EKONOMICZNIE OPTYMALNE KOSZTY UTRZYMANIA ZABEZPIECZEŃ W SYSTEMIE OCHRONY INFORMACJI

Karol KREFT

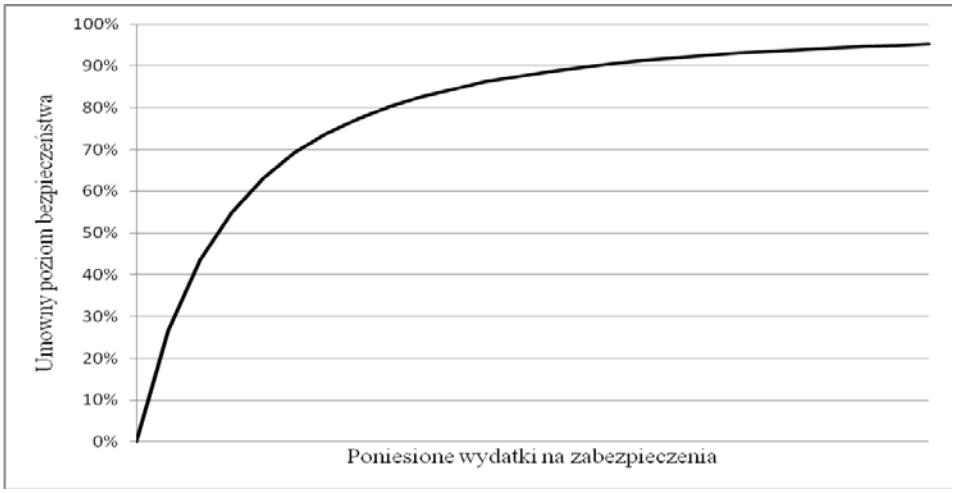
Streszczenie: Celem artykułu jest prezentacja opracowanej przez autora metody znajdywania optymalnej wielkości ryzyka ze względu na koszty utrzymania zabezpieczenia. W dostępnej literaturze opisuje się metody pomiaru i redukcji ryzyka, jednak nigdzie nie określa się w sposób poprawny poziomu ryzyka, przy którym system jest optymalnie, ze względów ekonomicznych, zabezpieczony.

Słowa kluczowe: bezpieczeństwo, efektywność kosztowa, koszty utrzymania zabezpieczenia, ryzyko.

1. Wstęp

W artykule autor przedstawi swoje nowatorskie podejście do optymalnego poziomu kosztów utrzymania zabezpieczenia na tle spotykanego w literaturze pojęcia efektywności kosztowej SCE (Safeguard Cost Efficiency).

Analiza ekonomiczna i zarządzanie ryzykiem jest istotnym elementem w procesie optymalizacji systemu bezpieczeństwa. Z punktu widzenia analizy ekonomicznej przy tworzeniu sytemu ochrony informacji należy uwzględnić koszty utrzymania zabezpieczenia, które podnoszą bezpieczeństwo.



Rys. 1. Zależność między umownym poziomem bezpieczeństwa a poniesionymi wydatkami na zabezpieczenia

Źródło: opracowanie własne na podstawie Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwo Naukowo-Techniczne, Warszawa 2007, s.359

Strategii transferowania ryzyka (ubezpieczenie się od utraty systemu informacyjnego) na instytucję ubezpieczającą nie można zrealizować bez pewnych obwarowań (w praktyce wymagana jest instalacja zabezpieczeń redukujących ryzyko) i takie rozwiązanie powinno się uznać za „uzupełniające".

Nie jesteśmy w stanie zbudować idealnie zabezpieczonego systemu informacyjnego, możemy jedynie poprzez ponoszenie wydatków na zabezpieczenia podnosić poziom bezpieczeństwa.

W przypadku systemu informatycznego wielkość ryzyka jest zależna od:

- wartości chronionego zasobu,
- prawdopodobieństwa wystąpienia zagrożenia,
- powagi podatności,
- prawdopodobieństwa niezadziałania zabezpieczenia.

2. Efektywność kosztowa SCE (i) jako wskaźnik jakości procesu zarządzania ryzykiem

W podejściu klasycznym (Courtneya) wielkość ryzyka jest iloczynem częstości zdarzenia niekorzystnego i wielkości konsekwencji nim spowodowanych. W systemach informatycznych trudno jest zdobyć dane dotyczące częstości zdarzeń niekorzystnych.

Dla dalszych obliczeń przyjmuje się założenie, że możliwość wystąpienia zdarzenia EP(i) (Event Possibility) zależna jest od powagi podatności VS(i) i powagi zagrożenia TS(i). Tak więc iloczyn powagi zagrożenia wyrażającej częstość zdarzenia inicjującego oraz powagi podatności wyrażającej prawdopodobieństwo niezadziałania zabezpieczenia, szacuje możliwość wystąpienia zdarzenia EP(i).

$$EP(i) = \frac{VS(i) * TS(i)}{VS_{\max} * TS_{\max}} \tag{1}$$

gdzie:

VS(i) – powaga podatności wyrażająca prawdopodobieństwo niezadziałania zabezpieczenia (Vulnerability Severity Level),

VS_{max} –maksymalna wartość powagi podatności,

TS(i) – powaga zagrożenia wyrażająca częstość zdarzenia inicjującego (Threat Severity Level),

TS_{max} – maksymalna wartość powagi zagrożenia.

Szacowanie ryzyka jest wielokrotnie powtarzalne przy założeniu, że występują porównywalne warunki. Działania tego typu pozwolą na podejmowanie trafnych decyzji dotyczących wybory zabezpieczenia. Kolejne analizy i związane z nimi parametry cząstkowe będą oznaczone za pomocą indeksu (i), umożliwia to porównywanie scenariuszy i śledzenie wielkości ryzyka w czasie.

Efektywność zabezpieczenia SE(i+1) w literaturze jest definiowana jako:

$$SE(i+1) = EP(i) - EP(i+1) \tag{2}$$

Analizując kolejne wartości *EP(i)* oraz *EP(i+1)* można ocenić skutki działań zabezpieczających.

SE(i+1) < 0 – nastąpił wzrost ryzyka, działania obniżyły bezpieczeństwo systemu,

SE(i+1) = 0 – ryzyko nie uległo zmianie, brak wpływu działań na bezpieczeństwo systemu, *SE(i+1)* > 0 – nastąpiło obniżenie ryzyka, działania podniosły bezpieczeństwo systemu.

Jeżeli założymy, że nie mamy wpływu na powagę zagrożenia (np.: nie mamy wpływu na to jak często komputer podłączony do Internetu będzie atakowany przez szkodliwe oprogramowanie – wirusy komputerowe), to *TS(i)=TS(i+1).*
Gdy przyjmiemy założenie, że *TS(i)=TS(i+1)=TS,* to

$$SE(i+1) = \frac{VS(i) * TS(i)}{VS_{\max} * TS_{\max}} - \frac{VS(i+1) * TS(i+1)}{VS_{\max} * TS_{\max}} = \frac{TS}{VS_{\max} * TS_{\max}} (VS(i) - VS(i+1)) \quad (3)$$

Powaga podatności *VS(i)* wyrażająca prawdopodobieństwo niezadziałania zabezpieczenia opisuje skuteczność działania zabezpieczenia. W większości przypadków droższe zabezpieczenia są bardziej skuteczne. Uogólniając możemy więc powiedzieć, że VS(i) zależy od kosztu utrzymania zabezpieczenia *SC(i)* (Safeguard Cost). Rysunek 1 przedstawiający zależność miedzy poziomem bezpieczeństwa a poniesionymi wydatkami na zabezpieczenia potwierdza nasze twierdzenie.

Koszt utrzymania zabezpieczenia *SC(i)* w przypadku nabycia zabezpieczenia nie będzie kosztem zakupu zabezpieczenia, lecz wartością amortyzacji powiększoną o koszty związane z utrzymaniem zabezpieczenia.

Wielkość ryzyka wyrażona w jednostkach walutowych *RVC(i)* (Risk Value – Currency) definiowana jest następująco:

$$RVC(i) = EP(i) * AVC(i) \quad (4)$$

gdzie: *AVC(i)* to wartość chronionego zasobu wyrażona w jednostkach walutowych.

W literaturze opisane jest pojecie efektywności kosztowej *SCE(i)* (Safeguard Cost Efficiency) wyrażające adekwatność kosztów utrzymania zabezpieczenia poniesionych na redukcję ryzyka w poniższy sposób:

$$SCE(i) = RVC(i) - SC(i) \quad (5)$$

Efektywność kosztowa, tak zdefiniowana według wielu źródeł, pozwala określić optymalny poziom kosztów utrzymania zabezpieczenia.
Sugeruje się następujące zależności:

- *SCE >0* system zabezpieczony za słabo, istnieje potrzeba redukcji ryzyka, należy zwiększyć koszty utrzymania zabezpieczenia,
- *SCE =0* system idealnie zabezpieczony, optymalny poziom kosztów utrzymania zabezpieczenia,
- *SCE <0* system zabezpieczony zbyt silnie, zbyt wysokie koszty utrzymania zabezpieczenia.

Efektywność kosztowa, tak zdefiniowana w literaturze, ma za zadanie wskazać optymalne koszty (nakłady) utrzymania zabezpieczenia i pełni ona rolę wskaźnika jakości procesu zarządzania ryzykiem.

Interpretacja zdefiniowanej powyżej efektywności kosztowej w wstępnej analizie wydaje się słuszna, ponieważ koszt utrzymania zabezpieczenia nie powinien być większy niż ryzyko wyrażone w jednostkach walutowych. Oczywiste jest przecież ze względów

ekonomicznych, że nie powinno się chronić zasobów o wartości 100 PLN zabezpieczeniem, którego koszt utrzymania wynosi np. 1000 PLN.

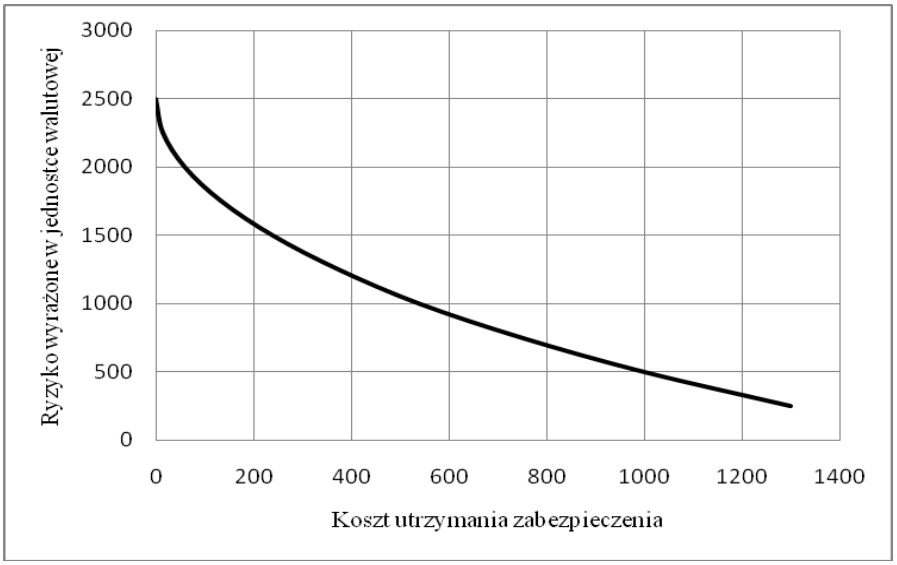
3. Krańcowy koszt utrzymania zabezpieczenia i krańcowe ryzyko wyrażone w jednostce walutowej

Według autora niniejszego artykułu tak zdefiniowana efektywność kosztowa *SCE(i)* nie może służyć do określenia optymalnych ekonomicznie kosztów utrzymania zabezpieczenia.

Posiadanie wiedzy o skuteczności zabezpieczenia (która zależy od nakładów na zabezpieczenia) jest niewystarczające do określenia optymalnych ekonomicznie kosztów utrzymania zabezpieczenia. Musimy również posiadać informację o wielkości ryzyka, które zależy także od skuteczności zabezpieczenia.

Wiemy, że większość droższych zabezpieczeń działa bardziej skutecznie. Tak więc istnieje zależność między kosztem utrzymania zabezpieczenia a prawdopodobieństwem niezadziałania zabezpieczenia – powagą podatności VS(i).

Nie jesteśmy w stanie zredukować ryzyka do zera, gdyż nie istnieją systemy idealnie zabezpieczone, ponieważ nie można wytworzyć niezawodnych urządzeń.



Rys. 2. Zależność między ryzykiem wyrażonym w jednostkach walutowych a kosztem utrzymania zabezpieczenia
Źródło: opracowanie własne

Na początku krzywej niewielkie koszty (nakłady) utrzymania zabezpieczenia powodują znaczą redukcję ryzyka wyrażonego w walucie, jednak od pewnego momentu zwiększanie kosztów (nakładów) utrzymania zabezpieczenia w niewielkim stopniu redukuje ryzyko wyrażone w jednostce walutowej.

Na problem optymalnych kosztów utrzymania zabezpieczenia należy spojrzeć z nowego punku widzenia. Poszukajmy odpowiedzi na pytanie do jakiego momentu należy zwiększać koszty utrzymania zabezpieczenia.

Tab. 1. Koszty utrzymania zabezpieczenia i ryzyko wyrażone w jednostce walutowej

Koszty utrzymania zabezpieczenia	0	15	60	135	240	375	540	750	1000	1300
Ryzyko wyrażone w jedn. walutowej	2500	2250	2000	1750	1500	1250	1000	750	500	250

Źródło: opracowanie własne.

Gdy np. koszty utrzymania zabezpieczenia zwiększamy z wartości 135 na wartość 240 to redukcja ryzyka następuje z wartości 1750 na wartość 1500. Wzrost kosztów utrzymania zabezpieczenia o wartość 105 powoduje zmniejszenie ryzyka o 250. Zmieniając koszty utrzymania zabezpieczenia w sensie ekonomicznym zyskujemy redukcję ryzyka o wartość (250-105)= 145. Takie podejście pozwala określić, jak zmiana kosztów utrzymania zabezpieczenia wpływa na redukcję ryzyka.

Autor definiuje w tym momencie pojecie krańcowego kosztu utrzymania zabezpieczenia i pojęcie krańcowego ryzyka wyrażonego w jednostce walutowej.
Krańcowy koszt utrzymania zabezpieczenia MSC (Marginal Safeguard Cost):

$$MSC(i) = SC(i+1) - SC(i) \tag{6}$$

Krańcowe ryzyko wyrażone w jednostce walutowej (Marginal Risk Valu - Currency):

$$MRVC(i) = RVC(i) - RVC(i+1) \tag{7}$$

Pojęcie krańcowego kosztu utrzymania zabezpieczenia i krańcowego ryzyka wyrażonego w jednostkach walutowych powinno być wykorzystywane do określenia optymalnego ekonomicznie kosztu utrzymania zabezpieczenia.
System optymalnie zabezpieczony ze względów ekonomicznych według autora to :

$$MSC(i) = MRVC(i) \tag{8}$$

Jeżeli krańcowy koszt utrzymania zabezpieczenia jest mniejszy niż krańcowe ryzyko wyrażone w jednostce walutowej należy zwiększać koszty (nakłady) utrzymania zabezpieczenia.

W sytuacji odwrotnej, gdy krańcowy koszt utrzymania zabezpieczenia jest większy niż krańcowe ryzyko wyrażone w jednostce walutowej należy zmniejszać koszty (nakłady) utrzymania zabezpieczenia.

4. Przykładowa analiza optymalizacji kosztów utrzymania zabezpieczenia ze względów ekonomicznych

4.1. Przedstawienie problemu

Przedsiębiorstwo rozważa zainstalowanie systemu ochrony poczty elektronicznej. Zabezpieczenie ma chronić maile przed czytaniem ich przez osoby nieupoważnione. W przypadku udostępnienia informacji, przechowywanej w poczcie elektronicznej, osobom nieupoważnionym (np. konkurencji) przedsiębiorstwo poniesie straty, które szacuje się na kwotę 5000 PLN. Na rynku dostępnych jest szereg zabezpieczeń, których skuteczność

uzależniona jest od ceny nabycia, która bezpośrednio wpływa na koszt utrzymania zabezpieczenia.

Dostępne zabezpieczenia poczty elektronicznej, ich skuteczność i koszt utrzymania zawiera tabela 2. Skuteczność zabezpieczenia E(i) wyraża prawdopodobieństwo prawidłowego zadziałania systemu bezpieczeństwa. W obliczeniach należy przyjąć, że statystycznie na dziesięć serwerów pocztowych w przypadku pięciu występuje próba ataku mającego na celu czytanie maili przez osoby nieupoważnione.

Tab. 2. Koszt utrzymania zabezpieczenia SC(i) i ich skuteczność E(i)

i	1	2	3	4	5	6	7	8	9	10
Koszty utrzymania zabezpieczenia SC(i)	0	15	60	135	240	375	540	750	1000	1300
Skuteczność zabezpieczenia E(i)	0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9

Źródło: opracowanie własne

Należy dobrać optymalne ekonomicznie zabezpieczenie poczty elektronicznej.

4.2. Kryterium wyboru optymalnego ekonomicznie zabezpieczenia SCE (i)=0

Pomiędzy skutecznością E(i) a powagą podatności VS(i) wyrażającą prawdopodobieństwo niezadziałania zabezpieczenia istnieje zależność:

$$VS(i) = 1 - E(i) \tag{9}$$

Ponieważ statystycznie na 10 serwerów pocztowych 5 jest atakowanych to powaga zagrożenia TS(i) wyrażająca częstość zdarzenia inicjującego wynosi 0,5.

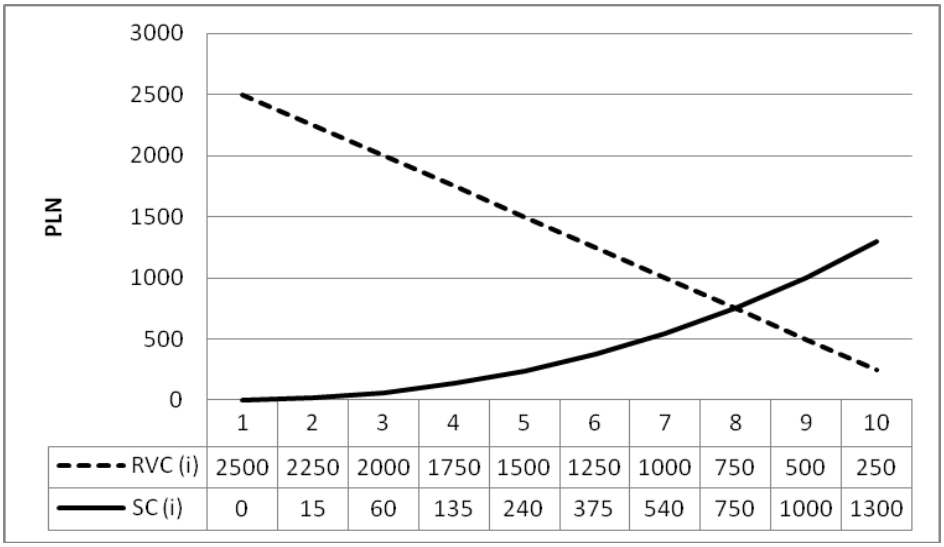
Wyniki obliczeń przeprowadzone na podstawie wzorów (1), (2), (4), (5) zamieszczono w tablicy 3.

Tab. 3. Ryzyko wyrażone w jednostce walutowej RVC (i), koszt utrzymania zabezpieczenia SC(i) oraz efektywność kosztowa SCE (i)

i	VS (i)	TS (i)	EP (i)	SE (i)	AVC (i)	RVC (i)	SC (i)	SCE (i)
1	1	0,5	0,5		5000	2500	0	2500
2	0,9	0,5	0,45	0,05	5000	2250	15	2235
3	0,8	0,5	0,4	0,05	5000	2000	60	1940
4	0,7	0,5	0,35	0,05	5000	1750	135	1615
5	0,6	0,5	0,3	0,05	5000	1500	240	1260
6	0,5	0,5	0,25	0,05	5000	1250	375	875
7	0,4	0,5	0,2	0,05	5000	1000	540	460
8	**0,3**	**0,5**	**0,15**	**0,05**	**5000**	**750**	**750**	**0**
9	0,2	0,5	0,1	0,05	5000	500	1000	-500
10	0,1	0,5	0,05	0,05	5000	250	1300	-1050

Źródło: opracowanie własne na podstawie danych z tab.2.

System idealnie zabezpieczony to system, w którym koszt utrzymania zabezpieczenia wynosi 750 PLN (i=8), gdyż SCE (8)= 0



Rys. 3. Ryzyko wyrażone w jednostce walutowej RVC (i) oraz koszt utrzymania zabezpieczenia SC (i)
Źródło: opracowanie własne

4.3. Kryterium wyboru optymalnego ekonomicznie zabezpieczenia MSC(i)=MRVC(i)

Według autora warunek SCE (i) = 0 nie określa optymalnych ekonomicznie kosztów utrzymania zabezpieczenia.

Przeanalizujmy krańcowy koszt utrzymania zabezpieczenia oraz krańcowe ryzyko wyrażone w jednostce walutowej. Wyniki przeprowadzonych obliczeń na podstawie wzorów (6), (7), (8) zamieszczono w tabeli 4.

Tab. 4. Krańcowy koszt utrzymania zabezpieczenia oraz krańcowe ryzyko wyrażone w jednostce walutowej

i	RVC (i)	SC (i)	SCE (i)	MSC (i)	MRVC (i)	MSC(i) - MRVC(i)
1	2500	0	2500			
2	2250	15	2235	15	250	235
3	2000	60	1940	45	250	205
4	1750	135	1615	75	250	175
5	1500	240	1260	105	250	145
6	1250	375	875	135	250	115
7	1000	540	460	165	250	85
8	750	750	0	210	250	40
9	**500**	**1000**	**-500**	**250**	**250**	**0**
10	250	1300	-1050	300	250	-50

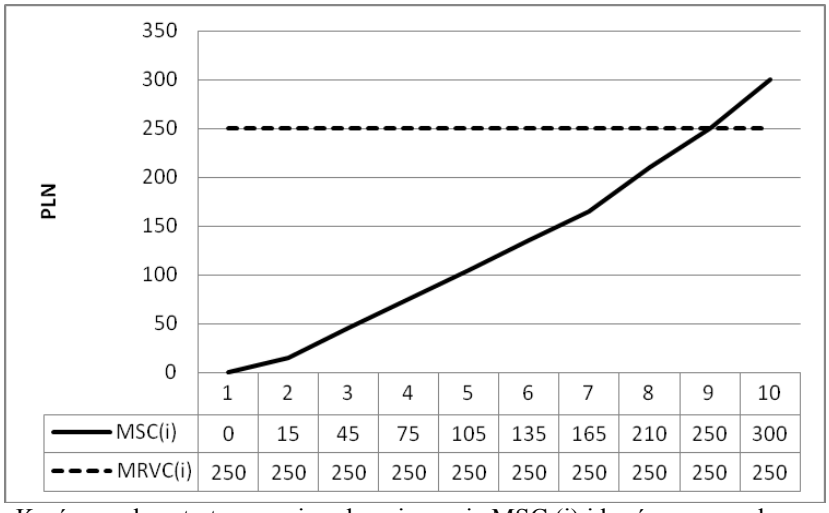
Źródło: opracowanie własne na podstawie danych z tab.2.

Gdy koszty utrzymania zabezpieczenia zwiększamy z 540 do 750, to krańcowy koszt utrzymania zabezpieczenia stanowi 210, przy krańcowym ryzyku wyrażonym w jednostce walutowej wynoszącym 250. Mamy sytuacje, gdzie MSC(8)-MRVC(8)=40, więc w sensie ekonomicznym zyskujemy 40.

Przy kolejnym zwiększeniu kosztów utrzymania zabezpieczenia z 750 do 1000, krańcowy koszt utrzymania zabezpieczenia równa sie 250, przy krańcowym ryzyku wyrażonym w jednostce walutowej wynoszącym 250.

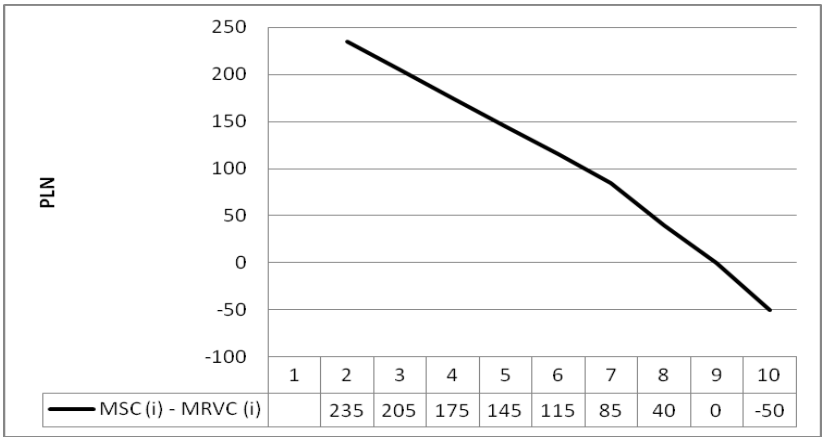
Spełniony jest więc warunek MSC(i)=MRVC(i) przy i =9.

Optymalny ekonomicznie koszt utrzymania zabezpieczenia wynosi 1000 PLN (i=9) , gdyż MSC(9)=MRVC(9).



	1	2	3	4	5	6	7	8	9	10
MSC(i)	0	15	45	75	105	135	165	210	250	300
MRVC(i)	250	250	250	250	250	250	250	250	250	250

Rys. 4. Krańcowy koszt utrzymania zabezpieczenia MSC (i) i krańcowe ryzyko wyrażone w jednostce walutowej MRVC (i)
Źródło: opracowanie własne



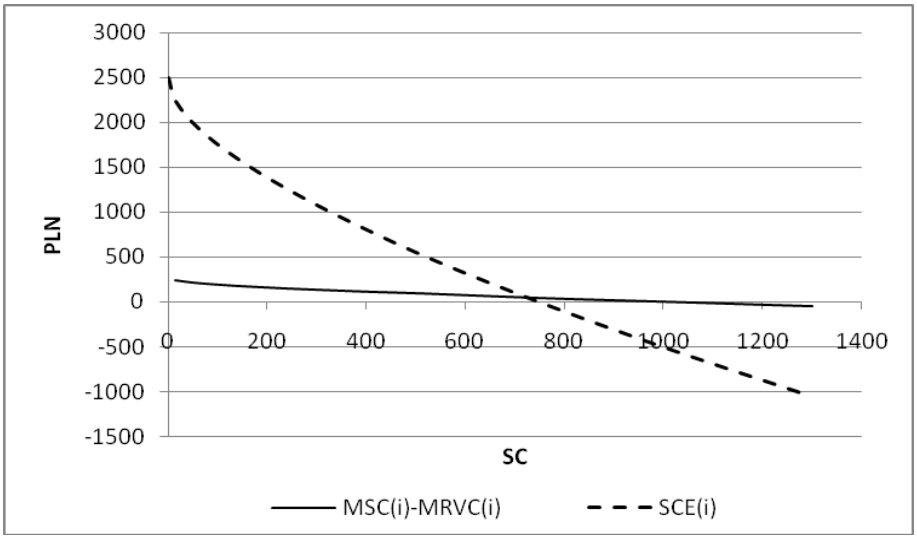
	1	2	3	4	5	6	7	8	9	10
MSC (i) - MRVC (i)		235	205	175	145	115	85	40	0	-50

Rys. 5. Optymaniy koszt utrzymania zabezpieczenia w sensie ekonomicznym MSC(i)=MRVC (i) i=9
Źródło: opracowanie własne

W przypadku zwiększenia kosztów utrzymania zabezpieczenia z 1000 do 1300, krańcowy koszt utrzymania zabezpieczenia równa sie 300, przy krańcowym ryzyku wyrażonym w jednostce walutowej wynoszącym 250. Na takiej operacji tracimy w sensie ekonomicznym 50, gdyż MSC(10)-MRVC(10)= -50

5. Wnioski

Dwie metody wyznaczania optymalnego poziomu kosztów utrzymania zabezpieczenia dają różne wyniki. Nie jest możliwe, aby dwa poziomy kosztów utrzymania zabezpieczenia były prawidłowe.



Rys. 6. Zależność między kosztem utrzymania zabezpieczenia SC(i) a efektywnością kosztową SCE(i) i MSC(i)-MRVC(i)
Źródło: opracowanie własne

Według autora wariant, w którym optymalny ekonomicznie poziom kosztów utrzymania zabezpieczenia jest wyznaczony na podstawie warunku MSC(i)=MRVC(i) jest poprawny.

Po wyznaczeniu wielkości optymalnych ekonomicznie kosztów utrzymania zabezpieczenia należy sprawdzić czy można zaakceptować poziom ryzyka.

Zaprezentowana przez autora metodologia określania optymalnego ekonomicznie poziomu kosztów utrzymania zabezpieczenia opiera się na teorii ekonomicznej, w której wykorzystujemy utarg krańcowy i koszt krańcowy do wyznaczenia optymalnej wielkości produkcji.

Literatura

1. Begg D., Fischer S., Dornbusch R.: Mikroekonomia. Polskie Wydawnictwo Ekonomiczne, Warszawa, 2007.
2. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwo Naukowo-Techniczne, Warszawa, 2007.

3. Drury C.: Rachunek kosztów. Wydawnictwo Naukowe PWN, Warszawa, 1995.
4. Lech P.: Metodyka ekonomicznej oceny przedsięwzięć informatycznych wspomagających zarządzanie organizacją. Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk, 2007.
5. Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. Wydawnictwo Naukowe PWN SA, Warszawa, 2008.
6. Pipkin D.: Bezpieczeństwo informacji. Wydawnictwo Naukowo-Techniczne, Warszawa, 2002.
7. Ross A.: Inżyniera zabezpieczeń. Wydawnictwo Naukowo-Techniczne, Warszawa, 2005.

Dr inż. Karol KREFT
Instytut Transportu i Handlu Morskiego
Uniwersytet Gdański
81-824 Sopot, ul. Armii Krajowej 119/121
tel/fax: 0 58 551 48 53
e-mail : krol@panda.bg.univ.gda.pl