Škola digitálnej bezpečnosti

INTEGRÁCIA DIGITÁLNYCH TECHNOLÓGIÍ DO RÁMCA OCHRANY MÄKKÝCH CIEĽOV A BEZPEČNOSTNÉHO VZDELÁVANIA SÚČASNOSTI

Spolufinancované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu
Škola digitálnej bezpečnosti č. 09I05-03-V04-00043

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD PODPREDSEDU VLÁDY SLOVENSKEJ REPUBLIKY PRE PLÁN OBNOVY A ZNALOSTNÚ EKONOMIKU
VAIA

Obsah

Úvod ... 4
1 Bezpečnosť ako základný spoločenský fenomén ... 5
2 Charakteristika mäkkých cieľov ... 6
3 Bezpečnostné riziká, hrozby a príčiny útokov ... 7
3.1 Formy útokov na mäkké ciele ... 7
3.2 Analýza rizík pri ochrane mäkkých cieľov a jej jednotlivé fázy ... 8
3.2.1 Podstata analýzy rizík ... 9
3.2.2 Fáza identifikácie aktív ... 9
3.2.3 Fáza identifikácie hrozieb ... 10
3.2.4 Fáza identifikácie zraniteľností ... 11
3.2.5 Stanovenie pravdepodobnosti vzniku rizika ... 12
3.2.6 Stanovenie následkov rizika ... 12
3.2.7 Hodnotenie rizík ... 13
3.2.8 Návrh bezpečnostných opatrení ... 14
3.2.9 Implementácia opatrení ... 15
3.2.10 Monitorovanie a preskúmavanie rizík ... 15
4 Systém ochrany mäkkých cieľov ... 17
5 Moderné technológie ochrany ... 19
5.1 Analýza správania osôb ... 19
5.2 Pokročilé technológie rozpoznávania tváre v systémoch ochrany mäkkých cieľov ... 20
5.3 Lokomočná identifikácia ako biometrická technológia budúcnosti ... 23
5.3.1 Výhody a obmedzenia lokomočnej identifikácie ... 24
5.4 Integrácia biometrických systémov do inteligentných bezpečnostných platforiem ... 25
6 Technológia počítania ľudí a jej využitie pri ochrane mäkkých cieľov ... 26
6.1 Počítanie ľudí ako súčasť inteligentných bezpečnostných systémov ... 26
6.2 Princíp fungovania technológie počítania ľudí ... 27
6.3 Využitie umelej inteligencie pri počítaní ľudí ... 27

6.4 Heat mapy a analýza pohybu osôb 28
6.5 Využitie počítania osôb pri ochrane mäkkých cieľov 28
6.6 Integrácia s ostatnými bezpečnostnými systémami 29
6.7 Budúci vývoj technológie 30
7 Technológie rozpoznávania záujmových položiek v ochrane mäkkých cieľov 31
7.1 Rozpoznávanie záujmových položiek ako súčasť moderných bezpečnostných systémov 31
7.2 Princíp fungovania systémov rozpoznávania predmetov 32
7.3 Detekcia strelných zbraní 32
7.4 Detekcia chladných zbraní 33
7.5 Detekcia opustenej batožiny 34
7.6 Rozpoznávanie výbušných systémov 34
7.7 Rozpoznávanie ochranných a maskovacích prostriedkov 35
7.8 Integrácia s analýzou správania osôb 35
7.9 Budúcnosť rozpoznávania záujmových položiek 36
8 Využitie simulácií a virtualizácie v bezpečnostnom vzdelávaní zameranom na ochranu mäkkých cieľov 37
8.1 Význam simulácií v bezpečnostnom vzdelávaní 38
8.2 Virtualizácia ako nástroj moderného vzdelávania 38
8.3 Virtuálne modelovanie mäkkých cieľov 39
8.4 Simulácia útoku aktívneho útočníka 40
8.5 Simulácia evakuácie osôb 41
8.6 Simulácia bombovej hrozby 42
8.7 Simulácia správania davu 42
8.8 Integrácia umelej inteligencie do simulačných systémov 43
8.9 Virtuálne strelnice a taktické simulátory 44
8.10 Ekonomické a organizačné prínosy simulácií 44
Záver 46

Úvod

Bezpečnosť patrí medzi základné podmienky existencie a rozvoja modernej spoločnosti. Dynamický rozvoj bezpečnostného prostredia, rastúca globalizácia, technologický pokrok a meniaci sa charakter hrozieb spôsobujú, že ochrana osôb a majetku nadobúda stále väčší význam. Mimoriadna pozornosť sa v posledných desaťročiach venuje ochrane takzvaných mäkkých cieľov, ktoré predstavujú špecifickú kategóriu objektov a priestorov charakteristických vysokou koncentráciou osôb a súčasne nižšou úrovňou bezpečnostnej ochrany. Práve tieto charakteristiky spôsobujú, že sa mäkké ciele stávajú atraktívnymi objektmi útokov organizovaných skupín, teroristov, extrémistov alebo jednotlivcov konajúcich z rôznych ideologických, náboženských či osobných pohnútok.

Problematika ochrany mäkkých cieľov sa postupne stáva jednou z hlavných oblastí moderného bezpečnostného manažmentu. Účinná ochrana si vyžaduje kombináciu organizačných, technických, personálnych a preventívnych opatrení. Popri tradičných formách ochrany sa čoraz výraznejšie presadzujú aj moderné informačné technológie, umelá inteligencia a pokročilé systémy videoanalytiky.

1 Bezpečnosť ako základný spoločenský fenomén

Bezpečnosť predstavuje stav, v ktorom sú minimalizované alebo eliminované hrozby ohrozujúce existenciu jednotlivcov, organizácií alebo spoločnosti ako celku. V bezpečnostnej teórii sa často spája s pojmami chránený záujem, nebezpečenstvo, hrozba a riziko. Chráneným záujmom sú všetky hodnoty, ktoré majú byť zachované a chránené pred poškodením, zničením alebo odcudzením. Medzi najvýznamnejšie chránené záujmy patria život a zdravie osôb, majetok, kultúrne dedičstvo, informačné zdroje a verejný poriadok.

Nebezpečenstvo predstavuje možnosť vzniku negatívnych javov, ktoré môžu narušiť fungovanie systému. Hrozba je konkrétny prejav nebezpečenstva smerujúci voči určitému objektu alebo subjektu. Riziko predstavuje kombináciu pravdepodobnosti vzniku nežiadúcej udalosti a závažnosti jej následkov. V modernom chápaní bezpečnosti sa kladie dôraz na riadenie rizík, ktoré umožňuje identifikovať potenciálne hrozby a prijímať primerané opatrenia na ich minimalizáciu.

Bezpečnostné prostredie 21. storočia je charakteristické vysokou mierou komplexnosti. Tradičné bezpečnostné hrozby sú dopĺňané novými fenoménmi, medzi ktoré patria medzinárodný terorizmus, organizovaný zločin, kybernetické hrozby, hybridné konflikty a extrémizmus. Význam bezpečnosti preto neustále rastie a stáva sa integrálnou súčasťou fungovania verejných aj súkromných organizácií.

2 Charakteristika mäkkých cieľov

Pojem mäkký cieľ označuje objekt, priestor alebo udalosť, kde sa nachádza väčší počet osôb a zároveň neexistuje primeraná úroveň ochrany voči potenciálnym útokom. Medzi typické mäkké ciele patria školy, univerzity, nemocnice, obchodné centrá, letiská, železničné stanice, trhoviská, kultúrne podujatia, športové podujatia, koncerty alebo verejné zhromaždenia.

Na rozdiel od tvrdých cieľov, ako sú vojenské objekty, väznice, bankové inštitúcie alebo vládne budovy, sú mäkké ciele vo väčšine prípadov navrhnuté tak, aby boli ľahko dostupné verejnosti. Táto otvorenosť je síce dôležitá z hľadiska ich spoločenskej funkcie, avšak zároveň predstavuje významný bezpečnostný problém.

Zraniteľnosť mäkkých cieľov vyplýva najmä z vysokej koncentrácie osôb, zložitej kontroly vstupov, obmedzených možností fyzickej ochrany a často aj z nedostatočnej pripravenosti na riešenie krízových situácií. Úspešný útok na mäkký cieľ môže mať rozsiahle materiálne škody, veľký počet obetí, ale aj výrazný psychologický dopad na spoločnosť.

3 Bezpečnostné riziká, hrozby a príčiny útokov

Príčiny útokov na mäkké ciele sú rôznorodé. Medzi najvýznamnejšie patrí terorizmus, ktorý využíva útoky proti civilistom ako prostriedok na dosiahnutie politických, náboženských alebo ideologických cieľov. Významným faktorom sú tiež prejavy rasizmu, xenofóbie, nacionalizmu, antisemitizmu a iných foriem extrémizmu.

Súčasná bezpečnostná situácia je ovplyvnená aj medzinárodným organizovaným zločinom, nelegálnou migráciou a rastúcou radikalizáciou jednotlivcov. Moderné technológie a sociálne siete umožňujú šírenie extrémistických ideológií a zvyšujú možnosti náboru potenciálnych páchateľov.

Osobitnú kategóriu predstavujú takzvaní osamelí útočníci, ktorí konajú individuálne bez priameho napojenia na teroristické organizácie. Ich identifikácia a odhalenie bývajú značne komplikované, pretože často nevykazujú typické znaky organizovanej prípravy útoku.

3.1 Formy útokov na mäkké ciele

Spektrum možných útokov je mimoriadne široké. Najčastejšie ide o útoky realizované pomocou chladných zbraní alebo strelných zbraní. Významné riziko predstavujú aj improvizované výbušné systémy a útoky realizované samovražednými páchateľmi.

Popri konvenčných útokoch existujú aj menej časté, ale potenciálne veľmi nebezpečné formy útokov, medzi ktoré patria chemické,

biologické alebo radiačné útoky (CBRNE). Ich spoločným znakom je schopnosť zasiahnuť veľký počet osôb a vyvolať rozsiahle spoločenské následky.

Moderné bezpečnostné analýzy upozorňujú aj na rastúci význam hybridných útokov kombinujúcich fyzické násilie, kybernetické útoky a informačné operácie. Tieto útoky sú často koordinované a ich cieľom je maximalizovať psychologický efekt a destabilizáciu spoločnosti.

3.2 Analýza rizík pri ochrane mäkkých cieľov a jej jednotlivé fázy

Analýza rizík predstavuje jeden zo základných nástrojov bezpečnostného manažmentu a tvorí východisko pre plánovanie ochrany mäkkých cieľov. Bez dôkladnej analýzy rizík nie je možné efektívne navrhovať bezpečnostné opatrenia, určovať priority ochrany ani racionálne využívať dostupné zdroje. V podmienkach ochrany mäkkých cieľov nadobúda analýza rizík mimoriadny význam, pretože tieto objekty sa vyznačujú vysokou koncentráciou osôb, otvorenosťou voči verejnosti a relatívne nízkou úrovňou ochrany.

Pod pojmom riziko sa rozumie kombinácia pravdepodobnosti vzniku nežiaducej udalosti a závažnosti jej následkov. Cieľom analýzy rizík je identifikovať možné hrozby, určiť ich dopad na organizáciu a navrhnúť opatrenia na elimináciu alebo minimalizáciu ich účinkov.

3.2.1 Podstata analýzy rizík

Analýza rizík predstavuje systematický proces zisťovania, hodnotenia a riadenia bezpečnostných rizík. Ide o nepretržitý proces, ktorý musí reagovať na meniace sa podmienky bezpečnostného prostredia, technologický rozvoj a nové druhy hrozieb.

Výsledkom analýzy rizík je získanie odpovedí na základné otázky:

→ Čo je potrebné chrániť?

→ Pred čím je potrebné chrániť?

→ Aká je pravdepodobnosť vzniku hrozby?

→ Aké môžu byť následky incidentu?

→ Aké opatrenia je potrebné prijať?

Pri ochrane mäkkých cieľov môže byť predmetom ochrany život a zdravie osôb, majetok, technologické zariadenia, informačné systémy, kultúrne hodnoty alebo dobré meno organizácie.

3.2.2 Fáza identifikácie aktív

Prvým krokom analýzy rizík je identifikácia aktív. Aktívom sa rozumie všetko, čo má pre organizáciu určitú hodnotu a čo môže byť predmetom ochrany.

V podmienkach mäkkých cieľov možno za aktíva považovať:

- návštevníkov objektu,
- zamestnancov,
- budovy a priestory,
- technické zariadenia,

- informačné systémy,
- finančné prostriedky,
- dokumentáciu,
- kultúrne a historické hodnoty,
- reputáciu organizácie.

Práve správna identifikácia aktív predstavuje základ efektívnej ochrany. Ak nie je jasne definované, čo je predmetom ochrany, nie je možné korektne posudzovať hrozby a riziká.

3.2.3 Fáza identifikácie hrozieb

Po identifikácii aktív nasleduje identifikácia možných hrozieb. Hrozba predstavuje potenciálnu príčinu nežiadúcej udalosti schopnej spôsobiť škodu alebo narušenie fungovania organizácie.

Pri ochrane mäkkých cieľov možno identifikovať niekoľko základných skupín hrozieb:

Úmyselné hrozby - Ide o hrozby vyvolané úmyselnou činnosťou človeka:

- terorizmus,
- aktívny útočník,
- vandalizmus,
- krádeže,
- sabotáže,
- organizovaný zločin,
- kybernetické útoky,
- výhražné správy,

- bombové hrozby.

Neúmyselné hrozby - Vznikajú bez priameho úmyslu poškodiť organizáciu:

- ľudské chyby,
- technické poruchy,
- chyby obsluhy,
- zlyhanie bezpečnostných systémov,
- výpadok elektrickej energie.

Prírodné hrozby - Patria sem:

- povodne,
- víchrice,
- požiare,
- zemetrasenia,
- extrémne klimatické javy.

Identifikácia hrozieb musí byť pravidelne aktualizovaná, pretože bezpečnostné prostredie sa neustále mení.

3.2.4 Fáza identifikácie zraniteľností

Zraniteľnosť predstavuje slabé miesto systému, ktoré môže byť zneužité hrozbou.

Pri ochrane mäkkých cieľov môžu byť zraniteľnosťou:

- voľný vstup verejnosti,

- chýbajúce kontroly vstupov,
- nedostatočné kamerové pokrytie,
- absencia fyzickej ochrany,
- nevyhovujúce evakuačné trasy,
- nedostatočné školenie personálu,
- zastarané technické zabezpečenie,
- nevhodné organizačné postupy.

Práve kombinácia hrozby a zraniteľnosti vytvára predpoklad vzniku bezpečnostného incidentu.

3.2.5 Stanovenie pravdepodobnosti vzniku rizika

Po identifikovaní hrozieb a zraniteľností sa určuje pravdepodobnosť ich výskytu. Pravdepodobnosť možno hodnotiť:

- Veľmi nízka - Výskyt je nepravdepodobný alebo výnimočný.
- Nízka - Hrozba sa môže vyskytnúť iba ojedinele.
- Stredná - Hrozba sa vyskytuje pravidelne.
- Vysoká - Pravdepodobnosť výskytu je významná.
- Veľmi vysoká - Výskyt je takmer istý alebo veľmi častý.

Pri hodnotení sa využívajú historické údaje, štatistiky kriminality, spravodajské informácie a skúsenosti odborníkov.

3.2.6 Stanovenie následkov rizika

Ďalšou fázou je posúdenie následkov jednotlivých rizík. Hodnotia sa najmä:

- straty na životoch,
- zranenia osôb,
- materiálne škody,
- finančné straty,
- prevádzkové škody,
- psychologické následky,
- poškodenie dobrého mena organizácie.

Pri ochrane mäkkých cieľov sú najzávažnejšími následkami predovšetkým straty na ľudských životoch a masové zranenia. Následky možno kategorizovať ako:

- zanedbateľné,
- malé,
- stredné,
- závažné,
- katastrofické.

3.2.7 Hodnotenie rizík

Po určení pravdepodobnosti a následkov sa vykonáva samotné hodnotenie rizík. Najčastejšie sa využíva vzťah:

Riziko = Pravdepodobnosť × Následok

Výsledky sa spravidla zapisujú do rizikovej matice.

Pravdepodobnosť	Dopad	Úroveň rizika
Nízka	Malý	Akceptovateľné
Stredná	Stredný	Monitorované
Vysoká	Veľký	Neprijateľné
Veľmi vysoká	Katastrofický	Kritické

Riziková matica umožňuje rýchlo identifikovať oblasti vyžadujúce okamžité bezpečnostné opatrenia.

3.2.8 Návrh bezpečnostných opatrení

Po identifikácii významných rizík nasleduje návrh bezpečnostných opatrení.

a) Organizačné opatrenia
   - ✓ bezpečnostné smernice,
   - ✓ kontrola vstupov,
   - ✓ režimové opatrenia,
   - ✓ krízové plány,
   - ✓ evakuačné plány.

b) Personálne opatrenia
   - ✓ školenia zamestnancov,
   - ✓ odborná príprava SBS,
   - ✓ nácvik krízových situácií,
   - ✓ simulačné cvičenia.

c) Technické opatrenia
   - ✓ CCTV systémy,

- ✓ elektronické zabezpečenie,
- ✓ detektory kovov,
- ✓ systémy kontroly vstupu,
- ✓ integrované bezpečnostné systémy.

d) Fyzické opatrenia

- ✓ fyzická ochrana,
- ✓ ploty,
- ✓ bezpečnostné dvere,
- ✓ turnikety,
- ✓ bezpečnostné zóny.

3.2.9 Implementácia opatrení

Po schválení návrhov nasleduje ich realizácia. V tejto fáze dochádza k:

- ✓ nákupu technológií,
- ✓ inštalácii systémov,
- ✓ vytvoreniu dokumentácie,
- ✓ školeniu personálu,
- ✓ overeniu funkčnosti opatrení.

Dôležitou súčasťou implementácie je kontrola, či navrhované riešenia skutočne znižujú analyzované riziká.

3.2.10 Monitorovanie a preskúmavanie rizík

Analýza rizík nekončí implementáciou opatrení. Riziká sa neustále menia a preto je potrebné ich pravidelne monitorovať.

Monitorovanie zahŕňa:

- ✓ bezpečnostné audity,
- ✓ kontroly objektov,
- ✓ hodnotenie incidentov,
- ✓ preverovanie účinnosti opatrení,
- ✓ aktualizáciu rizikových analýz.

Významnú úlohu zohrávajú aj moderné analytické nástroje využívajúce umelú inteligenciu, ktoré dokážu priebežne vyhodnocovať bezpečnostnú situáciu a upozorňovať na vznikajúce riziká.

Analýza rizík predstavuje základný pilier ochrany mäkkých cieľov. Umožňuje systematicky identifikovať aktíva, hrozby a zraniteľnosti, hodnotiť pravdepodobnosť vzniku incidentov a ich možné následky. Správne vykonaná analýza rizík poskytuje manažérom objektívny podklad pre rozhodovanie o bezpečnostných opatreniach a umožňuje efektívne využívať dostupné zdroje. V súčasnom dynamickom bezpečnostnom prostredí sa stáva nevyhnutným nástrojom pre zabezpečenie ochrany života, zdravia a majetku v prostredí mäkkých cieľov.

4 Systém ochrany mäkkých cieľov

Účinná ochrana mäkkých cieľov je založená na princípe viacvrstvovej ochrany. Základ tvoria štyri hlavné skupiny ochranných opatrení: fyzická ochrana, mechanická ochrana, režimová ochrana a technická ochrana.

- Fyzická ochrana predstavuje priamu prítomnosť bezpečnostných pracovníkov alebo iných osôb vykonávajúcich dohľad nad chráneným priestorom. Ich úlohou je monitorovať situáciu, kontrolovať vstupy a reagovať na vzniknuté incidenty.
- Mechanická ochrana zahŕňa využívanie bezpečnostných dverí, zámkov, mreží, turniketov, bezpečnostných skiel a ďalších mechanických bariér. Tieto prvky slúžia na obmedzenie alebo spomalenie neoprávneného vstupu do chráneného priestoru.
- Režimová ochrana pozostáva zo súboru organizačných a administratívnych opatrení. Zahŕňa kontrolu vstupov, evidenciu návštevníkov, bezpečnostné smernice, evakuačné plány a pravidelné školenia zamestnancov.
- Technická ochrana využíva elektronické zabezpečovacie systémy, kamerové systémy, požiarnu signalizáciu, systémy kontroly vstupu a ďalšie technologické prostriedky určené na detekciu a signalizáciu bezpečnostných incidentov.

Priestorové úrovne ochrany

Moderné bezpečnostné systémy využívajú niekoľko úrovní ochrany.

- Obvodová ochrana zabezpečuje monitorovanie okolia objektu a slúži na včasnú identifikáciu potenciálneho narušiteľa.
- Plášťová ochrana je orientovaná na zabezpečenie okien, dverí a ďalších vstupných otvorov objektu.
- Priestorová ochrana monitoruje vnútorné priestory a umožňuje identifikovať neoprávnený pohyb osôb.
- Predmetová ochrana je zameraná na ochranu konkrétnych hodnôt alebo predmetov nachádzajúcich sa v objekte.

Výhodou viacúrovňového systému – integrovaného bezpečnostného systému je vytváranie postupných bezpečnostných bariér, ktoré významne sťažujú úspešnú realizáciu útoku.

5 Moderné technológie ochrany

V posledných rokoch zaznamenávame prudký rozvoj moderných bezpečnostných technológií. Významnú úlohu zohrávajú integrované bezpečnostné systémy prepájajúce viaceré druhy ochrany do jedného riadiaceho celku. Moderné detektory umožňujú identifikovať kovové predmety, výbušniny alebo iné nebezpečné látky.

Najvýznamnejší pokrok však predstavuje nasadenie umelej inteligencie v kamerových systémoch. Tieto systémy dokážu automaticky vyhodnocovať obrazové informácie, identifikovať osoby, rozpoznávať podozrivé situácie a generovať upozornenia pre operátorov bezpečnostných centier.

5.1 Analýza správania osôb

Moderné videoanalytické systémy umožňujú monitorovať nielen identitu osôb, ale aj ich správanie. Analyzované môžu byť pohybové vzorce, interakcie medzi osobami alebo výskyt neštandardných situácií.

Systémy sú schopné rozpoznávať konflikty, pády osôb, beh, plazenie, nosenie nebezpečných predmetov alebo prítomnosť zbraní. Vďaka algoritmom umelej inteligencie môžu tieto systémy fungovať v reálnom čase a poskytovať okamžité upozornenia operátorom.

Takéto riešenia významne zvyšujú efektivitu preventívnych opatrení a umožňujú rýchlejší zásah bezpečnostných zložiek.

Počítanie ľudí predstavuje moderný nástroj určený na monitorovanie počtu a pohybu osôb v určitom priestore. Táto technológia nachádza široké využitie pri organizácii verejných podujatí, v doprave, obchodných centrách a na ďalších miestach s vysokou koncentráciou ľudí.

Systémy dokážu vytvárať takzvané heat mapy, ktoré zobrazujú intenzitu pohybu osôb v jednotlivých častiach priestoru. Takto získané údaje umožňujú identifikovať kritické miesta, optimalizovať organizáciu priestoru a znižovať riziko vzniku nebezpečných situácií.

5.2 Pokročilé technológie rozpoznávania tváre v systémoch ochrany mäkkých cieľov

Rozpoznávanie tváre predstavuje jednu z najvýznamnejších biometrických technológií využívaných v súčasných bezpečnostných systémoch. Jej význam neustále rastie predovšetkým v oblasti ochrany mäkkých cieľov, kde je potrebné monitorovať veľký počet osôb bez obmedzovania ich pohybu. Moderné systémy rozpoznávania tváre využívajú pokročilé algoritmy strojového učenia a hlbokých neurónových sietí, ktoré umožňujú identifikovať osoby s vysokou mierou presnosti aj vo veľmi náročných podmienkach.

Základom fungovania každého systému rozpoznávania tváre je detekcia ľudskej tváre v obraze. Ide o proces, pri ktorom softvér analyzuje každú snímku videozáznamu a vyhľadáva objekty vykazujúce charakteristické znaky ľudskej tváre. Súčasné algoritmy dokážu rozpoznávať tváre v

rôznych svetelných podmienkach, pri čiastočnom zakrytí tváre alebo pri rôznych uhloch natočenia hlavy. Významnou výhodou je schopnosť analyzovať záznam v reálnom čase, pričom identifikácia môže prebiehať bez vedomia monitorovanej osoby.

Po detekcii tváre nasleduje proces lokalizácie charakteristických bodov. Systém identifikuje oči, nos, ústa, lícne kosti, líniu čeľuste a ďalšie anatomické prvky. Tieto body predstavujú základ biometrického modelu tváre. Ich vzájomné vzdialenosti, uhly a proporcie vytvárajú jedinečný matematický profil, ktorý je pre každého jednotlivca charakteristický.

Významným krokom je extrakcia biometrických charakteristík. Počas tejto fázy sa z obrazu získavajú údaje opisujúce tvar tváre, vzdialenosť medzi očami, proporcie nosa, polohu úst a množstvo ďalších parametrov. Moderné systémy dokážu pracovať s desiatkami až stovkami biometrických charakteristík naraz, čo výrazne zvyšuje spoľahlivosť identifikácie.

Nasleduje vytvorenie digitálneho biometrického modelu. Tento model neobsahuje fotografiu osoby v klasickom zmysle slova, ale sériu matematických údajov reprezentujúcich jedinečné znaky tváre. Výhodou takéhoto prístupu je rýchle vyhľadávanie v rozsiahlych databázach obsahujúcich tisíce alebo milióny profilov.

Pri samotnom porovnávaní systém využíva algoritmy umelej inteligencie a neurónové siete. Tieto algoritmy analyzujú mieru podobnosti medzi aktuálne získaným modelom a profilmi uloženými v databáze.

Výsledkom je pravdepodobnostná zhoda, na základe ktorej systém rozhodne o identifikácii alebo verifikácii osoby.

Moderné bezpečnostné systémy už dnes využívajú trojrozmerné modelovanie tváre. Na rozdiel od starších dvojrozmerných systémov dokáže 3D rozpoznávanie pracovať aj pri zmenách osvetlenia alebo natočenia hlavy. Výrazne sa tak znižuje počet nesprávnych identifikácií a zvyšuje spoľahlivosť celého riešenia.

Pri ochrane mäkkých cieľov poskytujú systémy rozpoznávania tváre množstvo výhod. Umožňujú automatické vyhľadávanie hľadaných osôb, identifikáciu osôb nachádzajúcich sa na bezpečnostných zoznamoch a monitorovanie pohybu návštevníkov vo veľkých priestoroch.

Významným prínosom je možnosť okamžitého upozornenia operátora na výskyt rizikovej osoby. V prípade športových podujatí, koncertov alebo verejných zhromaždení môže systém identifikovať osobu ešte pred vstupom do objektu. Tým sa výrazne skracuje čas potrebný na reakciu bezpečnostných zložiek.

Rozpoznávanie tváre nachádza uplatnenie aj pri vyšetrovaní incidentov. Archivované videozáznamy je možné spätne analyzovať a vyhľadávať konkrétne osoby v rozsiahlych databázach záznamov. Takýto postup výrazne urýchľuje vyšetrovanie a pomáha pri dokumentovaní trestnej činnosti.

5.3 Lokomočná identifikácia ako biometrická technológia budúcnosti

Lokomočná identifikácia predstavuje relatívne novú oblasť biometrie založenú na analýze pohybových charakteristík človeka. Každý človek disponuje jedinečným spôsobom chôdze, ktorý je podmienený anatomickou stavbou tela, rozložením svalovej hmoty, dĺžkou končatín a pohybovými návykmi. Tieto charakteristiky vytvárajú špecifický pohybový podpis jednotlivca.

Na rozdiel od rozpoznávania tváre nevyžaduje lokomočná identifikácia detailný pohľad na tvár osoby. Osoba môže byť otočená chrbtom ku kamere alebo môže mať tvár zakrytú. Systém dokáže napriek tomu vykonať identifikáciu na základe analýzy pohybu.

Prvým krokom identifikácie je digitalizácia obrazu. Kamerový systém zaznamenáva pohyb osoby a vytvára sériu digitálnych snímok. Následne dochádza k segmentácii postavy od pozadia, čo umožňuje analyzovať výlučne pohyb sledovaného subjektu.

Po oddelení objektu od pozadia začína analýza pohybových vzorcov. Softvér monitoruje pohyb jednotlivých častí tela, najmä hlavy, trupu, rúk a nôh. Hodnotí sa dĺžka kroku, frekvencia krokov, rýchlosť pohybu, amplitúda pohybov končatín a ďalšie biomechanické parametre.

Nasleduje extrakcia biometrických údajov. Softvér vytvára matematický model pohybu, ktorý predstavuje jedinečný biometrický vzor osoby.

Tento vzor je následne ukladaný do databázy alebo porovnávaný s existujúcimi záznamami.

Dôležitou súčasťou procesu je klasifikácia subjektov. Po vytvorení biometrického modelu systém vykonáva porovnávanie s databázou osôb a určuje mieru zhody. Ak systém nájde dostatočne podobný profil, dôjde k identifikácii osoby.

5.3.1 Výhody a obmedzenia lokomočnej identifikácie

Významnou výhodou lokomočnej identifikácie je možnosť identifikácie na veľkú vzdialenosť. Zatiaľ čo rozpoznávanie tváre si často vyžaduje dostatočné rozlíšenie obrazu, lokomočné systémy môžu fungovať aj pri nižšej kvalite záznamu.

Ďalšou výhodou je vysoká odolnosť voči maskovaniu. Zakrytie tváre, použitie slnečných okuliarov alebo pokrývky hlavy neovplyvňuje základné pohybové charakteristiky človeka. Z tohto dôvodu je lokomočná identifikácia považovaná za vhodný doplnok portrétnej identifikácie.

Medzi obmedzenia patrí zmena pohybového prejavu spôsobená zdravotným stavom, únavou, zranením alebo prenášaním bremena. Tieto faktory môžu dočasne meniť charakteristiky pohybu a znižovať presnosť identifikácie. Napriek tomu vývoj algoritmov umelej inteligencie vedie k neustálemu zvyšovaniu spoľahlivosti tejto technológie.

5.4 Integrácia biometrických systémov do inteligentných bezpečnostných platforiem

Budúcnosť ochrany mäkkých cieľov spočíva v prepájaní jednotlivých identifikačných technológií do jednotných integrovaných bezpečnostných systémov. Moderné platformy dokážu súčasne využívať rozpoznávanie tváre, lokomočnú identifikáciu, analýzu správania osôb, rozpoznávanie objektov a počítanie ľudí.

Výstupy z jednotlivých subsystémov sú následne vyhodnocované umelou inteligenciou, ktorá dokáže určiť mieru rizika sledovanej osoby alebo situácie. Tým vzniká komplexný bezpečnostný nástroj schopný nielen identifikovať osoby, ale aj predvídať potenciálne nebezpečné správanie.

6 Technológia počítania ľudí a jej využitie pri ochrane mäkkých cieľov

6.1 Počítanie ľudí ako súčasť inteligentných bezpečnostných systémov

Technológia počítania ľudí (People Counting) predstavuje moderný nástroj videoanalytiky, ktorý umožňuje automatické monitorovanie počtu osôb nachádzajúcich sa v definovanom priestore. V súčasnosti patrí medzi významné súčasti integrovaných bezpečnostných systémov a nachádza široké uplatnenie pri ochrane mäkkých cieľov, akými sú nákupné centrá, letiská, železničné stanice, športové štadióny, školy, nemocnice, kultúrne podujatia či verejné zhromaždenia. Podstatou technológie je získavanie presných údajov o pohybe a koncentrácii osôb v priestore prostredníctvom kamerových systémov a špecializovaných analytických algoritmov.

Rozvoj výpočtovej techniky, strojového učenia a umelej inteligencie umožnil transformáciu tradičných kamerových systémov z pasívnych monitorovacích nástrojov na inteligentné analytické platformy. Moderné systémy už neslúžia len na zaznamenávanie obrazu, ale dokážu samostatne vyhodnocovať pohyb osôb, určovať ich počet, analyzovať smer pohybu a identifikovať vznikajúce rizikové situácie.

6.2 Princíp fungovania technológie počítania ľudí

Počítanie ľudí je založené na analýze obrazových dát získaných z kamerových systémov. Proces začína získaním videozáznamu, ktorý je následne spracovávaný analytickým softvérom. Prvým krokom je detekcia objektov predstavujúcich osoby. Softvér využíva algoritmy počítačového videnia na rozpoznanie ľudskej postavy bez ohľadu na osvetlenie, hustotu davu alebo rýchlosť pohybu.

Po identifikácii osôb systém sleduje ich pohyb v priestore. Každému objektu je priradený jedinečný identifikátor, ktorý umožňuje jeho sledovanie v čase. Vďaka tomu dokáže systém rozlišovať medzi vstupom a výstupom osoby, monitorovať smer pohybu a zabrániť viacnásobnému započítaniu tej istej osoby.

Dôležitou súčasťou technológie je vytváranie virtuálnych detekčných línií alebo zón. Pri prekročení definovanej hranice systém automaticky zaznamená pohyb osoby a aktualizuje štatistické údaje. Takýmto spôsobom možno získať presné informácie o počte vstupov, výstupov a aktuálnom počte osôb v priestore.

6.3 Využitie umelej inteligencie pri počítaní ľudí

Najmodernejšie systémy využívajú neurónové siete a algoritmy hlbokého učenia. Tieto technológie dokážu rozlišovať osoby od iných objektov, analyzovať správanie davov a minimalizovať chyby spôsobené prekrývaním osôb alebo zložitými svetelnými podmienkami.

Umelá inteligencia zároveň umožňuje predikciu pohybu osôb a automatické identifikovanie potenciálne nebezpečných situácií. Ak systém zaznamená nadmernú koncentráciu ľudí, vznik tlačenice alebo neobvyklý pohyb davu, môže automaticky upozorniť operátora bezpečnostného centra. Takáto funkcionalita významne prispieva k prevencii incidentov a zvyšovaniu bezpečnosti verejných priestorov.

6.4 Heat mapy a analýza pohybu osôb

Jedným z najvýznamnejších výstupov technológie počítania ľudí sú takzvané tepelné mapy (Heat Maps). Ide o grafické zobrazenie intenzity pohybu osôb v monitorovanom priestore. Farebná škála zobrazuje oblasti s najvyššou a najnižšou koncentráciou osôb, čím poskytuje cenné informácie o využívaní priestoru.

Heat mapy umožňujú identifikovať miesta s najväčšou fluktuáciou návštevníkov, potenciálne rizikové zóny, problematické komunikačné koridory alebo priestory, v ktorých môže dochádzať k vzniku tlačeníc. Na základe týchto údajov je možné optimalizovať organizáciu priestoru, navrhnúť bezpečnostné opatrenia alebo upraviť evakuačné trasy.

6.5 Využitie počítania osôb pri ochrane mäkkých cieľov

Pri ochrane mäkkých cieľov má technológia počítania ľudí mimoriadny význam. Umožňuje monitorovať počet návštevníkov v reálnom čase a zabezpečiť dodržiavanie maximálnej kapacity objektov. Takéto riešenie

je dôležité najmä pri koncertoch, športových podujatiach, festivaloch alebo náboženských zhromaždeniach.

Významným prínosom je aj možnosť včasnej identifikácie neštandardných javov. Ak systém zaznamená náhly prílev osôb do určitej zóny, neobvykle vysokú hustotu davu alebo panický pohyb, môže okamžite generovať alarm a informovať bezpečnostný personál. Takáto funkcionalita umožňuje prijať preventívne opatrenia ešte pred vznikom kritickej situácie.

Počas evakuácie umožňuje technológia monitorovať priebeh presunu osôb a vyhodnocovať efektivitu evakuačných trás. Analýza zhromaždených údajov následne poskytuje cenné podklady pre zlepšovanie krízového plánovania a organizácie budúcich podujatí.

6.6 Integrácia s ostatnými bezpečnostnými systémami

Systémy počítania ľudí sa v praxi často integrujú s ďalšími komponentmi bezpečnostnej infraštruktúry. Najčastejšie ide o prepojenie s kamerovými systémami CCTV, systémami kontroly vstupu, požiarnymi systémami, bezpečnostnými ústredňami a videoanalytickými platformami.

Kombináciou údajov z viacerých zdrojov vzniká komplexný obraz o aktuálnej bezpečnostnej situácii. Operátori bezpečnostných centier tak získavajú presné informácie nielen o identite osôb a ich správaní, ale aj o aktuálnom počte návštevníkov a rozložení davu v priestore.

6.7 Budúci vývoj technológie

Budúci vývoj technológie počítania ľudí bude úzko prepojený s rozvojom umelej inteligencie a prediktívnej analytiky. Očakáva sa, že budúce systémy budú schopné nielen monitorovať aktuálny stav, ale aj predvídať vývoj pohybu osôb a identifikovať potenciálne bezpečnostné riziká ešte pred ich vznikom.

V kombinácii s biometrickou identifikáciou, analýzou správania osôb a inteligentnými monitorovacími systémami sa technológia počítania ľudí stáva jedným zo základných pilierov moderných systémov ochrany mäkkých cieľov a predstavuje významný príspevok k zvyšovaniu bezpečnosti verejného priestoru.

7 Technológie rozpoznávania záujmových položiek v ochrane mäkkých cieľov

7.1 Rozpoznávanie záujmových položiek ako súčasť moderných bezpečnostných systémov

Jedným z najvýznamnejších trendov súčasnej bezpečnostnej praxe je automatická identifikácia takzvaných záujmových položiek (Interest Items Detection). Pod týmto pojmom sa rozumejú objekty alebo predmety, ktoré môžu predstavovať bezpečnostné riziko alebo si vyžadujú zvýšenú pozornosť bezpečnostných pracovníkov. Medzi najčastejšie identifikované záujmové položky patria strelné zbrane, chladné zbrane, výbušné systémy, opustené batožiny, podozrivé balíky, nebezpečné nástroje, ochranné prostriedky zakrývajúce identitu alebo predmety ponechané bez dozoru vo verejných priestoroch.

Vývoj umelej inteligencie a technológií počítačového videnia umožnil vytvoriť systémy schopné automatickej detekcie týchto predmetov v reálnom čase. Moderné kamerové systémy tak prestávajú byť iba pasívnym monitorovacím nástrojom a stávajú sa aktívnym prvkom prevencie bezpečnostných incidentov.

7.2 Princíp fungovania systémov rozpoznávania predmetov

Základom identifikácie záujmových položiek je analýza obrazových dát získavaných prostredníctvom kamerových systémov. Každá snímka videozáznamu je spracovaná algoritmami umelej inteligencie, ktoré vyhľadávajú charakteristické tvary, rozmery, kontúry a vizuálne znaky konkrétnych predmetov.

Počas procesu učenia sú neurónové siete trénované na miliónoch fotografií obsahujúcich rôzne typy zbraní, batožiny alebo nebezpečných predmetov. Na základe tohto tréningu sa algoritmus naučí rozpoznávať charakteristické znaky jednotlivých objektov a následne ich dokáže identifikovať aj v reálnom prostredí.

Po detekcii potenciálne rizikového predmetu systém automaticky vyhodnocuje jeho polohu, pohyb, vzdialenosť od osôb a ďalšie kontextové informácie. Výsledkom môže byť okamžité upozornenie operátora dohľadového centra alebo aktivácia ďalších bezpečnostných opatrení.

7.3 Detekcia strelných zbraní

Rozpoznávanie strelných zbraní patrí medzi najrozvinutejšie oblasti inteligentnej videoanalytiky. Algoritmy analyzujú tvar predmetu, jeho proporcie a charakteristické komponenty, ako sú hlaveň, pažba,

zásobník alebo rukoväť. Na základe týchto znakov môžu systémy identifikovať pištole, revolvery, samopaly či útočné pušky.

Významnou výhodou moderných riešení je detekcia zbrane ešte pred jej použitím. Ak osoba vytiahne zbraň alebo ju nesie viditeľne v monitorovanom priestore, systém dokáže v priebehu niekoľkých sekúnd vyhodnotiť riziko a odoslať alarm bezpečnostnému personálu.

Pri ochrane mäkkých cieľov môže byť takáto funkcionalita kľúčová. Každá sekunda získaná včasným odhalením útočníka môže rozhodnúť o úspešnosti zásahu a minimalizácii následkov incidentu.

7.4 Detekcia chladných zbraní

Podobné princípy sa využívajú aj pri rozpoznávaní nožov, mačiet, sekier alebo iných chladných zbraní. Identifikácia je však technicky náročnejšia, pretože tieto predmety bývajú menšie a často čiastočne zakryté oblečením alebo telom osoby.

Moderné algoritmy využívajú kombináciu analýzy tvarov a správania osoby. Systém sleduje nielen samotný predmet, ale aj spôsob jeho držania, pohyb rúk a ďalšie faktory naznačujúce možné nebezpečenstvo. Vďaka tomu je možné zvýšiť pravdepodobnosť správnej identifikácie aj v komplikovaných podmienkach.

7.5 Detekcia opustenej batožiny

Jednou z najčastejších funkcionalít bezpečnostných systémov vo verejných priestoroch je detekcia opustených predmetov. Táto technológia sa využíva predovšetkým na letiskách, železničných staniciach, autobusových termináloch, nákupných centrách a športových štadiónoch.

Systém najprv identifikuje batožinu alebo iný predmet. Následne analyzuje jeho vzťah k okoliu a k osobám nachádzajúcim sa v blízkosti. Ak je predmet ponechaný bez dozoru počas vopred definovaného času, automaticky sa vytvorí alarm.

Takéto riešenie umožňuje včasnú reakciu bezpečnostných zložiek a výrazne znižuje riziko spojené s možnou prítomnosťou výbušných systémov alebo iných nebezpečných predmetov.

7.6 Rozpoznávanie výbušných systémov

Automatická detekcia výbušných zariadení predstavuje jednu z najnáročnejších oblastí bezpečnostnej analýzy. V praxi sa využíva kombinácia viacerých technológií, vrátane kamerových systémov, röntgenových zariadení, termovíznych senzorov a detektorov chemických látok.

Umelá inteligencia analyzuje vzhľad predmetov, ich rozmery, sprievodné znaky a spôsob manipulácie. Pri identifikácii podozrivého objektu

dokáže systém okamžite upozorniť operátora a aktivovať bezpečnostné protokoly.

7.7 Rozpoznávanie ochranných a maskovacích prostriedkov

Moderné inteligentné systémy dokážu identifikovať aj osoby používajúce predmety určené na zakrytie identity. Ide napríklad o kukly, masky, nepriehľadné ochranné okuliare alebo iné prvky sťažujúce identifikáciu.

V prostredí s vysokým bezpečnostným rizikom môže byť výskyt takýchto predmetov považovaný za indikátor potenciálneho ohrozenia. Systém preto umožňuje vytváranie automatických upozornení na osoby využívajúce atypické prvky maskovania.

7.8 Integrácia s analýzou správania osôb

Najvyššiu efektivitu dosahuje detekcia záujmových položiek v kombinácii s analýzou správania osôb. Samotná prítomnosť predmetu nemusí znamenať nebezpečenstvo. Ak sa však spojí s agresívnym pohybom, neštandardným správaním alebo vstupom do zakázanej zóny, môže byť výsledné riziko vyhodnotené ako významne vyššie.

Moderné systémy preto kombinujú:

- rozpoznávanie tváre,

- lokomočnú identifikáciu,
- detekciu zbraní,
- analýzu správania,
- počítanie ľudí,
- monitorovanie davu,
- identifikáciu opustených predmetov.

Takáto integrácia vytvára komplexný bezpečnostný ekosystém schopný identifikovať široké spektrum potenciálnych hrozieb ešte pred vznikom bezpečnostného incidentu.

7.9 Budúcnosť rozpoznávania záujmových položiek

Budúci vývoj bude smerovať k využívaniu multimodálnych systémov kombinujúcich obrazové, termálne, radarové a akustické údaje. Umelá inteligencia bude schopná analyzovať celý kontext situácie a nielen samotný predmet. Nebude teda hodnotiť iba to, či osoba drží zbraň, ale aj spôsob manipulácie so zbraňou, smer pohybu osoby, hustotu davu a ďalšie rizikové indikátory.

V ochrane mäkkých cieľov budú systémy rozpoznávania záujmových položiek predstavovať jeden z najdôležitejších prvkov preventívnej bezpečnosti. Ich úlohou nebude iba odhalenie hrozby, ale predovšetkým jej včasná identifikácia, aby bolo možné zabrániť vzniku alebo eskalácii bezpečnostného incidentu.

8 Využitie simulácií a virtualizácie v bezpečnostnom vzdelávaní zameranom na ochranu mäkkých cieľov

Súčasné bezpečnostné prostredie kladie stále vyššie nároky na prípravu pracovníkov zodpovedných za ochranu mäkkých cieľov. Rastúce riziko teroristických útokov, násilných incidentov, aktívnych útočníkov a mimoriadnych udalostí si vyžaduje nové prístupy k vzdelávaniu a odbornej príprave bezpečnostných pracovníkov. Tradičné formy výučby založené na prednáškach, štúdiu dokumentácie alebo teoretických cvičeniach už nedokážu dostatočne pripraviť personál na riešenie komplexných bezpečnostných situácií. Z tohto dôvodu sa do popredia dostávajú simulačné a virtualizačné technológie, ktoré umožňujú vytvárať realistické modely krízových situácií bez ohrozenia osôb a majetku.

Simulácie a virtualizácia predstavujú moderné nástroje umožňujúce bezpečnostným pracovníkom, manažérom, členom zásahových tímov a pracovníkom ochrany objektov získavať praktické skúsenosti v bezpečnom a kontrolovanom prostredí. Ich hlavnou výhodou je možnosť opakovaného tréningu situácií, ktoré sa v reálnom živote vyskytujú len zriedkavo, avšak môžu mať katastrofálne následky.

8.1 Význam simulácií v bezpečnostnom vzdelávaní

Simulácia predstavuje proces modelovania reálnych udalostí alebo procesov za účelom získania poznatkov, overenia postupov alebo nácviku riešenia konkrétnych situácií. V oblasti bezpečnosti ide o vytváranie modelových situácií, ktoré verne napodobňujú podmienky reálnych incidentov.

Význam simulácií spočíva predovšetkým v možnosti bezpečne precvičovať rozhodovacie procesy počas kritických situácií. V podmienkach ochrany mäkkých cieľov umožňujú simulácie testovanie reakcií na teroristické útoky, hromadné narušenie verejného poriadku, evakuácie, požiare, bombové hrozby alebo útoky aktívneho strelca. Účastníci výcviku tak získavajú praktické skúsenosti bez rizika vzniku skutočných škôd alebo ohrozenia zdravia.

Veľkou výhodou simulačných systémov je možnosť vytvárať neobmedzené množstvo scenárov s rôznou úrovňou náročnosti. Tréning môže byť opakovane realizovaný pri rôznych podmienkach, čo umožňuje preveriť pripravenosť personálu na široké spektrum krízových udalostí.

8.2 Virtualizácia ako nástroj moderného vzdelávania

Virtualizácia predstavuje vytváranie digitálnych modelov reálnych objektov, priestorov alebo procesov v počítačovom prostredí. Pri bezpečnostnom vzdelávaní sa najčastejšie využíva vo forme virtuálnej reality (VR), rozšírenej reality (AR) alebo zmiešanej reality (MR).

Pomocou virtualizácie možno vytvoriť digitálnu kópiu obchodného centra, školy, nemocnice, športového štadióna alebo letiska. Výcvik účastníkov následne prebieha v prostredí, ktoré sa veľmi podobá reálnym podmienkam. Užívatelia sa pohybujú vo virtuálnom priestore, reagujú na vznikajúce situácie a precvičujú bezpečnostné postupy podobne ako počas skutočných zásahov.

Významnou výhodou virtualizácie je možnosť simulovať situácie, ktoré by bolo v reálnom prostredí náročné alebo nebezpečné pripravovať. Ide napríklad o masové evakuácie, výbuchy, útoky strelca alebo chemické incidenty.

8.3 Virtuálne modelovanie mäkkých cieľov

Moderné softvérové platformy umožňujú vytváranie digitálnych dvojčiat objektov (Digital Twin). Ide o presné virtuálne modely skutočných objektov, ktoré obsahujú nielen priestorové usporiadanie budov, ale aj technické zabezpečovacie systémy, evakuačné trasy a pohyb osôb.

Pri ochrane mäkkých cieľov možno vytvoriť virtuálne modely:

- škôl a univerzít,
- nemocníc,
- železničných staníc,
- letísk,

- športových štadiónov,
- obchodných centier,
- kultúrnych zariadení,
- koncertných hál,
- administratívnych budov.

Takéto modely umožňujú organizáciám analyzovať zraniteľnosť objektov a testovať účinnosť navrhovaných bezpečnostných opatrení ešte pred ich fyzickou realizáciou.

8.4 Simulácia útoku aktívneho útočníka

Jednou z najčastejších aplikácií virtuálnej reality v bezpečnostnom výcviku je simulácia útoku aktívneho útočníka. Ide o scenár, pri ktorom sa účastník výcviku nachádza vo virtuálnom prostredí školy, nákupného centra alebo administratívnej budovy a musí reagovať na vzniknutú bezpečnostnú situáciu.

Počas simulácie sa precvičujú:

- rozpoznanie hrozby,
- aktivácia bezpečnostných postupov,
- komunikácia s operačným strediskom,
- evakuácia osôb,

- poskytovanie prvej pomoci,
- koordinácia s policajnými jednotkami.

Výhodou takéhoto riešenia je možnosť opakovania scenára s rôznymi variantmi vývoja situácie. Účastník si tak osvojuje správne rozhodovacie procesy a znižuje pravdepodobnosť chybného konania v reálnej krízovej situácii.

8.5 Simulácia evakuácie osôb

Evakuácia predstavuje jednu z najkritickejších činností pri riešení mimoriadnych udalostí. Simulačné technológie umožňujú modelovať pohyb stoviek až tisícov osôb v budovách alebo na verejných priestranstvách.

Počítačové modely dokážu analyzovať:

- rýchlosť evakuácie,
- vznik úzkych miest,
- kapacitu únikových ciest,
- správanie davu počas krízy,
- efektivitu evakuačných plánov.

Praktickým príkladom môže byť simulácia evakuácie športového štadióna s kapacitou 15 000 návštevníkov po nahlásení bombovej

hrozby. Simulačný systém umožňuje identifikovať kritické body a navrhnúť optimálne evakuačné postupy ešte pred reálnym použitím.

8.6 Simulácia bombovej hrozby

Ďalším významným využitím virtualizácie je nácvik riešenia bombových hrozieb. Vo virtuálnom prostredí je možné simulovať nález podozrivého balíka v obchodnom centre alebo na železničnej stanici.

Účastníci tréningu si precvičujú:

- identifikáciu podozrivého predmetu,
- uzatvorenie rizikovej zóny,
- komunikáciu so záchrannými zložkami,
- organizáciu evakuácie,
- koordináciu bezpečnostných opatrení.

Takéto cvičenia výrazne zvyšujú pripravenosť personálu na reálne incidenty.

8.7 Simulácia správania davu

Mimoriadne dôležitou oblasťou je simulácia davového správania. Panika predstavuje jeden z najväčších faktorov zvyšujúcich počet obetí počas mimoriadnych udalostí.

Moderné simulačné nástroje využívajú matematické modely správania osôb a dokážu analyzovať:

- vznik tlačeníc,
- šírenie paniky,
- vytváranie davových vĺn,
- kritické zhromaždenia osôb,
- blokovanie únikových trás.

Tieto poznatky umožňujú navrhovať bezpečnejšie objekty a organizovať hromadné podujatia s vyššou úrovňou ochrany.

8.8 Integrácia umelej inteligencie do simulačných systémov

Najnovšie generácie simulačných systémov využívajú algoritmy umelej inteligencie. Virtuálne osoby dokážu reagovať na vývoj situácie podobne ako skutoční ľudia.

Umelá inteligencia umožňuje:

- vytvárať realistické správanie davu,
- simulovať útočníkov,
- generovať neočakávané udalosti,
- vyhodnocovať rozhodovanie účastníkov,

- automaticky hodnotiť priebeh výcviku.

Vďaka tomu sa simulácie stávajú realistickejšími a poskytujú vyššiu úroveň pripravenosti.

8.9 Virtuálne strelnice a taktické simulátory

Významné využitie nachádzajú aj virtuálne strelecké simulátory. Bezpečnostní pracovníci môžu absolvovať tréning používania zbraní bez potreby ostrých nábojov.

Tieto systémy umožňujú:

- nácvik streľby,
- reakciu na hrozby,
- rozhodovanie pod stresom,
- precvičovanie taktiky zásahu,
- koordináciu tímových operácií.

Virtuálne strelnice významne znižujú náklady na výcvik a zároveň poskytujú vysokú úroveň realizmu.

8.10 Ekonomické a organizačné prínosy simulácií

Používanie virtuálnych simulácií prináša organizáciám viacero výhod:

- znižovanie nákladov na výcvik,

- eliminácia rizík počas tréningu,
- možnosť opakovania scenárov,
- objektívne hodnotenie výkonu účastníkov,
- možnosť tréningu veľkého počtu osôb,
- detailný záznam priebehu cvičenia.

Taktiež umožňujú precvičovať situácie, ktoré by bolo v reálnom prostredí finančne alebo organizačne veľmi náročné realizovať.

Simulácie a virtualizácia predstavujú jednu z najperspektívnejších oblastí moderného bezpečnostného vzdelávania. V podmienkach ochrany mäkkých cieľov umožňujú realisticky pripravovať bezpečnostný personál na riešenie širokého spektra krízových situácií, od evakuácií až po útoky aktívnych útočníkov. Využívanie virtuálnej reality, digitálnych dvojčiat, umelej inteligencie a pokročilých simulačných modelov významne zvyšuje kvalitu prípravy personálu a prispieva k znižovaniu bezpečnostných rizík. Očakáva sa, že s ďalším rozvojom technológií sa simulácie stanú štandardnou súčasťou vzdelávania všetkých odborníkov pôsobiacich v oblasti ochrany mäkkých cieľov.

Záver

Ochrana mäkkých cieľov predstavuje jednu z najvýznamnejších výziev súčasnej bezpečnostnej praxe. Rastúca komplexnosť bezpečnostných hrozieb si vyžaduje využívanie moderných technológií, integrovaných bezpečnostných systémov a pokročilých metód analýzy dát. Významnú úlohu zohráva biometrická identifikácia, videoanalytika, analýza správania osôb a systémy riadenia davov. Budúcnosť ochrany mäkkých cieľov bude nepochybne spojená s ďalším rozvojom umelej inteligencie, automatizácie a prediktívnych bezpečnostných systémov, ktoré umožnia efektívnejšie identifikovať a eliminovať vznikajúce hrozby ešte pred ich realizáciou.