PROBLEMY WSPOMAGANIA PODEJMOWANIA DECYZJI W BEZPIECZEŃSTWIE

Edward Kołodziński, Piotr Zapert

Wojskowa Akademia Techniczna

Tomasz Lachowicz, Łukasz Tomczyk

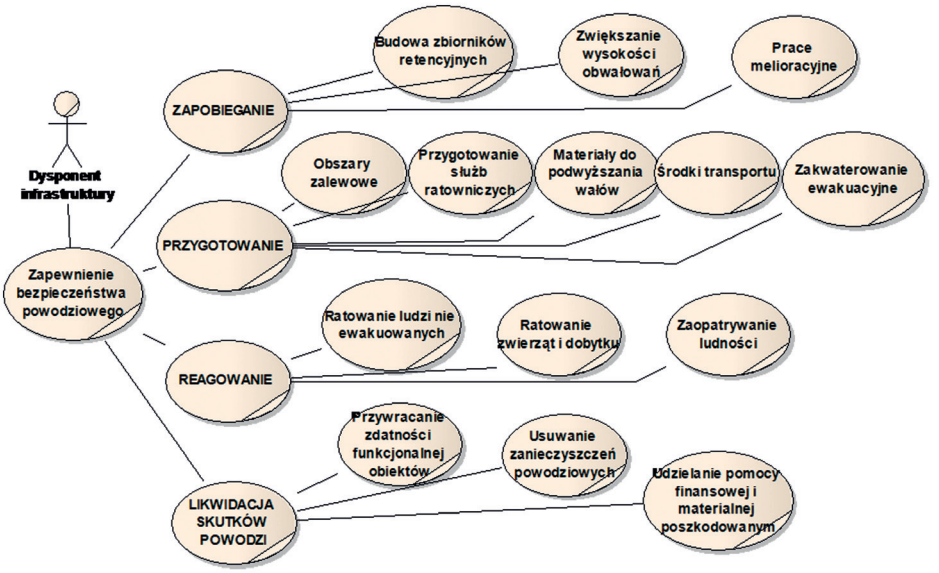
Uniwersytet Warmińsko-Mazurski

Streszczenie: Cechą charakterystyczną zarządzania bezpieczeństwem i kierowania ratownictwem jest złożoność problemów decyzyjnych wynikająca z: dużej liczby uwzględnianych czynników, nieskalarnych funkcji kryterium, silnego ograniczenia na czas rozwiązywania problemu, niepewności i nieokreśloności danych. Implikuje to konieczność komputerowego wspomagania decydentów w podejmowaniu przez nich decyzji. Rozwiązywane problemy można podzielić na cztery podstawowe grupy, tj. takie, które dadzą się:
1) ujmować formalnie w postaci zadań optymalizacyjnych i wyznaczać dla nich rozwiązania optymalne metodą analityczną bądź symulacyjną;
2) ujmować formalnie w postaci zadań optymalizacyjnych, lecz można je rozwiązywać jedynie przy zastosowaniu systemów ekspertowych,
3) przedstawiać jedynie w sposób opisowy, a przy ich rozwiązywaniu wykorzystać wiedzę nagromadzoną w bazie wiedzy w postaci przypadków,
4) przedstawiać jedynie w sposób opisowy i nie ma wiedzy szczegółowej odnośnie do sposobu ich rozwiązania.
Są to problemy, które występują po raz pierwszy. Powszechna losowość w bezpieczeństwie, dotycząca: zagrożeń i podatności na nie podmiotu, skutków zagrożeń, kosztów zapobiegania im i reagowania w przypadku wystąpienia itd., to czynniki, które powodują ryzyko podejmowanych decyzji. W artykule zostały przedstawione metody komputerowego wspomagania podejmowania decyzji w bezpieczeństwie z uwzględnieniem ryzyka. Dokonano analizy możliwości i uwarunkowań wykorzystania w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem: analiz sieciowych, symulacji komputerowej, metod eksperckich, systemów ekspertowych oraz systemów wnioskowania przez analogię.
Słowa kluczowe: bezpieczeństwo podmiotu, ryzyko decyzyjne, miara wartości decyzji, metody wspomagania decyzji.

1. Wprowadzenie

Dla zapewnienia pożądanego poziomu bezpieczeństwa funkcjonowania podmiotu [7, 8] niezbędna jest permanentna analiza jego zagrożeń oraz konieczności i sposobu wykonywania przedsięwzięć: zapobiegających ich powstawaniu i przygotowawczych na wypadek wystąpienia. Analiza zagrożeń obejmuje przede wszystkim prognozy: wystąpienia, przebiegu, wrażliwości podmiotu na poszczególne ich rodzaje, wielkości możliwych negatywnych skutków itd. Wyniki analizy zagrożeń stanowią

podstawę do określenia niezbędnych przedsięwzięć zapobiegających i przygotowawczych, zarówno podmiotu, jak i systemu jego bezpieczeństwa, tj. służb, inspekcji, podmiotów gospodarczych i administracji, na ich wystąpienie. Analizę możliwych rodzajów przedsięwzięć do wykonywania dla zapewnienia bezpieczeństwa dziedzinowego podmiotu zilustrowano na przykładzie bezpieczeństwa powodziowego aglomeracji miejskiej położonej w dolinie, przez którą przepływa rzeka (rys. 1.1).



Rys. 1.1. Diagram biznesowych przypadków użycia systemu bezpieczeństwa powodziowego aglomeracji (Źródło – opracowanie własne na podstawie [4])

Cechą charakterystyczną zarządzania bezpieczeństwem i kierowania ratownictwem jest: złożoność problemów decyzyjnych wynikająca z konieczności uwzględniania dużej liczby czynników, zazwyczaj wieloskładnikowa funkcja kryterium optymalizacji decyzji [1, 5], silne ograniczenie na czasy rozwiązywania problemów, niepewność i nieokreśloność danych, na podstawie których podejmowane są decyzje, a szczególnie niepewność odnośnie do uwarunkowań i następstw ich wdrożenia.

Zarządzanie bezpieczeństwem funkcjonowania podmiotu i kierowania ratownictwem powinno być realizowane z zastosowaniem modeli adekwatnych do rozwiązywanych problemów z wykorzystaniem zweryfikowanych w praktyce narzędzi programowych do przeprowadzania stosownych obliczeń. Warunek ich stosowania przez decydenta stanowi znajomość podstawowych metod wspomagania podejmowana decyzji, np. optymalizacji wielokryterialnej, analiz sieciowych, wnioskowania przez analogię, symulacji komputerowej, metod eksperckich, systemów ekspertowych itd.

i umiejętność posługiwania się oprogramowaniem narzędziowym komputerowego wspomagania wyznaczania rozwiązań problemów decyzyjnych w bezpieczeństwie.

2. Niepewność decydenta w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem

Każda analiza w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem poprzedzająca podjęcie decyzji przeprowadzana jest a priori, w oparciu o przyjęty model sytuacyjny oraz dane z dotychczasowego monitoringu zagrożeń. Decydent powinien mieć zatem świadomość niepewności uwarunkowań realizacji jego decyzji w odniesieniu do:

1) wystąpienia, skali i przebiegu określonych rodzajów zagrożeń;
2) rozmiaru negatywnych ich skutków;
3) kosztów i skuteczności wdrożenia rozpatrywanych rozwiązań, które jego zdaniem powinny zapewnić pożądany poziom bezpieczeństwa funkcjonowania podmiotu.

Możliwość i skala wystąpienia zagrożeń pochodzących od sił natury jest niezależna od człowieka. Mogą one jedynie być prognozowane na podstawie zarchiwizowanych danych historycznych. Jednakże wielkość ich negatywnych skutków zależy od decyzji podejmowanych w zarządzaniu bezpieczeństwem danego podmiotu. Odmiennie przedstawia się sytuacja w przypadkach, w których źródłem zagrożeń są już użytkowane, a także nowo wytwarzane i wdrażane jego artefakty. Człowiek ma możliwość zapobiegania generowaniu przez nie zagrożeń już na etapie ich projektowania.

Z każdą decyzją w zarządzaniu bezpieczeństwem funkcjonowania podmiotu i kierowania ratownictwem łączy się ryzyko następstw innych od zakładanych przy jej podejmowaniu. Dotyczą one zarówno strat, jak i kosztów. Wartość różnicy będzie zależała od trafności prognozy, zaś trafność prognozy od wiarygodności danych i adekwatności zastosowanego modelu prognostycznego. Uwzględniając powyższe uwarunkowania, nasuwa się wniosek, aby ***ryzyko decyzji*** oceniać jako relację pomiędzy:

1) ekstremalnymi stratami, jakie mogą powstać w podmiocie po wystąpieniu zagrożenia w przypadku zrealizowania danej decyzji, a stratami prognozowanymi przez decydenta przy jej podejmowaniu i nazwać je ***ryzykiem strat decyzji***;
2) ekstremalnymi nakładami, jakie mogą być niezbędne do zrealizowania danej decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu a nakładami prognozowanymi przez decydenta przy jej podejmowaniu i nazwać je ***ryzykiem kosztów decyzji***,
3) ekstremalnymi stratami łącznymi (tj. ekstremalnymi stratami bezpośrednio poniesionymi przez podmiot ochraniany powiększonymi o ekstremalne

koszty wykonania podjętej decyzji), jakie mogą powstać w wyniku wystąpienia zagrożenia po wykonaniu decyzji, a łącznymi stratami prognozowanymi przy jej podejmowaniu i nazwać je ***ryzykiem łącznym decyzji***.

W przedstawionych uwarunkowaniach wyznaczania rozwiązań problemów decyzyjnych w zagadnieniach bezpieczeństwa ryzyko jest wyłącznie i nierozerwalnie związane z decyzją – *nie ma decyzji bez ryzyka innych skutków od zakładanych przy jej podejmowaniu*. W zagadnieniach bezpieczeństwa ryzyko rozpatrywane jest w kontekście negatywnych skutków podejmowanych decyzji i nakładów niezbędnych na ich realizację. Za całkowicie błędne uważa się natomiast utożsamianie ryzyka z prognozowanymi stratami, jakie może ponieść podmiot wskutek wystąpienia zagrożenia, bądź kosztami wykonania decyzji.

Dla potrzeb uwzględniania ryzyka w procesach decyzyjnych w bezpieczeństwie niezbędne jest ustalenie jego miary. Przy przyjęciu założenia o losowości uwarunkowań podejmowanych decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu, a także strat materialnych i niematerialnych oraz kosztów z nią związanych, *miara ryzyka decyzji* może przykładowo przyjąć postać określoną wzorem [9, 11]:

$$E(R(D_I)) = <E(R_1(D_I)), E(R_2(D_I))>, \tag{2.1}$$

gdzie:

- $R_1(d_i) = < R_{11}(d_i), R_{12}(d_i)>$ – ryzyko strat innych od prognozowanych:
  - $R_{11}(d_i)$ – ryzyko strat niematerialnych:

$$R_{11}(D_I) = S_I^{inn}(D_I) - S_1(D_I), \tag{2.2}$$

  - $R_{12}(d_i)$ – ryzyko strat materialnych:

$$R_{12}(D_I) = S_2^{inn}(D_I) - S_2(D_I), \tag{2.3}$$

- $R_2(d_i)$ – ryzyko kosztów innych od prognozowanych:

$$R_2(D_I) = K^{INN}(D_I) - E(K(D_I)). \tag{2.4}$$

Użyty w powyższych wzorach indeks „inn" oznacza, że analityk arbitralnie może dokonać wyboru tej wielkości. Przykładowo może to być maksymalna wartość tej wielkości.

3. Miara jakości decyzji w zagadnieniach bezpieczeństwa

Naturalnym dążeniem decydenta jest, aby straty ponoszone przez podmiot oraz koszty wynikające z jego decyzji były minimalne. Ponadto, aby prognozowane przez niego straty i koszty podejmowanych decyzji (przyjętej reguły decyzyjnej) były jak najbliższe tym, jakie faktycznie wystąpią po ich zrealizowaniu – ryzyko strat i kosztów

było minimalne. Zatem za miarę jakości decyzji w zagadnieniach bezpieczeństwa – funkcję kryterium optymalizacji decyzji – proponuje się przyjąć wielkość [11]:

$$M(D_I) = < M_1(D_I), M_2(D_I), M_3(D_I) >, D_I \in \mathbf{D}, \tag{3.1}$$

gdzie:

- $M_1(d_i) = E(S(d_i))$ – wartość przeciętna prognozowanych strat poniesionych przez podmiot wskutek wystąpienia danego rodzaju zagrożenia, pomimo zrealizowania decyzji $d_i \in \mathbf{D}$,
- $M_2(d_i) = E(K(d_i))$ – wartość przeciętna prognozowanych kosztów realizacji decyzji $d_i \in \mathbf{D}$,
- $M_3(d_i) = E(R(d_i))$ – wartość przeciętna ryzyka następstw realizacji decyzji $d_i \in \mathbf{D}$, np. (2.1).
- **D** – zbiór decyzji dopuszczalnych o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu.

Poszczególne składowe funkcji kryterium (3.1) w różnym stopniu mogą być preferowane przez decydenta – mogą mieć dla niego różne wagi. Aby uwzględnić ten fakt, funkcja kryterium (3.1) zostanie zmodyfikowana do postaci:

$$M^W(D_I) = < M_1{}^W(D_I), M_2{}^W(D_I), M_3{}^W(D_I) >, D_I \in \mathbf{D}, \tag{3.2}$$

gdzie, na przykład:

$$M_G{}^W(D_I) = W_G M_G(D_I), G = 1, 2, 3,$$

w_g – stopień preferowania (waga) g-tej składowej (3.2) przez decydenta przy podejmowaniu decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu.

Wielkość (3.2) nazywana jest *preferencyjną funkcją kryterium oceny decyzji decydenta* przy podejmowaniu decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu, zaś jej składowe *ważonymi składowymi preferencyjnej funkcji kryterium oceny decyzji decydenta*. Model preferencji decydenta w zagadnieniach bezpieczeństwa to strategia wyboru decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu. Strategię tę określa się poprzez arbitralne wskazanie przez decydenta relacji dominowania $\mathbf{R}_d$ [1, 11]:

$$\mathbf{R}_d \subset \mathbf{Y} \times \mathbf{Y}, \tag{3.3}$$

gdzie:

Y – zbiór możliwych wartości ocen jakości (3.2) decyzji w zagadnieniach zapewnienia bezpieczeństwa funkcjonowania podmiotu:

$$\mathbf{Y} \subset \mathbf{R}^3 \tag{3.4}$$

$\mathbf{R}_d$ – zbiór takich par $(y, z) \in \mathbf{Y} \times \mathbf{Y}$, że podejmujący woli ocenę y niż z („y jest co najmniej tak dobra dla niego jak z").

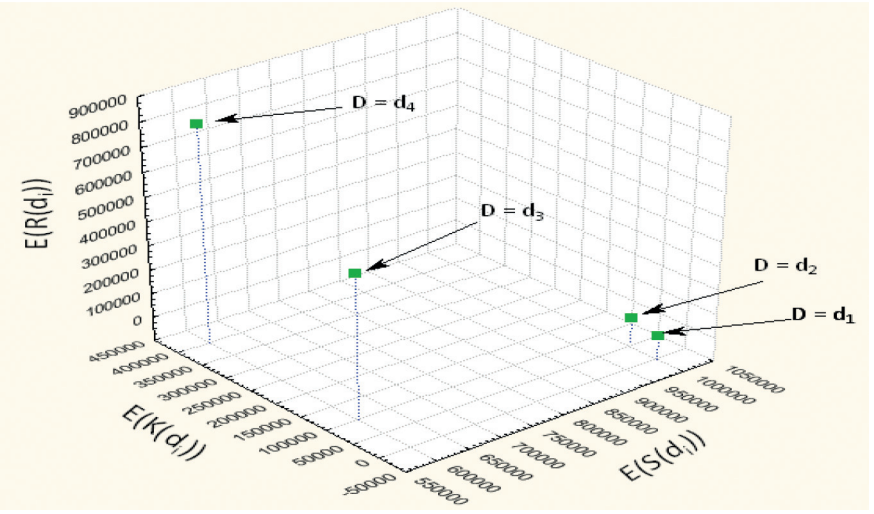
W przypadku trójskładnikowej funkcji kryterium optymalizacji (3.2) każdej decyzji ze zbioru **D** dopuszczalnych o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu odpowiada trójka liczb określająca punkt w trójwymiarowym układzie kartezjańskim, w odpowiedniej odległości od punktu odpowiadającego decyzji *idealnej* o współrzędnych <0,0,0>. W zależności od arbitralnie przyjętej przez decydenta miary odległości rozpatrywanych decyzji od idealnej różne będą wyniki optymalizacji. Omawiane zagadnienie zostanie zilustrowane na poniższym przykładzie, zaczerpniętym z [11].

Przykład 3.1

Dla podmiotu o pewnej wartości należy określić optymalny sposób zapewnienia bezpieczeństwa jego funkcjonowania, przy czym dane są [11]:

1) zbiór decyzji dopuszczalnych **D** = {d_1, d_2, d_3, d_4};
2) każdej decyzji $d_i \in$ **D** ($i = \overline{1,4}$) odpowiada:
   a) koszt jej realizacji k_i,
   b) prawdopodobieństwa zapobiegnięcia zagrożeniom p_i;
3) funkcja kryterium optymalizacji określona jest wzorem (3.1).

Dla danych przyjętych w [11] wyniki obliczeń zilustrowano na rys. 3.1.



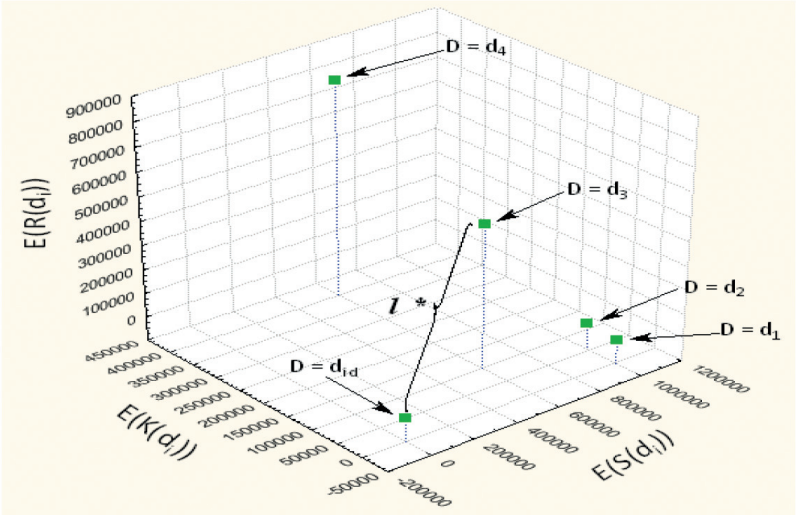
Rys. 3.1. Ilustracja wyników obliczeń strat łącznych, kosztów decyzji i ryzyka w zagadnieniu optymalizacji decyzji o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania podmiotu (Źródło: [11])

Z analizy następstw poszczególnych decyzji dopuszczalnych w świetle miary jakości decyzji (3.1) wynika, że:

– wartość przeciętna kosztów wykonania decyzji jest minimalna dla D = d_1,

- wartość przeciętna strat poniesionych przez podmiot jest minimalna dla $D = d_4$,
- wartość przeciętna ryzyka decyzji jest minimalna dla $D = d_1$.

Decydent powinien podjąć optymalną decyzję o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu. Którą decyzję, spośród dopuszczalnych, powinien wybrać? Która decyzja jest optymalna? Zależy to od arbitralnie przyjętej przez decydenta miary odległości wyników decyzji od punktu o współrzędnych <0, 0, 0>. Dla euklidesowej miary odległości decyzją optymalną jest decyzja d_3 (rys. 3.2). Dla innej miary odległości może ulec zmianie rozwiązanie przyjmowane za optymalne.



Rys. 3.2. Ilustracja wyznaczania decyzji optymalnej w rozpatrywanym w przykładzie zagadnieniu optymalizacji decyzji o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania podmiotu (Źródło: [11])

4. Uwarunkowania wyznaczania rozwiązań problemów decyzyjnych w zagadnieniach bezpieczeństwa

Problemy decyzyjne występujące w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem, ze względu na możliwość formalnego ich ujęcia, można podzielić na cztery podstawowe grupy, tj. takie, które dadzą się:

1) ujmować formalnie w postaci zadań optymalizacyjnych i dla których możliwe jest wyznaczenie rozwiązań optymalnych metodą analityczną bądź symulacyjną;
2) ujmować formalnie w postaci zadań optymalizacyjnych i dla których da się wyznaczyć jedynie rozwiązania suboptymalne;

3) przedstawiać wyłącznie w sposób opisowy i dla których możliwe jest jedynie wyznaczenie rozwiązań racjonalnych – satysfakcjonujących decydenta. Przy ich wyznaczaniu wykorzystana jest wiedza empiryczna ekspertów zawarta w postaci reguł decyzyjnych zapisanych w systemach ekspertowych lub też nagromadzona w dziedzinowych bazach wiedzy w postaci przypadków – stosowana jest wówczas metoda wnioskowania przez analogię;
4) przedstawiać jedynie w sposób opisowy i dla których nie ma pozyskanej dotychczas dostatecznej wiedzy empirycznej, aby można było ją z przekonaniem wykorzystać przy rozwiązywaniu danego problemu. W takim przypadku rozwiązanie wyznaczane jest w oparciu o posiadaną przez decydenta wiedzę empiryczną i wykorzystanie metod i technik heurystycznych.

Miary jakości decyzji podejmowanych w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem są zazwyczaj wieloskładnikowe. Poszczególne składniki mogą charakteryzować różne aspekty rozwiązywanego problemu i mieć różne wagi dla decydenta [11]. W literaturze dotyczącej optymalizacji wielokryterialnej opisanych jest wiele metod wyznaczania rozwiązań optymalnych przy ważonych składowych funkcji kryterium [5]. O tym, którą z nich zastosować w rozwiązywanym problemie, arbitralnie rozstrzyga decydent. Musi on jednak mieć na uwadze, że zastosowana metoda i wagi nadane poszczególnym składowym funkcji kryterium mają istotny wpływ na rozwiązanie problemu. Zastosowana metoda wyznaczania rozwiązania optymalnego odzwierciedla również preferencje decydenta odnośnie do stopnia uwzględniania strat w podmiocie spowodowanych przez wystąpienie zagrożeń, kosztów realizacji wybranej decyzji oraz odzwierciedla jego ostrożność w podejmowaniu decyzji. Powyższe stwierdzenia oparte są na zamieszczonych w [11] wynikach badań przeprowadzonych na przykładzie optymalizacji decyzji o sposobie zapewnienia bezpieczeństwa powodziowego aglomeracji położonej w dolinie, przez którą przepływa rzeka.

5. Dobór metody rozwiązania problemu decyzyjnego w zagadnieniach bezpieczeństwa

Rodzaj problemu, jego złożoność, ograniczenie czasowe na rozwiązanie, wiedza decydenta o metodach możliwych do zastosowania przy rozwiązywaniu problemu i ich implementacjach programowych, umiejętności posługiwania się nimi to podstawowe czynniki decydujące o zakresie zastosowania komputerowego wspomagania rozwiązywania problemów zapewnienia bezpieczeństwa podmiotu. Warunkiem koniecznym podejmowania jakichkolwiek działań ukierunkowanych na zapewnienie pożądanego poziomu bezpieczeństwa funkcjonowania podmiotu jest znajomość jego zagrożeń i wrażliwości podmiotu na te zagrożenia. Bardzo pomocne w identyfikacji zagrożeń okazuje się modelowanie obiektowe w dostatecznie rozpowszechnionym

języku (notacji) UML [16]. Model kontekstowy i przypadków użycia oraz analityczny podmiotu pozwalają jednoznacznie zidentyfikować zagrożenia. Technologię identyfikacji zagrożeń na podstawie biznesowych modeli obiektowych dla potrzeb określania wymagań na system bezpieczeństwa podmiotu przedstawiono w [12], zaś dla potrzeb ustalania bazowej infrastruktury podmiotu w pracy [13].

Przy rozwiązywaniu problemów w bezpieczeństwie sformułowanych w postaci zadań optymalizacyjnych powinny być preferowane metody analityczne [5], a tam gdzie nie jest możliwe ich zastosowanie, metoda symulacyjna [6]. Stosowanie metod analitycznych wymaga znaczących uproszczeń w modelach problemowych, co powoduje ich nieadekwatność [6] do rozpatrywanej rzeczywistości. Rozwiązanie problemu uzyskane w oparciu o model nieadekwatny jest optymalne dla sytuacji modelowej, a nie rzeczywistej.

W rozwiązywaniu wielu trudnych i złożonych problemów decyzyjnych bardzo pomocne mogą okazać się systemy ekspertowe. Są to dziedzinowe systemy informatyczne zawierające określone zasoby wyspecjalizowanej wiedzy przedmiotowej w postaci reguł decyzyjnych i umożliwiają wykorzystanie jej w sposób interakcyjny przez ich użytkowników. W [12] przedstawiono przykładowy system ekspertowy do wspomagania zarządzania bezpieczeństwem powodziowym aglomeracji miejskiej wykorzystywany między innymi do:

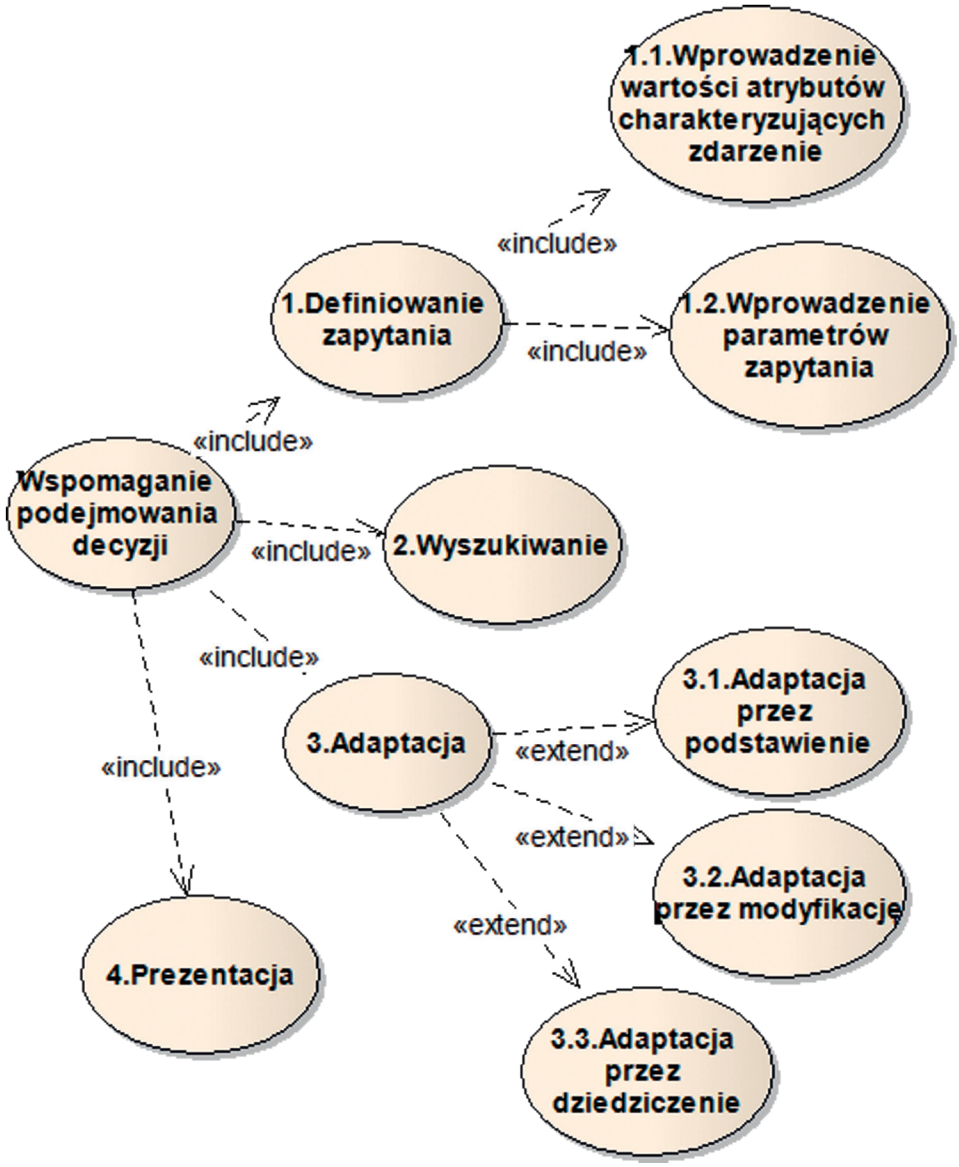
- wyznaczania optymalnej decyzji odnośnie do rodzaju przedsięwzięć związanych z zapewnieniem pożądanego poziomu bezpieczeństwa;
- oceny proponowanych wariantów decyzji według wskazanych kryteriów, takich jak: koszty, straty, ryzyko;
- oceny ryzyka strat i kosztów podejmowanych decyzji z uwzględnieniem preferencji decydenta.

Problemy decyzyjne w wielu obszarach bezpieczeństwa są trudne nawet do heurystycznej algorytmizacji ich rozwiązywania. Opracowanie zaś reguł decyzyjnych w zarządzaniu bezpieczeństwem dziedzinowym jest warunkiem koniecznym tworzenia dziedzinowych systemów ekspertowych. W takich sytuacjach pomocna okazuje się metoda wnioskowania przez analogię [10].

6. Metoda wnioskowania przez analogię we wspomaganiu podejmowania decyzji w bezpieczeństwie

Uwzględniając uwarunkowania informacyjne przy rozwiązywaniu problemów w bezpieczeństwie, jakimi są przede wszystkim: niekompletność, nieokreśloność i niepewność danych, a także nieraz brak pożądanej szczegółowej wiedzy przedmiotowej u decydenta, obiecującym sposobem jego wsparcia decyzyjnego jest zastosowanie metody *wnioskowania przez analogię* – ang. *CBR*. Jako rozwiązanie aktualnego problemu przyjmuje się bezpośrednio, ewentualnie zmodyfikowane

rozwiązania zastosowane w analogicznych zdarzeniach, które miały miejsce wcześniej i przyniosły pozytywne wyniki (rys. 6.1).



Rys. 6.1. Użycie systemu CBR do wspomagania podejmowania decyzji
(Źródło: opracowanie własne)

W metodzie CBR wykorzystuje się wiedzę pozyskaną z wcześniej rozwiązywanych problemów analogicznych, które wystąpiły w zdarzeniach w przeszłości. Aby stworzyć taką możliwość, każde zdarzenie należy opisać, ujmując je w postaci problemu i sposobu jego rozwiązania, oraz zapisać w systemie jako autonomiczny przypadek [10], z którym mieliśmy do czynienia. Najogólniej ujmując, *przypadek* (ang. *case)* to para: *problem i jego rozwiązanie.* Opis i-tego przypadku stanowi zatem para:

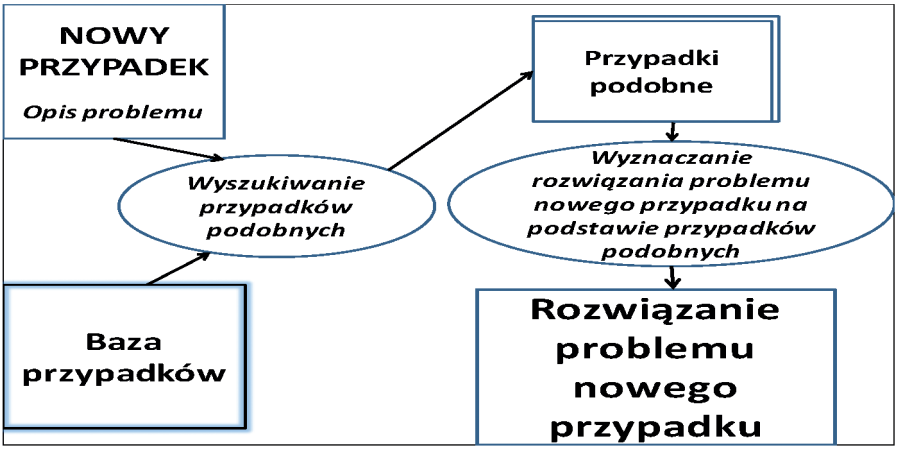
$$C_I = < C_{1,I}, C_{2,I} >, \qquad i = \overline{1, I} \tag{6.1}$$

gdzie:
- $c_{1,i}$ – składowa charakteryzująca problem z i-tego przypadku,
- $c_{2,i}$ – składowa charakteryzująca rozwiązanie problemu i-tego przypadku,
- I – liczba przypadków zgromadzonych w Bazie Przypadków (BP).

Zarówno problem, jak i jego rozwiązanie charakteryzowane są za pomocą atrybutów, które mogą być przedstawione w postaci: liczb, symboli, tekstu, zbiorów wartości, multimediów itp. Poszczególne przypadki są niezależne. Każdy z nich ma zatem swój opis problemu i jego rozwiązania w notacji przyjętej przez inżyniera wiedzy. Rozwiązanie problemu danego przypadku nie jest ujęte w postaci reguł, tak jak w systemach ekspertowych, lecz opisu w określonej notacji, za pomocą jakich sił i środków oraz przedsięwzięć zadanie zostało zrealizowane. Opisy przypadków gromadzone są w BP w postaci przypadków. Istotą metody CBR jest zatem *rozwiązywanie bieżącego problemu poprzez adaptację rozwiązań zastosowanych w przeszłości* [10, 11]. Idea metody bazuje na założeniu, że *podobne problemy mają podobne rozwiązania*, co odpowiada wnioskowaniu przez analogię.

Obszarem zastosowania systemów z BP są dziedziny, które spełniają następujące warunki konieczne [10]:
1) *przewidywalność* – można z dużym prawdopodobieństwem spełnienia podać prognozę przebiegu zdarzenia w zależności od zastosowanych środków oddziaływania na nie;
2) *powtarzalność* – wykonanie kolejny raz tych samych czynności, w tych samych lub podobnych sytuacjach prowadzi do tych samych lub podobnych wyników;
3) *podobieństwo sytuacji*, tzn. podobne problemy mają podobne rozwiązania;
4) *ciągłość modelowanej rzeczywistości*, czyli małe zmiany w modelowanej dziedzinie pociągają za sobą małe zmiany w sposobie rozwiązania problemów.

Metoda CBR może być szczególnie przydatna do wspomagania podejmowania decyzji w kierowaniu ratownictwem: medycznym, pożarowym, technicznym itp. Technologię wyznaczania rozwiązania problemu decyzyjnego z zastosowaniem metody CBR w kierowaniu ratownictwem zilustrowano na rys. 6.2.



Rys. 6.2. Koncepcja użycia systemu CBR do wspomagania decyzji w kierowaniu ratownictwem (Źródło: opracowanie własne)

7. Wsparcie informatyczne w bezpieczeństwie

Warunkiem koniecznym zapewnienia bezpieczeństwa funkcjonowania podmiotu jest znajomość genezy zagrożeń i negatywnych skutków oraz uwarunkowań skutecznego przeciwdziałania tym zagrożeniom. Pozyskanie wiedzy w tym zakresie ułatwia biznesowe modelowanie obiektowe podmiotu – w szczególności modelowanie kontekstowe i przypadków jego użycia w notacji UML [16]. Praktyczne jego stosowanie ułatwiają środowiska programowe wspomagające dokumentowanie wyników modelowania. Ponadto znacząco wspomagają one opracowywanie programów komputerowych do prowadzenia przedmiotowych badań. Najbardziej rozpowszechnione spośród nich to:

1) narzędzia do modelowania w UML, np.: Enterprise Architect, StarUML, Rational Rose, itd.;
2) narzędzia do tworzenia diagramów, np.: EDRAWMAX, SMARTDRAW, itd.

Za pomocą *narzędzi do modelowania w UML* uzyskuje się spójną dokumentację z modelowania przedmiotu badań w postaci diagramów. Narzędzia tego typu wspomagają proces produkcji oprogramowania (kodu źródłowego w języku Java, C++, C# i innych) na podstawie diagramów UML. Wspomaganie to obejmuje generowanie kodu źródłowego, zarządzanie wersjami, testowanie. Dodatkowo wspomaganie takie obejmuje tak zwaną inżynierię odwrotną (ang. *reverse engineering*) – pozwalającą tworzyć dokumentację programową nieudokumentowanego oprogramowania na podstawie kodu źródłowego.

Druga grupa środowisk programowych to narzędzia graficzne służące głównie do prezentacji modeli złożonych systemów. Wynikiem działania takich narzędzi jest plik graficzny w jednym z wielu formatów.

Dokonując wyboru środowiska (narzędzia) programowego do prowadzenia badań, należy mieć na uwadze, że modele obiektowe w UML tworzone są w określonym celu. Mają one wspomagać realizację przedmiotowych analiz, identyfikacji (np. infrastruktury podmiotu), opracowywanie programów komputerowych (np. do prowadzenia wpływu właściwości określonych rodzajów infrastruktury na zdatność funkcjonalną podmiotu) itp.

W zarządzaniu bezpieczeństwem podmiotu wyróżnia się cztery etapy działania: zapobieganie zagrożeniom, przygotowanie na wypadek wystąpienia zagrożeń, reagowanie na zagrożenia i likwidowanie skutków ich wystąpienia. W każdym z tych etapów realizowane są złożone procesy informacyjno-decyzyjne. Analizowane są zagrożenia i ustalane przedsięwzięcia, jakie mają być zrealizowane, aby zapewnić pożądany poziom bezpieczeństwa podmiotu. Przy podejmowaniu decyzji o potrzebie ich wykonania może być niezbędna znajomość czasów i kosztów: realizacji przedsięwzięć, wyodrębnionej grupy ich czynności składowych bądź kosztów skrócenia czasu ich wykonywania. W tym celu strukturę organizacyjną przedsięwzięcia przedstawia się w postaci sieci. Analiza możliwości i kosztów skracania czasu wykonania przedsięwzięcia przez zmniejszanie czasu realizacji określonych jego czynności, przeznaczając na ten cel dodatkowe środki, jest typowym zadaniem organizacyjno-technologicznym. Przyjmując koszt i czas wykonania czynności za wielkość zdeterminowaną, przedmiotową analizę można przeprowadzić *metodą CPM – COST* [3, 11] Do określania wartości analogicznych charakterystyk przedsięwzięcia, gdy czasy wykonywania czynności są losowe, stosowana jest *metoda PERT* [3, 4, 11, 12]. Bieżącą kontrolę i dokonywanie ewentualnych korekt czynności w trakcie realizacji przedsięwzięcia, zwłaszcza tych, które są związane z synchronizacją przebiegu poszczególnych składowych, przeprowadza się przy zastosowaniu Diagramu Gantta [11]. Praktyczne stosowanie przedstawionych metod do przedmiotowych analiz sieciowych związane jest z koniecznością wykonywania złożonych i czasochłonnych obliczeń. Niezwykle pomocny w ich realizacji okazuje się moduł programowy PERT – CPM pakietu WinQSB 2.0. Przykładowe analizy sieciowe realizacji przedsięwzięć w bezpieczeństwie za pomocą tego modułu programowego przedstawiono w [11].

Wyróżnia się trzy metody wspomagania podejmowania decyzji w bezpieczeństwie bazujące na wiedzy ekspertów: systemy ekspertowe, wnioskowanie przez analogię i metody eksperckie. W rozwiązywaniu problemów z zastosowaniem systemów ekspertowych wykorzystywana jest dziedzinowa wiedza ekspertów ujęta w postaci reguł. Opracowywane są z wykorzystaniem oprogramowania szkieletowego wykonanego zazwyczaj w środowisku systemu szkieletowego, np. AITECH Sphinx przy użyciu PC-SHELL [14], co istotnie skraca czas ich wytwarzania.

Do wspomagania rozwiązywania problemów, dla których występują istotne trudności ujęcia wiedzy w postaci reguł decyzyjnych, mogą być stosowane systemy informatyczne z zastosowaniem *metody wnioskowania przez analogię*. Ich wytwarzanie ułatwiają środowiska programowe MYCBR i jCOLIBRI [2] bazujące na języku JAVA.

W rozwiązywaniu problemów, dla których nie opracowano systemów komputerowego wspomagania, stosowane są metody eksperckie [11]. Ich mankamentem jest złożoność organizacyjna rozwiązywania problemu i długi czas niezbędny na jego uzyskanie. Opracowano trzy rodzaje programów komputerowego wspomagania stosowania metod eksperckich do rozwiązywania problemów w zarządzaniu bezpieczeństwem [12]:

1) edytory graficzne, np. EDRAWMAX [18], Essential Diagram, SWOT-Manager;
2) programy specjalizowane, np. SWOT-Manager, SWOT-ANALYSIS;
3) specjalizowane witryny internetowe, np. Creately, WIKISWOT, CYMEON, GLIFFY.

Wymienione rodzaje programów wspomagają przede wszystkim stosowanie metod: Delphi, SWOT, burzy mózgów oraz sporządzania diagramu Ishikawy, przy czym Delphi i SWOT posiadają dostępne w Internecie aplikacje programowe. Pozostałe metody są wspierane jedynie w zakresie ułatwień przy tworzeniu i prezentacji graficznej modeli opracowywanych za pomocą wymienionych metod.

8. Podsumowanie

Zapewnienie podmiotowi pożądanego poziomu bezpieczeństwa wymaga permanentnej analizy zagrożeń i potrzeby podejmowania przedsięwzięć zapobiegających ich powstawaniu, ciągłego monitorowania ewentualności ich wystąpienia i przeciwdziałania, gdy zajdzie taka konieczność. Zarządzanie bezpieczeństwem cechuje złożoność problemów decyzyjnych wynikająca z konieczności uwzględniania dużej liczby czynników, wieloskładnikowa funkcja kryterium, silne ograniczenie na czasy rozwiązania problemów, niepewność i nieokreśloność danych, na podstawie których podejmowane są decyzje, a szczególnie niepewność odnośnie do uwarunkowań i następstw ich wdrożenia.

Trafność decyzji podejmowanych w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem zależy od adekwatności modelu do rozpatrywanej rzeczywistości, w oparciu o który podejmowane są decyzje o niezbędnych przedsięwzięciach do zapewnienia bezpieczeństwa funkcjonowania podmiotu oraz wiarygodności danych z szeroko rozumianego monitoringu zagrożeń i stanu sił i środków, które mogą być użyte w ratownictwie.

W zarządzaniu bezpieczeństwem, a w szczególności w kierowaniu ratownictwem, występuje silna presja czasu i potrzeba uwzględniania wielu czynników przy

podejmowaniu przedmiotowych decyzji. Stąd konieczność informatycznego wspierania realizowanych w ich ramach procesów informacyjno-decyzyjnych.

LITERATURA:

1. A. Ameljańczyk, *Optymalizacja wielokryterialna*, Wydział Wydawniczy WAT, Warszawa 1986.
2. T.R. Berghofer i inni, *Building case-based reasoning applications with mycbr and colibri studio. In Proceedings of the UKCBR 2012 Workshop*, Springer, 2012.
3. A. Fusek, K. Nowak, H. Podlewski, *Analiza drogi krytycznej. CPM i PERT*, PWE, Warszawa 1967.
4. A.Z. Idźkiewicz, *PERT. Metody analizy sieciowej*, PWN, Warszawa 1967.
5. I. Kaliszewski, *Wielokryterialne podejmowanie decyzji*, WNT, Warszawa 2008.
6. E. Kołodziński, *Symulacyjne metody badania systemów*, PWN, Warszawa 2002.
7. E. Kołodziński, *O problemie oceny bezpieczeństwa podmiotu oraz skuteczności i efektywności działania Dziedzinowego Systemu Bezpieczeństwa Podmiotu*, w monografii *Bezpieczeństwo - wymiar współczesny i perspektywy badań* pod redakcją Mirosława Kwiecińskiego, Kraków 2010, s. 71-86.
8. E. Kołodziński, *Wprowadzenie do zarządzania bezpieczeństwem podmiotu*, praca zbiorowa pod redakcją Z. Mierczyka i R. Ostrowskiego pt. *Ochrona przed skutkami nadzwyczajnych zagrożeń*, tom 2, Wydawnictwo WAT, Warszawa 2011.
9. E. Kołodziński, *Ryzyko decyzji w zarządzaniu bezpieczeństwem powszechnym podmiotu. Współczesny wymiar bezpieczeństwa w aspekcie zmienności zagrożeń - Ratownictwo 2011*, WSZOP, Katowice 2012, s. 89-104, ISBN: 978-83-61378-31-0.
10. E. Kołodziński, *Wprowadzenie do wspomagania zarządzania bezpieczeństwem i kierowania ratownictwem z zastosowaniem metody wnioskowania przez analogię*, 2012, http://ptib.pl/pl/component/remository/?func=fileinfo&id=503.
11. E. Kołodziński, T. Lachowicz, Ł. Tomczyk, P. Zapert, *Wspomaganie decyzji w bezpieczeństwie*, Wyd. WAT, Warszawa 2014.
12. E. Kołodziński, T. Lachowicz, Ł. Tomczyk, P. Zapert, *Modelowanie w inżynierii bezpieczeństwa*, Wyd. WAT, Warszawa 2014.
13. E. Kołodziński, *Identyfikacja bazowych potrzeb infrastrukturalnych podmiotu z zastosowaniem modelowania obiektowego*, 2014, http://ptib.pl/pl/component/remository/?func=select&id=168.
14. K. Michalik, *PC-Shell Szkieletowy System Ekspertowy*, *Cz. II, Podręcznik inżyniera wiedzy*, Aitech, Katowice 2006.
15. A. Szymonik, *Logistyka w bezpieczeństwie*, Difin, Warszawa 2010.
16. M. Śmiałek, *Zrozumieć UML 2.0 – metody modelowania obiektowego*, Helion, Gliwice 2005.
17. WIKIPEDIA - http://pl.wikipedia.org/wiki/Proces_decyzyjny
18. Witryna firmy EDRAWSOFT – www.edrawsoft.com

PROBLEMS OF SUPPORTING DECISION-MAKING IN SECURITY

Abstract: In this paper the fundamental problems in the management of safety and directing rescue systems were considered. The factors that cause risks in decision making include: the common randomness in safety, concerning the risks and vulnerability of the entity, the effects of threat, the costs of prevention and response in case of the event, and so on. The notion of risk in safety and its measure were defined, and proposed the form of quality decision-making measurement in safety, taking into account the risk of its undertaking. It was analyzed the possibilities and conditions of use in safety management and directing rescue systems: multi-criterial optimization, network analysis, computer simulation, expert methods, expert systems and systems of analogy reasoning, and computer support in their designation.
Keywords: unit security, decision risk, decision metric value, decision support methods.