OCHRANA PRVKOV KRITICKEJ INFRAŠTRUKTÚRY A MOŽNOSTI JEJ OPTIMALIZÁCIE

Vladimír ANDRASSY [1], Ján JASENOVEC[2]

ABSTRAKT
Článok sa zaoberá ochranou kritickej infraštruktúry, ako komplexného súboru úloh súvisiacich s vytvorením podmienok funkčnosti, integrity a kontinuity kritickej infraštruktúry. V ďalšom sú analyzované možnosti využitia efektívnych a dostupných technológií vytvárajúcich predpoklady pre dosiahnutie optimálnej úrovne jej ochrany.

Kľúčové slová: Kritická infraštruktúra, ochrana kritickej infraštruktúry, prvok kritickej infraštruktúry, možnosti optimalizácie.

ABSTRACT
Article resolve critical infrastructure protection, as complex of measure in context with conditions of functions, integrity and continuity critical infrastructure. In next are analyzing possibility for using effective technologies, which are assumptions for achieve of optimal level her protection.

Key words: Critical infrastructure, critical infrastructure protection, element of critical infrastructure, optimization.

ÚVOD

Funkčnosť kritickej infraštruktúry podmieňujú viaceré faktory pôsobiace v rámci jej vnútorných väzieb (interné technologické systémy, procesy a pod.), ktoré sú pevne uzavreté v rámci jednotlivých prvkov a sektorov. Ďalšími faktormi sú vonkajšie väzby (vzájomne poskytované externé zdroje, podporné prvky a pod.) Pre zabezpečenie uvedenej funkčnosti jednotlivých systémov, je potrebné vytváranie optimálnych podmienok a vyváženosti pôsobiacich faktorov. Medzi tieto podmienky

[1] Vladimír Andrassy, Ing., AOS, Demänová 393, 031 01 Liptovský Mikuláš. E-mail: vladimir.andrassy@aos.sk
[2] Ján Jasenovec, Ing., doktorand Katedry bezpečnostného manažmentu ŽU. E-mail: jajasen@post.sk

patrí zabezpečenie ochrany z pohľadu výrobno-technologického, ako aj z pohľadu ochrany objektov ako takých. Krehkosť tohto vzťahu, môže pozitívne ovplyvniť výber optimálnej ochrany reagujúcej na potenciálne riziká. Dnešná doba prináša rôzne antagonistické situácie v celom spektre spoločenského diania, následky vyčíňania prírodných živlov alebo činnosti rôznych teroristických skupín, nás vedú k potrebe dôkladnej analýzy a pochopenia príčinných súvislostí týchto javov. Je preto opodstatnené zaoberať sa touto problematikou, nakoľko len dôsledný bezpečnostný výskum môže napomôcť k tomu, že opatrenia súvisiace s ochranou kritickej infraštruktúry budú optimálne.

1 VYMEDZENIE ZÁKLADNÝCH POJMOV

„Optimalizácia“ definuje systém vyhľadávania najlepšieho možného variantu určitého riadeného deja, rozhodnutia alebo postupu, poprípade zlepšenie určitých špecifických dejov a postupov.

„Bezpečnostný systém“ charakterizujeme ako modulárny systém integrujúci reálne existujúce prvky vytvárajúce nástroj na zaistenie bezpečnosti v danom priestore a čase. Je tvorený účelným usporiadaním a používaním technických prostriedkov, organizačných a režimových opatrení a fyzickej ochrany, ktoré sú vzájomne späté a na seba vzájomne pôsobiace. Ich hlavnou úlohou je zabezpečenie ochrany chráneného objektu, odvrátenie útokov zameraných na chránený priestor alebo chránený záujem a minimalizácia strát vznikajúcich pôsobením rizikových faktorov.

„Kritická infraštruktúra“ predstavuje systém, ktorý je nevyhnutný na uskutočňovanie hospodárskej funkcie štátu, a ktorého narušenie alebo zničenie by malo závažné nepriaznivé dôsledky na jej uskutočňovanie, a tým aj na kvalitu života obyvateľov, najmä z hľadiska ochrany života, zdravia, bezpečnosti, majetku a životného prostredia.

„Prvkom kritickej infraštruktúry“ je najmä inžinierska stavba, verejnoprospešná služba alebo informačný systém v sektore, ktorého narušenie alebo zničenie by malo závažné nepriaznivé dôsledky.

„Ochranou kritickej infraštruktúry“ rozumieme zabezpečenie funkčnosti, integrity a kontinuity kritickej infraštruktúry, sektora a prvku s cieľom odvrátiť alebo zmierniť hrozbu ich narušenia alebo zničenia.

2 OCHRANA KRITICKEJ INFRAŠTRUKTÚRY

Základným predpokladom ochrana kritickej infraštruktúry je prijatie adekvátnych opatrení k vyhodnoteným potenciálnym rizikám. Hlavnou úlohou ochrany bude eliminácia prípadne zníženie týchto rizík a ohrození. Dôraz by mal byť upriamený na možné scenáre ohrození akými sú:

- priama akcia – priamy ozbrojený fyzický útok na cieľ uskutočnený ozbrojenými teroristickými skupinami,
- bombový útok – útok, ktorý je spravidla vykonávaný jednotlivcom alebo malou skupinou s využitím napr. nekonvenčných náloží (nejde o letecké bombardovanie),

- CBRN útok – útok s použitím chemických, biologických, bakteriologických alebo rádioaktívnych látok,
- kybernetický útok – útok, ktorý je zameraný na zničenie informácií a dát alebo narušenie počítačových systémov a programov spravidla prostredníctvom internetovej siete,
- informačné operácie – útoky, ktoré majú za cieľ získať alebo zneužiť informácie, ovplyvniť procesy založené na informáciách (napr. ovplyvniť počítačový systém tak, že navonok sa javí ako plne funkčný, ale vnútri pracuje so zmanipulovanými údajmi), a zároveň svoje vlastné informácie a počítačové systémy chrániť,
- technologické riziká – závažná technologická porucha majúca zásadný vplyv na funkčnosť prvku kritickej infraštruktúry,
- riziká ľudského faktora – zlyhanie obslužného personálu zabezpečujúceho chod systémov prvkov kritickej infraštruktúry,

Nástroje ochrany a obrany prvkov kritickej infraštruktúry

Ochrana a obrana prvkov kritickej infraštruktúry pozostáva z nasledovných segmentov:
- prevencia pred ohrozením,
- zníženie rizika ohrozenia existencie a stability prvku,
- odvrátenie útoku na prvok alebo na systém jeho ochrany a obrany,
- odstránenie následkov útoku na prvok alebo na systém jeho ochrany a obrany, reakcia/odpoveď na narušenie alebo zničenie prvku.

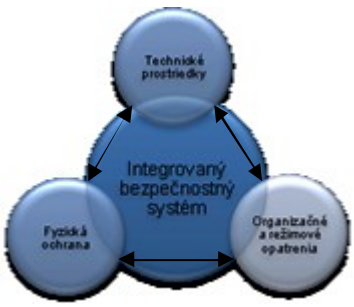
3 VÝBER OPTIMÁLNEJ OCHRANY PRVKU KRITICKEJ INFRAŠTRUKTÚRY

Ochrana prvku kritickej infraštruktúry, predpokladá vykonanie optimálnych preventívnych opatrení, ako reakcia na možné ohrozenia. V obecnej rovine obsahu ochranných opatrení sa odporúča vykonať:
- oddelenie vnútornej časti prvku kritickej infraštruktúry od vonkajšieho prostredia (napr. mechanické zábrany, oddelenie počítačov a lokálnych sietí s citlivými údajmi od internetovej siete, použitie špeciálneho prepojenia vo vymedzenom okruhu používateľov),
- systém vyrozumenia orgánov verejnej správy a systém varovania obyvateľstva napojený na budovaný európsky varovný informačný systém,
- režimové opatrenia pre vstup do vnútornej časti prvku kritickej infraštruktúry, napr.:
  - oprávnenie na vstup do objektu, splnenie určených podmienok na vstup do objektu, zabezpečenie pred neoprávneným vstupom,
  - prístupové práva k počítačom a lokálnym sieťam, certifikované zabezpečenie pred neoprávneným prístupom,
- režimové opatrenia pre prevádzku prvku kritickej infraštruktúry,
- kontroly, inšpekcie, simulácie, cvičenia, odborná príprava,

- kontrolné bezpečnostné prostriedky vnútri objektov alebo systémov (napr. integrovaný bezpečnostný systém, kamerové systémy),
- bezpečnostná dokumentácia (dokumentácia ochrany a obrany prvku kritickej infraštruktúry),
- právne normy upravujúce povinnosti, právomoci a zodpovednosť verejnej správy a súkromného sektora.

Realizáciou vyššie uvedených a popísaných nástrojov a opatrení, vystupuje do popredia potreba ochrany a obrany prvkov kritickej infraštruktúry, zahrnutá v komplexnom vyjadrení ako „integrovaný bezpečnostný systém“. Pri jeho tvorbe je potrebné vychádzať z vykonanej analýzy bezpečnostných rizík (odhad potencionálnych strát, ktoré môžu vyniknúť ako dôsledok zraniteľnosti systému a kvantifikáciu strát, ktoré môžu vyniknúť ako dôsledok existujúcich ohrození a analýzy bezpečnostného prostredia (proces skúmania zvláštností prostredia, ktoré môže byť zdrojom pre vznik bezpečnostných rizík a ohrození vo vzťahu k prvku kritickej infraštruktúry).

Vykonaná identifikácia a klasifikácia bezpečnostných rizík na základe možných scenárov ohrození bude rozhodujúcim článkom pri návrhu a realizácii bezpečnostného systému. Dôraz na už navrhnutý (prípadne nový) bezpečnostný systém skladajúci sa jednotlivých prvkov a vzájomných väzieb medzi nimi, by mal odrážať vzťah uvedený na (Obrázok 1).



Obrázok 1 Základné prvky integrovaného bezpečnostného systému

(zdroj: podľa REITŠPÍS, J., 2004, doplnené)

Jednotlivé prvky tvoriace integrovaný bezpečnostný systém sú usporiadané do samostatných celkov vytvárajúcich bezpečnostné vrstvy systému a rozdeľujeme ich na:

- vrstvu perimetrickej ochrany, zaisťujúcu „právnu hranicu“ chráneného objektu,
- vrstvu plášťovej ochrany, zabraňujúcu narušeniu vstupov do objektu,
- vrstvu priestorovej ochrany, zabezpečujúcu ochranu priestorov, vstupov a pod.,
- vrstvu predmetovej ochrany, zabezpečujúcu bezprostrednú ochranu chráneného predmetu.

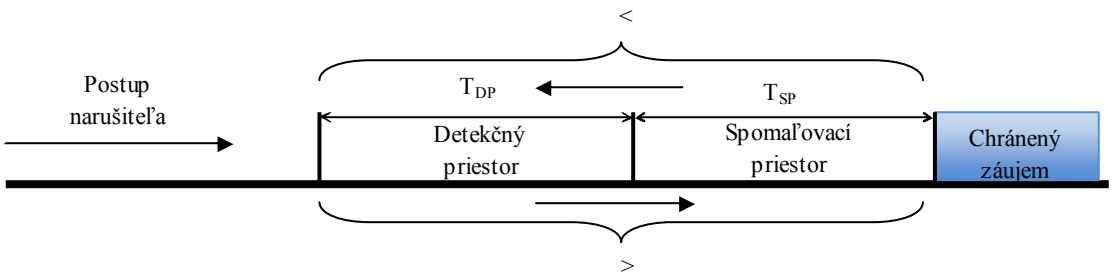
Možnosti optimalizácie ochrany

Tak, ako už bolo vyššie uvedené, aj existujúci integrovaný bezpečnostný systém je vo svojej podstate súhrn personálnych a technických prostriedkov vytvárajúcich fungujúci celok zabezpečujúci ochranu a bezpečnosť chráneného záujmu. Ak sa chceme zaoberať jeho optimalizáciou, musíme identifikovať možné kritické miesta z hľadiska časových, bezpečnostných a integrujúcich vlastností systému.

Pri optimalizácii z časového hľadiska (obrázok 2) musíme prihliadať na podstatu chráneného záujmu, ktorá zásadným spôsobom ovplyvňuje vzájomný vzťah časových intervalov doby reakcie fyzickej ochrany (T_{FO}) alebo zásahovej jednotky (polícia, bezpečnostná služba) a doby potrebnej na prekonanie systému ochrany objektu (T_{PO}).

T_{FO} - je čas potrebný na zásah zásahovej jednotky a je súčtom jednotlivých časov:

T_{zist} – čas zistenia napadnutia chráneného objektu,
T_{ver} – čas verifikácie poplachu,
T_{vyh} – čas vyhlásenia poplachu a vydania príkazu na zásah,
T_{prip} – čas prípravy zásahovej jednotky (ak je potrebný),
T_{pres} – čas presunu zásahovej jednotky na miesto zásahu.



Obrázok 2 Zobrazenie jednotlivých časov pri zabezpečovaní ochrany

(zdroj: podľa HOFREITER, L., 2007, doplnené)

Pri optimalizácii z bezpečnostného hľadiska je potrebné položiť dôraz na použité technické prostriedky, ich vzájomnú kompatibilitu a integráciu do bezpečnostného systému tak, aby boli vzájomne kooperujúce a funkčne zabezpečené v prípade ich možného zlyhania (porucha prostriedku, úmyselné zničenie a podobne).

Pri optimalizácii z hľadiska integrujúcich vlastností systému je potrebné zamerať pozornosť na spracované a aktualizované organizačné a administratívno-režimové opatrenia (štandardné operačné postupy) a zabezpečenie fyzickej ochrany, ako prvku na bezprostredné strážení objektu kritickej infraštruktúry strážnou službou a nasadenie zásahovej jednotky. Neoddeliteľnou súčasťou bezpečnostnej služby je odborná príprava zameraná na prípravu k výkonu strážnej služby a poskytovanie odborných rád pri jej prevádzkovaní.

ZÁVER

Kritická infraštruktúra, je špecifická z pohľadu jej dôležitosti na chod spoločnosti. Vzhľadom k tomu, že každý prvok má v celkovom systéme rôznu úroveň významu, bude potrebné pri výbere optimalizácie ochrany brať do úvahy tento fakt. Samotná ochrana musí v prvom rade spĺňať základné predpoklady určitých štandardov zabezpečenia objektu, ktoré sú osvedčené u nás alebo v zahraničí.

Bezpečnostný systém na ochranu prvkov kritickej infraštruktúry je možné realizovať počínajúc jednoduchým funkčným systémom zabezpečujúcim ochranu až po komplikované, komplexné, sofistikované riešenia bezpečnostných systémov, ktoré sú riadené, prispôsobované a diagnostikované na diaľku prostredníctvom vytvorenej bezpečnostnej siete.

Optimalizácia ochrany prvkov kritickej infraštruktúry je však určitou nadstavbou tohto aplikovaného bezpečnostného systému, ako optimálneho riešenia odpovedajúceho na možné riziká. Je však potrebné uviesť, že optimalizácia je hlavne nepretržitým procesom, ktorý vyžaduje neustálu revíziu bezpečnostného systému. Riziká ktoré v súčasnosti poznáme sa postupom vývoja spoločnosti kvalitatívne vyvíjajú a preto aj proces optimalizácie musí cyklicky prechádzať modernizáciou ako odpoveď na neustále sa meniace hrozby, ktoré súčasný pokrok ľudstva prináša.

LITERATÚRA

[1] Ministerstvo vnútra SR, Bratislava 2009, 1,2,s In.: Návrhu Zákona o ochrane kritickej infraštruktúry, Draft z 16.12.2009

[2] Ministerstvo hospodárstva SR, www.economy.gov.sk, Bratislava 2007, 5,6,s In.: Uznesenie Vlády SR č. 120 z 14. 2. 2007, k návrhu Koncepcie kritickej infraštruktúry v Slovenskej republike a spôsobu jej ochrany a obrany

[3] Mária Ivanová-Šalingová, 614 s, In: Vreckový slovník cudzích slov, ISBN 80-901160-2-7

[4] NEČAS P., OLEJNÍK F., In: Challenges of the 21st century global security: reflected, Košice: Air Force Academy of gen. M. R. Stefanik in Kosice, 2004, ISBN 80-7166-051-5

[5] NEČAS P., KELEMEN M., In: Call for more security: Technology revolution wanted! Brno: International conference on Military Technologies, 2009, ISBN 978-80-7231-648-9

[6] REITŠPÍS J. a kol., Manažérstvo bezpečnostných rizík. Žilina: Žilinská univerzita v Žiline, 2004. ISBN 80-8070-328-0

[7] HOFREITER L., KRIŽOVSKÝ S., Manažérstvo bezpečnostných systémov. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2007, ISBN 978-80-89282-16-6

Článok recenzoval:
prof. Ing. Miloslav Seidl, PhD.