PROBLEMATIKA ZABEZPEČENÍ OBJEKTŮ KRITICKÉ INFRASTRUKTURY ČESKÉ REPUBLIKY

Michaela Vašková[1]

ABSTRAKT

Práce pojednává o problematice zabezpečení objektů kritické infrastruktury České republiky. Vzhledem ke stále rostoucí důležitosti prvků kritické infrastruktury, roste i potřeba její ochrany. Z tohoto důvodu je nutné znát slabá místa objektu, která mohou být zneužita teroristy. Nejpravděpodobnější formou teroristického útoku na kritickou infrastrukturu je za použití výbušných látek a sloučenin. Proto je nutné zabezpečit jejich včasnou detekci a identifikaci.

Kľúčové slová: Kritická infrastruktura, ochrana, bezpečnostní audit, zabezpečení objektu

ABSTRACT

The paper is about the security of critical infrastructure objects in the Czech Republic. Because of the ever increasing importance of critical infrastructure objects, there is growing need for its protection. For this reason, it is necessary to know vulnerabilities of the object, which can be abused by terrorists. The most likely form of terrorist attack on critical infrastructure is using explosive substances and compounds. Therefore, it is necessary to ensure their timely detection and identification.

Key words: Critical infrastructure, protection, safety audit, object security

ÚVOD

Zajištění dostatečné míry ochrany objektů kritické infrastruktury před protiprávními činy představuje ucelený soubor aplikovaných bezpečnostních opatření prováděných státem a jednotlivými subjekty. Výchozím prvkem je legislativní nastavení těchto opatření. To by v optimálním případě mělo být provedeno tak, aby v případě správné aplikace těchto bezpečnostních opatření byla zvýšena

[1] Michaela Vašková, Ing., Fakulta vojenského leadershipu, Univerzita obrany, Kounicova 65, 602 00 Brno, tel.: +420 973 443 913, e-mail: michaela.vaskova@unob.cz

pravděpodobnost zabránění protiprávních činů na přijatelné (společensky akceptované) minimum.

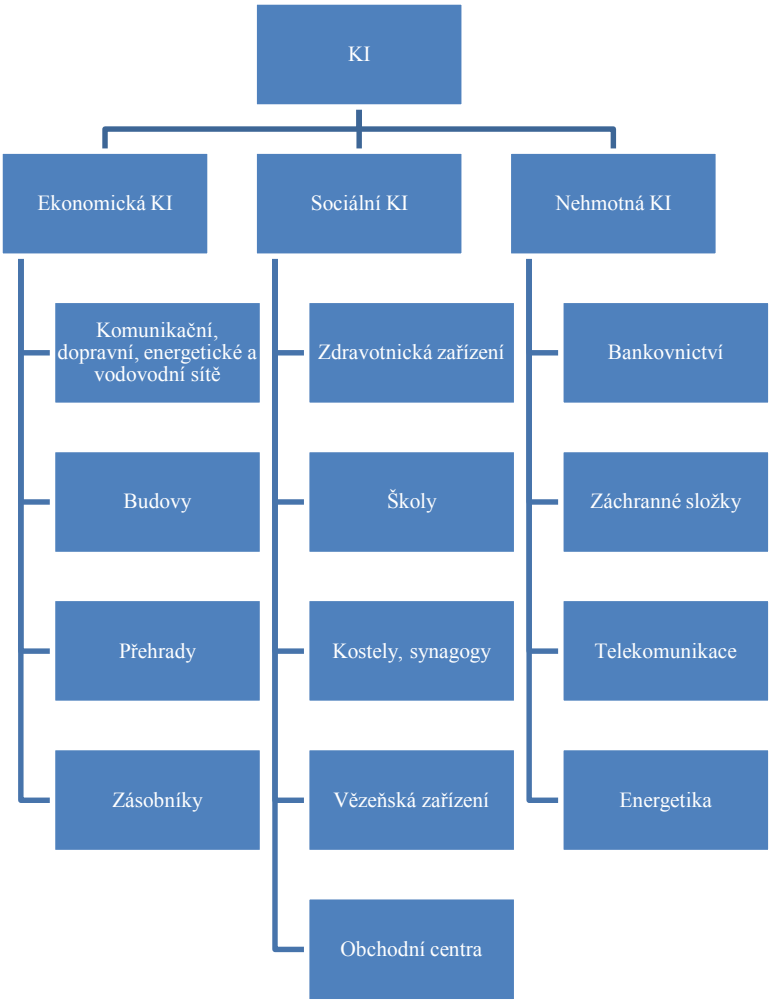
Vnesení zakázaného předmětu do vyhrazeného prostoru objektu kritické infrastruktury a jeho následné zneužití pachatelem představuje jeden ze základních prvků možného protiprávního činu proti bezpečnosti. Teroristické útoky spáchané zneužitím zakázaného předmětu, nejčastěji výbušnin [1], lze zařadit k útokům s největšími dopady na lidské životy. Důsledky těchto selhání bezpečnosti pak zprostředkovaně vedly k nejrůznějším krizím, válečným konfliktům, k ekonomickým kolapsům či k zásadním změnám právních systémů a jejich zákonných nástroj [2].

Pro účely této práce byl vybrán objekt dopravní letecké kritické infrastruktury České republiky, který však z důvodu citlivosti údajů nemůže být přesně jmenován, ani zde nelze uvádět konkrétní bezpečnostní mezery či opatření. Z tohoto důvodu jsou v článku uvedeny informace pouze v obecné rovině.

1 KRITICKÁ INFRASTRUKTURA

Ze společenského hlediska se kritickou infrastrukturou rozumí vzájemně propojené sítě či systémy, které obsahují různá odvětví, instituce, lidi a postupy, poskytující spolehlivý tok produktů a služeb, potřebných pro zajištění obrany a ekonomickou bezpečnost. Ekonomickou bezpečnost lze chápat jako konkurenceschopnost státu na globálních trzích. K ekonomické bezpečnosti se přidává i bezpečnost fyzická, která se týká zajištění ochrany fyzických aktiv a kybernetická bezpečnost, která se zabývá ochranou před neautorizovanými přístupy do počítačové sítě nebo před jejich poruchami [3].

V souvislosti s kritickou infrastrukturou nejde pouze o výjimečné situace ohrožení státu, ale především o zachování běžného chodu společnosti. Obecně se ze společenského hlediska kritická infrastruktura skládá z ekonomické, sociální a nehmotné infrastruktury. Přičemž ekonomická infrastruktura obsahuje komunikační, dopravní, energetické a vodovodní sítě, dále budovy, továrny, zásobníky, přehrady a další. Sociální infrastruktura se skládá z fyzických zařízení, jako jsou nemocnice, školy, kostely, stadiony, parky, obchodní centra, věznice, atd. A v neposlední řádě nehmotná infrastruktura, která je složena z nemateriálních aktiv vyjadřujících schopnosti a zdravotní stav komunity, její produktivitu a vlastnosti. Pro lepší přehlednost je dělení kritické infrastruktury ze společenského hlediska zobrazeno v obr. 1 [3].



Obrázok 1 Složení kritické infrastruktury ze společenského hlediska [3]

Kritická infrastruktura se v jednotlivých zemích světa definuje různě. Záleží především na problémech, se kterými se jednotlivé země potýkají, na jejich historii a zvyklostech [3]. Společné všem definicím je důraz kladený na nutnost správného fungování kritické infrastruktury a její důležitost pro chod společnosti.

Kritická infrastruktura České republiky je definována dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) 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 [4].

1.1 OCHRANA KRITICKÉ INFRASTRUKTURY

Ochrana kritické infrastruktury představuje ucelený systém, jehož kvalita závisí na všech jeho částech. Formy ochrany objektů kritické infrastruktury se rozdělují na tři části:

- organizační,
- informační,
- technická.

Pro efektivní volbu metod a prostředků, jakými objekty chránit, je třeba vycházet z předem provedeného průzkumu chráněného objektu, jeho důležitosti a důležitosti jeho okolí, požadované účinnosti ochrany a především z analýzy rizik. Dále rozborem adekvátního rozsahu ochrany, posouzením stávajících, vytvořených i přirozených ochranných mechanismů z hlediska možností jejich využití v novém systému ochrany a komplexní návrh nového systému, jež lze v budoucnosti modifikovat podle stávajících potřeb kritické infrastruktury [5].

1.1.1 ORGANIZAČNÍ OPATŘENÍ

Organizační opatření použitá při ochraně objektů kritické infrastruktury jsou zaměřená proti lidským chybám, chybějícím nebo nedokonale nastaveným provozním postupům, selhání techniky, či jiným náhodným vlivům [6]. Zpracování organizačních opatření a režimů ochrany vychází z bezpečnostní studie, která obsahuje výsledky průzkumu chráněného objektu, vyznačení citlivých míst objektu i celého systému v jejich kritických a snadno zranitelných místech [5]. Organizační opatření se rozdělují na:

- systém řízení fyzické bezpečnosti,
- řízení rizik,
- bezpečnostní politika a organizační bezpečnost,
- bezpečnost lidských zdrojů,
- plánování kontinuity činností,
- audit organizačních opatření fyzické bezpečnosti.

1.1.2 INFORMAČNÍ OPATŘENÍ

Správa a řízení bezpečnosti informací je v odpovědnosti statutárních orgánů a vrcholového vedení organizací. Statutární orgány odpovídají za to, aby správa bezpečnosti byla součástí prováděných procesů řízení kritických zdrojů organizací. Úkolem vrcholového vedení je vzít v úvahu a reagovat na závislosti vyvolané požadavky na bezpečnost informací. Společně musí dosáhnout shody o požadavcích na program bezpečnosti informací, jeho implementaci, hodnocení stavu současné bezpečnosti informací a formulaci jejího budoucího vývoje [7].

Základním východiskem pro realizaci bezpečnostních opatření je norma ISO/EIC 27002:2005 – Soubor postupů pro řízení bezpečnosti informací. Tato norma obsahuje zkušenosti s řízením bezpečnosti informací. Doporučení normy obsahuje 133 bezpečnostních opatření, která jsou rozdělena do 11 oblastí [7].

1.1.3 TECHNICKÁ OPATŘENÍ

Technická opatření slouží k ochraně celého objektu kritické infrastruktury před protiprávními činy. Slouží především k signalizaci proniknutí neznámého pachatele do objektu, ke znemožnění nebo alespoň k prodloužení doby průniku do budovy nebo k odstrašení pachatelů [6, 8]. Do technických opatření se řadí:

- **fyzická bezpečnost:**
  - mechanické zábranné prostředky,
  - poplachový systém pro detekci vniknutí a přepadení,
  - elektrická požární signalizace (EPS),
  - ochrana používané techniky a předmětů,
  - ostraha objektu,
- **nástroje pro realizaci fyzické bezpečnosti:**
  - přístupová opatření,
    - ověřování identity uživatelů,
    - oprávnění přístupu pomocí média,
  - sledování činností fyzické bezpečnosti:
    - bezpečnostní prostředky pro pozorování,
    - uzavřený kamerový dozorový a docházkový systém,
    - nouzové zvukové systémy,
    - technické prostředky proti aktivnímu a pasivnímu odposlechu,
  - detekce NL a výbušnin.

2 HROZBY PRO KRITIKOU INFRASTUKTURU

Na základě analýzy rizik, zpracované pomocí metody bezpečnostního auditu a nalezených slabých míst dopravní kritické infrastruktury (oblast letecké dopravy) bylo zjištěno, že největší hrozbou jsou teroristické útoky za použití výbušných látek a směsí. Dalšími příklady slabých míst zjištěných analýzou platné legislativy a pomocí **analýzy – know - how:**

- status známého dodavatele dodávek,
- status stálého odesílatele nákladu a pošty,
- povinnost provádění bezpečnostní prohlídky.

Příklady slabých míst zjištěných analýzou know - how– materiální:

- nedostatečná ochrana nebo možnost prostorů objektu určených pro veřejnost (veřejné haly, ale i další prostory, ve kterých může být shromážděno větší množství lidí, kde může být odloženo improvizované výbušné zařízení, přístup je velmi snadný a přímý zásah proti pachatelům přímého je velmi obtížný,
- nadměrná velikost perimetru (hranice) a celkového prostoru objektu,
- „spící buňka“ – pachatel infiltrující se např. mezi personál,
- „osamělý střelec“ – pachatel nespolupracující s dalšími osobami [9].

Jmenované příklady slabých míst představují nepřehlédnutelnou výzvu bezpečnostním složkám státu a podpůrným bezpečnostním složkám subjektů působících v civilním letectví. Bezpečnostní audit tak představuje jeden ze základních nástrojů kontroly implementace platných norem a tím zajištění stanovené úrovně ochrany civilního letectví před protiprávními činy. Již nyní je ale zřejmé, že jedinou možnou cestou je nekompromisní postoj společnosti k pachateli útoků s teroristickým modem operandi, který svým jednáním zneužívá ke splnění „cílů“ teroristické

organizace nevinné další osoby. „Lidská práva“ tohoto pachatele by měla být vždy pečlivě zvažována s ohledem na charakter činu, který spáchal, primární a další viktimizací obětí a blízkých a pozůstalých obětí, kteří byly takovým útokem zasaženy. Také „mediální ohlas“ teroristických útoků musí být snižován na minimum tak, aby nemohl být využíván samotnými pachateli jako nástroj propagandy příslušné teroristické organizace [2].

3 ANALYZÁTORY VÝBUŠNIN

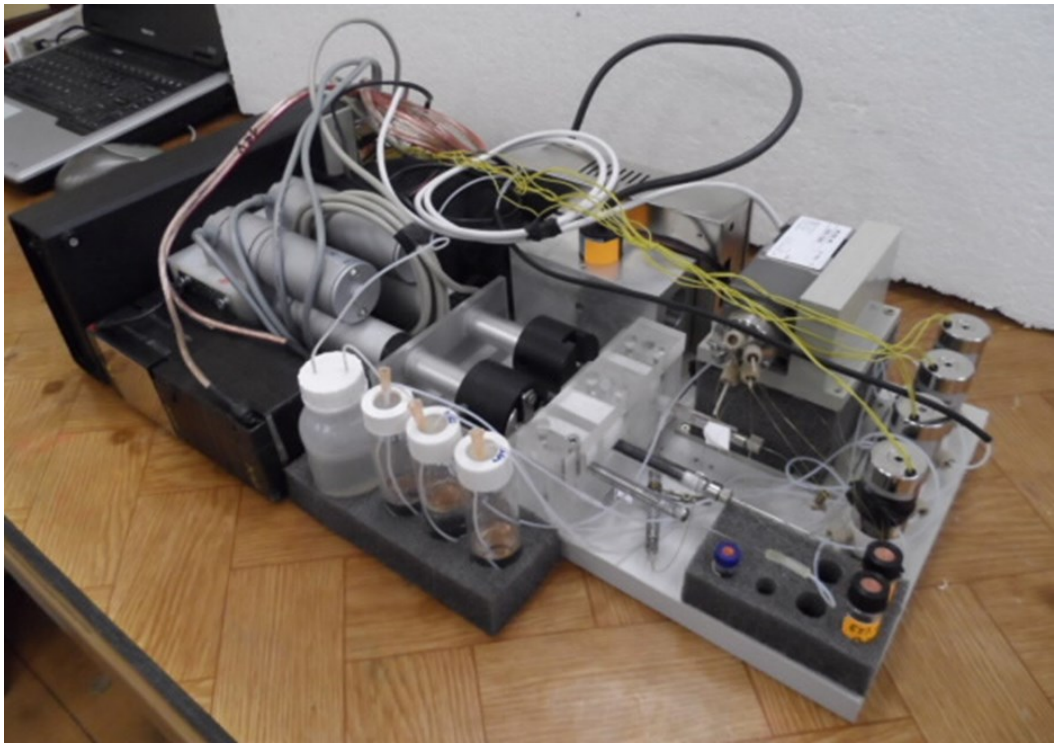
Vzhledem k největší hrozbě teroristického útoku za použití výbušných látek a směsí, je zapotřebí věnovat se problematice včasné detekce a identifikace těchto nebezpečných látek.

K detekci a identifikaci nástražných výbušných systémů, látek a směsí slouží řada přístrojů a pomůcek. Tyto přístroje a pomůcky využívají nejen pyrotechnici, ale i různé bezpečnostní kontroly na letištích a hraničních přechodech. Mezi ně patří pyrotechnické rentgeny, detektory kovů, prostředky pro detekci a vyhledávání výbušnin [10].

Detektory výbušných látek a směsí jsou schopny analyzovat vzorek látky pomocí mikroprocesoru nebo počítače. Dle druhu vzorku se detektory dělí na detektory analyzující páry, částice nebo jejich kombinace. Detektory analyzující páry vyhodnocují unikající plyn z výbušniny, jejich použití není zcela přesné, z důvodu nižší tenze par. Detektory analyzující částice jsou v přímém kontaktu s látkou, nepodléhají tolik vlivům prostředí [10, 11].

Další možností detekce výbušných látek je využití zvířat. Nejběžnější jsou služební psi, kteří jsou speciálně vycvičeni na vyhledávání a rozpoznání výbušných látek a směsí.

Pro zvýšení efektivnosti a rychlosti detekce a identifikace nebezpečných výbušných látek je vhodné vyvíjet nové efektivnější přístroje. Jedním z nově vyvinutých detektorů je Přenosný analyzátor výbušnin, vyvinutý na Univerzitě obrany ve spolupráci s Akademií věd České republiky. Přístroj pracuje na principu mikrokolonového kapalinového chromatografu s chemiluminiscenčním detektorem. Slouží k detekci výbušných nitrolátek z různých matric po předchozí extrakci, využití se předpokládá zejména v terénu [10, 11].



Obrázek 1 Fotografie analyzátoru [11]

ZÁVĚR

Vzhledem k citlivosti dat, týkajících se zabezpečení kritické infrastruktury České republiky, nelze veřejně publikovat výsledky z analýzy rizik vybraného objektu kritické infrastruktury. Obecně jmenované příklady slabých míst představují nepřehlédnutelnou výzvu bezpečnostním složkám státu a dalším podpůrným bezpečnostním složkám.

Již nyní je ale zřejmé, že jedinou možnou cestou v boji proti největší hrozbě kritické infrastruktury, je nekompromisní postoj k pachatelům teroristických útoků. Pro další zkoumání této oblasti se navrhuje hlouběji se zabývat následujícími body:

- zjištění stavu zabezpečení jednotlivých objektů kritické infrastruktury,
- vytvoření návrhu scénáře možných útoků na vybrané objekty kritické infrastruktury na základě nalezených slabých míst z analýzy rizik,
- zpracování návrhu metodiky použití bezpečnostního auditu na objekty kritické infrastruktury,
- komparace detektorů a analyzátorů používaných ve vybraných objektech kritické infrastruktury s nově vyvinutým analyzátorem výbušnin vyvinutým příslušníky Univerzity obrany ve spolupráci s Akademií věd České republiky – pro podporu rozvoje nových a efektivnějších technologií,
- návrh metodiky použití analyzátoru výbušnin vyvinutého příslušníky Univerzity obrany ve spolupráci s Akademií věd České republiky v Brně.

LITERATURA

[1] Integrated United States Security Database (IUSSD): Data on the Terrorist Attacks in the United States Homeland, 1970 to 2011: Final Report to Resilient Systems Division, DHS Science and Technology Directorate. In: *START.umd.edu* [online]. Maryland: A Department of Homeland Security Science and Technology Center of Excellence Based at the University of Maryland, 2012 [cit. 2016-04-02]. Dostupné z: https://www.start.umd.edu/sites/default/files/files/publications/START_IUSSDDataTerroristAttacksUS_1970-2011.pdf

[2] JOHANIDESOVÁ, J. Hrozby pro kritickou infrastrukturu. 2016. Osobní sdělení. Brno.

[3] MOZGA, J., VÍTEK, M., KOVÁŘÍK, F. 2008. Kritická infrastruktura společnosti. Hradec Králové: Gaudeamus, 2008. 156 s. ISBN 978-80-7041-299-2.

[4] Kritická infrastruktura – Ministerstvo vnitra České republiky. 2015. [online]. [cit. 2015-09-21]. Dostupné na: http://www.mvcr.cz/clanek/kriticka-infrastruktura.as.

[5] ŘÍHA, M. 2008. Bezpečnostní systémy. Praha: Námořní akademie České republiky, 2008. ISBN 978-80-87103-03-6.

[6] Bezpečnost na letišti Václava Havla Praha. 2015. [online]. [cit. 2016-03-02]. Dostupné na: http://www.prg.aero/cs/o-letisti-praha/bezpecnost-na-letisti/.

[7] DOUCEK, P., NOVÁK, L., SVATÁ, V. 2008. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 9788086946887.

[8] ZUZANIKOVÁ, P. 2011. Bezpečnostní problematika ochrany letišť. Zlín, 2011. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[9] JOHANIDESOVÁ, J. 2016. Hrozby pro kritickou infrastrukturu. Osobní sdělení. Brno.

[10] VAŠKOVÁ, M. Možnosti aplikace přenosného analyzátoru výbušnin při identifikaci výbušnin. In: Monitorování cizorodých látek v životním prostředí XVII.. Pardubice: Univerzita Pardubice, 2015, s. 141-147. ISBN 978-80-7395-926-5.

[11] BUMBOVÁ, A., KELLNER, J., VEČEŘA, Z., KAHLE, V., NAVRÁTIL, J. Functional Sample of the Portable Device for Fast Analysis of Explosives. Proceedings of World Academy of Science, Engineering and Technology, 2012, vol. 70, no. X, p. 445-448. ISSN 2010-376X.