Michał WIŚNIEWSKI

EKSPERCKI SYSTEM ZARZĄDZANIA RYZYKIEM OPERACYJNYM RAPORT Z BADAŃ

Streszczenie

W artykule omówiony zostały problemy związane z realizacją procesu zarządzania ryzykiem w organizacjach. Skupiono się na problematyce ryzyka operacyjnego, które dotyka codzienności funkcjonowania każdego przedsiębiorstwa. Jako punkt odniesienia przyjęto proces zarządzania ryzykiem operacyjnym w sektorze bankowym. Wybór ten został podyktowany faktem, że wskazany sektor ma największe doświadczenie w tym zakresie. W artykule omówiono proces zarządzania ryzykiem operacyjnym i wymieniano jego wady. Wskazano, że systemy eksperckie są potencjalnym remedium na wiele z nich. Celem jest prezentacja wyników prac badawczych prowadzonych nad Eksperckim Systemem Zarządzania Ryzykiem Operacyjnym. Zaproponowano modyfikację procesu zarządzania ryzykiem operacyjnym uwzględniającą wykorzystanie opracowywanego systemu oraz przedstawiono proponowany modułowy model tego systemu.

WSTĘP

Ryzyko operacyjne, rozumiane jako ryzyko strat w wyniku niewłaściwego (nieadekwatnego) lub błędnego działania procesu, ludzi i systemów lub wpływu wydarzeń zewnętrznych [22, s. 62], występuje powszechnie, w sposób ciągły i na wszystkich szczeblach zarządzania. W związku z tym musi być w podobny sposób zarządzane – poczynając od rady nadzorczej do pojedynczego stanowiska pracy. Odpowiedzią na tę potrzebę jest adekwatny system zarządzania, wspierany odpowiednimi narzędziami metodycznymi i technologicznymi.

Celem niniejszego artykułu jest prezentacja wyników badań i prac rozwojowych prowadzonych przez Wydział Zarządzania Politechniki Warszawskiej oraz firmę MyIT sp. z o.o. nad Eksperckim Systemem Zarządzania Ryzykiem Operacyjnym (ESZRO).

Specyfika branży i sposób funkcjonowania organizacji wyznacza sposób podejścia oraz metodę klasyfikacji i oceny ryzyka operacyjnego, dlatego na potrzeby projektu konieczne było wybranie branży wzorcowej. Projektowany system wzorowany jest na procesie zarządzania ryzykiem operacyjnym w sektorze bankowym. Ma to uzasadnienie w fakcie, że banki są zobowiązane ustawowo do zarządzania ryzykiem operacyjnym [18], a zatem stanowią interesujący punkt odniesienia. Docelowo system ESZRO będzie mógł być elastycznie dopasowywany do potrzeb i możliwości każdego użytkownika, zainteresowanego zarządzaniem tym ryzykiem.

1. PROCES ZARZĄDZANIA RYZYKIEM OPERACYJNYM W ORGANIZACJI

Jedną z podstawowych determinant efektywnego zarządzania przedsiębiorstwem jest skuteczne zarządzanie ryzykiem. Ryzyko występuje w każdym typie prowadzonej działalności i na każdym szczeblu organizacji. Towarzyszy realizacji każdego procesu biznesowego i jest związane z wpływem stale oddziaływujących oraz dynamicznie zmiennych czynników wewnętrznych i zewnętrznych.

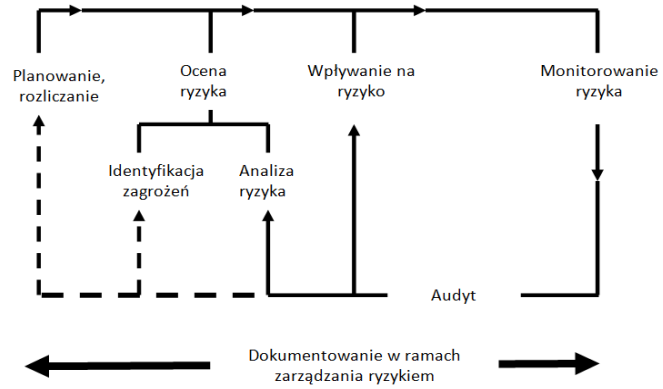
Zarządzanie ryzykiem koncentruje się na zwiększeniu prawdopodobieństwa osiągnięcia przez organizację zamierzonych celów. Zdefiniowanie celów umożliwia identyfikację tych rodzajów ryzyka, które mogą zagrozić ich realizacji. Stąd proces zarządzania ryzykiem obejmuje wdrożenie odpowiednio dopasowanych i operacyjnie efektywnych działań, zmniejszających poziom zidentyfikowanego ryzyka do poziomu akceptowalnego. W celu zapewnienia skuteczności tego procesu konieczne jest zachowanie jego ciągłości i spójności, co wiąże się z wprowadzeniem w organizacji polityki zarządzania ryzykiem [6].

Jedną z podstawowych kategorii ryzyka, dotyczącą każdej organizacji i mającą zasadniczy wpływ na efektywność jej funkcjonowania, jest ryzyko operacyjne. Decyduje ono o tym, na ile wewnętrzne procesy organizacyjne są skuteczne i odporne na zakłócenia wewnętrzne i zewnętrzne, aby organizacja bez przeszkód mogła realizować swoje cele gospodarcze [12, s. 42-45].

Proces zarządzania ryzykiem operacyjnym opiera się na triadzie Analiza – Prewencja – Terapia [22, s. 55-57]. Zapoczątkowuje go identyfikacja ryzyka oraz ocena zagrożenia tym ryzykiem. Na podstawie wyników analizy przygotowywane są działania prewencyjne, adekwatne do stopnia zagrożenia i przeciwdziałające spełnieniu się ryzyka.

Działania prewencyjne polegają na tworzeniu rezerw finansowych, organizacyjnych i technicznych oraz wdrażaniu zapobiegających procedur działania [21]. Rezerwy są dodatkowym obciążeniem dla organizacji, ale ich brak stanowi poważne zagrożenie dla jej sprawnego funkcjonowania. Dlatego tak istotna jest precyzyjna identyfikacja ryzyka oraz realna ocena stopnia zagrożenia nim na poziomie analizy ryzyka.

Na wypadek, kiedy uniknięcie skutków ryzyka nie jest możliwe, wdrażane są procedury niwelujące powstałe zakłócenia i służące podtrzymaniu ciągłości działania organizacji. Poprawna realizacja tych procedur jest warunkowana rezerwami zgromadzonymi na poziomie prewencji.



Rys. 1. *Cykl zarządzania ryzykiem operacyjnym w organizacji (źródło: [2])*

Kluczowym etapem procesu zarządzania ryzykiem operacyjnym jest etap analizy ryzyka, obejmujący następujące elementy [13]:
- identyfikację i wycenę wartości zasobów chronionych,
- identyfikację istniejących zagrożeń oraz podatności na te zagrożenia,
- oszacowanie istniejących zagrożeń oraz podatności na nie,
- ocenę ryzyka obejmującą oszacowanie jego wpływu na prowadzoną działalność operacyjną, mierzoną prawdopodobieństwem i częstotliwością spełnienia się ryzyka oraz szacowaną wielkością ponoszonej wtedy straty.

W prowadzonym projekcie ESZRO model procesu analizy ryzyka (rys. 2) został opracowany przy założeniu, że organizacja nie dysponuje systemem informatycznym wspomagającym analizę ryzyka i opiera się wyłącznie na opinii eksperta. Zatem każde zdarzenie związane z ryzykiem operacyjnym, wymaga przeprowadzenia wywiadu i zasięgnięcia porady eksperta. Wywiad ten jest przygotowywany na podstawie opisu zaistniałego zdarzenia, zidentyfikowanej kategorii ryzyka oraz pytań uszczegóławiających, prowadzących do ustalenia przyczyn oraz oceny skutków tego zjawiska.

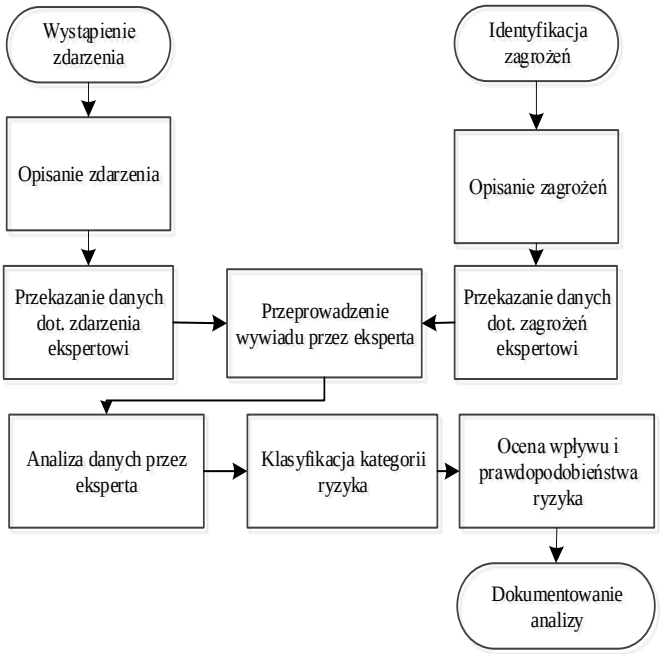
Na podstawie uzyskanych informacji ekspert przeprowadza analizę zdarzenia. Wynikiem analizy jest subiektywna klasyfikacja ryzyka oraz przydzielenie zaistniałego zdarzenia do już istniejącej lub nowo wydzielonej kategorii ryzyka operacyjnego. Na podstawie wartości i częstości występujących incydentów ustalana jest skala wpływu ryzyka oraz prawdopodobieństwo jego wystąpienia. Cały przebieg procesu analizy jest dokumentowany, w celu ponownego wykorzystania podczas oceny kolejnego incydentu.

W ten sposób sukcesywnie budowana jest i rozwijana wiedza o pewnej kategorii ryzyka, co może mieć postać drzewa klasyfikacji ryzyka oraz oceny wpływu i prawdopodobieństwa jego wystąpienia w organizacji. Dane te, uzupełnione rejestracją występujących incydentów, umożliwiają budowę mapy ryzyka [14], która w przystępny dla decydenta, graficzny sposób, prezentuje i charakteryzuje obszary zagrożenia, wspomagając właściwe dobranie rodzaju podejścia do zidentyfikowanej kategorii ryzyka operacyjnego. Możliwe są podejścia: redukcji ryzyka, transferu ryzyka, zaakceptowania ryzyka lub unikania ryzyka [15].

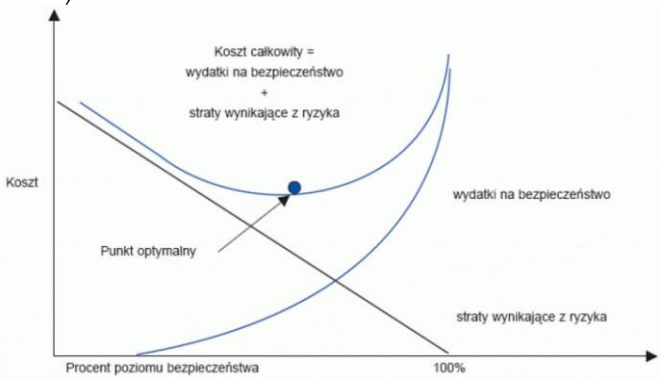
Kluczowym kryterium doboru podejścia w panowaniu nad ryzykiem jest optymalizacja kosztów ponoszonych na zabezpieczenie się przed wystąpieniem oraz usuwaniem skutków już zaistniałych strat w stosunku do rzeczywistej podatności organizacji na zidentyfikowane zagrożenia (Rys. 3). Z kolei właściwa optymalizacja kosztów nie jest możliwa bez prawidłowej klasyfikacji ryzyka, oceny stopnia zagrożenia, podatności oraz monitorowania występujących zdarzeń generujących straty.

Odnosząc się do przedstawionego procesu analizy ryzyka operacyjnego (Rys. 2) należy wskazać następujące jego wady: (1) proces nie jest zautomatyzowany, czego konsekwencją jest jego czasochłonność, pracochłonność oraz utrudnienia w zakresie zagwarantowania jednakowej jakości, zgodności proceduralnej i powtarzalności, (2) realizacja procesu jest całkowicie uzależniona od opinii eksperta/ekspertów, które są subiektywne i niesformalizowane, co może prowadzić do błędnej klasyfikacji i oceny sytuacji, (3) koszt klasyfikacji i oceny ryzyka jest wysoki, co wynika z konieczności zapewnienia stałego dostępu do eksperta/ekspertów, (4) brak jest ustalonych norm i standardów klasyfikacji ryzyka, co utrudnia porównywalność wpływu ryzyka oraz prawdopodobieństwa jego wystąpienia i może prowadzić do błędnych decyzji prewencyjnych i zapobiegawczych, (5) dokumentowanie procesu jest czasochłonne oraz trudne i związane z niezbędną agregacją gromadzonych danych, co może prowadzić do pomijania i nieuwzględniania istotnych informacji, (6) ograniczone są możliwości prowadzenia pogłębionej analizy zagrożeń oraz zaistniałych w przeszłości strat.

Wobec powyższego uzasadniona jest realizacja systemu informatycznego, który efektywnie wspomoże analizę ryzyka operacyjnego w organizacji.



Rys. 2. *Proces analizy ryzyka w organizacji (źródło: opracowanie własne)*



Rys. 3. *Optymalizacja kosztów zabezpieczeń w odniesieniu do podatności na zagrożenie (źródło: [13])*

2. WPROWADZENIE DO ZAGADNIEŃ SYSTEMÓW EKSPERCKICH

Systemy eksperckie (SE) stanowią gałąź „stosowanej sztucznej inteligencji". Jednym z wyników badań w dziedzinie sztucznej inteligencji jest rozwój technik, które pozwalają na modelowanie informacji na wyższych poziomach abstrakcji. Techniki te są zawarte w językach lub narzędziach, które z kolei umożliwiają budowę programów zbliżonych do ludzkiej logiki w ich działaniu, nazywanych systemami eksperckimi. SE starają się naśladować decyzje eksperta w konkretnej wybranej dziedzinie i potrafią robić to wielokrotnie w powtarzalny i przyjazny dla użytkownika sposób [11, s. 527-546]. Ich funkcjonowanie jest oparte o aplikacje komputerowe, które przechowują informacje w bazach wiedzy i posiadają umiejętności wnioskowania, rozwiązywania problemów i doradztwa w oparciu o zgromadzone w nich zasoby informacyjne [20, s. 547-586].

Początkowo ideą tworzenia SE było zastąpienie człowieka w wykonywanej przez niego pracy w przypadkach, gdzie potrzebna była wiedza ekspercka. Potrzeba implementacji takich systemów

wynikała z faktu posiadania niewielu ekspertów z danej dziedziny, nie radzących sobie ze zbyt dużą liczbą problemów jednocześnie oraz ze względu na zagrożenie utratą tych ekspertów jako pracowników. Wraz z rozwojem sztucznej inteligencji systemy eksperckie zaczęto traktować jako pomoc w podejmowaniu decyzji, dzięki czemu stały się jednym z typów systemów wspomagania decyzji. Aktualnie wyraźnie zaznacza się rozwój SE w kierunku łączenia wielu różnych metod sztucznej inteligencji oraz reprezentacji wiedzy, m.in. takich jak logika rozmyta, ontologia czy analiza języka naturalnego [16]. Zakres stosowania systemów eksperckich jest bardzo szeroki, obejmuje: finanse, przemysł, zarządzanie, naukę, technikę, medycynę, prawo [7, s. 284-298].

Modelowa struktura SE wynika ze sposobu jego funkcjonowania, który polega na wyznaczaniu wniosków i wyników z danych zapisanych w bazie wiedzy [5; 9; 8]. Ciąg kroków, potrzebny do wyznaczania wniosków i wyników, jest syntezowany dynamicznie przez system wnioskujący dla każdej bazy wiedzy, nie zaś programowany w trakcie tworzenia tej bazy [20, s. 547-586].

SE składa się z niezależnych fizycznie, lecz współpracujących ze sobą, następujących elementów: (1) bazy wiedzy przechowującej dane z wybranej dziedziny w postaci faktów (wiedza faktograficzna), reguł (wiedza o wnioskowaniu) oraz meta-wiedzy (wiedza o sposobach rozwiązywania problemów), (2) bazy danych zmiennych pamięci roboczej systemu przechowującej fakty wprowadzone w trakcie interakcyjnego dialogu z użytkownikiem, (3) mechanizmu wnioskowania wyszukującego rozwiązanie postawionego problemu na podstawie zgromadzonej wiedzy, (4) mechanizmu objaśniania tłumaczącego strategię wnioskowania i sposób dojścia do rozwiązania oraz prezentującego szczegółowe dane dotyczące rozwiązania, (5) edytora bazy wiedzy umożliwiającego modyfikację wiedzy zawartej w systemie, a tym samym jego rozbudowę, (6) interfejsu użytkownika umożliwiającego interaktywną komunikację człowieka z systemem.

Zastosowanie SE w tworzonym projekcie jest podyktowane dużą liczbą słabo sformalizowanych zmiennych wpływających na rzeczywistość funkcjonowania organizacji. SE najlepiej nadają się do zastosowania w tych dziedzinach, które są słabo sformalizowane, w których trudno jest sformułować teorie oparte na matematyce lub ścisłe algorytmy działania. Do tej grupy zalicza się zarządzanie ryzykiem operacyjnym. Zastosowanie SE pozwoli na wygenerowanie rozwiązań akceptowalnych przez użytkownika systemu. Możliwe będzie również prześledzenie toku generowania rozwiązania, co sprawi, że rozwiązania proponowane przez system będą zrozumiałe dla menadżerów przedsiębiorstwa.

3. ANALIZA RYZYKA OPERACYJNEGO Z UWZGLĘDNIENIEM SYSTEMU ESZRO

Projektowana automatyzacja procesu analizy ryzyka operacyjnego ma na celu wsparcie działań eksperta, a w dłuższej perspektywie ograniczenie jego udziału w procesie, do oceny nowo zidentyfikowanych zagrożeń. Praca systemu informatycznego, inicjowana przez opinię eksperta, po pewnym czasie będzie się opierała na analizie gromadzonych i przetwarzanych danych, dotyczących rejestrowanych incydentów. System powinien wspierać zarówno rejestrację zaistniałych incydentów, jak i uaktualnianie drzewa kategoryzacji ryzyka. Wstępne oszacowanie wartości wpływu i prawdopodobieństwa wystąpienia ryzyka musi być przeprowadzone przez eksperta. Jednak dzięki rejestracji kolejnych incydentów i powiększaniu się zasobów bazy danych, parametry te będą automatycznie korygowane przez system, co umożliwi obiektywizację oceny zagrożenia i optymalizację działań prewencyjnych i naprawczych.

W projekcie zakłada się przygotowanie SE, ponieważ jego działanie naśladuje i może być w związku z tym alternatywą dla działania eksperta. Na etapie uruchamiania systemu ekspert będzie odpowiedzialny za zdefiniowanie wstępnego drzewa klasyfikacji ryzyka oraz dokonanie jego pierwszej oceny. Dalszą pracę będzie wykonywał inżynier wiedzy [19, s. 213], rejestrujący w systemie kolejne incydenty i generujący raporty dla kierownictwa. W końcu kadra kierownicza będzie korzystała z najbardziej zaawansowanych, doradczo-informacyjnych funkcji systemu podczas podejmowania decyzji w zakresie zarządzania ryzykiem.

Wraz z rozwojem systemu oraz powiększaniem zasobów zgromadzonych danych, rolę eksperta będzie przejmować moduł wnioskujący systemu. Niezbędne jest jednak pozostawienie możliwości zasięgnięcia opinii i wsparcia merytorycznego ze strony eksperta, przykładowo w zakresie reguł rejestrowanych w bazie wiedzy. W tym przypadku naturalnym wydaje się, że ekspert będzie pełnił rolę inżyniera wiedzy w zakresie decyzji merytorycznych. Z czasem inżynier wiedzy będzie mógł zastąpić eksperta przy dodawaniu nowych i korygowaniu istniejących kategorii ryzyka w drzewie klasyfikacyjnym. Będzie również koordynował generowanie i aktualizację raportów dla kadry kierowniczej.

W większości przypadków kadra kierownicza będzie rutynowym odbiorcą raportów i sprawozdań generowanych przez system. Należy jednak przewidzieć możliwość kierowania zapytań do systemu przez menedżera w celu uzyskania porady eksperckiej.

Funkcjonalność systemu ESZRO wynika zarówno ze zdefiniowanych zadań użytkowników, jak i z niedostatków zdiagnozowane-

Tab. 1. *Wymagania funkcjonalne stawiane systemowi źródło: opracowanie własne*

Nazwa	Opis
Klasyfikacja ryzyka	System umożliwi rejestrację nowej kategorii lub klasy ryzyka z uwzględnieniem układu hierarchii pomiędzy nimi. Klasyfikacja ryzyka będzie realizowana ręcznie przez inżyniera wiedzy i akceptowana przez eksperta.
Ocena ryzyka	Inżynier wiedzy, wspomagany merytorycznie przez eksperta, będzie szacował wagę wpływu oraz prawdopodobieństwo wystąpienia ryzyka. Wraz z rozwojem systemu oraz gromadzonych w bazie danych dotyczących zachodzących incydentów, wartości te będą automatycznie sprawdzane i korygowane przez system.
Rejestracja incydentów	Informacje o zdarzeniach będą ręcznie rejestrowane w systemie przez inżyniera wiedzy.
Klasyfikacja incydentów	Każde zdarzenie musi być powiązane z odpowiadającą mu kategorią ryzyka. Przypisanie to będzie wykonywane w trakcie rejestracji zdarzenia przez inżyniera wiedzy. Wraz z rozwojem systemu oraz zasobów bazy danych będzie też podpowiadane przez system na podstawie dotychczasowej historii klasyfikowania zdarzeń.
Szacowanie zagrożeń	Szacowanie przewidywanej straty będzie realizowane przez inżyniera wiedzy, wspieranego merytorycznie przez eksperta. Wraz z rozwojem systemu i przyrostem zasobów w bazie danych będzie również prognozowane przez system na podstawie dotychczasowej historii strat.
Dobór programu prewencyjnego i naprawczego	Po przeprowadzeniu oceny ryzyka i w oparciu o bazę wiedzy, system wygeneruje listę mechanizmów kontrolnych zabezpieczających organizacje przed jego skutkami.
Generowanie raportów, map i wykresów	Wyniki oceny ryzyka, prognozowanych i odniesionych strat oraz sugerowane działania prewencyjno-naprawcze będą dokumentowane w systemie z możliwością ich swobodnej dystrybucji. Raporty generowane w wersji opisowej, tabelarycznej i graficznej zostaną dopasowane do konkretnego odbiorcy. Dla kadry kierowniczej będą tworzone raporty zagregowane.
Komunikacja z użytkownikiem	System będzie wspierał dowolną formę komunikacji z użytkownikiem – przez interfejs użytkownika, pocztę mailową, kokpit menedżerski, portal informacyjny, urządzenia mobilne.

go procesu analizy ryzyka operacyjnego (Tab. 1).

Podstawowa koncepcja funkcjonowania systemu ESZRO zakłada, że dzięki wspomaganej przez eksperta, pogłębionej analizie zdarzeń zachodzących w trakcie prowadzonej przez organizację działalności operacyjnej, możliwe będzie zwiększanie zasobów wiedzy, a w konsekwencji poprawa skuteczności zarządzania ryzykiem operacyjnym. ESZRO jest zasilany zasobami informacyjnymi, pochodzącymi z realizacji procesów organizacji. Źródłami zasilającymi mogą być osoby, systemy, baz danych, bazy wiedzy, dokumenty, wiadomości elektroniczne, procedury, itp., które dysponują danymi, informacjami i wiedzą z zakresu zagrożeń występujących w organizacji oraz podatności na te zagrożenia. System wykorzystując nabyte zasoby informacyjne i przetwarzając je w warstwie analizy i wiedzy, wspomaga przygotowanie podejścia do panowania nad ryzykiem operacyjnym. Pozytywna weryfikacja skutków wdrożenia wybranego podejścia przyczynia się do zwiększenia zasobów informacji i wiedzy całej organizacji, wpływając jednocześnie na stabilizację jej funkcjonowania oraz prawidłową realizację procesów.

ESZRO ma budowę modułową, tworzoną przez cztery główne warstwy:

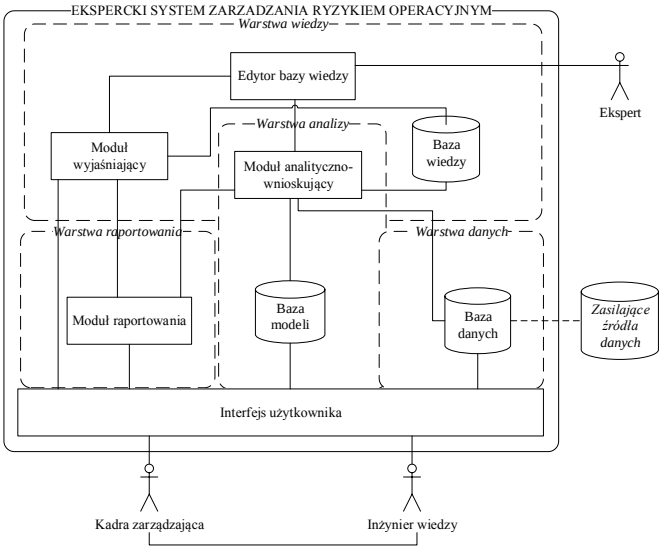
- danych – odpowiadającą za pozyskiwanie, gromadzenie i udostępnianie danych, niezbędnych do prawidłowej realizacji procesu analizy ryzyka operacyjnego,
- analizy – przetwarzającą dane do postaci informacji wspomagającej podejmowanie decyzji w procesie zarządzania ryzykiem operacyjnym,
- wiedzy – przetwarzającą dane i informacje do postaci sprawdzonych reguł i wskazówek postępowania w sytuacji zwiększonego zagrożenia ryzykiem, odpowiedzialną za gromadzenie i udostępnianie wiedzy eksperckiej z zakresu zarządzania ryzykiem,
- raportowania – odpowiadającą za elastyczne, wielodostępne i dopasowane do potrzeb użytkownika dokumentowanie wyników analizy ryzyka.

Warstwy te mogą, ale nie muszą, być implementowane i uruchamiane jednocześnie. Dzięki rozwiązaniu modułowemu użytkownik systemu może optymalizować koszty i korzyści jego wdrożenia oraz utrzymania. Kompletny model systemu ESZRO, uwzględniający implementację jego pełnej funkcjonalności, prezentuje Rys.4.

Na projekt warstwy danych składa się projekt bazy danych oraz powiązań integracyjnych z zasilającymi źródłami danych, interfejsem użytkownika oraz modułem analityczno-wnioskującym systemu. Dane z warstwy danych trafiają przez moduł analityczno-wnioskujący do modułu raportowania, bądź do bazy wiedzy, warunkując ich funkcjonowanie. Stąd jest to newralgiczny element systemu ESZRO, decydujący o poprawności i efektywności jego funkcjonowania.

Warstwa analizy obejmuje bazę modeli analitycznych oraz moduł analityczno-wnioskujący, współużytkowany również przez warstwę wiedzy. Warstwa analizy stanowi centrum rozwiązania, integrujące pozostałe jego warstwy i elementy strukturalne. Komunikuje się zarówno z warstwą danych, przez którą jest zasilana, jak i z generatorem raportów oraz interfejsem użytkownika, do których zwraca wyniki analiz. Pełni też funkcję usługową dla warstwy wiedzy, implementując reguły dla bazy wiedzy oraz realizując proces wnioskowania. Składa się z dwóch zasadniczych elementów:

- bazy modeli – implementującej modele analityczne,
- modułu analityczno-wnioskującego – realizującego analizy w oparciu o modele przechowywane w bazie modeli.



Rys. 4. *Model struktury Eksperckiego Systemu Zarządzania Ryzykiem Operacyjnym (źródło: opracowanie własne)*

Podstawową analizą prowadzoną w ramach systemu ESZRO, realizującą jednocześnie główny cel funkcjonowania systemu, jest szacowanie wielkości wpływu i wartości ryzyka operacyjnego. Pomiar ryzyka operacyjnego może być prowadzony m.in. według podejścia top-down, a weryfikowany według podejścia bottom-up lub odwrotnie [17, s. 72-76]. Pozwalają one oszacować prawdopodobieństwo wystąpienia oraz wielkość potencjalnych strat, a także zidentyfikować te zagrożenia, które mogą uniemożliwić realizację celów organizacji. Ponadto system ESZRO umożliwia prowadzenie analiz wskaźników kapitału operacyjnego, które zostały wprowadzone przez Bazylejski Komitet ds. Nadzoru Bankowego [1]. Nie kwantyfikują one wprost ryzyka operacyjnego, lecz pozwalają na wyznaczenie kapitału niezbędnego do pokrycia strat wywołanych tym ryzykiem.

Warstwa wiedzy odpowiada w SE za gromadzenie, przetwarzanie i udostępnianie wiedzy eksperckiej. Przy czym wiedza ta może być pozyskiwana od eksperta (i w początkowej fazie funkcjonowania systemu eksperckiego jest to niezbędny element funkcjonowania systemu) albo syntetyzowana na podstawie wyników analiz realizowanych w warstwie analizy. Będzie to możliwe pod warunkiem zgromadzenia odpowiedniej liczby danych o incydentach i związanych z nimi stratach. Szacuje się, że wymaga to około 2-letniego okresu funkcjonowania systemu celem rejestracji odpowiedniej liczby zdarzeń w systemie. Wiedza eksperta jest dostarczana do systemu przez edytor bazy wiedzy i składowana w postaci reguł. Reguła ma budowę zbioru warunków, które determinują wykonanie zbioru akcji. Reguły mogą być następnie prezentowane i przetwarzane jako tablice decyzyjne, w których wiersze reprezentują pojedyncze reguły, a kolumny są atrybutami warunkowymi lub decyzyjnymi tych reguł. Baza reguł jest porównywana z nowo wprowadzanymi incydentami w module wnioskującym. Przez mechanizmy dopasowania tworzone są zestawienia reguł, które odpowiadają zaistniałym zdarzeniom. Jeżeli występuje konflikt reguł na skutek tego, że np. dopasowane do zaistniałych zdarzeń reguły są wzajemnie sprzeczne, to moduł wnioskujący aktywuje procedury wariantowania reguł. Wybrane i przekazane do realizacji reguły wskazują na działania, które powinny być w związku z zaistniałą sytuacją podjęte.

Moduł raportowania służy jako generator raportów rozsyłanych dostępnymi kanałami dystrybucji do uprawnionych użytkowników. Moduł raportowania należy traktować, w perspektywie zarządzania

przedsiębiorstwem, jako narzędzie komunikacji i monitoringu zarządzania wewnętrznego firmy. Może być on też wykorzystywany jako element ogólnego sterowania rozwojem firmy i kształtowania jej wizerunku w kontekście społecznej odpowiedzialności i zrównoważonego rozwoju. W obszarze zarządzania raportowanie jest procesem inicjującym analizę i ocenę działalności firmy oraz podstawą do planowania celów na przyszłość. Jest też punktem odniesienia dla weryfikacji, modyfikacji i doskonalenia wewnętrznych systemów zarządzania. A przez to stanowi czynnik wdrażania i zarządzania zmianą w organizacji [10; 4; 3]. Wygodną formą raportu jest kokpit menedżerski, który może integrować dane wyselekcjonowane z wielu różnych raportów szczegółowych, agregując je oraz prezentując w formie zrozumiałej i użytecznej dla decydenta. Jest to nowoczesna forma raportowania, dedykowana kadrze menedżerskiej.

PODSUMOWANIE

Projekt systemu ESZRO został zainspirowany przez dostrzeżenie potrzeby inteligentnych narzędzi, o charakterze eksperckim i opartych na zarządzaniu wiedzą, wspierających zarządzanie ryzykiem operacyjnym w przedsiębiorstwach. System składa się z modułów funkcjonalnych, a jego wdrażanie i rozbudowa mogą być podzielone na iteracje, ułatwiające użytkownikowi adaptację nowej technologii. Jego interfejs jest nastawiony na prostotę działania i nie wymaga od użytkownika znajomości złożonych narzędzi oraz języków analizy danych czy przetwarzania wiedzy. Narzędzie ma na celu efektywnie wspomagać użytkownika na wszystkich etapach zarządzania ryzykiem operacyjnym – od budowy drzewa klasyfikacji ryzyka aż po wdrażanie mechanizmów przeciwdziałających jego skutkom materialnym. System może być rozwijany w kierunku wspierania pracy grupowej oraz zarządzania wszelkimi aspektami ryzyka w przedsiębiorstwie (nie ograniczając się tylko do ryzyka operacyjnego). Dzięki szkieletowej budowie oraz modułowej architekturze jego rozwój i modyfikacje będą możliwe w krótkim czasie i przy stosunkowo niewielkich nakładach inwestycyjnych.

Jego wprowadzenie na rynek może się przyczynić do rozwoju wiedzy na temat zastosowań systemów ekspertowych we wspomaganiu decyzji zarządczych.

BIBLIOGRAFIA

1. Basel Committee on Banking Supervision, Consultative Document, Operational Risk, Supporting Document to the New Basel Capital Accord. Bank for International Settlements, Basel, 2001.
2. Conrow E. H., *Effective Risk Management. Some keys to success*, American Institute of Aeronautics and Astronautics Inc., Reston, 2000.
3. Fazlagić A., J., *Innowacyjne zarządzanie wiedzą*, Difin, Warszawa, 2014.
4. Gierszewska G., *Zarządzanie wiedzą w przedsiębiorstwie: modele, podejścia, praktyka*, OWPW, Warszawa, 2011.
5. Giarratano J. C., Riley G.D., *Expert Systems: Principles and Programming*. 4th Edition. Thomson Course Technology, 2005.
6. Jajuga K. (red.), *Zarządzanie ryzykiem*, PWN, Warszawa, 2007.
7. Kisielnicki J., *Systemy informatyczne zarządzania*, Placet, Warszawa, 2013.
8. Kisielnicki J., *Zarządzanie i informatyka*, Placet, Warszawa 2014.
9. Niederliński A., *Regułowo-modelowe systemy ekspertowe*. Jacek Santorski & Co., Gliwice, 2006.
10. Rostek K., Witek M., *Znaczenie analizy i raportowania danych w procesie zarządzania przedsiębiorstwem*. Zarządzanie Przedsiębiorstwem, nr 2010(2).
11. Sitarski K., *Systemy informatyczne zarządzania wiedzą* [w] Informatyka Gospodarcza, t. 3 (red. Zawiła-Niedźwiecki J., Rostek. K., Gąsiorkiewicz A.). CH Beck, Warszawa, 2010.
12. Staniec I., Zawiła-Niedźwiecki J. (red.), *Ryzyko operacyjne w naukach o zarządzaniu*, C.H. Beck, Warszawa, 2015.
13. Szczepankiewicz E. I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*. Część 1 – Wybór podejścia do analizy [w] Monitor Rachunkowości i Finansów, nr 6/2006a.
14. Szczepankiewicz E. I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*. Część 2 – Etap oszacowania ryzyka [w] Monitor Rachunkowości i Finansów, nr 7/2006b.
15. Szczepankiewicz E. I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*. Część 3 – Strategie postępowania z ryzykiem operacyjnym [w] Monitor Rachunkowości i Finansów, nr 8/2006c.
16. Taboada M., Martínez-Tomás R., Ferrández J. M., *New perspectives on the application of expert systems.* [w] Expert Systems - The Journal of Knowledge Engineering. Vol. 28, nr. 4, 2011.
17. Thlon M., *Zarządzanie ryzykiem operacyjnym przedsiębiorstwa. Metoda szacowania ryzyka delta-EVT*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków.
18. Ustawa o prawie bankowym z dnia 29 sierpnia 1997: Dz. U. 2012 poz. 1376, 1385 i 1529 oraz Dz. U. 2013 poz. 777.
19. Wieleba R., *Inżynieria wiedzy w systemach ekspertowych*, Zeszyty naukowe WWSI, nr 5/2011.
20. Witkowski T., *Systemy informatyczne wspomagania podejmowania decyzji* [w] Informatyka Gospodarcza, t. 3 (red. Zawiła-Niedźwiecki J., Rostek. K., Gąsiorkiewicz A.). CH Beck, Warszawa, 2010.
21. Zawiła-Niedźwiecki J., *Analiza ryzyka operacyjnego z perspektywy teorii organizacji* [w] Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki finansowe, Ubezpieczenia, nr 51, 2012.
22. Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, edu-Libri, Warszawa, 2013.

EXPERT SYSTEM OF OPERATIONAL RISK MANAGEMENT - RESEARCH REPORT

Abstract

The subject of the article refers to the problems associated with the implementation of the risk management process in organizations. The article is focused on the issues of operational risk, which affects the everyday operation of each company. As a reference point the process of operational risk management in the banking sector was choosen. This choice was dictated

by the fact that the designated sector has the most experience in this area. The article discusses the operational risk management process and shows its defects, while pointing to expert systems as a potential solution to many of them. The purpose of this article is to present the results of research conducted on the Expert System of Operational Risk Management. The article presents basic information on expert systems and the proposed modification of the operational risk management process by using this developed system. Then it is presented the proposed model of ESORM, by discussing its main modules.

Autorzy:
mgr inż. Michał Wiśniewski, asystent, Politechnika Warszawska, Wydział Zarządzania, Zakład Informatyki Gospodarczej, M.Wisniewski@wz.pw.edu.pl