Problemy Zarządzania, vol. 15, nr 1 (66), cz. 2: 125–144
ISSN 1644-9584, © Wydział Zarządzania UW
DOI 10.7172/1644-9584.66.8

Sieć Bayesa jako narzędzie wspomagające zarządzanie ryzykiem operacyjnym w banku

Nadesłany: 26.09.16 | Zaakceptowany do druku: 25.01.17

Dominika Gadowska-dos Santos

W niniejszym artykule autor próbuje wykazać, że w procesie zarządzania ryzykiem operacyjnym w banku szczególnie istotne jest przeprowadzenie analizy źródeł ryzyka wraz z rozpoznaniem zależności przyczynowo-skutkowych. Jedynie gruntowna wiedza o powodach i konsekwencjach materializacji ryzyka daje bowiem szansę skutecznego prognozowania efektów podejmowanych działań zarządczych, planowania interwencji i poprzez to kształtowania rzeczywistości zgodnie z oczekiwaniami. Artykuł koncentruje się na zaprezentowaniu narzędzia badania łańcuchów przyczynowych – sieci Bayesa, które mogą pomóc bankom lepiej zrozumieć naturę ryzyka operacyjnego, zmniejszyć jego skalę i w efekcie zwiększyć efektywność działania instytucji. Zaprezentowana zostanie definicja, zasady konstrukcji, sposoby wykorzystania tej metody do analizy zależności przyczynowo-skutkowych pomiędzy czynnikami ryzyka operacyjnego, a także zalety i wady tego podejścia.

Słowa kluczowe: ryzyko operacyjne, bank, sieć Bayesa, zależności przyczynowo-skutkowe.

Bayes Belief Network as an Operational Risk Management Tool for Banks

Submitted: 26.09.16 | Accepted: 25.01.17

This paper shows that analysis of risk sources and identification of cause-effect relationships are crucial elements of the operational risk management process. Knowledge of the reasons and consequences of risk materialization is key for reliable forecasting of the effects of managerial actions and for planning interventions capable of shaping the reality according to expectations. The article concentrates on presenting one means of analyzing causal chains – Bayesian networks that can help banks understand the nature of operational risk, minimizing its scale, and, as a result, increasing the financial institutions' efficiency. The definition, design rules, ways of using the method to analyze cause-effect relationships between operational risk factors, as well as advantages and drawbacks of the approach, are discussed.

Keywords: operational risk, bank, Bayesian network, cause-effect relationships.

JEL: C11, D81, D83, G21, G31

* **Dominika Gadowska-dos Santos** – dr, Uniwersytet Warszawski, Wydział Nauk Ekonomicznych, Katedra Bankowości, Finansów i Rachunkowości.

Adres do korespondencji: Uniwersytet Warszawski, Wydział Nauk Ekonomicznych, ul. Długa 44/50, 00-241 Warszawa; e-mail: dgadowska@wne.uw.edu.pl.

1. Wprowadzenie

Sektor usług bankowych należy do najszybciej rozwijających się gałęzi gospodarki. Podobnie jak na innych rynkach, instytucje są tu zmuszone do działania w ciągle zmieniającym się otoczeniu, którego immanentną cechą jest niepewność. Skuteczność działania i jednocześnie sukces rynkowy zależą w ich przypadku od umiejętnego sformułowania i realizowania strategii, której zasadniczym elementem jest opracowanie metod radzenia sobie z ryzykiem. Wśród czyhających niebezpieczeństw na szczególną uwagę zasługuje ryzyko operacyjne. Do niedawna traktowane jako kategoria rezydualna, aktualnie często wymieniane wśród największych zagrożeń i stanowiące bardzo istotny element profilu ryzyka instytucji.

Artykuł rozpoczyna przedstawienie definicji ryzyka operacyjnego oraz ewolucji metod zarządzania nim – od standardowych po holistyczne podejście pod postacią zintegrowanego systemu zarządzania. W prezentowanym procesie zarządzania ryzykiem operacyjnym, wpisującym się w ramy koncepcji zarządzania adaptacyjnego, szczególnie ważne jest dokonanie pomiaru i przeprowadzenie analizy źródeł ryzyka wraz z rozpoznaniem zależności przyczynowo-skutkowych. Wydaje się bowiem, że jedynie gruntowna wiedza o źródłach i konsekwencjach materializacji ryzyka daje szansę prognozowania efektów podejmowanych działań, planowania interwencji i kształtowania rzeczywistości zgodnie z oczekiwaniami.

Niniejszy artykuł przedstawia narzędzie badania łańcuchów przyczynowych, którego wykorzystanie przez instytucje finansowe może się przyczynić do lepszego zrozumienia natury ryzyka operacyjnego, zmniejszenia jego skali i w efekcie – zwiększenia skuteczności działania. Narzędziem tym są sieci Bayesa. Opracowanie prezentuje definicję, zasady konstrukcji oraz sposoby wykorzystania tej metody do analizy zależności przyczynowo-skutkowych pomiędzy czynnikami ryzyka operacyjnego. Artykuł kończy zestawienie zalet i wad tego narzędzia.

2. Ryzyko operacyjne – przedmiot badań i instrumenty zarządzania

2.1. Obszar ryzyka operacyjnego

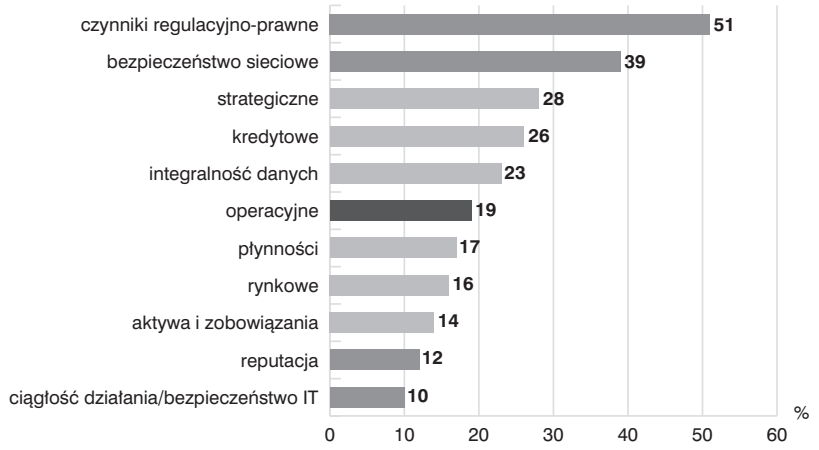
Mimo że ryzyko operacyjne jest wszechobecne i w działalności banków było obserwowane od zawsze, to do niedawna traktowane było jako kategoria rezydualna, inaczej mówiąc każde ryzyko, którego źródłami są czynniki inne niż rynkowe czy kredytowe (Da Costa Lewis, 2004). Jednak ze względu na mnożące się przypadki strat wykraczających poza tradycyjne kategorie ryzyka, a które można wyjaśnić jako efekt oddziaływania czynników ryzyka operacyjnego, zaczęto poświęcać mu coraz więcej uwagi. Potwierdzeniem tej tendencji może być fakt wprowadzenia obowiązku utrzymywania przez banki kapitału na pokrycie ewentualnych strat operacyjnych w Nowej Umowie

 DOI 10.7172/1644-9584.66.8

Kapitałowej (NUK)[1]. Decyzji tej przyświecała chęć nie tylko uodpornienia instytucji na szoki popytowe i podażowe oraz nieprzewidziane straty finansowe i pozafinansowe z nimi związane (np. utratę reputacji), ale również zmotywowania banków do poprawienia systemów pomiaru, zarządzania i kontroli ryzyka operacyjnego.

Stosunkowo najczęściej wykorzystywaną definicją ryzyka operacyjnego jest ta przygotowana przez Komitet Bazylejski w toku prac nad NUK. W dokumentach Komitetu definicja ta uzyskała następujące brzmienie: „Ryzyko operacyjne należy rozumieć jako ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych. W zakres ryzyka operacyjnego wchodzi ryzyko prawne, natomiast wyłącza się z niego ryzyko reputacji i strategiczne" (Komisja Nadzoru Bankowego, 2004). Do ryzyka operacyjnego możemy zwłaszcza zaliczyć: ryzyko związane ze zniszczeniem aktywów trwałych (np. akty wandalizmu), ryzyko technologii (np. przerwanie pracy systemu), ryzyko interakcji z otoczeniem (np. nadużycia zewnętrzne, takie jak kradzieże) i ryzyko zasobów ludzkich (np. nadużycia wewnętrzne czy roszczenia pracownicze).

Czynniki ryzyka operacyjnego niezmiennie wymieniane są wśród największych zagrożeń dla funkcjonowania organizacji. Dziewiąta edycja badania Deloitte *Global Risk Management Survey* z 2015 r. wskazuje na typy ryzyka, które zyskają na znaczeniu w perspektywie najbliższych dwóch lat (Deloitte, 2015). Okazuje się, że czynniki ryzyka operacyjnego wymieniano w tym zestawieniu zarówno wprost, jak i pośrednio (rysunek 1).



Rys. 1. Największe wyzwania dla organizacji w najbliższych dwóch latach. Źródło: Deloitte. (2015). Global Risk Management Survey. Pozyskano z: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/ru-global-risk-management-survey-9th-edition.pdf (15.06.2016).

Jeśli wyniki te zestawić ze stopniem przygotowania podmiotów do radzenia sobie z kluczowymi rodzajami ryzyka ocenionym w badaniu AON (*Global Management Survey*) przez sektor bankowy na 69% i tym, że odpowiadają one za średnio 33% utraconych przychodów tych instytucji (AON, 2015), to okaże się, iż istnieje potrzeba rozwijania i ulepszania systemu zarządzania ryzykiem operacyjnym, o którym mowa w dalszej części artykułu.

2.2. Zintegrowane zarządzanie ryzykiem operacyjnym

Mianem zarządzania ryzykiem określa się wszelkie działania „mające na celu planową i celową analizę, sterowanie typami ryzyka występującymi w działalności bankowej oraz kontrolę podejmowanych przedsięwzięć" (Zawadzka, 1998). Jest to z jednej strony nauka, na co wskazują Vaughan i Vaughan, stwierdzając, że „zarządzanie ryzykiem to naukowe podejście do postępowania z poszczególnymi rodzajami ryzyka poprzez antycypowanie przypadkowych strat i przygotowanie oraz wdrożenie procedur, które pozwalają minimalizować występowanie strat bądź znaczenie tych strat, które już wystąpiły" (Vaughan i Vaughan, 2003), ale z drugiej strony – jak zauważają Crouchy, Galai i Mark – także sztuka (Crouchy, Galai i Mark, 2001). Jest to związane z wszechobecnością ryzyka, trudnościami w identyfikacji jego źródeł, a także problemami w jego minimalizacji.

Podejście do zarządzania ryzykiem operacyjnym zmieniało się w miarę upływu czasu. Punktem wyjścia była próba wykorzystania standardowych metod zarządzania, które sprawdzały się w przypadku innych kategorii ryzyka. Jednak, w miarę jak rosła świadomość wagi tego ryzyka i ogromu związanych z nim zagrożeń, stopniowo starano się poszerzać spektrum analiz oraz podejmować próby monitorowania i szacowania tego ryzyka. Doprowadziło to do wypracowania szeregu całkowicie nowych podejść i rozwiązań, które wpisują się w tzw. *zintegrowany system zarządzania ryzykiem* (*Enterprise-wide Risk Management*, ERM). Jest to model wypracowany przez Committee of Sponsoring Organizations of the Treadway Commission (COSO), zgodnie z którym ERM to „proces, zapoczątkowany przez zarząd, kierownictwo lub inny personel, wbudowany w proces ustalania strategii przekrojowo w całej organizacji, mający na celu identyfikację potencjalnych zdarzeń, które mogą wpłynąć na organizację, dążący do zarządzania ryzykiem w ramach określonego apetytu na ryzyko, aby dostarczyć rozsądne zapewnienie osiągnięcia celów organizacji" (COSO, 2004).

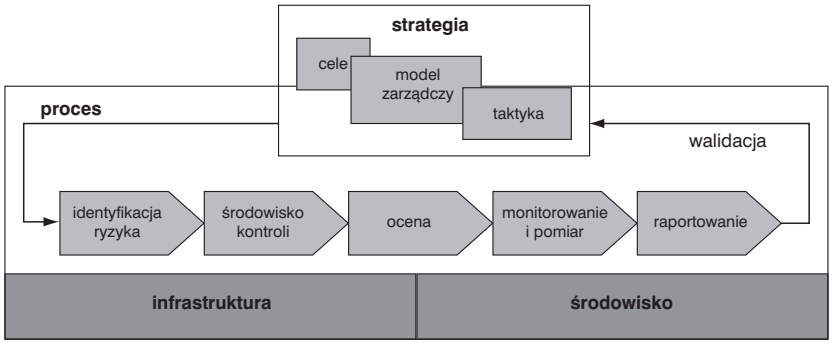
Ramy, na których powinien być zbudowany taki system zarządzania, stanowią cztery filary: *strategia*, która wytycza ogólny zakres działań, *proces zarządzania*, który opisuje działania i decyzje w obrębie wybranej strategii, *infrastruktura* będąca zestawem systemów, danych i narzędzi wykorzystywanych w procesie zarządzania ryzykiem oraz *środowisko*, czyli zestaw norm, wartości i zasad składających się na kulturę organizacji.

Zarysowany w strategii działania proces zarządzania ryzykiem jest zestawem codziennych czynności niezbędnych do skutecznego administrowania

 DOI 10.7172/1644-9584.66.8

nim. Składa się on z kilku etapów. Punktem wyjścia jest *identyfikacja* typów ryzyka, z którymi ma do czynienia instytucja. Ma tu miejsce analiza danych historycznych o stratach, konstrukcja wskaźników ryzyka, badanie potencjalnych źródeł tego ryzyka, identyfikacja zagrożeń płynących z otoczenia, które to czynności mogą zaowocować stworzeniem np. mapy ryzyka dla całej organizacji czy też poszczególnych procesów. W dalszej kolejności następuje określenie narzędzi *kontroli* ryzyka. Określane są zwłaszcza m.in. sposoby analizy danych, metody monitorowania procesów, podziały obowiązków czy dokładne procedury. W kolejnej fazie następuje *ocena* istniejącego systemu oraz identyfikacja jego słabych i mocnych stron oraz szans i zagrożeń z nim związanych. Po serii samoocen, krytyk grupowych przechodzi się do *pomiaru* ekspozycji na ryzyko. Zwykle korzysta się na tym etapie z sześciu typów analiz. Są to: badanie czynników sprawczych (np. wolumen transakcji), wskaźników ryzyka (np. transakcje rozliczone z opóźnieniem), mierników skuteczności działania (np. ilość wykrytych niezgodności), wnioskowanie na podstawie historii strat operacyjnych (np. koszty przegranego procesu sądowego), badanie modeli przyczynowych pozwalających przewidywać zdarzenia operacyjne, a także modeli kapitałowych zmierzających do określenia kapitału niezbędnego na pokrycie strat operacyjnych. Ostatnim ogniwem procesu zarządzania ryzykiem jest *raportowanie* odnośnie do całościowego profilu ryzyka, jak również poszczególnych jego kategorii. Generowane raporty mogą przybierać na przykład formę map ryzyka, wykresów kołowych, słupkowych czy radarowych, analizy scenariuszy lub proponowanych działań zapobiegawczych. Zorganizowany w ten sposób system zarządzania ryzykiem przedstawia rysunek 2.

W procesie zarządzania ryzykiem operacyjnym szczególne ważne jest dokonanie pomiaru i przeprowadzenie analizy źródeł ryzyka operacyjnego.



Rys. 2. Zintegrowany system zarządzania ryzykiem operacyjnym. Źródło: opracowanie na podstawie M. Haubenstock (2003). The operational risk management framework. W: C. Alexander (red.), Operational Risk Regulation, Analysis and Management Prentice Hall.

Pomiar ryzyka operacyjnego uznamy za efektywny tylko wówczas, gdy możliwe będzie określenie nie tylko fluktuacji osiąganych efektów, ale także ich prognozowanie oraz wpływanie na ich poziom. Kluczowe w tym zakresie jest oczywiście jasne zdefiniowanie celów organizacji i wskaźników ryzyka, które będą mierzyły stopień realizacji tych zamierzeń. Problemy, z jakimi przychodzi się zmierzyć, występują nie tylko na etapie pomiaru i prognozowania, ale już nawet w samej fazie identyfikacji przyczyn występowania tego ryzyka. Źródeł tego stanu rzeczy można upatrywać w naturze ryzyka operacyjnego: z rzadka dysponujemy szczegółowymi danymi co do często występujących niewielkich strat, a informacje o rzadko występujących znaczących stratach pojawiają się na tyle nieczęsto, że trudno jest zgromadzić próbę wystarczającą do przeprowadzenia niezbędnych analiz.

Powyższe problemy wskazują na konieczność przygotowania dla ryzyka operacyjnego specjalnych ram koncepcyjnych zestawiających ze sobą miary ryzyka i osiąganego wyniku, opracowania metodologii pomiaru rozmaitych źródeł tego ryzyka oraz metod modelowania, które pozwolą łącznie nie tylko na oszacowanie skali tego ryzyka, ale również określą wytyczne dla odpowiednich działań naprawczych. Absolutnie kluczowa w tym przypadku jest analiza przyczynowo-skutkowa. Bowiem jedynie gruntowna wiedza o źródłach i rezultatach występowania ryzyka daje szansę prognozowania efektów naszych działań, interweniowania i poprzez to kształtowania rzeczywistości wokół nas zgodnie z naszymi oczekiwaniami.

Jeśli przyjrzeć się wynikom badań nad systemami zarządzania ryzykiem operacyjnym, to różny jest stopień zaawansowania jeśli chodzi o rozwój i wykorzystanie poszczególnych narzędzi pomiaru ryzyka w ramach ERM (rysunek 3).

Rys. 3. Zaawansowanie narzędzi systemu zarządzania ryzykiem operacyjnym. Źródło: Deloitte. (2015). Global Risk Management Survey. Pozyskano z: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/ru-global-risk-management-survey-9th-edition.pdf, (15.06.2016).

 DOI 10.7172/1644-9584.66.8

Jak widać, 60% podmiotów przebadanych przez Deloitte uznało w 2015 r. swoje procedury samooszacowania ryzyka operacyjnego za co najmniej bardzo zaawansowane i dobrze rozwinięte. W przypadku pozostałych metod odsetek wskazań był niższy niż 50%, przy czym zdecydowanie najgorzej podmioty radzą sobie z przeprowadzaniem analiz scenariuszowych, korzystaniem z zewnętrznych baz o stratach, kartami wyników oraz śledzeniem zależności przyczynowo-skutkowych.

Stan zaawansowania badań nad łańcuchami powiązań pomiędzy czynnikami ryzyka operacyjnego może budzić niepokój. Wskazano bowiem wcześniej, że zarządzanie ryzykiem operacyjnym nie powinno mieć charakteru statycznego, co jest równoznaczne z ustawicznym uczeniem się i poszukiwaniem właśnie relacji przyczyna–skutek. Powinno ono być procesem ciągłym, realizowanym przez wszystkie komórki organizacji. Kluczem do sukcesu staje się oparcie na działaniach, które będą ciągle oceniane i aktualizowane wraz ze zmianą uwarunkowań wewnętrznych i zewnętrznych. W ten sposób alternatywą dla sztywnych i nieelastycznych klasycznych ram zarządzania staje się koncepcja *zarządzania adaptacyjnego* (*Adaptive Management*, AM). Jest to iteracyjny proces podejmowania decyzji w obliczu niepewności, z zamiarem ograniczenia tej niepewności poprzez monitorowanie systemu. W ten sposób, podejmując decyzję, nie tylko ustalamy konsekwencje wykorzystania zasobów, ale też zbieramy informacje, dzięki którym możliwa będzie poprawa zarządzania w przyszłości. Dzięki temu AM może być wykorzystane do wprowadzania zmian w systemie, jak też do lepszego rozpoznania środowiska podejmowania decyzji zarządczych (Holling, 1967).

Zarządzanie adaptacyjne to forma uczenia się poprzez działanie z uporządkowaną informacją zwrotną. Podejmowanie decyzji opiera się tu na założeniu, że posiadamy umiejętności przewidywania tendencji i ogólnego rozmiaru skutków działań, co powinno być poparte analizami scenariuszy zawierających przewidywania ilościowe. Adekwatność tych scenariuszy będzie uzależniona od dostępności odpowiednich danych i dobrego zrozumienia najważniejszych procesów, na które wpływ ma działanie w sferze zarządzania. Ponieważ wiedza naukowa jest zwykle niekompletna, to wiedzę tę należy uzupełniać wiedzą ekspercką. Osiąganie szczegółowych celów operacyjnych oraz celów strategicznych będzie wynikać z serii następujących po sobie dostosowań organizacji w odpowiedzi na obserwowane reakcje systemu. W procesie AM kluczowe jest rozumowanie przyczynowe, które sprowadza się do założenia relacji przyczynowo-skutkowej między procesami, które zamierzamy uruchomić, a zmianami, które chcemy zaobserwować (jeśli zadziałamy na X, to nastąpi Y).

2.3. Sieć Bayesa a zarządzanie adaptacyjne

Biorąc pod uwagę to, jak ważna dla koncepcji AM jest możliwość śledzenia zależności przyczynowo-skutkowych, szczególnie atrakcyjnym narzędziem analizy wydają się sieci Bayesa (*Bayes Belief Net*, BBN) nazywane

również sieciami przekonań lub też probabilistycznymi modelami graficznymi. Zyskały one ogromną popularność na przełomie poprzedniej dekady (Oniśko, Druzdzel i Wasyluk, 2002) jako bardzo przydatne narzędzie do prezentacji wiedzy w warunkach niepewności, pozwalające na śledzenie zależności przyczynowo-skutkowych przy wykorzystaniu różnych źródeł informacji: zarówno obiektywnych danych obserwowanych, jak i subiektywnych ocen eksperckich. Warto zaznaczyć, że podejście to może być wykorzystane na każdym z sześciu etapów zarządzania adaptacyjnego, które wyróżnił J. Nyberg (tabela 1).

Etap AM	Zastosowanie BBN
Określenie problemu lub szansy	Prezentacja graficzna systemu obejmująca: – pokazanie połączeń między elementami systemu, potencjalnymi działaniami oraz ich efektami – zdefiniowanie mierzalnych wskaźników i efektów adekwatnych do zamierzonych celów – oszacowanie wrażliwości prognozowanych efektów na zmianę nakładów, decyzji, czynników i hipotez
Opracowanie eksperymentu zarządzania	Wybór działań zarządczych, które zostaną porównane w ramach eksperymentu poprzez ocenę wrażliwości, kluczowych zagrożeń, wielkości efektów, kosztów implementacji i monitorowania
Implementacja eksperymentu	Sieć jako punkt odniesienia dla kadry zarządzającej utrzymujący uwagę na kluczowym aspekcie zarządzania
Monitorowanie reakcji systemu	Porównanie wyników monitoringu z prognozowanymi przez sieć reakcjami systemu w celu testowania tego, czy wysiłki monitorowania są wystarczające
Ewaluacja wyników i proces uczenia się	Aktualizacja prawdopodobieństw warunkowych na podstawie danych z monitoringu Modyfikacja sieci pod względem liczby ujętych w nim zmiennych oraz charakteru powiązań między nimi
Dostosowanie przyszłych decyzji	Wykorzystanie udoskonalonego modelu jako wskazówki do podejmowania decyzji zarządczych w przyszłości

Tab. 1. Wykorzystanie BBN w zarządzaniu adaptacyjnym. Źródło: J. Nyberg, B. Marcot i R. Sulyma. (2006). Using Bayesian Belief Networks in Adaptive Management. Canadian Journal of Forest Research, 36(12).

Jak widać, możliwości wykorzystania sieci Bayesa są bardzo rozległe. Warto zatem przyjrzeć się bliżej temu podejściu badawczemu – konstrukcji sieci, sposobom wnioskowania na jej podstawie i możliwym zastosowaniom praktycznym.

 DOI 10.7172/1644-9584.66.8

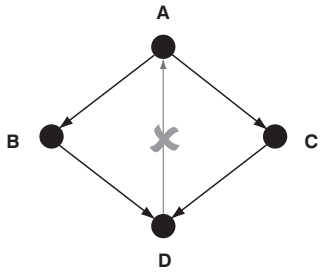
3. Sieć Bayesa – prezentacja podejścia badawczego

3.1. Podstawy teoretyczne

Celem niniejszego opracowania jest przedstawienie wykorzystania sieci Bayesa do wspierania procesu zarządzania ryzykiem operacyjnym, a nie szczegółowe omówienie aspektów teoretycznych tego podejścia badawczego. Dlatego też zostaną przedstawione jedynie kluczowe kwestie z zakresu teoretycznych podstaw sieci bayesowskich, które są niezbędne do zrozumienia prezentowanych w dalszej części przykładów zastosowania BBN. Osoby zainteresowane wnikliwym przestudiowaniem teorii stojącej za tym narzędziem badawczym, pragnące bardziej wnikliwie zbadać możliwości tej metody, a także zapoznać się z innymi przykładami jej wykorzystania odsyłam do literatury. Wśród pozycji zasługujących na uwagę warto wymienić: *Bayesian Networks: An Introduction* (Koski i Noble, 2009), *Modeling and Reasoning with Bayesian Networks* (Darwiche, 2009), *Probabilistic Graphical Models: Principles and Techniques. Adaptive Computation and Machine Learning Series* (Koller i Friedman, 2009) oraz *Risk Assessment and Decision Analysis with Bayesian Networks* (Fenton i Neil, 2012).

Zgodnie z formalną definicją, siecią Bayesa nazywamy skierowany graf acykliczny (*Directed Acyclic Graph*) o wierzchołkach reprezentujących zmienne losowe i łukach określających zależności. Istnienie łuku pomiędzy dwoma wierzchołkami oznacza istnienie bezpośredniej zależności przyczynowo-skutkowej pomiędzy odpowiadającymi im zmiennymi. Siła tej zależności jest określona przez tablice prawdopodobieństw warunkowych[2] (Wąsowski, 2000).

Konstrukcja przykładowej sieci bayesowskiej została przedstawiona na rysunku 4. Zauważmy, że zmienna A nie jest w grafie przez nic poprzedzana i stanowi tzw. *przyczynę podstawową.* Zmienne A i B są zależne bezpośrednio od siebie. Podobnie pary A i C, B i D oraz C i D są wzajemnie zależne. W takich wypadkach mówi się, że zmienne poprzedzające są *rodzicami* zmiennych bezpośrednio od nich zależnych (nazywanych *dziećmi*). Wierzchołek D reprezentuje zmienną, która zależy jednocześnie od B i C, które



Rys. 4. Przykładowa sieć Bayesa. Źródło: opracowanie własne.

to zmienne pozostają brzegowo niezależne, dopóki nie zostanie ustalona wartość B. Jednocześnie zmienne A i D są zależne pośrednio. Zmienna D nie może być z kolei zależna od A, bo wówczas mielibyśmy do czynienia z cyklem, co jest sprzeczne z definicją sieci Bayesa.

Sieć Bayesa składa się tym samym z dwóch podstawowych części: jakościowej – stanowiącej zbiór zmiennych (węzłów grafu) wraz z probabilistycznymi zależnościami pomiędzy nimi, ilościowej – reprezentującej łączny rozkład prawdopodobieństwa dla tych zmiennych (*Joint Probability Distribution*, JPD). Budowa BBN polega zatem na wyznaczeniu jej topologii (struktury) oraz na określeniu jej parametrów, czyli prawdopodobieństw warunkowych dla węzłów, dla których istnieją bezpośrednie zależności. Czynności te określa się mianem *uczenia sieci*. Nauka struktury może przybrać dwie formy: konstrukcja może zostać przygotowana przez eksperta na podstawie posiadanej wiedzy oraz teorii lub też może zostać wygenerowana zdalnie z baz danych przy użyciu szerokiego spektrum algorytmów odtwarzających, jak Chow-Liu, Pearl, SGS, PC, FCI i inne[3]. W tym drugim przypadku mamy do czynienia z uczeniem bez nadzoru i bez wstępnej wiedzy eksperckiej, co jest równoznaczne z przyjęciem założenia, że wszystkie prawidłowe struktury sieci są jednakowo prawdopodobne. Z kolei uczenie parametrów sprowadza się głównie do zliczania liczby rekordów dla różnych warunków kombinacji stanów parametryzowanego wierzchołka i jego poprzedników. Parametry są zwykle wyznaczane na podstawie algorytmu maksymalizacji oczekiwań (*Expectation Maximization Algorithm*, EM) polegający na określeniu lokalnie optymalnego estymatora największej wiarygodności parametrów.

Korzystając z podstawowej zależności (zwanej regułą Bayesa), że prawdopodobieństwo koniunkcji (łącznego zajścia) dwóch zdarzeń jest równe iloczynowi prawdopodobieństwa jednego z tych zdarzeń i prawdopodobieństwa warunkowego drugiego zdarzenia, pod warunkiem że pierwsze zaszło zgodnie ze wzorem (MacKay, 2005):

$$P(A,B) = P(A \mid B) \cdot P(B) = P(B \mid A) \cdot P(A), \tag{1}$$

gdzie:
$P(A)$ – prawdopodobieństwo zdarzenia A,
$P(B)$ – prawdopodobieństwo zdarzenia B,
$P(A,B)$ – prawdopodobieństwo koniunkcji zdarzeń,
$P(A \mid B)$ – prawdopodobieństwo zdarzenia A pod warunkiem B,
$P(B \mid A)$ – prawdopodobieństwo zdarzenia B pod warunkiem A

możliwe jest określenie prawdopodobieństwa wystąpienia określonego wartościowania wszystkich zmiennych sieci (określonej kombinacji stanów), znając jedynie lokalne prawdopodobieństwa warunkowe. Prawdopodobieństwo koniunkcji *n* zdarzeń jest bowiem równe iloczynowi prawdopodobieństwa dowolnego z tych zdarzeń i prawdopodobieństwa warunkowego każdego

 DOI 10.7172/1644-9584.66.8

z pozostałych zdarzeń obliczonego pod warunkiem, że zaszły wszystkie poprzednie zdarzenia. Zależność tę można przedstawić jako (Krysicki i in., 2002):

$$P(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid \Pi(X_i)), \tag{2}$$

gdzie:
$P(X_1, X_2, \ldots, X_n)$ – rozkład prawdopodobieństwa zmiennych danej sieci,
$\Pi(X_i)$ – zbiór rodziców danego wierzchołka X_i w grafie.

Dla przytoczonej sieci Bayesa mamy np.

$$P(A, B, C, D) = P(A) \cdot P(B \mid A) \cdot P(C \mid A, B) \cdot P(D \mid A, B, C) = \\ = P(A) \cdot P(B \mid A) \cdot P(C \mid B) \cdot P(D \mid B, C)$$

Przyjrzyjmy się teraz, jak można wykorzystać sieci Bayesa do analizy zależności przyczynowo-skutkowych.

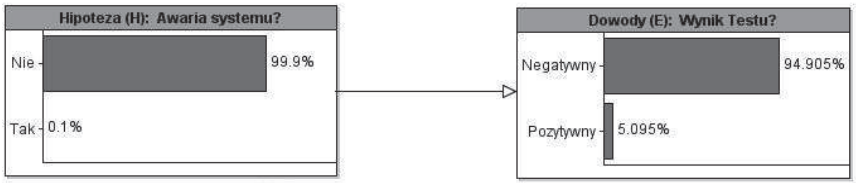
3.2. Wnioskowanie na podstawie sieci Bayesa

Dzięki wykorzystaniu w sieci reguły Bayesa możliwe jest reprodukowanie w przód i w tył prawdopodobieństw dla każdego węzła sieci. Ujawnia się w ten sposób podstawowa zaleta sieci Bayesa, a mianowicie to, że umożliwiają one przeprowadzanie dwóch rodzajów rozumowania: wnioskowania diagnostycznego *bottom-up* (od efektów do przyczyn) oraz analizy przyczynowej *top-down* (od przyczyn do skutków). Warto przy tym wspomnieć, że wśród innych walorów tej metody można wymienić klarowność, elastyczność, dopuszczalność zastosowania w przypadku niepełnych danych, możliwość wykorzystania różnych źródeł informacji: danych twardych i eksperckich. Konsekwencją tego jest oczywiście subiektywizm uzyskanego modelu. Dlatego też nie może być mowy o jedynym właściwym łańcuchu przyczynowo-skutkowym, a sieć Bayesa powinna być traktowana tylko i wyłącznie jako indywidualny i arbitralny pogląd badacza na zależności występujące w ramach analizowanego zjawiska (por. Infosys Case Study lub Alexander, 2003). Może się bowiem zdarzyć, że ten sam proces zostanie opisany za pomocą różnych BBN nie tylko akcentujących inne aspekty zagadnienia, ale też odzwierciedlając tym samym odmienne poglądy badaczy na otaczającą ich rzeczywistość.

Poniżej zaprezentowano możliwości wyciągania wniosków na podstawie przykładowych sieci.

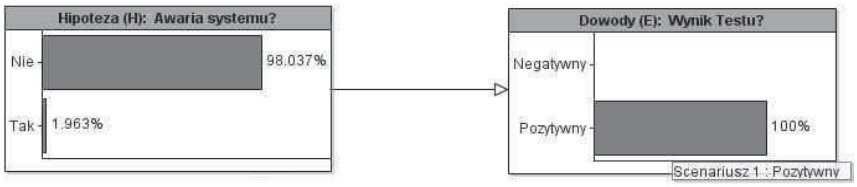
Przykład 1. Analiza prawdopodobieństwa awarii systemu teleinformatycznego banku. Załóżmy, że chcemy ocenić prawdopodobieństwo tego, że system teleinformatyczny banku będzie miał awarię (hipoteza – *Hipothesis*, H) jeśli możemy obserwować wyniki pewnego testu diagnostycznego tego

systemu (dowody – *Evidence*, E)[4]. Załóżmy przy tym, że system zawodzi średnio raz na 1000 razy. Wówczas prawdopodobieństwo awarii systemu wynosi $P(H) = 0{,}001$, a prawdopodobieństwo tego, że system będzie działał bez zarzutu, wynosi $P(notH) = 0{,}999$. Załóżmy również, że test systemu z prawdopodobieństwem 100% wyklucza jego awarię (*„no false negatives”*), ale w 5% przypadków daje wynik pozytywny (wskazujący na zbliżającą się awarię), mimo że do awarii nie dojdzie (5% *„false positives”*). Oznacza to, że prawdopodobieństwo tego, że system ulegnie awarii, gdy test dał wynik pozytywny, wynosi $P(E|H) = 1$, a prawdopodobieństwo tego, że system będzie działał bez zarzutu, gdy test dał wynik pozytywny, wynosi $P(E|notH) = 1$. Sytuację tę możemy przedstawić za pomocą schematu sieci (rysunek 5).



Rys. 5. Prognozowanie awarii systemu. Źródło: opracowanie własne w programie AgenaRisk.

Na podstawie tak skonstruowanej sieci możemy powiedzieć, że nie znając kondycji systemu, prawdopodobieństwo otrzymania pozytywnego wyniku testu wynosi 5,1%. A co się stanie, jeśli wiemy, że test systemu dał wynik pozytywny? Jakie jest prawdopodobieństwo tego, że system rzeczywiście ulegnie awarii? Możemy to sprawdzić, wprowadzając do sieci uzyskaną informację „wynik testu jest pozytywny” i sprawdzając, jak to zmieni prawdopodobieństwo w węźle H. Proces ten nosi nazwę propagacji wstecznej i można go zobrazować jak na rysunku 6.



Rys. 6. Wprowadzanie obserwacji do sieci. Źródło: opracowanie własne w programie AgenaRisk.

Widać, że jeśli test dał wynik pozytywny, to jest mniej niż 2% szans na to, że system faktycznie ulegnie awarii. Ten sam wynik uzyskamy, wyliczając to prawdopodobieństwo z reguły Bayesa:

 DOI 10.7172/1644-9584.66.8

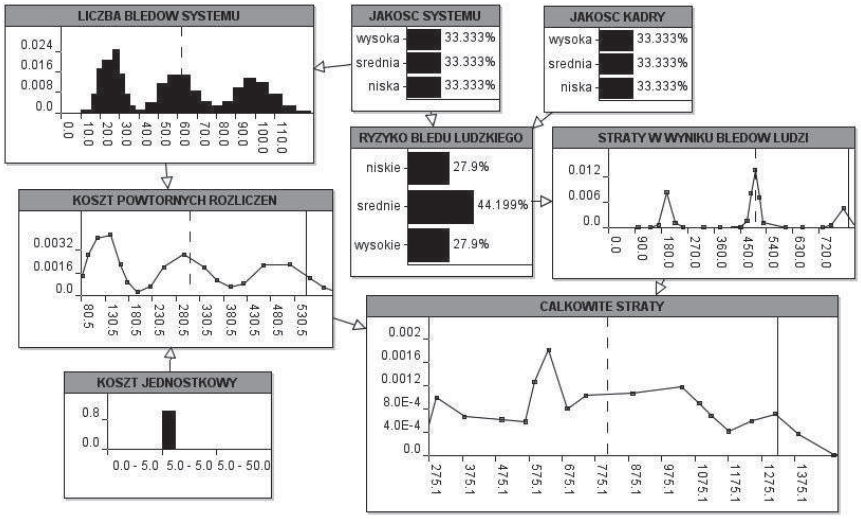
$$P(H|E) = \frac{P(E|H) \cdot P(H)}{P(E|H) \cdot P(H) + P(E|notH) \cdot P(notH)} =$$

$$= \frac{1 \cdot 0{,}001}{1 \cdot 0{,}001 + 0{,}5 \cdot 0{,}999} = 0{,}01963.$$

Sieć Bayesa okazała się w tym przypadku sposobem rewizji naszych przekonań na podstawie napływających informacji. Znajomość wyniku testu sprawiła, że prawdopodobieństwo awarii systemu wzrosło z 0,001 do 0,01963.

Przedstawiony przykład stanowi ilustrację prowadzenia z wykorzystaniem sieci Bayesa prostej analizy dla zmiennych binarnych. Kolejny przykład pokaże wykorzystanie nieco bardziej złożonej sieci do analizy czynników materializacji ryzyka operacyjnego w instytucji finansowej. Prezentowana sieć jest ogromnym uproszczeniem rzeczywistości, ale nawet w takiej postaci pozwala na wskazanie ogromnych możliwości tego narzędzia. Należy zaznaczyć, że faktycznie wykorzystywane sieci mają przeważnie od kilkuset do kilku tysięcy węzłów.

Przykład 2. Analiza strat operacyjnych będących konsekwencją wadliwego systemu. Załóżmy w dużym uproszczeniu, że ryzyko tego, że któryś z pracowników popełni błąd, wprowadzając dane do systemu teleinformatycznego, zależy od tego, jaka jest jakość naszej kadry (a ta może być wysoka, średnia i niska) oraz jaka jest jakość naszego systemu, który takie błędy powinien wykrywać (ta również może być wysoka, średnia i niska). Oczywiście im lepszej jakości kadra/system, tym ryzyko błędu ludzkiego jest mniejsze (niskie, średnie, wysokie), przy czym to pracownik jest sprawcą zdarzenia, a zatem można założyć, że wpływ jakości kadry na ryzyko błędu jest silniejszy niż jakości systemu (powiedzmy trzykrotnie silniejszy). Wartość strat wynikających z błędów ludzkich będzie bez wątpienia zależała od tego, jakie jest ryzyko błędu. Im to ryzyko wyższe, tym wyższych strat należy się spodziewać z tego tytułu (przyjęto, że straty generowane są zgodnie z rozkładem normalnym o średniej tym wyższej, im wyższe ryzyko błędu). Załóżmy jednocześnie, że zdarzają się usterki systemu, które powodują, iż niektóre transakcje zostają nieprawidłowo zaksięgowane, przy czym im wyższa jakość systemu, tym błędnych rozliczeń mniej (założono, że błędy pojawiają się zgodnie z rozkładem Poissona o średniej tym wyższej, im niższa jakość systemu). Każdą z takich błędnie rozliczonych transakcji należy sprawdzić i skorygować księgowanie, co jest związane z poniesieniem określonego kosztu (będącego iloczynem liczby zaobserwowanych błędów oraz jednostkowego kosztu). W konsekwencji łączne straty wynikające z jakości naszego systemu są sumą strat związanych z błędami pracowników oraz kosztem powtórnych rozliczeń. Zależności te zaprezentowano na schemacie (rysunek 7).



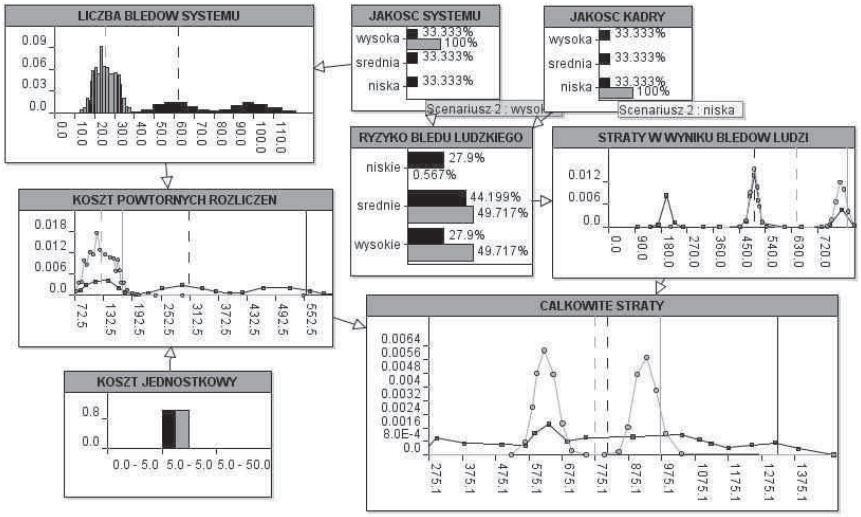
Rys. 7. Analiza strat będących konsekwencją wadliwego systemu – scenariusz 1. Źródło: opracowanie własne w programie AgenaRisk.

Schemat pokazuje, że jeśli nie dysponujemy żadną wiedzą na temat ani jakości kadry, ani jakości systemu (prawdopodobieństwo każdego ze stanów jest identyczne i wynosi 33,33%), to najbardziej prawdopodobny poziom ryzyka błędu jest średni. Wówczas oczekiwana strata w wyniku błędów ludzkich osiąga poziom około 500 jednostek (pionowa linia przerywana), a z prawdopodobieństwem 95% straty nie przekroczą poziomu 822 jednostek (pionowa linia ciągła). Oczekiwany koszt powtórnych rozliczeń będzie wynosił około 310 jednostek, a z prawdopodobieństwem 95% nie przekroczy 556 jednostek. W efekcie oczekiwany poziom strat będących konsekwencją wadliwego systemu to 812 jednostek. Istnieje ponadto 5% szans, że łączne straty przekroczą 1323 jednostki.

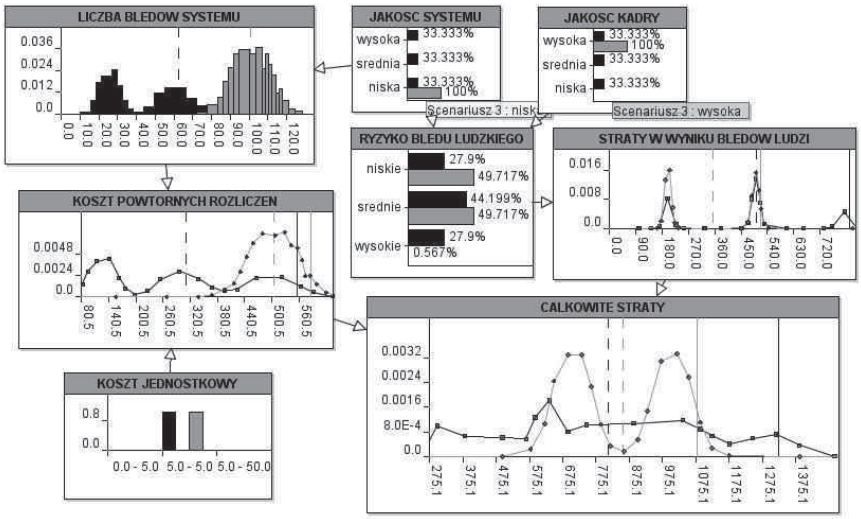
Dokonajmy teraz klasycznej *analizy scenariuszowej od przyczyn do skutków*. Załóżmy, że bank zastanawia się, co powinno być dla niego priorytetem: inwestowanie w system teleinformatyczny czy w szkolenia kadry. Rozważmy zatem dwa scenariusze. W jednym jakość kadry będzie niska, a jakość systemu wysoka (scenariusz 2), a w kolejnym jakość kadry będzie wysoka, a jakość systemu niska (scenariusz 3). Rezultaty przedstawiają rysunki 8 oraz 9.

W scenariuszu 2, gdy jakość kadry jest niska, nawet wysoka jakość systemu nie jest dla nas zabezpieczeniem przed ryzykiem błędu ludzkiego. Nie ma właściwie szans na to, że ryzyko to będzie niskie, równie prawdopodobne będzie to, że będzie ono średnie lub wysokie. Oczekiwane straty z tytułu błędów pracowników osiągną wówczas poziom 647 jednostek. Wysoka jakość

 DOI 10.7172/1644-9584.66.8



Rys. 8. Analiza od przyczyn do skutków – scenariusz 2. Źródło: opracowanie własne w programie AgenaRisk.



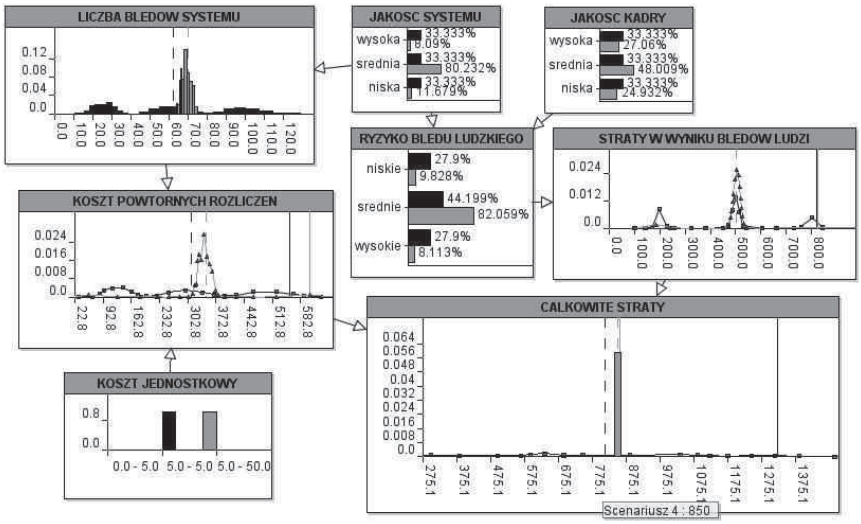
Rys. 9. Analiza od przyczyn do skutków – scenariusz 3. Źródło: opracowanie własne w programie AgenaRisk.

systemu zmniejszy nam jednak liczbę błędnie rozliczonych transakcji. Średni koszt powtórnych rozliczeń spadnie znacząco – do poziomu 127 jednostek, powodując, że łączne oczekiwane straty operacyjne osiągną poziom 774 jednostki, a z prawdopodobieństwem 95% nie przekroczą poziomu 970 jednostek.

Tymczasem w scenariuszu 3, gdy jakość systemu jest niska, a jakość kadry wysoka, wyraźnie zmniejsza się ryzyko błędu ludzkiego, które w tym momencie będzie z dużym prawdopodobieństwem albo niskie, albo średnie. Powoduje to, że zmniejszają się istotnie oczekiwane straty z tego tytułu – do poziomu 352 jednostek. Niestety jednak niska jakość systemu przekłada się na wyższą oczekiwaną liczbę błędnie rozliczonych transakcji, sięgającą teraz 504. W rezultacie całkowite straty wynikające z analizowanych czynników ryzyka operacyjnego z prawdopodobieństwem 95% nie przekroczą poziomu około 1077 jednostek.

Widać zatem, że w analizowanym przykładzie wysoka jakość kadry nie jest w stanie zrekompensować bankowi negatywnych konsekwencji posiadania niskiej jakości systemu teleinformatycznego. I jeśli rzeczywiście bank musi dokonać wyboru, czy inwestować w system czy w kadrę, to powinien zdecydować się na rozwijanie swojego systemu.

W ostatnim kroku dokonajmy *analizy od skutków do przyczyn*. Załóżmy, iż wiemy dokładnie, że w naszej organizacji całkowite straty wynikające z wadliwego systemu osiągnęły poziom 850 jednostek. Sprawdźmy, jakie jest najbardziej prawdopodobne wytłumaczenie tego stanu. Przedstawia to rysunek 10.



Rys. 10. Analiza od skutków do przyczyn – scenariusz 4. Źródło: opracowanie własne w programie AgenaRisk.

 DOI 10.7172/1644-9584.66.8

W tej sytuacji okazuje się, że taki poziom strat operacyjnych najprawdopodobniej wynika ze średniej jakości kadry (prawdopodobieństwo 48%) oraz średniej jakości systemu (prawdopodobieństwo 80%). Oczekiwane straty wynikające z błędów ludzkich sięgają wówczas 500 jednostek, a oczekiwany koszt powtórnych rozliczeń to kwota rzędu 348 jednostek.

Po prześledzeniu przykładowej, bardzo prostej sieci Bayesa warto przyjrzeć się, jaki może być zakres wykorzystania tego narzędzia w procesie zarządzania ryzykiem operacyjnym.

3.3. Zakres wykorzystania sieci przekonań

Wykorzystanie sieci przekonań jest szczególnie interesujące w tych obszarach, gdzie mamy do czynienia z ograniczonym dostępem do danych. Ponieważ BBN nie bazuje jedynie na danych historycznych, to może być z powodzeniem stosowana nawet wówczas, gdy przeszłość nie jest dobrym wyznacznikiem przyszłości, gdy brakuje nam informacji o zdarzeniach bardzo rzadkich lub katastroficznych, a także wówczas gdy chcemy włączyć do analizy dane o charakterze jakościowym czy eksperckim.

Niewątpliwą zaletą sieci Bayesa jest jej elastyczność sprawiająca, że może być ona stosowana do analizy szerokiego spektrum typów zdarzeń. Przegląd zastosowań sieci Bayesa znajdziemy w opracowaniu M. Neil i N. Fenton (2007). W swojej pracy pt. *The Use of Bayes and Causal Modelling in Decision Making, Uncertainty and Risk* wskazują oni na najbardziej popularne zastosowanie BBN w usługach finansowych – kalkulacja i alokacja kapitału na pokrycie strat spójna ze strategią firmy oraz apetytem na ryzyko, biorąca pod uwagę czynniki ryzyka i kontroli (Neil i Fenton, 2011).

Według B. Younga (2000) BBN dobrze sprawdzają się w następujących zastosowaniach w sektorze finansowym:

– monitorowaniu ryzyka w odniesieniu do kluczowych czynników sukcesu podmiotu;
– procesie alokowania kapitału, gdzie sieci przekonań pozwalają modelować zarówno częstotliwość, jak i dotkliwość strat jako funkcje kluczowych przyczyn ryzyka (*key risk drivers*, KRDs); w ten sposób zarządzanie i kontrola ryzyka operacyjnego może być powiązana z kapitałem ekonomicznym czy regulacyjnym;
– walidacji kwestionariuszy samooceny ryzyka (*self-assessment reviews*) poprzez zapewnienie niezależnie uzyskanych ocen.

C. Alexander (2003) dodaje z kolei, że sieci mogą być przydatne także w:

– przygotowaniu analizy scenariuszy zintegrowanej z systemem budżetowania;
– ustaleniu awaryjnych poziomów wskaźników ryzyka sygnalizujących konieczność podjęcia działań zaradczych;
– określeniu najskuteczniejszych sposobów kontroli ryzyka dzięki symulacjom i badaniu wrażliwości uzyskiwanych efektów na zmiany parametrów ryzyka;
– analizie kosztów–korzyści podejmowanych działań zarządczych.

Warto także wspomnieć o pracach, które wykorzystywały BBN do celów aktywnego zarządzania ukierunkowanego na identyfikację kluczowych czynników ryzyka wraz z analizą wrażliwości systemu na zmianę ich wartości/jakości. I tak, praca J. Kinga koncentruje się na przykład na wnioskowaniu dotyczącym ryzyka rozliczeniowego (King, 2001). Opracowanie C. Alexander skupia się z kolei na ryzyku błędów przy rozliczaniu transakcji swapowych (Alexander, 2003). Studium Infosys bada natomiast przyczyny i konsekwencje przeoczenia przez inwestora ważnego raportu dotyczącego spółki, której papiery wartościowe posiada (Infosys Case Study). I w końcu, M. Neil poddaje analizie utratę reputacji przez bank na skutek niepoprawnego rozliczenia transakcji klienta (Neil, 2000). Z kolei w wystąpieniu podczas konferencji N. Fenton prezentował wyższość sieci Bayesa nad tradycyjnymi miarami ryzyka na przykładzie analizy defektów systemu (Fenton, 2006).

4. Wnioski

W artykule starano się pokazać, jak skutecznym narzędziem wspomagającym zarządzanie ryzykiem operacyjnym w banku może być sieć Bayesa. Na koniec warto podsumować główne zalety i wady tego podejścia. Wśród zalet prezentowanej metody najczęściej wymienia się następujące elementy:

- Sieć to klarowna i oszczędna reprezentacja łącznego rozkładu prawdopodobieństwa.
- BBN to przejrzysta reprezentacja wiedzy o zależnościach przyczynowo-skutkowych.
- Wnioskowanie od przyczyn do skutków i od skutków do przyczyn czyni z sieci skuteczne narzędzie zarządzania.
- Możliwość wykorzystania danych ilościowych, jak i jakościowych danych eksperckich.
- Możliwość zwiększenia wiarygodności modelu poprzez uwzględnienie punktów widzenia różnych grup interesu w modelach uwzględniających wiele poziomów organizacji.
- Możliwość ewaluacji analizowanego systemu i wskazania zmiennych mających największy wpływ na osiąganie celów organizacji przy jednoczesnym określeniu optymalnej alokacji zasobów.
- Możliwość sformułowania wskazówek dotyczących potencjalnych strategii rozwoju z uwzględnieniem kosztów niezbędnych do wdrożenia tych strategii.
- Możliwość wykorzystania analizy wrażliwości do określenia najbardziej skutecznych sposobów rozwiązywania problemów.
- Zapewnia wnioski, które mogą być z powodzeniem analizowane i interpretowane przez menedżerów, którzy nie posiadają wiedzy dotyczącej aparatu matematycznego.
- Sieć Bayesa zapewnia, że każdy czynnik ryzyka jest ujęty w swoim indywidualnym kontekście, dzięki czemu możliwe jest odejście od tradycyjnego

 DOI 10.7172/1644-9584.66.8

traktowania ryzyka jako iloczynu prawdopodobieństwa oraz wielkości straty.
– Choć Sieć Bayesa nie oferuje uniwersalnej miary ryzyka, to daje możliwość obserwowania tego, co najprawdopodobniej się stanie, biorąc pod uwagę aktualny stan wiedzy. Jest szansą na dokonanie priorytetyzacji czynników ryzyka poprzez analizę rozmaitych scenariuszy rozwoju zdarzeń.

Sceptycy tej metody wskazują z kolei takie jej negatywne aspekty, jak:
– Subiektywizm modelu.
– Problemy w identyfikowaniu zależności przyczynowo-skutkowych – czy aby na pewno A wpływa na B, a nie B na A, a może zarówno A, jak i B są konsekwencjami C?
– Trudności w szacowaniu prawdopodobieństw w poszczególnych węzłach sieci.
– Ryzyko zbytniego uproszczenia rzeczywistości.
– Konieczność skupienia się tylko na tych zależnościach, które są kluczowe dla wyjaśnienia zjawiska, ale tak by model nie stał się zbyt szczegółowy, a tym samym mało czytelny i trudny w interpretacji.

Wymienione wady – jakkolwiek istotne – nie dyskredytują zdaniem autorki sieci Bayesa jako narzędzia wspomagającego zarządzanie ryzykiem operacyjnym. Nie sposób przecenić bowiem możliwości zanalizowania zależności przyczynowo-skutkowych między czynnikami ryzyka, których właściwe rozpoznanie warunkuje osiągnięcie przez bank sukcesu rynkowego.

Przypisy

1 Nowa Umowa Kapitałowa (Basel II) to opracowana przez Komitet Bazylejski zrewidowana wersja powstałej w 1988 roku Umowy Kapitałowej dotyczącej oceny adekwatności kapitałowej instytucji finansowych.

2 Prawdopodobieństwo bezwarunkowe (a priori) określa liczbowo szansę wystąpienia jakiegoś zjawiska, gdy nie są znane żadne okoliczności towarzyszące temu zjawisku. Z kolei prawdopodobieństwo warunkowe (a posteriori) to prawdopodobieństwo zdarzenia w sytuacji, gdy posiadamy jakąś wiedzę o innych, być może zależnych zdarzeniach (opracowanie na podstawie: Paluszyński, niedatowane).

3 Przegląd algorytmów służących generacji podstawowej struktury BBN znaleźć można w: Wąsowski, 2000.

4 Przykład opracowany na podstawie: Fenton i Neil, 2011.

Bibliografia

Alexander, C. (2003). Managing operational risks with Bayesian networks. W: C. Alexander (red.), *Operational risk. Regulation, Analysis and Management*, Prentice Hall.

AON. (2015). *Global Risk Management Survey*. Pozyskano z: http://www.aon.com/2015GlobalRisk (15.06.2016).

COSO. (2004). *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa. Streszczenie dla kierownictwa.* Pozyskano z: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Polish.pdf (10.06.2016).

Crouchy, M., Galai, D. i Mark, R. (2001). *Risk Management*. McGraw-Hill.
Da Costa Lewis, N. (2004). *Operational Risk with Excel and VBA. Applied Statistical Methods for Risk Management*. Wiley.
Darwiche, A. (2009). *Modeling and Reasoning with Bayesian Networks*. Cambridge: Cambridge University Press.
Deloitte. (2015). *Global Risk Management Survey*. Pozyskano z: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/ru-global-risk-management-survey-9th-edition.pdf, (15.06.2016).
Fenton, N. i Neil, M. (2012). *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press.
Fenton, N. (2006). *New Directions for Software Metrics*. Referat wygłoszony na: CIO Symposium on Software Best Practices.
Haubenstock, M. (2003). *The operational risk management framework*. W: C. Alexander (red.), *Operational Risk. Regulation, Analysis and Management*. Prentice Hall.
Holling, C.S. (red.). (1978). *Adaptive Environmental Assessment and Management*. Wiley.
Infosys Case Study (niedatowane). *Operational Risk and Probabilistic Networks. An Application to Corporate Actions Processing*. Pozyskano z: http://www.hugin.com/cases/Finance/Infosys/oprisk.article (10.02.2010).
King, J. (2001). *Operational Risk. Measurement and Modelling*. Wiley.
Koller, D. i Friedman, N. (2009). *Probabilistic Graphical Models: Principles and Techniques. Adaptive Computation and Machine Learning Series*. The MIT Press.
Komisja Nadzoru Bankowego. (2004). *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*. Warszawa: Komisja Nadzoru Bankowego.
Koski, T. i Noble, J. (2009). *Bayesian Networks: An Introduction*. Wiley.
Krysicki, W., Bartos, J., Dyczka, W., Królikowska, K. i Wasilewski, M. (2002). *Rachunek prawdopodobieństwa i statystyka matematyczna w zadaniach, cz. I*. Warszawa: Wydawnictwo Naukowe PWN.
MacKay, D. (2005). *Information Theory, Inference, and Learning Algorithms*. Cambridge: Cambridge University Press.
Neil, M. (2000). *Bayesian Belief Networks: Operational Risk and the Turnbull Guidelines*. Referat wygłoszony na: Operational Risk Research Forum.
Neil, M. i Fenton, N. (2007). *Managing Risk in the Modern World: Bayesian Networks and the Applications*. London: London Mathematical Society.
Neil, M. i Fenton, N. (2011). The Use of Bayes and Causal Modelling in decision Making, Uncertainty and Risk. *CEPIS Upgrade*, *12*(5) 10–21.
Nyberg, J., Marcot, B. i Sulyma, R. (2006). Using Bayesian Belief Networks in Adaptive Management. *Canadian Journal of Forest Research*, *36*(12).
Oniśko, A., Druzdzel, M.J. i Wasyluk, H. (2002). Uczenie parametrów sieci bayesowskich z danych z wykorzystaniem bramek Noisy-OR. W: Z. Bubnicki, O. Hryniewicz, R. Kulikowski (red.), *Badania operacyjne i systemowe wobec wyzwań XXI wieku*, *Problemy współczesnej nauki. Teoria i zastosowania*. Akademicka Oficyna Wydawnicza EXIT.
Paluszyński, W. (niedatowane). *Przegląd pojęć z prawdopodobieństwa*. Pozyskano z: http://sequoia.ict.pwr.wroc.pl/~witold/aiuwr/beliefnet_s.pdf (13.07.2011).
Vaughan, E. i Vaughan, T. (2003). *Fundamentals of Risk and Insurance*. Wiley.
Wąsowski, A. (2000). *Zdalna generacja sieci bayesowskich z baz danych*. Niepublikowana praca dyplomowa. Politechnika Warszawska, Wydział Matematyki i Nauk Informacyjnych.
Young, B.J. (2000). *Bayesian Belief Networks: A Powerful New Tool with Which to Analyse and Quantify Operational Risk*. Pozyskano z: http://www.orrf.org/papers/bayesian_belief_networks.pdf (15.08.2006).
Zawadzka, Z. (1998). Ryzyko bankowe – uwagi ogólne. W: W. Jaworski (red.), *Współczesny bank*. Poltext.

 DOI 10.7172/1644-9584.66.8