Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 241 · 2015

Informatyka i Ekonometria 3

Dorota Kuchta

Politechnika Wrocławska
Wydział Informatyki i Zarządzania
Katedra Systemów Zarządzania
dorota.kuchta@pwr.edu.pl

Stanisław Stanek

Wyższa Szkoła Oficerska Wojsk Lądowych
im. gen. T. Kościuszki
Wydział Zarządzania
Katedra Inżynierii Systemów
s.stanek@wp.pl

Barbara Gładysz

Politechnika Wrocławska
Wydział Informatyki i Zarządzania
Katedra Badań Operacyjnych, Finansów
i Zastosowań Informatyki
barbara.gladysz@pwr.edu.pl

Stanisław Drosio

Uniwersytet Ekonomiczny w Katowicach
Wydział Informatyki i Komunikacji
Katedra Informatyki
stanislaw.drosio@gmail.com

ZARZĄDZANIE RYZYKIEM W KRYTYCZNYCH SYSTEMACH INFORMATYCZNYCH NA PRZYKŁADZIE CENTRUM ZARZĄDZANIA KRYZYSOWEGO

Streszczenie: Artykuł poświęcony jest zarządzaniu ryzykiem w krytycznych systemach informatycznych. Zaproponowano zastosowanie podejścia rozmytego oraz modyfikację znanej metody HAZOP. Zaproponowane modyfikacje pozwolą na skuteczniejsze zarządzanie ryzykiem w rozpatrywanym typie systemów informatycznych. Propozycje są uzasadnione i zilustrowane dwoma studiami przypadku z jednej z polskich jednostek samorządowych.

Słowa kluczowe: zarządzanie ryzykiem, system krytyczny, zmienna rozmyta, metoda HAZOP.

Wprowadzenie

Niniejszy artykuł odnosi się do zarządzania ryzykiem w krytycznych systemach informatycznych, czyli takich, których awaria lub nieprawidłowe działanie może skutkować śmiercią lub poważnymi obrażeniami ludzi, utratą bądź

poważnymi uszkodzeniami urządzeń albo zanieczyszczeniem środowiska [Srinivas i Seetharamaiah, 2015]. Charakter tych systemów wymusza konieczność niezwykle starannego zarządzania ryzykiem. Dotyczy to na przykład zastosowania wysokich technologii w centrach zarządzania kryzysowego czy szpitalach. W niniejszym artykule zajęto się tym pierwszym przypadkiem.

W systemach krytycznych, w których materializacja ryzyka może skutkować śmiercią czy uszczerbkiem na zdrowiu, należy stosować jak najskuteczniejsze metody zarządzania ryzykiem. Ważne jest, by testować w nich różne znane podejścia do zarządzania ryzykiem i do modelowania niepewności, oceniać je, ewentualnie modyfikować i wdrażać do codziennego użycia.

W niniejszym artykule zostanie podjęta próba modyfikacji klasycznego podejścia do zarządzania ryzykiem w krytycznych systemach informatycznych. Zostanie ono uzupełnione o podejście rozmyte. Zostanie zaproponowana modyfikacja znanej metody zarządzania ryzykiem HAZOP, polegająca na połączeniu jej z podejściem rozmytym oraz uzupełnieniu jej o wymóg dokładniejszej analizy odchyleń i anomalii. Zaproponowane podejście jest pracochłonne, ale w zarządzaniu ryzykiem w systemach krytycznych konieczny jest wyjątkowo duży nakład pracy, bo skutki materializacji ryzyka mogą być katastrofalne.

W systemach informatycznych, które często mają za zadanie wspomagać podejmowanie decyzji w sytuacjach trudnych i złożonych, zwłaszcza w systemach krytycznych, bardzo ważne jest zapewnienie bezpieczeństwa ich działania. Bezpieczeństwo działania systemu obejmuje różne aspekty i pojęcia (ich przegląd można znaleźć np. w: [Srinivas i Seetharamaiah, 2015], m.in. różne typy wydarzeń (np. awaria bez poważnych skutków, awaria z poważnymi skutkami, zdarzenie anormalne itp.). Ryzyko definiuje się w takich systemach jako kombinację możliwości wystąpienia zdarzenia anormalnego lub awarii i skutków tego zdarzenia bądź awarii dla komponentów systemu, jego operatorów, użytkowników lub otoczenia. Ryzyko, w przypadku którego konsekwencje mogą być bardzo poważne lub krytyczne, musi zostać wyeliminowane.

Zarządzanie ryzykiem w omawianym typie systemów informatycznych obejmuje identyfikację możliwych zdarzeń anormalnych i awarii, ocenę ich prawdopodobieństwa, skutków, a także umiejscowienia (zasięgu) oraz możliwości wczesnego wykrycia [Srinivas i Seetharamaiah, 2015].

W kolejnym punkcie chwilowo odejdzie się od tematu zarządzania ryzykiem, aby wprowadzić podejście rozmyte, które następnie będzie wykorzystane w zarządzaniu ryzykiem.

1. Rozmyte podejście do definicji złożonych lub nieprecyzyjnych pojęć

L.A. Zadeh [1983] wprowadził możliwość matematycznego modelowania nieprecyzyjnych pojęć, takich jak „wysoki", „inny" itp., oraz stosowania ich wzmocnień, osłabień, rozszerzeń itp. w taki sposób, że po ustaleniu matematycznych modeli znaczeń pojęć podstawowych, a także określonych na nich funkcji, można posługiwać się nimi w sposób zbliżony do języka naturalnego. Definiowanie pojęć odbywa się za pomocą tzw. funkcji przynależności, określonej na przestrzeni, której elementy podlegają ocenie, o wartościach w przedziale [0,1].

Niech zatem przestrzeń, której elementy podlegają ocenie, będzie oznaczona jako U, a definiowane jest pojęcie jako r. Funkcja przynależności μ_{r}, zdefiniowana na U, o wartościach w przedziale [0,1], jest modelem opinii eksperta, w jakim stopniu $x \in U$ jest r.

Na przykład w odniesieniu do odchylenia od określonej wartości pożądanej można definiować (na podstawie opinii ekspertów) znaczenie słowa „duży" za pomocą funkcji $\mu_{\mathrm{duży}}$, zdefiniowanej na zbiorze liczb nieujemnych.

$$\mu_{\mathrm{duży}}(x) = \begin{cases} 1 \text{ jeśli } x \geq 80\% \\ \frac{10x}{6} - \frac{1}{3} \text{ jeśli } 20\% \leq x \leq 80\% \\ 0 \text{ jeśli } x \leq 20\% \end{cases} \quad (1)$$

Zgodnie z (1) odchylenie uznane jest za w pełni duże, jeśli jest równe lub przewyższa 80% pożądanej wartości, i za w pełni małe, jeśli jest mniejsze od 20% pożądanej wartości. Jeśli odchylenie przyjmuje wartości między 20% i 80%, to jest duże w różnym, niepełnym stopniu.

Funkcja μ_{r} pozwala na stopniowanie stopnia posiadania cechy r, tak jak to robi umysł ludzki.

Ponadto, również wzorem ludzkiego umysłu, rozpatruje się różne niuanse cech podstawowych [Zadeh, 1983]. Na przykład wzmocnienia pojęcia r, oznaczane umownie r2, r3 itd., oznaczają takie pojęcia, jak „bardzo r", „wyjątkowo r" itp. Wzmocnienia są funkcjami pojęcia podstawowego r. Funkcje te są również określane na podstawie opinii ekspertów. Przykładowo funkcja μ_{r^2} może być określona na następujące sposoby:

a) $\mu_{\mathrm{r}^2}(x) = \left(\mu_{\mathrm{r}}(x)\right)^2$,

b) $\mu_{\mathrm{r}^2}(x) = \mu_{\mathrm{r}}(x - a)$,

gdzie:

a – stała podana przez eksperta.

W przypadku a) nie zmienia się zbiór elementów posiadających cechę w stopniu większym od zera, jednak tym elementom „trudniej" jest podsiadać tę cechę w wysokim stopniu. W drugim przypadku zbiór elementów posiadających cechę w stopniu zero zmienia się – następujący zbiór jest niepusty: $\{x\colon \mu_{\text{r}^2}(x) = 0 \text{ i } \mu_{\text{r}}(x) > 0\}$.

W podobny sposób można definiować osłabienia pojęcia r („trochę r", „mało r", „około r") i jego rozszerzenia (np. „w przybliżeniu r", „r lub p", gdzie p jest inną cechą itp.). Ważną funkcją pojęcia r jest pojęcie „na granicy r". Przykładowo, dla pojęcia „duży" można zdefiniować pojęcie „na granicy dużego" (w oryginale *borderline* [Zadeh, 1983]) za pomocą następującej funkcji:

$$\mu_{\text{na granicy dużego}}(x) = \begin{cases} 1 \text{ jeśli } \mu_{duży}(x) \geq 0{,}9 \\ 5\mu_{\text{duży}}(x) - 3{,}5 \text{ jeśli } 0{,}7 \leq \mu_{\text{duży}}(x) \leq 0{,}9 \\ 0 \text{ jeśli } \mu_{\text{duży}}(x) \leq 0{,}7 \end{cases}$$

Teraz powrócimy do problemu zarządzania ryzykiem, wykorzystując w nim podejście rozmyte.

2. Zastosowanie podejścia rozmytego w zarządzaniu ryzykiem

W zarządzaniu ryzykiem ważne zastosowanie mają reguły rozmyte, czyli zdania warunkowe w trybie rozkazującym, wyrażone w języku naturalnym, których przesłanki są oparte na pojęciach rozmytych [np. Kuchta i Ptaszyńska, 2011; Anooj, 2012]. Przykładowo, w zarządzaniu ryzykiem danego systemu informatycznego możemy wykorzystywać następujące reguły:

a) jeśli kwalifikacje operatora są małe i opady duże, wyślij innego operatora do pomocy;
b) jeśli opady są duże i wiatr jest silny, zastosuj działania przygotowujące odpowiednie ekipy do działań ratowniczych.

Reguły są albo generowane na podstawie opinii eksperta, albo na podstawie doświadczeń z przeszłości [Kuchta i Ptaszyńska, 2013]. Warunki w regułach są oparte na pojęciach rozmytych, definiowanych tak, jak to opisano w punkcie 1. Reguły stosowane są w ten sposób, że jeśli w danej sytuacji wszystkie funkcje przynależności przesłanek przyjmują wartości nieujemne, to wykonywane jest polecenie reguły. Jeśli dwie reguły mają różne następniki, wybierana jest ta reguła, której przesłanki są spełnione w większym stopniu.

Trzeba również zauważyć, że choć literatura dotycząca reguł decyzyjnych zazwyczaj nie podkreśla tego wystarczająco wyraźnie, w regułach decyzyjnych

warto wykorzystywać wzmocnienia, osłabienia i inne funkcje podstawowych pojęć, opisane w poprzednim punkcie.

Następnie zostanie uzasadnione stosowanie reguł z rozmytymi przesłankami, z wykorzystaniem funkcji podstawowych pojęć.

3. Studium przypadku – realizacja osłony hydrogeologicznej powiatu

Studium przypadku wykorzystane w niniejszym punkcie jest uproszczoną wersją rzeczywistego przypadku, pochodzącego z jednej z polskich jednostek samorządowych.

Instytut Meteorologii i Gospodarki Wodnej w rozpatrywanym województwie, na podstawie danych własnych oraz pochodzących z innych źródeł, opracowuje prognozę pogody, do której wchodzą następujące podstawowe czynniki:

a) wysokość opadu,
b) natężenie opadu,
c) siła wiatru,
d) wysokość wody na wodowskazach rzek powiatu.

Dane do bieżącej pracy operacyjnej przekazywane są do Centrum Zarządzania Kryzysowego Wojewody, Powiatowego Centrum Zarządzania Kryzysowego, Centrów/Urzędów Gmin wchodzących w skład powiatu. Analizy parametrów odbywają się zgodnie z tabelami, w których zawarte są „klasyczne" przedziały wartości powyższych czynników wraz ze słownym opisem. Przedziały są rozłączne i pokrywają całą przestrzeń możliwych wartości. Tytułem przykładu, w tab. 1 podane są odpowiednie informacje dla wysokości opadów.

Tabela 1. Wysokość opadu – grubość warstwy wody, jaka powstaje na skutek opadu na poziomej powierzchni podłoża (mm/m^2 dla okresu ważności prognozy)

Opady	Deszcz [mm]	Śnieg [mm]
Małe	0,0–5,0	0,0–2,5
Umiarkowane	5,1–10,0	2,6–5,0
Dość silne	10,1–20,0	5,1–10,0
Silne	> 20,0	> 10,0

Źródło: Materiały wewnętrzne jednostki samorządowej.

Podobnie dla pozostałych czynników zdefiniowane są pojęcia „małe", „umiarkowane", „dość silne (wysokie)", „silne (wysokie)", a dla wiatru dodatkowo „wichura", „huragan", „nawałnica". Należy jeszcze raz podkreślić, że w doku-

mentach rozpatrywanej jednostki samorządowej nie są to pojęcia rozmyte, ponieważ granice poszczególnych przedziałów są ostre.

Przy takim podejściu do zarządzania ryzykiem stosowane są reguły typu:

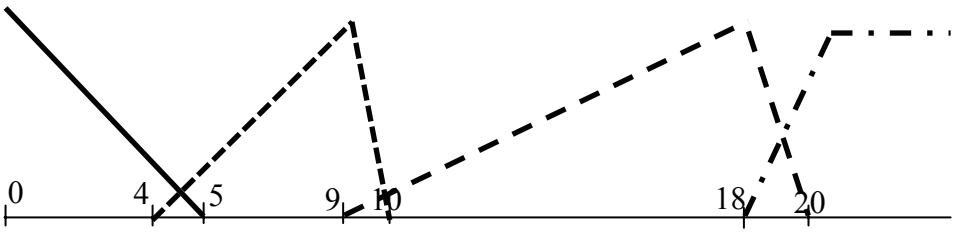
a) jeśli opady umiarkowane, wprowadzić stan gotowości;
b) jeśli opady małe, nie podejmować żadnych środków.

Reguły – nierozmyte, ponieważ ich przesłanki nie są oparte na pojęciach rozmytych – stosowane są w ten sposób, że jeśli wartości wspominane w przesłankach reguł należą do odpowiednich przedziałów, to wykonywane jest polecenie reguły.

Jeśli chodzi o drugą z powyższych reguł, to przy takim podejściu może ona okazać się zbyt słaba w skutkach i doprowadzić do niepożądanych skutków. Może tak się stać w przypadku, kiedy wysokość opadu (deszczu) będzie wprawdzie „tylko" mała zgodnie z tab. 1, ale jednocześnie przyjmie wartość 4,9. Wówczas tak naprawdę mamy do czynienia z sytuacją, gdy powinna być zastosowana reguła a) albo „prawie" reguła a).

Stosując podejście opisane w punkcie 2, należałoby przeformułować tab. 1 np. w następujący sposób (omawiamy wyłącznie drugą kolumnę, dotyczącą deszczu, o definicji poszczególnych funkcji przynależności decydowałby ekspert). Na rys. 1 zostały graficznie przedstawione propozycje rozmycia cech opisujących deszcz z tab. 1, za pomocą odpowiednich funkcji przynależności. I tak:

- funkcja reprezentowana jako ——— dotyczy pojęcia „małe", $\mu_{\text{małe}}$;
- funkcja reprezentowana jako – – – – – – dotyczy pojęcia „umiarkowane", $\mu_{\text{umiarkowane}}$;
- funkcja reprezentowana jako — — — · dotyczy pojęcia „dość silne", $\mu_{\text{dość silne}}$;
- funkcja reprezentowana jako — · — · · dotyczy pojęcia „silne", μ_{silne}.



Rys. 1. Propozycja rozmycia definicji cech deszczu z tab. 1

Następnie można by postąpić na dwa sposoby:

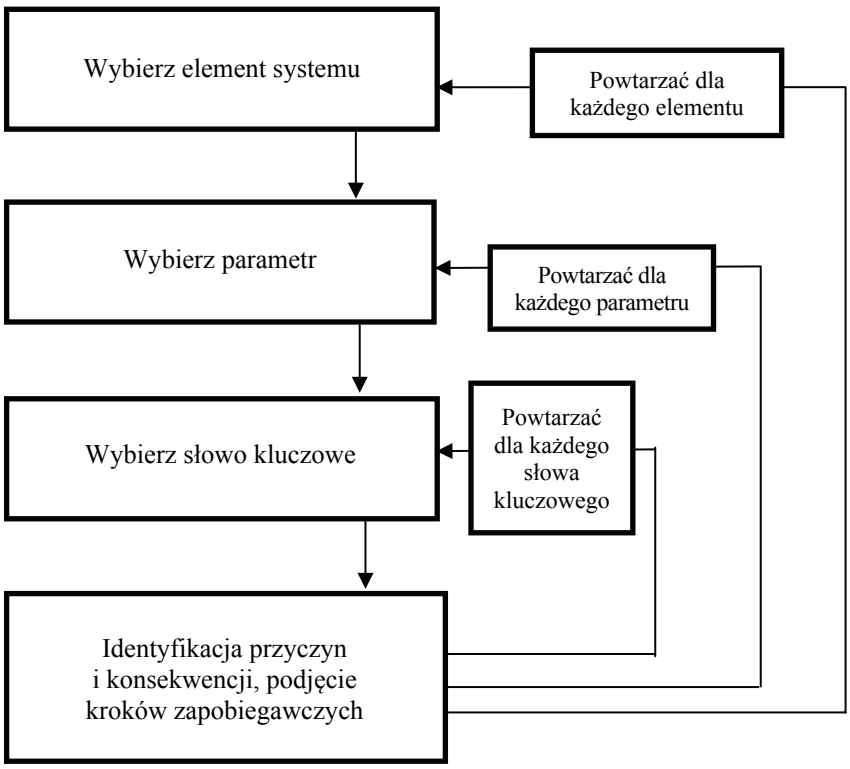
a) albo definiować reguły, w których w przesłankach wykorzystywałoby się wartości zmiennych decyzyjnych, np. $\mu_{\text{małe}}(x) \leq 0{,}2$ i $\mu_{\text{umiarkowane}}(x) \geq 0{,}1$, jednak takie reguły nie byłyby wyrażone w języku zbliżonym do naturalnego;

b) albo wykorzystać opisane w poprzednim rozdziale funkcje pojęć i definiować pojęcia takie jak „na granicy małego", „na granicy umiarkowanego". Wówczas można by formułować reguły w języku zbliżonym do naturalnego, takie jak: jeśli opady na granicy małych i umiarkowanych, to przygotować się do wprowadzenia stanu gotowości. Takie podejście pozwoliłoby szybciej zareagować wówczas, kiedy opady jednak osiągnęłyby poziom „umiarkowany".

W dalszej części artykułu przejdziemy do zastosowania w zarządzaniu ryzykiem krytycznych systemów informatycznych metody HAZOP.

4. Metoda HAZOP w ujęciu klasycznym

Metoda HAZOP (Hazard and Operability Study) w ujęciu klasycznym opisana jest np. w [Angel i in., 2015]. Wywodzi się z przemysłu chemicznego, na potrzeby którego została opracowana w latach 60. XX w.



Rys. 2. Metoda HAZOP w ujęciu klasycznym

Źródło: Na podstawie: [Angel i in., 2015].

Jej zastosowanie do systemów informatycznych przedstawione jest np. w: [Redmill i in., 1997] oraz w standardzie opracowanym przez rząd brytyjski [Ministry of Defence, 1990]. Poniżej przedstawimy jej ujęcie klasyczne. Wyjdziemy od uproszczonego diagramu ilustrującego jej działanie (rys. 2).

Elementy systemu to węzły, kanały przesyłowe itd. Parametry systemu to np. szybkość (przepływu), częstotliwość (np. sygnału), jakość (np. sygnału), kierunek (np. przepływu informacji) itp. Istota metody HAZOP polega na wykorzystywaniu listy słów kluczowych, które mają wskazywać na odchylenia i anomalie wartości parametrów. Dla tych odchyleń oraz anomalii należy zidentyfikować przyczyny i skutki, ocenić skutki i prawdopodobieństwo odchyleń oraz anomalii, a także podjąć środki zaradcze, jeśli to zostanie uznane za konieczne.

Lista słów kluczowych jest podawana w literaturze, ale w dużej mierze powinna ona być budowana na podstawie doświadczenia i być dopasowana do danego systemu. W tab. 2 podano przykładową listę wraz z przykładową interpretacją.

Tabela 2. Przykładowa lista słów kluczowych do metody HAZOP

Atrybut	Słowo kluczowe	Interpretacja
Przepływ (danych lub sterowania)	brak	Brak przepływu
	więcej	Przesyłanych jest więcej danych niż oczekiwano
	częściowo	Przesyłana informacja jest niekompletna (dotyczy przepływów grupowych)
	odwrotnie	Przepływ informacji w niewłaściwym kierunku
	inaczej	Informacja kompletna, ale niewłaściwa
	wcześniej	Przepływ informacji następuje wcześniej niż oczekiwano
	później	Przepływ informacji następuje później niż wymagano
Częstotliwość przesyłania	więcej	Częstotliwość przesyłania danych jest zbyt duża
	mniej	Częstotliwość przesyłania danych jest zbyt mała
Wartość danej	więcej	Wartość danej jest za wysoka (w zakresie lub poza zakresem)
	mniej	Wartość danej jest za niska (w zakresie lub poza zakresem)

Źródło: [Ministry of Defence, 1990].

Metoda HAZOP została poddana obszernej krytyce w: [Baybutt, 2015]. Krytyka ta dotyczy wielu aspektów, ale m.in. tego, że w oryginalnej metodzie HAZOP nie są rozpatrywane odchylenia złożone, czyli kombinacje różnych

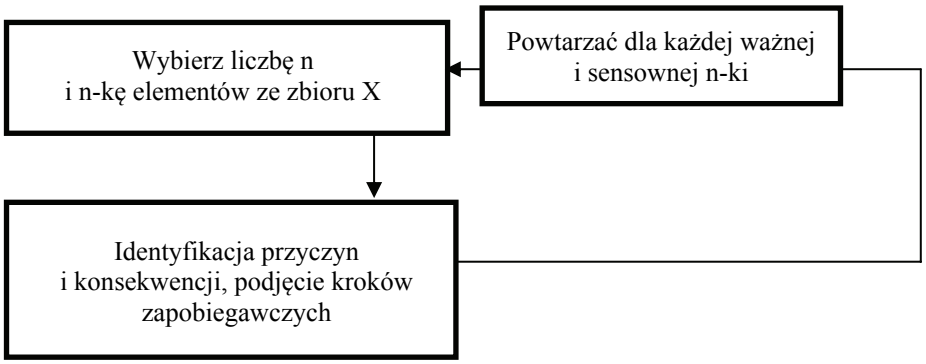
odchyleń. Na rys. 2 widać, że każde słowo kluczowe, połączone z parametrem i elementem systemu, jest rozpatrywane pojedynczo; potem algorytm każe przejść do innego słowa kluczowego. Jak pisze Baybutt [2015], złożone odchylenia mogą prowadzić do konsekwencji, które przy analizie pojedynczych odchyleń mogą pozostać niewykryte, co będzie pokazane również w punkcie 5. Mimo iż złożone odchylenia mają często stosunkowo niskie prawdopodobieństwo [Baybutt, 2015], w systemach krytycznych trzeba je brać pod uwagę, nawet jeśli zwiększy to pracochłonność metody. Małe prawdopodobieństwo zdarzenia nie zwalnia bowiem od jego analizy, jeśli jego konsekwencje mogą być bardzo duże czy wręcz katastrofalne. To właśnie rozpatrywanie złożonych odchyleń, wraz z podejściem rozmytym, jest istotą proponowanego uogólnienia metody HAZOP.

5. Uogólnienie metody HAZOP jako narzędzie analizy ryzyka w krytycznych systemach informatycznych

Biorąc pod uwagę zarzuty sformułowane w: [Baybutt, 2015] oraz propozycję Zadeha [1983] opisaną w punkcie 1, proponujemy, w przypadku krytycznych systemów informatycznych wymuszenie uwzględniania kombinacji słów kluczowych i odchyleń (dla tych samych elementów systemu i dla różnych), mając świadomość tego, że znacznie zwiększy to pracochłonność metody, a także tego, że problem wyznaczania tych kombinacji w praktyce pozostaje otwarty. Niektóre kombinacje nie będą bowiem miały sensu, inne mogą być w pierwszej chwili uznane za niemające sensu (niemożliwe), ale w rzeczywistości będą możliwe, tylko oceniający padną ofiarą swoich utartych poglądów oraz przyzwyczajeń. Problem ten jest otwarty i trudny, niemniej jednak naszym zdaniem z rozpatrywania kombinacji odchyleń w przypadku rozpatrywanych tutaj systemów zrezygnować nie wolno, co potwierdzi studium przypadku w następnym punkcie.

Ponadto naszym zdaniem pojęcia występujące w słowach kluczowych należy definiować jako zmienne rozmyte, tak jak to pokazano w punkcie 1, i uwzględniać ich niuanse, czyli wzmocnienia, osłabienia, uogólnienia itd. Oczywiste jest bowiem, że może się zdarzyć, iż w przypadku dwóch średnich odchyleń oraz w przypadku serii piętnastu bardzo małych odchyleń wystąpią podobne konsekwencje, a zupełnie inne konsekwencje wystąpią w przypadku jednego małego i jednego ogromnego odchylenia. Naszym zdaniem uwzględnianie kombinacji oraz niuansów pojęć rozmytych pozwoli zidentyfikować wiele wydarzeń o poważnych konsekwencjach, których przy tradycyjnym stosowaniu metody HAZOP zidentyfikować by się nie dało.

Zmodyfikowany diagram metody HAZOP jest zaprezentowany na rys. 3. Występujący tam zbiór X to zbiór wszystkich sensownych czwórek (element systemu, parametr, słowo kluczowe, niuans słowa kluczowego). Na przykład elementem X jest czwórka (przepływ informacji od A do B, częstotliwość, rzadziej, bardzo). Liczba n, również występująca na rys. 1, to potencjalnie dowolna liczba naturalna, reprezentująca liczbę odchyleń, jaka będzie uwzględniana w jednej kombinacji. Oczywiście zazwyczaj będą to liczby stosunkowo małe, 2, 3, 4, ale jeśli w systemie istnieje długi łańcuch powiązań, to być może należy rozpatrywać kombinacje złożone z wielu elementów – tylu, ile składa się na taki łańcuch. Tak jak wspomniano wyżej, problem wyznaczania kombinacji, które należy rozpatrzyć, jest otwarty. Dużo będzie zależało od danego systemu, a także od wiedzy i doświadczenia ekspertów.



Rys. 3. Uogólniona metoda HAZOP

W kolejnym punkcie zostanie zaprezentowane studium przypadku, którego celem jest uzasadnienie wyżej przedstawionych propozycji dotyczących zarządzania ryzykiem w krytycznych systemach informatycznych.

6. Studium przypadku – akt terroryzmu lub bioterroryzm na terenie powiatu

Opis przypadku

Ma miejsce zdarzenie terrorystyczne lub bioterrorystyczne. Przepływ informacji będzie następujący:

1. Ktoś musi powiadomić jeden z poniższych elementów systemu (każdy element, który otrzyma wezwanie, musi powiadomić pozostałe elementy):
   a) Gminne Centrum Zarządzania Kryzysowego na terenie gmin, w których doszło do zdarzenia;

b) Komendę Powiatową Policji;
c) Komendę Powiatową Państwowej Straży Pożarnej,
d) Powiatowe Stanowiska Koordynacji Ratownictwa,
e) Powiatowe Centrum Zarządzania Kryzysowego,
f) Wojewódzkie Stanowisko Koordynacji Ratownictwa,
g) Wojewódzkie Stanowisko Koordynacji Ratownictwa Medycznego,
h) Wojewódzkie Centrum Zarządzania Kryzysowego,
i) inne służby ratownicze.

2. Gminne Centrum Zarządzania Kryzysowego ustala, z maksymalną możliwą dokładnością (na podstawie informacji napływających od pierwszych patroli policji oraz zastępów straży pożarnej): zakres, dokładny czas i miejsce zdarzenia oraz rozmiar i charakter zdarzenia, ilość ofiar i rannych. Na podstawie tych informacji rozdysponowuje odpowiednie siły i środki w celu:
   a) zabezpieczenia miejsca zdarzenia;
   b) uregulowania ruchu drogowego w celu ograniczenia ilości pojazdów na miejscu zdarzenia, a także kontroli wjazdu i wyjazdu pojazdów;
   c) zabezpieczenia ratowniczego miejsca zdarzenia (ratownictwo medyczne);
   d) ewakuacji ofiar zamachu i mieszkańców terenu zagrożonego pośrednio poszkodowanych w zdarzeniu.

3. Jeśli zaistnieje taka potrzeba, należy zadysponować przyjazd specjalistycznych grup ratowniczych:
   a) negocjatora i pododdziałów realizacyjnych policji, jeśli są zakładnicy;
   b) specjalistycznej grupy ratownictwa chemicznego, w przypadku zagrożenia rozprzestrzenienia się substancji szkodliwych;
   c) specjalistycznych grup saperskich, celem neutralizacji zagrożenia bombowego i poszukiwania kolejnych ładunków wybuchowych w miejscach określonych przez stanowisko kierowania.

„Klasyczne" zastosowanie metody HAZOP

1. *Wybór elementu systemu*: przepływ informacji od kogoś na miejscu zdarzenia do jednego z elementów a) … i).
2. *Wybór parametru*: szybkość.
3. *Wybór słowa kluczowego*: „mniej".
4. *Interpretacja, identyfikacja przyczyn i konsekwencji*: zbyt późno powiadomiono odpowiednie służby, z powodu np. braku zasięgu telefonu lub braku osób, które byłyby w na tyle dobrym stanie, by móc zadzwonić. Konsekwen-

cje: osoby poszkodowane, którym można by pomóc, otrzymają pomoc zbyt późno – konsekwencje poważne.
5. *Podjęcie kroków zapobiegawczych lub minimalizujących wystąpienie zdarzenia, jego prawdopodobieństwa i konsekwencji* – tu nieomawiane.

1. *Wybór elementu systemu*: przepływ informacji od służb na miejscu zdarzenia do Centrum Zarządzania Kryzysowego.
2. *Wybór parametru*: zawartość.
3. *Wybór słowa kluczowego*: „mniej".
4. *Interpretacja, identyfikacja przyczyn i konsekwencji*: informacje na temat charakteru i zakresu zagrożeń są zbyt optymistyczne. Przyczyną mógł być brak specjalistów, pośpiech, emocje, rozmiar szkód. Konsekwencje: zostaną wysłane niewłaściwe lub zbyt mało liczne ekipy ratunkowe, osoby poszkodowane, którym można by pomóc, otrzymają pomoc zbyt późno, wcale albo otrzymają pomoc niefachową – konsekwencje poważne.
5. *Podjęcie kroków zapobiegawczych lub minimalizujących wystąpienie zdarzenia, jego prawdopodobieństwa i konsekwencji* – tu nieomawiane.

Jak wspomniano w punkcie 4, w klasycznym zastosowaniu metody HAZOP analizy poszczególnych węzłów, parametrów i słów kluczowych odbywają się niezależnie. Ponadto nie rozróżnia się niuansów rozmiarów odchylenia – jego cechy definiowane są „ostro". Teraz zaprezentujemy zastosowanie proponowanych uogólnień metody HAZOP. Zaczniemy od wprowadzenia samego rozmycia pojęć, a następnie wprowadzimy uwzględnianie kombinacji.

Zastosowanie rozmytej metody HAZOP

1. *Wybór elementu systemu*: przepływ informacji od kogoś na miejscu zdarzenia do jednego z elementów a) … i).
2. *Wybór parametru*: szybkość.
3. *Wybór słowa kluczowego*: „mniej" – „nieznacznie mniej", „trochę mniej", „znacznie mniej", „katastrofalnie mniej".
4. *Interpretacja, identyfikacja przyczyn i konsekwencji*:
   a) nieznacznie mniej – przyczyną mogą być chwilowe problemy z zasięgiem lub chwilowy szok; konsekwencje średnie;
   b) trochę mniej – przyczyny jak wyżej bądź czas potrzebny, by poszkodowany człowiek sięgnął po telefon i wybrał numer; konsekwencje duże;
   c) znacznie mniej – ludzie są tak poszkodowani, że dopiero osoba przybyła z zewnątrz może zadzwonić; konsekwencje poważne;

   d) katastrofalnie mniej – nikt w pobliżu miejsca zdarzenia nie jest w stanie zawiadomić służb ratowniczych; konsekwencje katastrofalne.
5. *Podjęcie kroków zapobiegawczych lub minimalizujących wystąpienie zdarzenia, jego prawdopodobieństwa i konsekwencji* – tu nieomawiane.

1. *Wybór elementu systemu*: przepływ informacji od służb na miejscu zdarzenia do Centrum Zarządzania Kryzysowego.
2. *Wybór parametru*: zawartość.
3. *Wybór słowa kluczowego*: „mniej" – „nieznacznie mniej", „trochę mniej", „znacznie mniej", „katastrofalnie mniej".
4. *Interpretacja, identyfikacja przyczyn i konsekwencji*:
   a) nieznacznie mniej – nieznaczna pomyłka w ocenie sytuacji z powodu pośpiechu i emocji; konsekwencje niewielkie, ponieważ zostaną wysłane „prawie" właściwe ekipy;
   b) trochę mniej – mała pomyłka w ocenie sytuacji z przyczyn jw., która może skutkować wysłaniem zbyt mało licznej lub trochę gorzej wyposażonej ekipy, co przełoży się na zbyt późną pomoc lub pomoc nie do końca fachową dla małej grupy ofiar; konsekwencje duże;
   c) znacznie mniej – poważny błąd w ocenie sytuacji, wynikający z niefachowości lub emocji osób oceniających, może skutkować wysłaniem ekip o wyposażeniu i liczebności nieadekwatnych do charakteru zdarzenia, a co za tym idzie, nieudzieleniem odpowiedniej pomocy znacznej grupie ofiar; konsekwencje poważne;
   d) katastrofalnie mniej – całkowicie błędna (w sensie: zbyt optymistyczna, nierealistyczna) ocena sytuacji, wynikająca z rozmiarów i charakteru zdarzenia, które uniemożliwiły jego prawidłową ocenę; będzie to skutkowało wysłaniem zbyt mało licznych ekip, być może o nieodpowiednich kwalifikacjach, niesięgnięciem po pomoc z innych województw czy nawet państw; większość poszkodowanych nie otrzyma fachowej pomocy; konsekwencje katastrofalne.
5. *Podjęcie kroków zapobiegawczych lub minimalizujących wystąpienie zdarzenia, jego prawdopodobieństwa i konsekwencji* – tu nieomawiane.

W rozmytej metodzie HAZOP analiza poszczególnych elementów systemu przebiega osobno, ale rozróżniane są różne stopnie intensywności odchyleń. Pozwala to rozróżnić przyczyny, skutki i ewentualne środki zaradcze w przypadku odchyleń o różnych intensywnościach, oraz skoncentrować się na tym, co naprawdę ważne. Jednak, jak wspomniano w punkcie 4, w systemach krytycznych należy rozpatrywać kombinacje elementów systemu, parametrów i słów kluczowych. Oto jak mogłoby to wyglądać w rozpatrywanym przypadku.

Zastosowanie uogólnionej metody HAZOP

Określenie zbioru X czwórek (element systemu, parametr, słowo kluczowe, niuans):

1. *Wybór liczby naturalnej*: n=2.
2. *Wybór 2 elementów ze zbioru X*: przepływ informacji od kogoś na miejscu zdarzenia do jednego z elementów a) … i), szybkość, „mniej", „trochę"; przepływ informacji od służb na miejscu zdarzenia do Centrum Zarządzania Kryzysowego, zawartość, „mniej", „trochę".
3. Wybrana kombinacja jest sensowna.
4. *Interpretacja, identyfikacja przyczyn i konsekwencji*: jeśli służby zostaną powiadomione trochę za późno i dodatkowo przedstawiciele służb na miejscu zdarzenia, kiedy już tam dotrą, przekażą trochę zbyt optymistyczną ocenę sytuacji, będzie mniej czasu na korektę liczby oraz charakteru ekip wysłanych na miejsce zdarzenia i znaczna grupa poszkodowanych może nie uzyskać odpowiedniej pomocy – konsekwencje poważne.
5. *Podjęcie kroków zapobiegawczych lub minimalizujących wystąpienie zdarzenia, jego prawdopodobieństwa i konsekwencji* – tu nieomawiane.

Jak widać na powyższym przykładzie, rozpatrywanie kombinacji elementów ze zbioru X pozwoliło zidentyfikować poważne konsekwencje w przypadku kombinacji zdarzeń, które przy osobnym traktowaniu zostałyby ocenione jako zdarzenia o konsekwencjach „jedynie" dużych. Wydaje się, że przedstawiona wyżej kombinacja ma na tyle istotne prawdopodobieństwo, że nie można jej ignorować. Klasyczna metoda HAZOP nie doprowadziłaby do jej identyfikacji.

Podsumowanie

W niniejszym artykule zaproponowano systematyczne uwzględnianie w zarządzaniu ryzykiem krytycznych systemów informatycznych podejścia rozmytego oraz rozpatrywanie kombinacji możliwych odchyleń i anomalii. Zaproponowano uogólnienie znanej metody HAZOP, co zostało zilustrowane za pomocą dwóch studiów przypadku z Centrum Zarządzania Kryzysowego jednej z polskich jednostek samorządowych.

Zaproponowane podejście znacznie zwiększy pracochłonność zarządzania ryzykiem, dlatego musi być poddane dalszym badaniom, przede wszystkim dotyczącym sposobów zmniejszenia liczebności kombinacji podlegających sprawdzeniu bez szkody dla skuteczności metody. Jednak wydaje się, że w krytycznych systemach informatycznych, w których materializacja ryzyka może mieć bardzo poważne skutki, nie ma innej drogi – nie można rezygnować z rozpatry-

wania podczas analizy ryzyka kombinacji oraz niuansów różnych cech i właściwości elementów systemu tylko dlatego, że jest to pracochłonne. Konsekwencje takiej rezygnacji mogą być katastrofalne.

Literatura

Anooj P.K. (2012), *Clinical Decision Support System: Risk Level Prediction of Heart Disease Using Weighted Fuzzy Rules*, „Journal of King Saud University – Computer and Information Sciences", No. 24(1), s. 27-40.

Baybutt P. (2015), *A Critique of the Hazard and Operability (HAZOP) Study*, „Journal of Loss Prevention in the Process Industries", No. 33, s. 52-58.

Kuchta D., Ptaszyńska E.D. (2011), *The Concept of System Supporting Risk Management in European Projects* [w:] Z. Wilimowska i in. (eds.), *Information Systems Architecture and Technology: Information as the Intangible Assets and Company Value Source*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, s. 53-62.

Kuchta D., Ptaszyńska E.D. (2013), *Wykorzystanie procesu uczenia się w zarządzaniu ryzykiem projektów rolnych*, „Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. T. Kościuszki", 4(45), s. 124-134.

Ministry of Defence (1990), *HAZOP Studies on Systems Containing Programmable Electronics.*

O Herrera M.A. de la, Luna A.S., Costa A.C.A. da, Blanco Lemes E.M. (2015), *A Structural Approach to the HAZOP – Hazard and Operability Technique in the Biopharmaceutical Industry*, „Journal of Loss Prevention in the Process Industries", No. 35, s. 1-11.

Redmill F., Chudleigh M.F., Catmur J.R. (1997), *Principles Underlying a Guideline for Applying HAZOP to Programmable Electronic Systems*, „Reliability Engineering and System Safety", Vol. 55(3), s. 283-293.

Srinivas Acharyulu P.V., Seetharamaiah P. (2015), *A Framework for Safety Automation of Safety-critical Systems Operations*, „Safety Science", No. 77, s. 133-142.

Zadeh L.A. (1983), *A Computational Approach to Fuzzy Quantifiers in Natural Languages*, „Computers & Mathematics with Applications", No. 9(1), s. 149-184.

RISK MANAGEMENT IN CRITICAL SYSTEMS OF INFORMATION ON THE EXAMPLE OF CRISIS MANAGEMENT CENTER

Summary: This article is devoted to risk management in critical information systems. We propose a fuzzy approach and modify the well-known HAZOP method. The proposed modifications will enable more effective risk management in the type of systems considered. The proposals are justified and illustrated by two case studies from a Polish local government unit.

Keywords: risk management, critical system, fuzzy variable, HAZOP method.