



Studia i Materiały. Miscellanea Oeconomicae

Rok 21, Nr 4/2017, tom I

Wydział Prawa, Administracji i Zarządzania

Uniwersytetu Jana Kochanowskiego w Kielcach

Zarządzanie kryzysowe i bezpieczeństwo

Marek Kisilowski¹

METODY ILOŚCIOWE (MATEMATYCZNE I TECHNICZNE) W OCENIE RYZYKA W PUBLICZNYM ZARZĄDZANIU KRYZYSOWYM

Streszczenie: W artykule ukazano, że istnieje konieczność szerszego wykorzystania metod matematycznych i technicznych do oceny ryzyka w publicznym zarządzaniu kryzysowym.

Opierając się na badaniach realizowanych w ramach prowadzonego na Wydziale Zarządzania Politechniki Warszawskiej projektu: „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo-Gaśniczego” wskazano możliwość zastosowania nowoczesnych technik w logistycznych sieciach społecznych (LSN), takich jak Internet rzeczy (IoT) lub Machine to Machine (M2M) umożliwiających zbieranie wielkich liczby danych w sieciach funkcjonujących na terenie całego państwa, a także w wymiarze transgranicznym i globalnym. Jako przykład metod ilościowych możliwych do szerszego zastosowania w ocenie ryzyka przywołano zastosowanie teorii wrażliwości oraz metody diagnostyki technicznej. Racjonalne zarządzanie ryzykiem w publicznym zarządzaniu kryzysowym, zdaniem autora powinno mieć charakter interdyscyplinarny. Systemy wspomagające ocenę i zarządzanie ryzykiem będą generowały coraz większą liczbę danych, koniecznych do sprawnego funkcjonowania tych systemów, ale będą powodowały również konieczność zapewnienia bezpieczeństwa informacji, jako dodatkowego źródła ryzyka.

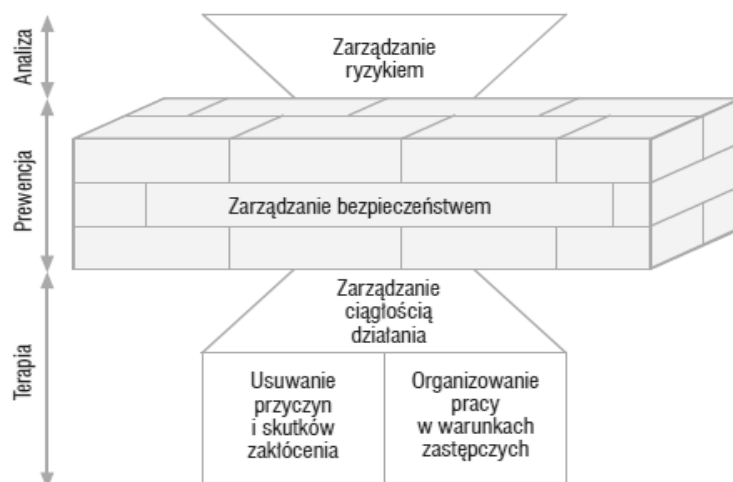
Słowa kluczowe: zarządzanie kryzysowe, logistyka społeczna, diagnostyka techniczna

¹ Dr inż. Marek Kisilowski, Docent na Wydziale Zarządzania, Politechniki Warszawskiej

1. Uwagi wstępne

W celu zdefiniowania metod ilościowych w publicznym zarządzaniu kryzysowym konieczne jest przyjęcie paru podstawowych założeń, które będą stanowić podstawę do sformułowania konkretnych zadań.

W polskiej literaturze problem ten podejmuje Janusz Zawila-Niedźwiecki formułując, że „Jeśli przyjmujemy jako punkt wyjścia system pokazany na rysunku 1, przedstawiający relacje zadań zarządzania ryzykiem, zapewnianie bezpieczeństwa i ciągłości działania, to wynikiem będą trzy elementy: analiza, prewencja i terapia”.



Rysunek 1. Relacje zadań zarządzania ryzykiem, zapewnianie bezpieczeństwa i ciągłości działania²

Analiza tego schematu potwierdza możliwości zastosowania tego modelu w paru innych obszarach, np. technicznych, w których ta triada: ryzyko – bezpieczeństwo – reagowanie również może mieć zastosowanie. Dotyczy to przede wszystkim tych obszarów, gdzie ważna jest ilościowa ocena ryzyka.

Wykorzystując badania realizowane w ramach prowadzonego na Wydziale Zarządzania Politechniki Warszawskiej projektu: „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo-Gaśniczego”³ można stwierdzić, że istnieje konieczność szerszego wykorzystania metod matematycznych i technicznych do oceny ryzyka w publicznym zarządzaniu kryzysowym.

² J. Zawila-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*, edu-Libri, Kraków 2013, s. 56.

³ Projekt finansowany przez NCBiR w ramach konkursu 7/2015.

Opierając się na pracy Marvin Rausand, *Risk Assessment, Theory, Methods and Applications*⁴, oraz pracach S. Kaplan⁵ i S. Kaplan, B.J. Garrick⁶. Można przyjąć za M. Rausand⁷, że ryzyko jest związane z tym co może zdarzyć się w przyszłości, uznając, że można analizować i zarządzać racjonalnie ryzykiem opierając się na metodach matematycznych.

2. Metody ilościowe oceny ryzyka

Ilościowa ocena ryzyka to złożony proces, którego etapy zależą od szeregu elementów. Dwa z nich można uznać za podstawowe: zakres analizy oraz złożoność badanych obiektów. W procesie tym istotne są też metody stosowane do ilościowych ocen stanu badanego urządzenia. W wielu pracach naukowych dotyczących tej problematyki stosuje się podobne metody matematyczne. Obecnie zagadnieniem tym zajmuje się co najmniej kilka ośrodków w świecie, które w swych badaniach uwzględniają wiele identycznych elementów.

Zakres analizy dotyczy metod matematycznych stosowanych na różnych etapach analizy ryzyka. Podstawowe z nich to: procesy stochastyczne, metody statystyczne, zbiory rozmyte, analiza wrażliwości, równania Fokkera Plancka, równania Lagrange'a, elementy teorii grafów oraz elementy teorii niezawodności. Metody te stosowane są zarówno w ujęciu statycznym, jak i dynamicznym, oraz prowadzą do podobnych merytorycznie rozwiązań mimo różnych obszarów ryzyka, w których występują. Wynik zawsze odpowiada na pytanie: co jest istotą ryzyka w aspekcie możliwości jego powstania? Należy podkreślić, że we wszystkich przytoczonych metodach zawsze istnieje możliwość sformułowania końcowego raportu, który w postaci elektronicznej może być przekazany do różnego typu sieci, np. logistyczne sieci społeczne (*Logistics Social Networks* – w skrócie LSN), co daje możliwość tworzenia systemów zarządzania ryzykiem na dowolnym poziomie struktury państwa. Takie możliwości zostaną pokazane w prezentowanym artykule. Istotą jest zawsze to, aby uzyskać z danej analizy sygnał kwantyfikujący możliwość powstania ryzyka.

Mając opisany model matematyczny, na podstawie którego można wykonywać analizę ilościową oceny ryzyka proponuje się następujący zakres działań:

- sformułowanie programu analizy ryzyka,
- określenie struktury i zakresu analizy,
- zdefiniowanie zagrożeń możliwych zdarzeń niebezpiecznych,
- ustalenie przyczyn każdego zdarzenia niebezpiecznego,
- wyznaczenie częstości wystąpienia zdarzenia niebezpiecznego,
- ustalenie sekwencji zdarzeń niebezpiecznych,
- ustalenie scenariuszy, które mogą pojawić się w zdarzeniu niebezpiecznym,

⁴ M. Rausand, *Risk assessment, Theory, Methods, and Applications*, John Wiley & Sons, Inc., 2011.

⁵ S. Kaplan, *The words of risk analysis*, *Risk Analysis*, 17, 1997, s. 407-417.

⁶ S. Kaplan, B.J. Garrick, *On the quantitative definition of risk*, *Risk Analysis*, 1, 1981, s. 11-27,

⁷ M. Rausand, *Risk...*, *op.cit.*

- zdefiniowanie istotnych i typowych scenariuszy dla mogących wystąpić wypadków,
- ustalenie konsekwencji jakie pojawią się po każdym wypadku,
- wyznaczenie częstości niebezpiecznych zdarzeń,
- ocenienie możliwości powstania niebezpiecznego zdarzenia (na podstawie przyjętych metod matematycznych),
- opisanie powstających obrazów ryzyk – sformułowanie modeli matematycznych,
- przygotowanie analizy ryzyka – raportu końcowego – następnie w postaci sygnałów możliwych do rejestracji w LSN.

W celu przeprowadzenia ilościowej analizy ryzyka niezbędnym jest posiadanie dostępu do szerokiego zakresu danych. Analiza ta wymaga zbierania, analizowania i przechowywania danych dotyczących zdarzeń, np. wypadków. Gromadzeniem tego typu danych zajmują się różnego typu instytucje, np. w USA – Reliability Information Analysis Center (RIAC), czy w Europie – the European Safety, Reliability and Data Association (ESReDA). Zadania z zakresu zbierania danych praktycznie nie mają jednolitej struktury, a są tworzone dla różnego typu obszarów np. energetyka jądrowa, lotnictwo, transport kolejowy, przemysł. W Europie zakres zbierania danych reguluje Dyrektywa Unii Europejskiej Seveso III⁸ zobowiązująca do zbierania danych w określonym formacie i kierowania ich do władz krajowych i do bazy ESReDA.

Na podstawie analiz modeli matematycznych uzyskuje się odpowiedź na pytanie, jakie są niezbędne parametry techniczne dla prowadzenia ilościowej oceny ryzyka. Modele te opisują system funkcjonowania systemów technicznych. Ważną grupą danych jest wiedza o poprzednich wypadkach w systemie badanym lub w systemach podobnych.

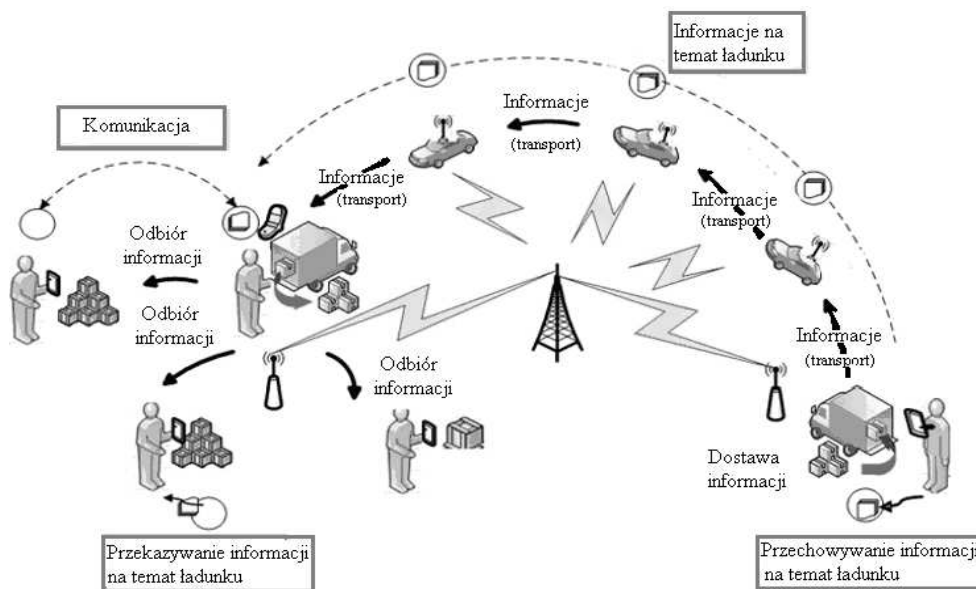
Dla poprawnego funkcjonowania systemu konieczne jest określenie jego niezawodności. Zbierane są zatem dane o częstościach występowania uszkodzeń elementów. Powinny one być zbierane i grupowane w bazach danych. Powinny też być powiązane z sieciami LSN tak, aby można było z nich korzystać dla potrzeb systemów tego samego typu, funkcjonujących w sieciach. Wymaga to również prawidłowej archiwizacji z możliwością dostępu wg. określonych kluczy. Niektóre takie rozwiązania już istnieją, np. Offshore Reliability (OREDA)⁹.

Informacje uzyskane z analiz ilościowych ocen dotyczących ryzyka dla publicznego zarządzania powinny być kierowane do LSN. Zadanie takie można krótko scharakteryzować następująco: wszelkiego rodzaju informacje powinny docierać do

⁸ System ten wprowadziła Dyrektywa 96/82/WE w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi zwana dyrektywą Seveso II zmieniona Dyrektywą Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE, Dziennik Urzędowy UE L 197.

⁹ OREDA (2009), OREDA Reliability Data, OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 4th edition.

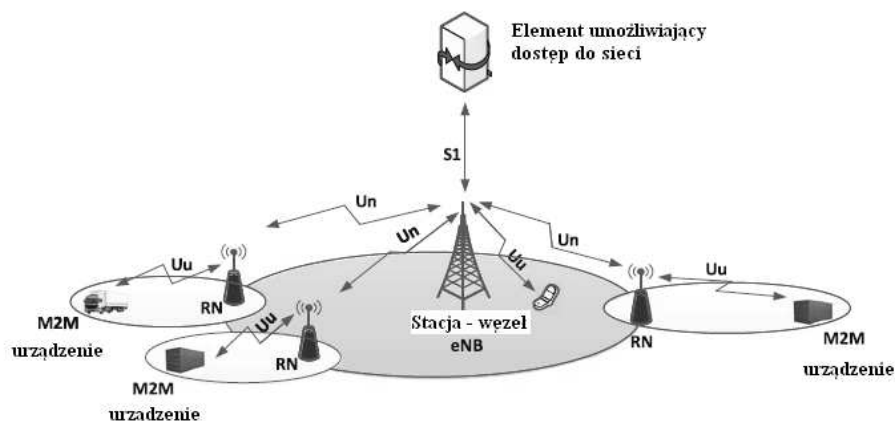
logistycznych sieci społecznych (LSN). W sieciach tych wykorzystuje się wiele nowoczesnych technologii. W ostatnich latach pojawiło się zastosowanie Internetu rzeczy (*Internet of Things* – w skrócie IoT), również dla społecznych sieci logistycznych. Jedną z istotnych w tym zakresie jest praca L. Atzori, A. Iera i G. Morabito¹⁰, która pokazuje nową architekturę w społecznym Internecie rzeczy (*Social Internet of Things* – w skrócie SIoT). Wykorzystywane są sieci internetowe (Twitter, Facebook, Weibo, QQ) dla badania różnych elementów życia społecznego w tym również dla analizy ryzyka. Równoległe IoT stała się silnym narzędziem przesyłania cyfrowych informacji logistycznych co pokazano na rys. 2.



Rysunek 2. Informacje logistyczne przemieszczające się w systemie

Zbiór informacji przepływających przez sieć może dotyczyć różnych obszarów, konkretne informacje mogą dotyczyć również ilościowych elementów oceny ryzyka. Rozpatrując IoT w odniesieniu do logistyki musimy uwzględnić trzy problemy. Po pierwsze występuje pełna integracja informacji przez całą drogę jej transportu w sieci logistycznej, co jest niezwykle ważne dla ilościowych informacji dotyczących ryzyka. Po drugie mogą pojawić się możliwości zachowań ułatwiających komunikowanie się z organizacjami (w różnych sieciach) co umożliwi sygnalizację powstających ryzyk. Po trzecie można wykorzystać IoT do zbierania danych dotyczących procedur logistycznych związanych również z ilościowymi ocenami ryzyka.

¹⁰ L. Atzori, A. Iera, G. Morabito: *SIoT: Giving a Social Structure to the Internet of Things*, IEEE Communications Letters, 15(11), Nov. 2011, s. 1193-1195.



Rysunek 3. M2M-LTE-A architektura z węzłem przekaźnikowym¹¹

gdzie:

eNB – eNodeB – bazowa stacja – węzeł – element dostępowy,

Uu – połączenie między M2M a RN,

Un – połączenie między stacją bazową a RN.

Nowym paradygmatem w sieciach logistycznych jest „*Machine to Machine*” w skrócie M2M, który przedstawiony został w pracach Farhan Ahmad, Safdar Nawaz Khan Marwat, Yasir Zaki, Yasir Mehmood i Carmelita Görg¹² oraz Yasir Mehmood, Thomas Pötsch, Safdar Nawaz Khan Marwat, Farhan Ahmad, Carmelita Görg i Imran Rashid¹³, w których przewiduje się spotkanie miliardów inteligentnych urządzeń do komunikowania się bez lub z niewielkim udziałem człowieka, czyli maszyn do komunikowania się ze sobą. Ważnym zadaniem, które spełnia M2M w logistyce, jest problem komunikowania się różnych rodzajów informacji, które są generowane przez M2M. Zakres tych informacji jest bardzo szeroki i może również obejmować informacje o stanie urządzenia, jego niezawodności i możliwości powstania zagrożenia dla funkcjonowania urządzenia podmiotu i otoczenia. Liczba urządzeń, które mogą generować informację może być bardzo duża i może zawierać dowolny ich zakres. Jest to istotne dla przetwarzania informacji o stanie ryzyka; maszyny, fabryki i otoczenia. Ilości danych dotyczące ilościowych elementów oceny ryzyka są relatywnie niewielkie (w stosunku do komunikacji międzyludzkiej)

¹¹ F. Ahmad, SNK Marwat, Y. Zaki, Y. Mehmood, C. Görg, *Machine-to-Machine Sensor Data Multiplexing Using LTE-Advanced Relay Node for Logistics*, [w:] H. Kotzab, J. Panek, KD. Thoben (Eds.), *Dynamics in Logistics*, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014, s. 251.

¹² F. Ahmad, SNK. Marwat, Y. Zaki, Y. Mehmood, C. Görg, *Machine-to-Machine Sensor Data Multiplexing Using LTE-Advanced Relay Node for Logistics*, [w:] Kotzab H., Panek J., Thoben K.D. (Eds), *Dynamics in Logistics*, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014, s. 247-258.

¹³ Y. Mehmood, T. Pötsch., SNK Marwat, F. Ahmad, C. Görg, I. Rashid, *Impact of Machine-to-Machine Traffic on LTE Data Traffic Performance*, [w:] H. Kotzab, J. Panek, KD. Thoben (Eds.), *Dynamics in Logistics*, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014, s. 259-270.

co prowadzi do możliwości prowadzenia procesów optymalizacyjnych zapewniających dobrą wydajność M2M w ocenie ryzyka. W sieci M2M ważnym urządzeniem jest węzeł przekaźnikowy (ang. *Relay Node* w skrócie RN). Zasady funkcjonowania tego systemu można scharakteryzować za pomocą rys. 3.

Szczegóły systemu można znaleźć w pracy Farhan Ahmad i in. (2016)¹⁴. Przedstawiona koncepcja może mieć szerokie zastosowanie do zbierania sygnałów, które charakteryzują stan urządzenia czy przedsiębiorstwa.

3. Przykłady metod matematycznych w ocenie ilościowej ryzyka

3.1. Zastosowanie teorii wrażliwości dla oceny ryzyka

Uzasadniając potrzebę wykorzystania metod matematycznych w ocenie ilościowej ryzyka dla przykładu można pokazać dwa zastosowania metod matematycznych.

Marvin Rausand w swojej pracy¹⁵ sugeruje wykorzystanie analizy wrażliwości w procesie oceny ryzyka.

Postawiony problem można rozwiązać w oparciu o analizę modelu matematycznego opisującego obiekt techniczny. Przy czym dla przeprowadzenia poprawnego procesu budowy modelu matematycznego należy przyjąć następujące założenia:

- obiekt rzeczywisty przyjmuje się jako liniowy, o stałych parametrach, bryłach sztywnych; prowadzi to do dynamiki obiektu za pomocą liniowych równań różniczkowych rzędu dwa;
- zaburzenia przyjmuje się, że posiadają własności stacjonarności w szerszym sensie i globalnej ergodyczności;
- układy współrzędnych uogólnionych przyjęto tak, że można trajektorię rozwiązania porównywać z trajektoriami ruchu poszczególnych mas dla rzeczywistego obiektu.

Posiadając założenia jak powyżej możemy zapisać równania ruchu mas obiektu. Metody formułowania tych równań są stosunkowo skomplikowane i dla potrzeb niniejszej pracy nie ma potrzeby ich cytowania. Wystarczy jedynie zapis nazwy dwóch podstawowych, które stosuje się najczęściej. I tak pierwsza metoda to równania Lagrange'a lub druga równania d'Alemberta¹⁶.

Ogólną postać równań liniowych można zapisać w postaci macierzowej:

$$A\ddot{q}(t) + B\dot{q}(t) + Cq(t) = F(t), \quad (1)$$

gdzie:

A, B, C – są macierzami zawierającymi stałe (masowo-bezwładnościowe, tłumienia, sprężystości);

q – jest wektorem współrzędnych uogólnionych;

F(t) – jest wektorem wymuszeń.

¹⁴ *Ibidem*, s. 247-258.

¹⁵ M. Rausand, *Risk assessment, Theory, Methods, and Applications*, John Wiley & Sons, Inc., 2011, rozdział 16.

¹⁶ J.R. Taylor, *Mechanika klasyczna T.1* Warszawa, 2006, s. 212-271 oraz B. Kozak, *Mechanika techniczna*, Warszawa 2004, s. 294-295.

Własności takiego układu zależą wyłącznie od parametrów macierzy A, B i C. Dlatego można określić, które parametry mają wpływ na cechy obiektu, którego zmiany mogą wywołać powstanie zagrożenia, co pozwala na zdefiniowanie relacji między parametrami a cechami, które mogą stanowić zagrożenie. Dla właściwego toku postępowania konieczne jest określenie zakresu zmiany parametrów, które powinny zostać zachowane, aby nie powstało zagrożenie niebezpiecznym zdarzeniem. Określenie wartości poprawnych parametrów spowoduje, że w rozważanych ryzykach powstanie bariera ograniczająca powstanie zagrożeń. Jeśli zakres parametrów będzie znajdował się w przewidzianym przedziale to niebezpieczne zdarzenie nie powstanie. Tak więc należy określić związki między parametrami a wybranymi cechami (które mogą być powodem niebezpiecznych zdarzeń).

Na podstawie elementarnych przekształceń otrzymujemy równanie:

$$\dot{x} = Gx, \quad (2)$$

gdzie:

$$G = \begin{bmatrix} -A^{-1}B & -A^{-1}C \\ I & 0_1 \end{bmatrix}, \quad x = \begin{bmatrix} \dot{q} \\ q \end{bmatrix},$$

$$\dim A = \dim B = \dim C = \dim I = \dim 0_1 = n \times n, \quad \dim G = 2n \times 2n$$

I jest macierzą jednostkową; 0_1 – macierzą zerową.

Równanie to nazywa się równaniem stanu, a macierz G – macierzą stanu.

Dla równania stanu można wyznaczyć (numerycznie) wartości im odpowiadające i wektory własne, które dotyczą również modelu matematycznego, równanie (1).

Obliczenia można wykonać dla parametrów rzeczywistego obiektu.

Jako przykład wybranej cechy układu przyjęto wartości własne:

$$\lambda_j = a_j + ib_j \quad (3)$$

gdzie:

a_j – współczynnik tłumienia, jeśli wszystkie $a_j < 0$, wahania są tłumione, tzn. ruch obiektu jest asymptotycznie stateczny w sensie Lapunowa;

b_j – częstość oscylacji o okresie $T_i = 2\pi/b_j$.

Po przekształceniach i obliczeniach numerycznych otrzymano w efekcie zależność, która umożliwiła zdefiniowanie algorytmu dla obliczeń:

$$\frac{\partial \lambda_i}{\partial p_j} = \bar{k}_i \frac{\partial G}{\partial p_j} \bar{w}_i \quad (4)$$

gdzie:

\bar{k}_i, \bar{w}_i – i-ty wektor i wiersz własny.

Po przeprowadzeniu pełnej analizy możliwe jest ustalenie zależności zaburzeń parametrów na wybrane cechy układu. Pozwala to odpowiedzieć na pytanie, który parametr może wywoływać zaburzenie cechy wpływającej na powstanie zagrożenia. Należy dodać, że cechy obiektu są dobierane tak, aby można je wyznaczyć w modelu i porównywać je z cechami obiektu rzeczywistego. Najczęściej są to sygnały pochodzące z obiektów rzeczywistych, które mogą być kierowane do sieci, które zarządzają ryzykiem.

3.2. Metody diagnostyki technicznej dla określenia ryzyka powstania zagrożenia

Drugi obszar, który można wykorzystać dla określania zagrożeń prowadzących do ilościowej oceny ryzyka to zagadnienie wykorzystania metod diagnostyki technicznej dla określenia ryzyka powstania zagrożenia w dowolnym systemie technicznym. Można tu zacytować podejście wykorzystujące do oceny stanu urządzenia krzywe życia maszyny. Zadanie to zostało szczegółowo omówione w pracach S. Radkowski, J. Kisilowski, M. Kisilowski¹⁷ oraz M. Kisilowski¹⁸.

Stan maszyny jest określane za pomocą symptomów. Symptomy maszyny mogą być np. wibroakustyczne. Więcej szczegółów na ten temat można znaleźć w pracach Cz. Cempel¹⁹ i J. Morela²⁰.

Na podstawie tych prac można zdefiniować tribowibroakustyczny model maszyny i można to analitycznie opisać (dla danego symptomu):

$$\frac{S(\Theta)}{S_0} = \left[1 - \frac{\Theta}{\Theta_b} \right]^{\frac{1}{\gamma}} ; \Theta \subset \Theta_b ; \quad (5)$$

gdzie:

S_0 – początkowa wartość symptomu;

$\frac{\Theta}{\Theta_b}$ – bezwymiarowy czas zużycia maszyny;

$\frac{1}{\gamma}$ – wykładnik krzywej zużycia maszyny, wyznaczony wg krzywej z rys. 4;

$S(\Theta)$ – symptom po czasie Θ ;

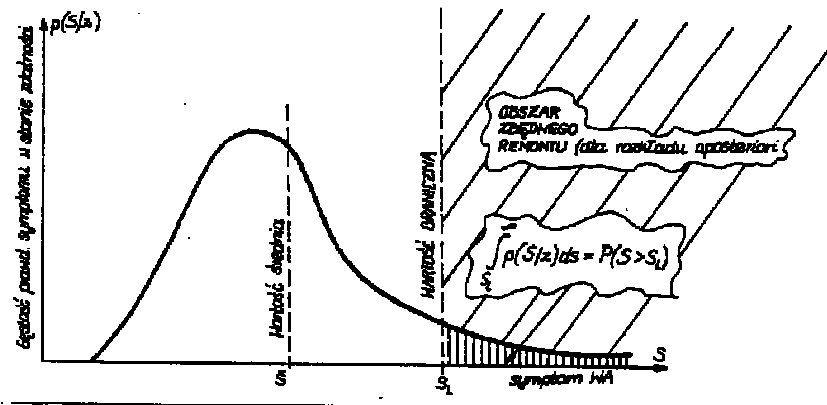
wielkości γ, Θ_b, S_0 – ocenia się na podstawie eksperymentu.

¹⁷ S. Radkowski, J. Kisilowski, M. Kisilowski, *Technical diagnosis in risk assessment in property insurance, Diagnostyka 2000*, II International Congress of Technical Diagnostics, Warsaw, Poland, 19-22 September 2000.

¹⁸ M. Kisilowski, *Zasady zarządzania ryzykiem ubezpieczeniowym maszyn i urządzeń technicznych*, rozprawa doktorska, Orgmasz, Warszawa 2002.

¹⁹ Cz. Cempel, *Diagnostyka wibroakustyczna maszyn*, PWN, Warszawa 1989.

²⁰ J. Morela, *Drgania maszyn i diagnostyka ich stanu technicznego*, Polskie Towarzystwo Diagnostyki Technicznej, Warszawa 1992.



Rysunek 4. Ilustracja podstawy wyjściowej diagnostycznego modelu probabilistycznego do wyznaczenia wartości granicznej SI techniką Neymana-Pearsona teorii decyzji statystycznych²¹

Kluczowym problemem w realizacji procesu analizy ryzyka jest zagadnienie oceny potencjalnych zagrożeń, w tym hipotetycznego procesu uszkodzania. Zastosowanie tego podejścia oznacza w praktyce przeprowadzenie systematycznej analizy działania układu dla wykrycia i określenia zagrożeń, w tym nieprzewidywalnych w normalnej eksploatacji oraz ewentualnych problemów eksploatacyjnych wynikających z faktu istnienia niepewności co do sposobu i intensywności przebiegu procesów degradacji i zużycia.

Przy przyjęciu określonych założeń dotyczących obciążeń S i obciążalności L jako zmiennych losowych można doprowadzić do uzyskania zależności na prawdopodobieństwo wystąpienia uszkodzenia określonego zależnością:

$$P_f = \int_{\Omega} f_{x_1 \dots x_n} S(X_1 \dots X_n) dX_1 \dots dX_n \quad (6)$$

Ponieważ funkcja gęstości prawdopodobieństwa jest najczęściej nieznana a procedury całkowania w równaniu (6) uciążliwe, w celu obliczenia prawdopodobieństwa wystąpienia uszkodzenia (awarii) należy opracować odpowiednio uproszczone techniki obliczeń, które pokazano w pracy M. Kisilowski²².

Przedstawiona procedura umożliwia wyznaczenie prawdopodobieństwa wystąpienia awarii w funkcji czasu eksploatacji maszyny. Parametry te powinny być znane w sieci, w której funkcjonują oceniane urządzenia, np. LSN.

²¹ Cz. Cempel, *Diagnostyka wibroakustyczna maszyn*, PWN, Warszawa 1989.

²² M. Kisilowski, *Zasady zarządzania ryzykiem ubezpieczeniowym maszyn i urządzeń technicznych*, rozprawa doktorska, Orgmasz, Warszawa 2002.

4. Podsumowanie

Z zaprezentowanych badań literaturowych wynika, że w zarządzaniu kryzysowym należy wykorzystać logistyczne sieci społeczne (LSN), w których można zastosować nowoczesne techniki np. Internet rzeczy (IoT) lub Machine to Machine (M2M) umożliwiające zbieranie dowolnej ilości danych w sieci LSN funkcjonującej na terenie całego państwa, a nawet szerzej. Przedstawiono również dwie ilościowe metody umożliwiające ocenę ryzyka i procedurę przekazywania tych wyników do sieci LSN, która jest narzędziem w publicznym zarządzaniu kryzysowym. Zapewnienie bezpieczeństwa publicznego we współczesnym świecie, przy istnieniu tak szerokiej taksonomii zagrożeń wymaga sięgnięcia w zarządzaniu kryzysowym do metod matematycznych i technicznych, które pozwolą na skuteczniejsze zarządzanie ryzykiem. Badania naukowe dotyczące bezpieczeństwa muszą mieć charakter interdyscyplinarny uwzględniający wszystkie aspekty zarządzania kryzysowego. Nie można jednak nie dostrzegać, że generowanie coraz większej ilości danych powoduje, że zastosowanie metod matematycznych i technicznych to również konieczność zapewnienia bezpieczeństwa informacji i określenia granic wolności osobistej. Nie zmienia to faktu, że ryzykiem należy zarządzać racjonalnie i można się tu oprzeć na zaprezentowanych metodach matematycznych i technicznych.

Bibliografia:

- Ahmad F., Marwat SNK, Zaki Y., Mehmood Y. and Görg C., *Machine-to-Machine Sensor Data Multiplexing Using LTE-Advanced Relay Node for Logistics*, [w:] Kotzab H., Panek J., Thoben K.D. (Eds.), *Dynamics in Logistics*, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014.
- Atzori L., Iera A. and Morabito G., *SloT: Giving a Social Structure to the Internet of Things*, IEEE Communications Letters, 15(11), Nov. 2011.
- Cempel Cz., *Diagnostyka wibroakustyczna maszyn*, PWN, Warszawa 1989.
- Dyrektywa 96/82/WE w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi zwana dyrektywą Seveso II zmieniona Dyrektywą Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE, Dziennik Urzędowy UE L 197.
- Kaplan S., Garrick B. J., *On the quantitative definition of risk*, Risk Analysis, 1: 11-27, 1981.
- Kaplan S., *The words of risk analysis*, Risk Analysis, 17:407-417, 1997.
- Kisilowski J., Kisilowski M., Radkowski S., *Technical diagnosis in risk assessment in property insurance*, *Diagnostyka 2000*, II International Congress of Technical Diagnostics, Warsaw, Poland, 19-22 September 2000.
- Kisilowski M., *Zasady zarządzania ryzykiem ubezpieczeniowym maszyn i urządzeń technicznych*, rozprawa doktorska, Orgmasz, Warszawa 2002.
- Kozak B., *Mechanika techniczna*, Warszawa 2004.
- Mehmood Y., Pötsch T., Marwat SNK, Ahmad F., Görg C. and Rashid I., *Impact of Machine-to-Machine Traffic on LTE Data Traffic Performance*, [w:] Kotzab H., Panek J., Thoben K.D. (Eds.), *Dynamics in Logistics*, Proceedings of the 4th International Conference LDIC, Bremen, Germany 2014.

- Morela J., *Drgania maszyn i diagnostyka ich stanu technicznego*, Polskie Towarzystwo Diagnostyki Technicznej, Warszawa 1992.
- OREDA (2009), OREDA Reliability Data, OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 4th edition.
- Rausand M., *Risk assessment, Theory, Methods, and Applications*, John Wiley & Sons, Inc., 2011.
- Taylor J. R., *Mechanika klasyczna*, T. 1, Warszawa 2006.
- Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnieniu ciągłości działania organizacji*, edu-Libri, Kraków 2013.

Abstract

Mathematical and technical quantitative methods of risk evaluation in public crisis management

The article discusses the necessity of broader application of mathematical and technical methods of risk evaluation in public crisis management. Referring to the project being realised at the Faculty of Management, Warsaw University of Technology "Highly specialized platform supporting civil emergency planning and rescue in the Polish public administration and organizational units of the National Firefighting and Rescue System" the possibility of application of modern techniques in social networks (LSN), like the Internet of things (IoT) or Machine to Machine (M2M), enabling collection of big data in national, regional or global networks. The sensitivity theory and technical diagnostics methods are presented as exemplification of quantitative methods for potential broader application in risk evaluation. The author suggests that rational risk management in public crisis management should have an interdisciplinary character. Systems supporting risk evaluation and management will generate more and more data indispensable for their efficient functioning, causing the necessity of assuring safety of information as an additional source of risk.

Keywords: crisis management, social logistics, technical diagnostics