# OCHRANA OBJEKTOV KRITICKEJ INFRAŠTRUKTÚRY

**Selinger Petr** *

## ABSTRAKT
V 21. storočí ochrana osôb a majetku nič nestráca na svojom význame. Naopak jej význam raste a spoločnosť sa snaží zákonnými prostriedkami posilniť ochranu osôb a majetku. Na jednej strane sa sprísňuje legislatíva, na druhej strane sa neustále zdokonaľujú technické prostriedky ochrany osôb a majetku. Článok rieši problematiku potreby definovania kritickej infraštruktúry ako takej oblasti infraštruktúry, ktorej zničenie vyvolá vážne politické a hospodárske dôsledky. Zničenie alebo znefunkčnenie kritickej infraštruktúry by znamenalo veľké straty na životoch a majetku, morálne škody.

**Kľúčové slová:**
kritická infraštruktúra, ochrana objektov kritickej infraštruktúry, technická ochrana, fyzická ochrana.

## ABSTRACT
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 of persons and property by legal means. 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

* Petr Selinger, Ing., PhD., KBM, Fakulta špeciálneho inžinierstva, ŽU v Žiline, Petr.Selinger@fsi.uniza.sk

# 1 LEGISLATÍVNE VYMEDZENIE POJMU KRITICKÁ INFRAŠTRUKTÚRA

Vychádzajúc zo súčasných bezpečnostných rizík vznikla vo vyspelých štátoch sveta potreba definovania kritickej infraštruktúry ako takej oblasti infraštruktúry, ktorej zničenie vyvolá 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 alebo trestná činnosť, sa rozšírila o novodobú hrozbu teroristických útokov. Viaceré európske krajiny sú teroristami považované za potenciálne ciele a Európa je aj jednou zo základní ich pôsobenia. 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 zo strany Európskej únie bolo vypracovanie viacerých dokumentov, v ktorých bola 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).

Výstražnej informačnej siete kritickej infraštruktúry (Critical Infrastructure Warning Information Network, skr. CIWIN, ďalej len CIWIN). Komisia usporiadala dva semináre, ktorých sa zúčastnili členské štáty i priemyselné združenia a predložili svoje návrhy v tejto oblasti. Výsledkom bolo vypracovanie Zelenej knihy o európskom programe na ochranu kritickej infraštruktúry.

V zelenej knihe sú predložené 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 obsahovala čo najmenej možností zlyhania a rýchle nápravné opatrenia. Úroveň ochrany by pritom nemala byť pre všetky prvky rovnaká, ale 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. Úroveň ochrany by pritom nemala byť pre všetky prvky rovnaká, ale 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.

## 1.1 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. 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 systémy nevyhnutných na bezpečné fungovanie základných funkcií štátu a zaručí sa za bezpečnosť kritickej infraštruktúry pred teroristickými útokmi.

Doposiaľ bola koncepcia braná ako základný dokument, ktorý rieši otázky ochrany a obrany kritickej infraštruktúry v Slovenskej republike a keďže ide o novú tému musí sa zaviesť terminológia, ktorá sa bude spájať s touto problematikou.

O tejto problematike pojednával doposiaľ zákon č. 319/2002 Z.z o obrane Slovenskej republiky v znení neskorších predpisov, kde sa definoval 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 prijaté v uzneseniach vlády SR 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, ktoré sú charakterizované ako: „prvkom kritickej infraštruktúry najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia.

# 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. Úkolom spoločnosti je takúto infraštruktúru ochrániť tak, aby fungovala za akejkoľvek situácie, tj. za bežných, mimoriadnych i kritických podmienok. Prístupy k ochrane kritické infraštruktúry sa dlhodobo vyvíjajú, a to nielen v zahraničí, ale i u nás. Vývoj v posledných 50 rokoch zaznamenal rôznorodosť priorít v jej ochrane.

Zatiaľ čo v polovine minulého storočia bola prioritou hrozba jadrového napadnutia, o 30 let neskôr začalo prevládať ohrozenie živelnými pohromami. Infraštruktúra predstavuje v najvšeobecnejším zmyslu slova množinu prvkov, ktoré sú štruktúrované, navzájom prepojené a poskytuj určitému celku rámcovou podporu. Pojem infraštruktúra sa zvyčajne používa iba pre štruktúry, ktoré sú vytvorené umelo.

## 2.1 OCHRANA KRITICKEJ INFRAŠTRUKTÚRY

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

Subjekty kritické infraštruktúry predstavujú vlastníci a prevádzkovatelia výrobných a nevýrobných systémov vytvárajúcich produkty nebo poskytujúcich služby kritické infraštruktúry. Objekty kritické infraštruktúry sú vybrané stavby a zariadenia verejnej infraštruktúry a ďalšie prvky, ktoré vlastní nebo prevádzkujú subjekty kritické infraštruktúry.

Na ochrane kritické infraštruktúry sa podieľajú niekoľkí aktéri - štát ako predstaviteľ vôle lidu, štát a súkromné subjekty ako vlastníci jednotlivých stavieb a zariadení kritické infraštruktúry a ďalej obyvateľstvo, ktorému štát garantuje prežitie v dobe kríze a v následnom období zaistení stability a ďalší rozvoj.

Je zrejmé, že kritická infraštruktúra je zviazaná s územím ako takým a obyvateľstvom, ktoré dané území obýva. V území patrí do kritické infraštruktúry vybraná technická infraštruktúra spojená s daným územím a vybrané služby.

Každý systém sa skladá z prvkov, väzieb a tokov. Systém je priestorovo a časovo vymedzený (hranice systému, jeho životnosť). Prvky systému môžu byť ďalej nedeliteľné alebo vytvárať systém samy o sebe (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

Ako náhle sme dospeli k záveru, že chránený zajem sa vyznačuje vysokou mierou rizika napadnutia, je potrebný komplexný prístup k riešeniu problémov spojených s ochranou príslušného objektu. 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 cez nepriaznivé vonkajšie vplyvy dosiahnuť ich maximálnu účinnosti. Výsledkom tohto prístupu bude integrovaný bezpečnostný systém, ktorý umožni eliminovať alebo aspoň výrazne minimalizoval riziká, ktorá týmto objektom hrozí. Ak má byť totiž zabezpečenie skutočne účinné, búdou opatrenia aplikované nielen na zabezpečenie samotného objektu, ale aj na chod celej 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 aspoň sčasti v peniazoch).

Pri posudzovaní miery rizika napadnutia objektu nutne k zásadným a obecným faktorom ovplyvňujúcim formu prostriedkov a opatrení použitých pri ochrane je samozrejmé miera rizika, ktorá objektívne hrozí chránenému záujmu (zdraví nebo život občana nebo majetok). 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, tj. 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,
- ohodnotiť riziko a úplné ho popísať,
- stanoviť výšku rizika,
- navrhnúť opatrenia k ochrane pred rizikom.

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 prevádzky, na jeho vnútornom dispozičnom riešení, na konkrétnom umiestnení predmetov, ktoré sú chránené, na počte vstupov do objektu a ich prístupnosti. Ďalej je nutné posúdiť stavajúci spôsob zabezpečenia objektu, a to vrátania 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 získaní úplné predstavy sa nedá vynechať ani posúdenie stavu kriminality danej lokality (zdrojom bývajú štatistiky trestných činov spáchaných v danej oblasti). Nedá sa zabudnúť ani na 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 vniknutí 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 požiarnej ochrany**, 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 priepustková službou, prípadne bezpečnostným výjazdom (zásahom). Fyzická ochrana je nasmerovaná na nevyhnutnú kontrolu, ostatné kontrolne mechanizmy sú kombinované s technickými prostriedkami ochrany.

## LITERATÚRA


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



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