Marek SZULIM[1], Katarzyna CIOSK[2], Marek KUCHTA[1], Jacek PAŚ[1]

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych (1),
Politechnika Świętokrzyska, Wydział Elektrotechniki, Automatyki i Informatyki, Katedra Informatyki, Elektroniki i Elektrotechniki (2)

doi:10.15199/48.2016.01.15

Błąd metody oszacowania skuteczności systemu ochrony fizycznej obiektu

Streszczenie. *W pracy przedstawiono model matematyczny błędu metody oceny skuteczności systemu ochrony fizycznej obiektu. Przyjęto, że różnica czasu działań ochronnych i czasu działań przeciwnika jest zmienną losową, której wartość dystrybuanty w zerze określa prawdopodobieństwo skutecznej ochrony obiektu. Zaprezentowano wyniki obliczeń błędu dla wybranych rozkładów zmiennej losowej.*

Abstract*. The paper presents a mathematical model of error of the evaluation method of the effectiveness of the object's physical protection system. It was assumed that the difference between protection actions time and enemy actions time is a variable whose distribution function value at zero determines probability of object's effective protection. Results of the error calculation for selected distributions of random variable were presented.* ***(Error of the evaluation method of the effectiveness of object's physical protection system)***

Słowa kluczowe: system ochrony fizycznej, ocena, skuteczność, błąd.
Keywords: physical protection system, assess, effectiveness, error.

Wprowadzenie

System ochrony fizycznej, odgrywa pierwszoplanową rolę w zapewnieniu właściwego poziomu bezpieczeństwa obiektów infrastruktury krytycznej - zwłaszcza obiektów jądrowych [1].

System ten obejmuje szereg przedsięwzięć natury organizacyjnej oraz technicznej. Do tych pierwszych należy w szczególności powołanie służby ochrony oraz określenie: sposobu rozmieszczenia środków zabezpieczających, sposobu ich funkcjonowania i współdziałania, sposobu postępowania w przypadku kradzieży, aktów terroru, dywersji i sabotażu oraz innych zagrożeń. Natomiast do przedsięwzięć technicznych, zalicza się w szczególności stosowanie: środków zabezpieczających obszar chroniony przed dostępem osób nieupoważnionych, głownie środków mechanicznych i budowlanych; elektronicznych urządzeń, w tym systemów alarmowych sygnalizujących zagrożenie oraz systemów służących do obserwacji i rejestracji. Właściwa realizacja przedsięwzięć organizacyjnych i technicznych, wymaga uwzględnienia lokalizacji oraz funkcjonowania chronionego obiektu.

System ochrony fizycznej powinien przede wszystkim zapewnić wykrywanie i zapobieganie aktom terroru, kradzieżom, dywersji i sabotażu. By mieć przekonanie, że spełnia swe zadania i zapewnia odpowiedni poziom ochrony obiektu - konieczna jest ocena jego skuteczności.

Ocena skuteczności

Proponowane są różne metody analizy i oceny systemu ochrony fizycznej obiektu. Istnieją metody uwzględniające ilość informacji, jaką system jest w stanie dostarczyć [2], wykorzystujące teorię gier [3]. Jednak najpopularniejsza jest reprezentująca podejście probabilistyczne, opracowana przez Sandia National Laboratories metoda EASI (Estimate of Adversary Sequence Interruption) [4, 5, 6].

Ciągle rozbudowywana [7] Metoda EASI stanowi punkt odniesienia dla innych rozwiązań [8] i jest podstawą szkoleń służb ochrony [9]. Korzystając z tej metody można wyznaczyć prawdopodobieństwo skuteczności systemu [10] oraz określić tzw. CDP (Critical Detection Point) – ostatnie miejsce na drodze napastnika, w którym jeśli system ochrony wykryje jego obecność, siły reagowania mogą zatrzymać napastnika jeszcze przed zakończeniem ataku.

Jest rzeczą oczywistą, że każda metoda ilościowej oceny skuteczności – jak każde narzędzie - oprócz zalet, posiada również wady. Z punktu widzenia użytkownika odpowiedzialnego za osiągnięcie (podczas projektowania systemu) bądź podniesienie (w trakcie jego modernizacji) odpowiedniego poziomu bezpieczeństwa chronionego obiektu, niewątpliwie kluczowe jest, by uzyskany za pomocą danego narzędzia wynik oceny był najbliższy wynikowi prawdziwemu. Istotne jest zatem, by narzędzie służące do oceny skuteczności systemu ochrony fizycznej, samo objęte było oceną dokładności. Ponieważ, podobnie jak *skuteczność*, pojęcie *dokładności* ma charakter jakościowy - niezbędne staje się dysponowanie miarą ilościową niedokładności (błędem, niepewnością) metody oceny skuteczności.

Powyższe rozważania wskazują, że narzędzie oferujące kompletny zestaw trzech instrumentów pozwalających na wyznaczenie prawdopodobieństwa skuteczności ochrony, niepewności oceny skuteczności oraz błędu metody oceny skuteczności, posiadałoby wielce pożądane walory użytkowe. Niestety, trudno znaleźć opracowanie dotyczące oszacowania niepewności bądź błędu prawdopodobieństwa skuteczności systemu wyznaczanego zgodnie z AESI, Podobna sytuacja występuje w przypadku pozostałych wspomnianych metod.

Zdaniem autorów niniejszej pracy, zagadnienie oceny skuteczności systemu można sprowadzić do procesu pomiaru i korzystając z ujęcia metrologicznego problemu, sformułować nowe uniwersalne narzędzie. Stąd też, pierwszym krokiem było wykorzystanie teorii niepewności do wyznaczania współczynnika skuteczności [11, 12]. Kolejnym, zastosowanie metody Monte Carlo do opracowania drugiego instrumentu – procedury szacowania złożonej niepewności standardowej współczynnika skuteczności oraz przedziału rozszerzenia dla założonego prawdopodobieństwa rozszerzenia [13]. Ostatni brakujący instrument – błąd metody – proponuje się opracować korzystając z teorii (rachunku) błędu.

Współczynnik skuteczności

Rozpatrując dowolny scenariusz ataku, dopuszczalne jest uznanie systemu ochrony fizycznej obiektu za skuteczny jedynie wówczas, gdy napastnik zostanie zatrzymany przez siły reagowania przed osiągnięciem celu ataku. Innymi słowy czas działania systemu ochrony (liczony od chwili ataku do chwili ujęcia napastnika) musi być krótszy niż czas jaki musi upłynąć, by napastnik zrealizował swój cel na terenie obiektu. Wprowadzając dodatkowo parametr ΔT, będący różnicą czasu działań systemu ochrony i czasu działań przeciwnika, otrzymuje się następujące zależności:

(1) $$\Delta T = \sum_{i=1}^{N} T_{Si} - \sum_{l=1}^{L} T_{Dl} \ ,$$

(2) $$\Delta T < 0 \ ,$$

gdzie: N – liczba elementów systemu aktywnych od chwili ataku do zakończenia działań sił reagowania, T_{Si} – czas działania i-tego elementu systemu, L – liczba niezbędnych działań przeciwnika od chwili ataku do osiągnięcia założonego celu, T_{Dl} – czas l-tego działania przeciwnika.

Zgodnie z teorią niepewności [14], równanie (1) jest modelem pomiaru, a wszystkie wielkości wejściowe T_{Si}, T_{Dl} są zmiennymi losowymi. Zatem wielkość wyjściowa ΔT jest także zmienną losową o swoim własnym rozkładzie.

Uwzględniając zależność (2) opisującą zasadę skutecznej interwencji oraz przyjmując, że rozkład wielkości ΔT opisuje funkcja gęstości prawdopodobieństwa $p(\Delta T)$, można zdefiniować współczynnik skuteczności [11, 12, 13]

(3) $$K_S = \int_{-\infty}^{0} p(\Delta T)\, d\Delta T \ ,$$

wyrażający prawdopodobieństwo skuteczności systemu.

Przy czym, estymatę wartości oczekiwanej zmiennej losowej ΔT, oznaczoną przez μ, oblicza się z równania (1) dla estymat wartości oczekiwanych t_{Si}, t_{Dl} wielkości wejściowych, jako

(4) $$\mu = \sum_{i=1}^{N} t_{Si} - \sum_{l=1}^{L} t_{Dl}$$

Natomiast, estymatę odchylenia standardowego, daną przez σ, oblicza się zgodnie z prawem propagacji niepewności dla estymat odchyleń standardowych $u(t_{Si})$, $u(t_{Dl})$ wielkości wejściowych, stąd

(5) $$\sigma = \left| \sqrt{\sum_{i=1}^{N} u^2\left(t_{Si}\right) + \sum_{l=1}^{L} u^2\left(t_{Dl}\right)} \right|$$

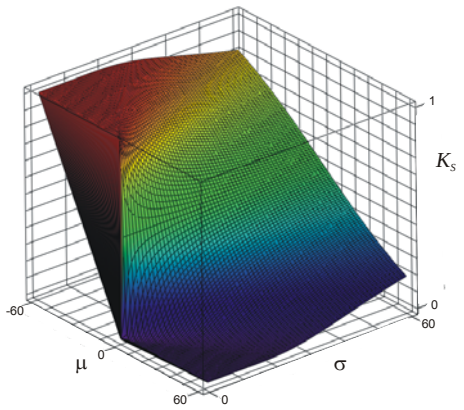
Posiadanie informacji o wartościach parametrów opisowych zmiennej losowej ΔT jest cenne ($\mu < 0$ oznacza skuteczną interwencję), jednak niewystarczające do obliczenia współczynnika skuteczności. Konieczna jest tutaj znajomość funkcji gęstości prawdopodobieństwa $p(\Delta T)$ wielkości wyjściowej.

Ponieważ wielkość wyjściowa jest sumą wielkości wejściowych, to rozkład ΔT często, na mocy centralnego twierdzenia granicznego, można aproksymować rozkładem normalnym, nawet jeśli rozkłady wielkości wejściowych nie są normalne. Twierdzenie to orzeka bowiem, że rozkład ΔT będzie w przybliżeniu normalny z wartością oczekiwaną μ i odchyleniem standardowym σ, jeśli σ jest dużo większe niż jakiekolwiek pojedyncze $u(t)$ wielkości wejściowej mającej inny rozkład niż rozkład normalny [14].

Opierając się na centralnym twierdzeniu granicznym, rozkład ΔT aproksymuje się rozkładem normalnym - co oznacza, że równanie (3) przyjmuje postać

(6) $$K_S = \int_{-\infty}^{0} \left(\frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(\Delta T-\mu)^2}{2\sigma^2}} \right) d\Delta T$$

Zależność wartości współczynnika skuteczności od rozważanych parametrów opisowych rozkładu wielkości wyjściowej ΔT ilustruje rysunek 1.



Rys.1. Wpływ wartości oczekiwanej μ i odchylenia standardowego σ rozkładu ΔT na wartość współczynnika skuteczności K_S

Z powyższego rysunku wynika, że zmniejszanie wartości oczekiwanej wielkości wyjściowej, prowadzi do zwiększenia prawdopodobieństwa skuteczności systemu ochrony. Widać również, że dla μ < 0, zmniejszanie wartości odchylenia standardowego wielkości wyjściowej wywołuje wzrost wartości współczynnika skuteczności, natomiast dla μ > 0 przeciwnie.

Błąd metody

Przedstawiona metoda oceny skuteczności systemu ochrony fizycznej obiektu, bazuje na założeniu, iż rozkład prawdopodobieństwa wielkości wyjściowej jest rozkładem normalnym. Współczynnik skuteczności jest wówczas równy dystrybuancie rozkładu normalnego N(μ,σ) obliczonej w zerze (6). To fundamentalne założenie może prowadzić do błędnej oceny skuteczności.

Niebezpieczna jest zwłaszcza sytuacja – przy dążeniu do zapewnienia wysokiej dokładności metody – gdy liczba wielkości wejściowych jest niewielka i jedna z nich, mając inny rozkład niż normalny, charakteryzuje się wartością odchylenia standardowego porównywalną z σ (przypadek tzw. wielkości wejściowej dominującej).

Zatem błąd metody oceny skuteczności systemu ochrony, można zdefiniować jako różnicę pomiędzy wartością współczynnika skuteczności K_S obliczoną dla rozkładu normalnego a wartością prawdziwą tego współczynnika (oznaczoną przez K_{Sreal}) określoną dla rozkładu prawdziwego zmiennej losowej ΔT, czyli

(7) $$\Delta K_S = K_S - K_{Sreal}$$

Zgodnie z teorią pomiaru [14] nie można wyznaczyć wartości (prawdziwej) błędu ΔK_S, ponieważ wartość prawdziwa współczynnika skuteczności jest ze swej natury nieznana. Można jednak zawsze określić *graniczną* odległość między znaną wartością obliczoną K_S a nieznaną wartością prawdziwą K_{Sreal}.

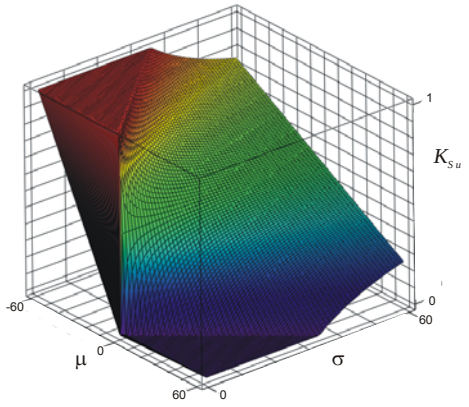
Graniczny błąd metody

Powszechnie przyjmuje się, że rozkład prostokątny jest krańcowym przykładem rozkładu odbiegającego od normalnego [14]. Oznacza to, że wartości współczynnika skuteczności obliczone dla rozkładu ΔT aproksymowanego rozkładem prostokątnym będą krańcowo różne od tych obliczonych za pomocą zależności (6). Stąd też, uzasadnione wydaje się założenie, że graniczny błąd metody ΔK_{Smax}, można wyznaczyć, gdy wartość K_{Sreal} będzie reprezentowana przez współczynnik skuteczności K_{Su} obliczony dla rozkładu prostokątnego, czyli

(8) $$\Delta K_{S\,max} = K_S - K_{Su}$$

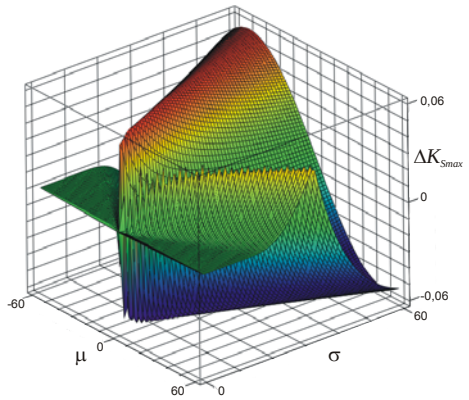
(9) $$K_{Su} = \begin{cases} 0 & dla \quad \Delta T < \left(\mu - \sigma\sqrt{3}\right) \\ \frac{1}{2} - \frac{\mu}{\sigma 2\sqrt{3}} & dla \quad \left(\mu - \sigma\sqrt{3}\right) \le \Delta T \le \left(\mu + \sigma\sqrt{3}\right) \\ 1 & dla \quad \Delta T > \left(\mu + \sigma\sqrt{3}\right) \end{cases}$$

Zależność wartości współczynnika skuteczności K_{Su} od rozważanych parametrów opisowych rozkładu ΔT ilustruje rysunek 2. Już nawet pobieżne porównanie rysunku 2 z rysunkiem 1 wskazuje, na identyczny wpływ μ oraz σ na obydwa współczynniki (K_{Su} i K_S).



Rys.2. Wpływ wartości oczekiwanej μ i odchylenia standardowego σ rozkładu ΔT na wartość współczynnika skuteczności K_{Su}

Na rysunku 3 przedstawiono natomiast, kluczowy dla niniejszej pracy, wykres powierzchniowy granicznego błędu metody. Okazuje się, że w żadnym przypadku wartość bezwzględna tego błędu nie przekroczy 0,06.



Rys.3. Wpływ wartości oczekiwanej μ i odchylenia standardowego σ rozkładu ΔT na wartość granicznego błędu metody ΔK_{Smax}

Podsumowanie

Zaprezentowany model matematyczny błędu metody oceny skuteczności systemu ochrony fizycznej można traktować jako ostatni brakujący instrument do pełnego skompletowania narzędzia oceny systemu. Możliwe staje się już udzielenie odpowiedzi na pytanie, nie tylko jakie jest prawdopodobieństwo, że oceniany system ochrony wykona stawiane mu zadanie, ale również jaki jest maksymalny błąd oszacowania tego prawdopodobieństwa.

Przedstawione wyniki symulacji jednoznacznie wskazują, że współczynnik skuteczności (6) jest solidnym instrumentem oceny prawdopodobieństwa skuteczności systemu. Wykluczona została bowiem sytuacja, w której system niezapewniającego właściwej ochrony może zostać uznany za skuteczny. Graniczny błąd metody osiąga niewielką wartość maksymalną ($\Delta K_{Smax} \cong 0{,}06$) i to tylko dla systemów posiadających wysoką wartość współczynnika skuteczności (na poziomie 0,69), co raczej nie prowadzi do poważnych konsekwencji.

Powyższe rozważania, zdają się uzasadniać przekonanie, że zaproponowano instrument użyteczny przy ocenie systemu ochrony fizycznej.

***Autorzy**: dr inż. Marek Szulim, Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa 49, E-mail: marek.szulim@wat.edu.pl; dr inż. Katarzyna Ciosk, Politechnika Świętokrzyska, Wydział Elektrotechniki, Automatyki i Informatyki, Katedra Informatyki, Elektroniki i Elektrotechniki, Al. Tysiąclecia Państwa Polskiego 7, 25-314 Kielce, E-mail: k.ciosk@tu.kielce.pl; dr hab. inż. Marek Kuchta, Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa 49, E-mail: marek.kuchta@wat.edu.pl; dr inż. Jacek Paś, Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa 49, E-mail: jacek.pas@wat.edu.pl,*

LITERATURA

[1] Rozporządzenie Rady Ministrów z dnia 4 listopada 2008 r. w sprawie ochrony fizycznej materiałów jądrowych i obiektów jądrowych, Dz.U. 2008 nr 207 poz. 1295.
[2] Dai J. et al., Benefit-cost analysis of security systems for multiple protected assets based on information entropy, *Entropy*, 14 (2012), 571-580.
[3] Zhuang J., Bier V.M., Alagoz O., Modeling secrecy and deception in a multiple-period attacker-defender signaling game, *European Journal of Operational Research*, 203 (2010), 409–418.
[4] Garcia M. L., Vulnerability assessment of Physical Protection Systems, Second Edition, *Elsevier Butterworth–Heinemann*, Burlington, 2006.
[5] Garcia M. L., The Design and Evaluation of Physical Protection Systems, Second Edition, *Elsevier Butterworth–Heinemann*, Burlington, 2008.
[6] Fennelly L.J., Effective Physical Security, Fourth Edition, *Elsevier Butterworth–Heinemann*, Burlington, 2013.
[7] Terao N., Suzuki M., A Probabilistic Extension of the EASI Model, *Journal Of Physical Security*, 7 (2014), n 2, 12-29.
[8] Bassam S., Herrmann J.W., Schmidt L.C., Using SysML for model-based vulnerability assessment, *Procedia Computer Science*, 44 (2015), 413 – 422.
[9] Anti-Terrorism Officer (ATO) Course, *S2 Safety & Intelligence Institute/International Association of Counterterrorism and Security Professionals*, 19-22 May 2015, Den Haag.
[10] Evaluation of the effectiveness of the physical protection system of nuclear facilities (with the exemption of those operating reactor having less than 1 MW thermal power), and radioactive waste temporary storage and final disposal facilities, *Hungarian Atomic Energy Authority*, Budapest 2011.
[11] Szulim M. i inni, Zastosowanie teorii niepewności do oceny skuteczności systemu bezpieczeństwa obiektu, *Biuletyn WAT*, LVII (2008), nr 2, 389÷396.
[12] Szulim M., Kuchta M., Metoda analizy skuteczności systemu bezpieczeństwa obiektu, *Biuletyn WAT*, LIX (2010), nr 4, 111÷121.
[13] Szulim M., Ciosk K., Kuchta M., Dukata A., Niepewność oceny skuteczności systemu bezpieczeństwa obiektu, *Przegląd Elektrotechniczny*, 90 (2014), nr 2, 182 – 185.
[14] Evaluation of measurement data — Guide to the expression of uncertainty in measurement, JCGM 100:2008, *Joint Committee for Guides in Metrology*, 2008.