Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 235 · 2015

Edward Kołodziński

Wojskowa Akademia Techniczna
Instytut Optoelektroniki
ekolodzinski@wp.pl

Tomasz Lachowicz

Uniwersytet Warmińsko-Mazurski w Olsztynie
Wydział Nauk Technicznych
Katedra Inżynierii Bezpieczeństwa
tomasz_lachowicz@wp.pl

Łukasz Tomczyk

Uniwersytet Warmińsko-Mazurski w Olsztynie
Wydział Nauk Technicznych
Katedra Inżynierii Bezpieczeństwa
korazzone@tlen.pl

Piotr Zapert

Wojskowa Akademia Techniczna
Instytut Optoelektroniki
piotrzapert@gmail.com

PROBLEMY WSPOMAGANIA PODEJMOWANIA DECYZJI W BEZPIECZEŃSTWIE

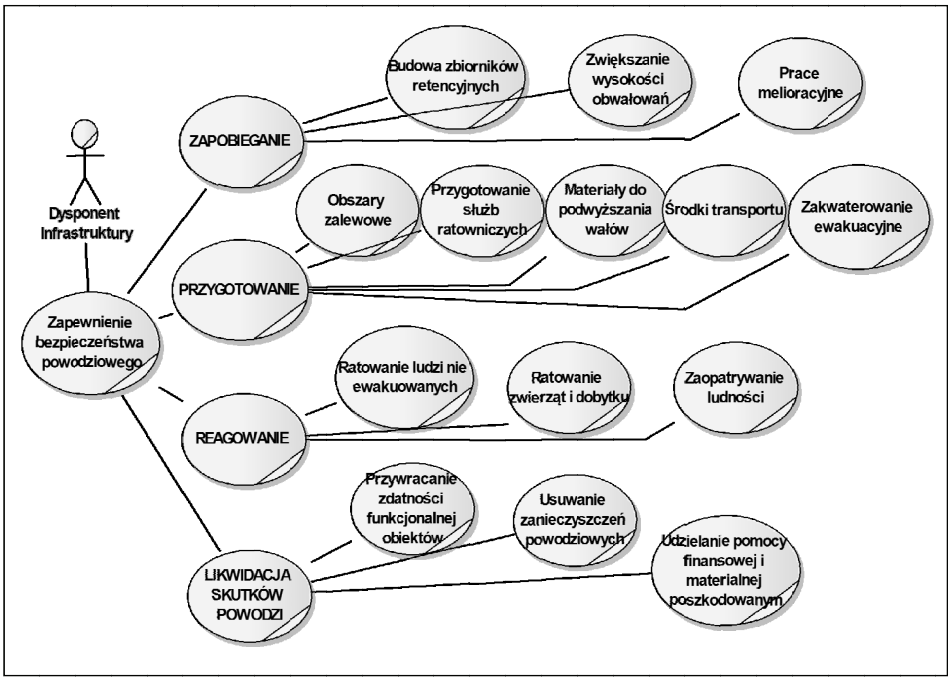
Streszczenie: W artykule rozpatrzono podstawowe problemy występujące w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem. Powszechna losowość w bezpieczeństwie dotycząca: zagrożeń i podatności na nie podmiotu, skutków zagrożeń, kosztów zapobiegania im i reagowania w przypadku wystąpienia itd. to czynniki, które powodują ryzyko podejmowanych decyzji. Zdefiniowano pojęcie ryzyka w bezpieczeństwie i jego miary. Zaproponowano postać miary jakości decyzji w zagadnieniach bezpieczeństwa, uwzględniającą ryzyko jej podjęcia. Dokonano analizy możliwości i uwarunkowań wykorzystania w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem: optymalizacji wielokryterialnej, analiz sieciowych, symulacji komputerowej, metod eksperckich, systemów ekspertowych oraz systemów wnioskowania przez analogię i komputerowego wspomagania ich wyznaczania.

Słowa kluczowe: bezpieczeństwo podmiotu, ryzyko decyzji, optymalizacja decyzji, komputerowe wspomaganie podejmowania decyzji.

Wprowadzenie

Dla zapewnienia pożądanego poziomu bezpieczeństwa funkcjonowania podmiotu [Kołodziński, 2010, 2011] niezbędna jest permanentna analiza jego zagrożeń oraz konieczność określania sposobu wykonywania przedsięwzięć: zapobiegających ich powstawaniu i przygotowawczych na wypadek wystąpie-

nia. 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 jego systemu bezpieczeństwa, tj. służb, inspekcji, podmiotów gospodarczych i administracji na ich wystąpienie. Analizę możliwych rodzajów przedsięwzięć do wykonywania w celu zapewnienia bezpieczeństwa dziedzinowego podmiotu zilustrowano na przykładzie bezpieczeństwa powodziowego aglomeracji miejskiej położonej w dolinie, przez którą przepływa rzeka (rys. 1).



Rys. 1. Diagram biznesowych przypadków użycia systemu bezpieczeństwa powodziowego aglomeracji

Źródło: [Kołodziński i in., 2015].

Cechą charakterystyczną zarządzania bezpieczeństwem i kierowania ratownictwem jest: złożoność problemów decyzyjnych wynikająca z konieczności uwzględniania dużej liczby czynników, zazwyczaj wieloskładnikowa funkcja kryterium optymalizacji decyzji [Ameljańczyk, 1986; Kaliszewski, 2008], 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 kierowanie ratownictwem powinny być realizowane z zastosowaniem modeli adekwatnych do rozwiązywanych problemów [Kołodziński, 2002], z wykorzystaniem zweryfikowanych w praktyce narzędzi programowych do przeprowadzania stosownych obliczeń. Warunek ich stosowania przez decydenta stanowi znajomość podstawowych metod wspomagania podejmowania 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.

Niniejszy artykuł stanowi przeglądową prezentację aktualnych wyników prac prowadzonych przez autorów nad doskonaleniem komputerowego wspomagania zarządzania bezpieczeństwem i kierowania ratownictwem.

1. Niepewność decydenta w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem

Każda analiza w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem poprzedzająca podjęcie decyzji przeprowadzana jest *a priori*, na podstawie przyjętego modelu sytuacyjnego oraz danych 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 kierowaniu ratownictwem występuje *ryzyko* następstw innych od zakładanych przy jej podejmowaniu [Kołodziński, 2012]. Dotyczy ono zarówno strat, jak i kosztów. Wartość ryzyka będzie zależała od trafności prognozy, zaś trafność prognozy od wiarygodności danych i adekwatności zastosowanego modelu prognostycznego [Kołodziński, 2002]. Uwzględniając powyższe uwarunkowania można wysnuć 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 [Kołodziński, 2011; Kołodziński i in., 2014]:

$$\mathrm{E}(R(d_i)) = < \mathrm{E}(R_1(d_i)), \mathrm{E}(R_2(d_i)) >, \; i = \overline{1, I} \tag{1}$$

gdzie:

– E – symbol wartości przeciętnej,
– $R_1(d_i) = < R_{11}(d_i), R_{12}(d_i) >$ – ryzyko strat [Kołodziński, 2012] innych od prognozowanych:

- $R_{11}(d_i)$ – ryzyko strat niematerialnych:

$$R_{11}(d_i) = S_1^{\text{inn}}(d_i) - S_1(d_i), \tag{2}$$

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

$$R_{12}(d_i) = S_2^{\text{inn}}(d_i) - S_2(d_i), \tag{3}$$

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

$$R_2(d_i) = K^{\text{inn}}(d_i) - \mathrm{E}(K(d_i)), \tag{4}$$

– $S(d_i)$ – straty poniesione przez podmiot przy decyzji d_i,
– $K(d_i)$ – koszty realizacji decyzji d_i,
– I-liczność zbioru decyzji.

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

2. Miara jakości decyzji w zagadnieniach bezpieczeństwa

Naturalnym dążeniem decydenta jest, aby straty ponoszone przez podmiot oraz koszty wynikające z jego decyzji były minimalne, a 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 będącą trójką [Kołodziński i in., 2014]:

$$M(d_i) = < M_1(d_i), M_2(d_i), M_3(d_i) >,\ d_i \in \mathbf{D}, \tag{5}$$

gdzie:
– $M_1(d_i) = \mathrm{E}(S(d_i))$ – wartość przeciętna prognozowanych strat poniesionych przez podmiot wskutek wystąpienia danego rodzaju zagrożenia, pomimo zrealizowania decyzji $d_i \in \mathbf{D}$,
– $M_2(d_i) = \mathrm{E}(K(d_i))$ – wartość przeciętna prognozowanych kosztów realizacji decyzji $d_i \in \mathbf{D}$,
– $M_3(d_i) = \mathrm{E}(R(d_i))$ – wartość przeciętna ryzyka następstw realizacji decyzji $d_i \in \mathbf{D}$, np. (1),
– **D** – zbiór decyzji dopuszczalnych o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu,

przy czym wielkości oznaczone symbolami: S, K, R są losowe, a ich jednostki określa analityk.

Poszczególne składowe funkcji kryterium (5) w różnym stopniu mogą być preferowane przez decydenta – mogą mieć dla niego różne wagi. Aby uwzględnić ten fakt, funkcja kryterium (5) zostanie zmodyfikowana do postaci:

$$M^w(d_i) = < M_1{}^w(d_i),\ M_2{}^w(d_i),\ M_3{}^w(d_i) >,\ d_i \in \mathbf{D}, \tag{6}$$

gdzie np.:

- $M_g{}^w(d_i) = w_g M_g(d_i),\ g = \overline{1,3}$
- w_g – stopień preferowania (waga) g-tej składowej (6) przez decydenta przy podejmowaniu decyzji o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu.

Wielkość (6) 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 $\mathbf{R}_\mathrm{d}$ [Ameljańczyk, 1986; Kołodziński i in., 2014]:

$$\mathbf{R}_d \subset \mathbf{Y} \times \mathbf{Y}, \tag{7}$$

gdzie:

- $\mathbf{Y}$ – zbiór możliwych wartości ocen jakości (6) decyzji w zagadnieniach zapewnienia bezpieczeństwa funkcjonowania podmiotu:

$$\mathbf{Y} \subset \mathbf{R}^3, \tag{8}$$

- $\mathbf{R}_d$ – 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"). Relację dominowania określa analityk.

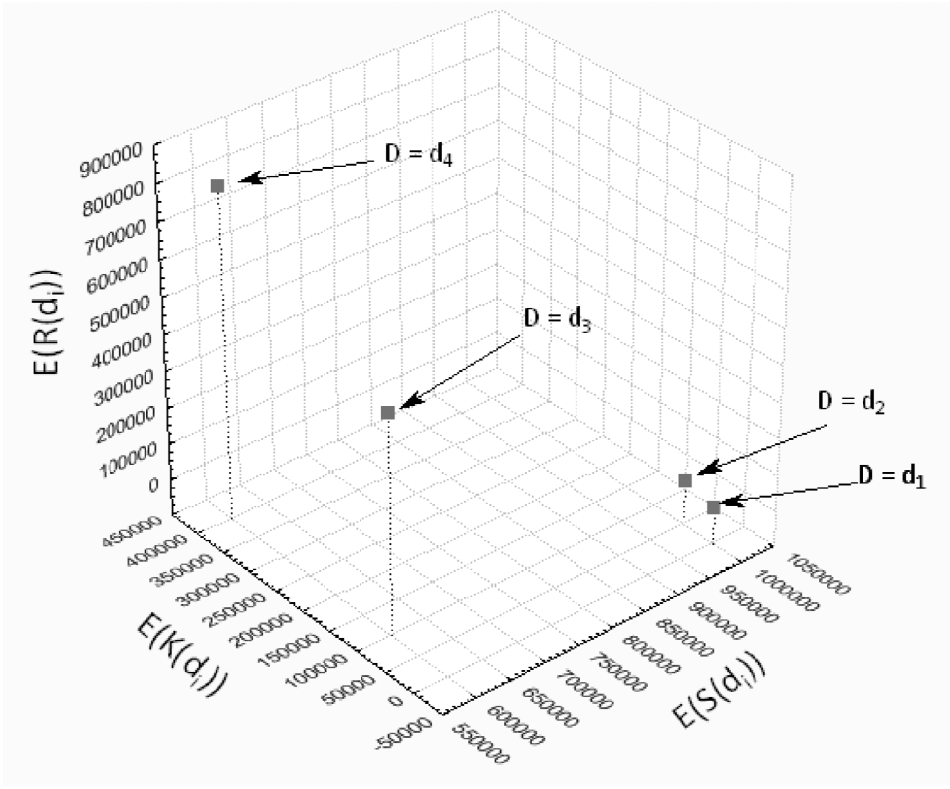
W przypadku trójskładnikowej funkcji kryterium optymalizacji (6) każdej decyzji ze zbioru **D** dopuszczalnych o sposobie zapewnienia bezpieczeństwa funkcjonowania podmiotu odpowiada trójka liczb określająca punkt w trójwymiarowym układzie kartezjańskim, w odpowiedniej odległości od punktu odpowiadającego decyzji *idealnej* o współrzędnych <0, 0, 0>. W zależności od arbitralnie przyjętej przez decydenta miary odległości rozpatrywanych decyzji od idealnej [Kołodziński i in., 2014; Kołodziński i in., 2015] różne będą wyniki optymalizacji. Omawiane zagadnienie zostanie zilustrowane na poniższym przykładzie, zaczerpniętym z [Kołodziński i in., 2014].

Przykład 1.

Dla podmiotu o pewnej wartości należy określić optymalny sposób zapewnienia bezpieczeństwa jego funkcjonowania, przy czym dane są [Kołodziński i in., 2014]:

1) zbiór decyzji dopuszczalnych $\mathbf{D} = \{d_1, d_2, d_3, d_4\}$;
2) każdej decyzji $d_i \in \mathbf{D}$ ($i = \overline{1,4}$) odpowiada:
   a) koszt jej realizacji k_i,
   b) prawdopodobieństwa zapobiegnięcia zagrożeniom p_i;
3) funkcja kryterium optymalizacji określona jest wzorem (5).

Dla danych przyjętych w [Kołodziński i in., 2014] wyniki obliczeń zilustrowano na rys. 2.



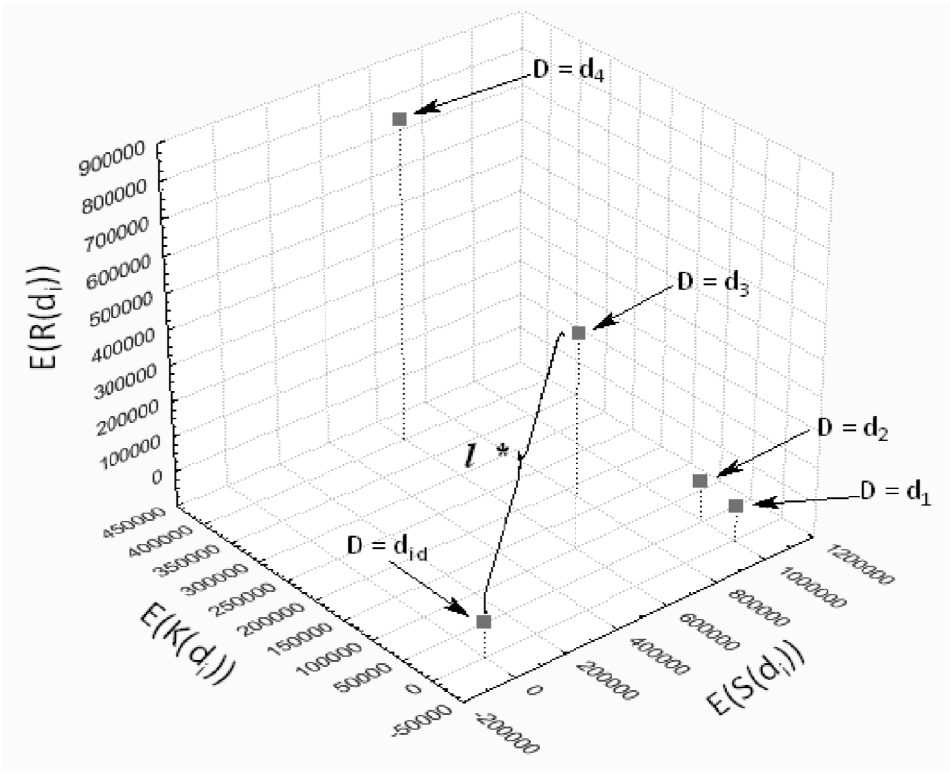
Rys. 2. Ilustracja wyników obliczeń strat łącznych, kosztów decyzji i ryzyka w zagadnieniu optymalizacji decyzji o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania podmiotu (przyjęto, że jednostki na osiach ustalił analityk)

Źródło: Kołodziński i in. [2014].

Z analizy następstw poszczególnych decyzji dopuszczalnych, w świetle miary jakości decyzji (5), 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, 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). Dla innej miary odległości może ulec zmianie rozwiązanie przyjmowane za optymalne.



Rys. 3. Ilustracja wyznaczania decyzji optymalnej w rozpatrywanym w przykładzie zagadnieniu optymalizacji decyzji o sposobie zapobiegania zagrożeniom bezpieczeństwa funkcjonowania podmiotu

Źródło: Kołodziński i in. [2014].

3. 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 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 na podstawie posiadanej przez decydenta wiedzy empirycznej i przy wykorzystaniu 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 [Kołodziński i in., 2014]. W literaturze dotyczącej optymalizacji wielokryterialnej opisanych jest wiele metod wyznaczania rozwiązań optymalnych przy ważonych składowych funkcji kryterium [Kaliszewski, 2008]. 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, a także jego ostrożność w podejmowaniu decyzji. Powyższe stwierdzenia oparte są na zamieszczonych w [Kołodziński i in., 2014] wynikach badań przeprowadzonych na przykładzie optymalizacji decyzji o sposobie zapewnienia bezpieczeństwa powodziowego aglomeracji położonej w dolinie, przez którą przepływa rzeka.

4. 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 [Śmiałek, 2005]. 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 [Kołodziński i in., 2015], zaś dla potrzeb ustalania bazowej infrastruktury podmiotu w pracy [www 2].

Przy rozwiązywaniu problemów w bezpieczeństwie sformułowanych w postaci zadań optymalizacyjnych powinny być preferowane metody analityczne [Kaliszewski, 2008], a tam, gdzie nie jest możliwe ich zastosowanie, metoda symulacyjna [Kołodziński, 2002]. Stosowanie metod analitycznych wymaga znaczących uproszczeń w modelach problemowych, co powoduje ich nieadekwatność [Kołodziński, 2002] do rozpatrywanej rzeczywistości. Rozwiązanie problemu uzyskane na podstawie modelu nieadekwatnego jest optymalne dla sytuacji modelowej, a nie rzeczywistej.

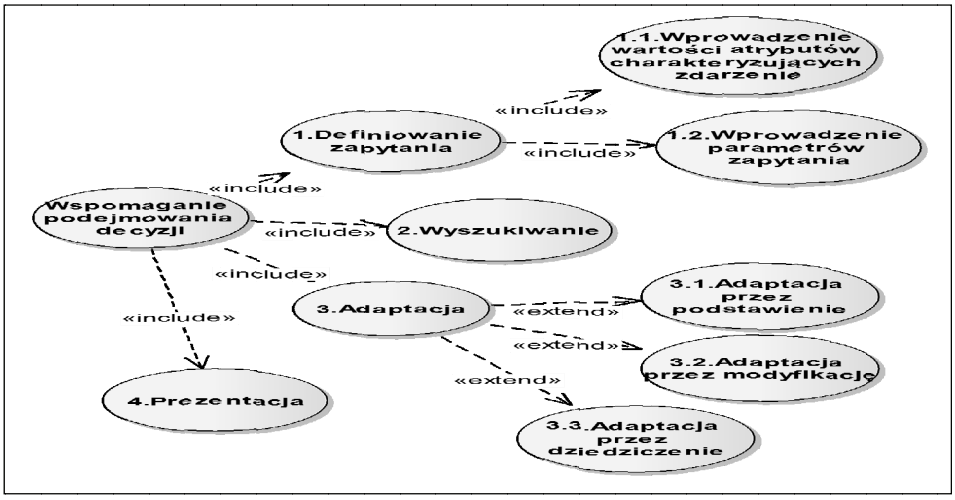
W rozwiązywaniu wielu trudnych i złożonych problemów decyzyjnych bardzo pomocne mogą okazać się systemy ekspertowe. Są to dziedzinowe systemy informatyczne zawierające określone zasoby wyspecjalizowanej wiedzy przedmiotowej w postaci reguł decyzyjnych i umożliwiają wykorzystanie jej w sposób interakcyjny przez ich użytkowników. W [Kołodziński i in., 2015] przedstawiono przykładowy system ekspertowy do wspomagania zarządzania bezpieczeństwem powodziowym aglomeracji miejskiej wykorzystywany m.in. 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 [www 1].

5. 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. 4.).



Rys. 4. Użycie systemu CBR do wspomagania podejmowania decyzji

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 [www 1], z którym mieliśmy do czynienia. Najogólniej ujmując, *przypadek* (ang. *case)* to para: *problem i jego rozwiązanie.* Opis *i*-tego przypadku stanowi zatem para:

$$c_i = < c_{1,i}, c_{2,i} >, \; i = \overline{1, I}, \tag{9}$$

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 w formie 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* [www 1; Kołodziński i in., 2014]. Idea metody bazuje na założeniu, że *podobne problemy mają podobne rozwiązania,* co odpowiada wnioskowaniu przez analogię.

W metodzie CBR naśladowany jest proces podejmowania decyzji przez człowieka, w którym można wyróżnić cztery etapy [www 1]:

1) *wyszukanie* (ang. *retrieve)* w BP przypadków najbardziej podobnych do rozpatrywanego;
2) *wykorzystanie* (ang. *reuse)* rozwiązań zastosowanych w wybranych z BP przypadkach najbardziej podobnych do bieżącego do wyznaczenia rozwiązania problemu w nim występującego;
3) *ocena przydatności* (ang. *revise) wyznaczonego* rozwiązania w przyszłości. Jeśli ocena jest pozytywna, to nowe zdarzenie jest archiwizowane w BP jako nowy przypadek;
4) *zapamiętanie* (ang. *retain)* rozpatrywanego problemu wraz z zastosowanym jego rozwiązaniem jako nowego przypadku (doświadczenia) w celu późniejszego wykorzystania podczas rozwiązywania nowych problemów w przyszłości.

Obszarem zastosowania systemów z BP są dziedziny, które spełniają następujące warunki konieczne [www 1]:

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.

Do podstawowych zalet metody CBR, które odróżniają ją od innych technik rozwiązywania zadań, można zaliczyć następujące cechy:

1) *Nie wymaga od decydenta bardzo szczegółowej znajomości dziedziny, z której pochodzi problem.* Wiedza o dziedzinie na początku nie musi być kompletna. Może być zdobywana sukcesywnie podczas zapoznawania się z problemami i zastosowanymi w nich rozwiązaniami w analogicznych przypadkach, które zostały zarchiwizowane w BP. Zastosowanie CBR pozwala uczyć się na sukcesach i błędach. Gdy budowany jest system CBR, nie musi być znany sposób rozwiązania problemu, wystarczy podać jego rozwiązanie bez wskazywania reguł, na podstawie których powstało. Cecha ta w sposób znaczący odróżnia CBR od systemów opartych na regułach;
2) *Proste uczenie się systemu*. Sprowadza się do dopisywania nowych przypadków do BP. Zwiększana jest w ten sposób jej liczebność, a co za tym idzie, wzrasta potencjalna możliwość, że przypadek, który wystąpi w przyszłości, będzie problemowo bliższy jednemu z BP niż bez dopisanego;
3) *Redukcja kosztów pozyskania wiedzy, zmniejszenie wysiłku włożonego w rozwiązywanie nowego problemu, łatwość implementacji metody, stosunkowo niewielki koszt utrzymania systemu w porównaniu z systemami ekspertowymi, wykorzystanie wiedzy zawartej w zgromadzonych przypadkach, możliwość szybkiego uzyskania propozycji rozwiązań problemu, łatwość opanowania i używania metody,* a przede wszystkim *wysoka akceptowalność przez użytkowników końcowych*.

Podstawowe ograniczenia stosowania metody CBR wynikają przede wszystkim z ograniczeń technik stosowanych w każdej z faz jej cyklu. Rozpatrywane są one w kontekście niedogodności praktycznego stosowania. Podstawowe z nich to przede wszystkim:

1) ograniczenie do dziedzin, które spełniają omówione wyżej warunki konieczne: *przewidywalność, powtarzalność, podobieństwo sytuacji, ciągłość modelowanej dziedziny*.

2) niezbędna jest hierarchizacja atrybutów, ze względu na które dokonywany jest wybór z BP przypadków najbardziej podobnych do nowego zdarzenia. Wymaga to dodatkowej wiedzy od użytkownika metody;
3) praktycznie jest użyteczna przy dużej liczbie przypadków zgromadzonych w BP. Od liczności przypadków w BP z dziedziny nowego zdarzenia, trafności ich scharakteryzowania za pomocą atrybutów zależy, czy znaleziony przypadek będzie bardziej lub mniej podobny do rozpatrywanego. Im więcej przypadków zostanie zarchiwizowanych w BP, tym potencjalnie można uzyskać lepsze przybliżenie przypadków z bazy do rozpatrywanego;
4) kolejnym mankamentem metody CBR jest konieczność opracowania miary podobieństwa dostosowanej do reprezentacji przypadków i metody przeszukiwania BP. Może to stanowić bardzo duże utrudnienie w jej stosowaniu.

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. 5.

Rys. 5. Koncepcja użycia systemu CBR do wspomagania decyzji w kierowaniu ratownictwem

6. 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 [Śmiałek, 2005]. 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 in.) na podstawie diagramów UML. Wspomaganie to obejmuje generowanie kodu źródłowego, zarządzanie wersjami, testowaniem. Dodatkowo wspomaganie takie obejmuje tzw. 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 następujące etapy działania: zapobieganie zagrożeniom, przygotowanie na wypadek wystąpienia zagrożeń, reagowanie na zagrożenia i likwidowanie skutków ich wystąpienia. W każdy z tych etapów realizowane są złożone procesy informacyjno-decyzyjne. Analizowane są zagrożenia i ustalane są przedsięwzięcia, jakie mają być zrealizowane, aby zapewnić pożądany poziom bezpieczeństwa podmiotu, w szczególności zaś przedsięwzięcia logistyczne [Szymonik, 2010]. 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 reali-

zacji określonych jego czynności dzięki przeznaczeniu na ten cel dodatkowych środków jest typowym zadaniem organizacyjno-technologicznym. Przyjmując koszt i czas wykonania czynności za wielkość zdeterminowaną, przedmiotową analizę można przeprowadzić *metodą CPM – COST* [Fusek, Nowak i Podlewski, 1967; Kołodziński i in., 2014]. Do określania wartości analogicznych charakterystyk przedsięwzięcia, gdy czasy wykonywania czynności są losowe, stosowana jest *metoda PERT* [Fusek, Nowak i Podlewski, 1967; Idźkiewicz, 1967; Kołodziński i in., 2014; Kołodziński i in., 2015]. 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 [Kołodziński i in., 2014]. 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 [Kołodziński i in., 2014].

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 [Michalik, 2006], 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 [Berghofer, 2012], bazujące na języku JAVA.

W rozwiązywaniu problemów, dla których nie opracowano systemów komputerowego wspomagania, stosowane są metody eksperckie [Kołodziński i in., 2014]. 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 [Kołodziński i in., 2015]:

1) edytory graficzne, np. EDRAWMAX [www 4], 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 sporządzanie 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.

Podsumowanie

Jednym z czynników warunkujących zdatność funkcjonalną podmiotu jest bezpieczeństwo jego funkcjonowania. 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. Analityk bezpieczeństwa w ramach realizacji swoich zadań musi podejmować wiele arbitralnych decyzji odnośnie do: miar jakości wyznaczanych rozwiązań, zastosowanych metod rozwiązywania problemów, możliwości i zakresu wsparcia informatycznego w realizacji procesów analityczno-decyzyjnych itd.

Trafność decyzji podejmowanych w zarządzaniu bezpieczeństwem i kierowaniu ratownictwem zależy od adekwatności do rozpatrywanej rzeczywistości modelu, na podstawie którego podejmowane są decyzje o przedsięwzięciach niezbędnych do zapewnienia bezpieczeństwa funkcjonowania podmiotu oraz wiarygodności danych z szeroko rozumianego monitoringu zagrożeń i stanu sił i środków, które mogą być użyte w ratownictwie. Szczegółową dyskusję tego zagadnienia przeprowadzono w [Kołodziński i in., 2014].

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 ramach nich procesów informacyjno-decyzyjnych.

Literatura

Ameljańczyk A. (1986), *Optymalizacja wielokryterialna*, Wydział Wydawniczy WAT, Warszawa.

Berghofer T.R. i in. (2012), *Building case-based reasoning applications with myCBR and COLIBRI studio* [w:] *Proceedings of the UKCBR 2012 Workshop*, Springer.

Fusek A., Nowak K., Podlewski H. (1967), *Analiza drogi krytycznej. CPM i PERT*, PWE, Warszawa.

Idźkiewicz A.Z. (1967), *PERT. Metody analizy sieciowej*, PWN, Warszawa.

Kaliszewski I. (2008), *Wielokryterialne podejmowanie decyzji*, WNT, Warszawa.

Kołodziński E. (2002), *Symulacyjne metody badania systemów*, Wydawnictwo Naukowe PWN, Warszawa.

Kołodziński E. (2010), *O problemie oceny bezpieczeństwa podmiotu oraz skuteczności i efektywności działania Dziedzinowego Systemu Bezpieczeństwa Podmiotu* [w:] M. Kwieciński (red.), *Bezpieczeństwo – wymiar współczesny i perspektywy badań*, Akademia Frycza Modrzewskiego, Kraków.

Kołodziński E. (2011), *Wprowadzenie do zarządzania bezpieczeństwem podmiotu* [w:] Z. Mierczyk, R. Ostrowski (red.), *Ochrona przed skutkami nadzwyczajnych zagrożeń*, tom 2, Wydawnictwo WAT, Warszawa.

Kołodziński E. (2012), *Ryzyko decyzji w zarządzaniu bezpieczeństwem powszechnym podmiotu. Współczesny wymiar bezpieczeństwa w aspekcie zmienności zagrożeń – Ratownictwo 2011*, Wydawnictwo WSZOP, Katowice.

Kołodziński E., Lachowicz T., Tomczyk Ł., Zapert P. (2014), *Wspomaganie decyzji w bezpieczeństwie*, Wydawnictwo WAT, Warszawa.

Kołodziński E., Lachowicz T., Tomczyk Ł., Zapert P. (2015), *Modelowanie w inżynierii bezpieczeństwa*, Wydawnictwo WAT, Warszawa.

Michalik K. (2006), *PC-Shell szkieletowy system ekspertowy*. *Podręcznik inżyniera wiedzy*, część 2, Aitech, Katowice.

Szymonik A. (2010), *Logistyka w bezpieczeństwie*, Difin, Warszawa.

Śmiałek M. (2005), *Zrozumieć UML 2.0 – metody modelowania obiektowego*, Helion, Gliwice.

[www 1] Kołodziński E., *Wprowadzenie do wspomagania zarządzania bezpieczeństwem i kierowania ratownictwem z zastosowaniem metody wnioskowania przez analogię*, czasopismo internetowe „Zagadnienia Inżynierii Bezpieczeństwa", 2012, http://ptib.pl/pl/component/remository/?func=fileinfo&id=503 (dostęp: 10.08.2014).

[www 2] Kołodziński E., *Identyfikacja bazowych potrzeb infrastrukturalnych podmiotu z zastosowaniem modelowania obiektowego*, czasopismo internetowe „Zagadnienia Inżynierii Bezpieczeństwa", 2014, http://ptib.pl/pl/component/remository/?func=select&id=168 (dostęp: 10.08.2014).

[www 3] https://pl.wikipedia.org/wiki/Proces_decyzyjny (dostęp: 10.08.2014).

[www 4] www.edrawsoft.com (dostęp: 10.08.2014).

PROBLEMS OF SUPPORTING DECISION-MAKING IN SAFETY

Summary: 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: safety of an entity, decision-making risk, optimization of the decision, computer aided decision-making.