

**THE RISK OF THE DECISION IN COMMON SECURITY  
OF AN ENTITY**

**RYZIKO DECYZJI W BEZPIECZEŃSTWIE POWSZECHNYM  
PODMIOTU**

Dr hab. inż. Edward Kołodziński, prof. WAT

Wojskowa Akademia Techniczna, Instytut Optoelektroniki

*ekolodzinski@wp.pl*

**ABSTRACT**

The global security of an entity (an individual, business, institution, urban area, municipality, district, etc.) is not a stable or permanent state that is enjoyed by an entity throughout its existence. To ensure a satisfactory level of global security, an entity has to initiate preventive measures, it has to prepare for, respond to and effectively counteract the consequences of a materialized risk. At every stage of this process, vital decisions are made as regards the course of actions whose combined effect should minimize the adverse consequences of a threat. The relevant decisions are made in the face of a high number of mutually interactive factors which significantly influence the outcomes of the decision-making process. It entails the risk that the actual costs and losses will be much greater in magnitude than those anticipated at various stages of the decision-making process. A clear set of criteria for assessing decision quality is needed for optimal decision-making. This study proposes criteria for evaluating decision quality and the relevant risks in the decision-making process that aims to ensure the operational security of entities. The optimization process based on the proposed criteria has been illustrated with an example.

**KEYWORDS:** *security system of an entity, evaluation of decision-making risk, optimization of decisions, security analyst, rescue action management*

## 1. BEZPIECZEŃSTWO FUNKCJONOWANIA PODMIOTU

Bezpieczeństwo powszechne<sup>1</sup> podmiotu (np. człowieka, zakładu, instytucji, aglomeracji, gminy, powiatu itp.) nie jest stanem stabilnym - nie jest dobrem danym podmiotowi raz na zawsze. W świecie realnym występują permanentne jego zagrożenia, zarówno od sił natury, jak i niezamierzonych i zamierzonych skutków działalności człowieka. Należy zatem czynić starania o zapewnienie stabilności stanu bezpiecznego funkcjonowania podmiotu. W tym celu tworzony jest *System Bezpieczeństwa Podmiotu* (SBP), rozumiany jako zorganizowany zespół sił i środków zapewniających akceptowalny, przez dany podmiot, stan bezpieczeństwa (rys.1.).

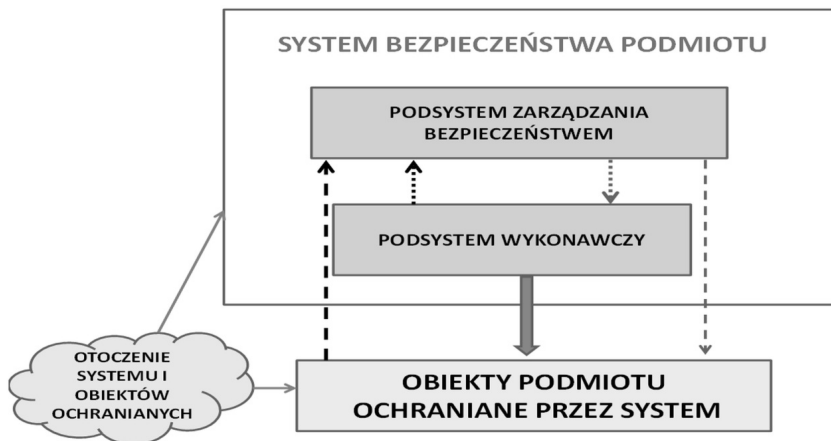
Rys. 1. Diagram kontekstowy bezpieczeństwa funkcjonowania podmiotu



(źródło: opracowanie własne)

Modelowe ujęcie systemu bezpieczeństwa podmiotu przedstawiono na rys.2.

Rys. 2. Model Systemu Bezpieczeństwa Podmiotu



(źródło: opracowanie własne)

W modelowym ujęciu SBP wyróżnia się dwa podsystemy<sup>2</sup>:

- **wykonawczy**, który stanowią siły i środki realizujące procesy wykonawcze, np. straż pożarna, straż miejska, policja, pogotowie techniczne, itd.;
- **zarządzania**, który realizuje procesy informacyjno-decyzyjne stanowiące o sposobie zapewnienia podmiotowi bezpieczeństwa przez podsystem wykonawczy.

**Podsystem zarządzania bezpieczeństwem podmiotu** zawiera dwa elementy składowe (rys.3.) :

- **podsystem informacyjny** – odpowiedzialny za permanentne opracowywanie danych niezbędnych do podejmowania decyzji związanych z zapewnieniem bezpieczeństwa podmiotu,
- **podsystem decyzyjny** – podejmujący decyzje o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu. Precyzują one:
  - ✓ sposób prowadzenia działań przez podsystem wykonawczy SBP w poszczególnych etapach zarządzania bezpieczeństwem podmiotu<sup>3,4</sup>,
  - ✓ działania, jakie powinny podjąć obiekty podmiotu w celu zapewnienia sobie bezpieczeństwa funkcjonowania. Dotyczą one przede wszystkim

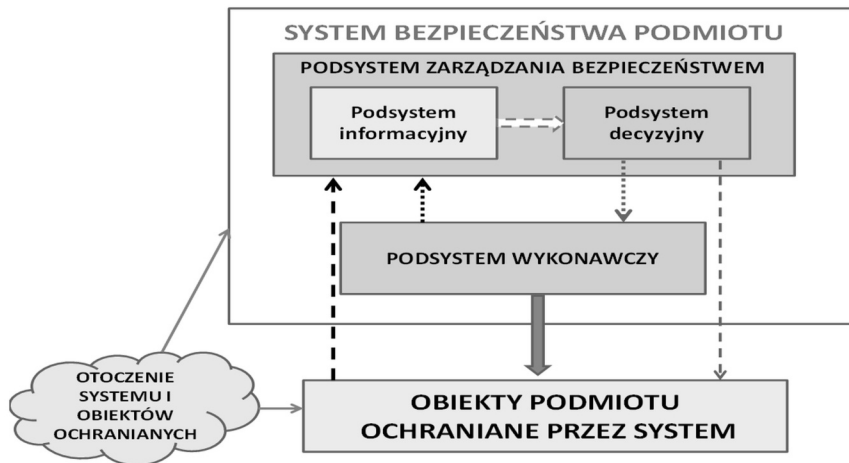
2 Kołodziński E., 2009

3 Kołodziński E., 2009

4 Kołodziński E., 2004

kim zapobiegania zagrożeniom i przygotowania obiektów na wypadek ich wystąpienia.

Rys. 3. Uszczegółowienie podsystemu zarządzania bezpieczeństwem

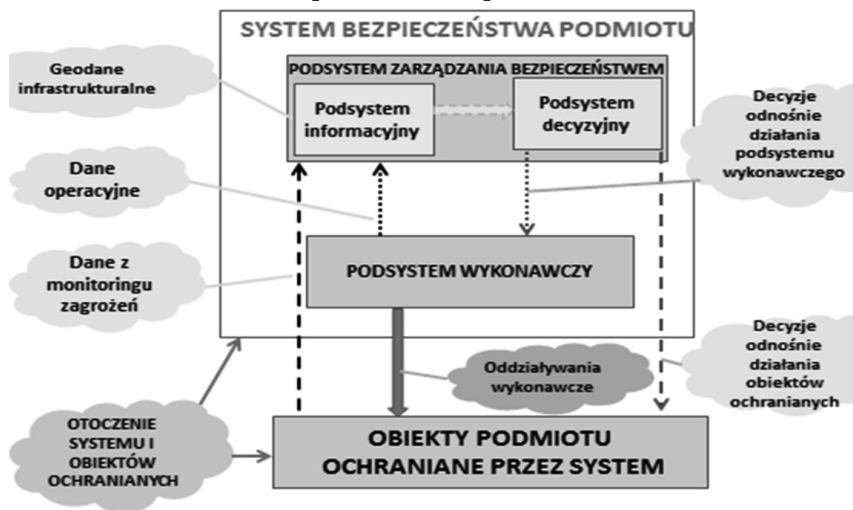


(źródło: opracowanie własne)

Do podejmowania decyzji związanych z zapewnieniem bezpieczeństwa podmiotu wykorzystywane są następujące rodzaje danych (rys. 4.):

- *geodane infrastrukturalne* obszaru dyslokacji obiektów podmiotu i jego otoczenia – istotne z punktu widzenia zapewnienia podmiotowi bezpieczeństwa jego funkcjonowania,
- *dane operacyjne o siłach i środkach* możliwych do użycia w przypadku wystąpienia określonego rodzaju zagrożenia bezpieczeństwa podmiotu,
- *dane z monitoringu zagrożeń* bezpieczeństwa podmiotu oraz czynników mających wpływ na ich stan.

Rys. 4. Przepływy danych i informacji sterującej w zarządzaniu bezpieczeństwem podmiotu



(źródło: opracowanie własne)

*Geodane infrastrukturalne SBP-* to dane o rzeźbie i obiektach technicznych obszaru podmiotu i jego otoczenia, infrastrukturze podziemnej i naziemnej oraz obiektach terenowych o istotnym znaczeniu dla zapewnienia bezpieczeństwa podmiotu. Na geodane infrastrukturalne składają się: dane graficzne zawarte w mapie obszaru oraz dane opisowe charakteryzujące wyróżnione na niej obiekty – istotne z punktu widzenia podsystemu decyzyjnego, stanowiącego o przedsięwzięciach zapewniających bezpieczeństwo podmiotu.

*Dane operacyjne o siłach i środkach, które mogą być użyte do zapewnienia bezpieczeństwa podmiotu-* to dane o siłach i środkach, które potencjalnie mogą być przez niego użyte w działaniach związanych z zapewnieniem bezpieczeństwa, w tym w działaniach ratowniczych oraz w eliminowaniu skutków wyzwolonego zagrożenia. Przykładowymi elementami tego zasobu mogą być dane o: stanach osobowych jednostek organizacyjnych systemu, ich wyposażeniu technicznym, parametrach sprzętu, infrastrukturze obiektów własnych, a ponadto dokumentacje jednostek, zakresy obowiązków osób funkcyjnych, procedury postępowania w określonych sytuacjach, plany ratownicze itp.

*Dane z monitoringu zagrożeń* bezpieczeństwa podmiotu oraz czynni-

ków mających wpływ na ich stan – to dane pochodzące z szeroko rozumianego monitoringu. Warunkiem koniecznym przeciwdziałania zdarzeniom, powodującym zagrożenia bezpieczeństwa podmiotu, jest przewidywanie ich wystąpienia na podstawie określonych symptomów, wykrywanie i identyfikacja. Od danych o aktualnym stanie możliwych zagrożeń bezpieczeństwa podmiotu, uzyskiwanych z systemów monitoringu zależy rodzaj i ilość środków użytych do przeciwdziałania ich skutkom, a także sposób prowadzenia działań ratowniczych. Sposób monitorowania rodzaju i stopnia zagrożeń oraz wykrywania i identyfikacji zdarzeń przez nie spowodowanych, a także czynników wpływających na rozmiar zagrożeń zależy od ich natury, tj. fizykochemicznych objawów i skutków. Abstrahujemy tu od przyczyn, czy są to zagrożenia naturalne, czy też cywilizacyjne, a wśród nich celowo powodowane przez określone grupy ludzi – terrorystów. Na podstawie danych z monitoringu zagrożeń podmiotu podsystemem informacyjny, posługując się modelami matematycznymi i programowymi symulatorami, opracowuje prognozy i scenariusze możliwego rozwoju zdarzeń.

Jakość danych infrastrukturalnych, operacyjnych i o zagrożeniach (ich aktualność, kompletność i komunikatywność) udostępnianych podsystemowi decyzyjnemu (rys.4.) ma istotny wpływ na trafność decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu, podejmowanych przez osoby funkcyjne tego systemu.

Pożądaný poziom bezpieczeństwa funkcjonowania podmiotu zapewniany jest poprzez<sup>5</sup>:

- **zapobieganie** powstawaniu zagrożeń dziedzinowych (np. powodziowych, epidemiologicznych itp.),
- **przygotowanie** podmiotu i Systemu Bezpieczeństwa Podmiotu (SBP) na ewentualność ich wystąpienia,
- prowadzenie skutecznych **działań ratowniczych** w przypadku wystąpienia zagrożeń dziedzinowych,
- **likwidację** skutków wystąpienia zagrożeń dziedzinowych.

Każdy z wyżej wyróżnionych etapów działania SBP, w ramach zapewniania dziedzinowego bezpieczeństwa funkcjonowania podmiotu, ma swoją specyfikę zadaniową i uwarunkowania odnośnie dynamiki realizacji procesów informacyjno-decyzyjnych. Powyższe przybliżymy na przykładzie.

---

<sup>5</sup> Kołodziński E., 2009

### **Przykład 1.**

Rozpatrzmy bezpieczeństwo powodziowe aglomeracji dyslokowanej w dolinie, przez którą przepływa rzeka. Można je zapewnić podejmując, między innymi, następujące działania:

#### **1. na etapie zapobiegania:**

- budowa zbiorników retencyjnych w górnym biegu rzeki,
- zwiększanie wysokości obwałowań rzeki przed i w obszarze aglomeracji,

- prowadzenie prac melioracyjnych;

**2. na etapie przygotowania** na wypadek przekraczania przez rzekę stanu alarmowego- przygotowanie:

- obszarów zalewowych,
- sił o odpowiednich kwalifikacjach,
- materiałów do podwyższania poziomu obwałowania rzeki i zabezpieczenia obiektów- worki, piasek, narzędzia, środki transportu elementów umocnień obwałowania itp.,
- środków transportu ludności i ich dobytku - łodzie, pontony, amfibie, samochody itp.,
- pomieszczeń do czasowego zakwaterowania ludności ewakuowanej z zalanych terenów oraz wyżywienia, wody, ubrań, środków czystości dla nich itp., na ewentualność wystąpienia powodzi;

#### **3. na etapie działań ratowniczych:**

- ratowanie ludzi, którzy nie zostali ewakuowani przed wystąpieniem powodzi,
- ratowanie zwierząt i dobytku,
- zaopatrywanie ludności pozostałej na obszarach zalanych w środki do przetrwania itd.

**4. na etapie likwidacji** skutków powodzi:

- przywracanie zdolności funkcjonalnej obiektów,
- usuwanie zanieczyszczeń powodziowych,
- itd.

W etapach 1., 2. i 4. mamy do czynienia z zarządzaniem bezpieczeństwem, zaś w etapie 3. z kierowaniem działaniami ratowniczymi. Każdy z wyróżnionych w przykładzie etapów działań, podejmowanych przez SBP

w celu zapewnienia bezpieczeństwa funkcjonowania podmiotu, ma swoją specyfikę zadaniową i uwarunkowania odnośnie dynamiki realizacji procesów informacyjno-decyzyjnych.

## 2. NIEPEWNOŚĆ I RYZYKO W ZARZĄDZANIU BEZPIECZEŃSTWEM I KIEROWANIU RATOWNICTWEM

Cechy wspólne zarządzania i kierowania działaniami zapewniającymi bezpieczeństwo funkcjonowania podmiotu to przede wszystkim:

- **niepewność** odnośnie uwarunkowań jego funkcjonowania, wynikająca ze: specyfiki działalności, możliwych wewnętrznych i zewnętrznych zagrożeń prowadzenia tej działalności oraz wrażliwości na te zagrożenia,
- trudności w ujmowaniu w kategoriach wymiernych i oceny: zagrożeń i ich wpływu na jakość funkcjonowania podmiotu,
- konieczność uwzględniania bardzo dużej liczby czynników przy podejmowaniu decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu,
- trudności w zakresie modelowania oddziaływania zagrożeń na ochraniane obiekty podmiotu, możliwości przeciwdziałania ich skutkom oraz algorytmizacji sposobu realizacji procesów informacyjno-decyzyjnych zarządzania i kierowania przeciwdziałaniem.

Decyzje zarówno w zarządzaniu bezpieczeństwem, jak i kierowaniu ratownictwem podejmowane są *a priori*, tzn. dotyczą przyszłości. Z faktu tego wynikają **niepewności** między innymi odnośnie:

- a) rodzaju, skali i możliwych synergii zagrożeń, jakie mogą wystąpić,
- b) przedsięwzięć, które należy zrealizować dla zapewnienia pożądanego poziomu bezpieczeństwa funkcjonowania podmiotu,
- c) bezpośrednich następstw dla podmiotu zrealizowania się poszczególnych zagrożeń w uwarunkowaniach wynikających z wykonania podjętych decyzji,
- d) faktycznych kosztów zrealizowania przedsięwzięć określonych w decyzjach.

Niepewności te powodowane są w szczególności:

- trudnościami w odpowiednio wczesnym wykrywaniu zagrożeń i ich precyzyjnym monitorowaniu oraz przewidywaniu następstw dla bezpieczeństwa funkcjonowania podmiotu,



- losowym charakterem wszystkich zjawisk związanych z bezpieczeństwem funkcjonowania podmiotu,
- dużą liczbą losowych czynników, od których zależy bezpieczeństwo funkcjonowania podmiotu.

Wszystkie te czynniki, w znacznej liczbie przypadków, można charakteryzować za pomocą rozkładu prawdopodobieństwa. Przykładowo, w przypadku rozpatrywanego już bezpieczeństwa powodziowego aglomeracji, taką charakterystyką może być prawdopodobieństwo, że poziom wody w rzece przekroczy stan alarmowy, że środki ratownictwa będą dostarczone przed osiągnięciem przez wodę stanu alarmowego itp. Charakterystyki probabilistyczne niepewności uwarunkowań realizacji podejmowanej decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu nie odzwierciedlają jej skutków: strat i kosztów, a przede wszystkim tego, że mogą one być inne od zakładanych przez decydenta.

Niepewność prognozy uwarunkowań realizacji podejmowanej decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu i jej skutków stanowi genezę *ryzyka decyzji*<sup>6,7,8</sup>- *ryzyka następstw* (nie tylko dla podmiotu) *innych od zakładanych przy podejmowaniu przedmiotowej decyzji*. Ryzyka następstw dotyczących strat i kosztów. Zazwyczaj bardziej niekorzystnych od zakładanych przy podejmowaniu decyzji o przedsięwzięciach do zrealizowania w poszczególnych fazach zapewniania bezpieczeństwa funkcjonowania podmiotu.

### 3. MIARA JAKOŚCI DECYZJI W ZAGADNIENIACH BEZPIECZEŃSTWA

Decyzje o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu podejmowane są w oparciu o posiadaną wiedzę i informację, przy założeniu spełnienia prognozowanych warunków jej realizacji. Podejmując decyzje o sposobach zapewnienia określonego poziomu bezpieczeństwa, należy zdawać sobie sprawę z konieczności poniesienia odpowiednich nakładów na ich wykonanie. Należy również mieć świadomość, że nawet mimo wykonania tych decyzji podmiot może ponieść pewne, szeroko rozumiane, straty, np. uszczerbek na zdrowiu ludzi, zniszczenia obiektów itp.

Każda decyzja może być realizowana w zgoła innych uwarunkowaniach niż decydent zakładał przy jej podejmowaniu. A wówczas zarówno koszty, jak i straty związane z nią mogą być inne od przyjmowanych przez

6 Kaczmarek T., 2006

7 Kołodziński E., 2011

8 Pritczard C., 2002

niego w momencie podejmowania decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu. Naturalną rzeczą jest dążenie, aby decyzje były optymalne. Zatem musi być ustanowiona miara ich jakości.

W celu ustanowienia miary oceny *a priori* jakości decyzji zapewniających bezpieczeństwo dziedzinowe funkcjonowania podmiotu zostaną wprowadzone następujące oznaczenia:

- $\mathbf{D} = \{d_1, d_2, \dots, d_p, \dots, d_1\}$  - zbiór decyzji dopuszczalnych o sposobie zapewnienia dziedzinowego bezpieczeństwa funkcjonowania podmiotu,
  - ✓  $d_i$  - i-ta decyzja związana z zapewnieniem pożądanego poziomu bezpieczeństwa dziedzinowego funkcjonowania podmiotu,
  - ✓ I-liczba wyróżnionych decyzji;
- $S(d_i)$  - straty poniesione bezpośrednio przez podmiot wskutek wystąpienia danego rodzaju zagrożenia, pomimo zrealizowania decyzji  $d_i \in \mathbf{D}$ ,  
gdzie:  $S(d_i) = \langle S_1(d_i), S_2(d_i) \rangle$  przy czym:
  - ✓  $S_1(d_i)$  straty materialne, które można wyrazić np. w jednostkach monetarnych,
  - ✓  $S_2(d_i)$  straty niematerialne – dotyczą w szczególności uszczerbku na zdrowiu osób poszkodowanych w wyniku wystąpienia zagrożenia;
- $K(d_i)$  - koszty realizacji decyzji  $d_i \in \mathbf{D}$ ;
- $R(d_i)$  - ryzyko następstw decyzji  $d_i \in \mathbf{D}$  - bardziej niepożądanych od zakładanych przy jej podejmowaniu.

W pracach dotyczących teorii jakości, np. <sup>9</sup> określa się pożądaną właściwość miary oceny jakości decyzji. Odnosząc je do zagadnień bezpieczeństwa, można ująć następująco:

1. zgodność z miarą decyzji nadrzędnej (np. strategią), której podejmowana decyzja stanowi uszczegółowienie,
2. zgodność z celem podejmowania decyzji,
3. wrażliwość na zmiany wartości wielkości charakteryzujących uwarunkowania podejmowania decyzji,
4. możliwość wyznaczenia jej wartości,

---

<sup>9</sup> Kiliński A., 1979

5. możliwość interpretacji zmian jej wartości.

Uwzględniając powyższe oraz fakt, że zarówno straty ponoszone przez podmiot, jak i koszty realizacji decyzji są wielkościami losowymi proponuje się, aby za miarę jakości decyzji w zagadnieniach zapewnienia bezpieczeństwa funkcjonowania podmiotu przyjąć wielkość:

$$M(d_i) = < M_1(d_i), M_2(d_i), M_3(d_i) >, d_i \in D \quad (1)$$

przy czym:

$M_1(d_i) = E(S^{\text{bez}}(d_i))$  – wartość przeciętna strat bezpośrednio poniesionych przez podmiot przy realizacji decyzji  $d_i \in D$ ,

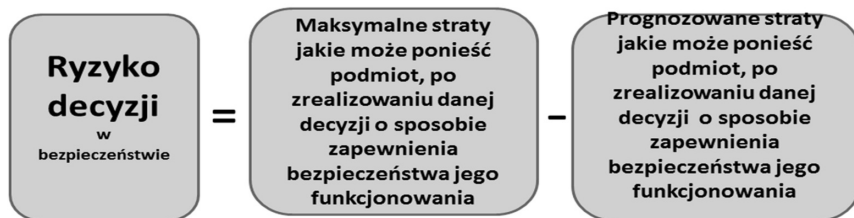
$M_2(d_i) = E(K(d_i))$  – wartość przeciętna kosztów realizacji decyzji  $d_i \in D$ ,

$M_3(d_i) = R(d_i)$  – ryzyko następstw realizacji decyzji  $d_i \in D$ .

#### 4. MIARA RYZYKA DECYZJI W ZAGADNIENIACH BEZPIECZEŃSTWA

Proponuje się, aby *ryzyko decyzji w zagadnieniach bezpieczeństwa* oceniać jako różnicę pomiędzy stratami maksymalnymi, jakie mogą powstać w wyniku podjętej decyzji, a stratami prognozowanymi (zakładanymi) przy jej podejmowaniu – (rys.5.). Przy czym koszty realizacji decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu traktować również jako straty. Uzasadnieniem takiego podejścia jest fakt, że nakłady na zapewnienie bezpieczeństwa funkcjonowania podmiotu uszczuplają środki, które mogłyby być spożytkowane na inne cele.

Rys. 5. Propozycja sposobu oceny ryzyka decyzji w bezpieczeństwie



(źródło: opracowanie własne)

Ponadto proponuje się, aby za *miarę ryzyka decyzji w zagadnieniach bezpieczeństwa* przyjąć wielkość określoną wzorem:

$$R(d_i) = S_{\max}(d_i) - E(S(d_i)) \quad (2)$$

przy czym:

$$E(S(d_i)) = E(S^{\text{bez}}(d_i)) + E(K(d_i)), \quad (3)$$

$$S_{\max}(d_i) = S_{\max}^{\text{bez}}(d_i) + K_{\max}(d_i), \quad (4)$$

gdzie:

$S_{\max}^{\text{bez}}(d_i)$  – maksymalne straty poniesione przez podmiot przy decyzji  $D = d_i$ ,

$K_{\max}(d_i)$  – maksymalne koszty realizacji decyzji  $D = d_i$ .

## 5. OPTYMALIZACJA DECYZJI O SPOSOBIE ZAPEWNIENIA BEZPIECZEŃSTWA FUNKCJONOWANIA PODMIOTU

Naturalnym dążeniem w zagadnieniach *bezpieczeństwa powszechnego podmiotu* jest minimalizacja<sup>10</sup>:

1. strat bezpośrednio poniesionych przez podmiot na skutek wystąpienia zagrożeń,
2. kosztów zapewnienia określonego poziomu bezpieczeństwa funkcjonowania podmiotu,
3. ryzyka decyzji o sposobie zapewnienia bezpieczeństwa.

Zarówno straty poniesione przez podmiot, jak i koszty zapewnienia bezpieczeństwa jego funkcjonowania powinny być rozpatrywane z określonym horyzontem czasowym – być odnoszone do określonego przedziału czasowego. Zasadność tego wynika z faktu, że poszczególne zagrożenia występują z charakterystyczną dla nich częstością (zazwyczaj z losowym odstępem czasu), powodując za każdym razem określone (zazwyczaj losowe):

- straty ponoszone przez ochraniające obiekty podmiotu,
- koszty realizacji poszczególnych faz zarządzania jego bezpieczeństwem.

Decyzją optymalną o sposobie zapewnienia bezpieczeństwa funkcjo-

---

<sup>10</sup> Kołodziński E., 2011

nowania podmiotu będzie zatem decyzja minimalizująca wartości składowych przyjętej miary (wskaźnika) (1) jej jakości:

$$d_{i^*}: M(d_{i^*}) = \min_{d_i \in D} < M_1(d_i), M_2(d_i), M_3(d_i) >, d_{i^*} \in D \quad (5)$$

Znaczenie symboli użytych we wzorze (5) określono w (1,2,3,4).

Zagadnienie wyznaczania optymalnej decyzji o sposobie zapewnienia bezpieczeństwa podmiotu zilustrujemy na poniższym przykładzie.

### **Przykład 2.**

Dany jest obiekt o wartości  $V = 1000\ 000$  jednostek. Istnieje potencjalne zagrożenie bezpieczeństwa jego funkcjonowania. Należy dokonać wyboru optymalnej decyzji, spośród dopuszczalnych, o sposobie zapobieżenia zagrożeniom bezpieczeństwa jego funkcjonowania.

Dla uproszczenia rozważań przyjmujemy następujące założenia odnośnie możliwych sposobów zapobiegania zagrożeniom funkcjonowania podmiotu, ich kosztów i następstw:

1. zbiór decyzji dopuszczalnych jest równy:

$$D = \{d_1, d_2, d_3, d_4\};$$

2. koszty realizacji wyróżnionych decyzji są zdeterminowane i wynoszą odpowiednio:

$$d_1: k_1 = 0, \quad d_2: k_2 = 60000, \quad d_3: k_3 = 100000, \quad d_4: k_4 = 400000;$$

3. prawdopodobieństwa zapobieżenia zagrożeniom dla poszczególnych decyzji wynoszą odpowiednio:

$$d_1: p_1 = 0, \quad d_2: p_2 = 0.05, \quad d_3: p_3 = 0.5, \quad d_4: p_4 = 0.8.$$

Decydent musi podjąć optymalną decyzję o sposobie zapobiegania. Którą decyzję, spośród dopuszczalnych, powinien wybrać? Która decyzja jest optymalna?

Zgodnie z (5) decyzją optymalną będzie:

$$d_{i^*}: M(d_{i^*}) = \min_{d_i \in D} < E(S^{bez}(d_i)), E(K(d_i)), R(d_i) > d_{i^*} \in D$$

Przy przyjętych założeniach:

1. wartość przeciętna strat poniesionych bezpośrednio przez obiekt,

w przypadku decyzji dopuszczalnych  $d_i \in \mathbf{D}$ , wyznaczana jest na podstawie wzoru:

$$E(S^{\text{bez}}(d_i)) = V (1-p_i) = 1000000 (1-p_i)$$

i wynosi:  $E(S^{\text{bez}}(d_1)) = 1000000j$ ,  $E(S^{\text{bez}}(d_2)) = 950000j$ ,  $E(S^{\text{bez}}(d_3)) = 500000j$ ,  
 $E(S^{\text{bez}}(d_4)) = 200000j$ ;

2. zgodnie z przyjętym założeniem, wartość przeciętna kosztów wykonania decyzji dopuszczalnych  $d_i \in \mathbf{D}$  wyznaczana jest na podstawie wzoru:

$$E(K(d_i)) = k_i$$

i wynosi:  $E(K(d_1)) = 0j$ ,  $E(K(d_2)) = k_2 = 60000j$ ,  $E(K(d_3)) = k_3 = 100000j$ ,  
 $E(K(d_4)) = k_4 = 400000j$ ;

3. wartość przeciętna strat łącznych dla wyróżnionych decyzji dopuszczalnych  $d_i \in \mathbf{D}$  wyznaczana jest na podstawie wzoru (3):

$$E(S(d_i)) = E(S^{\text{bez}}(d_i)) + E(K(d_i))$$

i wynosi:  $E(S(d_1)) = 1000000j$ ,  $E(S(d_2)) = 1010000j$ ,  $E(S(d_3)) = 600000j$ ,  
 $E(S(d_4)) = 600000j$ ;

4. straty maksymalne dla wyróżnionych decyzji dopuszczalnych  $d_i \in \mathbf{D}$  wyznaczane są na podstawie wzoru (4):

$$S_{\max}(d_i) = S_{\max}^{\text{bez}}(d_i) + K_{\max}(d_i),$$

Przyjmując, dla uproszczenia, że dla każdego  $d_i \in \mathbf{D}$ :

$$S_{\max}^{\text{bez}}(d_i) = V = 1000000j \text{ oraz } K_{\max}(d_i) = k_i$$

to straty maksymalne, jakie mogą powstać przy poszczególnych decyzjach wyniosą:

$S_{\max}(d_1) = 1000000j$ ,  $S_{\max}(d_2) = 1060000j$ ,  $S_{\max}(d_3) = 110000j$ ,  $S_{\max}(d_4) = 1400000j$ ;

5. Ryzyko dla poszczególnych decyzji dopuszczalnych  $d_i \in \mathbf{D}$  wyznaczane jest na podstawie wzoru (2):

$$R(d_i) = S_{\max}(d_i) - E(S(d_i))$$

i wynosi:  $R(d_1) = 0$ ;  $R(d_2) = 50000j$ ;  $R(d_3) = 500000j$ ;  $R(d_4) = 800000j$ .

Wyniki obliczeń pośrednich zestawiono w tabeli 1. oraz zilustrowano na rys. 6.

Tabela1. Wyniki analizy następstw decyzji o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania obiektu.

Decyzja $d_i \in \mathbf{D}$	Wartość przeciętna kosztów wykonania decyzji $d_i \in \mathbf{D}$ $E(K(d_i))$	Prawdopod. zapobieżenia zagrożeniom przy decyzji $d_i \in \mathbf{D}$	Wartość przeciętna strat poniesionych przez podmiot przy decyzji $d_i \in \mathbf{D}$ $E(S^{bez}(d_i))$	Wartość przeciętna strat łącznych przy decyzji $d_i \in \mathbf{D}$ $E(S(d_i))$	Straty maksymalne łączne przy decyzji $d_i \in \mathbf{D}$ $S_{max}(d_i)$	Ryzyko decyzji $d_i \in \mathbf{D}$ $R(d_i)$
$d_1$	0	0	1000000	1000000	1000000	0
$d_2$	60000	0.05	950000	1010000	1060000	50000
$d_3$	<b>100000</b>	<b>0.5</b>	<b>500000</b>	<b>600000</b>	<b>1100000</b>	<b>500000</b>
$d_4$	400000	0.8	200000	600000	1400000	800000

(źródło: opracowanie własne)

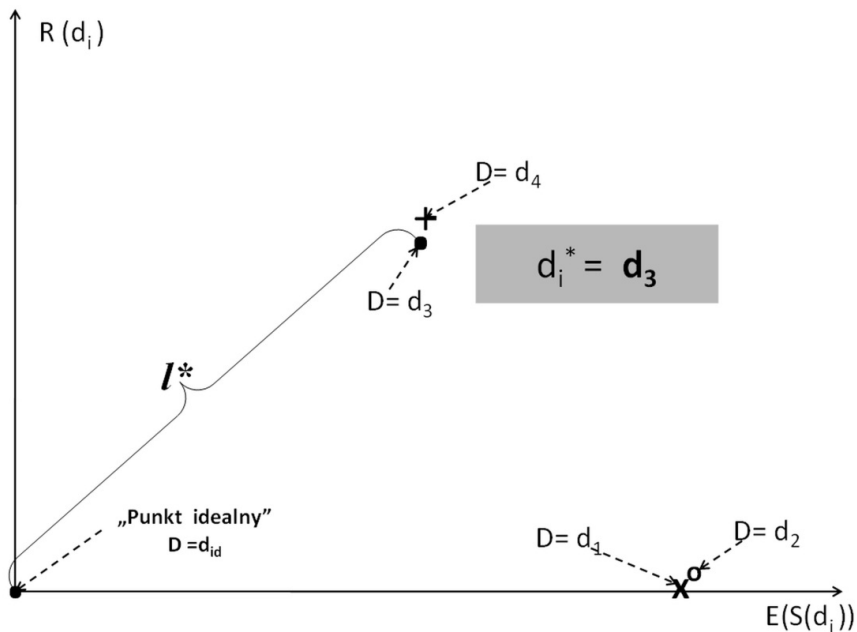
Decyzją idealną o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania obiektu jest decyzja dla której:  $E(S(d_{id})) = 0$  oraz  $R(d_{id}) = 0$ . Na rys. 6. odpowiada jej punkt idealny o współrzędnych (0,0).

Decyzją optymalną  $D = d_i^*$  o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania obiektu jest decyzja  $D = d_i$ , dla której punkt o współrzędnych  $(E(S(d_i)), R(d_i))$  będzie najbliższy w sensie przyjętej miary odległości. Jeżeli przyjmiemy odległość euklidesową:

$$l = ((E(S(d_i)))^2 + (R(d_i))^2)^{1/2},$$

to decyzją optymalną będzie decyzja  $d_i^* = d_3$  (rys.6.).

Rys. 6. Ilustracja wyników obliczeń strat łącznych i ryzyka w zagadnieniu optymalizacji decyzji o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania obiektu



(źródło: opracowanie własne)

## PODSUMOWANIE

W procesie decyzyjnym zarządzania bezpieczeństwem podmiotu zachodzi potrzeba:

1. identyfikacji możliwości i częstości występowania danego rodzaju zagrożeń bezpieczeństwa funkcjonowania podmiotu,
2. wyznaczania prognozy jego przebiegu i skutków,
3. dokonywania analizy możliwych sposobów zapewnienia pożądanego poziomu bezpieczeństwa funkcjonowania podmiotu, uwzględniających występujące ograniczenia, np. zbiór dopuszczalnych rozwiązań, dopuszczalny czas analizy rozwiązań i podjęcia decyzji, dopuszczalny czas realizacji poszczególnych rozwiązań itd.

4. **analizy kosztów, strat i ryzyka** przyjęcia dopuszczalnych rozwiązań (sposobów) zapewnienia pożądanego poziomu bezpieczeństwa funk-



cjonowania podmiotu oraz ryzyka z nimi związanego,

5. ustalenia kryterium optymalizacji rozwiązania,
6. wyznaczenia rozwiązania optymalnego.

W procesie decyzyjnym kierowania ratownictwem dziedzicznym podmiotu zachodzi potrzeba:

1. identyfikacji zdarzeń wymagających podjęcia działań ratowniczych,
2. identyfikacji rozwiązań (decyzji) dopuszczalnych racjonalnego przeprowadzenia akcji ratowniczej, **analizy kosztów, strat i ryzyka** przyjęcia dopuszczalnych rozwiązań skutecznego przeprowadzenia akcji ratowniczej po zajściu zdarzenia,
3. ustalenia kryterium optymalizacji decyzji,
4. oceny ryzyka decyzji optymalnej.

Cechą istotnie różniącą zarządzanie bezpieczeństwem i kierowanie ratownictwem, pomijając aspekty merytoryczne i złożoność, jest dynamika procesów informacyjno-decyzyjnych. Kierowanie działaniami ratowniczymi charakteryzuje, przede wszystkim:

- duża dynamika tych procesów i wynikające z niej ograniczenie na dopuszczalny czas podjęcia decyzji,
- praktyczna niemożliwość, bez informatycznego wsparcia, analizy nawet podstawowych czynników przy podejmowaniu decyzji o sposobie prowadzenia działań ratowniczych,
- istotnie utrudniona możliwość konsultacji z ekspertami odnośnie sposobu prowadzenia działań ratowniczych,
- podejmowanie decyzji przez osoby funkcyjne przedsięwzięć ratowniczych pod czasową i psychiczną presją odpowiedzialności za skutki błędnie podjętych decyzji.

Niezależnie od różnorodności problemów występujących w zarządzaniu bezpieczeństwem podmiotu i kierowaniu ratownictwem mają one wspólną potrzebę. Jest nią potrzeba komputerowego wspomaganie: wykrywania zagrożeń i identyfikacja ich cech oraz **podejmowania optymalnych decyzji** o sposobie przeciwdziałania tym zagrożeniom. Warunkiem koniecznym optymalizacji decyzji jest ustanowienie miary ich jakości i kryteriów optymalizacji. Próbę taką podjęto w niniejszym artykule.

## **REFERENCES**

1. Kołodziński E. (2011), Zarządzanie bezpieczeństwem wewnętrznym w Rzeczypospolitej Polskiej, Czasopismo internetowe „Zagadnienia Inżynierii Bezpieczeństwa”, <http://www.ptib.pl/component/remository/?func=fileinfo&id=416> [2.06.2011].
2. Kołodziński E. (2009), Wprowadzenie do zarządzania bezpieczeństwem, Czasopismo internetowe “Zagadnienia Inżynierii Bezpieczeństwa”, <http://www.ptib.pl/component/remository/?func=fileinfo&id=102> [2.06.2011].
3. Kołodziński E. (2004), Zagrożenia bezpieczeństwa i organizacja przeciwdziałania ich skutkom, <http://www.infocorp.com.pl/publikacje/bezpieczenstwo9.pdf> [2.06.2011]
4. Kaczmarek T. (2006), Ryzyko i zarządzanie ryzykiem, Ujęcie interdyscyplinarne, Warszawa, Difin.
5. Kołodziński E. (2011), Analiza ryzyka w zarządzaniu bezpieczeństwem powszechnym, Czasopismo internetowe “Zagadnienia Inżynierii Bezpieczeństwa”, <http://www.ptib.pl/component/remository/?func=fileinfo&id=408> [2.06.2011].
6. Pritzard C. (2002), Zarządzanie ryzykiem w projektach, teoria i praktyka, Warszawa, WIG-PRESS.
7. Kiliński A. (1979), Jakość, Warszawa, Wydawnictwo Naukowo-Techniczne.