KRITICKÁ INFRAŠTRUKTÚRA A MOŽNOSTI JEJ OCHRANY

Petr SELINGER[1]

SUMMARY

Protection of persons and property does not lose anything of its importance in 21st century. On the contrary, its significance increases and society strives to strengthen protection. On one side, the legislation gets stricter, on the other side technical means of persons and property protection are constantly getting improved. This article deals with issue of need for definition of critical infrastructure as part of infrastructure, destruction of which would cause serious political and economical impacts. Destruction or disablement of critical infrastructure would mean great casualties, losses on property and moral damages.

KEY WORDS: *critical infrastructure, critical infrastructure object protection, technical protection, physical protection.*

1. LEGISLATÍVNE VYMEDZENIE POJMU KRITICKÁ INFRAŠTRUKTÚRA

Vychádzajúc zo súčasných bezpečnostných rizík vznikla vo vyspelých štátoch sveta potreba definovania kritickej infraštruktúry ktorej zničenie spôsobí vážne politické a hospodárske dôsledky. Objektívna potreba zabezpečiť ochranu a obranu dôležitých objektov národnej infraštruktúry pred tradičnými hrozbami, akými boli a sú prírodné katastrofy, nedbalosť, technologické havárie, neoprávnené vniknutie do počítačových systémov a ďalšie zjavné a latentné kriminálne aktivity, sa rozšírila aj o hrozbu teroristických útokov. Viaceré európske krajiny sú teroristami považované za potenciálne ciele. Terorizmus sa sústreďuje na útoky proti civilnému obyvateľstvu, ako aj na kritickú infraštruktúru štátu s cieľom spôsobiť masové obete, škody, vyvolať strach a pocit ohrozenia.

Reakciou na hore uvedené zo strany Európskej únie bolo vypracovanie viacerých dokumentov, v ktorých je riešená prevencia, pripravenosť a reakcie na hrozby ohrozujúce kritickú infraštruktúru so zameraním najmä na hrozbu terorizmu. Spoločným cieľom Európskej rady a Európskej komisie bolo vypracovanie Európskeho programu na ochranu kritickej infraštruktúry (European Programme for Critical Infrastructure Protection, skr. EPCIP, ďalej len EPCIP) a Výstražnej informačnej siete kritickej infraštruktúry (Critical Infrastructure Warning Information Network, skr. CIWIN, ďalej len CIWIN).

V zelenej knihe sú uvedené možnosti, ktoré môže Komisia využiť na zriadenie EPCIP a CIWIN. Ako sa uvádza v Zelenej knihe, cieľom EPCIP je zaistiť, aby v celej EÚ existovala primeraná úroveň bezpečnostnej ochrany kritickej infraštruktúry, ktorá by minimalizovala možnosti zlyhania ale aj rýchle nápravné opatrenia. Úroveň ochrany nie je pre všetky prvky rovnaká, je odvodená od možného dopadu, ktorý by mohlo spôsobiť zlyhanie. Ako základné princípy EPCIP sú v dokumente uvedené: subsidiarita, doplnkovosť, dôvernosť, spolupráca zainteresovaných subjektov a proporcionalita. Dokument taktiež zdôrazňuje potrebu vypracovania národných programov na ochranu kritickej infraštruktúry, ktoré by vychádzali z EPCIP.

Kritická infraštruktúra v Slovenskej republike

Termín „kritická infraštruktúra“ bol prvý krát zavedený a definovaný pre podmienky v Slovenskej republike v dokumente Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany. Vláda Slovenskej republiky svojím uznesením č. 967 zo 7. decembra 2005 schválila „Plán práce Bezpečnostnej rady Slovenskej republiky na rok 2006“, ktorý uložil podpredsedovi vlády Slovenskej republiky a ministrovi hospodárstva Slovenskej republiky v súčinnosti s vybranými ústrednými orgánmi

štátnej správy a inými štátnymi orgánmi predložiť v 4. štvrťroku 2006 na rokovanie Bezpečnostnej rady Slovenskej republiky a následne na rokovanie vlády Slovenskej republiky „Koncepciu kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany“.

Podľa Zákona o kritickej infraštruktúre sa kritickou infraštruktúrou rozumie „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“.

Národná rada Slovenskej republiky schválila Bezpečnostnú stratégiu, ktorá je východiskom tejto koncepcie, a ktorá deklaruje že Slovenská republika sa zameria na zníženie zraniteľnosti informačných a komunikačných systémov, prevažne na systémov nevyhnutných na bezpečné fungovanie základných funkcií štátu a zaručí bezpečnosť kritickej infraštruktúry pred teroristickými útokmi.

Spomínaný materiál bol braný ako základný dokument, ktorý rieši otázky ochrany a obrany kritickej infraštruktúry v Slovenskej republike a keďže ide o novú tému bolo treba zaviesť novú terminológiu, ktorá sa spája s touto problematikou.

Táto problematika je obsiahnutá aj v zákone č. 319/2002 Z. z o obrane Slovenskej republiky v znení neskorších predpisov, kde je definovaný pojem „obranná infraštruktúra“, ktorý podľa §26 ods. 1 tohto zákona je „súhrn pozemkov, stavieb, budov a zariadení, telekomunikačných, komunikačných a dopravných systémov, ktoré slúžia v čase vojny alebo vojnového stavu na zabezpečenie obrany štátu“ .

Celý legislatívny proces v oblasti KI v súčasnosti vyústil do schválenia zákona Národnej rady SR č. 45 z 8.2.2011 o kritickej infraštruktúre. Tento zákon v nadväznosti na vyššie uvedené legislatívne dokumenty aplikuje do praxe nášho štátu Smernicu Rady EU č.114/2008 z 8. 12. 2008 „o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu“. Z uvedeného zákona vyplýva konkretizácia predmetu ochrany KI pozostávajúca z jej jednotlivých prvkov. Prvkom kritickej infraštruktúry je najmä inžinierska stavba, verejnoprospešná služba alebo informačný systém v sektore, ktorého narušenie alebo zničenie by malo závažné nepriaznivé dôsledky. [4]

2. PRÍSTUPY K OCHRANE KRITICKEJ INFRAŠTRUKTÚRY

V každej spoločnosti existuje časť infraštruktúry, ktorá má rozhodujúci význam pre jej fungovanie. Táto infraštruktúra sa označuje ako životne dôležitá, resp. kritická. Ide o súhrn systémov (fyzikálnych alebo virtuálnych), ale aj inštitúcií, zariadení a služieb, ktorých narušenie alebo zničenie spravidla spôsobuje narušenie spoločenskej stability a bezpečnosti štátu, vyvoláva krízovú situáciu a negatívne ovplyvňuje fungovanie štátu (resp. štátnej správy a samosprávy) v krízových situáciách. Úlohou spoločnosti je takúto infraštruktúru ochrániť tak, aby fungovala za akejkoľvek situácie, tj. za normatívnych, mimoriadnych i kritických podmienok. Prístupy k ochrane kritickej infraštruktúry sa dlhodobo vyvíjajú, a to tak v zahraničí, ako aj u nás. Vývoj v posledných päťdesiatich rokoch zaznamenal rôznorodosť priorít vo vzťahu k jej ochrane.

Zatiaľ čo v polovici minulého storočia bolo prioritou čeliť hrozbe jadrového napadnutia, o 30 rokov neskôr začalo prevládať ohrozenie živelnými pohromami a teda aj ochrana pred nimi. Infraštruktúra predstavuje množinu prvkov, ktoré sú štruktúrované, navzájom prepojené a dávajú určitému celku rámcovou podporu.

Ochrana kritickej infraštruktúry

Ochranou kritickej infraštruktúry sa rozumie proces, ktorý pri zohľadnení všetkých rizík a hrozieb smeruje k zaisteniu fungovania subjektov kritickej infraštruktúry a väzieb medzi nimi.

Subjektmi kritickej infraštruktúry sú vlastníci a prevádzkovatelia výrobných a nevýrobných systémov vytvárajúcich produkty alebo poskytujúcich služby kritickej infraštruktúry. Objektmi kritickej infraštruktúry sú vybrané stavby a zariadenia verejnej infraštruktúry a ďalšie prvky, ktoré vlastnia alebo prevádzkujú subjekty kritickej infraštruktúry.[4]

Na ochrane kritickej infraštruktúry sa podieľajú niekoľkí aktéri - štát ako predstaviteľ vôle ľudu, súkromné subjekty, napr. vlastníci jednotlivých stavieb a zariadení kritickej infraštruktúry a ďalej obyvateľstvo, ktorému štát garantuje

prežitie v dobe krízy a v následnom období zaistenia stability a ďalšieho rozvoja.

Je zrejmé, že kritická infraštruktúra je zviazaná s územím ako takým a obyvateľstvom, ktoré sa na danom území nachádza. V území patrí do kritické infraštruktúry vybraná technická infraštruktúra spojená s daným územím a vybrané služby. Patrí sem systém dodávky energie, vody, zásobovanie potravinami, doprava, telekomunikačné systémy, zdravotnícke služby, záchranné služby, bezpečnostné služby, štátna správa, samospráva a iné.

Každý systém sa skladá z prvkov, väzieb a vzťahov medzi prvkami. Systém je priestorovo a časovo vymedzený (hranicami, životnosťou). Prvky systému môžu byť ďalej nedeliteľné alebo môžu vytvárať systém samy o sebe (sú subsystémom daného systému). To isté platí o kritickej infraštruktúre, kedy každá časť kritickej infraštruktúry tvorí sama o sebe systém.

Vstupy do systému, resp. výstupy zo systému sa realizujú na hraniciach systému a to buď bodovo (líniové stavby) alebo kontinuálne po celej dĺžke hranice (lesné masívy, hraničné rieky). Vstupy a výstupy na hraniciach systému môžu byť charakteru energetického, surovinového, finančného, informačného apod.

3. KOMPLEXNÉ RIEŠENIE OCHRANY OBJEKTOV S VYSOKÝM RIZIKOM NAPADNUTIA

V prípade, že chránený objekt sa vyznačuje vysokou mierou rizika napadnutia, je potrebný komplexný prístup k riešeniu problémov spojených s jeho ochranou. Pod pojem objekt musíme zaradiť nielen budovy alebo jednotlivé miestnosti, ale aj akékoľvek ohraničené priestory, ako napr. pozemky priľahlé k budovám, samostatné pozemky apod. Komplexným prístupom a vhodnou kombináciou použitých prostriedkov môžeme dosiahnuť ich maximálnu ochranu. Výsledkom tohto prístupu bude vznik bezpečnostného systému, ktorý umožni eliminovať alebo aspoň výrazne minimalizoval riziká, ktorá týmto objektom hrozia. Ak má byť zabezpečenie skutočne účinné, musia byť opatrenia aplikované nielen na zabezpečenie samotného objektu, ale aj na chod celej chránenej organizácie.

Zjednodušene sa dajú objekty s vysokým rizikom napadnutia charakterizovať ako objekty, u ktorých je výrazne vyšší predpoklad vzniku rizikovej situácie a následne i vzniku škôd na majetku, na zdraví a životoch ľudí, alebo u ktorých v dôsledku vzniku rizikovej situácie dôjde k poškodeniu, zničeniu, zneužitiu alebo strate dát a informácií významného charakteru, ktorá sa prejaví vysokou škodou (spravidla vyčísliteľnou v peniazoch).

Pri posudzovaní rizika napadnutia objektu je nutne k zásadným a obecným faktorom zaradiť mieru rizika, ktorá objektívne hrozí chránenému záujmu (zdravie alebo život občana alebo poškodenia majetku). Pri posudzovaní skutočnej miery rizika sa snažíme vždy zodpovedať otázky, napr. čo a prečo chránime a pred čím alebo pred kým chránime. Potom po čo najpresnejšej odpovedi na tieto otázky si môžeme položiť otázku, ako máme chrániť, t j. aké opatrenia musíme realizovať, aby ochrana osôb, majetku alebo informácií bola maximálne účinná.

Zabezpečenie objektu s vysokým stupňom rizika napadnutia by malo plniť predovšetkým nasledujúce funkcie:

- odradiť páchateľa od úmyslu preniknúť do chráneného objektu,
- znemožniť páchateľovi vniknutie do chráneného objektu alebo aspoň toto vniknutie výrazné spomaliť a sťažiť mu postup,
- donútiť páchateľa k zanechaniu stop pri preniknutí do objektu,
- vyvolať poplach a zaistiť včasný prenos informácie k zložkám, ktoré vykonajú zásah a dopadnú páchateľa pri čine,
- zadokumentovať vniknutie páchateľa do objektu a jeho pohyb v ňom.

Ohodnotenie a popísanie rizika je závislé na polohe objektu na pozemku, na jeho stavebne architektonickom riešení, či je umiestnený samostatne alebo v blízkosti iných objektov, na hustote zaľudnenia danej oblasti a hustote prevádzok, na jeho vnútornom dispozičnom riešení, na konkrétnom umiestnení predmetov, ktoré sú chránené, na počte vstupov do objektu a ich prístupnosti. Ďalej je nutné posúdiť existujúci spôsob zabezpečenia objektu, a to vrátanie posúdenia režimových opatrení, najmä organizáciu vstupu osôb do objektu a ich pohybu v ňom. Pre ohodnotenie a popísanie rizika je ďalej dôležité i to, čo je v objekte chránené (napr. peniaze, cennosti, umelecké diela alebo napr. výpočtová technika s uloženými informáciami apod.). Pre získanie úplnej predstavy o objekte sa nedá

vynechať ani posúdenie stavu kriminality v danej lokalite (zdrojom bývajú štatistiky trestných činov a priestupkov spáchaných v danej oblasti). Svoj význam majú aj skúsenosti zo skôr vykonaných napadnutí objektu rovnakého charakteru i na iných miestach, napr. napadnutie objektu galérií a múzeí, kedy môžeme získať prehľad o spôsoboch, ktoré páchatelia použili, aby porušili ochranu objektu.

Mechanické zábranné systémy:
Mechanické zábranné systémy sú historicky najstaršími technickými zabezpečovacími prostriedkami. Ich zmyslom je zabrániť nežiaducemu vniknutiu do objektu, nech už týmto objektom je ohraničený voľný priestor (pozemok) alebo budova, miestnosť či len úschovný objekt, ako je skriňa alebo trezor, prípadne dopravný prostriedok.

Technické prostriedky ochrany:
Z prvkov priestorovej ochrany je používaný **poplachový systém**, v prípade potreby je signál prenášaný prevažne do miesta stálej služby. V rámci snímačov sú v prevažnej miere využívané PIR hlásiče. Podobne je tomu i v prípade využívania elektrickej požiarnej ochrany, prostredníctvom **hlásičov požiaru**, ktorých signál je tiež prenášaný do miesta stálej služby. V prípade požiarnych hlásičov sú využívané automatické prevedenia v kombinácií s ionizačnými hlásičmi dymu. Z ďalších technických prostriedkov, sú využívané **systémy priemyselných televízií**, za využitia dlhodobých záznamov. **Ústredne EZS**, využívajú bezdrôtový prenos poplachového signálu od snímačov.

Organizačné a režimové opatrenia:
Pre zabezpečenie vstupu osôb, vjazdov vozidiel a pod. sú spracované a používané organizačné a režimové opatrenia. Organizácia napr. ochrany, ako aj ďalšie aktivity sú riešené v súlade so smernica pre danú činnosť. Fyzická ochrana je vykonávaná formou strážnej služby, bezpečnostným dohľadom, kontrolnou priepustkovou službou, prípadne bezpečnostným výjazdom (zásahom). Fyzická ochrana je nasmerovaná na nevyhnutnú kontrolu, ostatné kontrolne mechanizmy sú kombinované s technickými prostriedkami ochrany.

ZÁVER:

Ochranou kritickej infraštruktúry môžeme rozumieť súbor opatrení, ktoré zabezpečuje vlastník, prípadne správca objektu, súkromné bezpečnostné služby a určené jednotky policajného zboru s cieľom chrániť majetok objektov kritickej infraštruktúry. Vykonáva sa nepretržite, ako v stave bezpečnosti, tak aj v období krízovej situácie. Identifikácia a ochrana kritickej infraštruktúry je náročný a dlhotrvajúci proces. Z hľadiska zabezpečenia bezpečnosti štátu je to však úloha, u ktorej sa dá predpokladať vzhľadom na vývoj technológií, stále väčší význam a prioritné postavenie. Zároveň vytvára podmienky na zvládnutie mimoriadnych udalostí a krízových situácií.

LITERATÚRA

[1] Bezpečnostná stratégia EÚ. EK Brusel, Belgicko, 2003.
[2] Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry, KOM(2005) Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany 576, Brusel, 2005.
[3] Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany, Bratislava, 2007
[4] Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.
[5] Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky.

Táto práca bola podporovaná projektom APVV 0471-10
Ochrana kritickej infraštruktúry v sektore doprava.

This paper was supported by project APVV 0471-10
Critical infrastructure protection in sector transport