PROJEKT ROZVOJA SIMCENTRA AOS V MODULE: OCHRANA VOJSK A PRVKOV KRITICKEJ INFRAŠTRUKTÚRY

Miroslav Kelemen,[1] Pavel Nečas,[2] Ján Buzalka,[3] Vladimír Blažek,[4] Martin Hromada[5]

ABSTRAKT

Pripravovaná štúdia realizovateľnosti je zameraná na budovanie špecializovaného pracoviska, simulačného centra, pre využitie potenciálu simulačného nástroja OTB OneSAF Akadémie ozbrojených síl vo vzťahu k skúmaniu bezpečnostného systému a odolnosti vybraných prvkov obrannej infraštruktúry, ako súčasti národnej kritickej infraštruktúry, pri vojenských a nevojenských ohrozeniach.

Kľúčové slová:
Simulácia, ochrana, ozbrojené sily, kritická infraštruktúra.

ABSTRACT

Prepared feasibility study is focused on the development of specialized department at Armed Forces Academy, Simulation center, and on the potential use of the simulation tool OTB OneSAF in relation to the security system and resilience of the selected defense infrastructure components as components of national critical infrastructure at the military and non – military threats.

Key words:
Simulation, protection, armed forces, critical infrastructure.

1 ÚVOD

Asymetrickosť bezpečnostného prostredia ako aj zvyšujúca sa zložitosť a vzájomná previazanosť systémov či závislosť spoločnosti na týchto systémoch,

[1] Miroslav Kelemen, brig. gen. doc. Ing. PhD., AOS GMRŠ v Liptovskom Mikuláši, 0960/422222, miroslav.kelemen@aos.sk
[2] Pavel Nečas, doc. Ing. PhD., AOS GMRŠ v Liptovskom Mikuláši, 0960/422222, pavel.necas@aos.sk
[3] Ján Buzalka, prof. PhDr. CSc., Akadémia PZ v Bratislave, 0961/057223, jan.buzalka@minv.sk
[4] Vladimír Blažek, Mgr. Dr. CSc., Akadémia PZ v Bratislave, 0961/057423, vladimir.blazek@minv.sk
[5] Martin Hromada, Ing. interný doktorand UTB Zlín, 00420/576035243, hromada@utb.cz

vytvorila potrebu definovania kritickej infraštruktúry ako takej oblasti infraštruktúry, ktorej narušenie či zničenie vyvolá vážne politické a hospodárske následky [1]. Tento fakt vytvoril rámec pre dialóg, ktorý prehodnocuje prístupy k ochrane takýchto infraštruktúr a vytvára normatívne, legislatívne a inštitucionálne nástroje pre efektívnejšiu ochranu kritickej infraštruktúry.

2 SÚČASNÝ STAV RIEŠENIA PROBLEMATIKY SIMULÁCIE V AOS V OBLASTI OCHRANY KRITICKEJ INFRAŠTRUKTÚRY

Akadémia ozbrojených síl rozvíja špecializované pracovisko, budované na základe simulačného nástroja OTB OneSAF, ktoré umožňuje realizovať počítačom podporované vzdelávacie a výcvikové aktivity v rámci profesionálnej prípravy časti bezpečnostnej komunity. Inštitucionálny projekt akadémie upriamuje pozornosť na spracovanie štúdie realizovateľnosti, s dôrazom na ďalšie budovanie simulačného centra v dvoch moduloch: v module Ochrana vojsk a prvkov kritickej infraštruktúry, v module: Ochrana obyvateľstva a budovaním pracoviska virtuálnych simulátorov. V súčasnosti je Simulačné centrum zamerané len na počítačom podporované cvičenia pre prípravu kľúčového personálu velenia a riadenia jednotiek v operáciách medzinárodného krízového manažmentu, v krízových situáciách vojenského charakteru. V rámci riešenia modulu: Ochrana vojsk a prvkov kritickej infraštruktúry rešpektujeme skutočnosť, že bezpečnostné opatrenia pre ochranu prvku v súvislosti s fyzickou a objektovou ochranou je možné rozdeliť na:

- Mechanické zábranné systémy – sú definované ako systémy alebo zariadenia, ktoré slúžia na zabránenie prístupu nepovolaným osobám. Medzi tieto systémy je možné zaradiť:
  - prostriedky obvodovej ochrany (pevné bariéry, ploty, vrcholové zábrany, brány, závory, turnikety, bezpečnostné priepuste a iné),
  - prostriedky plášťovej ochrany (mreže, rolety, fólie, žalúzie, bezpečnostné sklá, okná, dvere, zárubne, steny, zámky, zámkové vložky, visacie zámky a iné),
  - prostriedky predmetovej ochrany (komorové trezory, komerčné úschovné objekty a iné).
- Technické zabezpečovacie prostriedky – sú vnímané ako zariadenia alebo systémy informujúce o stave a narušení objektu či objektov alebo chránených priestorov. Za technické zabezpečovacie prostriedky je možné považovať:
  - systémy na kontrolu vstupu,
  - poplachové systémy na hlásenie narušenia,
  - kamerové systémy v rámci uzatvoreného televízneho okruhu,
  - elektrická požiarna signalizácia,
  - zariadenia na detekciu látok a predmetov,
  - zariadenia proti aktívnemu a pasívnemu odpočúvaniu,
  - zariadenia fyzického ničenia nosičov informácií,
  - tiesňové systémy.
- Fyzickú ochranu – jedná sa o ochranu objektu a chráneného priestoru, ktorá môže byť vykonávaná príslušníkmi ozbrojených bezpečnostných zborov,

ozbrojených síl Slovenskej republiky, trvalo prítomnými ozbrojenými vlastnými zamestnancami, či miestnou nepretržitou ochranou.

- Režimové opatrenia – sú opatrenia, ktoré určujú podmienky vstupu, pohybu osôb, automobilov, či postupy v prípade mimoriadnej udalosti ako aj podmienky manipulácie s mechanickými zábrannými systémami, či technickými zabezpečovacími prostriedkami a iné [2].

V súvislosti s komplexným využitím bezpečnostného systému sa uvažuje o troch hlavných funkciách systému:

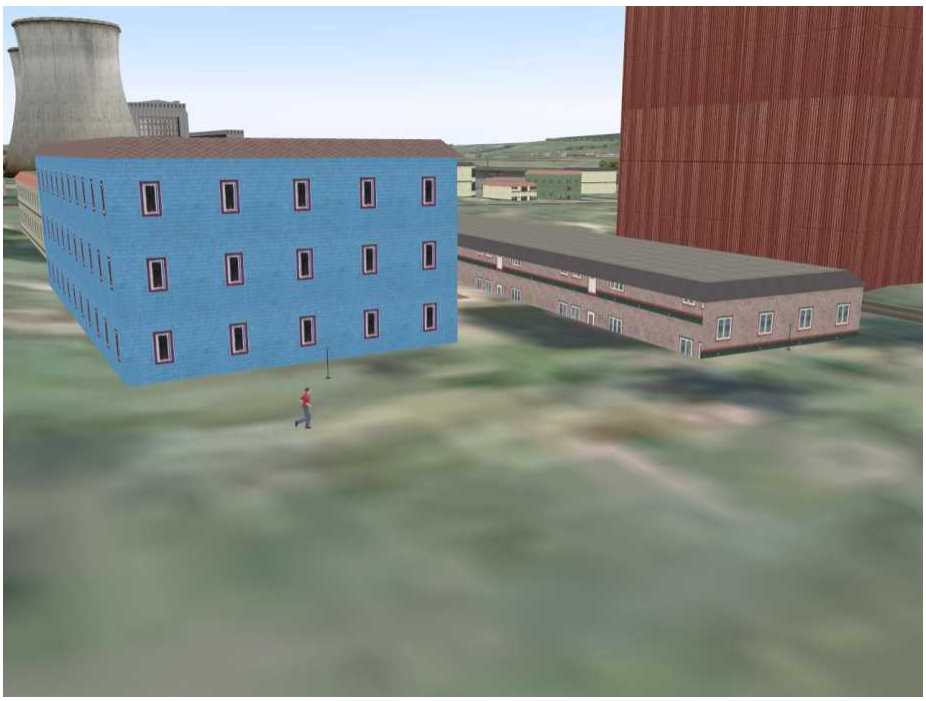
- Detection – detekcia narušiteľa, s využitím technických zabezpečovacích prostriedkov (AIR, PIR, MW Bistatic, MW Monostatic, dual senzor, atď.), overenie poplachovej informácie (CCTV).
- Delay – spomalenie narušiteľa s využitím mechanických zábranných systémov (ploty, brány, prelezové bariéry, mreže, bezpečnostné dvere, sklá a iné).
- Response – odozva – reakcia fyzickej ochrany objektu – zamedzenie, prerušenie alebo zadržanie narušiteľa – k čomu majú prispieť aj režimové opatrenia [3].

Medzi použiteľné nástroje hodnotenia bezpečnostného systému objektu je vhodné zaradiť napríklad tzv. EASI model (Estimate of Adversary Sequence Interruption/ pravdepodobnosť prerušenia činnosti narušiteľa), ktorý pracuje s pravdepodobnosťami detekcie, svojim spôsobom s prielomovou odolnosťou, so smerodajnou odchýlkou, ktorá je vytváraná na základe praktických skúšok činnosti fyzickej ochrany, alebo s pravdepodobnosťou správnej komunikačnej činnosti. Kde ako výstup matematických vzťahov medzi pravdepodobnosťami a prielomovými odolnosťami je pravdepodobnosť zadržania páchateľa, resp. narušiteľa. Tento model bol prezentovaný napríklad aj v rámci práce M. L. Garciu [3] a môže byť vnímaný ako spôsob hodnotenia bezpečnostného systému aj v súvislosti s odolnosťou kritickej infraštruktúry. Napriek presvedčeniu, že EASI model by mohol byť použitý pri hodnotení bezpečnostného systému objektov obrannej infraštruktúry - prvkov národnej kritickej infraštruktúry, a tým pri formulovaní určitých východísk pre stanovenie celkovej odolnosti kritickej infraštruktúry, je však potrebné využiť ďalšie metódy, ktoré sú použiteľné v súvislosti s overením funkcií bezpečnostného systému, či činnosti fyzickej ochrany pri narušení chráneného priestoru. Medzi použiteľné metódy a simulačné nástroje je možné zaradiť simulačný nástroj OTB OneSAF dostupný v Akadémii ozbrojených síl, ktorý ale vyžaduje špecifickú softvérovú modifikáciu pre uvedený modul.

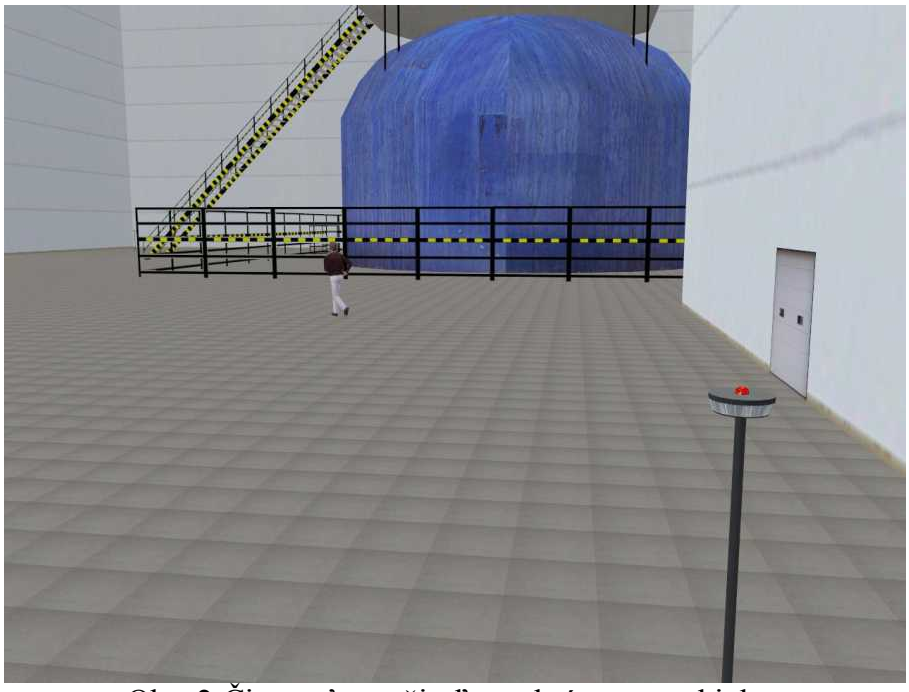
3 PRVOTNÉ VÝSLEDKY SW ÚPRAVY SIMULAĆNÉHO NÁSTROJA PRE OVEROVANIE OCHRANY A OBRANY OBJEKTU KRITICKEJ INFRAŠTRUKTÚRY

Pred konkrétnou simuláciou časových závislostí pohybu narušiteľa a fyzickej ochrany je nutné definovať a aplikovať parametre bezpečnostných zón, ktoré v prípade, kedy je stanovená prielomová odolnosť, budú vnímané ako určité „kontrolné body – checkpoints“. Časové hľadisko prekonania týchto bodov bude totožné so stanovenou prielomovou odolnosťou. V zónach, kde nie je stanovená prielomová odolnosť, sa bude posudzovať nekonštantnosť pohybu narušiteľa, a tým

pádom rozdielnosť časových parametrov. Tento prístup sa uplatní aj kontexte s činnosťou a reakčným časom fyzickej ochrany. Definované parametre bezpečnostných zón boli implementované do vytvoreného fiktívneho objektu, ktorý je svojim charakterom vnímaný ako prvok kritickej infraštruktúry. Pre potreby projektu bol vytvorený model objektu jadrovej elektrárne (ukážka Obrázok 1 a 2), v ktorom boli zohľadnené a implementované prístupy čiastočne prezentované v predchádzajúcom texte.



Obr. 11 Penetračné testy navrhnutého systému fyzickej ochrany objektu



Obr. 2 Činnosť narušiteľa v chránenom objekte

Pre kompletizáciu modelu EASI pre jednotlivé bezpečnostné zóny a triedy bolo potrebné vykonať simulácie v troch rozdielnych oblastiach a úrovniach: simuláciu v oblasti činnosti fyzickej ochrany, narušiteľa, tvorby scenárov činnosti fyzickej ochrany pri narušení objektu a podobne.

Zámerom autorov je ďalšie podrobnejšie skúmanie technickej a fyzickej ochrany jadrovej elektrárne typu Jaslovské Bohunice, vojenskej základne koaličných síl v zahraničí, vojenského letiska – ako špecifického vojenského objektu, dopravného a logistického centra, a podobne. [4]

4 ZÁVER

Vzhľadom na skutočnosť, že špecifický modul simulačného nástroja OTB OneSAF, ktorý by umožňoval overovanie bezpečnostného systému a odolnosti vybraného objektu kritickej infraštruktúry, na základe simulácie činnosti jednotlivých entít zatiaľ neexistuje, príspevok prezentuje prvotný teoretický vstup pre jeho vytvorenie. Praktickým výsledkom takéhoto modulu bude spôsobilosť pre simuláciu činností narušiteľa a činností fyzickej ochrany objektu, čím sa vytvorí rámec pre optimalizáciu plánovania činností fyzickej ochrany v kontexte reálnych podmienok v reálne existujúcich objektoch.

Nový, špecifický modul a následne celý simulačný nástroj OTB OneSAF je využiteľný pre plánovanie činností ozbrojených zložiek pri ochrane a obrane dôležitých objektov kritickej infraštruktúry, ale aj v súvislosti s verifikáciou činností fyzickej ochrany v rámci ochrany kritickej infraštruktúry a prípravy personálu pre tieto činnosti. Optimalizácia bezpečnostného systému by následne bola východiskom pre hodnotenie celkovej odolnosti daného prvku a následne sektoru kritickej infraštruktúry. Vytvorenie takéhoto modulu poukazuje na nevyhnutnosť určitej spolupráce civilného a vojensko-policajného sektoru a prekonania určitej bipolarity riešenia bezpečnostných otázok [pozri 5,6]. Zložitosť vytvorenia takéhoto modulu si vyžaduje ďalší výskum a vývoj, ktorý však bude mať oporu v spolupráci s Akadémiou ozbrojených síl generála Milana Rastislava Štefánika v Liptovskom Mikuláši, s Univerzitou Tomáša Baťu v Zlíne a Akadémiou Policajného zboru v Bratislave. Prvým praktickým krokom k realizácii zámerov je riešenie spoločného projektu vedy a výskumu v roku 2011, so zameraním na budovanie spôsobilostí Simulačného centra Akadémie ozbrojených síl a modifikáciu dostupného simulačného nástroja pre riešenie komplexných otázok ochrany vojsk a prvkov kritickej infraštruktúry štátu, ako aj ochrany obyvateľstva.

LITERATÚRA

[1] Smernica rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu. Dostupné on-line http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SK:PDF

[2] HOFREITER L. – LOVEČEK T. – VEĽAS A.: Zásady a princípy analýzy rizík v oblasti fyzickej a objektovej bezpečnosti, Žilinská univerzita v Žiline, Fakulta

špeciálneho inžinierstva, Žilina, 2006, dostupné on-line: http://www.nbusr.sk/i publisher/files/nbusr.sk/oblasti-bezpecnosti/objektova-afyzicka/docs_of/analyza/zasady_metodika
[3] GARCIA M.L.: The Design and Evaluation of Physical Protection Systems, Second edition, Sandia National Laboratories, 2007, ISBN – 10: 0-7506-8352
[4] KELEMEN, M. – JEZNÝ, M. – PULIŠ, P.: Letisko – komplex ochrany osôb, majetku a bezpečnostných technológií. 1. vyd. – Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2010. - 179 s. - ISBN 978-80-8040-413-0.
[5] LUKÁŠ, L. – HROMADA, M.: Možnosti hodnocení odolnosti kritické infrastruktury/ Evaluating the Resistance of Critical Infrastructure, Bezpečnost v informační společnosti, Brno, 2009.
[6] HROMADA, M.: Stanovení odolnosti kritickej infraštruktúry – teoretický rámec/Critical Infrastructure Resilience Determination – Theoretical Framework, Security Magazín, 2010. ISBN 1210-8723.

Príspevok bol spracovaný v rámci riešenia inštitucionálneho projektu v roku 2011„Štúdia realizovateľnosti budovania a rozvoja Simulačného centra AOS - pracoviska operácií národného a medzinárodného krízového manažmentu“ AOS-4-4-3/2010-PVe 4.2.2.1, zo dňa 22. októbra 2010.

Článok recenzoval:
prof. Ing. Josef Reitšpís, PhD.