DOI: https://doi.org/10.52651/vr.a.2022.2.08-27
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2022, Číslo 2, Strana 08-27

TEORETICKO-METODOLOGICKÉ VÝCHODISKÁ OCHRANY „MÄKKÝCH CIEĽOV“

THEORETICAL-METHODOLOGICAL ASPECTS OF THE SOFT TARGETS PROTECTION

Ladislav HOFREITER

HISTÓRIA ČLÁNKU

Doručený: *13. 10. 2022*
Schválený: *12. 12. 2022*
Vydaný: *31. 12. 2022*

ABSTRACT

Over the last few years, the number of terrorist attacks in Europe has increased considerably, causing considerable tension and nervousness. Not only in Europe, but also around the world, terrorist attacks and other violent crimes are increasingly concentrated around targets that are easy to access and characterized by a high concentration of people and a relatively low level of protection – soft targets. In this article, we will present methods of identifying factors that affect the protection of soft targets. We will use mind mapping to identify an attacker, as well as conditions for attacking soft targets. We will also present possible concepts of soft targets protection.

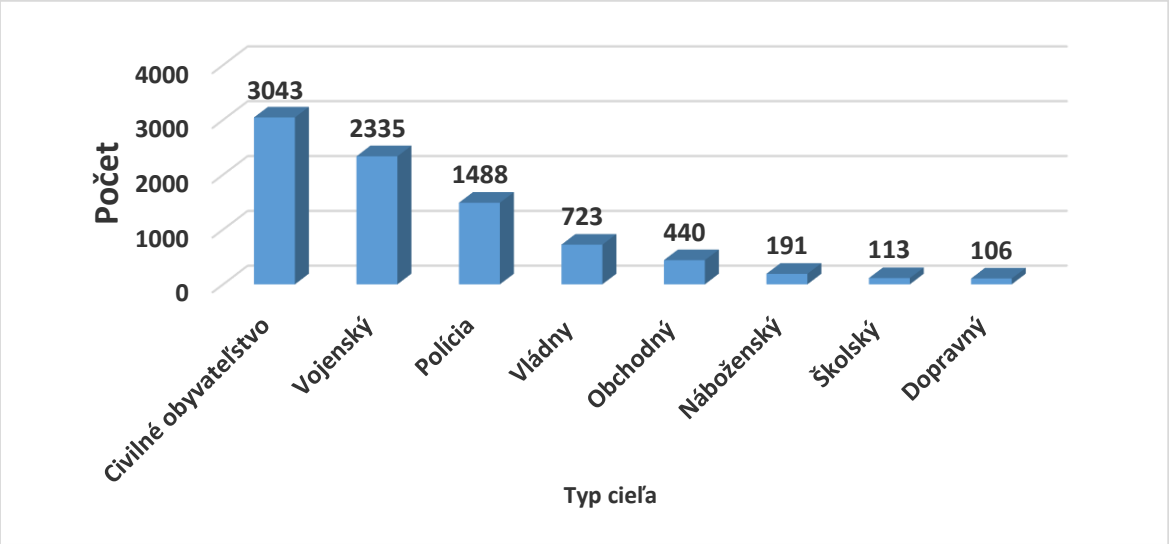
KEYWORDS

Soft target, qualitative methods, assumptions and conditions of attack, concepts of protection

ÚVOD

Bezpečnosť je základná ľudská potreba. Jeho význam a hodnota narastá, keď sa prejavujú nové bezpečnostné výzvy a hrozby. Keď Ulrich Beck nazval túto spoločnosť rizikovou spoločnosťou (Beck, 1986), mal na mysli predovšetkým riziká vyplývajúce z katastrof spojených s modernizáciou spoločnosti, z rozvojom technológií a ich vplyvu na životné prostredie. Spektrum súčasných hrozieb a rizík, ktoré vyvolávajú v ľuďoch strach, je širšie. Útoky na objekty a priestory s hromadným výskytom osôb sa stali novým typom hrozieb, ovplyvňujúcim mieru a efekt bezpečnostných rizík. Najväčším ohrozením pre človeka sa tak stal človek s iným hodnotovým systémom, s iným videním sveta, človek frustrovaný z nemožnosti uspokojiť svoje potreby, človek vzdorujúci, protestujúci. Ako cieľ na prezentovanie svojej nespokojnosti si vyberá tých najzraniteľnejších – ľudí, ktorí nakupujú, cestujú alebo sa zabávajú. Terčom ich útokov sú spravidla ľahko dostupné a tým

aj zraniteľné objekty s hromadným výskytom ľudí, čím dosahujú mimoriadne vysoký efekt svojho konania.



Graf 1 Vybrané ciele teroristických útokov na svete v roku 2020.
Zdroj: vlastné spracovanie podľa statista.com/statistics

V posledných rokoch pribúdali vo svete útoky na ciele, ktoré sa vyznačovali obmedzenou ochranou. Teroristi a iní zločinci čoraz častejšie útočia na nechránené objekty a miesta, kde sa zhromažďujú ľudia, bez ohľadu na to, či ide o politickú, náboženskú alebo inú symbolickú zámienku (obr.1). Útoky v Paríži, Bruseli, Barcelone, Nice, Manchestri, Štrasburgu, Štokholme či Berlíne sú typickými útokmi na mäkké ciele (Hofreiter, Kubíková, 2020). Tieto príklady ukazujú, že viac ako kedykoľvek predtým, je potrebné riešiť bezpečnosť ľudí na otvorených priestranstvách alebo vo voľne dostupných objektoch. Priamo to súvisí s jedným z pilierov koncepcie ľudskej bezpečnosti, t. j. zabezpečiť, aby boli ľudia zbavení strachu, že sa stanú kdekoľvek a kedykoľvek cieľom a obeťou útoku. To znamená vyriešiť problém ochrany takzvaných „mäkkých cieľov".[1] Kľúčová otázka znie: je možné takýto typ cieľov ochrániť? Odpoveď na túto otázku je veľmi ťažká a komplikovaná.

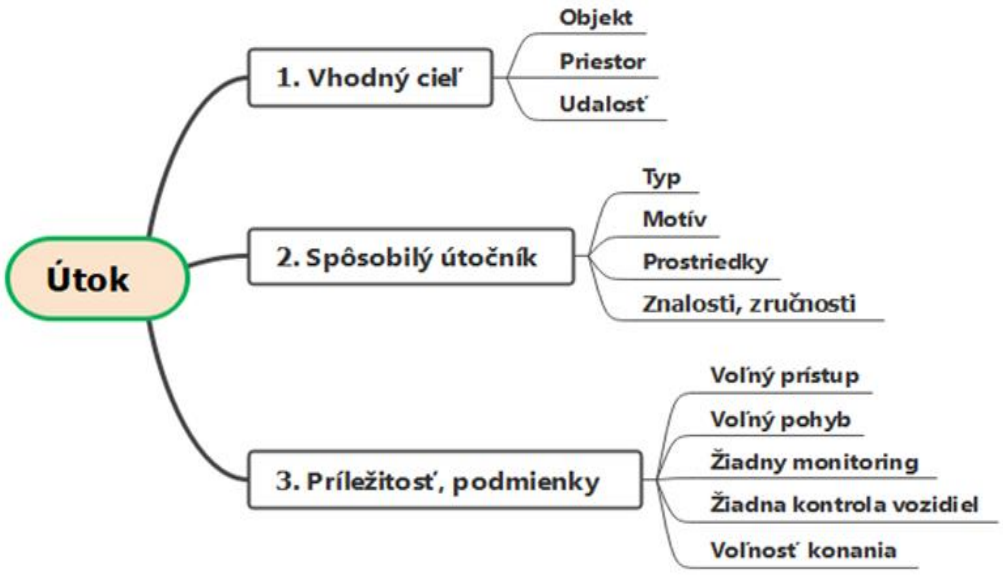
1 METÓDY

Teoretický prístup k ochrane tzv. mäkkých cieľov je založený na objasnení nasledujúcich otázok (Hofreiter,2015):

[1] *V bezpečnostnej komunite je tento pojem všeobecne známy a jeho opozitom je pojem „tvrdý cieľ" (Hard Target), ktorým sa označujú ciele, resp. objekty, ktoré sú dobre chránené a strážené , napr. niektoré vládne objekty, štátne objekty, vojenské objekty, objekty ďalších bezpečnostnýchch zložiek, ale i medzinárodné summity, stretnutia štátnikov, alebo i niektoré dobre chránené či strážené neštátne či komerčné objekty. (Kalvach, 2016; UN 2022: Protecting vulnerable targets from terrorist attacks,...)*

- ČO treba chrániť, KTO je objektom ochrany?
- Pred ČÍM, pred KÝM treba objekt chrániť?
- AKO bude ohrozený objekt?
- AKO objekt chrániť?

Grafické vyjadrenie postupu riešenia problému je na obrázku 1.



Obrázok 1 Myšlienková mapa identifikácie podmienok útoku na mäkký cieľ.
Zdroj: vlastné spracovanie

Základom ochrany mäkkých cieľov je jasný popis predmetu ochrany. Optimálne metódy na objasnenie tohto aspektu sú klasifikačná analýza a metóda myšlienkovej mapy. Použitím klasifikačnej analýzy identifikujeme na základe charakteristických znakov a vlastností možné objekty útokov a tým aj objekty ochrany (Hofreiter, Zvaková, 2019). Myšlienková mapa je vysoko efektívna metóda, ktorá je ideálna na identifikáciu štruktúry objektov, ktoré môžu byť cieľom útoku.

Druhý aspekt spočíva v objasnení faktorov, príčin a podmienok, ktoré umožňujú útok na mäkký cieľ. Metódu kauzálnej analýzy použijeme na identifikáciu príčin útoku, metódu eliminačnej indukcie použijeme na identifikovanie a vyčlenenie tých príčin, okolností a podmienok, ktoré sú nevyhnutné na uskutočnenie útoku na mäkký cieľ. V tejto súvislosti použijeme aj produkčné pravidlá (Popper, Kelemen, 1989) a Booleovskú logiku, ako aj fuzzy logiku (Hofreiter, Zvaková, 2019).

Cieľom identifikácie možného spôsobu útoku na mäkký cieľ je odhaliť vzťah medzi typmi útočníka, jeho motívom, úmyslom a prostriedkami použitými na útok. Na vyriešenie

tohto problému použijeme metódu morfologickej analýzy. Morfologická analýza je nekvantifikovaná, heuristická metóda na štruktúrovanie a analýzu súboru vzťahov vo viacrozmernom, nekvantifikovateľnom komplexnom probléme (Hofreiter, 2019).

Na základe znalosti typu cieľa a pravdepodobného spôsobu útoku použijeme indukčnú metódu na predstavenie možných koncepcií ochrany mäkkého cieľa.

Teoretickými východiskami riešenia problému ochrany mäkkých cieľov bola obsahová analýza literárnych zdrojov, ktorých prehľad je uvedený v zozname bibliografických odkazov.

2 VÝSLEDKY

2.1 Popis objektu ochrany

Za objekt ochrany budeme považovať „mäkký cieľ“. V súčasnosti neexistuje jednotná definícia takýchto cieľov, avšak vo všeobecnosti sa jedná o nedostatočne chránené civilné objekty, v ktorých sa zhromažďuje veľké množstvo ľudí. Vzhľadom na uvedené sa často stretávame aj s označením „miesta hromadného výskytu osôb“ (places of mass gathering) (National Guidelines for the Protection..., 2011). Miesta hromadného výskytu osôb sú potenciálnymi cieľmi teroristických útokov, najmä vo väčších mestách. Spravidla sú to otvorené priestranstvá alebo uzavreté priestory, či prostredia s vysokou koncentráciou ľudí, ako sú napr. verejné zhromaždenia, nákupné centrá, športové štadióny, bary, kluby, ktoré sú ľahko prístupné verejnosti. Tieto priestory sú príťažlivým cieľom pre útočníkov, pretože, sú ľahko prístupné a ponúkajú šancu na dosiahnutie úspechu pri útoku.

Je dôležité si tiež uvedomiť, že o vymedzení mäkkých cieľov hovoríme iba v spojitosti s teroristickými alebo násilnými útokmi, voči ktorým nie sú jednotlivé objekty alebo priestory dostatočne chránené. Neznamená to teda, že nie sú dobre chránené voči iným hrozbám (napríklad majetková trestná činnosť) a často disponujú rôznymi kvalitnými prvkami ochrany ako sú napr. kamerový systém, poplachové zabezpečovacie a tiesňové systémy či fyzická ochrana (napríklad obchodné centrá).

Prístupy k definovaniu tzv. mäkkých cieľov možno vnímať z rôznych perspektív. Vo vojenstve sa za mäkký cieľ pokladá všetko, čo sa dá zničiť guľometmi, puškami alebo trieštivo-trhavými granátmi.

V stavebníctve pod týmto pojmom chápu stavby a budovy, ktoré treba chrániť a spevniť a záchranári – ako hasiči si nemyslia, že mäkké ciele sú spojené len s útokmi, ale uvažujú aj o haváriách s možnosťou úniku nebezpečnej látky, meteorologických vplyvoch, požiaroch a pod. (Hofreiter, Kubíková, 2017).

Bezpečnostná komunita vníma ako objekt ochrany ľudí a ich životy, ktoré môžu byť ohrozené. Mäkké ciele sú definované len v súvislosti s teroristickými alebo násilnými útokmi,

proti objektom a priestorom, ktoré nie sú dostatočne chránené (Karlos, Larcher, Solomos, 2018).

Ministerstvo vnútornej bezpečnosti USA uvádza, že mäkké ciele (Soft Target) , ako sú športoviská, nákupné strediská, školy a dopravné systémy sú miesta, ktoré sú ľahko dostupné veľkému počtu ľudí a ktorých zavedené bezpečnostné a ochranné opatrenia sú obmedzené alebo žiadne, a preto sú zraniteľné voči útokom (US Department, 2018).

Jenifer Hasterman uvádza, že mäkké ciele sú akékoľvek miesto, ktoré nie je dobre chránené alebo opevnené, takže je obzvlášť zraniteľné voči útoku (Hesterman, 2015). V kontexte terorizmu sa môžu za mäkké ciele označovať oblasti, kde sa voľne pohybuje veľké množstvo ľudí a je tam toľko aktivity, že zabezpečiť kontrolovaný tok davu je značne náročné.

Podľa anglických Oxford Living Dictionaries mäkký cieľ (Soft Target) je osoba alebo vec, ktorá je relatívne nechránená alebo zraniteľná, najmä voči vojenskému alebo teroristickému útoku (Definition... 2017)

Podľa Travel Security Handbook je mäkkým cieľom osoba, ktorá je v dôsledku svojho konania a/alebo nedostatku vhodných ochranných opatrení vydaná na milosť a nemilosť existujúcim rizikám, a preto predstavuje ľahký cieľ.

Ako mäkké ciele sú tiež uvádzané civilné miesta, kde sa zhromažďujú ľudia vo veľkom počte (napr. verejné priestranstvá, nemocnice, školy, športové arény, kultúrne centrá, kaviarne a reštaurácie, nákupné centrá a dopravné uzly). Tieto miesta sú svojou povahou zraniteľné a je ťažké ich chrániť a vyznačujú sa vysokou pravdepodobnosťou hromadných obetí v prípade teroristického útoku. Z týchto dôvodov sú teroristami zvýhodňované. (Jurčák,V., Sasarák, L., 2019).

Ako uvádza Kalvach, aj keď neexistuje oficiálna definícia pojmu „mäkké ciele “, v bezpečnostných kruhoch sa tento termín používa na označenia miest s vysokou koncentráciou ľudí a nízkym stupňom ochrany pred útokmi, čo vytvára atraktívny cieľ, hlavne pre teroristov (Kalvach, 2016).

Vo všeobecnosti môžeme mäkké ciele ako objekty ochrany charakterizovať a opísať takto:

- sú to objekty a miesta s hromadným výskytom ľudí,
- kontrola vstupu a pohybu osôb je sťažená alebo nemožná,
- sú relatívne nechránené, a preto zraniteľné.

V kontexte uvedených atribútov mäkký cieľ znamená ľahký cieľ útoku. Minimálna ochrana a vysoký počet ľudí na jednom mieste zvyšuje ich atraktivitu a záujem útočníkov. Pri výbere budúceho cieľa útoku preto zavážia také kritériá, ako napr. ľahký a nepozorovaný prístup (cieľ je dostupný), významnosť cieľa, mediálna pozornosť, slabá ochrana či vysoká

symbolická hodnota. Takýmto kritériám vyhovujú objekty, priestory a podujatia s veľkým výskytom osôb.

2.2 Identifikácia faktorov a podmienok útoku

V tejto fáze analýz potrebujeme identifikovať faktory, ktoré sú potrebné na rozhodnutie o potrebe ochrany. To znamená, že musíme identifikovať čo sa môže stať, prečo a ako sa to môže stať. Identifikujeme, ktoré faktory primárne určujú útok na objekt. Udalosť, ktorá má potenciál ohroziť mäkký cieľ, je vonkajší útok. Útok je nepriateľský násilný čin proti objektu s úmyslom zabiť, zničiť a vyvolať strach. Podľa teórie „čiernej labute“ (Black Swan theory) je útok na mäkký cieľ udalosťou s nasledujúcimi tromi atribútmi:

- je neočakávaný, prekvapivý,
- má mimoriadne negatívny vplyv na verejnú morálku,
- po útoku je možné objasniť jeho príčiny a spôsob vykonania.

Pri uvažovaní o možnosti útoku na mäkký cieľ budeme vychádzať z produkčného pravidla, ktoré môžeme rozdeliť na dve časti (Popper, Kelemen, 1989):

- predpokladovú, situačnú (*ancendent*),
- dôsledkovú, akčnú (*konzekvent*),

čo môžeme vyjadriť zápisom:

AK (je splnená) predpokladová časť, TAK (platí) dôsledková časť. (1)

Predpokladová časť produkčného pravidla vyjadruje predpoklady, ktoré ak sú splnené, platí aj dôsledková časť. Platnosť dôsledku pri splnených predpokladoch nemá vo všeobecnosti kategorickú povahu, ale len určitú vierohodnosť.

V súvislosti s predmetom skúmania môžeme za predpoklady útoku (Ú) na mäkký cieľ považovať (Hofreiter, 2015):

- vhodný cieľ (VC),
- spôsobilý útočník, ktorý má motív a spôsobilosti vykonať útok (SÚ),
- priaznivé podmienky (príležitosť) na útok (PP).

Na základe identifikovaných predpokladov môžeme produkčné pravidlo (1) zapísať v tvare:

$$Ak\ VC \wedge SÚ\ \wedge PP\ Tak\ Ú \qquad (2)$$

Produkčné pravidlo (2) vyjadruje, že podmienkou, aby došlo k útoku na mäkký cieľ, musia nevyhnutne byť súčasne splnené všetky tri predpoklady – vhodný cieľ, spôsobilý útočník a príležitosť, resp. vhodné podmienky.

Vzhľadom na kritériá uvedené v kapitole 2.1, budeme za **vhodné ciele** považovať:

a. Objekty:

- komerčné objekty: obchodné objekty, nákupné centrá, obchodné komplexy,
- školy a školské zariadenia, posluchárne vysokých škôl,
- športové objekty , napr. plavárne, športové haly,
- kultúrne objekty, napr. divadlá, kiná, múzeá, galérie,
- cirkevné objekty, napr. kostoly, pútnické miesta , cirkevné pamiatky ap.
- dopravné objekty, ako napr. železničné stanice, stanice podzemných dráh, letiskové terminály, prístavy,
- zábavné objekty, napr. bary, diskotéky, kluby, koncertné sály ap.

b. Priestory. Medzi priestory spĺňajúce podmienky na klasifikovanie ako mäkkých cieľov môžeme zaradiť:

- mestské centrá,
- námestia,
- pešie zóny,
- bulváre,
- parky,
- tržnice ap.

c. Udalosti, ktoré môžu priťahovať pozornosť útočníkov, a z toho dôvodu môžu byť klasifikované ako mäkké ciele, sú najmä:

- verejné masové zhromaždenia , sprievody, demonštrácie,
- náboženské akcie, púte,
- športové masové akcie,
- veľké koncerty ap.

Každý z týchto objektov a/alebo priestorov spĺňa podmienku súčasného výskytu veľkého počtu osôb a minimálnych alebo žiadnych ochranných opatrení na zamedzenie ohrozenia osôb násilnými útokmi.

Dôležitým predpokladom, aby došlo k útoku na mäkký cieľ je existencia spôsobilého útočníka, teda niekoho (osoby, skupiny), kto chce (má motív), má zámer a vie (má spôsobilosti, zručnosti) (Hofreiter,2015).

Nositeľom tohto typu hrozby sú najčastejšie teroristi, a to buď v skupine alebo jednotlivci, ktorí sú členmi teroristickej skupiny. Potom sú to tzv. „osamelí vlci", útočníci bez priameho prepojenia na akúkoľvek teroristickú skupinu. Napriek ich neexistujúcemu prepojeniu sa páchatelia verejne hlásia k takýmto skupinám a často konajú v ich mene. Rozdiel medzi členom teroristickej skupiny a osamelým vlkom spočíva často aj v ich motivácií. V zásade však platí, že osamelí vlci sa vyznačujú nepredvídateľnosťou konania a ich ciele sú vyberané často celkom náhodné, čo sťažuje aj prácu bezpečnostných zložiek v procese odhaľovania útokov.

Spôsobilosť útočníka (SÚ) uskutočniť útok na mäkký cieľ môžeme hodnotiť podľa nasledujúcich činiteľov (Hofreiter,2015):

- motívu, zámeru útoku (M),
- možnosť získania vhodného prostriedku útoku (VP),
- znalosti a zručnosti v použití prostriedku, nástroja útoku (Z).

Motívy, pohnútky konania útočníkov môžu byť:

- Politické, ako snaha zmeniť politický systém, získať moc, alebo zdiskreditovať vládnucu politickú reprezentáciu (M1),
- Ideologické, vyvolané úsilím presadiť určitú ideológiu alebo eliminovať, likvidovať zástancov inej ideológie (M2).
- Rasové, vyvolané nenávisťou voči iným z dôvodov ako je rasa, farba pleti, jazyk, náboženstvo, štátna príslušnosť alebo národnostný či etnický pôvod (M3).
- Náboženské, majúce korene vo fundamentalizme a v presadzovaní určitého náboženstva ako určujúceho činiteľa verejného a politického života, nezmieriteľnosťou k iným náboženstvám alebo porušovateľom daných náboženských noriem a pravidiel (M4),
- Osobné, vyvolané krivdou, patologickou nenávisťou, pomstou za skutočné alebo domnelé krivdy, (M5).
- Iné, ako napr. potreba zabíjať, alebo len konanie v afekte, bez predchádzajúcej prípravy, resp. ako dôsledok psychickej poruchy (Mn).

Existenciu, resp. vierohodnosť relevantného motívu môžeme vyjadriť použitím produkčného pravidla spojeného s fuzzy logikou (vzorec 3).

$$Ak(M1 = 1) \vee (M2 = 1) \vee (M3 = 1) \vee \ldots \vee (Mn = 1) Tak\ M=1 \qquad (3)$$

Zápis (3) vyjadruje, že na identifikovanie vierohodného a relevantného motívu útočníka postačuje existencia ktoréhokoľvek z možných motívov, pretože vzťah predpokladov je disjunktný.

Útočníci môžu pri útoku na mäkké ciele použiť rôzne **prostriedky**, ktorých dostupnosť v súčasnej dobe nie je nijako zvlášť obmedzená alebo sťažená. Na útok môžu byť použité:

- improvizované výbušné zariadenia (IVZ),
- strelné, väčšinou automatické zbrane,
- otravné alebo dráždivé látky,
- motorové vozidlá,
- chladné zbrane (nože, sekery, bajonety atď.),
- zápalné prostriedky,
- bezpilotné prostriedky – drony,
- kybernetické útoky.

Znalosti a zručnosti budú závisieť od typu útočníka a od použitého prostriedku na vykonanie útoku. Pomocou matice morfologickej analýzy a podľa pravdepodobného typu útočníka, jeho motívu a zámeru môžeme identifikovať možné znalosti a zručnosti potenciálneho útočníka.

Tabuľka 1 Matica morfologickej analýzy potrebných znalostí a zručností i útočníka

Stavy premenných	**Premenné**		
	Útočník -U	Prostriedky útoku -PÚ	Znalosti, zručnosti- Z
	U1:Jednotlivec	PÚ1:Improvizované výbušné zariadenie-IVZ	Z1:Žiadne
	U2:Jednotlivec terorista	PÚ2:Chladná zbraň	Z2:Minimálne
	U3:Jednotlivec extrémista	PÚ3:Strelná zbraň	Z3:Dostatočné
	U4:Skupina extrémistov	PÚ4:Automobil	Z4:Pokročilé
	U5:Skupina teroristov	PÚ 5:Otravné látky	Z5:Excelentné
	U6:Skupina- org. zločin	PÚ6:Zápalné prostriedky	
		PÚ7:UAV - dron	
		PÚ8: Kybernetické útoky	

Zdroj: vlastné spracovanie

Vstupom do použitia metódy morfologickej analýzy je ujasnenie si (stanovenie) cieľa analýzy (Hofreiter, 2019). V tomto prípade riešeným problémom môže byť hľadanie požadovaných (očakávaných) znalostí a zručností na uskutočnenie útoku na mäkký cieľ s dostupnými prostriedkami útoku.

V prvom kroku analytickej fázy ide o hľadanie odpovede na otázku: Ktoré faktory ovplyvňujú existenciu daného problému? Výsledkom je identifikovanie nezávislých premenných, ktoré determinujú existenciu problému. Premennými sú útočník, prostriedky útoku, znalosti a zručnosti.

V druhom kroku vymedzíme stavy, ktoré by mohla príslušná premenná teoreticky dosiahnuť.

V treťom kroku vytvoríme morfologické pole (maticu) problému. Postupujeme tak, že do prvého riadku matice vpíšeme premenné a do stĺpcov pod každou premennou jej potenciálne podmienky (stavy). Tým získame morfologické pole, (Tab. 1) pričom počet možných konfigurácií stavov premenných zodpovedá počtu uvažovaných stavov. V našom príklade sú stavy premenných U=6 ; PÚ=8; Z=5, teda počet konfigurácií je 6x8x5 = 240.

Obsahom syntetickej fázy je hľadanie vhodných konfigurácii zo všetkých možných konfigurácií, ktoré morfologické pole problému poskytuje (Hofreiter, 2019). Prvou úlohou syntetickej fázy je vylúčiť nereálne konfigurácie, t. j. tie, ktoré obsahujú vzájomne si odporujúce podmienky (stavy) premenných. V tomto kroku postupujeme tak, že vytvoríme párové kombinácie podmienok (stavov) vo vzájomne odlišných parametroch a každý pár vyšetrujeme položením otázky, či sú členy dvojice vo vzájomnej zhode. Postupujeme tak, že kladieme otázky, napr.:

- môže podmienka (stav) U1 koexistovať s podmienkou (stavom) PÚ1?
- môže podmienka (stav) U1 koexistovať s podmienkou (stavom) Z1?
- môže podmienka (stav) PÚ1 koexistovať s podmienkou (stavom) Z1?
- atď.

Výsledok je buď áno (A), alebo nie (N). Takto postupujeme so všetkými párovými podmienkami (stavmi). Ak nie, potom vylúčime konfiguráciu, ktorá obsahuje takýto pár. Podmienkou pre riešenie problému je, aby súčasne existovali všetky identifikované premenné, a podmienkou na to, aby bola prítomná požadovaná premenná, musí existovať aspoň jeden z jej definovaných stavov.

Vierohodnosť existencie spôsobilého útočníka (SÚ) môžeme vyjadriť , vychádzajúc z predchádzajúcich analýz, pomocou produkčného pravidla spojeného s fuzzy logikou (vzorec 4).

$$Ak\ (M = 1)\ \wedge (VP = 1\ ) \wedge (Z = 1)\ Tak\ S\acute{U}\ = 1 \qquad (4)$$

Za **priaznivé podmienky** (PP) pre útok na mäkký cieľ môžeme považovať:

- voľný prístup k cieľu,
- nekontrolovateľný pohyb v priestore cieľa,

- žiadny monitoring v priestore cieľa,
- žiadna kontrola vozidiel, donášaných, dovážaných zásielok a tovarov.
- voľnosť konania.

2.3 Ohodnotenie vierohodnosti útoku

Podľa Booleovej logiky (Frištacký, et al., 1986) a produkčných pravidiel môže dôjsť k útoku (Ú), ak existuje vhodný cieľ (VC), spôsobilý útočník (SÚ) a vhodná príležitosť (PP) na útok. Existencia útočníka, vhodný cieľ a príležitosť sú nevyhnutné podmienky. Táto podmienka je vyjadrená nasledujúcim spôsobom:

$$Ak\ (VC = 1)\ \wedge (SO = 1\ ) \wedge (PP = 1)\ Tak\ \text{Ú}\ = 1 \tag{5}$$

Bez splnenia tejto podmienky nemôže dôjsť k útoku (tabuľka 2).

Tabuľka 2 Pravdivostná tabuľka Booleovskej logiky na posúdenie podmienok, aby došlo k útoku

Vhodný cieľ	**Spôsobilý útočník**	**Priaznivé podmienky, príležitosť**	**Dôjde k útoku?**
1	1	1	1
1	1	0	0
1	1	0	0
1	0	1	0
0	1	0	0

Zdroj: Vlastné spracovanie

Ak je potvrdená pravdivosť podmienky (5), ohodnotíme vierohodnosť (plauzibilitu) útoku. Pretože súčasná existencia vhodného cieľa a schopného útočníka, ako aj vhodnej príležitosti na útok je nevyhnutnou podmienkou (vzorec 6), ich vierohodnosť (plauzibilitu) ohodnotíme podľa škály vierohodností útoku uvedených v tabuľke 3.

$$\wp(\text{Ú}) = \wp(\text{VC}) \wedge \wp(\text{SÚ}) \wedge \wp(\text{PP}) \tag{6}$$

Tabuľka 3 Možná škála vyjadrenie stupňov vierohodnosti (plauzibility) predpokladov útoku

Slovná deskripcia	**Číselná hodnota**
Úplne nevierohodné	0
Takmer nevierohodné	0,1
Veľmi nevierohodné	0,2 – 0,3
Nevierohodné	0,4

Slovná deskripcia	Číselná hodnota
Vierohodné	0,5 -0,6
Veľmi vierohodné	0,7 – 0,8
Takmer vierohodné	0,9
Úplne vierohodné	1

Zdroj: Vlastné spracovanie

Výslednú ($\wp$(Ú)) ohodnotíme podľa vzorca (7).

$$\wp(\text{Ú}) = \min\{\wp(VC), \wp(S\text{Ú})\ \ \wp(PP)\} \tag{7}$$

Vzorec (7) môžeme interpretovať tak, že vierohodnosť útoku na mäkký cieľ bude mať takú hodnotu vierohodnosti, ako je minimálna hodnota vierohodnosti ktoréhokoľvek z jeho predpokladov. Keď minimálna hodnota vierohodnosti predpokladov útoku bude napr. „veľmi nevierohodné“, potom aj vierohodnosť útoku bude, (bez ohľadu na vyššie vierohodnosti ostatných predpokladov) ohodnotená ako „veľmi nevierohodné“.

2.4 Identifikácia taktiky útoku

Pri riešení tejto úlohy hľadáme odpovede na otázku: ako dôjde k útoku, akú taktiku a aké prostriedky útočník použije? Útoky na mäkké ciele mali podobu masovej streľby v školách, komunitných centrách, kinách a koncertoch, v náboženských objektoch, útoky ostrou zbraňou v nákupnom stredisku, na ulici; boli použité vozidlá na útoky boli evidované odpálenia alebo pokus o odpálenie improvizovaných výbušných zariadení na športových podujatiach a iných miestach masových zhromaždení.

Útoky teroristov sú často vykonávané použitím improvizovaných výbušných zariadení (IVZ), z ktorých hlavné typy sú tieto:

- prenášané osobou (IVZ na osobe alebo prenášané v taške),
- vo vozidle (ktoré môžu byť samovražedné alebo nesamovražedné IVZ),
- ručne dodávané alebo IVZ uložené v objekte, resp. uložené na danom priestore (nesamovražedné zariadenia iniciované typicky časovačom alebo diaľkovým ovládaním),
- bezpilotné lietadlá (drony).

Varianty použitia IVZ sú uvedené v tabuľke 4. Hodnota účinku IVZ zodpovedá hmotnosti výbušniny (nálože) uvedenej v tabuľke.

Tabuľka 4 Scenáre teroristických útokov s použitím IVZ.

Typ prostriedku	Spôsob použitia	Hmotnosť nálože (kg)	Účinok na nezodolnené časti /osoby (m)	Maximálny ničivý účinok (m)
Trubková bomba	Vhodenie, Uloženie	2,3	21	259
Opasok	Samovražedný atentátnik	4,5	27	330
Vesta		9	34	415
Kufríková bomba	Uloženie. Dopravenie ako zásielky	23	46	564
Bomba v automobile - stojacom /idúcom	Compact sedan/limuzína	227	98	457
	Sedan	454	122	534
	Combi, malá dodávka	1 814	195	838
	Malý nákl. automobil	4 536	263	1 143
	Veľký nákl. automobil, cisterna	13 608	375	1 982
	Náves		475	2 134

Zdroj: Hofreiter, 2015.

Útočníci v poslednom čase použili aj iné prostriedky, ako sú napríklad vozidlá, strelné zbrane alebo chladné zbrane. Vozidlá boli použité na útok na skupinu ľudí na verejných priestranstvách. Strelné zbrane (pištoľ, automatické pušky a pod.) sa používajú na útoky proti jednotlivcom, ale aj proti veľkým skupinám ľudí, ide o takzvanú „hromadnú streľbu“ (mass shooting). Chladné zbrane (nože, sekery, bajonety atď.) použili útočníci pri útokoch na verejných priestranstvách.

Ak budeme uvažovať o možnosti útoku proti mäkkému cieľu, potom sú možné tieto scenáre (Hofreiter,2015):

- priama akcia – priamy ozbrojený fyzický útok na cieľ uskutočnený ozbrojenými jednotlivcami alebo teroristickými skupinami,
- bombový útok – útok, ktorý je spravidla vykonávaný jednotlivcom alebo malou skupinou s využitím napr. nekonvenčných náloží – IVZ ,
- 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 , v dôsledku čoho môžu byť ohrozené životy ľudí, fungovanie kritickej infraštruktúry apod. Kybernetické útoky sú čoraz viacej zameriavané na radikalizáciu, na šírenie nenávisti medzi náboženskými komunitami, polarizáciu spoločnosti a na vyvolávanie strachu (UN,2022).

Tabuľka 5 Matica morfologickej analýzy taktiky útoku.

Útočník			Vhodný cieľ			Použité prostriedky	Taktika útoku
Typ	Motív	Zámer	Objekt	Priestor	Udalosť		
jednotlivec	Krivda	Zabíjať	Dopravný	Mestské centrum	Masové zhromaždenie	IED, VNS -nesené	Priamy útok
Jednotlivec -terorista	Nenávisť	Šíriť strach	Obchodný	Námestie	Kultúrne podujatie	IED na vozidle	Nepriamy útok
Jednotlivec -extrémista	Pomsta	Donútenie	Školský	Pešia zóna	Športové podujatie	Strelná zbraň	Priamy útok -samovražedný
Extrémistická skupina	Náboženský	Vydieranie	Kultúrny	Bulvár	Náboženské podujatie	Chladná zbraň	CBRN úrok
Teroristická skupina	Politický	Varovanie, výstraha	Športový	Park	Trhy, jarmoky	Automobil	Kybernetický útok
Skupina org. zločinu	Ideologický	Posolstvo	Náboženský	Tržnica		RCHBL	
	Rasový		Administratívny	Iný verejný priestor		Zápalné látky	
	Iný		Zdravotnícky			UAV-dron	
			Objekt KI			Počítačové víry, Hoaxy, dezinformácie	
			Sociálna skupina, obyvateľstvo				

Zdroj: Vlastné spracovanie

Taktika útoku a spôsob útoku bude závisieť od typu útočníka, jeho motívu a zámeru. Tieto faktory ovplyvňujú výber cieľa a prostriedkov útoku proti cieľu. Pomocou matice morfologickej analýzy vyhodnotíme vhodné konfigurácie premenných: pravdepodobný typ útočníka, jeho motívu a zámeru, ako aj možný cieľ útoku, pravdepodobné prostriedky útoku a taktika útoku (pozri tabuľku 5). Týmto spôsobom zároveň vylúčime tie konfigurácie, ktoré nie sú možné (sú nereálne).

2.5 Návrh koncepcie ochrany mäkkých cieľov

Pri riešení ochrany objektov a priestorov, ktoré sú charakterizované ako mäkké ciele, ide o súhrn opatrení a činností na zabránenie udalostí, činov alebo javov, ktoré by mohli ohroziť chránené objekty či priestory, ako aj na zabránenie ohrozenia objektu, osôb, majetku a iných chránených záujmov, ktoré sa nachádzajú v objekte.

Ochranu mäkkých cieľov môžeme vnímať ako súčasť priamej a situačnej stratégie prevencie proti majetkovej kriminalite. Ide o plánovanie a realizáciu takých opatrení, ktoré zmenšia pravdepodobnosť vzniku bezpečnostných hrozieb tým, že zmenia podmienky tých

predpokladov, ktoré umožňujú ich aktiváciu (Hofreiter, 2015). Ide o realizáciu takých opatrení, ktoré :

- bránia alebo zabránia vzniku bezpečnostných ohrození (bezpečnostných incidentov),
- ovplyvňujú výšku „nákladov“ a „zisku“ potenciálneho útočníka,
- zvyšujú riziko odhalenia a zadržania útočníka.

Vo všeobecnosti môžeme charakterizovať tri prístupy k ochrane mäkkých cieľov:

- proaktívny,
- preventívny,
- reaktívny prístup (Hofreiter. Kubíková, 2020).

Proaktívny prístup sa zameriava na odstraňovanie príčin skôr, ako sa môžu objaviť. Musíme sa sústrediť na odstránenie tých príčin, ktoré vytvárajú hrozbu. Spôsobilosť a schopnosť eliminovať príčiny útoku na mäkký cieľ najviac závisí od spravodajských informácií a informácií o bezpečnostnej situácii a jej vývoji.

Preventívne prístupy pozostávajú z vytvorenia vhodného systému na odstrašenie (odradenie) útočníka a/alebo na zabránenie mu v útoku. Využijeme pritom príslušné prvky bezpečnostných systémov, polície a bezpečnostných služieb. Podstatou tejto koncepcie je názor, že príležitosť (Opportunity), cieľ (Target), riziko (Risk), vynaložené úsilie (Effort) a úžitok (Profit) sú činitele, ktoré majú zásadný vplyv na uskutočnenie útoku na mäkký cieľ. Obmedzením príležitosti, sťažením prístupu k cieľu alebo dizajnom prostredia donútime útočníka vyvinúť vyššie úsilie na dosiahnutie cieľa, čím zvýšime riziko odhalenia či znížime očakávaný efekt z útoku. Tým môžeme ovplyvniť rozhodovania útočníka, a zároveň aj znížiť pravdepodobnosť (možnosť, vierohodnosť) napadnutia objektu, čo je vlastne cieľom ochrany. Z hľadiska riešenia bezpečnosti v objektoch a priestoroch môžeme ovplyvňovať predpoklad vytváranie vhodných príležitostí na vykonanie útokov. Zamedzenie vytvorenia vhodnej príležitosti na vykonanie útoku by mal predstavovať súhrn technických, organizačných a režimových opatrení s cieľom znížiť pravdepodobnosť dosiahnutia cieľa útoku, úspechu útoku, zvýšiť riziko pre potenciálneho útočníka.

Možným riešením ochrany mäkkých cieľov je použitie metódy Target Hardening. Spočíva v realizácii opatrení, ktoré dodávajú objektu, chránenému priestoru také fyzikálne vlastnosti, ktoré sťažujú uskutočnenie útoku na chránený objekt či chránený záujem. Tou vlastnosťou je zvýšenie odolnosti objektu, jeho systému ochrany voči pokusom o napadnutie objektu. Prostriedky na zvýšenie odolnosti objektov členíme na :

- prostriedky pasívnej ochrany (mechanické zábranné prostriedky, najmä bariéry),
- aktívne prvky ochrany , najmä kamerové systémy – CCTV,
- systémy kontroly a riadenia vstupu- SKV,

- prvky fyzickej ochrany (polícia, strážna služba, vlastná ochrana),
- režimové opatrenia, zamerané na efektívne uplatňovanie systému ochrany objektov a priestorov mäkkých cieľov.

Žiadne opatrenia nemajú absolútnu účinnosť, musíme vždy počítať aj s možnosťou uskutočnenia útoku. Preto by súčasťou opatrení na zaistenie bezpečnosti v priestoroch s hromadným výskytom osôb malo byť zaistenie akcieschopnosti síl reagovania, aby sa minimalizovali ľudské straty a obete eventuálneho útoku. Reaktívny prístup je založený na reagovaní na udalosti potom, čo sa stali. Podstatou tohto prístupu je zabezpečiť včasnú reakciu na útok s cieľom aktivovať záchranné zložky a poskytnúť potrebnú pomoc obetiam útoku.

Veľmi efektívnou metódou, ktorú možno použiť na plánovanie ochrany mäkkých cieľov, je metóda DDRM (Deter - Detect - React - Mitigate impact) (Hofreiter, Kubíková, 2017). Tento prístup spája všetky tri prístupy – proaktívny, preventívny aj reaktívny. Je to nástroj určený na plánovanie bezpečnostných opatrení určených na ochranu mäkkých cieľov. Po definovaní možných hrozieb, ktoré by mohli objekt ovplyvniť (útočník, taktika útoku atď.), navrhujeme najlepšie opatrenia na odstrašenie, detekciu, reakciu a zmiernenie dopadu. Opatrenia, ktoré sa ukážu ako najefektívnejšie, by mali byť začlenené do celkového bezpečnostného riešenia na ochranu mäkkých cieľov. Konečný návrh by sa mal preskúmať, aby sa zabezpečilo, že poskytuje usmernenie vo všetkých fázach – pred (odstrašiť, odhaliť), počas (reagovať) a po (zmierniť) nastúpení každého z prípadov identifikovaných ako relevantná hrozba.

Projektovanie efektívnej ochrany mäkkých cieľov vyžaduje identifikovať hrozby, ktorým môže byť daný objekt (priestor, udalosť) vystavený. Je to logická požiadavka, lebo ak nevieme, čo sa môže stať, nemôžeme ani vytvoriť efektívny systém ochrany. Uplatnenie toho prístupu znamená zamerať sa na skúmanie príčin javov a udalostí, ktoré vyvolávajú hrozby, alebo môžu ohroziť mäkký cieľ. Využitím kauzálnych vzťahov príčin a následkov, induktívnych i deduktívnych metód môžeme získať prehľad o relevantných hrozbách.

3 DISKUSIA

Návrh ochrany mäkkých cieľov nie je jednoduchý problém. Efektívnosť opatrení na ochranu mäkkých cieľov ovplyvňujú predovšetkým informácie. Môžeme identifikovať potenciálne ciele útokov. Nie vždy však vieme, alebo môžeme predvídať, kto bude útočníkom, kedy k útoku dôjde, ako k útoku dôjde. Prezentovaný prístup je založený na odhade vierohodnosti identifikovaných faktorov a ich vzájomnej závislosti a podmienenosti. Tento prístup poskytuje viac možností na korektnejšie vyjadrenie identifikovaných predpokladov, najmä ak nie sú dostupné relevantné štatistické údaje a vyjadrenie pravdepodobností by nebolo možné, alebo veľmi nepresné. Podrobnejšie určenie

vierohodnosti útoku a taktiky útoku závisí od vyjadrenia optimálnej kombinácie relevantných faktorov a ich prvkov.

Pri posudzovaní podmienok útoku na mäkké ciele a z toho vyplývajúcich požiadaviek na ich ochranu môžeme využiť aj postupy využívané pri posudzovaní bezpečnostných rizík. Kvantifikácia bezpečnostného rizika, vyplývajúceho z hrozby útoku na mäkký cieľ, a následné rozhodnutie o zaobchádzaní s ním, nám poskytuje východisko pre rozhodnutie o potrebe projektovania systému ochrany mäkkého cieľa. Pre posudzovanie a kvantifikáciu bezpečnostného rizika je možné použiť aj tzv. trojprvkový model, ktorý spočíva v hľadaní odpovedí na tri základné otázky:

1. Čo sa môže stať?
2. Aká je pravdepodobnosť, že sa to stane?
3. Ak sa to stane, aké budú následky?

Odpoveďou na prvú otázku je vypracovanie scenárov udalostí, všetkých možných spôsobov, ktorými môže dôjsť k ohrozeniu mäkkého cieľa. Pri tvorbe scenárov udalosti budeme vychádzať z toho, že útočník sa chová racionálne a inteligentne, využíva všetky objektívne dostupné informácie, jeho konanie je uvedomelé a zamerané na dosiahnutie cieľa. Vie, aký postup, aké konanie najlepšie maximalizuje jeho šance na úspech, čo maximalizuje jeho zisk a minimalizuje neúspech.

Pravdepodobnosť útoku vyjadruje predpoklad (šancu), že dôjde k útoku na mäkký cieľ. Pravdepodobnosť úspechu pri útoku ovplyvňuje dostupnosť cieľa, jeho zraniteľnosť a účinnosť použitých prostriedkov (spôsobov) útoku. Pravdepodobnosti môžu byť definované, určené alebo merané objektívne alebo subjektívne a môžu byť vyjadrené kvalitatívne alebo kvantitatívne (Hofreiter, Zvaková,2019).

Následky útoku na mäkký cieľ vyjadrujú rozsah, stupeň pravdepodobných (predpokladaných, možných) škôd, strát či iných negatívnych následkov, ktoré môžu vzniknúť v dôsledku útoku.

Bezpečnostné riziko vyplývajúce u hrozby útoku na mäkký cieľ môžeme vyjadriť nasledujúcim spôsobom:

$$R = P(\text{Ú}) \cdot P(S/\text{Ú}).C \tag{8}$$

kde: P (Ú) je pravdepodobnosť útoku

P (S|Ú) je pravdepodobnosť úspešného útoku,

C sú následky útoku.

Ak výsledkom posúdenia bezpečnostného rizika je, že riziko je neprijateľné, je nutné rozhodnúť o spôsobe zaobchádzania s ním. V prípade ochrany mäkkých cieľov môžeme veľkosť rizika znižovať nasledujúcimi spôsobmi :

- buď eliminujeme (znižujeme) pravdepodobnosť hrozby,
- alebo znižujeme pravdepodobnosť úspešného útoku, teda:
  - zamedzíme potenciálnemu útočníkov v prístupe k objektu ochrany,
  - znížime zraniteľnosť mäkkých cieľov a existujúcich systémov ochrany,
  - alebo zvyšujeme odolnosť cieľa,
- alebo znižujeme veľkosť následkov útoku.

ZÁVER

Z predloženej analýzy vyplývajú tieto závery:

1. Bezpečnosť mäkkého cieľa výsledkom procesov a činností subjektov bezpečnosti, ktoré sú orientované na včasnú identifikáciu, varovanie, zníženie, elimináciu alebo odvrátenie nebezpečenstiev alebo hrozieb, ktoré majú potenciál zničiť alebo výrazne ohroziť životy ľudí, poškodiť duchovné a materiálne statky, spôsobiť výrazné morálne škody, znemožniť alebo obmedziť slobody a rozvoj jednotlivca i sociálnych skupín.
2. Z hľadiska výberu metód riešenia problému ochrany mäkkého cieľa sa javia ako optimálne kvalitatívne metódy, pretože:
   - podmienky a predpoklady vzniku hrozby útoku sú veľmi premenlivé,
   - kvantitatívne vyjadrenie parametrov podmienok a predpokladov útoku je s ohľadom na rôznorodosť podmienok a výrazný vplyv ľudského činiteľa veľmi obtiažne,
   - kvalitatívne metódy nevyžadujú množstvo štatistických údajov, ale využívajú logické väzby medzi predpokladmi útoku,
   - kvalitatívne metódy poskytujú jasnú a zrozumiteľnú deskripciu predpokladov útoku.
3. Ochrana mäkkého cieľa založená na ovplyvňovaní činiteľov, ktoré umožňujú vznik a prejavy hrozby útoku. Zvyšovanie odolnosti a znižovanie zraniteľnosti mäkkých cieľov nie je ľahká úloha a ak im nie je venovaná pozornosť, ak nedosahujú požadované parametre, zvyšuje sa pravdepodobnosť úspešnosti útoku.
4. Ochrana mäkkého cieľa je systematická činnosť na zaistenie jeho bezpečnosti pomocou preventívnych programov a opatrení.
5. Ochrana mäkkých cieľov je možná tam, kde je možná kontrola prístupu.

6. Ochrana mäkkých cieľov je skôr taktický ako technický problém. Okrem realizácie preventívnych opatrení je nevyhnutné vypracovanie postupov a opatrení, ako reagovať na prípadný útok na mäkký cieľ.
7. Pri niektorých útokoch je preventívny prístup nemožný alebo ťažký, najmä keď sa predpokladá:
   - použitie strelných zbraní na väčšiu vzdialenosť,
   - používanie krátkych strelných zbraní alebo chladných zbraní v dave,
   - použitie netradičných nosičov IVZ.
8. Predpokladom účinnej ochrany je znalosť situácie, t. j. mať informácie o bezpečnostnej situácii a prognóze jej vývoja. Osoba alebo inštitúcia zodpovedná za ochranu mäkkých cieľov musí:
   - vedieť, čo vie a vedieť, ako to používať,
   - vedieť, čo nevie, a snažiť sa získať potrebné informácie a znalosti .

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BECK, U. 1986. *Risikogesellschaft. auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp Verlag, , 1986. 396 s. ISBN 978-3-518-11365-3.

Definition of soft target in English. 2017. English Oxford Living Dictionaries. [online]. [cit. 2022-10-6]. Dostupné na internete: < https://lnk.sk/sst3>.

FRIŠTACKÝ,N.- KOLESÁR,M.- KOLENIČKA,J.- HLAVATÝ,J. : *Logické systémy*. Bratislava: Alfa, 1986. s. 592. ISBN 80-05-00414-1.

HESTERMAN, J. 2015. *Soft Target Hardening: Protecting People from Attack*. 4. New York: CRC Press Taylor & Francis Group, 2015. 460.s ISBN 978-1482244212.

HOFREITER,L. 2015. *Manažment ochrany objektov*. Žilina: EDIS – vydavateľstvo Žilinskej univerzity, 2015. 229 s. ISBN: 978-80-554-1164-4.

HOFFREITER,L., - KUBÍKOVÁ, Z. 2017. Ochrana mäkkých cieľov ako problém národnej bezpečnosti. In: *Bezpečné Slovensko a Európska únia* [elektronický zdroj] Košice: Vysoká škola bezpečnostného manažérstva, 2017. s. 145-152. ISBN 978-80-8185-025-7.

HOFREITER,L. – KUBÍKOVÁ, Z. 2020. Theoretical basis of soft target protection In: *Soft target protection: theoretical basis and practical measures.* Dordrecht: Springer Nature, 2020. s. 149-160 . ISBN 978-94-024-1757-9.

HOFREITER, L.- ZVAKOVÁ,Z. 2017. Theoretical aspects of critical infrastructure protection In: *Durability of critical infrastructure, monitoring and testing : proceedings of the ICDCF 2016.* - Singapore: Springer Nature, 2017. S. 139-147. ISBN 978-981-10-3246-2.

HOFREITER, L. – ZVAKOVÁ, Z. 2019. *Teória bezpečnosti*. Kraków: EAS, 2019. 258 s. ISBN 978-83-61645-35-1.

HOFREITER,L. 2019. Využitie morfologickej analýzy pri manažérstve ochrany objektov. In: *Kvantitatívne a kvalitatívne metódy využívané v bezpečnostnej praxi.* Žilina: EDIS - vydavateľské centrum Žilinskej univerzity.2019. s. 32-37. ISBN 978-80-554-1608-3.

JURČÁK, V.-SASARÁK, L. 2019.Analýza pojmu mäkké ciele. In: *Bezpečné Slovensko a Európska únia*. Košice: Vysoká škola bezpečnostného manažérstva, 2019. s. 123-133. ISBN : 978-80-8185-036-3.

KALVACH , Z. et al. 2016. *Základy ochrany měkkých cílů – metodika* [online]. [cit. 2022-10-5]. Praha: Soft Targets Institute. 2016. Dostupné na Internete <https://www.mvcr.cz>.

KARLOS, V.- LARCHER M.-SOLOMOS, G. 2018. *Review on soft target/public space protection guidance*. Luxembourg: Publications Office of the European Union, 2018 .25 s. ISBN 978-92-79-79907-5, doi:10.2760/553545.

National Guidelines for the Protection of Places Of Mass Gathering from Terrorism. 2011. [online].[cit.2022-10-5].Dostupné na Internete: <https://www.safeguarding.qld.gov.au>.

POPPER, M.- KELEMEN, J. 1989. Expertné systémy. Bratislava: ALFA, 1989. 358 s. ISBN 80-05-00051-0

US Department of Homeland Security 2018. *Soft Targets and Crowded Places. Security Plan Overview* [online]. [cit. 2022-09-22]. Dostupné na Internete:<https://www.cisa.gov/sites>.

UN 2022: *Protecting vulnerable targets from terrorist attacks. Good Practices Guide.* [on line]. [cit. 2022-9-23]. Dostupné na internete: < https://lnk.sk/krs6>.

What is the Soft – Target and Hard – Target principle ? Travel Security Handbook. [online]. [cit. 2022-9-23]. Dostupné na Internete < http://www.travel-security-handbook.com>.

prof. Ing. Ladislav HOFREITER. CSc.

Katedra bezpečnosti a obrany

Akadémia ozbrojených síl generála Milana Rastislava Štefánika

Demänová 393, 031 01 Liptovský Mikuláš

+421 960 422 619

ladislav.hofreiter@aos.sk