NÁVRH MODELU NA HODNOTENIE ÚČINNOSTI FYZICKEJ BEZPEČNOSTI

Vaculík Juraj [1], Loveček Tomáš [2]

ABSTRAKT

Článok opisuje návrh modelu na hodnotenie účinnosti bezpečnosti objektu, ktorý by sa uplatnil predovšetkým pri projektovaní rozsiahlych bezpečnostných systémov určených na ochranu osôb a majetku. Možno vytýčiť dva základné ciele, ktorých naplnenie očakávame od vytvorenia modelu : účinná ochrana chráneného záujmu a optimalizácia vynaložených prostriedkov na zabezpečenie.

Kľúčové slová:
Bezpečnostný systém, účinnosť bezpečnostného systému.

ABSTRACT

The article describes a draft of model for measuring of efficiency of physical protection system. This draft of model is supposed to be used mostly for evaluation of medium to large vital areas and security systems that are designed for protection of property and tangible assets. We can describe two main objectives that can be done with such simulation of physical protection system: to effectively design physical protection system and to optimize financial costs spent on security.

Key words:
Physical protection system, efficiency of physical protection system.

1 ZÁKLADNÉ POJMY

Účinnosť bezpečnostného systému vyjadruje vzťah reálnych procesov v bezpečnostnom systéme k ideálnym procesom, pričom iba ideálnymi procesmi sa rozumie úplná eliminácia rizík, ktoré boli identifikované a proti ktorým bol

[1] Ing. Juraj Vaculík, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, Ul. 1.mája 32, 01026 Žilina, Tel.: +421415136669, email: juraj.vaculik@fsi.uniza.sk
[2] doc. Ing. Tomáš Loveček, PhD., Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, Ul. 1.mája 32, 01026 Žilina, Tel.: +421415136664, email: tomas.lovecek@fsi.uniza.sk

bezpečnostný systém projektovaný. Bezpečnostný systém všeobecne predstavuje nástroj na tvorenie a uskutočňovanie bezpečnostnej politiky.[4] Popisovaný model sa zaoberá problematikou fyzického zabezpečenia objektu, teda pod pojmom bezpečnostný systém budeme rozumieť opatrenia vykonané na úseku fyzickej bezpečnosti. Jednou z hlavných úloh fyzickej bezpečnosti je ochrániť objekt pred útokom narušiteľa, čo v podmienkach fyzickej bezpečnosti znamená predovšetkým potrebu maximalizovať pravdepodobnosť detekcie narušiteľa v chránenom priestore a zdržať narušiteľa čo najdlhší čas v chránenom priestore, teda až do príchodu zásahovej jednotky.

Z hľadiska hodnotenia účinnosti sa javí ako kľúčová znalosť dĺžky času prekonávania najkratšej cesty narušiteľa k rozličným aktívam a rovnako tak cesta, ktorá je minimálna z hľadiska kumulatívnej pravdepodobnosti detekcie narušiteľa.[1]

Za hlavné parametre účinnosti bezpečnostného systému možno označiť nasledujúce hodnotiace kritéria :

- kumulatívna pravdepodobnosť detekcie narušiteľa,
- koeficient účinnosti ochranných opatrení.

Kumulatívna pravdepodobnosť detekcie sa používa v prípadoch, kedy páchateľ prechádza niekoľkými detekčnými zónami s rôznou pravdepodobnosťou detekcie. [2] Koeficient účinnosti ochranných opatrení vychádza zo vzťahu medzi celkovým časom napadnutia narušiteľom od momentu detekcie a celkovým časom reakcie zásahovej jednotky.

Cieľom našej snahy je navrhnutie modelu, ktorý by sa uplatnil pri hodnotení a projektovaní rozsiahlych bezpečnostných systémov určených na ochranu osôb a majetku. Možno vytýčiť dva základné ciele, ktorých naplnenie očakávame od vytvorenia modelu :

- naprojektovanie bezpečnostného systému takým spôsobom, aby aj najhoršie chránené cesty útoku narušiteľa dosahovali uspokojivú ochranu (aj čo sa týka celkového času útoku páchateľa a súčasne aj kumulatívnej pravdepodobnosti jeho detekcie),
- optimalizácia vynaložených prostriedkov na zabezpečenie, čo sa v praxi prejavuje predovšetkým tým, že ak sú útoky rôznymi spôsobmi rovnako pravdepodobné, tak aj ochrana rôznych ciest musí byť rovnako účinná, nakoľko narušiteľ aj tak pravdepodobne selektívne vyberie najzraniteľnejší spôsob útoku.

2 VLASTNOSTI MODELU

Samotný model bude reprezentovaný hranovo ohodnoteným sieťovým grafom. Z pohľadu hodnotenia účinnosti celého bezpečnostného systému je neakceptovateľné zamerať sa iba na určitú kombináciu dvoch vrcholov (počiatočného a koncového) a hodnotiť účinnosť bezpečnostného systému akýmikoľvek výpočtami vykonávanými

nad touto dvojicou, ale je nevyhnutné vykonávať výpočty nad všetkými možnými počiatkami (prístupovými zónami) a všetkými koncovými bodmi, pričom cieľovým vrcholom, ktorý je stredobodom útoku páchateľa, môže byť teoreticky akýkoľvek vrchol s nenulovou hodnotou chráneného záujmu. To zodpovedá faktu, že u mnohých objektov je chránený záujem rozmiestnený v mnohých zónach, ktoré môžu byť geograficky vzdialené a predsa sú chránené jedným bezpečnostným systémom. [6] Zároveň je to nevyhnutné pre optimalizovanie bezpečnostného systému.

Jednotlivé výpočty je účelné zapisovať v tabuľkovej forme. Nemá zmysel počítať cesty medzi prístupovými zónami, nakoľko prístupové zóny nie sú pod kontrolou organizácie, ktorá zabezpečuje prevádzku bezpečnostného systému, takže riešenie problému nájdenia prechodu z jednej prístupovej zóny do inej s požiadavkou na najmenší odpor má vždy triviálne riešenie, ktoré spočíva v úplnom vylúčení celého bezpečnostného systému.

Účelné je zameriavať sa na dva druhy ciest :

- Najrýchlejšie cesty (najrýchlejšie pre páchateľa), teda cesty do rôznych zón s čo najnižším súčtom časov na prekonanie všetkých mechanických zábranných prostriedkov a iných prekážok a časov zdržania sa v zónach,
- Cesty s najnižšou kumulatívnou pravdepodobnosťou detekcie páchateľa, teda cesty do jednotlivých zón s čo najnižšou hodnotou kumulatívnej pravdepodobnosti detekcie.

Sieťový graf by mal obsahovať nesledujúce informácie :

- pravdepodobnosť detekcie páchateľa v každej zóne,
- zdržanie pri prechode zónou / pri pôsobení v zóne (čas presunu, čas útoku v zóne),
- hodnota chráneného záujmu v každej zóne,
- pravdepodobnosť detekcie pri prekonávaní MZP,
- zdržanie pri prekonávaní MZP (najmä prielomová odolnosť), múrov a stien.

Zónou sa chápu predovšetkým jednotlivé miestnosti a sekcie objektu, časti vonkajšieho areálu chránené rovnakým spôsobom (vonkajšími PIR, CCTV, alebo aj bez ochrany) alebo podľa uváženia môže byť samostatnou zónou napr. aj trezor.

3 HODNOTENIE ÚČINNOSTI

Podľa fyzickej bezpečnosti môžeme hodnotiť účinnosť bezpečnostného systému dvoma spôsobmi :

1. relatívne (porovnávaním medzi sebou) - či platí, že cesty s vyšším kumulatívnym chráneným záujmom sú z hľadiska doby útoku a pravdepodobnosti detekcie páchateľa lepšie zabezpečené ako cesty s menšou hodnotou CHZ, teda či boli finančné prostriedky vynaložené účelne alebo je bezpečnostný systém naprojektovaný bez prihliadnutia na rozmiestenie chráneného záujmu.

2. absolútne (pevne stanovenou hodnotou)
    - či najnižšia kumulatívna pravdepodobnosť detekcie narušiteľa pri každej zóne z každej prístupovej zóny je vždy vyššia ako určitá pevne daná hodnota,
    - či najnižší koeficient kvality ochranných opatrení pre každú zónu z každej prístupovej zóny je vyšší ako určitá pevne daná hodnota,
    - či kumulatívna pravdepodobnosť detekcie v kritickom bode detekcie na najrýchlejších cestách do všetkých zón prekračuje vždy stanovenú hodnotu.

3.1 POPIS ABSOLÚTNEHO HODNOTENIA BEZPEČNOSTNÉHO SYSTÉMU

Pre vykonanie absolútneho hodnotenia je potrebné nájsť tieto dve cesty v sieťovom grafe pre každú vnútornú zónu s nenulovým chráneným záujmom :

- najrýchlejšiu cestu (z akejkoľvek prístupovej zóny)
- cestu s najnižšou kumulatívnou pravdepodobnosťou detekcie (z akejkoľvek prístupovej zóny).

Pri riešení tohto problému možno použiť osvedčené algoritmy pre hľadanie najkratšej cesty v grafoch. Po úvodných výpočtoch možno prikročiť k absolútnemu hodnoteniu účinnosti bezpečnostného systému. Výsledky je účelné zapisovať v tabuľkovej forme podľa preddefinovanej šablóny, čím sa dá vyhnúť chaosu, ktorý by mohol inak vzniknúť.

Tab. 1 znázorňuje príklad takejto šablóny pre absolútne hodnotenie bezpečnostného systému. Do riadkov tabuľky je vhodné písať jednotlivé vnútorné zóny a do stĺpcov vkladať nasledujúce informácie :

- Kumulatívnu pravdepodobnosť detekcie na najrýchlejšej ceste,
- Koeficient kvality ochranných opatrení na najrýchlejšej ceste,
- Kumulatívnu pravdepodobnosť detekcie na ceste s najnižšou kumulatívnou pravdepodobnosťou detekcie,
- Koeficient účinnosti ochranných opatrení na ceste s najnižšou kumulatívnou pravdepodobnosťou detekcie.

Tabuľka 1 Absolútne hodnotenie účinnosti bezpečnostného systému

Cesta	Najrýchlejšia		Najnižšie KP(D)	
Zóna	KP(D)	Q	KP(D)	Q
1	a1	b1	c1	d1
2	a2	b2	c2	d2
...	...	...	...	...

3.2 INTERPRETÁCIA VÝSLEDKOV ABSOLÚTNEHO HODNOTENIA

Pri nízkom počte jednotlivých zón je hodnotenie účinnosti bezpečnostných opatrení intuitívne a jednoduché, ale pri vyššom počte zón môže predstavovať zdanlivý nadbytok informácií o bezpečnostnom systéme problém. Preto je potrebné zadefinovať jasné a zrozumiteľné pravidlá, podľa ktorých sa budú interpretovať výsledky absolútneho hodnotenia účinnosti bezpečnostného systému. Najdôležitejšie je samozrejme nájsť minimum spomedzi všetkých hodnôt v tabuľke a porovnať, či spĺňajú minimálne kritéria. Povedzme, že by sme požadovali pevnú hodnotu pre kumulatívnou pravdepodobnosť detekcie 0,99 a pevnú hodnotu 1,3 pre koeficient účinnosti ochranných opatrení. Ak táto pevná hodnota nie je dosiahnutá, je potrebné analyzovať ďalej túto cestu – predovšetkým kumulatívny chránený záujem na celej ceste a samozrejme chránený záujem v samotnej zóne. Niekedy je akceptovateľné aj zlé zabezpečenie vnútornej zóny, ak sa v nej nenachádzajú cenné aktíva.

V zmysle absolútneho hodnotenia bezpečnostného systému by bolo možné stanoviť nejakú pevnú hranicu aj pre chránený záujem, ktorý sme ochotný ponechať bez relevantného zabezpečenia, prípadne riešiť tento problém zložitejším spôsobom. Napríklad, akceptovateľný koeficient účinnosti ochranných opatrení a kumulatívnu pravdepodobnosť detekcie by mohli byť rôzne pre rozličné hodnoty chráneného záujmu v príslušnej zóne. Vhodnou by mohla byť napríklad lineárna závislosť medzi týmito hodnotami a chráneným záujmom.

3.3 POPIS RELATÍVNEHO HODNOTENIA BEZPEČNOSTNÉHO SYSTÉMU

Relatívne hodnotenie, na rozdiel od absolútneho, vychádza z porovnania jednotlivých ciest medzi sebou. Tab.2 znázorňuje príklad relatívneho hodnotenia objektu. Cesty sa do tabuľky zoradia podľa druhého stĺpca, v ktorom sa nachádza kumulatívny chránený záujem. Do tohto stĺpca sa pre každú zónu vkladá menšia hodnota spomedzi dvoch hodnôt :

- Kumulatívnej hodnoty chráneného záujmy na najrýchlejšej ceste do príslušnej zóny (výsledná hodnota tejto cesty je v treťom stĺpci tabuľky),
- Kumulatívnej hodnoty chráneného záujmu na ceste s najnižšou hodnotou kumulatívnej pravdepodobnosti detekcie (výsledná hodnota tejto cesty je v štvrtom stĺpci tabuľky).

Tabuľka 2 Relatívne hodnotenie účinnosti bezpečnostného systému

Zóna	Kumulatívny chránený záujem	Najnižší kumulatívny čas	Najnižšia kumulatívna pravdepodobnosť detekcie
x1	a1	b1	c1
x2	a2	b2	c2
...	...	...	...

3.4 INTERPRETÁCIA VÝSLEDKOV RELATÍVNEHO HODNOTENIA

Ak máme n zón a postupnosť čísel v stĺpci s kumulatívnym CHZ (ktorý je utriedený) označíme $a_1..a_n$, postupnosť čísel v stĺpci s kumulatívnym časom ako $b_1..b_n$ a postupnosť čísel s kumulatívnou pravdepodobnosťou detekcie ako $c_1..c_n$, tak potom relatívne hodnotenie pozostáva zo zisťovania toho, či platí nasledujúci vzťah:

$(a_i>=a_{i+1})$ $(b_i>=b_{i+1})$ a súčasne $(a_i>=a_{i+1})$ $(c_i>=c_{i+1})$, pre i=1..n.

4 MOŽNOSTI SOFTVÉROVÉHO RIEŠENIA ZALOŽENÉHO NA DANOM MODELY

Softvérové riešenie hodnotenia účinnosti bezpečnostného systému by zahrňovalo nasledujúce možnosti :

- Možnosť voľby nástrojov páchateľa pre prekonávanie múrov a stien,
- Možnosť voľby nástrojov narušiteľa pre prekonávanie MZP,
- Kontrolu možnosti pokrytia celej zóny zvoleným detekčným prvkom,
- Možnosť nastavenia pevných hodnôt pre absolútne hodnotenie účinnosti,
- Približná kalkulácia nákladov na zakúpenie použitých komponentov,
- Možnosť využitia softvéru pri projektovaní aj hodnotení systémov.

LITERATÚRA

[1] HAMMER C. 1992. Tactics and Techniques for bypassing alarms and defeteing locks: Paladin Press. 107 p. ISBN 0-87364-686-6

[2] LOVEČEK T., NAGY P. 2008. Kamerové bezpečnotsné systémy: Edis - vydavateľstvo Žilinskej univerzity. 283 p. ISBN 978-80-8070-893-1

[3] PETRUZZELLIS T. 1994. Alarm, Sensor & Security Circuit Cookbook: TAB Books. 296 p. ISBN 0-8306-4314-1

[4] SMIETAN I. 1997. Perimeter Security Sensor Technologies Handbook: Defense Advanced Research Projects Agency (DARPA). 108 p.

[5] YEAGER W. B. 1990 Techniques of safecracking: Loompanics Unlimited. 88 p. ISBN 1-55950-052-2

[6] FM 3-19.30 : Physical Security, 2001, Headquarters, Department of the Army, USA, 317 p.

Článok recenoval:
prof. Ing. Josef Reitšpís, PhD.