Zeszyty Naukowe SGSP 2018, Nr 66 (TOM 2)/2/2018

dr hab. inż. Jarosław Prońko, prof. UJK
Wydział Prawa, Administracji i Zarządzania
Uniwersytet Jana Kochanowskiego w Kielcach

mgr Beata Wojtasiak
Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy

Analiza wielokryterialna w badaniach nad bezpieczeństwem

Abstrakt

Celem artykułu jest prezentacja metodyki oceny poziomu bezpieczeństwa wykorzystującej analizę wielokryterialną. Analiza wielokryterialna kojarzona jest najczęściej z problematyką podejmowania decyzji, która powinna optymalizować więcej niż jedną funkcję celu. Jednoznaczne rozwiązanie takich problemów jest niemożliwe, ponieważ decyzja optymalna dla jednego z celów nie jest jednocześnie decyzją optymalną dla pozostałych. Udowodnił to już włoski ekonomista i socjolog V. Pareto, wprowadzając pojęcie zbioru decyzji niezdominowanych. Jest to zbiór decyzji, z których każda jest lepsza od pozostałych pod względem jednego z kryteriów wyboru. Istnieje wiele metod rozwiązywania takich problemów. Sprowadzają się one do sposobu połączenia wszystkich kryteriów wyboru w jedno metakryterium. To połączenie może odbywać się na drodze matematycznej lub heurystycznej. Do drugiej grupy należy metoda Analytic Hierarchy Process (AHP) zaliczana do amerykańskiej szkoły wielokryterialnego podejmowania decyzji (ang. *multiple-criteria decision-making* – MCDM). Podobną metodą jest analiza morfologiczna opracowana przez F. Zwicky'ego – uznawana za jedną z ważniejszych metod stymulujących twórcze myślenie. W metodzie tej tworzy się rozwiązania oparte na łączeniu wielu parametrów charakteryzujących dany problem. Prowadzi to często do odkrycia nietypowych zestawień stymulujących twórcze myślenie badacza. Metodę tę często wykorzystuje się w różnych konfiguracjach, do tworzenia nowych produktów zarówno w sferze materialnej, jak i intelektualnej. Poczucie bezpieczeństwa jest zawsze wieloaspektowe, dlatego też jego pomiar powinien być wielokryterialny. Problemem pozostaje jednak ocena poziomu bezpieczeństwa, którą należy sprowadzić do jednego metakryterium. Bo tylko wówczas możemy porównywać ze sobą różne rozwiązania tego samego problemu pod kątem ryzyka.

W badaniach zastosowano podejście teoretyczne, skupiając się przede wszystkim na sformułowaniu definicji bezpieczeństwa przydatnej w kontekście analizy wielokryterialnej oraz przedstawiono wybrane rozwiązania stosowane w ocenie poziomu bezpieczeństwa. Analiza wielokryterialna poziomu bezpieczeństwa może również służyć odkrywaniu prawdziwych przyczyn zagrożeń. Często prosta, jednokryterialna analiza prowadzi do niewłaściwych wniosków zarówno co do poziomu bezpieczeństwa, jak i przyczyn jego zagrożeń.

Słowa kluczowe: bezpieczeństwo, analiza wielokryterialna, analiza ryzyka

Multicriterial Analysis in Safety Research

Abstract

The aim of the article is to present the methodology for assessing the level of security using multicriterial analysis. Multicriterial analysis is mostly associated with the decision-making issues which should optimize more than one objective function. Unequivocal solution of such problems is impossible because optimal decision for one of the objectives is not optimal for the remaining at the same time. An Italian economist and sociologist, Vilfredo Pareto, already proved it by introducing the concept of a set of non-dominated decisions. It is a set of decisions, each of which is better than the others in terms of one of the selection criteria. There are a lot of methods of solving such problems. They boil down to the way of connecting all the selection criteria in one metacriterion. This connection can be carried out in a mathematical or heuristic way. The second method is the Analytic Hierarchy Process (AHP), which is included in the American school of Multi-Criteria decision making (MCDM). The similar method is a morphological analysis developed by Fritz Zwicky, which was considered as one of the most important methods stimulating creative thinking. This method is used to create solutions based on a combination of many parameters characterizing the problem. This often leads to the discovery of the unusual combinations that stimulate creative thinking of the researcher. This method is often used in a variety of configurations to create the new products, both in the material and intellectual sphere. Sense of security is always multifaceted; therefore, its measurement should be multicriterial. Because only then we can compare different solutions to the same problem, in terms of risk. Theoretical framework was used in the research focus primarily on the wording of the definition of security useful in the multicriterial analysis and several solutions applied in assessing the level of security are presented. Multicriterial analysis of

the safety level may also be used for discovering the real causes of threats. Simple, single-criterion analysis leads to incorrect conclusions, both in relation to the level of safety and the causes of threats.

Keywords: safety, multicriterial analysis, risk analysis

1. Wielowymiarowość bezpieczeństwa

W języku polskim bezpieczeństwo oznacza stan niezagrożenia, spokoju, pewności [1, s.147]. Dokonując szczegółowej analizy tego pojęcia [2, s. 53–56], należy stwierdzić, iż jest ono subiektywnym odczuwaniem spokoju, pewności, braku zagrożeń; wynikającym z indywidualnej oceny zjawisk, aktualnie postrzeganych i antycypowanych przez konkretną osobę. Można zatem postawić hipotezę, że człowiek bezpieczny nie odczuwa strachu, lęku czy obaw o dalsze swoje istnienie i możliwość osiągania osobistych celów.

Realizując własne aspiracje, każdy człowiek pragnie mieć pewność ich zaspokojenia. Pewność taką daje otoczenie, a właściwie sposób jego postrzegania przez konkretnego człowieka. Tworzą je zarówno inni ludzie, jak i elementy przyrody ożywionej, nieożywionej oraz wytwory cywilizacji. Dążąc do zaspokojenia własnych aspiracji, każdy człowiek stara się kształtować, według własnych wyobrażeń i możliwości, zasady i normy postępowania społecznego, sposób rozdziału dóbr materialnych i dostępu do dóbr wspólnych, otaczającą go przyrodę. Wypadkowa działań wielu ludzi tworzy i nadaje kierunek zmianom w środowisku społecznym i przyrodniczym. Efektem tego jest poczucie bezpieczeństwa, jego braku lub jakiegoś stanu pośredniego odczuwanego przez ludzi tworzących daną społeczność. Każda z osób będzie miała inny stopień poczucia bezpieczeństwa, ze względu na inną istotę własnego istnienia, określoną przez siebie samego.

Istotą bezpieczeństwa jest jego zależność od czynników zewnętrznych. Zarówno zaspokajanie potrzeb podstawowych, jak i kreowanie własnej istoty jest zależne od otoczenia konkretnego człowieka. Nie tylko od otoczenia społecznego, ale również przyrodniczego i materialnego[1]. Natomiast sposób

1 Wyodrębnienie otoczenia materialnego związane jest z potrzebą uwypuklenia dóbr materialnych będących w dyspozycji konkretnego człowieka lub jemu dostępnych.

postrzegania środowiska zewnętrznego zależy od wartości wewnętrznych konkretnego człowieka. Stąd też poczucie bezpieczeństwa każdego człowieka kształtują wartości wewnętrzne, doświadczenia osobiste i sposób postrzegania świata, jak również byty zewnętrzne i ich istota (jego o nich wiedza) oraz wzajemna konfiguracja (istota układu bytów).

Bezpieczeństwo można zatem zdefiniować jako przekonanie (pewność) podmiotu o zdolności do zachowania tego, co dla niego cenne, wartościowe w otoczeniu podmiotu oraz atrybutów i istotnych akcydensów samego podmiotu, niezbędnych w procesie zaspokajania podstawowych potrzeb oraz kształtowania, według własnej woli, sposobu istnienia.

W nieco uproszczonej wersji, definicję bezpieczeństwa można sformułować w następującej postaci: bezpieczeństwo to przekonanie podmiotu, że może on nadal istnieć i swobodnie kształtować własną egzystencję. Określenie to, pomimo że niemal w intuicyjny sposób oddaje istotę bezpieczeństwa, nie wskazuje metody jego osiągania ani tego, od czego ono zależy, poza subiektywnymi odczuciami. Z tego powodu trudno, opierając się na nim, określić procedurę pomiaru bezpieczeństwa. Znacznie lepszą pod tym względem, choć jednocześnie bardziej skomplikowaną, jest rozbudowana definicja zaproponowana w poprzednim akapicie. Wskazuje ona jednoznacznie, że poczucie bezpieczeństwa jest efektem postrzegania przez podmiot rzeczywistości, a w niej samego siebie w kontekście dalszego istnienia i rozwoju.

Układ wartości wewnętrznych i zewnętrznych, cennych dla podmiotu ze względu na jego poczucie bezpieczeństwa, można nazwać konfiguracją bezpieczeństwa [2, s. 69]. Jest ona w sposób ciągły kreowana przez podmiot w miarę zmian zachodzących w nim samym i w jego otoczeniu. Dlatego też bezpieczeństwo może być postrzegane jako proces ciągłej kreacji konfiguracji bezpieczeństwa, którą tworzy splot:

- cenionych wartości wewnętrznych;
- kluczowych aspiracji;
- elementów otoczenia i relacji między nimi.

Holistyczna ocena tych trzech aspektów, tworząca personalne poczucie bezpieczeństwa, zależy od wiedzy, osobowości i światopoglądu konkretnego człowieka.

Z powyższych powodów poczucie bezpieczeństwa jest zawsze subiektywne, a stan bezpieczeństwa organizacji jest efektem działań interesariuszy kreujących osobiste poczucie bezpieczeństwa.

Powszechnie postrzeganym przeciwieństwem bezpieczeństwa jest zagrożenie. Wywołuje ono, podobnie jak bezpieczeństwo, pewien stan emocjonalny. O ile jednak poczucie bezpieczeństwa implikuje uczucie pewności, o tyle zagrożenie wywołuje obawy, lęk strach, wzbudza emocjonalną chęć działania. Jest bardzo silnym motywatorem przywracania poczucia bezpieczeństwa. Bezpieczeństwo i zagrożenie opisują to samo zjawisko, ale na przeciwnych biegunach. Podobnie jak centralizacja i decentralizacja wskazują na sposób rozłożenia uprawnień decyzyjnych wewnątrz organizacji, tak bezpieczeństwo i zagrożenie opisują sposób postrzegania przez podmiot poznający wpływu zjawisk na jego dalsze istnienie i możliwość swobodnego kształtowania jego treści – zaspokajania potrzeb i aspiracji.

Istotnymi cechami zagrożenia są:

- subiektywność oceny;
- możliwość utraty wartości uznanych przez podmiot za cenne;
- stan dyskomfortu emocjonalnego – w związku z zaistniałą lub potencjalną sytuacją.

Należy jednak podkreślić, że zagrożenie to możliwość potencjalnej straty, nie zaś aktualnej. Choć często te elementy są ze sobą utożsamiane. Zaistniałe skutki powodzi nie są zagrożeniem, ale ich przyszłe konsekwencje mogą nim być. Trwałe kalectwo nie jest zagrożeniem, jest stanem faktycznym. Natomiast jego skutki mogą być i najczęściej są postrzegane jako zagrożenie dla egzystencji rozumianej w kategoriach egzystencjalizmu. Konsekwencją kalectwa jest utrata pracy, wykluczenie społeczne, wysokie koszty rehabilitacji, potrzeba opieki osób trzecich. To wszystko wzbudza obawy nie tylko o możliwość dalszego istnienia, ale przede wszystkim zaspokajania własnych aspiracji.

Można zatem skonstatować, że zagrożeniem są wszystkie te zjawiska, które w ocenie podmiotu mogą pozbawić go istnienia, aktualnej treści istnienia lub stanowią barierę dla jego rozwoju. Zjawiska te mogą oddziaływać na podmiot bezpośrednio lub pośrednio poprzez zmianę (lub unicestwienie) bytów konkretnych z otoczenia podmiotu, ich układu i wzajemnych relacji, uznawanych przez podmiot za istotne dla jego istnienia i swobody kształtowania jego treści.

Stąd też istnieje pewna gradacja zagrożeń:

- możliwość naruszenia konfiguracji bezpieczeństwa – tego typu zagrożenia występują zawsze, jednakże różnią się prawdopodobieństwem zaistnienia zmian;
- naruszenie konfiguracji bezpieczeństwa – są to zdarzenia znacznie rzadsze, jednakże ze względu na fakt, iż konfiguracja bezpieczeństwa jest

splotem ocen: wartości, aspiracji i otoczenia, jej naruszenie może prowadzić do kolejnych zmian niszczących personalne poczucie bezpieczeństwa;
- konfiguracja bezpieczeństwa zniszczona w stopniu znacznym, uniemożliwiającym proste jej odtworzenie.

Przejście pomiędzy wskazanymi poziomami zagrożeń jest płynne i w znacznym stopniu zależne od aktualnego stanu psychofizycznego osoby oceniającej poziom bezpieczeństwa. Dlatego też indywidualne oceny siły zagrożenia są dość pobieżne i silnie zabarwione emocjonalnie. Bardzo często konkretni ludzie nie są do końca świadomi kształtu własnej konfiguracji bezpieczeństwa. Zmiany, jakie w niej zaszły, dostrzegane są przez nich dopiero po pewnym czasie, niezbędnym do refleksji uświadamiającej wpływ poszczególnych jej elementów i relacji na zdolność do istnienia oraz kreowania własnej egzystencji.

Podchodząc jednak do problemu oceny siły zagrożeń pragmatycznie, należy stwierdzić, że jest ona zależna od:
- wielkości zmian w personalnej konfiguracji bezpieczeństwa oraz ich wpływu na zdolność do dalszego istnienia i swobody kreowania jego treści;
- prawdopodobieństwa, z jakim owe zmiany mogą zaistnieć.

Te dwa parametry, uzupełnione definicją personalnej konfiguracji bezpieczeństwa, określają siłę zagrożeń. Stąd też metodyka jej pomiaru obejmuje następujące etapy:
- identyfikację atrybutów, ważnych akcydensów, bytów z otoczenia lub ich relacji, które w efekcie zdarzenia mogą utracić dotychczasową wartość – zdefiniowanie personalnej konfiguracji bezpieczeństwa;
- oszacowanie, w jakim stopniu ich aktualna wartość może ulec pomniejszeniu i jaki to będzie miało wpływ na dalszą egzystencję;
- oszacowanie prawdopodobieństwa, z jakim może to nastąpić.

Ujmując rzecz bardziej lapidarnie, należy ocenić co cennego dla poczucia bezpieczeństwa może zostać utracone, jaka będzie wielkość tej straty oraz jakie jest tego prawdopodobieństwo. A przede wszystkim, jaki to będzie miało wpływ na dalszą egzystencję podmiotu.

2. Metodyka szacowania siły zagrożeń

Każdy ze wskazanych powyżej trzech etapów pomiaru siły zagrożenia kończy się pewną oceną. Etapy splecione w jedną całość wywołują określony poziom

negatywnych emocji, który może być utożsamiany z personalną miarą siły zagrożenia. Stąd też jej szacowanie należy rozpocząć od identyfikacji konfiguracji bezpieczeństwa, którą tworzy układ wewnętrznych i zewnętrznych wartości oraz relacji między nimi. Indywidualna konfiguracja bezpieczeństwa jest pochodną osobowości, światopoglądu i aspiracji, ukształtowanych przez wychowanie, zdobytą wiedzę i doświadczenie życiowe. Zależność ta sugeruje, że konfiguracje bezpieczeństwa ludzi, wywodzących się z określonej wspólnoty społecznej, są w pewnej części wspólne ze względu na kultywowane tradycje, sposób myślenia, preferowane normy zachowań społecznych, czyli wszystko to, co tworzy mentalność danej społeczności. Wspólność pewnej części konfiguracji bezpieczeństwa ludzi należących do określonych społeczności, nie niweluje problemu jej indywidualizmu.

Zdefiniowane wartości wewnętrzne i zewnętrzne mają różny wpływ na poczucie bezpieczeństwa. Dlatego też proces definiowania personalnej konfiguracji bezpieczeństwa można sprowadzić do czterech etapów:

- określenia elementów wewnętrznych – cennych atrybutów i akcydensów podmiotu;
- określenia elementów zewnętrznych tworzących otoczenie;
- określenia relacji między podmiotem i otoczeniem oraz poszczególnymi elementami wewnętrznymi i zewnętrznymi;
- określenia rangi (wagi, znaczenia) poszczególnych elementów i relacji w konfiguracji bezpieczeństwa.

Zdefiniowanie personalnej konfiguracji bezpieczeństwa stanowi wstępny etap oceny siły zagrożeń. Kolejnym jest identyfikacja zjawisk, których skutki mogą mieć negatywny wpływ na konfigurację bezpieczeństwa lub poszczególne jego elementy. Rozpoznanie zagrożeń umożliwia prognozowanie ewolucji zjawisk, które je powodują, ze szczególnym uwzględnieniem potencjalnych skutków i prawdopodobieństwa ich wystąpienia.

Reasumując, metodyka szacowania siły zagrożenia sprowadza się do:

- określenia konfiguracji bezpieczeństwa:
  – elementów wewnętrznych – cennych atrybutów i akcydensów podmiotu,
  – elementów zewnętrznych – bytów z jego otoczenia,
  – relacji między podmiotem i otoczeniem oraz poszczególnymi elementami wewnętrznymi i zewnętrznymi,
  – rangi (wagi, znaczenia) poszczególnych elementów i relacji w konfiguracji bezpieczeństwa;

- identyfikacji zdarzeń, które mogą mieć negatywny wpływ na konfigurację bezpieczeństwa;
- oceny wpływu przewidywanych zdarzeń na konfigurację bezpieczeństwa (poszczególne jej elementy, relacje);
- oszacowania prawdopodobieństwa ich zaistnienia.

Kluczowym i najtrudniejszym elementem tej metodyki jest trafne zdefiniowanie personalnej konfiguracji bezpieczeństwa. Bardzo rozbudowana konfiguracja powoduje, że niemal wszystkie zjawiska i zdarzenia wywoływać będą lęk i obawy o przyszłość. Z kolei zbyt uboga konfiguracja prowadzi do nadmiernego poczucia bezpieczeństwa, nieadekwatnego do rzeczywistych warunków. Ludzie często nie wiedzą, od czego naprawdę zależy ich dalsze istnienie i zdolność do kreowania jego treści. Dlatego też w ich życiu znacznie częściej pojawiają się kryzysy psychiczne, których pierwszym etapem jest konfrontacja z wydarzeniem wywołującym kryzys. W etapie tym uświadamiają sobie, że nagle z ich życia zniknęło coś, co nadawało mu sens, chociaż być może, nie byli tego wcześniej świadomi. Wymusza to konieczność zbudowania nowej konfiguracji bezpieczeństwa opartej na innych wartościach.

W wymiarze personalnym każdy samodzielnie definiuje konfigurację bezpieczeństwa i adekwatnie do niej postrzega zagrożenia i ocenia ich siłę. Natomiast w wymiarze społecznym siłę zagrożenia można szacować w dwóch aspektach:

- bezpieczeństwa członków organizacji jako zbiorowości społecznej;
- bezpieczeństwa samej organizacji.

Każdy z nich wskazuje inną drogę oceny siły zagrożeń i służy innym celom. Oba jednak związane są z procesem kierowania organizacjami. W pierwszym przypadku kierownictwo nastawione jest na zapewnienie bezpieczeństwa członków organizacji nawet kosztem jej samej, w drugim zaś odwrotnie – najważniejsza jest organizacja i cele, ku którym zmierza. Aspekty te są wyraźnie widoczne w kulturze organizacji.

Kolejna faza szacowania siły zagrożeń związana jest z identyfikacją zagrożeń oraz predykcją ich wpływu na konfigurację bezpieczeństwa. Zagrożenie to jedynie potencjalna możliwość zaistnienia niekorzystnych dla podmiotu sytuacji lub zdarzeń. Dlatego też ich ocena w dużym stopniu zależy od umiejętności wiarygodnego prognozowania. [3, s. 56–57].

Podstawą oceny i interpretacji zdarzeń, a tym bardziej przewidywania ich skutków są docierające do podmiotu informacje oraz zgromadzone i uporządkowane fakty z przeszłości, częściowo już zinterpretowane przez podmiot

poznający i stanowiące jego zasób wiedzy. Rzetelność oceny wynika z wiarygodności zgromadzonych faktów.

Poczynione uwagi wskazują na dwa zasadnicze problemy związane z wiarygodną oceną siły zagrożeń:

- pierwszy dotyczy definiowania konfiguracji bezpieczeństwa zarówno w wymiarze indywidualnym, jak również społecznym i organizacyjnym. Jej kształt, w wymiarze indywidualnym, zależy od osobowości, światopoglądu i aspiracji konkretnego człowieka. Natomiast w wymiarze społecznym i organizacyjnym od kontekstu definiowania oraz osobowości, światopoglądu i aspiracji osób definiujących;
- drugi dotyczy możliwości trafnego prognozowania prawdopodobieństwa zaistnienia i skutków zjawisk uznanych za zagrożenia.

Dotychczasowe rozważania upoważniają do stwierdzenia, że ocena poziomu bezpieczeństwa (indywidualnego i grupowego) oraz siły zagrożeń jest oceną wielokryterialną. Ze względu przede wszystkim na konfigurację bezpieczeństwa uwzględniającą wiele elementów otoczenia oraz atrybutów i ważnych akcydensów podmiotu mających wpływ na komfort życia, każde zagrożenie powinno zostać ocenione pod kątem wpływu na poszczególne elementy konfiguracji bezpieczeństw. Otrzymamy wówczas wiele ocen, które należy właściwie zagregować i przedstawić w zrozumiały sposób. Agregacja musi uwzględniać wzajemne korelacje poszczególnych elementów konfiguracji bezpieczeństwa i ich wpływu na poczucie bezpieczeństwa.

3. Podstawy wybranych metod wielokryterialnych

Do oceny tak złożonych problemów jak ocena poziomu bezpieczeństwa czy siły zagrożeń można wykorzystywać metody wielokryterialnej analizy decyzyjnej. Do najważniejszych z nich możemy zaliczyć:

- programowanie wielokryterialne;
- Analytic hierarchy proces (AHP) [10, s. 1–29];
- psychologiczne reguły wyboru [4, s. 148];
- analizę morfologiczną [11];
- Quality Function Deployment (QFD) [19, s. 122, 137–142].

Oczywiście żadna z tych metod nie może być wykorzystana wprost, należy je nieco zmodyfikować. Jednakże najważniejszym ich elementem w ocenie poziomu bezpieczeństwa jest sposób podejścia do agregacji wyników.

Jak stwierdzono w poprzednich częściach artykułu, ocena poziomu bezpieczeństwa sprowadza się do:

- zidentyfikowania elementów konfiguracji bezpieczeństwa;
- identyfikacji zjawisk mających negatywny wpływ na poszczególne elementy konfiguracji;
- oceny prawdopodobieństwa ich wystąpienia;
- skutków, jakie mogą przynieść dla danego elementu konfiguracji.

Załóżmy, że zidentyfikowano elementy konfiguracji bezpieczeństwa oraz zjawiska, które mogą mieć na nie negatywny wpływ. Określono również prawdopodobieństwo jego wystąpienia i skutki, jakie wywołuje w poszczególnych elementach konfiguracji. Problemem pozostaje ocena poziomu bezpieczeństwa, czyli odpowiedź na pytanie: Jak bardzo dane zjawisko wpłynie na nasze poczucie bezpieczeństwa? Odpowiedź jest bardzo istotna w sytuacji identyfikacji wielu zjawisk i odpowiedzi na pytanie: Które z nich jest dla nas najgroźniejsze? Wybór nie jest prosty. Zwłaszcza, jeżeli nałożymy na to nasze możliwości ochrony przed skutkami tych zjawisk oraz możliwości odbudowy lub zastąpienia utraconych wartości.

Klasyfikując wpływ poszczególnych zagrożeń na nasze poczucie bezpieczeństwa, możemy posłużyć się jedną z siedmiu reguł wyboru, wymienianych przez psychologów [4, s. 148]:

- dominacji – za najważniejsze zagrożenie uważamy to, które ma największy wpływ na istotne element konfiguracji bezpieczeństwa;
- koniunkcji – za najważniejsze uważamy zagrożenie, którego wpływ na wszystkie elementy konfiguracji bezpieczeństwa przekracza pewien próg krytyczny;
- dysjunkcji – za najważniejsze uznajemy to zagrożenie, które przynajmniej dla jednego elementu konfiguracji przekracza założony próg krytyczny – odmienny od wymienionego w poprzednim punkcie;
- leksykografii – za najważniejsze zagrożenie uważamy to, którego wpływ na poszczególne elementy konfiguracji bezpieczeństwa jest największy, wynikający z gradacji jego wpływu, procedura jest wieloetapowa;
- eliminacji – z katalogu zagrożeń wyłączamy te, których skutki na poszczególne elementy konfiguracji bezpieczeństwa nie przekroczyły progu krytycznego, procedura jest wieloetapowa;
- maksymalizacji – za najważniejsze zagrożenie uważamy to, którego sumaryczny wpływ na poszczególne elementy konfiguracji bezpieczeństwa jest największy;

- sumowania strat – za najważniejsze zagrożenie uważamy to, którego zagregowany wpływ na poszczególne elementy konfiguracji bezpieczeństwa jest największy.

Przy klasyfikacji zagrożeń i ocenie poziomu zagrożenia często spotykamy się z problemem, iż poszczególne zagrożenia wywołują największe skutki jedynie dla jednego elementu konfiguracji bezpieczeństwa. Cechę tę po raz pierwszy wyróżnił V. Pareto. Stąd w teorii decyzji zbiór decyzji, które są od innych lepsze pod względem jednej cechy określa się mianem decyzji optymalnych w sensie Pareto lub decyzji niezdominowanych [21, s. 46]. Podobnie możemy podejść do problemu oceny siły zagrożeń. Otrzymamy wówczas zbiór zagrożeń, które dla jednego elementu konfiguracji niosą najbardziej negatywne skutki, dla pozostałych zaś nieco mniejsze od pozostałych zagrożeń. Do określenia, które zagrożenia możemy nazwać „niezdominowanymi" można wykorzystać graf Hassego [22, s. 154].

Ustalenia hierarchii zagrożeń „niezdominowanych" można dokonać podobnie jak w programowaniu wielokryterialnym – poprzez sprowadzenie wszystkich elementów konfiguracji bezpieczeństwa do jednego metakryterium, poprzez:

- wybór najważniejszego elementu konfiguracji bezpieczeństwa;
- utworzenia metakryterium:
  - ważona suma kryteriów,
  - ważona suma stopnia spełnienia kryteriów [12, s. 328–346].

Wskazane powyżej metody analizy wielokryterialnej sprowadzają ocenę zagrożeń do pojedynczej liczby, według której możemy je porządkować. Bardziej rozbudowanymi metodami są metody macierzowe: Analytic hierarchy proces (AHP) [10], analiza morfologiczna [11], Quality Function Deployment (QFD) [19, s. 122, 137–142].

Wyszczególnione metody opierają się na ustaleniu korelacji między wpływem poszczególnych zagrożeń na elementy konfiguracji bezpieczeństwa i badania ich w układzie macierzowym. Wydaje się, że te metody są rzetelniejsze w ocenie poziomu bezpieczeństwa, jednakże ze względu na subiektywność tworzenia owych macierzy spotykają się z dużą krytyką.

Nieco innymi metodami wielokryterialnej oceny poziomu bezpieczeństwa są rating kredytowy, analiza SWOT, metody scenariuszowe [5, 7].

Rating można zdefiniować jako proces oceny lub jego wynik, w zakresie wiarygodności pożyczkobiorców, emitentów lub konkretnych papierów

wartościowych, najczęściej obligacji lub też wiarygodności firmy ubezpieczeniowych, banku lub innej instytucji finansowej. Oceny takiej dokonują niezależne agencje ratingowe. Ich ocena bardzo często brana jest pod uwagę przez inwestorów. Ocena ratingowa to nic innego, jak ustalenie w określonej skali ryzyka związanego z niewypłacalnością pożyczkobiorcy, wiarygodnością instytucji finansowej w realizacji swoich zobowiązań itp. W ocenie tej uwzględnia się nie tylko wartości wewnętrzne samej instytucji, ale również wpływ otoczenia na jej funkcjonowanie.

Na przykład w ocenie stanu gospodarki państwa bierze się pod uwagę takie obszary, jak:

- system polityczny, w tym formę sprawowania władzy, procedurę zmiany rządu, stabilność systemu politycznego;
- sytuację społeczną, w tym podział dochodów, dane demograficzne, standard życia ludności, warunki pracy, poziom bezrobocia, rolę związków zawodowych, różnice etniczne i religijne;
- relacje wewnątrz kraju: transfer funduszy, podatków, odpowiedzialność decyzyjną;
- stosunki polityczne i gospodarcze kraju z zagranicą;
- zadłużenie zagraniczne państwa pomniejszone o rezerwy dewizowe;
- elastyczność bilansu płatniczego;
- strukturę gospodarki: poziom rozwoju gospodarczego, wielkość produkcji, stopień zróżnicowania produkcji, dynamikę wzrostu gospodarczego, dostępność zasobów naturalnych i infrastrukturę;
- system kierowania gospodarką narodową obejmujący efektywność polityki podatkowej, monetarnej i przemian strukturalnych;
- system administracyjny, w tym ograniczenia prawne, system zarządzania i kontroli, system podatkowy.

Wyszczególnione obszary należy traktować jedynie jako przykłady, gdyż każda z agencji ratingowych dokonuje procesu oceny według własnych procedur. Efektem tej oceny jest nadanie odpowiednich stopni wiarygodności, według przyjętej skali wraz z krótkim uzasadnieniem.

Przykład procesu ratingowego uświadamia, że skonstruowanie kompleksowej procedury oszacowania bezpieczeństwa jest bardzo trudne, jednakże wskazuje, że bardzo duże znaczenie posiada jakość wewnętrzna podmiotu bezpieczeństwa i relacje otoczeniem. Ale jej efekt bywa trudny do interpretacji. Dlatego też znacznie częściej dokonuje się oceny wpływu poszczególnych

zagrożeń, traktując te procedury jako ocenę ryzyka związanego z określonym obszarem aktywności lub konkretnym zagrożeniem. Niezależnie od niej, dokonuje się oceny szans rozwojowych. Dopiero złożenie tych dwóch elementów wpływa na indywidualną ocenę bezpieczeństwa w określonej sferze aktywności.

Swoistymi procedurami kompleksowej oceny bezpieczeństwa są analiza SWOT i metody scenariuszowe [2, s. 163–166]. Zadaniem pierwszej jest identyfikacja szans i zagrożeń oraz wewnętrznych wartości wspierających lub obniżających zdolność kształtowania istoty organizacji. Analiza taka bywa niekiedy pogłębiona o ocenę siły wpływu tych czynników na realizację zamierzonych zmian w sposobie funkcjonowania danej organizacji [5, s. 35–38]. Metody scenariuszowe zaś służą kompleksowej identyfikacji przyszłych stanów zewnętrznych i wewnętrznych organizacji oraz ich wpływu na jego istnienie, a przede wszystkim na zdolność kształtowania istoty. W metodach tych uwzględnia się zarówno pozytywny, jak i negatywny wpływ poszczególnych czynników pogrupowanych w określone sfery otoczenia[2].

4. Wybrane przykłady wielokryterialnej oceny zagrożenia

Siła zagrożenia płynie z oceny jego wpływu na konfigurację bezpieczeństwa, która jest splotem wewnętrznych i zewnętrznych wartości oraz ich wzajemnych relacji. Dlatego też konkretne zagrożenie może przynieść straty w wielu obszarach konfiguracji bezpieczeństwa. Jeżeli natomiast ocenę siły zagrożenia sprowadzi się do jednego wymiaru, np. liczby ofiar śmiertelnych lub wielkości strat materialnych, to stanie się ona równoważna ryzyku w procesach decyzyjnych. Chociaż w języku naturalnym ryzyko jest miarą zagrożenia, to jednak szczegółowa analiza prowadzi do wniosku, iż występuje między tymi pojęciami istotna różnica. Zagrożenie dotyczy szerokiego spektrum „strat", obejmującego różne aspekty poczucia bezpieczeństwa[3], natomiast ryzyko odnosi się do konkretnego wymiaru, np. utraty życia, zachorowania na konkretną chorobę, wielkości strat zainwestowanych pieniędzy itd. Ryzyko jest

2 Szczegółowe opisy metod scenariuszowych można znaleźć na przykład w: [5] i [7].

3 Straty mogą dotyczyć: atrybutów, akcydensów, bytów konkretnych lub ich konfiguracji w ujęciu jednostkowym jak i pewnej ich konfiguracji. To samo zagrożenie może powodować skutki we wszystkich obszarach poczucia bezpieczeństwa.

precyzyjnie oszacowane w przeciwieństwie do zagrożenia, które może być wiązane także z niepewnością.

Angielski ekonomista F. Knight twierdził, że w praktyce gospodarczej dominują zdarzenia niepowtarzalne[4], do których nie można zastosować żadnej miary prawdopodobieństwa, czyli tzw. zdarzenia niepewne. Zdarzenia, których potencjalne istnienie można zmierzyć za pomocą prawdopodobieństwa matematycznego, statystycznego lub szacunkowego, Knight określił mianem ryzyka [13, s. 79]. Można zatem powiedzieć, że ryzyko do dobrze skalkulowana niepewność.

Natomiast R. Gallati zdefiniował ryzyko w węższym zakresie jako okoliczności, w których istnieje ekspozycja na przeciwności losu. W szerszym zakresie określił je jako warunki, w których istnieje możliwość odchyleń od pożądanego oczekiwanego wyniku [14, s. 7–8]. W ujęciu węższym ryzyko traktowane jest jako możliwość poniesienia szkody lub straty. W szerszym zaś jako możliwość zarówno pozytywnego, jak i negatywnego odchylenia od oczekiwań [15, s. 99]. Stąd też ryzyko można podzielić na:

- ryzyko czyste (ang. *pure risk*), które występuje wówczas, gdy w stosunku do obecnego stanu alternatywą jest wystąpienie straty;
- ryzyko spekulacyjne (ang. *speculative risk*), które występuje, gdy nieznane przyszłe zdarzenia mogą spowodować zarówno straty, jak i zyski [16, s. 19].

Potocznie ryzyko rozumiane jest najczęściej jako czyste, co kładzie nacisk na możliwość pogorszenia się sytuacji. Stąd też utożsamiane bywa z zagrożeniem, co nie jest właściwe, ze względu na leksykalne znaczenie obu pojęć. Zagrożenie jest wielowymiarowe i dotyczy również niepewności, natomiast ryzyko jest jednowymiarowe, wskazuje wielkość potencjalnych strat w zakresie tylko jednej wartości.

Część autorów twierdzi, że nie można jednoznacznie zdefiniować ryzyka inaczej jak poprzez zbiór opisujących je cech [17, s. 14–15]:

- źródło i przedmiot ryzyka, czyli powód, który czyni rozważania nad ryzykiem uzasadnionym oraz sytuację (zjawisko) równoznaczną z przedmiotem analizy ryzyka;
- możliwe następstwa ryzyka, czyli potencjalny charakter skutków podjętych decyzji oraz miary tych skutków w ujęciu podmiotowym i przedmiotowym;

4 Jest to oczywisty wniosek płynący z II zasady termodynamiki – w rzeczywistym świecie wszystkie procesy są nieodwracalne i pozostawiają trwały ślad.

- podjęcie ryzyka, czyli decyzja podjęcia aktywnych działań związanych z realizacją zadań potrzebnych do uzyskania korzyści i minimalizacji strat;
- realizacja ryzyka, czyli wystąpienie przewidywanych lub nieprzewidywanych skutków zdarzeń, których źródłem jest przedmiot ryzyka;
- możliwość manipulacji ryzykiem, czyli podatność przedmiotu ryzyka na stosowanie środków i metod ukierunkowujących zachodzące procesy w pożądanym kierunku.

Pojęcie ryzyka stosowane jest w sytuacjach, gdy rezultat zdarzenia nie jest znany, ale możliwe jest zidentyfikowanie przyszłych sytuacji oraz gdy znane lub możliwe do oszacowania jest prawdopodobieństwo zrealizowania się poszczególnych możliwości w przyszłości [18, s. 56–57]. Można zatem stwierdzić, że niepewność ma wymiar informacyjny, a jej przyczyną jest bariera dostępu do informacji lub niewiarygodność uzyskanych informacji. Ryzyko natomiast ma wymiar ilościowy, ponieważ można dokonać jego pomiaru. Zagrożenie zaś jest czymś pośrednim między niepewnością a ryzykiem. Określa się nim potencjalne skutki zdarzeń zarówno te określone (ryzyko), jak i nieokreślone (niepewność) lub jedynie częściowo określone.

Coraz częściej do szacowania skutków poważnych zagrożeń, ze względu na ich wielowymiarowość, stosuje się wielowskaźnikową analizę ryzyka. Dla każdej istotnej, ze względu na poczucie bezpieczeństwa wartości, szacuje się niezależny wskaźnik opisujący wielkość strat w zakresie tej wartości. Jeżeli jeden ze wskaźników jest silnie dominujący nad pozostałymi, to w dalszej analizie uwzględnia się tylko ten wskaźnik. Jeżeli natomiast nie ma wskaźnika dominującego, to określa się zagregowany, według określonego algorytmu, wskaźnik syntetyczny.

W Szwajcarii zaproponowano dziewięciowskaźnikową metodykę szacowania ryzyka (tabela 1).

Tabela 1. Opis wskaźników szkód stosowanych w Szwajcarii

Wskaźnik	Opis
Ludzie i istoty żywe	
N1 = liczba zgonów i przypadki ciężkiego inwalidztwa	Zgony natychmiastowe i odległe
N2 = liczba rannych	Ciężko i lekko ranni, a także liczba osób z długoczasowym negatywnym skutkiem dla zdrowia

cd. Tabeli 1.

Wskaźnik	Opis
Ludzie i istoty żywe	
N3 = liczba ewakuowanych	Liczba osób ewakuowanych na okres powyżej jednego roku
N4 = współczynnik alarmu	Iloczyn czasu trwania alarmu lub stan niepokoju i liczby osób, których to dotyczy
N5 = liczba zabitych zwierząt domowych	Liczba padłych dużych zwierząt domowych i dziko żyjących, takich jak: konie, krowy, owce, jelenie, kozice, itd. Liczba małych zwierząt, takich jak: kury, koty, zające lub lisy uwzględniona jest ze współczynnikiem 0,01. Ryby są uwzględnione przez współczynnik N6.
Podstawy życia	
N6 = powierzchnia zdegradowanego ekosystemu	Powierzchnia ekosystemu, którego naturalna równowaga została naruszona. W przypadku skażenia wód należy uwzględnić zarówno obszar, jak również tereny łowieckie. W przypadku skażeń wód, powinna być włączona strefa nadbrzeżna, jak również tereny łowieckie w przypadku zdziesiątkowania zwierząt drapieżnych. Powierzchnia obszarów skażonych ważnych ekosystemów chronionych prawem powinna być uwzględniona z mnożnikiem 10.
N7 = powierzchnia skażonej gleby	Powierzchnia obszaru, który stał się nieurodzajny, nie nadający się do zamieszkania, nieużyteczny lub wymagający zastosowania specjalnych środków rekultywacji.
N8 = powierzchnia obszarów skażonej wody gruntowej	Suma powierzchni stref ochronnych wód gruntowych typów A i S, które zostały skażone w taki sposób i w takim rozmiarze, że zagraża to przeniknięciem skażeń do wód gruntowych.
Dobra materialne	
N9 = straty dyskontowe	Wszystkie szkody bezpośrednie i pośrednie takie jak np. straty w zmniejszeniu zamieszkania, uszkodzenia dóbr materialnych, koszty leczenia, ewakuacji, procesów sądowych, itp.

Źródło: [6, s. 19–20]

Pierwsze pięć wskaźników (N1–N5) dotyczy ludzi i istot żywych, trzy wskaźniki dotyczą podstaw życia, natomiast ostatni wskaźnik (N9) związany jest z dobrami materialnymi. Za pomocą tych dziewięciu wskaźników można uzyskać dostatecznie pełny opis potencjalnych szkód. Ich wartość przelicza się według określonych algorytmów, tak, aby mieściła się w przedziale od 0 do 1. Następnie dokonuje się ich agregacji w jeden syntetyczny wskaźnik. Jeżeli jego wartość jest mniejsza niż 0,3, to przyjmuje się, że wielkość strat odpowiada awarii. Przy wskaźniku należącym do przedziału od 0,3 do 0,5 mówi się o możliwości poważnej awarii. Natomiast wskaźnik powyżej 0,5 sugeruje, że może zdarzyć się katastrofa [8, s. 19–23].

Zastosowanie wielowskaźnikowej oceny ryzyka pozwala na kompleksową ocenę siły konkretnego zagrożenia. Rzetelność oszacowania związana jest z doborem wskaźników oraz algorytmem syntezy tych wskaźników w jeden – oddający siłę zagrożenia.

W Polsce w 2013 r. Rządowe Centrum Bezpieczeństwa przyjęło wielokryterialną metodykę oceny zagrożeń opisaną w podręczniku „Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego" [9]. Według tego poradnika proces oceny siły zagrożeń obejmuje ich identyfikację w kontekście zadań realizowanych przez instytucję dokonującą analizy ryzyka, opracowanie scenariuszy przebiegu zagrożeń, ocenę skutków i prawdopodobieństwo ich wystąpienia oraz ocenę ryzyka – podsumowującą analizę.

Każde zidentyfikowane zagrożenie może mieć różny przebieg, dlatego też należy uwzględnić kilka scenariuszy dla każdego zagrożenia w następujący sposób:

- opis scenariusza;
- potencjalne miejsce wystąpienia;
- potencjalne przyczyny;
- wskazanie roli, jaką będzie pełniła dana instytucja (sporządzająca raport) – wiodąca, koordynującą, pomocniczą – w czasie wystąpienia danego zagrożenia;
- ocena skutków:
  – ludność,
  – gospodarka,
  – mienie,
  – środowisko,
  – infrastruktura krytyczna.

Jeżeli istnieje taka możliwość, prognozę rozwoju zagrożeń należy uzupełnić o elementy graficzne: mapę, zestawienia tabelaryczne lub graficzne (wykresy).

Klasyfikacji skutków zagrożenia dokonuje się w trzech kategoriach: życie i zdrowie, mienie, środowisko. Do oceny skutków przyjęto pięciostopniową skalę oznaczoną literami:

- A – zagrożenia nieistotne;
- B – zagrożenia małe;
- C – zagrożenia średnie;
- D – zagrożenia duże;
- E – zagrożenia katastrofalne.

Jeżeli ocena skutków dla każdego obszaru jest inna, to dla tego scenariusza przypisujemy skalę wyznaczoną dla kategorii życie i zdrowie. Jeżeli dwa z trzech obszarów mają tę samą ocenę, to ją właśnie przypisujemy dla każdego scenariusza.

Prawdopodobieństwo zaistnienia danego scenariusza oceniane jest w pięciostopniowej skali oznaczonej cyframi:

- 1 – bardzo rzadkie – występujące raz na 500 lat;
- 2 – rzadkie – występujące raz na 100 lat;
- 3 – możliwe – występujące raz na 20 lat;
- 4 – prawdopodobne – występujące raz na 5 lat;
- 5 – bardzo prawdopodobne – występujące raz na rok lub częściej.

Po dokonaniu tych analiz każdy scenariusz jest kombinacją cyfry i litery, które określają prawdopodobieństwo wystąpienia danego zdarzenia oraz jego skutki opisane według skal przedstawionych powyżej. Aby odczytać rozmiar ryzyka, kombinację znaków należy odnieść do matrycy ryzyka. Możliwe rozmiary ryzyka:

- minimalne (1A);
- małe (2A, 3A, 2B, 1B, 1C);
- średnie (4A, 5A, 3B, 4B, 5B, 2C, 3C, 4C, 1D, 2D, 3D, 1E, 2E);
- duże (5C, 4D, 5D, 3E, 4E);
- ekstremalne (5E).

Na tej podstawie dla każdego scenariusza oceniamy jego akceptowalności w czterostopniowej skali (ocena ta jest subiektywna):

- ryzyko akceptowane (A) – nie wymagane są żadne dodatkowe środki bezpieczeństwa, akceptowane są aktualne rozwiązania i przypisane im siły i środki, działania monitorujące;

- ryzyko tolerowane (dopuszczalne) (T) – należy dokonać oceny alternatyw czy wprowadzenie niewielkich zmian organizacyjnych, prawnych bądź funkcjonalnych nie przyczyni się do poprawy jakości bezpieczeństwa;
- ryzyko warunkowo tolerowane (WT) – należy wprowadzić dodatkowe środki bezpieczeństwa w ciągu 6 miesięcy, należy ulepszyć stosowane rozwiązania;
- ryzyko nieakceptowane (N) – należy podjąć natychmiastowe działania w celu zwiększenia bezpieczeństwa, wprowadzić dodatkowe, nowe rozwiązania.

Przyjęta w Polsce metodyka analizy ryzyka w sferze zarządzania kryzysowego jest dość skomplikowana. Jeżeli przeprowadzona zostanie w oparciu o modele matematyczne wydaje się być oceną bardzo dokładną. Jednakże złożoność procedury i brak danych dla wielu rodzajów zagrożeń może powodować, że ocena ich siły będzie oceną subiektywną i w wielu przypadkach nieadekwatną do rzeczywistości. Dodatkowym mankamentem tej metodyki, trudnym do uniknięcia, jest analiza ryzyka jedynie dla kilku scenariuszy ewolucji zagrożenia.

Podsumowanie

Zarówno poziom bezpieczeństwa, jak i siła zagrożenia są wielowymiarowe i silnie skorelowane między poszczególnymi wymiarami. Stąd też ich ocena powinna być dokonywana metodami wielokryterialnymi. Wiele takich metod opracowano w ramach teorii decyzji – zarówno normatywnej, jak i psychologicznej. Znajdziemy tam metody czysto matematyczne opierające się na danych statystycznych i analitycznych oraz metody heurystyczne. Wiele z tych metod służy jedynie większej rzetelności opracowywania analiz, starając się eliminować główne słabości ludzkiego myślenia i zbiorowego opracowywania prognoz. Są również metody zwiększające kreatywność, jak na przykład analiza morfologiczna.

Główną trudność w stosowaniu tych metod stanowi duży nakład pracy obliczeniowej i wyszukiwania danych. Jednakże obecnie dysponujemy dużymi mocami obliczeniowymi i wielkimi bazami danych. Wymagają one zupełnie nowych metod wyszukiwania danych i ich analizy, ale to stanowi coraz mniejszy problem.

Stosowanie metod analizy wielokryterialnej do oceny siły zagrożeń lub poziomu bezpieczeństwa staje się faktem, dlatego też może dziwić wydawanie

przez wielu polityków i pseudoekspertów prostych jednokryterialnych ocen bez uwzględniania innych aspektów.

Stosowanie tych metod przyczynia się do lepszego prognozowania przyszłych zdarzeń, zapobiegania im i przygotowania się na ich wystąpienie. Poprawia to nasze poczucie bezpieczeństwa, a tym samych komfort naszego życia.

Literatura

[1] Słownik Języka Polskiego PWN, t. I, Warszawa 1978.
[2] Prońko J., Bezpieczeństwo, zagrożenie, kryzys w kontekście kierowania organizacjami, AON, Warszawa 2011.
[3] Tyszka T., Zaleśkiewicz T., Racjonalność decyzji. Pewność i ryzyko, PWE, Warszawa 2001.
[4] Nosal Cz. S., Umysł menedżera. Problemy-decyzje-strategie, WW Przecinek, Wrocław 1993.
[5] Romanowska M., Zarządzanie strategiczne firmą, wyd. Centrum Informacji Menedżera, Warszawa 1995.
[6] Borysiewicz M., Markowski A. S., Kryteria akceptowalności ryzyka poważnych awarii przemysłowych, wyd. CIOP, Warszawa 2003.
[7] Gierszewska G., Romanowska M., Analiza strategiczna przedsiębiorstwa, Polskie Wydawnictwo Ekonomiczne, Warszawa 2004.
[8] Borysiewicz M., Markowski A. S., Kryteria akceptowalności ryzyka poważnych awarii przemysłowych, wyd. CIOP, Warszawa 2003, www.openpdf.com/ebook/katastroficznych-pdf.html (dostęp: 23.07.2006).
[9] Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, Warszawa, http://rcb.gov.pl/wp-content/uploads/ocenaryzyka.pdf (dostęp: 19.10.2017).
[10] Vaidya O. S., Kumar S., Analytic hierarchy process: An overview of applications, *European Journal of Operational Research* 2006, Volume 169. 1, s. 1–29.
[11] Ritchey T., General Morphological Analysis: A general method for non-quantified modeling, *Swedish Morphological Society* 2002 (Revised 2013), www.swemorph.com/ma.html, (dostęp: 10.09.2017).
[12] Badania operacyjne w przykładach i zadaniach, red. K. Kukuła, PWN, Warszawa 2011, s. 328–346.

[13] Gątarek D. i inni, Nowoczesne metody zarządzania ryzykiem finansowym, WIG-Press, Warszawa 2001.
[14] Gallati R., Risk Management and Capital Adequacy, McGraw-Hill, New York 2003.
[15] Jajuga K., Jajuga T., Inwestycje. Instrumenty finansowe. Ryzyko finansowe. Inżynieria finansowa, PWN, Warszawa 1998.
[16] Tarczyński W., Mojsewicz M., Zarządzanie ryzykiem, PWE, Warszawa 2001.
[17] Jedynak P., Szydło S., Zarządzanie ryzykiem, Wydawnictwo Ossolineum, Wrocław 1997.
[18] Tyszka T., Zaleśkiewicz T., Racjonalność decyzji. Pewność i ryzyko, PWE, Warszawa 2001.
[19] Vaidya O. S., Kumar S., Analytic hierarchy process: An overview of applications. *European Journal of Operational Research* 2006, Volume 169. 1, s. 1–29.
[20] Jedliński M., Jakość w nowoczesnym zarządzaniu, Wydawnictwo Zachodniopomorskiej Szkoły biznesu, Szczecin 2000.
[21] Malesa A. , Optymalizacja wielokryterialna w zastosowaniu do zagadnień transportowych, *Zeszyty Naukowe WSEI* 2012, nr 2.
[22] Mirończuk M., Maciak T., Proces i metody eksploracji danych tekstowych do przetwarzania raportów z akcji ratowniczo – gaśniczych, *Metody Informatyki Stosowanej* 2011, nr 4 (29), Polska Akademia Nauk, s. 147–175.