Securitologia/Securitology/Секюритология
2013, nr 1(17). ISSN 1898-4509

Juraj VACULÍK*

ZLEPŠOVANIE NÁSTROJOV NA HODNOTENIE ÚČINNOSTI BEZPEČNOSTNÉHO SYSTÉMU POMOCOU APLIKÁCIE NOVÝCH MODELOV A VÝSTUPNÝCH PARAMETROV

ABSTRAKT

V článku sú popísané nové modely a výstupné parametre využiteľné pri hodnotení účinnosti bezpečnostných systémov. Dôraz je kladený na bezpečnostné systémy v bežných komerčných aplikáciách, pre ktoré sú typické nižšie hodnoty chráneného záujmu a problematické získavanie niektorých typov vstupných dát. Navrhované výstupné parametre skúmajú možnosť, že narušiteľ dokončí útok bez konfrontácie so zásahovou jednotkou alebo možnosť, že narušiteľ dokončí útok a aj úspešne unikne. Navrhnuté modely a výstupné parametre boli pre testovacie účely softvérovo implementované a v článku sú zhodnotené výsledky ich testovania. Celková koncepcia navrhnutých modelov a parametrov je zameraná na univerzálnosť výsledného testovacieho nástroja, čo poskytuje značnú výhodu pri problematickom získavaní vstupných dát, ktoré je často prekážkou pre nasadenie kvantitatívnych nástrojov hodnotenia účinnosti v podmienkach praxe.

Kľúčové slová: účinnosť bezpečnostných systémov, pravdepodobnosť prerušenia

UPGRADING OF TOOLS FOR EFFICIENCY ESTIMATION OF PHYSICAL PROTECTION SYSTEM USING NEW MODELS AND OUTPUT PARAMETERS

ABSTRACT

The article describes new models and output parameters that can be used for efficiency estimation of physical protection systems. The article focuses especially on smaller commercial physical protection systems. Evaluation of these physical protection systems can be difficult because of limited input data. Proposed output parameters estimate the option that intruder will successfully accomplished attack on protected assets without confronting with intervention unit or that intruder will also successfully escape from the vital area. Proposed models and output parameters were implemented in testing software and the article contains results of their testing. The main conception of new elements design is the versatility of evaluation tool. This versatility provides advantages in situations with limited input data, which is common obstacle in efficiency evaluation in practical situations.

Key words: efficiency of physical protection systems, probability of interruption

* Ing. Juraj VACULÍK - Katedra bezpečnostného manažmentu, Fakulta špeciálneho inžinierstva, Žilinská univerzita, e-mail: juraj.vaculik@fsi.uniza.sk

УЛУЧШЕНИЕ ИНСТРУМЕНТОВ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРЕДОХРАНИТЕЛЬНЫХ СИСТЕМ ПУТЕМ ПРИМЕНЕНИЯ НОВЫХ МОДЕЛЕЙ И ВЫХОДНЫХ ПАРАМЕТРОВ

РЕЗЮМЕ

В статье описаны новые модели и параметры выхода используемые для оценки эффективности предохранительных систем. Упор делаем на предохранительные системы при текущих коммерческих применениях, для которых типичны более низкие ценности охраняемого интереса и проблематическое получение некоторых видов входных данных. Предлагаемые выходные параметры исследуют возможность, что нарушитель окончит атаку и ускользнет без конфронтации с отделом вмешательства. Предлагаемые модели и выходные параметры были для целей тестов в области софтвера введены в действие и в статье представлены оцененные результаты их тестирования. Общая концепция предложенных моделей и параметров направлена для универсальности инструмента тестирования, что представляет значительное преимущество в случае проблематического приобретения входных данных, которое часто является препятствием приложения количественных инструментов в оценку эффективности при условиях практики.

Ключевые слова: эффективность предохранительных систем, вероятность перерыва

1. Úvod

Hodnotenie účinnosti bezpečnostných systémov je dôležitou súčasťou posudzovania bezpečnostných rizík v oblasti fyzickej bezpečnosti objektu. Úlohou fyzickej bezpečnosti je ochrana osôb a zabránenie neautorizovanému prístupu k vybaveniu, zariadeniam, materiálom a dokumentom, ktoré by mohli byť zničené alebo ukradnuté.[19]

Posudzovanie rizík, ktoré pozostáva z identifikácie, analýzy a hodnotenia rizík[11] môže byť vykonávané s využitím kvalitatívneho alebo kvantitatívneho prístupu.[8] Pri kvantitatívnom hodnotení účinnosti bezpečnostných opatrení sa používa matematický model stráženého priestoru a na získavanie výstupných hodnôt sa používa špecializovaný softvér. Výsledná hodnota rizika sa získava výpočtovo, typicky podľa vzťahu z [1]:

$$R = P_A.[1 - P_E].C$$

kde R je riziko, P_A je pravdepodobnosť útoku daná hrozbami a zraniteľnosťami (často sa v praxi používa hodnota 1) , P_E je pravdepodobnosť účinnosti systému (pravdepodobnosť prerušenia a pravdepodobnosť zneškodnenia narušiteľa) a C je hodnota aktíva, resp. veľkosť dopadu.

Softvérové nástroje na hodnotenie účinnosti sa vyvíjajú od šesťdesiatych rokov minulého storočia a dnes predstavujú dôležitý podporný nástroj pri hodnotení a projektovaní bezpečnostných systémov. Za dobu svojej existencie softvérové nástroje

na hodnotenie účinnosti prešli značným vývojom.[7] Prvé nástroje umožňovali iba približné ohodnotenie úrovne bezpečnosti systému proti vonkajšiemu narušiteľovi. S postupom času sa začali rozširovať sofistikovanejšie nástroje na hodnotenie interných a externých hrozieb, ktoré detailnejšie skúmajú jednotlivé procesy, ktoré sprevádzajú ohrozenie chráneného záujmu.

Faktory, ktoré mohli byť v minulosti zanedbateľné, sú dnes pri prísnejších nárokoch na výstup hodnotenia dôležité a predstavujú nové výzvy, ktorým treba čeliť pomocou rozširovania a zdokonaľovania modelov hodnotenia. Napríklad je potrebné podrobnejším spôsobom modelovať prechody narušiteľa medzi jednotlivými mechanickými zábrannými prostriedkami a počítať čas, ktorý narušiteľ reálne strávi pri presune a úniku v stráženom priestore. Z hľadiska výstupných parametrov najdôležitejším výstupným parametrom zostáva pravdepodobnosť prerušenia, t.j. kumulatívna pravdepodobnosť do kritického bodu detekcie[12], ktorú je vhodné rozšíriť aj o pravdepodobnosť bezporuchového stavu detekčných zariadení, pravdepodobnosť bezporuchového stavu komunikačných systémov a spoľahlivosť ľudského faktora podľa vzťahu v [5] :

$$P_{KDET} = \left[1 - \prod_{i=1}^{n}(1 - P_{Di})\right] . P_{PPS} . P_P . P_{LF}$$

kde P_{KDET} je kumulatívna pravdepodobnosť detekcie, n je počet zón, P_{Di} je pravdepodobnosť detekcie v zóne i, P_P je pravdepodobnosť bezporuchového stavu detekčných zariadení, P_{PPS} je pravdepodobnosť bezporuchového stavu komunikačných systémov a P_{LF} je spoľahlivosť ľudského faktora.

Skúsenosti ukazujú, že samostatné používanie pravdepodobnosti prerušenia nemusí byť v meniacich sa podmienkach postačujúce. Súčasne s rozvojom daných nástrojov sa podstatne rozširuje aplikovateľnosť nástrojov na rôzne situácie.[16] Z kedysi ťažko dostupných softvérových nástrojov určených na hodnotenie bezpečnosti jadrových objektov na stávajú nástroje aplikovateľné v komerčnej sfére aj pre bezpečnostné systémy s neporovnateľne nižším chráneným záujmom. To predstavuje výzvu pre proces modelovania a hodnotenia bezpečnostných systémov. Napríklad novým cieľom bezpečnostného systému často môže byť zadržanie narušiteľa a nie priamo zabránenie akéhokoľvek prístupu a manipulácie s chráneným záujmom.[4] Z praktického hľadiska to znamená modelovanie nielen postupu, ale aj úniku narušiteľa zo stráženého priestoru.

Postupne vznikli aj výstupné parametre zohľadňujúce únik narušiteľa, ako napr. koeficient účinnosti ochranných opatrení definovaný v [5] pomocou vzťahu:

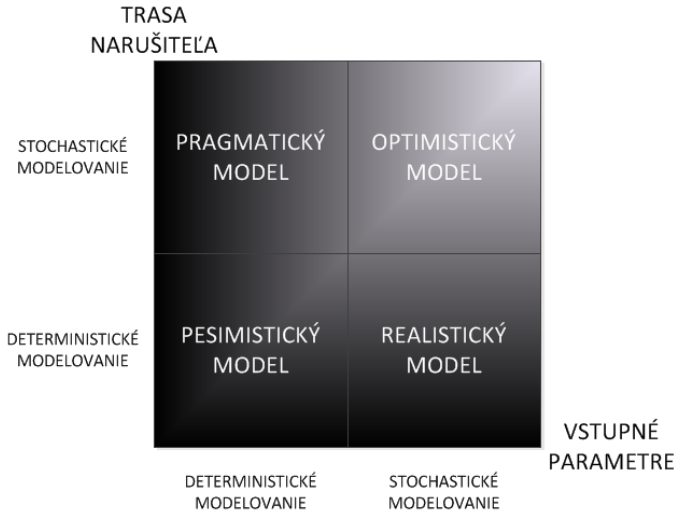
$$\frac{T_{PRL}}{T_{FO}} = \frac{T_P + T_{PRES} + T_{út} + T_{ún}}{T_{pop} + T_{ver} + T_{pres} + T_{zás}}$$

kde T_{PRL} je celkový čas prekonávania všetkých prvkov, T_{FO} celkový čas zásahu, T_P je súčet časov prekonávania prvkov s prielomovou odolnosťou, T_{PRES} je čas zdržania pri prechodoch, T_{pop} je čas poplachu, T_{ver} je čas verifikácie poplachu, T_{pres} je čas príchodu na miesto zásahu, $T_{zás}$ je čas zásahu , $T_{út}$ je celkový čas prekonávania všetkých prvkov a $T_{ún}$ celkový čas zásahu.

Tento výstupný parameter však nezohľadňuje detekciu narušiteľa[5] a preto je jeho výpovedná hodnota nižšia ako v prípade pravdepodobnosti prerušenia. Meniace sa podmienky väčšej dostupnosti nástrojov vplývajú aj na značný nárast potreby vstupných dát. Získavanie a validácia vstupných dát, ako sú prielomové odolnosti, pravdepodobnosti detekcie a pod., predstavujú špecifický a zložitý problém[8], ktorý komplikuje praktické nasadenie vytvorených hodnotiacich nástrojov. Je dôležité, aby navrhnuté modely hodnotenia boli natoľko univerzálne, aby dokázali správne interpretovať rôzne vstupné dáta získané podľa rôznych metodík.

Matematické modely môžu byť deterministické alebo stochastické. Deterministické modely majú jednotlivé vstupné parametre určené jednoznačne, zatiaľ čo stochastické modely majú vstupné parametre určené pomocou pravdepodobnostného rozdelenia hodnôt.[9] Pri matematickom modelovaní bezpečnostných systémov bolo v minulosti bežné predovšetkým stochastické modelovanie vstupných dát a deterministické modelovanie trás narušiteľa. Nástroje tak boli založené na vyhľadávaní kritických (minimálnych) ciest a vstupné dáta boli definované pomocou pravdepodobnostné rozloženia vstupných parametrov.[15]

V súčasnosti vzrastá význam nástrojov, ktoré vnútorne implementujú väčšie množstvo modelov. Takéto nástroje sú využiteľné aj pri obmedzených možnostiach získavania vstupných dát a dokážu sa skôr prispôsobiť získaným dátam, ako by sa mali metodiky získavania dát prispôsobovať požiadavkám konkrétnych nástrojov. Takéto modely boli definované v [5] a sú zhrnuté na obr.1.



Obr. 1. Modely hodnotenia účinnosti bezpečnostných systémov

Deterministické modelovanie trás používa algoritmus na nájdenie (jednej) minimálnej trasy, ktorá má najnižšie hodnoty výstupných parametrov a možno ju považovať za najväčšiu zraniteľnosť systému.[4] Stochastické modelovanie trás je založené na vykonávaní veľkého množstvo simulácií, pri ktorých sa vytvárajú a ohodnocujú náhodne vygenerované trasy. Pravdepodobnosť, že konkrétny prvok bude

súčasťou vygenerovanej trasy je daná nepriamo jeho váhou, ktorú definuje pre každý prvok používateľ.

Deterministické zadávanie vstupných údajov používa pre každý parameter jednu konkrétnu hodnotu.[5] Táto hodnota môže byť minimálna (zaručená) hodnota parametra, alebo jeho stredná hodnota. Stochastické zadávanie definuje vstupné parametre pomocou normálneho rozdelenia pravdepodobnosti a používa strednú hodnotu a smerodajnú odchýlku pre definovanie vstupného parametra.

Na základe súčasného stavu možno zadefinovať niekoľko problémových oblastí. Jednou z týchto oblastí je absencia výstupných parametrov, ktoré by boli vhodné na využitie pri hodnotení účinnosti bezpečnostného systému voči krádežiam, kedy postačuje narušiteľa zadržať pri jeho úniku.

Ďalšou oblasťou je problematický výpočet dĺžky prechodov narušiteľa medzi jednotlivými mechanickými zábrannými prvkami a vplyvy vlastností terénu a prostredia na čas prechodu narušiteľa. Model EASI počíta aj s časmi prechodov[2], podobne ako všetky nástroje založené na modeli EASI (SAVI, ASSESS). Diagram ASD, ktorý je využitý v GUI, je však neprehľadný, zložitý na používanie a aj nepresný pre výpočty.[3] Pri prechode jednotlivých oblastí sa vždy pripočítava k celkovému času konštantná hodnota bez ohľadu na konkrétnu trasu, ktorú narušiteľ zvolí (napr. bez ohľadu na konkrétne miesto, kde narušiteľ prekonal plot a pod.). Vplyv terénu a ďalších podmienok na čas presunu narušiteľa nebol v literatúre zatiaľ dostatočne popísaný.

Samostatný problém predstavuje úroveň a kvalita podpory nástrojov pri projektovaní bezpečnostných systémov. Samotné hodnotenie statického stavu systému nie je dostatočné. Bezpečnostný manažment požaduje nástroje schopné vyhľadávať vhodné riešenia aj so zreteľom na minimalizáciu investičných nákladov.[5] V tomto zmysle je potrebné hlbšie preskúmať možnosti, ktoré poskytujú súčasné a perspektívne riešenia pri projektovaní bezpečnostných systémov.

2. Materiály a metódy

V rámci riešenia popísaných problémových oblastí sme navrhli nové vstupné a výstupné parametre hodnotenia a navrhli sme postup vykonávania systematickej analýzy vylepšení bezpečnostného systému, ktorá by poskytovala väčšiu podporu bezpečnostnému manažmentu pri projektovaní bezpečnostných systémov. Pre účely praktického overenia návrhov sme vytvorili testovací softvér.

V rámci testovania sme skúmali viaceré aspekty :

- skúmanie presnosti výpočtu výstupných parametrov a faktory, ktoré presnosť zásadne ovplyvňujú,
- spôsob kvantifikácie spomalenia postupu a úniku narušiteľa v dôsledku sťaženého terénu,
- vplyv meniacej sa rýchlosti narušiteľa pri postupe a úniku na výstupné parametre,
- možnosti analýzy citlivosti a iných analytických nástrojov pri hľadaní najefektívnejších vylepšení bezpečnostného systému.

Našou prvoradou úlohou bolo zadefinovanie výstupných parametrov hodnotenia. Spolu sme navrhli pre účely testovania tri výstupné parametre :

- Pravdepodobnosť prerušenia – tento výstupný parameter je podrobne popísaný v literatúre, napr.[1], [2], [3], [4], [5], [12], [15],
- Pravdepodobnosť úniku – parameter vychádza z pravdepodobnosti prerušenia, ale zohľadňuje aj únik narušiteľa; navrhli sme presný algoritmus výpočtu,
- Koeficient účinnosti – parameter vychádza z koeficientu účinnosti ochranných opatrení, ktorí je popísaný v [3,[4]; navrhli sme presný algoritmus výpočtu.

Navrhované výstupné parametre sme implementovali do štyroch modelov hodnotenia účinnosti (pesimistický, realistický, optimistický a pragmatický model) popísaných v [3], [4].

Je zrejmé, že medzi faktory, ktoré zásadne ovplyvňujú presnosť výpočtu patrí aj štruktúra bezpečnostného systému. Napr. bezpečnostný systém zložený z veľkého počtu rýchlo prekonateľných prvkov s detektormi bude prirodzene vykazovať vyššie odchýlky pri opakovaní simulácií, ako bezpečnostný systém s malým množstvom detektorov (napr. iba v perimetri a pod.).

Pre abstrahovanie od týchto vplyvov sme pri zisťovaní vplyvu počtu simulácií na výslednú strednú hodnotu výstupných parametrov používali konkrétnu pevne danú trasu narušiteľa definovanú podľa tab.1.

Tab. 1. Vybraná trasa na testovanie presnosti

P.č.	Názov	μ (s)	Σ (s)	P(d)	Typ detekcie
1.	**Prekonanie plota**	20	6	0,9	Pred
2.	**Prechod cez areál**	40	12	0,6	Uprostred
3.	**Vstupné dvere**	110	33	0,95	Po
4.	**Hala**	16	4,8	0	-
5.	**Dvere**	90	27	0,9	Po
6.	**Sabotáž**	100	30	0	-

Pesimistický a realistický model používa na definovanie vstupných parametrov normálne pravdepodobnostné rozdelenie dané vzťahom :

$$f(x;\mu,\sigma^2) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2}$$

kde μ stredná hodnota a σ^2 je rozptyl. Stanovenie štandardnej odchýlky závisí od metodiky získavania časov prielomovej odolnosti. V literatúre sa odporúča na základe testov v *Sandia National Laboratories* a skúseností z praxe používať 30 % strednej hodnoty, čo platí aj pre iné vstupné parametre.[1] Túto hodnotu sme používali na všetky vstupné parametre.

3. Výsledky

3.1 Výstupné parametre

Pre výpočet koeficientu účinnosti bol navrhnutý nový algoritmus výpočtu. Koeficient účinnosti predstavuje priemerný pomer medzi časom od momentu detekcie po dokončenie útoku a celkovým časom zásahu. Koeficient sa počíta ako priemer hodnôt získaných podľa vzťahu :

$$\frac{T_{PRL(D)}}{T_{FO}} = \frac{T_{P(D)} + T_{PRES(D)}}{T_{pop} + T_{ver} + T_{pres} + T_{zas}}$$

kde $T_{PRL(D)}$ je čas prekonávania všetkých prvkov po detekcii narušiteľa, T_{FO} celkový čas zásahu, $T_{P(D)}$ je súčet časov prekonávania prvkov s prielomovou odolnosťou po detekcii narušiteľa, $T_{PRES(D)}$ je čas zdržania pri prechodoch po detekcii narušiteľa, T_{pop} je čas poplachu, T_{ver} je čas verifikácie poplachu, T_{pres} je čas príchodu na miesto zásahu a $T_{zás}$ je čas zásahu.

Bod detekcie je bod na trase narušiteľa, kedy kumulatívna pravdepodobnosť detekcie do daného bodu prekročila určitú medznú hodnotu z intervalu (0,100), ktorá sa s každou iteráciu zvyšuje.

Koeficient účinnosti nezahrňuje do výpočtu čas úniku narušiteľa. Úspešná detekcia narušiteľa závisí okrem pravdepodobnosť detekcie aj od pravdepodobnosti úspešnej komunikácie.[6],[10] Jednotlivé kumulatívne pravdepodobnosti detekcie sú preto vynásobené s pravdepodobnosťou úspešnej komunikácie, takže podľa terminológie uvedenej v [1],[2] sa pri výpočte používa pravdepodobnosť poplachu daná vzťahom :

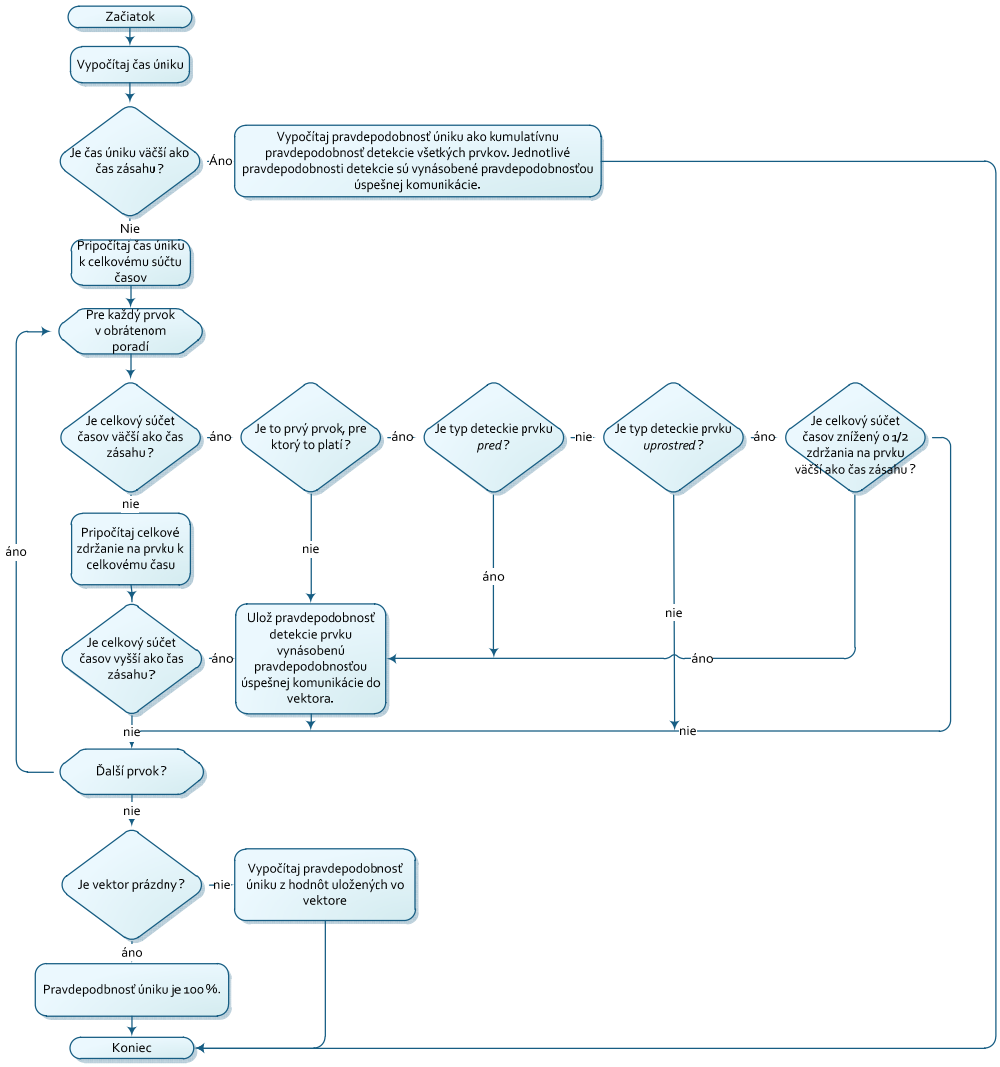
$$P_{pop} = P_d . P_{úk}$$

kde P_d je pravdepodobnosť detekcie a $P_{úk}$ je pravdepodobnosť úspešnej komunikácie.

Výhodou koeficientu účinnosti je, že umožňuje dobre odhadnúť časovú rezervu zásahovej jednotky, ktorú je možné využiť pri vzniku nečakaných komplikácií v súvislosti s prípravou zásahu. Tento výstupný parameter je vhodný na ohodnotenie najzávažnejších hrozieb, pri ktorých môže tento typ informácie zaujímavý.

Ďalej sme navrhli algoritmus na výpočet pravdepodobnosti úniku, ktorý je znázornený na obr.2. Jedná sa o pravdepodobnosť, že narušiteľ dokončí útok a opustí strážený priestor bez konfrontácie so zásahovou jednotkou. Tento výstupný parameter je použiteľný v situáciách, kedy postačuje zadržanie narušiteľa pri jeho úniku.

Pri našom výpočte pravdepodobnosti úniku sa predpokladá, že narušiteľ bude unikať po tej istej trase, po ktorej postupoval cez strážený priestor pri útoku a bude tak využívať už prekonané prvky ochrany. Pravdepodobnosť úniku je počítaná podobne, ako pravdepodobnosť prerušenia a predstavuje kumulatívnu pravdepodobnosť detekcie do kritického bodu detekcie, ktorý bol na trase narušiteľa posunutý časom úniku.



Obr. 2. Algoritmus výpočtu pravdepodobnosti úniku.
zdroj: autor

Z hľadiska výpočtu možno zadefinovať pravdepodobnosť úniku pomocou vzťahu:

$$P_{ú} = 1 - KP_d$$

kde KP_d je kumulatívna pravdepodobnosť detekcie do kritického bodu detekcie.

Ak čas, ktorý strávi narušiteľ únikom je zanedbateľný v porovnaní s časom prekonávania mechanických zábranných prostriedkov, tak medzi pravdepodobnosťou úniku a pravdepodobnosťou prerušenia platí vzťah :

$$P_{ú} \approx 1 - P_p$$

kde $P_{ú}$ je pravdepodobnosť úniku a P_p je pravdepodobnosť prerušenia.

Pri ohrozeniach menšieho chráneného záujmu možno odporučiť výpočet pravdepodobnosti úniku. Pri vyšších hodnotách chráneného záujmu možno odporučiť používanie pravdepodobnosti prerušenia a prípadne aj koeficientu účinnosti.

3.2 Presnosť výpočtu výstupných parametrov

Medzi skúmané otázky sme zaradili aj otázku presnosti daného výpočtu, nakoľko pri všetkých výpočtoch (s výnimkou plne deterministického pesimistického modelu) sa využívajú simulácie a výpočet strednej hodnoty. Na základe testov boli označené faktory, ktoré výrazne ovplyvňovali presnosť výpočtu :

- Štruktúra bezpečnostného systému,
- Štandardné odchýlky vstupných parametrov (realistický a optimistický model),
- Vykonaný počet simulácií.

Za účelom zistenia vzťahu medzi počtom simulácií a výslednými hodnotami výstupných parametrov boli vykonané merania na vybranej trase. Čas zásahu sme zadali nasledovne:

1. Čas poplachu a verifikácie: $\mu = 30$, $\sigma = 9$,
2. Čas prípravy zásahu: $\mu = 240$, $\sigma = 72$.

Z našich výsledkov vyplýva, že rozsah nameraných hodnôt pre konkrétnu trasu pri 100 iteráciách je 4 % (pravdepodobnosť prerušenia), resp. 0,2 (koeficient účinnosti) a pri 10 000 iteráciách 2 % (pravdepodobnosť prerušenia), resp. 0,03 (koeficient účinnosti).

3.3 Modelovanie prechodov medzi mechanickými zábrannými prostriedkami

V testovacom softvéri sme vyriešili vzťah medzi terénom a spomalením postupu a úniku narušiteľa zavedením koeficientu spomalenia. Pre čas prekonávania *t* potom platí:

$$t = \frac{s}{v.(1 - ks)}$$

kde *s* je dĺžka prechodu, *v* je základná rýchlosť presunu narušiteľa a *ks* je koeficient spomalenia. Spomalenie sme vyjadrili relatívne vzhľadom na pevnú referenčnú hodnotu rýchlosti, ktorou by išiel narušiteľ, ak by mal úplne ideálne podmienky pre presun.

Rozlišovali sme medzi základnou rýchlosťou postupu, ktorou narušiteľ postupuje cez strážený priestor a základnou rýchlosťou úniku, ktorou narušiteľ uniká po dokončení útoku.

3.4 Počítačová podpora projektovania bezpečnostných systémov

Poslednou skúmanou oblasťou bola možnosť počítačovej podpory pri vyhľadávaní vylepšení bezpečnostného systému. Jednou z možností pri vyhľadávaní

najefektívnejšieho vylepšenia systému je analýza citlivosti výstupných parametrov. Do testovacieho softvéru sme implementovali iný nástroj na hodnotenie vylepšení.

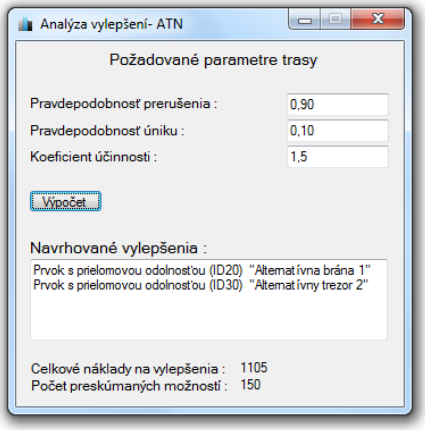
Vytvorili sme možnosťou zadávať pre každý prvok alternatívne prvky, ktoré by mohli daný primárny prvok nahradiť. Pre alternatívne prvky sme zadefinovali aj približné náklady na vylepšenie (výmenu) prvku.

Pri analýze vylepšení sa potom zadefinujú požadované minimálne hodnoty výstupných parametrov a program pomocou rekurzívneho algoritmu vypočíta výstupné parametre pre všetky možné trasy a následne hľadá najlacnejšiu trasu, ktorá vyhovuje požiadavkám. Táto trasa môže mať použitých jeden alebo viacero alternatívnych prvkov. Alternatívne prvky môžu byť :

- Alternatívne mechanické zabezpečovacie prostriedky (s vyššou prielomovou odolnosťou alebo vyššou pravdepodobnosťou detekcie pri prekonávaní),
- Alternatívne prechody (s vyššou pravdepodobnosťou detekcie pohybu),
- Alternatívne parametre zásahu (s nižším časom prípravy zásahu).

Hlavnou výhodou v porovnaní s analýzou citlivosti je, že je možné zisťovať efektívnosť výmeny viacerých prvkov naraz v rôznych kombináciách a tak odhaliť najefektívnejšie riešenie z hľadiska ich nákladov.

Obr.3 ukazuje príklad vykonávania analýzy vylepšení v testovacom programe. Po zadaní 11 alternatívnych prvkov bolo preskúmaných spolu 150 rôznych možností (150 kombinácií prvkov) a pre každú možnosť boli vypočítané tri výstupné parametre. Každý výpočet výstupného parametra pozostával zo 100 000 simulácií. Celkovo bolo teda vykonaných 45 miliónov simulácií a bolo nájdené najlacnejšie riešenie, ktoré vyhovuje požiadavkám. Toto riešenie pozostáva z výmeny dvoch prvkov na trase za navrhnuté alternatívy.



Obr. 1 Analýza vylepšení

4. Diskusia

V článku bol demonštrovaný spôsob výpočtu dvoch nových výstupných parametrov – pravdepodobnosti úniku a koeficientu účinnosti. Boli determinované faktory, ktoré vplývajú na presnosť ich výpočtu.

Parameter pravdepodobnosť úniku je využiteľný pri hodnotení účinnosti bezpečnostného systému proti krádežiam. Existujúce nástroje na hodnotenie účinnosti sa hodnotením ochranných opatrení proti tomuto riziko zaoberajú iba okrajovo. Navrhnutý výpočet je rozšírením výpočtu pravdepodobnosti prerušenia. Čas úniku v zásade iba posúva kritický bod detekcie a analogicky ako v prípade pravdepodobnosti prerušenia sa počíta kumulatívna pravdepodobnosť detekcie.

Koeficient účinnosti je naopak využiteľný pri chránení najvýznamnejších aktív, nakoľko na rozdiel od pravdepodobnosti prerušenia jeho hodnota rastie neustále lineárne s rastúcimi protiopatreniami. Pri výpočte koeficientu účinnosti sa núka možnosť vytvoriť ešte jeden výstupný parameter, ktorý by bol počítaný obdobne ako koeficient účinnosti, ale zohľadňoval by aj čas úniku.

Otázkou zostáva praktická aplikovateľnosť takéhoto výstupného parametra, keďže samotný koeficient účinnosti je aplikovateľný iba v prípadoch ohrozenia najvyššieho chráneného záujmu veľmi významnými rizikami a oblasť krádeží hmotného majetku (kde únik zohráva rolu) do tejto kategórie nepatrí.

Zaujímavejšou otázkou môže byť vhodnosť zmeny charakteru koeficientu účinnosti z pomerového parametra na parameter rozdielový, v ktorom by sa priamo kvantifikovala primeraná časová rezerva zásahovej jednotky podľa obr.3 daného vzťahom :

$$T_{PRL(D)} - T_{FO} = (T_{P(D)} + T_{PRES(D)}) - (T_{pop} + T_{ver} + T_{pres} + T_{zas})$$

kde $T_{PRL(D)}$ je čas prekonávania všetkých prvkov po detekcii narušiteľa, T_{FO} celkový čas zásahu, $T_{P(D)}$ je súčet časov prekonávania prvkov s prielomovou odolnosťou po detekcii narušiteľa, $T_{PRES(D)}$ je čas zdržania pri prechodoch po detekcii narušiteľa, T_{pop} je čas poplachu, T_{ver} je čas verifikácie poplachu, T_{pres} je čas príchodu na miesto zásahu a $T_{zás}$ je čas zásahu.

Takýto parameter by v praxi mohol byť zrozumiteľnejší ako koeficient účinnosti daný pomerom časov a jednoduchšie by sa interpretoval bezpečnostným manažérom.

Problematickým bodom hodnotenia účinnosti sa stáva modelovanie prechodov medzi jednotlivými mechanickými zábrannými prostriedkami, ako z hľadiska programovej implementácie, tak v oblasti získavania vstupných dát, ktoré kvalifikujú spomalenie narušiteľa v dôsledku vlastností prostredia, ktoré vplývajú na rýchlosť presunu. Časy strávené pri prechodoch nemožno zanedbať predovšetkým pri objektoch s nižšími hodnotami prielomových odolností. Význam kvantifikácie spomalenia v dôsledku terénu vzrastá pri objektoch s rozsiahlejšími areálmi a v prípadoch, kedy je vhodné modelovať aj únik narušiteľa.

V tejto oblasti sme zadefinovali vstupný parameter koeficient spomalenia, ktorý kvantifikuje spomalenie presunu narušiteľa vzhľadom na základnú (referenčnú) rýchlosť. Koeficient spomalenia nezohľadňuje únavu narušiteľa pri prekonávaní dlhších

vzdialeností. Otázne je, do akej miery je tento prístup akceptovateľný aj pri hodnotení rozsiahlych areálov a takisto, ktoré ďalšie vplyvy treba zahrnúť do metodiky stanovenia koeficientu spomalenia (ako napr. hmotnosť záťaže, poveternostné podmienky pri prekonávaní prechodov a pod.).

Na posudzovanie výhodnosti inštalácie nových zabezpečovacích prvkov sme navrhli a otestovali spôsob vykonávania analýzy vylepšení, ktorý pozostáva s definovania alternatívnych prvkov a ich nákladov a rekurzívny algoritmus na overenie všetkých teoretických možností s cieľom nájdenia najlacnejšej kombinácie vylepšení.

Zadávanie alternatívnych prvkov pre jednotlivé prvky by bolo v praxi veľmi zložité. Z praktického hľadiska sa javí ako efektívnejšie, aby používateľ v takomto programe nedefinoval alternatívy pre jednotlivé prvky, ale aby definoval celé alternatívne množiny prvkov, ktoré by nahrádzali celú skupinu prvkov v pôvodnom systéme. Pre rôzne subsystémy bezpečnostného systému by boli zadefinované alternatívne subsystémy, pričom celý tento alternatívny subsystém by bol ocenený z hľadiska nákladov na inštaláciu a prevádzku (ak náklady na prevádzku by boli vyššie ako náklady na prevádzku pôvodného subsystému).

Napríklad by bolo možné definovať alternatívnu množinu prvkov perimetrickej ochrany, ktorá by zahrňovala rôzne prvky, ktoré chránia perimeter (napríklad aj prvky s prielomovou odolnosťou, aj prvky s detekčnými charakteristikami). Takýchto množín by používateľ mohol zadefinovať neobmedzený počet a program by hľadal najlacnejšiu alternatívnu konfiguráciu bezpečnostného systému, ktorá by spĺňala zadané hodnoty výstupných parametrov.

Dôležitou otázkou je aj možná integrácia simulácie ozbrojeného boja do perspektívneho komerčného nástroja na hodnotenie účinnosti bezpečnostných systémov. Simulácia ozbrojeného boja je moderný a dynamicky sa rozvíjajúci nástroj hlavne v oblasti vojenstva a ochrany obzvlášť významných objektov.[7], [17], [18] V oblasti komerčných aplikácií s nižšou a stredne vysokou hodnotou chráneného záujmu je možné predpokladať prevahu zásahovej jednotky a náročná simulácia ozbrojeného boja nemusí byť taká zaujímavá. Nepochybne je potrebné pri vývoji softvérového riešenia dôkladne zvážiť potreby a požiadavky potenciálnych používateľov a určiť, do akej miery je pre nich simulácia ozbrojeného boja dôležitá.

LITERATÚRA

[1] GARCIA M.L. 2008. *The Design nad Evaluation of Physical Protection Systems*: Sandia National Laboratories. 351 s. ISBN 978-0-7506-8352-4

[2] GARCIA M.L. 2006. *Vulnarability Assessment of Physical Protection Systems:* Sandia National Laboratories. 382 s. ISBN 978-0-7506-7788-2

[3] JANG S. 2009. *Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection (SAPE)*. IN: Nuclear Engineering and Technology, VOL.41 NO.5 Jún 2009

[4] LOVEČEK T. 2009. *Systémy ochrany majetku a možnosti ich kvalitatívneho a kvantitatívneho ohodnotenia*: Habilitačná práca. Žilina.

[5] LOVEČEK T. 2005. *Hodnotenie kvality bezpečnostných systémov:* Dizertačná práca. Žilina.
[6] PETRUZZELLIS T. 1994. *Alarm, Sensor & Security Circuit Cookbook*: TAB Books. 296 s. ISBN 0-8306-4314-1
[7] PHILLIPS G. 2004. *New Vulnerability Assessment Technologies vs the Old VA Tools*. New Meets Old. National Security Program Office.
[8] REITŠPÍS J. 2004. *Manžérstvo bezpečnostných rizík*: Edis. Žilina. 296 s. ISBN 80-8070-328-0
[9] RYBÁR M. 2000. *Modelovanie a simulácia vo vojenstve*: Vydavateľská a informačná agentúra, Ministerstvo obrany Slovenskej republiky. Bratislava. ISBN 80-88842-34-4
[10] SMIETAN I. 1997. *Perimeter Security Sensor Technologies Handbook*: Defense Advanced Research Projects Agency (DARPA). 108 s.
[11] ISO 31000: Manažment rizika
[12] SAVI 4.0, Reference manual, Sandia National Laboratories
[13] *A Risk Assessment Methodology (RAM) for Physical Security.* 2005. Sandia Corporation, White Paper.
[14] FM 3-19.30: Physical Security, 2001, Headquarters, Department of the Army, USA , 317 s.
[15] Analýza účinnosti systému bezpečnostní ochrany jaderných zařízení a jadrných materiálu, 1991, Ústav jaderných informácí
[16] Joint Conflict and Tactical Simulation (JCATS) at Sandia National Laboratories, Fact Sheet, Sandia National Laboratories, 11/2006, SAND2006-7256P
[17] The OneSAF Testbed Baseline SAF Puts Added Simulation Capabilities Into Users' Hands. Pamela Bowers. IN: CrossTalk, The Journal of Defense Software Engineering. Júl 2003.
[18] OneSAF. Program Overview, John R. "Buck" Surdu. PM OneSAF. Máj 2004.
[19] McCrie R. 2001. Security Operations Management: Butterworth–Heinemann. Woburn. 429 s. ISBN 0-240-80384-1.

Recenzent - Reviewer - Рецензент:

Artykuł recenzowany przez dwóch niezależnych recenzentów – wykaz na rewersie strony tytułowej.

An article reviewed by two independent critics – see a list on the back of the title page.

Статья, оценивается двумя независимым рецензентами - перечень на обороте заглавного листа.