto prostředky ochrany můžeme rozdělit do těchto skupin:

- Bezpečnostní opatření pro ochranu prvků v souvislosti s fyzickou a objektovou ochranou.
- Bezpečnostní prostředky a ochrany technických a technologických zařízení a systémů.[11]

2.2.1 Bezpečnostní opatření pro ochranu prvků v souvislosti s fyzickou a objektovou ochranou

Tuto skupinu upravuje „Vyhláška Národního bezpečnostního úřadu (NBÚ) ze dne 13. prosince 1999 o objektové bezpečnosti“.[11] Tato vyhláška stanovuje způsob zabezpečení objektů, technické prostředky, požití technických prostředků, podmínky nasazení fyzické ostrahy a režimová opatření pro účely objektové bezpečnosti. Ochrana objektu se zabezpečuje kombinací bezpečnostních opatření a těmi jsou:

- technické prostředky
- fyzická ostraha objektu

- režimová opatření.[11]

2.2.1.1 Technické prostředky

Za technický prostředek považujeme prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení zabezpečené oblasti nebo objektu. Technickými prostředky například jsou:

- mechanické zábranné systémy (MZS) – tvoří základní část bezpečnostního komplexu, jsou tvořeny soustavou překážek a mají za úkol vytvořit časové zpoždění mezi okamžikem napadení a dokončení napadení. Dále se dělí na:
  - MZS pro obvodovou ochranu – ploty, závory, brány, turnikety, pevné bariéry a jiné
  - MZS pro plášťovou ochranu – mříže, rolety, dveře, zárubně, bezpečnostní skla, rolety, zámky, zámkové vložky a jiné
  - MZS pro předmětovou ochranu – trezory, trezorové skříně, komerční úschovné objekty a jiné
- zařízení elektrické zabezpečovací signalizace (EZS) sloužící k zjišťování a vyhodnocování neoprávněného vstupu
- speciální televizní systémy pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků v objektech
- tísňové systémy, tísňové hlásiče
- zařízení elektrické požární signalizace (EPS).[11]

2.2.1.2 Fyzická ostraha objektu

„Zde se jedná o ochranu chráněného prostoru, která může být vykonávána vyškolenými zaměstnanci provozovatele objektu, příslušníky ozbrojených sil nebo ozbrojených sboru nebo zaměstnanci pověřené bezpečnostní ochranné služby. Provádění fyzické ostrahy objektu je upraveno bezpečnostními standarty Úřadu.“[11]

2.2.1.3 Režimová opatření

„Režimová opatření nám stanovují například oprávnění osob a dopravních prostředků pro vstup do objektu, výstup a výjezd z objektu a způsob kontroly. Podmínky a způsoby kontroly vynášení a vyvážení utajovaných skutečností z objektu. Dále stanovuje režim pohybu osob, dopravních prostředků a utajovaných skutečností, režim manipulace s klíči, identifikačními prostředky a medii, které se používají pro systémy zabezpečení vstupů a režim manipulace s technickými prostředky a jejich používání.“[11]

V této kapitole jsem chtěl také naznačit, že přínos našeho studijního oboru, tedy bezpečnostní technologie, systémy a management má v ochraně kritické infrastruktury důležité místo, a že používání prostředků průmyslu komerční bezpečnosti mají podstatný vliv na tuto problematiku. Používáním těchto prostředku je ale jen jedním z mnoha aspektů ochrany KI.

3 SPECIFIKACE POŽADAVKŮ NA BEZPEČNOSTNÍ PLÁNY PRVKŮ KI

Směrnice rady 2008/114/ES nám v příloze uvádí minimální obsah postupu vypracování bezpečnostního plánu provozovatele EKI. „Plán bezpečnosti provozovatele určuje prostředky kritické infrastruktury a bezpečnostní řešení, která existují či jsou zaváděna na její ochranu. Postup vypracování plánu bezpečnosti provozovatele EKI zahrnuje alespoň:

- určení důležitých prostředků;
- analýzu rizik založenou na scénářích závažných hrozeb, typech zranitelnosti jednotlivých prostředků a možných dopadech a
- určení, výběr a stanovení priorit a protiopatření a postupů s rozlišením mezi
    - - stálými bezpečnostními opatřeními, která určují nezbytné investice do bezpečnosti a bezpečnostní prostředky, jejichž použití je kdykoli opodstatněné. Tato oblast zahrnuje informace týkající se obecných opatření, jako jsou technická opatření (včetně instalace prostředků pro detekci, kontrolu přístupu, ochranu a prevenci); organizační opatření (včetně postupů pro varování a řešení krizí); kontrolní a ověřovací opatření; komunikace; zvyšování informovanosti a odborná příprava; bezpečnost informačních systémů,
    - - odstupňovanými bezpečnostními opatřeními, která mohou být aktivována podle různého stupně rizika a ohrožení.“[8]

O důležitosti ochrany kritické infrastruktury sem pojednával v předešlých kapitolách. Jedním z nejvýznamnějších aspektů ochrany KI je vypracování bezpečnostního plánu. Směrnice 2008/114/ES určuje povinnosti provozovatele v souvislosti s tímto aspektem. Při postupu řešení vypracování plánu bezpečnosti provozovatele se musí určit analyzovat aktuální bezpečnostní prostředky a jiné bezpečnostní řešení v souvislosti s ochranou EKI, které již existují nebo jsou zaváděna na jejich ochranu. V případě, že bezpečnostní opatření existují v dostatečné míře a jsou součástí určitého bezpečnostního plánu a jsou aktualizovány, není zapotřebí vytvářet nový bezpečnostní plán a tím se vyhnout duplicitě. Každý provozovatel EKI musí zajistit vypracování takovýchto plánů bezpečnosti

provozovatele nebo zavedení rovnocenných opatření. Dále je nutné aby byl pravidelně do jednoho roku po označení kritické infrastruktury za EKI prováděn jejich přezkum.

4 ROZBOR DOSTUPNÝCH METODIK ZPRACOVÁNÍ BEZPEČNOSTNÍCH PLÁNŮ POUŽITELNÝCH I VE VZTAHU K OCHRANĚ KRITICKÉ INFRASTRUKTURY

Jako už jsem naznačil na předešlých stránkách této práce je možné v souvislosti s povinností vypracovat bezpečnostní plán, použít i alternativní bezpečnostní dokumenty. V této kapitole se proto zaměřuji na dokumenty a plány které mohou být v této souvislosti použitelné a perspektivě označené jako bezpečnostní plány.

4.1 Zákon o prevenci závažných havárií - 59/2006

„Tento zákon zapracovává příslušné předpisy Evropských společenství, stanoví systém prevence závažných havárií pro objekty a zařízení, v nichž je umístěna vybraná nebezpečná chemická látka nebo chemický přípravek s cílem snížit pravděpodobnost vzniku a omezit následky závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek v objektech a zařízeních a v jejich okolí. Zákon stanovuje povinnosti právnických osob a podnikajících fyzických osob, které vlastní, užívají nebo budou uvádět do užívání takovýto objekt nebo zařízení. Dále stanovuje působnost orgánů veřejné správy na úseku prevence závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky.“[13]

4.1.1 Bezpečnostní program prevence závažné havárie

„V bezpečnostním programu prevence závažné havárie jsou stanoveny zásady a cíle prevence a popis systému řízení bezpečnosti, a to zvláště způsob řízení bezpečnosti podniku, preventivní bezpečnostní opatření a jejich realizace, hodnocení rizik, kontrola plnění cílu, atd.

Bezpečnostní program se člení na následující části:

- základní informace o objektu nebo zařízení, údaje o provozované činnosti a počtech zaměstnanců,
- analýzu a hodnocení rizik závažné havárie v rozsahu odpovídajícím míře rizika závažných havárií a závažnosti jejich následků,
- zásady, cíle a politiku prevence závažné havárie,

- popis systému řízení bezpečnosti,
- závěrečné shrnutí.“[17]

„Provozovatel je povinen na základě rozhodnutí krajského úřadu do návrhu bezpečnostního programu zahrnout preventivní bezpečnostní opatření vztahující se k možnému vzniku domino efektu. Dále je povinen předložit návrh bezpečnostního programu nebo jeho aktualizaci ke schválení krajskému úřadu.“[13]

4.1.2 Bezpečnostní zpráva

„Bezpečnostní zpráva je dokument, který dává informaci o zavedení systému řízení bezpečnosti, zhodnocení rizik a existenci preventivních opatření v objektu nebo zařízení. Uvádí podrobný popis objektu nebo zařízení, identifikaci a hodnocení objektivních rizik, včetně posouzení vlivu lidského činitele, popis scénářů havarijních situací, možných účinků a vlivů při vzniku havárie, podrobný popis preventivních opatření, souborů a systémů technických zařízení zajišťujících bezpečnost provozu a popis disponibilních lidských a materiálních prostředků k zmírnění následků případné závažné havárie.“[18]

„V bezpečnostní zprávě je provozovatel objektu nebo zařízení povinen uvést:

- informace o systému řízení u provozovatele s ohledem na prevenci závažné havárie,
- informace o složkách životního prostředí v lokalitě objektu nebo zařízení,
- technický popis objektu nebo zařízení,
- postup a výsledky identifikace zdrojů rizika (nebezpečí), analýz a hodnocení rizik a metody prevence,
- opatření pro ochranu a zásah k omezení dopadů závažné havárie,
- aktualizovaný seznam
- jmenovitě uvedené právnické osoby a fyzické osoby, podílející se na vypracování bezpečnostní zprávy,
- stanovení politiky prevence závažné havárie a zavést systém řízení bezpečnosti pro její provádění,

- vyhodnocení nebezpečí závažné havárie a navržení a zavedení nezbytných opatření k zabránění vzniku těchto havárií a omezení jejich důsledků na zdraví a životech lidí, hospodářských zvířat, životního prostředí a majetku,
- stanovení zásad bezpečnosti a spolehlivosti přiměřené zjištěnému nebezpečí při stavbě, provozu a údržbě jakéhokoli zařízení, vybavení a infrastruktury spojené s jejím provozem, které představují nebezpečí závažné havárie,
- vypracování zásad vnitřního havarijního plánu a poskytnutí informací umožňující vypracování vnějšího havarijního plánu aby bylo možno provést nezbytná opatření v případě vzniku závažné havárie,
- zajištění odpovídajícího informování příslušných orgánů veřejné správy a obcí pro přijetí rozhodnutí z hlediska rozvoje nových činností nebo rozvoje v okolí stávajících objektů nebo zařízení.“[18]

„Pro vypracování této bezpečnostní zprávy lze využít i dokumenty nebo jejich částí, zpracované podle jiných právních předpisů pro vnitřní potřebu provozovatele, ovšem jen pokud odpovídají svým obsahem požadavkům na bezpečnostní zprávu nebo jsou v jejich smyslu upraveny a doplněny.“[13]

4.2 Vyhláška o fyzické bezpečností a certifikaci technických prostředků

„Tato vyhláška stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku.“[19]

4.2.1 Ověřování opatření fyzické bezpečnosti a vyhodnocení rizik

Provozovatel objektu nebo jím pověřená osoba provádí průběžně ověření, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací. Ověření je třeba provádět minimálně však každých 12 měsíců.

„Vyhodnocení rizik se provádí:

- identifikací stupňů utajovaných informací a zjištěním množství utajovaných informací, které se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následků jejich vyzrazení nebo zneužití,
- popisem a vyhodnocením hrozeb, kterým jsou tyto utajované informace vystaveny,
- popisem a vyhodnocením zranitelnosti utajovaných informací vůči těmto hrozbám,
- stanovením míry rizika, jako „malé“, „střední“ nebo „velké“, na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací.“[19]

4.3 Vyhláška o fyzické ochraně jaderných materiálů a jaderných zařízení

„Tato vyhláška upravuje podrobnosti ke způsobu a rozsahu zajištění fyzické ochrany jaderných materiálů a jaderných zařízení, přeprav a zařazení jaderných materiálů a zařazení jaderných zařízení nebo jejich části do kategorií, k vymezení střeženého, chráněného a vnitřního prostoru jaderných zařízení. Dále upravuje podrobnosti k uchovávání skutečností důležitých z hlediska fyzické ochrany a k rozsahu a způsobu provedení schvalované dokumentace.“[16]

4.3.1 Rozsah a způsob provedení úřadem schvalované dokumentace

„Dokumentace o způsobu zajištění fyzické ostrahy obsahuje především:

- průkaz, že změny původního konstrukčního řešení nesníží úroveň zajištění fyzické ochrany,
- zhodnocení výsledků zkoušek 144 hodinového komplexního vyzkoušení funkčnosti technického systému fyzické ochrany nebo zabezpečovací techniky, výsledků zkoušek televizní techniky, účinnosti fyzické ochrany a testování prvků technického systému nebo zabezpečovací techniky použité pro fyzickou ochranu
- administrativní opatření, kterými jsou například:
    - režimová opatření
    - směrnice pro klíčové hospodářství a vedení příslušné evidence

  - směrnice pro obsluhu, provoz, údržbu a testování technického stavu fyzické ochrany nebo zabezpečovací techniky

- provozní předpisy, případně limity a podmínky jaderného zařízení a opatření týkající se omezení provozu jaderného zařízení při pokusu neoprávněné činnosti
- dohody s policií k zabezpečení pohotovostní ochrany jaderných zařízení a policejního doprovodu přeprav jaderných materiálů a k připojení zabezpečovací techniky na pultu centralizované ochrany policie, pokud byly uzavřeny.“[16]

Tato část byla koncipovaná jako analýza některých legislativních norem, které přímo souvisí s ochranou důležitých infrastruktur a zařízení, tedy obecně s ochranou majetku, informací, života a zdraví obyvatelstva a které ve své podstatě definují požadavky na dokumenty, které v kontextu této práce mohou být chápány, jako ekvivalent bezpečnostního plánu. Uvědomuji si, že tyto normy jsou jen určitými vybranými zástupci, a že složitost dané problematiky by si vyžadovala další výzkum.

ZÁVĚR

Tato práce pojednávala o důležitosti použití bezpečnostního plánu v kontextu ochrany kritické infrastruktury, která byla definovaná a označená hlavně v souvislosti s udržením funkční kontinuity společností, která se svojí závislostí na složitých systémech stává zranitelnější. Ne jen vzpomínaná složitost systémů ale i neustálá změna bezpečnostního prostředí vytvořila potřebu přehodnocení aktuálních přístupů k ochraně majetku a osob. Změnily se požadavky na bezpečnostní dokumentaci, o čem vypovídá i aktuální dokument řešící ochranu evropské kritické infrastruktury – směrnice rady 2008/114/ES o identifikaci a označení evropských kritických infrastruktur a o potřebě zlepšit jejich ochranu. Složitost a časová náročnost vyhotovení bezpečnostní dokumentace a to ne jen v souvislosti s OKI může negativním způsobem ovlivnit aktuální úroveň ochrany majetku a osob. Vytvořil se tu přístup k eliminování duplicity a časové prodlevy. Na základě už vzpomínané směrnice je možné použít ve vztahu k povinnostem provozovatele OKI i jiné dokumenty, které jsem podrobil rozboru a analýze. Přínosem této práce je fakt, že umožňuje potenciálním provozovatelům zorientovat se v dané problematice a za podmínek stanovených směrnicí označit svojí bezpečnostní dokumentaci jako operační plán pro bezpečnost a tím eliminovat už vzpomínanou duplicitu a časovou prodlevu.

CONCLUSION

This thesis deals with the importance of using the security plan in the context of critical infrastructure protection which was defined and described mainly in connection with maintaining functional continuity of companies that its dependence on complex systems is becoming more vulnerable. Not only remembered complexity but also the continuing change of the security environment created a need for reassessment of current approaches to protection of properties and people. The requirements for safety documentation changed. This problem solves a current document about protection of European critical infrastructure – standard 2008/114/ES on the identification and designation of European critical infrastructures and the need of improvement of their protection. The complexity and time-consuming preparation of safety documentation can have negative influence on the current level of protection of persons and properties. There was created an approach to eliminate duplicity and delays. Based on the already remembered standards it is possible to be used in relation to the duties of OKI operators and other documents which were analysed. The contribution of this work is to allow potential operators to understand the relevant issues and in terms of the standards to indicate their security as an operational plan for the safety and to eliminate the remembered duplicity and delays.

SEZNAM POUŽITÉ LITERATURY

[1] The Clinton Administration´s Policy on Critical Infrastructure Protection: Presidential Decision Directive 64, White Paper, 1998, dostupné on-line <http://www.fas.org/irp/offdocs/paper598.htm>

[2] George W. Bush, Vládní nařízení na ochranu kritické infrastruktury, 2001, dostupné on-line < http://www.iwar.org.uk/cip/resources/bush/executive-order.htm >

[3] National strategy for homeland security. Washington : White house, 2002. 90 s. Dostupné z WWW: <http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf>.

[4] Research for secure europe. Luxembourg : Office for Official Publications of the European Communities, 2003. 34 s. Dostupné z WWW: <http://www.src09.se/upload/External%20Documents/gop_en.pdf>.

[5] T 10 Bezpečnostní výzkum. [online]. [s.l.] : [s.n.], 2004. 3 s. Dostupný z WWW: <http://www.vyzkum.cz/storage/att/90A40B9019397F671589C821870D9632/DZSV-RVV-T10.doc>.

[6] Ochrana kritické infrastruktury v boji proti terorismu, dostupné on-line < http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2004)0701_/ com_com(2004)0701_cs.pdf >

[7] Zelená kniha o evropském programu na ochranu kritické infrastruktury. Brusel : Komise evropských společenství, 2005. 26 s. Dostupné z WWW: <http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf>.

[8] SMĚRNICE RADY 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Brusel : Komise evropských společenství, 2008. 8 s. Dostupné z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF >.

[9] Východiska a principy zajištění ochrany kritické infrastruktury v České republice. 112 [online]. 2008, č. 4, [cit. 2010-05-18]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html>.

[10] HROMADA, Martin. Technologické aspekty ochrany kritickej infraštruktúry SR. Zlín, 2010. 45 s. Pojednání o disertační práci k státní závěrečné zkoušce. Univerzita Tomáš Bati ve Zlíně

[11] Česká republika. VYHLÁŠKA Národního bezpečnostního úřadu o objektové bezpečnosti. In Sagit. 1999, částka 108, s. 1. Dostupný také z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb99339&cd=76&typ=r>.

[12] Česká republika. ZÁKON o ochraně utajovaných skutečností a o změně některých zákonů. In Sagit. 1998, částka 52, s. 1. Dostupný také z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb98148&cd=76&typ=r>.

[13] Česká republika. ZÁKON o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky. In Sagit. 2006, částka 25, s. 1. Dostupný také z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb06059&cd=76&typ=r>.

[14] Pppcentrum [online]. 2010 [cit. 2010-05-18]. Stručně o PPP. Dostupné z WWW: <http://www.pppcentrum.cz/index.php?cmd=page&id=122>

[15] HORÁK R., SALINGER T., NAVRÁTIL J., Řešení kritické infrastruktury s možností využití nástrojů EU, Ochrana obyvatel 2007, Ostrava, 2007, ISBN 80-86634-51-5 dostupné on-line < http://www.btv.cz/download/Ochrana_kriticke_infrastruktury _2007.pdf>

[16] Vyhláška státního úřadu pro jadernou bezpečnost o fyzické ochraně jaderných materiálů a jaderných zařízení a jejich zařazování do jednotlivých kategorií. [s.l.] : Státní úřad pro jadernou bezpečnost, 1997. 15 s. Dostupné z WWW: <http://www.sujb.cz/docs/144_97.pdf>.

[17] Portál veřejné zprávy České republiky [online]. 2006 [cit. 2010-05-18]. Dostupné z WWW: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=256/2006&PC_8411_l=256/2006&PC_8411_ps=10#10821>.

[18] Isatech [online]. 2008 [cit. 2010-05-18]. Produkty a služby, prevence závažných havárií. Dostupné z WWW: <http://www.isatech.cz/produkty.html>.

[19] Nbu [online]. 2005 [cit. 2010-05-18]. VYHLÁŠKA o fyzické bezpecnosti a certifikaci technických prostredku, ve znení vyhlášky. Dostupné z WWW: <http://www.nbu.cz/_downloads/pravni-predpisy/container-nodeid-1382/5282005192008.pdf>.

[20] European industrial potential in the field of security research. Brusel : Komise evropských společenství, 2004. 12 s. Dostupné z WWW: <ftp://ftp.cordis.europa.eu/pub/era/docs/communication_security_030204_en.pdf> .

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

KI	Kritická infrastruktura
WTC	Světové obchodní centrum
EACP	Euroatlantická rada partnerství
EU	Evropská unie
OKI	Ochrana kritické infrastruktury
EPCIP	Evropský program na ochranu kritické infrastruktury
EKI	Evropská kritická infrastruktura
VCNP	Výbor pro civilní a nouzové plánování
NBÚ	Národní bezpečnostní úřad
OSP	Bezpečnostní plán provozovatele
SLO	Styčný úředník pro bezpečnost
PPP	Partnerství soukromého a veřejného sektoru
MZS	Mechanické zábranné systémy
EZS	Elektrická zabezpečovací signalizace
EPS	Elektrická požární signalizace

SEZNAM TABULEK