POSTAVENÍ FYZICKÉ OCHRANY U PRVKŮ KRITICKÉ INFRASTRUKTURY

THE ROLE OF PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE ELEMENTS

Martina SYRUČKOVÁ, Petr ROSTEK, Radomír ŠČUREK
martina.syruckova.st@vsb.cz, petr.rostek.st@vsb.cz, radomir.scurek@vsb.cz

Došlo 23. 4. 2012, upraveno 29. 5. 2012, přijato 4. 6. 2012.
Dostupné na http://www.population-protection.eu/
attachments/041_vol4n2_syruckova_rostek_scurek.pdf.

Abstract

The article deals with the issue of legal requirements for physical protection of critical infrastructure elements, the need to fix the role of physical protection and possibilities to identify and asses security threats. It also compares requirements for physical protection of selected facilities and suggests possible measures concerning key security elements.

Key words
Critical infrastructure, physical protection, risk, serious accidents prevention.

Úvod

Kritická infrastruktura tvoří centrální nervovou soustavu moderní společnosti. Jejím prostřednictvím jsou občanům poskytovány nejen služby pokrývající základní životní potřeby, ale zajišťuje také bezpečnost státu a jeho ekonomický rozvoj. Proto je důležité zajistit její funkčnost za jakékoliv situace. Význam kritické infrastruktury vzrůstá v době rozsáhlé mimořádné události, kdy je postiženo velké množství osob a značné území. Za krizových situací představuje nezbytnou podporu pro zasahující složky a vytváří podmínky nepostradatelné pro přežití postižených obyvatel.

Zvláštní postavení v rámci odvětví kritické infrastruktury má oblast energetiky, respektive elektro-energetiky. Elektrická energie hraje klíčovou roli v oblasti kritické infrastruktury, protože na jejích dodávkách a funkčnosti elektrizační soustavy jsou více či méně závislé i ostatní prvky kritické infrastruktury. Z tohoto důvodu by se zvláštní pozornost měla věnovat nejen její ochraně, ale také možnostem obnovy v případě selhání preventivních opatření.

Prvky kritické infrastruktury lze také vnímat jako objekty zvláštního významu [1], z čehož vyplývá potřeba řešit bezpečnostní problematiku těchto prvků před širokým spektrem hrozeb. Ty mohou být způsobeny nejen nepříznivými přírodními jevy a technickými závadami, ale také bezpečnostními

hrozbami, které lze vnímat jako protiprávní činnost, jež je motivovaná různorodými pohnutkami (např. pomsta nespokojeného zaměstnance nebo zákazníka, movitý zisk, zviditelnění se).

Komparace řešené problematiky

V současnosti právní řád [2] ČR rozlišuje objekty a zařízení, ale také významné prvky kritických infrastruktur, které by v případě narušení funkčnosti měly významný vliv na bezpečnost v území. V následujících podkapitolách budou analyzovány a vzájemně porovnávány legislativní požadavky, týkající se problematiky prevence závažných havárií a kritické infrastruktury.

Požadavky zákona o prevenci závažných havárií

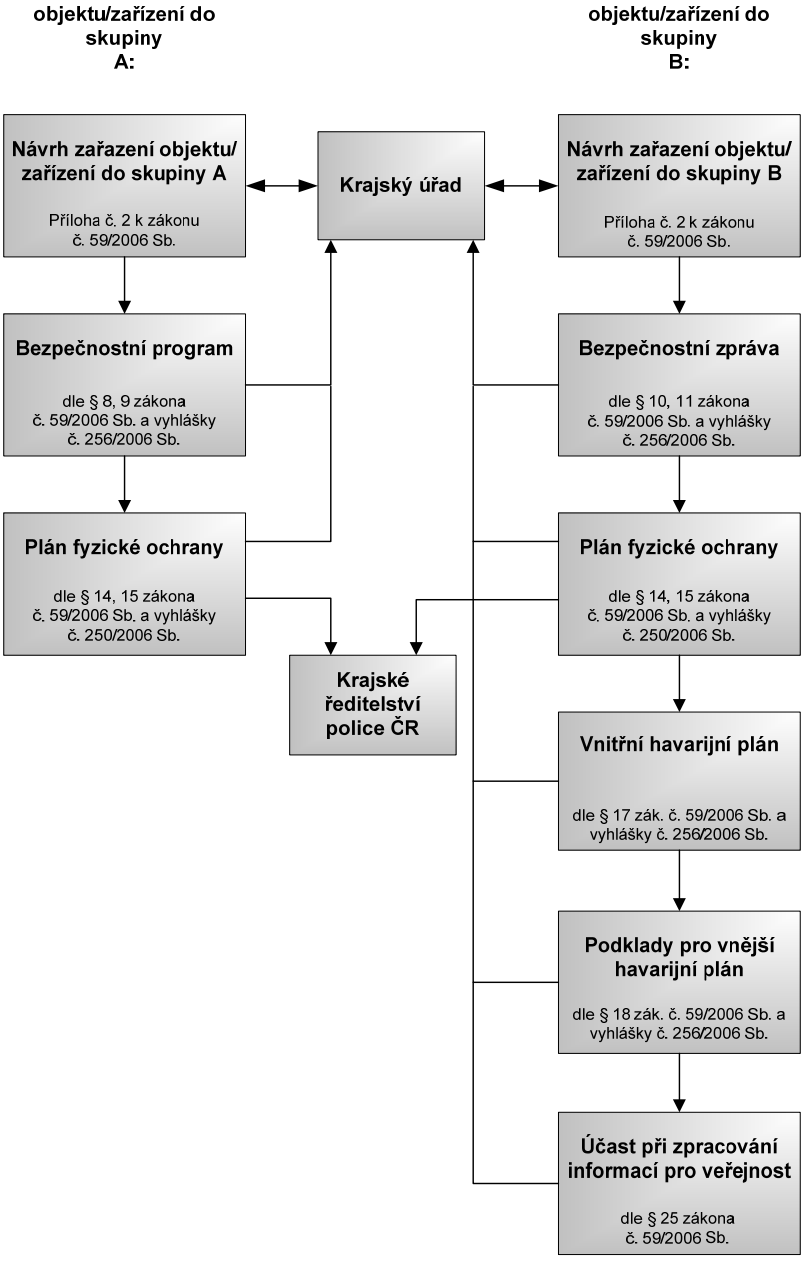
Problematikou závažné havárie se zabývá zákon [2] o prevenci závažné havárie, který mimo jiné specifikuje závažnou havárii jako *mimořádnou, částečně nebo zcela neovladatelnou, časově a prostorově ohraničenou událost, například závažný únik, požár nebo výbuch, která vznikla nebo jejíž vznik bezprostředně hrozí v souvislosti s užíváním objektu nebo zařízení, v němž je nebezpečná látka vyráběna, zpracovávána, používána, přepravována nebo skladována, a vedoucí k vážnému ohrožení nebo k vážnému dopadu na životy a zdraví lidí, hospodářských zvířat a životní prostředí nebo k újmě na majetku*. Zákon dále definuje pojmy, jako jsou objekt/zařízení či provozovatel objektu/zařízení nakládající s nebezpečnou látkou.

Provozovateli nakládajícímu s nebezpečnou látkou je zákonem definovaným způsobem dána povinnost zpracovat návrh na zařazení objektu nebo zařízení do systému prevence závažných havárií. V samotné definici závažné havárie je uvedeno, že např. závažný únik, požár nebo výbuch může vést k vážnému ohrožení nebo k vážnému dopadu na životy a zdraví lidí, hospodářských zvířat a životního prostředí.

Dopad havárie je podobný dlouhodobé zátěži životního prostředí průmyslovou činností s tím rozdílem, že při havárii může dojít poměrně rychle k nevratným změnám či zničení životů lidí a organismů nebo zničení materiálních hodnot. Pro podnik znamená havárie hlavně ztráty na poli image a obchodního trhu, například ztrátou zájmu odběratelů, více než přímé materiální ztráty a pokles výroby.

Požadavky zákona na bezpečnostní dokumentaci

Základní povinnosti vyplývající ze zákona o prevenci závažných havárií pro průmyslové podniky jsou znázorněny ve schématu (viz obrázek č. 1). Podle zařazení objektu nebo zařízení (skupina A – menší množství nebezpečných látek na území podniku, skupina B – větší množství nebezpečných látek) vyplývají zákonné požadavky na zpracování bezpečnostní dokumentace.



Obr. 1
Postup vypracování bezpečnostní dokumentace podle zákona o prevenci závažných havárií (upraveno dle [2])

Jednou ze základních povinností je u objektu i zařízení zařazených do skupiny A nebo B zpracovat plán fyzické ochrany. Rozsah a obsah bezpečnostních opatření implementovaných v plánu fyzické ochrany jsou upraveny zejména §14 a §15 zákona [2] a z něho vyplývající vyhlášky [5].

Požadavky zákona o krizovém řízení

V České republice vyústil mnohaletý vývoj v oblasti kritické infrastruktury přijetím novely krizového zákona [3], ve kterém byla implementována Směrnice Evropské rady [12]. Přijetím novely krizového zákona došlo ke změně doposud platných definic a také ke změně diferenciovaného přístupu k pojetí kritické infrastruktury. Novela krizového zákona definuje kritickou infrastrukturu *jako prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu*. Pokud by kritická infrastruktura měla v případě narušení závažný dopad i na další členský stát Evropské unie, hovoříme o evropské kritické infrastruktuře.

Prvkem kritické infrastruktury, jež je definován prostřednictvím výše jmenovaného legislativního předpisu, se pak rozumí *zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určená podle průřezových a odvětvových kritérií.* Subjektem kritické infrastruktury *se má na mysli provozovatel prvku kritické infrastruktury.*

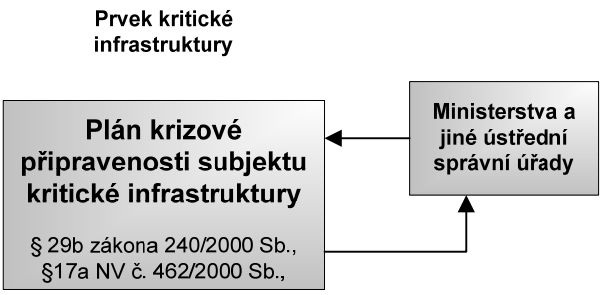
Pro určení prvku kritické infrastruktury je nutná aplikace průřezových a odvětvových kritérií, která jsou specifikována v samostatném právním předpise [6]. Průřezové kritérium charakterizuje závažný dopad prvku kritické infrastruktury, jako hlediska:

- rozsahu ztrát na životě, dopadu na zdraví osob,
- mimořádně vážného ekonomického dopadu nebo
- dopadu na zdraví osob v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života.

Oproti tomu je odvětvové kritérium zastoupeno jednotlivými oblastmi kritické infrastruktury a jedná se o především o provozní a technické hodnoty sloužící k určení prvku kritické infrastruktury.

Požadavky na bezpečnostní dokumentaci

Subjektu kritické infrastruktury je dáno za povinnost zpracovat plán krizové připravenosti subjektu kritické infrastruktury. Povinnost zpracovat tento bezpečnostní dokument, identifikující možná ohrožení funkce prvku kritické infrastruktury, včetně stanovených opatření na jeho ochranu, ukládá jak zákon o krizovém řízení [3], tak prováděcí právní předpis k tomuto zákonu, zejména pak nařízení vlády [7].



Obr. 2
Postup vypracování bezpečnostní dokumentace podle zákona o krizovém řízení

Komparace

Pro přehlednost je uvedená komparace řešené problematiky znázorněná v tabulce č. 1. I když je daná problematika velmi rozdílná (nebezpečné látky x služby kritických infrastruktur), je zde možné sledovat společné náležitosti.

Společné požadavky je možné nalézt např. v identifikaci objektu. Jelikož objekt nebo zařízení je identifikováno na základě množství nebezpečné látky, tedy jejího limitního množství. U prvku kritických infrastruktur je odvětvové kritérium dáno technickými a provozními hodnotami, tedy limitami, které slouží pro určení potenciálního prvku kritické infrastruktury. Rozdílnost hodnocení je zřetelná např. u klasifikace dopadu a požadavkům na bezpečnostní dokumentaci.

Klasifikace dopadu je u objektu a zařízení nakládajícího s nebezpečnou látkou vyjádřena jako hledisko, které znázorňuje poškození života a zdraví, životního prostředí a také majetku. Oproti tomu u prvku kritické infrastruktury se závažnost dopadu týká rozsahu ztrát na životě, dopadu na zdraví osob, ekonomického dopadu nebo dopadu na veřejnost. Limitní hodnoty klasifikující závažný dopad, uvedené v průřezovém kritériu, jsou mnohonásobně vyšší než u prevence závažných havárií. Lze dovodit, že narušení funkčnosti prvku kritické infrastruktury má celostátní, popřípadě také evropský rozměr. Z výše uvedeného textu vyplývá, že narušení kritické infrastruktury nebude mít vliv na životní prostředí, jelikož toto kritérium není definováno v procesu identifikace prvku kritické infrastruktury v průřezovém kritériu.

Požadavky zákonů na bezpečnostní dokumentaci jsou velice rozdílné. Pokud pomineme jejich rozdílné odvětvové zaměření, vyvstává zde problém ohledně zajištění fyzické ochrany prvku kritické infrastruktury. Z analýzy právních předpisů týkajících se kritické infrastruktury tato povinnost nevyplývá. Přičemž subjekt kritické infrastruktury podle § 29a krizového zákona [3] odpovídá za ochranu prvku kritické infrastruktury. Tedy musí podle analýzy rizik mimo jiné vyhodnotit, zda prvek je zranitelný vůči protiprávním činům, a také možnosti

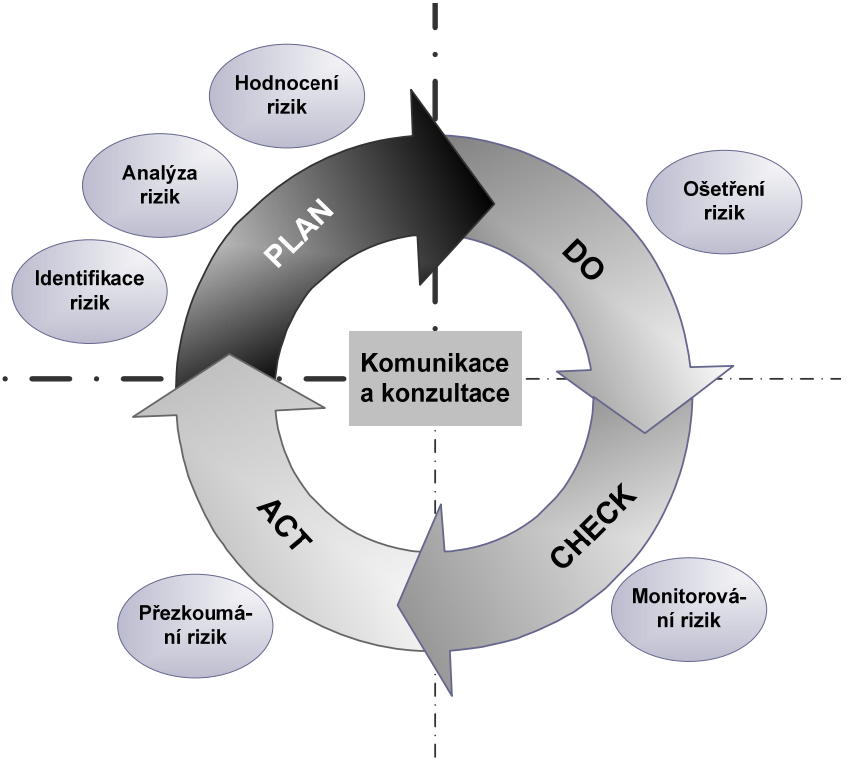
teroristického útoku. Následně by měl pak přijmout opatření k zajištění fyzické ochrany prvku kritické infrastruktury.

Tabulka 1
Komparace řešené problematiky

<table>
<tr><th></th><th colspan="2">Oblast prevence závažných havárií</th><th>Oblast kritické infrastruktury</th></tr>
<tr><td>Předmět</td><td colspan="2">Nebezpečná látka</td><td>Služby kritických infrastruktur</td></tr>
<tr><td>Legislativa</td><td colspan="2">Zákon č. 59/2006 Sb., o prevenci závažných havárií</td><td>Zákon č. 240/2000 Sb., o krizovém řízení</td></tr>
<tr><td>Objekt</td><td colspan="2">Objekt a zařízení</td><td>Prvek kritické infrastruktury</td></tr>
<tr><td>Subjekt</td><td colspan="2">Provozovatel objektu nebo zařízení</td><td>Provozovatel prvku kritické infrastruktury, případně evropské kritické infrastruktury</td></tr>
<tr><td>Identifikace</td><td colspan="2">Limitní množství nebezpečné látky</td><td>Průřezová a odvětvová kritéria</td></tr>
<tr><td rowspan="3">Klasifikace dopadu</td><td colspan="2">Hledisko životu a zdraví osob</td><td>Prahové hodnoty - rozsah ztrát na životě, dopad na zdraví osob</td></tr>
<tr><td colspan="2">Hledisko poškození životního prostředí</td><td>Prahová hodnota - vážný ekonomický dopad nebo</td></tr>
<tr><td colspan="2">Hledisko poškození majetku</td><td>Prahové hodnoty - dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života</td></tr>
<tr><td rowspan="6">Bezpečnostní dokumentace</td><td>Skupina A</td><td>Skupina B</td><td>Subjekt kritické infrastruktury</td></tr>
<tr><td>Návrh zařazení</td><td>Návrh zařazení</td><td>Plán krizové připravenosti subjektu kritické infrastruktury</td></tr>
<tr><td>Bezpečnostní program</td><td>Bezpečnostní zpráva</td><td rowspan="5"></td></tr>
<tr><td>Plán fyzické ochrany</td><td>Plán fyzické ochrany</td></tr>
<tr><td rowspan="3"></td><td>Vnitřní havarijní plán</td></tr>
<tr><td>Podklady pro vnější havarijní plán</td></tr>
<tr><td>Účast při zpracování informací pro veřejnost</td></tr>
</table>

Management rizik v oblasti fyzické ochrany

Prvním krokem procesu snižování rizik je jejich analýza. Jedná se o proces definování hrozeb, pravděpodobnost jejich uskutečnění a dopadu na chráněné zájmy (aktiva), z čehož následně vyplynou rizika a jejich závažnost. Zde je třeba zdůraznit, že každý prvek kritické infrastruktury, jeho zranitelnost nebo atraktivita vůči vytypovaným hrozbám je značně odlišná, proto jsou požadavky na bezpečnostní opatření značně individuální. Prostřednictvím analýz lze provádět strategické plánování v oblasti prevence nebo represe. V průběhu času se aktiva i hrozby mohou v důsledku různých faktorů měnit. Systém managementu bezpečnosti, který formuluje záměry a bezpečnostní strategii organizace, musí být schopný na tyto změny pružně reagovat. Proto se doporučuje využívat metodu Demingova cyklu (PDCA = Plan – Do – Check – Act) [8], který je znázorněn na obrázku 3. Model se v organizacích zavádí zejména proto, aby nebyla přijímána nepromyšlená opatření, jejichž účinnost bude nedostatečná, neefektivní a způsobí organizaci zbytečné výdaje.



Obr. 3
Proces řízení rizika podle ISO/EIC 31000:2009 implementovaný do PDCA [9]

Jak vyplývá z obrázku 3, v části cyklu s označením PLAN se provádí kroky, které tvoří základ procesu řízení rizika. Důležitým krokem v celém procesu snižování rizik je správný výběr vhodné metody, bezpečnostní management by měl zvážit, jaké údaje má k dispozici, zdali tvoří vhodné vstupy pro vybranou analýzu a také zdali analýza splňuje jejich požadavky na výstupní informace, které lze prostřednictvím analýzy získat.

Postup při analýze rizik

1. Stanovení hranice analýzy rizik

Hranice analýzy rizik stanovuje aktiva, která budou zahrnuta do analýzy, od aktiv ostatních. Je stanovena záměrem managementu nebo z úvodní studie (pokud byla zpracována). Uvnitř hranice budou ležet jednotlivá aktiva, ze kterých je subjekt složen, nebo jsou z hlediska aktuálního záměru relevantní. Dále je nutné vzít v potaz rizika ohrožující aktiva jak z vnitřního, tak z vnějšího prostředí [10]. V této části analýzy by se měl také popsat hodnocený objekt a jeho umístění (např. snadná dostupnost, umístění stranou od urbanizace).

2. Identifikace aktiv

Identifikace spočívá ve vytvoření soupisu všech aktiv ležících uvnitř hranice analýzy rizik. Při rozhodování o zařazení daného aktiva na soupis se uvede název aktiva a jeho umístění [10]. Hodnota aktiva se vyjadřuje z ekonomického hlediska finanční částkou.

3. Stanovení hodnoty a seskupování aktiv

Posuzování hodnoty aktiva je založeno na velikosti škody způsobené zničením či ztrátou aktiva. Velmi podstatné je rozlišit, zda se jedná o jedinečné aktivum nebo o aktivum jednoduše nahraditelné. Do hodnoty se promítá závislost subjektu na existenci, ale i na správném fungování hodnoceného aktiva, tedy k jakým škodám dojde omezením funkčnosti nebo ztrátou aktiva, než dojde k jeho obnově. Hodnota aktiva pro analýzu rizik se může stanovit také jako vážený průměr hodnot podle všech použitých hledisek. [10]

Vzhledem k tomu, že aktiv je obvykle veliké množství, snižuje se jejich počet tak, že se provede seskupení aktiv podle různých hledisek, aby se vytvořily skupiny aktiv podobných vlastností. Seskupovat se mohou aktiva podobné kvality, ceny, účelu apod. Takto vytvořená skupina aktiv pak dále vystupuje jako jedno aktivum. Potom se musí zabezpečit, aby protiopatření, navržená v etapě zvládání rizik pro skupinu aktiv, byla aplikována na všechna aktiva, která jsou do této skupiny sdružena. [10]

Se stanovením hodnoty aktiva souvisí také míra snižování rizika, kdy riziko je nutné snižovat na takovou úroveň, dokud se výdaje na snížení rizika stávají neúměrnými ve srovnání s příslušným omezením rizika, uplatňuje se zde princip ALARA (výdaje na optimalizaci systému by neměly přesáhnout hodnotu 10 - 15% ceny aktiva). [11]

4. Identifikace hrozeb

V této etapě analýzy rizik se identifikují hrozby, které připadají pro analýzu v úvahu. Identifikace hrozeb se provádí tak, že se vybírají ty, které by mohly ohrozit alespoň jedno z aktiv subjektu. Pro identifikaci hrozeb lze vycházet ze seznamu hrozeb, sestavených podle literatury, vlastních zkušeností, průzkumů dříve provedených analýz. Hrozby se mohou odvozovat také od subjektu, jeho statusu (podnikatelský subjekt, orgán státu, nezisková organizace, atd.) [10].

5. Popis současného způsobu zabezpečení

Bezpečnostní hrozby může podstatnou mírou snižovat nebo zvyšovat současný způsob zabezpečení posuzovaného prvku. V této fázi se popisují a hodnotí technická a režimová opatření, kterými posuzovaný objekt disponuje, případně fyzická ostraha (např. způsob zabezpečení střežení, způsob provádění střežení, rozsah střežení), je-li k dispozici. V rámci objektu mohou být stanoveny tzv. bezpečnostní zóny, které mají režimovým a technickým opatřením upravený systém vstupu jednotlivých kategorií uživatelů (vnější zóna objektu, zóna s přístupem veřejnosti, zóna zaměstnanců, interní zóna a interní chráněná zóna). Vhodným rozdělením aktiv do jednotlivých bezpečnostních zón a jejich správným zabezpečením se může předejít protiprávní činnosti insiderů.

6. Analýza hrozeb a zranitelností

Každá hrozba se hodnotí vůči každému aktivu (skupině aktiv). Aktiva, na které může mít hrozba dopad, budou ohodnocena z hlediska úrovně hrozby a zranitelnosti aktiva vůči této hrozbě. Při stanovení úrovně hrozby se vychází z faktorů, jako nebezpečnost, motivace a přístup. Pro stanovení úrovně zranitelnosti se vychází z faktorů, jako citlivost a kritičnost.

Analýza hrozeb a zranitelností vyhodnocuje i realizovaná protiopatření. Přijatá protiopatření mohou snížit jak úroveň hrozby, tak úroveň zranitelnosti aktiv. Výsledkem analýzy je seznam dvojic „hrozba-aktivum“ (pouze těch dvojic, kde se hrozba může vůči aktivu uplatnit) se stanovenou úrovní hrozby a zranitelnosti. [10] Analýza bezpečnostních rizik musí prověřit:

- vnější vlivy (stavební dispozice, okolní prostředí, snadnost přístupu);
- chráněné hodnoty (význam objektu, majetku, informací v objektu);
- historii kriminality v objektu a dané lokalitě;
- bezpečnostní rizika (možné hrozby z vnějšku, pravděpodobnost jejich uplatnění, dopad na aktiva, možnost útoku insidera).

7. Pravděpodobnost jevu

Občas nevíme, zdali jev, který zkoumáme, nastane. Jde o situaci, kdy soubor výchozích podmínek vždy nevede ke stejnému výsledku. V takovém případě k popisu určitého jevu doplňujeme údaj, s jakou pravděpodobností tento jev může nastat. Abychom mohli počítat s pravděpodobnostmi, musíme určit, zdali je analyzovaný jev náhodný či nikoliv, zda patří do určitého intervalu pravděpodobnosti, případně zda jej můžeme vyloučit, jaké jsou jeho pravděpodobnostní charakteristiky. Pro výpočet pravděpodobnosti je výhodné

používat metody matematické statistiky. Tyto metody v sobě zahrnují např. střední hodnoty, rozptyl, směrodatnou odchylku, dále lze využít metody matematicko-statistické indukce (statistické rozdělení, náhodný výběr, teorie odhadu, testování statistických hypotéz, regresivní a korelační analýza). [10]

Vytypované metody

Metod existuje nepřeberné množství, jak bylo již uvedeno v kapitole management rizik v oblasti fyzické ochrany, musí bezpečnostní manažer zvážit, jaký výstup informací chce použitou metodou získat. Pokud není k dispozici úvodní studie, doporučuje se jako první udělat screeningovou metodu – např. *Ishikawův diagram, Kontrolní seznam, Katalogový list, Studie nebezpečí a kritické kontrolní body (HAZOP), Analýza příčin a důsledků nebo Brainstorming*.

Prostřednictvím uvedených metod se naleznou aktiva a hrozby v posuzovaném systému. Následuje samotná analýza rizika, pomocí ní se stanovují následky, pravděpodobnost výskytu hrozby a úroveň rizika. Vhodné metody pro posouzení jsou např. *What – If, FMEA, FTA – Analýza stromem poruch, ETA – Analýza stromem událostí, Matice následků a pravděpodobností*. Neměli bychom opomenout ani *Analýzu souvztažnosti*, kterou lze hodnotit celé objekty. Pomocí ní lze určit vazby mezi zdroji rizik a postiženými objekty. Posuzuje celkové riziko (zohledňuje vznik domino efektu nebo synergických efektů). V neposlední řadě se nabízí také metoda *CARVER* [13], která na rozdíl od předešlých metod nehodnotí bezpečnostní systém prvku z pohledu obránce, ale pohlíží na problematiku bezpečnosti z pohledu útočníka. Cílem je nalézt cestu nejmenšího odporu, která bude mít zároveň nejefektivnější výsledky v případě napadení vytypovaného cíle.

Na základě zpracovaných analýz budou nalezeny nejvážnější bezpečnostní hrozby ohrožující existenci a funkčnost prvku kritické infrastruktury. Bezpečnostní management na základě zjištěných informací navrhne systém fyzické ochrany a implementuje jej do provozu prvku kritické infrastruktury. Přijatá opatření mohou být technická (např. vhodné umístění poplachových zabezpečovacích systémů, mechanické zábranné systémy, systémy ochrany proti požáru), dále pak režimová (např. vstupní režim objektu, režim návštěv, klíčový režim a režim uzamykání prostor, oprávnění fyzické ostrahy) a fyzická ostraha. Fyzická ostraha zabezpečuje ochranu osob, jejich životů a zdraví, ochranu majetku, dozor nad režimovými opatřeními, ale také plnění úkolů požární ochrany a bezpečnosti a ochrany zdraví při práci.

Résumé

Using cross-sector and cross-cutting criteria, the most significant elements of a country's infrastructure are identified. These elements should be either subject to permanent protection or there should be a system which provides operative protection in case the elements are a target of potential threat. Destruction or distraction of the elements' function can have a local impact, such as in objects from group A or B, or they might affect the the country as a whole.

They might even affect other continental states, e.g. in the field of electro-energetics, or cause a domino-effect.

Results of comparison have revealed that despite falling into different fields of interest, the jointly assessed buildings, facilities and elements have both common and different features. A physical security plan is one of the most important parts of a security documents of a building and a facility with the need of serious accidents prevention. However, there is no legislative obligation to devise such plan which might suggest that illegal activity is not considered to be such a significant threat and elements of critical infrastructure do not need to be obliged to devise and implement a physical protection plan.

The article suggests possible uses of risk-analysing methods which have been implemented in physical protection and can be used to propose security measures against selected threats. Nuclear energetics can serve as a source of inspiration as this field boasts the most developed system of physical protection. Another source which can be used are findings included in Act 59/2006 Coll. on the prevention of serious accidents caused by selected hazardous chemical substances or chemical preparations as amended followed by directive 250/2006 as amended, which sets the extent and content of security measures concerning physical protection of a building or facility from group A or B. Closely connected with building protection is also National Security Authority (NBÚ) directive 339/1999 Coll. on building security.

Literatura

[1] ŠENOVSKÝ, Michail. *Objekty zvláštního významu a kritická infrastruktura*. Ostrava: SPBI, 2005. ISBN 80-86634-66-3.

[2] Zákon č. 59/2006 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými přípravky, ve znění pozdějších předpisů.

[3] Zákon č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů.

[4] BERNATÍK, Aleš. *Prevence závažných havárií I*. 1. vyd. Ostrava: SPBI, 2006. 89 s. ISBN 80-86634-89-2.

[5] Vyhláška č. 250/2006 Sb., kterou se stanoví podrobnosti o rozsahu bezpečnostních opatření fyzické ochrany objektu nebo zařízení zařazených do skupiny A nebo do skupiny B, ve znění pozdějších předpisů.

[6] Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů.

[7] 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 pozdějších předpisů.

[8] VEBER, Jaromír, et al. *Řízení jakosti a ochrana spotřebitele.* 2. vyd. Praha: Grada Publishing, a.s., 2006. 204 s. ISBN 978-80-247-1782-1.

[9] ROSTEK, Petr, SYRUČKOVÁ, Martina. Posuzování rizik kritické infrastruktury se zaměřením na elektrizační soustavu. In *Sborník vědeckých*

prací Vysoké školy báňské – Technické univerzity Ostrava, v tisku.
[10] SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 3. vyd. Praha: Grada Publishing, a.s., 2009. 360 s. ISBN 978-80-247-3051-6.
[11] ŠČUREK, Radomír. *Analýza rizik objektů kritické infrastruktury* [online]. [cit. 20. 2. 2012]. Dostupné na WWW: <http://www.population-protection.eu/attachments/038_vol3n1_scurek.pdf >.
[12] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.
[13] GrowJOB [online]. [cit. 15. 3. 2012]. Dostupný na WWW: <http://www.growjob.com/clanky-personal/metoda-carver/>.