Jerzy Stanik[1], Maciej Kiedrowicz[2]

Metoda analizy i szacowania ryzyka zasobu informacyjnego

1. Wstęp

Artykuł prezentuje autorską metodę analizy i szacowania ryzyka, uwzględniającą szeroki zakres czynników ryzyka odnoszący się do zagrożeń występujących w poszczególnych fazach cyklu życia zasobu informacyjnego i wiążące je w sposób pozwalający na możliwie pełne i jednoznaczne oszacowanie poziomu ryzyka, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia. Przedstawiona metoda ma charakter jakościowy. Podzielona jest na etap analizy ryzyka i etap szacowania ryzyka zasobów informacyjnych. Do jej opracowania wykorzystano metody badawcze typu studia literatury fachowej, a także krytyczna analiza aktualnie dostępnych metod ilościowych i jakościowych analizy ryzyka stosowanych w badanych organizacjach, szczególnie jednostek kancelaryjnych przetwarzających dokumenty o różnych poziomach wrażliwości. Elementem obiektywizacji proponowanej metody jest odejście od wykorzystywania na etapie ewaluacji ryzyka tradycyjnych map ryzyka, a wykorzystanie/zastosowanie wektora ryzyka, którego składowe odzwierciedlają szeroką gamę czynników mających istotny wpływ na bieżący poziom ryzyka zasobu informacyjnego. Liczba czynników ryzyka uwzględnianych w proponowanej metodzie oraz ich wszechstronność zdecydowanie wyróżniają proponowane podejście na tle wykorzystywanych obecnie metod oceny ryzyka zasobów informacyjnych/systemów informatycznych, co zdaniem autorów stanowi jego niezaprzeczalną zaletę.

Rozdział drugi artykułu zawiera przegląd i ocenę aktualnie dostępnych metod oceny ryzyka, zarówno w literaturze fachowej, jak i w normach serii ISO ISO/IEC 31010 Risk Management w aspekcie ich wad i rekomendacji oraz skuteczności ewentualnego wykorzystania do oceny ryzyka zasobów informacyjnych.

[1] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.
[2] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.

Rozdział trzeci zawiera opis autorskiej metody analizy i szacowania ryzyka zasobów informacyjnych zawierający założenia, koncepcję oraz pewne rozwiązania aplikacyjne.

2. Przegląd metod oceny ryzyka i ich ocena

Obecnie w literaturze fachowej opisywanych jest wiele metod oceny ryzyka zasobów informacyjnych, wykorzystujących zarówno metody tradycyjne, jak i techniki komputerowe, z których każdą cechują pewne zalety i wady. Zakres dostępnych metod jest bardzo szeroki, poczynając od metod opisowych i prostej klasyfikacji opartej na ocenie ryzyka w podziale na wysokie, średnie i niskie, a kończąc na metodach opartych na złożonych obliczeniach, których wynikiem jest wyrażona ilościowo wielkość ryzyka zasobów informacyjnych lub systemów informacyjnych/informatycznych.

W praktyce wyróżnia się trzy podstawowe grupy metod oceny ryzyka:

- metody ilościowe (ang. *quantitative*), w ramach których próbuje się skwantyfikować i wyrazić liczbowo – na podstawie danych statystycznych – wielkość potencjalnych strat, prawdopodobieństwo ich wystąpienia, a w efekcie poziom występujących ryzyk;
- metody jakościowe (ang. *qualitative*) bazujące na ocenie zagrożeń, ich istotności oraz płynących z nich ewentualnych strat, na podstawie znajomości analizowanych zagadnień i doświadczenia osoby oceniającej;
- metody mieszane wykorzystuje elementy ilościowej i jakościowej analizy ryzyka.

2.1. Metody oceny ryzyka według międzynarodowych norm ISO

W normie ISO/IEC 31010 Risk Management – Risk Assessment Techniques opisano ich ponad 30. Obrazują one przekrój metod oceny ryzyka od rozważań eksperckich po metody oparte na budowaniu schematów i logicznych scenariuszy zdarzeń. Pozwalają na zapoznanie się z różnym podejściem do tego zagadnienia.

Każda metoda oceny ryzyka zawiera pewne podstawowe elementy, takie jak identyfikacja zagrożeń, oszacowanie prawdopodobieństwa wystąpienia danego zagrożenia oraz ewentualnych strat, które ze sobą niesie. Nie ma znaczenia, czy ocena ryzyka jest wykonywana na płaszczyźnie biznesowej, jakościowej, bezpieczeństwa czy społecznej. Wymienione etapy czy też elementy są nierozerwalnie

związane z procesem oceny ryzyka. Należy zauważyć, że zawierają one wiele elementów wspólnych i mogą się uzupełniać. Dokonując wyboru metody oceny ryzyka, należy kierować się dobrymi praktykami oraz specyfiką obszaru działania.

Tabela 1. Lista metod możliwych do zastosowania przy analizie ryzyka

Lp.	NAZWA METODY	ANALIZA RYZYKA		
		Identyfikowanie ryzyka	Konsekwencje ryzyka	Poziom ryzyka
1.	Metoda Courtney'a	**++**	++	++
2.	Metoda Fishera	++	++	++
3.	Metoda Parkera	++	++	++
4.	Metoda Marcello	++	++	++
5.	NIST SP 800–30	++	++	++
6.	Analiza przyczyn i konsekwencji	++	++	+
7.	Analiza przyczynowo-skutkowa	++	-	-
8.	Analiza warstw ochrony	++	+	+
9.	Analiza drzewa decyzji	++	++	-
10.	Analiza drzewa błędów	-	++	+
11.	Analiza drzewa zdarzeń	++	+	+
12.	Ocena niezawodności człowieka	++	++	++
13.	Metodyka CRAMM	++	++	++
14.	Analiza muchy	+	++	++
15.	Metoda „co, jeśli?"	++	++	++
16.	OPSEC	++	++	++
17.	Analiza scenariuszowa	++	+	+
18.	FRAP – *Facilitated Risk Analysis Process*	++	++	++
19.	STIR – *Simple Technique Illustrating Risk*	++	++	++
20.	Analiza wpływu na działalność	++	+	+
21.	Matryca skutek/prawdopodobieństwo	++	++	++

Legenda:
++ – zdecydowanie dotyczy; + – dotyczy; - – nie dotyczy
Źródło: opracowanie własne.

Analizując normy rekomendowane przez ISO, jak również te przyjęte przez PKN, dostrzeżemy, że problematyka metod oceny i zarządzania ryzykiem pojawia się w wielu normach dotyczących różnorodnych dziedzin. Do czasu przyjęcia normy ISO 31000:2009 Risk Management – Principles and Guidelines, ISO

Guide 73:2009 Risk Management – Vocabulary oraz normy ISO/IEC 31010 Risk Management – Risk Assessment Techniques, problematykę tę poruszały między innymi normy: ISO 14001:2015 Zarządzanie środowiskowe, ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji, PN-EN ISO 9001:2015 Zarządzanie jakością czy normy związane z bezpieczeństwem urządzeń technicznych, tj. PN – IEC 60300 Analiza ryzyka w systemach technicznych, EN ISO 14121–1 oraz EN ISO 12100:2010.

Normy te zalecają stosowanie metod oceny ryzyka, jednak nie wskazują szczegółowych procedur postępowania w całym procesie oceny ryzyka.

2.2. Wady metod analizy ryzyka dostępnych w międzynarodowych normach ISO

Zbiorcze zestawienie wad metod analizy i oceny ryzyka, dostępnych w literaturze fachowej, przedstawia się następująco:

1) Do podstawowych wad należy zaliczyć: zbyt ogólne, nie dostarczają informacji na temat analizy kosztowej w zakresie wprowadzenia nowych zabezpieczeń lub mechanizmów jakości i bezpieczeństwa, częsty brak danych do wyznaczenia prawdopodobieństwa zdarzeń elementarnych, trudności w ustaleniu pełnego zbioru kategorii ryzyka, niezdolność do badania skutków negatywnych o wspólnej przyczynie, nieuwzględnianie ryzyka wtórnego, nieuwzględnianie zagrożenia spowodowanego rozmyślnie, trudności w interpretacji wyników.
2) W przeważającej liczbie metod: szacowane ryzyka odbywa się na podstawie dwóch podstawowych czynników, tj. prawdopodobieństwa oraz konsekwencji; narzędziem służącym do wizualizacji wartości ryzyka (wyników analizy ryzyka) są matryce ryzyka; brak technik i narzędzi agregacji wyników wpływu (parametru określanego za pomocą szacunków ilościowych i jakościowych) przekonwertowanego po zsumowaniu do wyniku bliskiego, wyrażonego w skali jakościowej; brak wytycznych w zakresie stosowania narzędzi stanowiących wsparcie dla osób prowadzących ocenę oraz analizę ryzyka.
3) W metodach wyraźnie nie podkreśla się: konieczności zagregowania wyników wpływu za pomocą obliczeń matematycznych, poszczególne wyniki wartości wpływu dla poszczególnych parametrów wpływu w ramach danej kategorii są dodawane i dzielone przez liczbę parametrów (bardzo często bez uwzględniania wagi dla poszczególnych parametrów wpływu); konieczności uwzględniania podatności zasobów, mogącej skutkować zwiększeniem

szacowanej wartości prawdopodobieństwa oraz skutków, a w konsekwencji zmianą prognozowanej wartości ryzyka.

4) Metody ilościowe analizy ryzyka zawarte w normie ISO/IEC 31010 Risk Management – Risk Assessment Techniques są przeznaczone do analizy zdarzeń związanych z awariami i nie można przetransponować ich na potrzeby systemu zarządzania ryzykiem. W każdej z metodyk efektem finalnym jest jednak zbiorcza matryca ryzyka, na której prezentuje się łącznie wszystkie ryzyka poszczególnych zagrożeń, co utrudnia lub uniemożliwia ich interpretację oraz wskazanie skutecznej strategii postępowania z ryzykiem.

2.3. Rekomendacje – zbiór dobrych praktyk dotyczących szacowania ryzyka zasobów informacyjnych

Od momentu wprowadzenia elementów dobrych praktyk zarządzania ryzykiem oraz standardów i metodyk zarządzania ryzykiem jego znaczenie stale rośnie. Stąd też rekomenduje się wykorzystanie uznanych elementów „dobrych praktyk" w zakresie zarządzania ryzykiem, które ujednolicają terminologię, wnoszą uniwersalne zasady, elastyczną strukturę ramową i właściwie dopasowane procesy, w tym metody i narzędzia wspomagające ocenę ryzyka oraz dokumentowanie zarządzania ryzykiem.

Przy wyborze metody zaleca się wziąć pod uwagę następujące przesłanki i wytyczne, zwane dobrymi praktykami:

- analiza ryzykiem jest składową procesu podejmowania decyzji, ułatwiającą kierującym podejmowanie świadomych i właściwych wyborów;
- analiza ryzyka i zarządzanie prowadzone systematycznie i w sposób ciągły przyczynia się do poprawy efektywności oraz uzyskania spójnych, porównywalnych i wiarygodnych rezultatów;
- analiza ryzyka i zarządzanie nim powinny być dostosowane do zewnętrznych i wewnętrznych uwarunkowań organizacji i profili ryzyk, jakie występują w danej organizacji, bo tylko wtedy przynosi to oczekiwane wyniki;
- prawidłowo prowadzona analiza ryzyka bazuje na najlepszych dostępnych źródłach informacji, takich jak: dane historyczne, doświadczenia, informacje zwrotne od wszystkich interesariuszy, obserwacje, prognozy i opinie ekspertów z uwzględnieniem ich różnorodności i ograniczeń, czyli równocześnie przyczynia się do gromadzenia informacji z wielu źródeł z uwzględnieniem i wyraźnym określeniem stopnia tej niepewności;

- automatyczne przenoszenie metod i wyników do innych obszarów skutkuje pomyłkami w konsekwencji prowadzącymi do sytuacji kryzysowych o niewyobrażalnych skutkach;
- analizując ryzyka, musimy brać także pod uwagę czynniki ludzkie i kulturowe, rozpoznając tym samym możliwości, percepcję i intencje osób zarówno wewnątrz, jak i na zewnątrz organizacji, które mogą ułatwić bądź utrudnić osiągnięcie celów organizacji – w ten sposób zmniejszymy ryzyko i niepewność w podejmowaniu decyzji i wyborze możliwości przeciwdziałania;
- przejrzysta oraz wszechstronna analiza ryzyka daje nam gwarancję, dzięki odpowiedniemu określonemu czasowo zaangażowaniu kierujących na wszystkich poziomach zarządzania w organizacji, efektywnego i wczesnego określenia możliwych sytuacji kryzysowych, a w efekcie powoduje minimalizację oczekiwanych w wyniku zdarzenia strat;
- analiza ryzyka powinna być dynamiczna, powtarzalna oraz reagować na zmiany, ponieważ wewnętrzne i zewnętrzne ryzyka zmieniają się, pojawiają się nowe, a niektóre zanikają; właściwe ich monitorowanie i przegląd zapewnia organizacji stałą aktualną wiedzę co do niepewności i ryzyka działań oraz możliwość podjęcia skutecznych przeciwdziałań;
- dzięki analizie i zarządzaniu ryzykiem można doskonalić system zarządzania organizacją, wskazać kierunki koniecznych zmian w otoczeniu, priorytety podejmowania działań oraz możliwe straty, gdyby te zdarzenia wystąpiły. Analiza umożliwia także podejmowanie działań zapobiegawczych, prowadzących do minimalizacji poniesionych strat.

Zbiorcze porównanie metod ryzyka możliwych do oceny ryzyka zasobów informacyjnych prezentuje tabela 1.

Analizując przedstawione powyżej wybrane metodyki oceny i zarządzania ryzykiem zasobów informacyjnych/systemów informatycznych, łatwo zauważyć, że:

- nie istnieją uniwersalne metody pozwalające na dokładne określenie poziomu ryzyka zasobów informacyjnych, ponieważ każda z metod oceny ryzyka odnosi się jedynie do pewnego wycinka rzeczywistości, który modeluje i bierze pod uwagę wyłącznie wybrane czynniki wpływające na ryzyko zasobu informacyjnego/systemu informacyjnego;
- nie można także mówić o dokładnej wycenie ryzyka i potencjalnych strat, ponieważ każda z metod oceny ryzyka zawiera na pewnym etapie elementy subiektywnej oceny, takie jak na przykład przydział wag poszczególnym parametrom, określenie istotności danych czy określenie prawdopodobieństw zajścia pewnych zdarzeń;

- również nie można mówić o w pełni precyzyjnej i jednoznacznej ocenie poziomu ryzyka, a jedynie o pewnym przybliżeniu, którego dokładność zależy od przyjętego podejścia oraz liczby i adekwatności czynników, których wpływ na ryzyko brany jest pod rozwagę.

Tabela 1. Porównanie wybranych metod oceny ryzyka mających zastosowanie do zasobów informacyjnych

	Metoda wykorzystuje elementy ilościowej analizy ryzyka	Metoda wykorzystuje elementy ilościowej analizy ryzyka	Metoda uwzględnia wpływ czynnika ludzkiego na poziom ryzyka	Metoda wykorzystuje techniki komputerowe	Metoda zawiera elementy graficznej prezentacji ryzyka	Metoda uwzględnia aspekty bezpieczeństwa	Metoda zawiera elementy zarządzania ryzykiem
Metoda Courtney'a	X						
Metoda Fishera	X					X	X
Metoda Parkera	X		X			X	X
NIST SP 800–30		X				X	X
Metodyka CRAMM		X		X			X
Metoda Marcello	X		X				
OPSEC		X	X			X	X
FRAP		X					X
STIR		X			X		X

Źródło: opracowanie własne.

Na uwagę zasługuje podejście do szacowania ryzyka w bezpieczeństwie informacji opisane w normie PN-ISO/IEC 27005 Technika informatyczna, Zarządzanie ryzykiem w bezpieczeństwie informacji – załącznik informacyjny E. W tym załączniku proponuje się, aby proces szacowania ryzyka przebiegał w dwóch krokach: najpierw *Ogólne szacowanie ryzyka w bezpieczeństwie informacji*, a następnie *Szczegółowe szacowanie ryzyka w bezpieczeństwie informacji*. Zamieszczone również w tym załączniku przykłady pokazują, w kategoriach systemów informacyjnych, sposoby podejścia do analizy i szacowania ryzyka w kontekście procesów biznesowych. Można je zastosować także do wybranej grupy zasobów informacyjnych. Opisane podejścia jednak bazują na trójskładnikowym modelu oceny ryzyka.

Powyższy stan rzeczy prowadzi do konieczności powstawania coraz bardziej zaawansowanych narzędzi – metod oraz metodyk zarządzania ryzykiem – do oceny poziomu ryzyka zasobów informacyjnych. Jednym z takich narzędzi jest proponowana w naszych artykułach metoda i metodyka, które uwzględniają możliwie szeroką gamę czynników mających wpływ na poziom ryzyka oraz inne elementy pomijane w stosowanych obecnie podejściach do analizy ryzyka zasobów informacyjnych, co w połączeniu z wprowadzonym w metodzie aparatem matematycznym zwiększa dokładność przybliżenia estymacji ryzyka będącej jej wynikiem.

3. Autorska metoda analizy i szacowania ryzyka zasobu informacyjnego

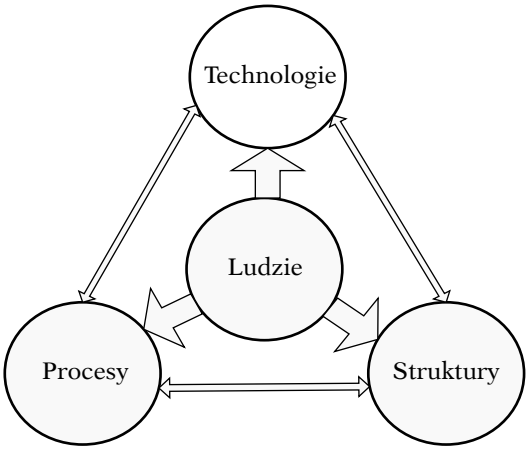
3.1. Założenia

Na potrzeby metody prezentowanej w niniejszy artykule ryzyko zasobu informacyjnego definiowane jest jako zagrożenie, iż technologie (rysunek 1), na przykład technologia informacyjna/informatyczna lub inne technologie stosowane w danej organizacji (niezależnie od jej rodzaju i skali działalności):

- nie zapewniają odpowiedniej integralności, poufności, niezaprzeczalności oraz dostępności zasobów informacyjnych;
- nie zostaną odpowiednio wdrożone i nie działają zgodnie z założeniami;
- nie zapewniają utrzymania bezpieczeństwa organizacji i jej zasobów na akceptowalnym poziomie;
- nie spełniają wymogów zawartych w politykach, takich jak: polityka bezpieczeństwa, polityka jakości, polityka ciągłości działania itp.;
- uniemożliwiają wdrożenie i doskonalenie infrastruktury technicznej i technologicznej wspierającej zarządzanie ryzykiem adekwatnego do aktualnego profilu ryzyka;
- nie zapewniają odpowiedniej struktury organizacyjnej w zakresie służb bezpieczeństwa;
- nie zapewniają prowadzenia właściwej dokumentacji w zakresie bezpieczeństwa, jakości lub ciągłości działania.

Ryzyko zasobu informacyjnego rozpatrywane jest w podziale na obszary, na przykład: bezpieczeństwa (B), ciągłości działania (C), technologii (T), złożoności (S) lub jakości (J), zdekomponowane na różne kategorie, grupy czynników

lub rodzaje czynników ryzyka, wynikających zarówno ze złożoności lub struktury samego zasobu informacyjnego, jak i technologii zastosowanych do jego przetwarzania lub atrakcyjności zasobu informacyjnego.



Rysunek 1. Podstawowe elementy organizacji oraz powiązania między nimi
Źródło: opracowanie własne.

Poniżej zilustrowano przykładową dekompozycję czynników ryzyka wraz z atrybutami podlegającymi pomiarowi:

1. W obszarze bezpieczeństwa informacji są to następujące atrybuty: dostępność zasobu informacyjnego, poufność przetwarzanych danych, integralność zasobu informacyjnego, spełnienie wymagań bezpieczeństwa zawartych w polityce bezpieczeństwa, straty rozumiane jako koszty poniesione w wyniku utraty atrybutów bezpieczeństwa, plan bezpieczeństwa teleinformatycznego, szczególne wymagania bezpieczeństwa systemu teleinformatycznego, procedury bezpiecznej eksploatacji.
2. W obszarze, wynikającym z unormowań prawnych, regulujących problematykę bezpieczeństwa, są to następujące elementy: powołanie pełnomocnika do ochrony zasobu informacyjnego; powołanie pionu ochrony w organizacji do realizacji przewidywanych zadań związanych z przetwarzaniem zasobu informacyjnego w organizacji; dostosowanie systemu informacyjnego do wymagań w zakresie wytwarzania, przetwarzania, przyjmowania, nadawania, wydawania i ochrony zasobów informacyjnych wynikające z przepisów prawa; zorganizowanie punktu (miejsca, obiektu) przetwarzania zasobów informacyjnych, w tym systemów teleinformatycznych służących wykonywaniu i przetwarzaniu dokumentów wrażliwych.

3. W obszarze bezpieczeństwa ciągłości działania są to następujące atrybuty: spełnienie wymagań zawartych w polityce bezpieczeństwa z zakresu ciągłości działania procesów, plan ciągłości działania skutki finansowe wstrzymania/ /przerwania realizacji procesu, skutki pozafinansowe wstrzymania/ przerwania realizacji procesu, koszty i czas niedostępności.
4. W pozostałych obszarach to: spełnienie wymagań zawartych w polityce jakości, niezawodność systemów informatycznych, elastyczność procesu przetwarzania zasobów informacyjnych, efektywność zarządzania architekturą zasobów informacyjnych, koszty oraz długość realizacji procesu przetwarzania zasobów informacyjnych, znaczenie zasobu dla organizacji i jej klientów.

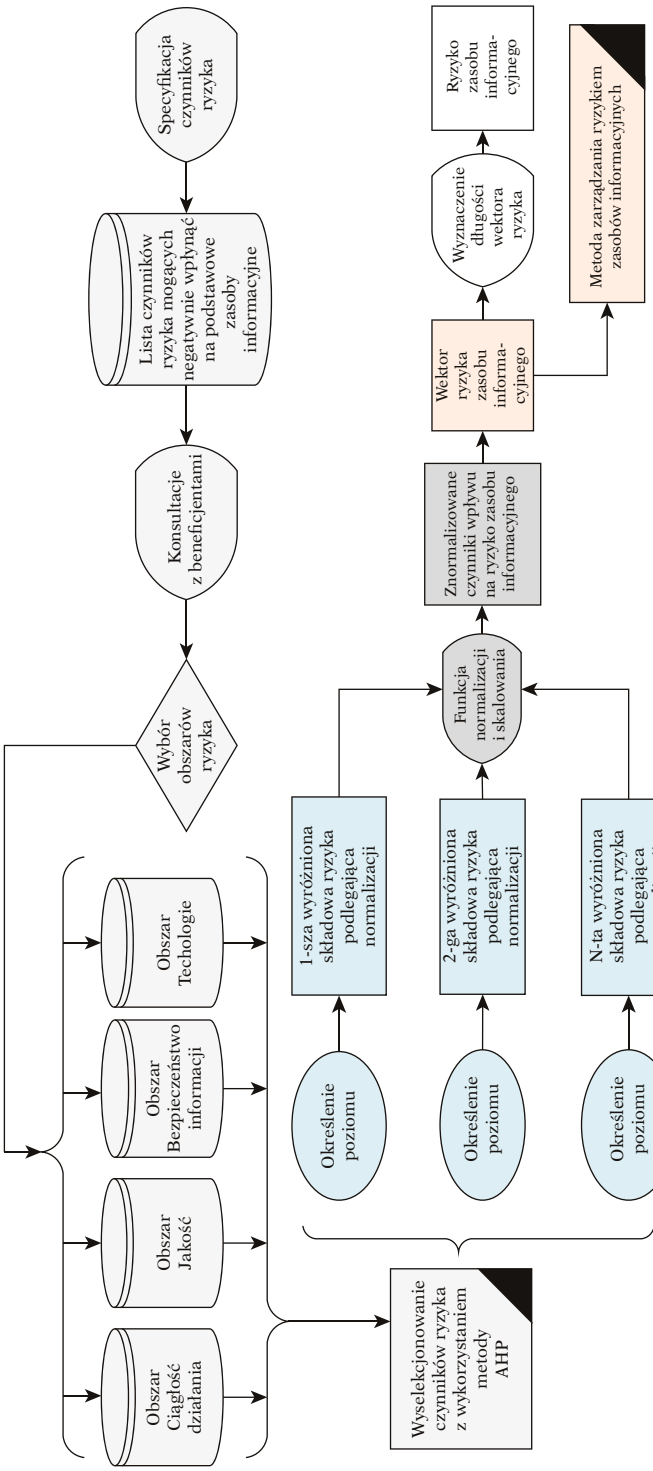
Oczywiście nic nie stoi na przeszkodzie rozszerzeniu lub zawężeniu proponowanej listy obszarów i atrybutów w ramach tych obszarów.

3.2. Koncepcja oceny ryzyka zasobu informacyjnego

Ogólny schemat działania proponowanej metody analizy ryzyka zasobu informacyjnego przedstawia rysunek 2. Ocena poziomu ryzyka według metody analizy ryzyka zasobów informacyjnych, proponowanej w pracy, dla każdego z zasobów informacyjnych organizacji przebiega zgodnie z następującymi krokami:

1. Identyfikacja czynników ryzyka – proces wyszukiwania, rozpoznawania i opisywania obszarów i czynników ryzyka.
2. Określenie poziomu czynników mających wpływ na ryzyko. Metoda bierze pod uwagę te warianty czynników, które zdaniem autorów pozwalają na stosunkowo obiektywną i dokładną ocenę poziomu ryzyka zasobów informacyjnych. W tym celu proponuje się zastosowanie metody AHP[3].
3. Normalizacja wyznaczonych wartości czynników mających wpływ na ryzyko.
4. Określenie wektora ryzyka na podstawie znormalizowanych wielkości składowych ryzyka.
5. Określenie wielkości wag wpływu poszczególnych czynników na całkowity poziom ryzyka dla danego zasobu informacyjnego. Wagi te określane są w zależności od typu zasobu informacyjnego, jakie przetwarza dana organizacja.
6. Wyznaczenie ważonego wektora ryzyka. Wektor ten uwzględnia wpływ zasobu na ryzyko danego systemu informacyjnego/informatycznego.

[3] *Analytic Hierarchy Process* (AHP) – wielokryterialna metoda hierarchicznej analizy problemów decyzyjnych. Umożliwia ona dekompozycję złożonego problemu decyzyjnego oraz utworzenie rankingu finalnego dla skończonego zbioru wariantów.



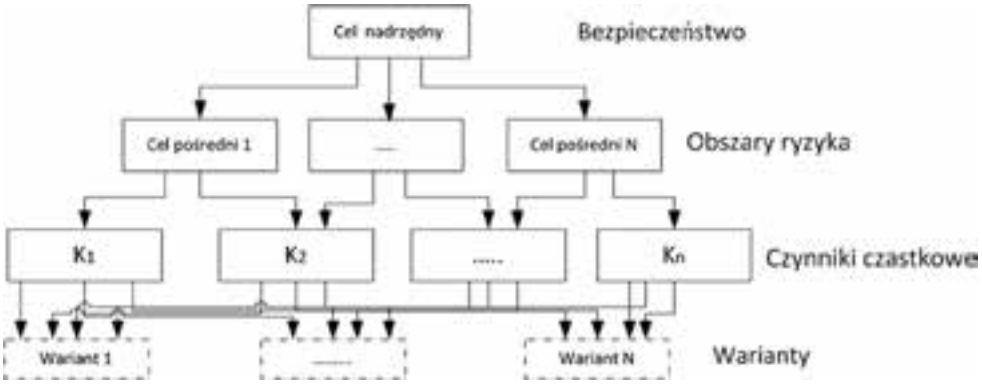
Rysunek 2. Podstawowe elementy organizacji oraz powiązania między nimi

Źródło: opracowanie własne.

7. Wyznaczenie ostatecznego poziomu ryzyka dla danego zasobu informacyjnego. W kolejnych podrozdziałach zostały scharakteryzowane tylko[4] punkty od 1–4.

3.2.1. Etap identyfikacji

Celem identyfikacji ryzyka jest zestawienie kompletnej listy ryzyk, wynikających z możliwych zdarzeń, które w zależności od okoliczności mogą kreować, zapobiegać, ograniczać, przyspieszać, opóźniać lub uniemożliwiać prawidłowe przetwarzanie zasobów informacyjnych.



Rysunek 3. Schemat struktury hierarchicznej zadania w metodzie Saaty'ego

Źródło: opracowanie własne za: T.L. Saaty, *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*, PA: RWS Publications, Pittsburgh 1994.

Identyfikacja ryzyka jest działalnością ciągłą, ponieważ niewykryte na czas ryzyko lub jego czynniki mogą nie tylko uniemożliwić osiągnięcie celu, ale także stanowić zagrożenie dla organizacji. Możliwe metody identyfikacji to: pomiary, dyskusje, symulacje, doświadczenia, oceny ekspertów, badania laboratoryjne, systemy detekcyjne, modelowanie, scenariusze, kwestionariusze, prognozy, analizy zagrożeń, struktur, rozwiązań (słabych i mocnych stron, możliwości i potrzeb). Możliwe źródła ryzyka to: zagrożenia naturalne i techniczne, niedoskonałość (brak) prawa, niewłaściwe nawyki, mentalność ludzi, słabość organizacji, brak wyszkolenia, niska świadomość zagrożeń, brak gotowości, nieprzygotowany personel, brak systemu, nieprzystające do rzeczywistości standardy bezpieczeństwa, zapóźnienia techniczne i technologiczne, nieprzestrzeganie norm technologicznych, błędy w działaniu, zaniechania i zaniedbania, ignorancja,

[4] Zagadnienia 5–8 zostały pominięte z uwagi na wymogi edytorskie.

niekompetencja, korupcja (systemowa). Etap identyfikacji kończy zastosowanie metody AHP. Metoda AHP służy przede wszystkim wspomaganiu wyboru wariantów decyzyjnych. Przebiega w czterech krokach: budowa modelu hierarchicznego obszarów i czynników ryzyka, ocena istotności czynników przez porównywanie parami, wyznaczenie globalnych i lokalnych preferencji czynników i preferencji wariantów decyzyjnych, klasyfikacja wariantów decyzyjnych. Wynikiem zastosowania metody AHP jest wektor uporządkowania wariantów grup czynników ryzyka zasobu informacyjnego (rysunek 3).

3.2.1. Etap określenia poziomu czynników mających wpływ na ryzyko

Metoda bierze pod uwagę takie grupy czynników i ich atrybuty, które zdaniem członków zespołu analizy ryzyka (ZAR) pozwalają na stosunkowo obiektywną i dokładną ocenę poziomu ryzyka zasobów informacyjnych. Przykładowe sposoby określania czynników mających wpływ na ryzyko ilustruje tabela 2.

Tabela 2. Przykładowe sposoby określania poziomu czynników dla obszaru „Bezpieczeństwo informacyjne"

Czynnik ryzyka	Sposób określania poziomu
Dostępność zasobu informacyjnego λ_{Z_i}	Dostępność zasobu intelektualnego Z_i nazywamy właściwość bycia możliwym do wykorzystania w założonym czasie na żądanie autoryzowanego podmiotu działania w przedsiębiorstwie. Dostępność danych w systemie informatycznym Z_i wyrażana jest poprzez przynależność zasobu informacyjnego Z_i do klasy dostępności $\lambda \in \Lambda$ i oznaczana λ_{Z_i}. Zbiorem klas zasobu informacyjnego Z_i nazywany zbiór L = {I, II, III, IV, V}, przy czym: I – określa zasób intelektualny Z_i, dla którego oczekiwana dostępność w skali roku wynosi 99,99%, a maksymalna jednorazowa niedostępność systemu nie przekracza 30 minut, V – określa zasób intelektualny Z_i, dla którego oczekiwana dostępność w skali roku wynosi poniżej 70%, a maksymalna jednorazowa niedostępność systemu przekracza trzy tygodnie.
Poufność zasobu informacyjnego – α_{Z_i}	Poufnością zasobu intelektualnego Z_i nazywamy właściwość nieujawniania informacji stronom nieupoważnionym do jej pozyskania. Poufność zasobu informacyjnego Z_i wyrażana jest przez przynależność go do klasy poufności $\alpha \epsilon A$ i oznaczana jako α_{Z_i}. Zbiorem klas poufności zasobu informacyjnego nazywamy zbiór A = {A, B, C, D, E}, przy czym: A – określa system informatyczny, przetwarza dane tajne, których ujawnienie może spowodować zagrożenie dla ludzkiego życia lub zdrowia, E – określa system informatyczny przetwarza dane publicznie dostępne.

Czynnik ryzyka	Sposób określania poziomu
Efektywność systemu monitorowania bezpieczeństwa informacji $-\beta^{\mathrm{B}}_{\mathrm{Z_i}}$,	Efektywnością zasobu intelektualnego Z_i nazywamy wielomian: $$\beta^B_{S_i} = d^B_{SM}\left(S_i\right) * \sum_j \left(\delta^m_{S_i} * \upsilon^{k^j}_{S_i}\right),$$ gdzie: j – numer kolejnego kryterium oceny efektywności systemu monitorowania bezpieczeństwa, $\delta^m_{S_i}$ – priorytet *j–tego* kryterium oceny efektywności systemu monitorowania bezpieczeństwa względem systemu S_i, $\upsilon^{k^j}_{S_i}$ – wartość *j–tego* kryterium oceny efektywności systemu monitorowania bezpieczeństwa względem systemu S_i.
Spełnienie wymagań określonych w polityce bezpieczeństwa informacji $-\eta^{\mathrm{B}}_{Z_i}$	Zbiorem wymagań polityki Organizacji O nazywany skończony zbiór $W^B_{P(O)} = \left\{w_1, w_2, \ldots \mathrm{w}_{\mathrm{M^B}}\right\}$, gdzie: M^B jest liczbą wymagań polityki bezpieczeństwa względem zasobu informacyjnego. Dla każdego z wymagań $w_m \epsilon W^B_{Z(i)}$ definiujemy wielkość priorytetu wymagania względem zasobu intelektualnego Z_i. Priorytetem wymagania $w_m \epsilon W^B_{Z(i)}$ nazywamy liczbę $p^m_{Z_i} \in \left\{0,1, \ldots 5\right\}$. Spełnieniem wymagań polityki względem zasobu intelektualnego Z_i nazywamy procentowo wyrażoną wielkość: $$\eta^B_{S_i} = \frac{\sum_{m=1}^{W^B_{P(O)}} \left(p^m_{S_i} * s^m_{S_i}\right)}{\sum_{m=1}^{W^B_{P(O)}} p^m_{S_i}}$$ gdzie: $W^B_{S_i}$ – zbiór wymagań bezpieczeństwa względem zasobu intelektualnego Z_i, $p^m_{S_i}$ – priorytet wymagania m względem systemu S_i, $s^m_{S_i}$ – spełnienie wymagania m w względem systemu S_i.

Źródło: opracowanie własne.

3.2.2. Normalizacja wyznaczonych wartości czynników mających wpływ na ryzyko

Ze względu na fakt, że poszczególne czynniki ryzyka w ramach wyróżnionych obszarów należą do różnych zbiorów wartości, koniecznym jest wprowadzenie funkcji ξ lub zbioru funkcji $\xi \in \Xi$ jednoznacznie odwzorowujących te składowe na jednolity przedział wartości. Funkcją normalizacji nazywamy rodzinę funkcji $\xi \in \Xi$

$$\xi : X \rightarrow [1, 2, \ldots, N]. \tag{1}$$

Postacie funkcji normalizacji z rodziny Ξ określone powinny być w taki sposób, aby odwzorować ich wartości na przedział [1,..., N] oraz aby zachować właściwe proporcje ich wpływu na całkowite ryzyko zasobu, uwzględniając zbiór X wszystkich wyspecyfikowanych czynników ryzyka. Zbiór X powinien być zdekomponowany na podzbiory X^B, X^T, X^C, reprezentujące wyróżnione obszary/ /aspekty.

W artykule przyjęto następujące wartości: dla obszaru bezpieczeństwo informacji – $\xi: X^B \to [1, 2, \ldots, 24]$, dla obszaru IT – $\xi: X^T \to [1, 2, \ldots, 8]$, dla obszaru ciągłości działania – $\xi: X^C \to [1, 2, \ldots, 24]$. Zaproponowane przedziały nie są obligatoryjne i mogą być dostosowane do indywidualnych potrzeb.

Przykładowe postacie funkcji normalizacji zawiera tabela 3.

Tabela 3. Przykładowe postacie funkcji normalizacji

A. Dla funkcji $\xi \in \Xi^B$	*dostępności* $\xi_\lambda\left(\lambda_{z_i}\right)=$	*poufności danych* $\xi_\alpha\left(\alpha_{z_i}\right)=$	spełnienie *wymagań PB* $\xi_\eta^B\left(\eta_{z_i}^B\right)=$	*monitorowanie bezpieczeństwa* $\xi_\eta^B\left(\beta_{z_i}^B\right)=$
Postać funkcji normalizacji	$\begin{cases} 1, gdy\ \lambda_{z_i} = V \\ 7, gdy\ \lambda_{z_i} = IV \\ 13, gdy \lambda_{z_i} = III \\ 19, gdy\ \lambda_{z_i} = II \\ 24, gdy\ \lambda_{z_i} = I \end{cases}$	$\begin{cases} 1, gdy\ \alpha_{z_i} = E \\ 7, gdy\ \alpha_{z_i} = D \\ 13, gdy\ \alpha_{z_i} = C \\ 19, gdy\ \alpha_{z_i} = B \\ 24, gdy\ \alpha_{z_i} = A \end{cases}$	$1+23*\left(1-\frac{\eta_{z_i}^B}{100\%}\right)$	$24-\sqrt[3]{\frac{\beta_{z_i}^C}{2}}$
B. Dla funkcji $\xi \in \Xi^C$	koszt niedostępności $\xi_\kappa\left(\kappa_{z_i}\right)=$	maksymalny czas niedostępności $\xi_\pi\left(\pi_{z_i}\right)=$	spełnienie wymagań PC $\xi_\eta^C\left(\eta_{z_i}^C\right)=$	monitorowanie ciągłości $\xi_\beta^C\left(\beta_{z_i}^C\right)=$
Postać funkcji normalizacji	$\begin{cases} 1, gdy\ \kappa_{z_i} = V \\ 7, gdy\ \kappa_{z_i} = IV \\ 13, gdy\ \kappa_{z_i} = III \\ 19, gdy\ \kappa_{z_i} = II \\ 24, gdy\ \kappa_{z_i} = I \end{cases}$	$\begin{cases} 1, gdy\ \pi_{z_i} = 4 \\ 7, gdy\ \pi_{z_i} = 3 \\ 13, gdy\ \pi_{z_i} = 2 \\ 19, gdy\ \pi_{z_i} = 1 \\ 24, gdy\ \pi_{z_i} = 0 \end{cases}$	$1+23*\left(1-\frac{\eta_{z_i}^C}{100\%}\right)$	$24-\sqrt[3]{\frac{\beta_{z_i}^C}{2}}$,
C. Dla podzbioru funkcji $\xi \in \Xi^T$	znaczenie systemu $\xi_\zeta\left(\zeta_{z_i}\right)=$	elastyczność systemu $\xi_\vartheta\left(\vartheta_{z_i}\right)=$	spełnienia wymagań polityki jakości $\xi_\eta^T\left(\eta_{z_i}^T\right)=$	monitorowania jakości $\xi_\eta^T\left(\beta_{z_i}^T\right)=$

Postać funkcji normalizacji	$\begin{cases} 1, gdy\ \zeta_{z_i} = VI \\ 7,\ gdy\ \zeta_{z_i} = V \\ 13, gdy\ \zeta_{z_i} = IV \\ 16,\ gdy\ \zeta_{z_i} = III \\ 20, gdy\ \zeta_{z_i} = II \\ 24, gdy\ \zeta_{z_i} = I \end{cases}$	$\begin{cases} 1, gdy\ \vartheta_{z_i} = 4 \\ 7, gdy\ \vartheta_{z_i} = 3 \\ 13, gdy\ \vartheta_{z_i} = 2 \\ 19, gdy\ \vartheta_{z_i} = 1 \\ 24, gdy\ \vartheta_{z_i} = 0 \end{cases}$	$1+23*\left(1-\frac{\eta_{z_i}^T}{100\%}\right);$	$24-\sqrt[3]{\frac{\beta_{z_i}^T}{2}};$

Źródło: opracowanie własne.

3.2.3. Wektor ryzyka zasobu informacyjnego i jego wielkość

Mając określoną bazę przestrzeni wektorowej $(M_{\text{m×n}}, \boldsymbol{R},+,\cdot)$ w algebrze $(M_{\text{m×n}}, \boldsymbol{R},+,,\otimes)$ można wprowadzić pojęcie wektora ryzyka zasobu intelektualnego Z_i. Wektorem ryzyka zasobu intelektualnego Z_i w algebrze $(M_{\text{m×n}}, \boldsymbol{R},+,,\otimes)$ nazywamy wektor $\overrightarrow{R_{P_i}} \in M^{mxn}$ będący kombinacją liniową elementów ryzyka zasobu informacyjnego Z_i w bazie przestrzennej liniowej $(M_{\text{m×n}}, \boldsymbol{R},+,\cdot)$:

$$\overrightarrow{R_{Z_i}} = \xi_{\alpha^1}\left(\alpha^1_{Z_i}\right)\cdot\overrightarrow{\alpha^1} + \xi_{\alpha^2}\left(\alpha^2_{Z_i}\right)\cdot\overrightarrow{\alpha^2} + \ldots + \xi_{\alpha^J}\left(\alpha^M_{Z_i}\right)\cdot\overrightarrow{\alpha^M}. \tag{2}$$

Wymiar algebry $(M_{\text{m×n}}, \boldsymbol{R},+,,\otimes)$ wynosi: dim $(M_{\text{m×n}}, \boldsymbol{R},+,,\otimes) = M$. Z faktu, że wymiar algebry $(M_{\text{m×n}}, \boldsymbol{R},+,,\otimes)$ wynosi M, wynika, że istnieje M wektorów bazowych przestrzeni wektorowej $(M_{\text{m×n}}, \boldsymbol{R},+,\cdot)$ z algebry $(M_{\text{m×n}}, \boldsymbol{R},+,,\otimes)$, zdefiniowanych następująco:

$$\overrightarrow{\alpha^1} = \begin{pmatrix} 1 & \cdots & 0^n \\ \vdots & \ddots & \vdots \\ 0^m & \cdots & 0^M \end{pmatrix}; \ldots; \overrightarrow{\alpha^M} = \begin{pmatrix} 0 & \cdots & 0^n \\ \vdots & \ddots & \vdots \\ 0^m & \cdots & 1 \end{pmatrix}. \tag{3}$$

Z kombinacji liniowej powyższego wzoru wynika, że wpływ wszystkich M wymiarów analizy ryzyka zasobu intelektualnego Z_i na uzyskany wektor ryzyka $\overrightarrow{R_{Z_i}} \in M^{mxn}$ jest jednakowy. Dlatego w celu uszczegółowienia oszacowania poziomu ryzyka zasobu intelektualnego Z_i może być konieczne przypisanie poszczególnym składowym ryzyka wag ich wpływu na końcowy poziom ryzyka zasobu intelektualnego Z_i oraz modyfikacja współrzędnych wektora ryzyka $\overrightarrow{R_{Z_i}} \in M^{mxn}$ z wykorzystaniem tych wag wpływu. W artykule zagadnienie to zostanie pominięte.

3.2.4. Wyznaczenie ostatecznego poziomu ryzyka dla danego zasobu informacyjnego

Mając zdefiniowane pojęcie wektora ryzyka zasobu intelektualnego Z_i w algebrze $(M_{m\times n}, \boldsymbol{R}, +, , \otimes)$, możemy ostatecznie wprowadzić definicję całkowitego ryzyka zasobu intelektualnego Z_i.

Ryzykiem zasobu informacyjnego Z_i w algebrze $(M_{m\times n}, \boldsymbol{R}, +, , \otimes)$ nazywamy liczbę $R_{Z_i} \in \mathcal{R}$ równą długości wektora, będącego wektorem ryzyka zasobu intelektualnego Z_i, czyli:

$$R_{Z_i} = \left\| \overrightarrow{R_{Z_i}} \right\|. \tag{4}$$

Przedstawiona wielkość R_{Z_i} określa w sposób ilościowy wielkość ryzyka zasobu informacyjnego Z_i, co stanowi wielkość wynikową proponowanej w niniejszej pracy metody analizy ryzyka zasobu intelektualnego Z_i. W celu jakościowego przedstawienia poziomu ryzyka wyznaczonego za pomocą przedstawionej powyżej metody półilościowej, można przyjąć następujące przedziały ryzyka: $R_{Z_i} > 70$ – ryzyko katastroficzne, $R_{Z_i} \in (60, \ldots, 70]$ – ryzyko bardzo wysokie, $R_{Z_i} \in (50, \ldots, 60]$ – ryzyko wysokie, $R_{Z_i} \in (40, \ldots, 50]$ – ryzyko średnie, $R_{Z_i} \in (30, \ldots, 40]$ – ryzyko niskie, $R_{Z_i} \in (20, \ldots, 30]$ – ryzyko bardzo niskie, $R_{Z_i} < 20$ – ryzyko śladowe.

4. Podsumowanie i kierunki dalszych badań

Z niniejszej pracy wynika, że istnieje możliwość stworzenia „dość dobrej" i spójnej metody analizy i szacowania ryzyk zasobów informacyjnych, uwzględniającej zarówno czynniki ilościowe, jak i jakościowe, która pozwala wyznaczyć w sposób możliwie dokładny i jednoznaczny poziom ryzyka zasobów informacyjnych danej organizacji. Elementem obiektywizacji proponowanej w pracy metody jest odejście od wykorzystywania na etapie ewaluacji ryzyka tradycyjnych map ryzyka, a wykorzystanie/zastosowanie wektora, którego składowe odzwierciedlają szeroką gamę czynników, mających istotny wpływ na bieżący poziom ryzyka zasobu informacyjnego. Liczba czynników ryzyka uwzględnianych w proponowanej metodzie oraz ich wszechstronność zdecydowanie wyróżniają proponowane podejście na tle wykorzystywanych metod oceny ryzyka zasobów informacyjnych/systemów informatycznych, co zdaniem autorów stanowi jego niezaprzeczalną zaletę. Metoda ta może stanowić podstawę systemu zarządzania

ryzykiem w organizacji. Ponadto należy stwierdzić, że nie istnieją uniwersalne metody pozwalające na dokładne określenie poziomu ryzyka zasobów informacyjnych, ponieważ każda z metod oceny ryzyka odnosi się jedynie do pewnego wycinka rzeczywistości, który modeluje i bierze pod uwagę tylko wybrane czynniki wpływające na ryzyko systemu informacyjnego. Również nie można mówić o dokładnej wycenie ryzyka i potencjalnych strat, gdyż każda z metod oceny ryzyka zawiera na pewnym etapie elementy subiektywnej oceny, takie jak: wybór obszarów i grup czynników ryzyka, przydział wag poszczególnym czynnikom, określenie istotności danych czy określenie prawdopodobieństw zajścia pewnych zdarzeń. Także nie można mówić o w pełni precyzyjnej i jednoznacznej ocenie poziomu ryzyka, a jedynie o pewnym przybliżeniu, którego dokładność zależy od przyjętego podejścia oraz liczby i adekwatności czynników, których wpływ na ryzyko brany jest pod uwagę.

Opracowana metoda została wykorzystana w kilku projektach badawczo-rozwojowych realizowanych w WAT, zwłaszcza w projekcie pt. „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości", jako podstawowy element systemu zarządzania ryzykiem i systemu zarządzania jakością.

Bibliografia

Hoffmann R., Kiedrowicz M., Stanik J., *Evaluation of information safety as an element of improving the organization's safety management*, w: MATEC Web of Conferences, CSCC 2016, DOI: 10.1051/matecconf/20167604011, vol. 76. Hoffmann R., Kiedrowicz M., Stanik J., *Risk management system as the basic paradigm of the information security management system in an organization*, w: MATEC Web of Conferences, CSCC 2016, DOI:10.1051/matecconf/20167604010, vol. 76.

Kiedrowicz M., *Wybrane problemy projektowania rozproszonych baz danych*, WAT, Warszawa 2000.

Kiedrowicz M., *Publiczne zasoby informacyjne jako podstawa tworzenia platform integracyjnych*, w: *INTERNET. Prawno-informatyczne problemy sieci, portali i e-usług*, G. Szpor (red.), C.H. Beck, Warszawa 2012, s. 231–246.

Kiedrowicz M., *Dostęp do publicznych zasobów danych – Big data czy Big brother*, w: *INTERNET. Publiczne bazy danych i Big data*, G. Szpor (red.), C.H. Beck, Warszawa 2014, s. 15–39.

Kiedrowicz M., *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych*, „Roczniki Kolegium Analiz Ekonomicznych" 2014, z. 33, s. 209–234.

Kiedrowicz M., Stanik J., *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*, w: *Information Management in Practice*, B. Kubiak, J. Maślankowski (red.), Uniwersytet Gdański, Gdańsk 2015, s. 231–249.

PN-ISO/IEC 27005, Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN 2013.

PN-ISO 31000:2012(2012), Zarządzanie ryzykiem -Zasady i wytyczne, PKN 2012.

Saaty T.L., *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*, PA: RWS Publications, Pittsburgh 1994.

Stanik J., Kiedrowicz M., Protasowicki T., *Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2014, vol. 113/2, s. 113–130.

Stanik J., *Koncepcja systemu zarządzania ryzykiem w bezpieczeństwie informacji na przykładzie„Kancelarii RFID"*, w: *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*, M. Kiedrowicz (red.), WAT, Warszawa 2015, s. 43–67.

Stanik J., Protasowicki T., *Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego*, w: *Od procesów do oprogramowania: badania i praktyka*, P. Kosiuczenko, M. Śmiałek, J. Swacha (red.), Polskie Towarzystwo Informatyczne, Warszawa 2015, s. 27–44.

Stanik J., *Charakterystyka podstawowych elementów systemu zarządzania bezpieczeństwem informacji na przykładzie„Kancelarii RFID"*, w: *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*, M. Kiedrowicz (red.), WAT, Warszawa 2015, s. 19–35.

Stanik J., Hoffmann R., Napiórkowski J., *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2016, nr 123, s. 321–336.

Stanik J., Kiedrowicz M., *Uwarunkowania zarządzania ryzykiem operacyjnym w bezpieczeństwie systemu zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości*, w: *Zarządzanie informacjami wrażliwymi. Bezpieczeństwo dokumentów, wykorzystane technologii RFID*, M. Kiedrowicz (red.), WAT, Warszawa 2016, s. 25–54.

Stanik J., Hoffmann R., *Model ryzyka procesów biznesowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2017, nr 126/1, s. 325–338.

Stanik J., Kiedrowicz M., *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Ekonomiczne Problemy Usług" 2017, nr 126/1, s. 339–354.

Trajdos T., *Matematyka*, Wydawnictwa Naukowo-Techniczne, Warszawa 1993.

* * *

Method of Analyzing and Estimating the Risk of an Information Resource

Summary

The article presents the author's method of analyzing and estimating the risk of information resources/IT systems, taking into account the different categories of risk factors relevant for ensuring the completeness of the process of determining or determining the risk level of an information resource that is processed both traditionally and with the use of information systems. The method described is of a qualitative nature. It is divided into the stage of risk analysis and the stage of risk assessment of information resources. The objectivization element proposed in this paper is a departure from the use of risk assessment from traditional risk maps and the use of a vector whose components reflect a wide range of factors that have a significant impact on the current level of risk of the information resource.

Keywords: information resource, information system, risk analysis method, risk vector, risk management system.