Jerzy Stanik[1]

Wieloaspektowy model oceny ryzyka zasobu informacyjnego

1. Wstęp

Świadomość zagrożeń i skutków, jakie one mogą wywołać w przedsiębiorstwach, zmusza kierownictwo tych jednostek do ciągłego analizowania czynników[2] i obszarów ryzyka[3] oraz przyjęcia określonych sposobów jego pomiaru, oceny, ewaluacji i zabezpieczania się przed nim. Prowadząc badania na temat wykorzystywania przez organizacje różnych modeli oceny ryzyka i systemów zarzadzania ryzykiem, można stwierdzić, że dotychczas nie powstał ujednolicony, spójny i wspólny dla wszystkich rodzajów jednostek organizacyjnych model oceny ryzyka kapitału intelektualnego organizacji[4], a w szczególności zasobów informacyjnych. W normie ISO/IEC 31010 Risk Management – Risk Assessment Techniques zostało opisanych ponad 30 różnych instrumentów typu: metody, modele, techniki i narzędzia, wspierających proces zarządzania ryzykiem. Obrazują one przekrój sposobów 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. Mimo to trudno znaleźć rozwiązania typu model ryzyka, który bezpośrednio można zaaplikować do oceny poziomu ryzyka zasobów informacyjnych, przy czym rozwiązanie to powinno posiadać możliwość uwzględniania szerokiej gamy czynników, mających wpływ na poziom ryzyka zasobu oraz inne elementy pomijane w stosowanych obecnie podejściach do analizy ryzyka zasobów informacyjnych.

---

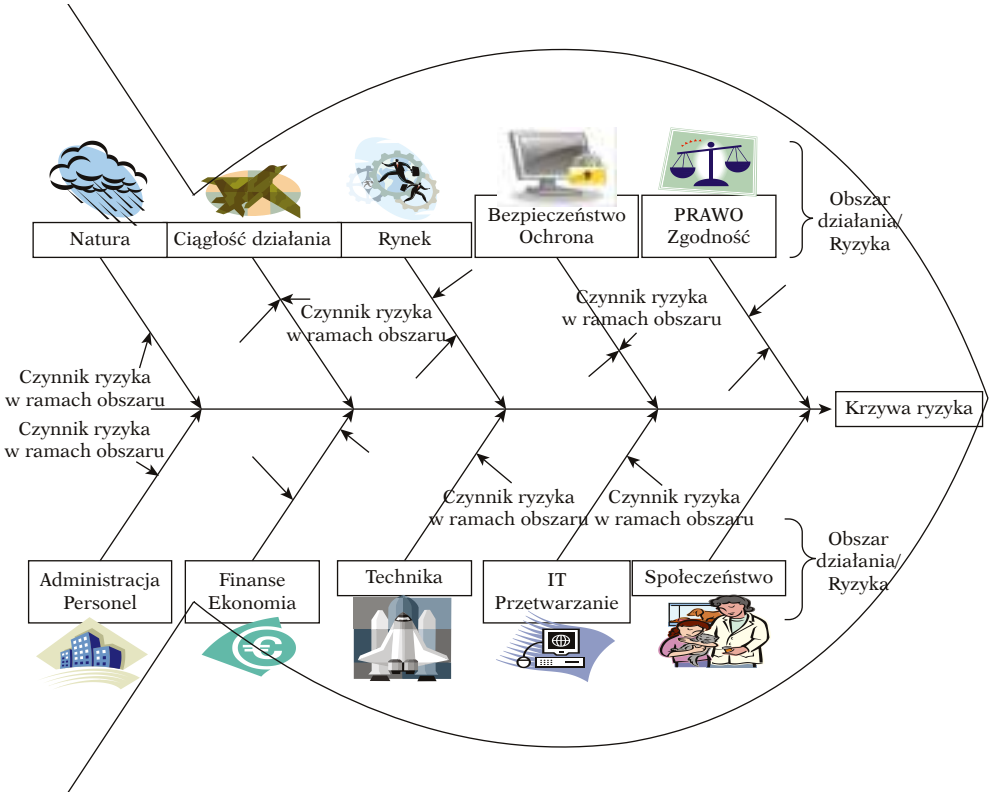
[1] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.

[2] Czynnik ryzyka – okoliczności, sytuacja, stan prawny lub stan faktyczny, które mogą wywołać ryzyko wystąpienia nieprawidłowości.

[3] Obszar ryzyka to obszar, w którym występują istotne z punktu widzenia jednostki czynniki ryzyka

[4] Kapitał intelektualny to majątek powstający na bazie wiedzy. Stanowi on sumę wielu składników niematerialnych, które kształtują wartość rynkową przedsiębiorstwa i niejednokrotnie określany jest mianem kapitału wiedzy lub materii intelektualnej.

Standardem, na bazie którego można skonstruować „dość dobry" model ryzyka dla zasobu informacyjnego, jest norma PN-ISO/IEC 27005 Technika informatyczna, Zarządzanie ryzykiem w bezpieczeństwie informacji. Z treści tej normy wynika, że proces zarządzania ryzykiem w bezpieczeństwie informacji może być zastosowany do organizacji jako całości, dowolnej części organizacji (np. działu, fizycznej lokalizacji, usługi), dowolnego systemu informacyjnego, zabezpieczeń istniejących, planowanych lub o wybranym aspekcie (np. planowanie ciągłości działania). Mimo to jest to tylko dokument ustalający zasady, wytyczne lub charakterystyki do powszechnego i wielokrotnego stosowania, odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzające do uzyskania optymalnego stopnia uporządkowania w określonej dziedzinie. Powyższy stan rzeczy prowadzi do konieczności powstawania coraz bardziej zaawansowanych modeli ryzyka wykorzystywanych do oceny poziomu ryzyka kapitału intelektualnego organizacji, między innymi i zasobów informacyjnych.



Rysunek 1. Obszary działania, w których organizacja narażona jest na zagrożenia

Źródło: opracowanie własne.

Celem niniejszego artykułu jest prezentacja kompleksowego i wieloaspektowego modelu oceny ryzyka zasobu informacyjnego, który stanowiąc podstawowe narzędzie do kolejnych etapów oceny ryzyka, dostarcza wszechstronnej informacji do procesu analizy i zarządzania ryzykiem. Prezentowane podejście bierze pod uwagę różne kategorie czynników ryzyka (rysunek 1), a szczególnie:

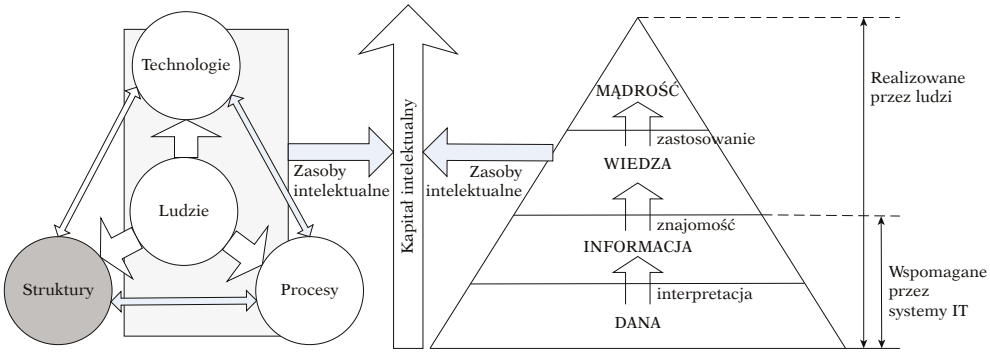
- bezpieczeństwa (B) – czynniki bezpieczeństwa informacji w myśl normy ISO serii 27000:2015,
- jakości (J) – czynniki jakości w myśl normy ISO 9001:2015,
- ciągłości działania (C) – czynniki ciągłości działania w myśl normy ISO 22301 dotyczącej ciągłości działania organizacji,
- technologii (T) – czynniki ryzyka w myśl normy ISO 31000 w zakresie zarządzania ryzykiem
- złożoności (S) oraz wynikających z architektury samego zasobu informacyjnego.

2. Pojęcie zasobu informacyjnego

Pojęcie zasobu informacyjnego na gruncie przepisów powszechnie obowiązującego prawa to: „Informacje o szczególnym znaczeniu dla rozwoju innowacyjności w organizacji, państwie i rozwoju społeczeństwa informacyjnego, które ze względu na sposób przechowywania i udostępniania pozwalają na ich ponowne wykorzystywanie w rozumieniu przepisów ustawy z dnia 25 lutego 2016 roku o ponownym wykorzystywaniu informacji sektora publicznego" (Dz. U. poz. 352), w sposób użyteczny i efektywny, stanowią zbiór, zwany dalej zasobem informacyjnym, i są udostępniane w centralnym repozytorium.

W języku potocznym funkcjonuje sformułowanie „To wszelkiego rodzaju użyteczne dane, informacje i wiedza potrzebne do skutecznego podejmowania decyzji"[5]. Na potrzeby artykułu przyjęto następujące określenie: Zasoby informacyjne organizacji to jej *aktywa intelektualne*, będące sumą wiedzy pracowników lub wydzielonych grup (struktur) pracowników, które organizacja wykorzystuje w swoich działaniach biznesowych, korzystając z aktualnie dostępnych technologii. Aktywa te mogą mieć charakter danych, informacji lub wiedzy (rysunek 2). Nośnikiem zasobu informacyjnego może być: papier, elektronika lub człowiek.

[5] R.W. Griffin, *Podstawy Zarządzania Organizacjami*, WN PWN, Warszawa 2010, s. 5.



Rysunek 2. Podstawowe elementy organizacji, kapitał intelektualny, zasoby informacyjne oraz powiązania między nimi

Źródło: opracowanie własne.

3. Modele oceny ryzyka

Odbiegając od wszelkich prób zdefiniowania pojęcia ryzyka, jego postrzeganie w dużym uproszczeniu oznacza:

- perspektywę konsekwencji wynikających z podjętych decyzji,
- zagrożenie, iż technologie, na przykład informacyjna czy informatyczna, stosowane w danej organizacji (niezależnie od jej rodzaju i skali działalności):
  a) nie spełniają wymogów biznesowych,
  b) nie zostały odpowiednio wdrożone i nie działają zgodnie z założeniami,
  c) nie zapewniają odpowiedniej integralności, bezpieczeństwa oraz dostępności zasobów informacyjnych,
  d) nie spełniają wymogów zawartych w politykach, takich jak: polityka bezpieczeństwa, polityka jakości, polityka ciągłości działania itp., a jednocześnie może być miarą zagrożenia:
- zaistniałych zdarzeń,
- wystąpienia sytuacji,
- utrzymania przypisanych cech lub właściwości.

Dobrze ukierunkowane i systematyczne zapobieganie jest najlepszym działaniem, mającym na celu uniknięcie skutków potencjalnych zagrożeń oraz zwiększenie szans na osiągnięcie wyższej efektywności bądź też skuteczne realizowanie celów organizacji. Przyjęcie odpowiedniej definicji pojęcia ryzyka zasobów informacyjnych oraz jego modelu stanowi punkt wyjścia do wskazania wszelkich metod oceny ryzyka oraz zarządzania jego poziomem.

W literaturze fachowej opisane są liczne modele oceny ryzyka, opierające się na normach, doświadczeniach czy wiedzy eksperckiej. Podstawą ich specyfikacji jest liczba składowych uwzględnionych w procesie oceny ryzyka. Pierwszą i jednocześnie podstawową składową jest szeroka lista ryzyk lub rejestr ryzyk, które będą wpływały na zdefiniowane cele modelowania – bez względu na to, czy ich źródła znajdują się pod kontrolą organizacji, czy też nie.

Drugą składową są sprecyzowane kryteria oceny ryzyka, które będą wykorzystane na etapie analizy i szacowania ryzyka, a później jego ewaluacji. Najczęściej do zbioru tych kryteriów zalicza się między innymi:

- definicje konsekwencji (charakter i rodzaj oraz sposób pomiaru),
- definicje prawdopodobieństw (rodzaj oraz sposób pomiaru),
- kategorie poziomu ryzyka (sposób ustalenia),
- kategorie ewaluacji (określenie poziomu ryzyka akceptowalnego lub tolerowanego).

Kolejnym elementem mogą być modele dziedzinowe, na przykład bezpieczeństwa informacji, bezpieczeństwa teleinformatycznego czy ciągłości działania organizacji. Modele te stanowią „dobry" punkt wyjścia do konstrukcji wieloskładnikowych[6] modeli oceny ryzyka.

3.1. Dwuskładnikowy model oceny ryzyka

Za normą ISO/IEC Guide 73:2002, jako model oceny ryzyka, można przyjąć:

$$\mathcal{R} = \mathbf{P(z)} \cdot \mathbf{S(z)} \tag{1}$$

kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji.

W myśl tej definicji określanie poziomu ryzyka dla zasobu informacyjnego sprowadza się do przypisania danemu zagrożeniu prawdopodobieństwa oddziaływania na zasób informacyjny oraz ustalenia wpływu materializacji zagrożenia na poszczególne atrybuty bezpieczeństwa: dostępności, integralności, poufności, niezaprzeczalności a następnie wyznaczenia poziomu/wartości ryzyka. Poziom ryzyka można wyznaczyć według następującego wzoru:

$$R_p = P \times \left(S_d + S_i + S_p + S_n \right), \tag{2}$$

gdzie:

[6] Nazwa pochodzi od liczby zmiennych decyzyjnych branych pod uwagę w procesie oceny ryzyka.

R_p – pierwotny poziom ryzyka – poziom ryzyka przed zastosowaniem środka sterowania ryzykiem w postaci zabezpieczenia, dobranego adekwatnie do charakteru tego ryzyka.
P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,

$$P \in \{0, 1, 2, 3, 4\},$$

przy czym: 0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje), 1 – zdarzenie prawie nieprawdopodobne, 2 – zdarzenie mało prawdopodobne, 3 – zdarzenie wysoce prawdopodobne, 4 – zdarzenie niemal pewne.
S_d – wartość przypisana skutkowi dla dostępności zasobu,
S_i – wartość przypisana skutkowi dla integralności zasobu,
S_p – wartość przypisana skutkowi dla poufności zasobu,
S_n – wartość przypisana skutkowi dla niezaprzeczalności,

gdzie: $$\left(S_d, S_i, S_p, S_n\right) \in \{0, 1, 2, 3, 4\},$$

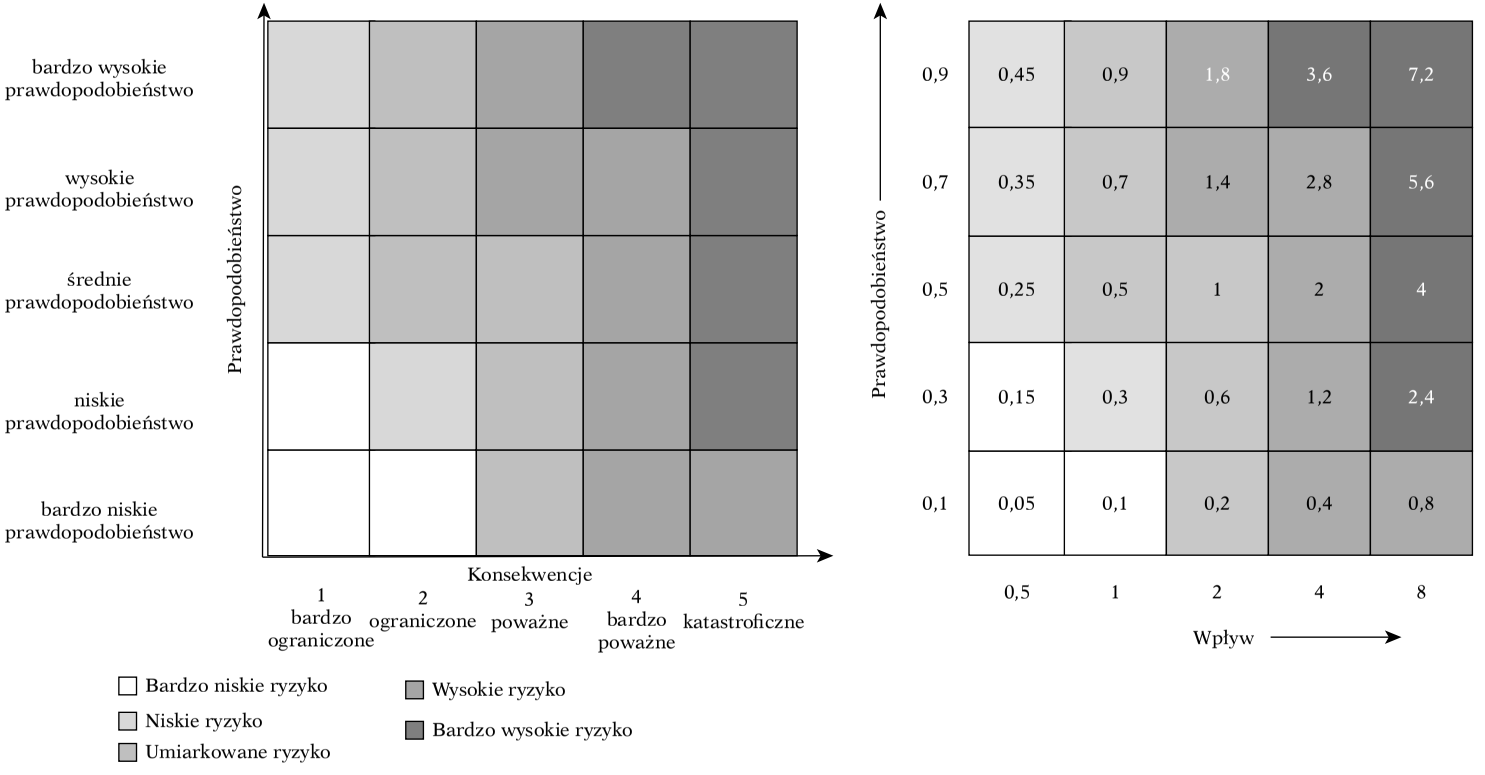
przy czym: 0 – zdarzenie nie powoduje skutku (brak podatności), 1 – zdarzenie wywołuje niewielki skutek, 2 – zdarzenie wywołuje znaczący skutek, 3 – zdarzenie wywołuje bardzo znaczący skutek, 4 – zdarzenie wywołuje skutek katastrofalny.

W świetle tej definicji ocena ryzyka polega na porównaniu wyznaczonych poziomów ryzyka z ustalonymi wstępnie kryteriami akceptowania ryzyka i umożliwia ustalenie priorytetów w zarządzaniu ryzykiem. Kryteria akceptacji ryzyka ustala dany podmiot (np. Kierownik jednostki organizacyjnej). Kryteria i kompetencje w zakresie akceptacji ryzyka zatwierdza również Kierownik podmiotu.

Analiza ryzyka sprowadza się do wykorzystania tzw. Matryc Ryzyka jako narzędzi ewaluacji ryzyka. Składają się one z dwóch połączonych (najczęściej pięciostopniowych) skali: prawdopodobieństwa i skutków, pozwalając na określenie poziomu akceptowalności danego ryzyka (rysunek 3). Bardzo często Matryca Ryzyka stanowi podstawę dla planowania oraz wdrażania środków ograniczających ryzyko.

Ryzyka, które na poziomie oceny nie zostały uznane za ryzyka szczątkowe, podlegają procedurze postępowania z ryzykiem. Postępowanie z ryzykiem może polegać na:

1) wpływaniu na zmianę poziomu ryzyka poprzez zastosowanie zabezpieczenia,
2) unikaniu ryzyka,
3) przeniesieniu ryzyka,
4) akceptacji ryzyka, mimo że jego poziom przekracza poziom ryzyka szczątkowego.



Rysunek 3. Przykładowa matryca ryzyka

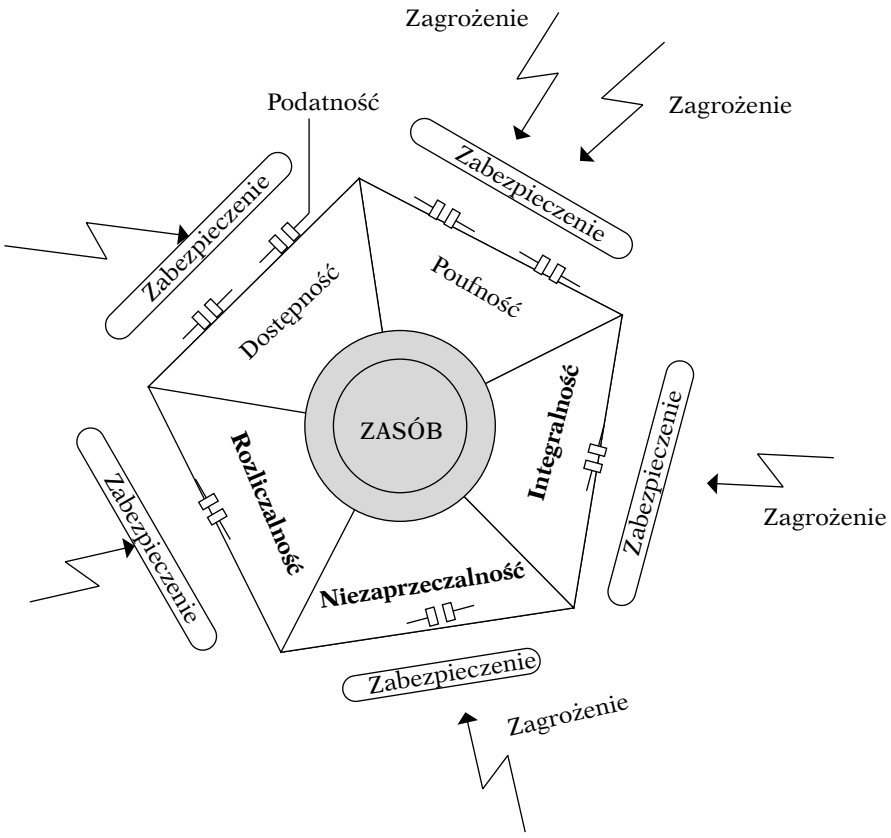
Źródło: opracowanie własne.

3.2. Trójskładnikowy model oceny ryzyka

Podstawowymi elementami trójskładnikowego modelu oceny ryzyka są:

1. Rejestr zasobów informacyjnych podlegających ochronie,
2. Model bezpieczeństwa zasobu informacyjnego,
3. Rejestr możliwych do zaimplementowania mechanizmów bezpieczeństwa – zabezpieczeń technicznych i organizacyjnych.

Punktem wyjścia do konstrukcji trójskładnikowego modelu oceny ryzyka, zapewniającym kompletność prezentowanego podejścia, jest model bezpieczeństwa zasobu informacyjnego przedstawiony na rysunku 4.



Rysunek 4. Model bezpieczeństwa zasobu informacyjnego

Źródło: opracowanie własne.

Zaprezentowany na rysunku 4 model bezpieczeństwa zasobu informacyjnego oparty jest na następujących elementach bezpieczeństwa:

1. Zasób informacyjny podlegający ochronie wraz z przypisanymi atrybutami bezpieczeństwa (z),
2. Wycena zasobu w aspekcie ewentualnych strat w przypadku utraty przypisanych atrybutów bezpieczeństwa (WS),
3. Zbiór typowych zagrożeń dla zasobu (zaleca się zwrócenie szczególnej uwagi na źródła zagrożeń osobowych (Z),
4. Zbiór podatności zasobu na zagrożenia w różnych obszarach bezpieczeństwa (P),
5. Zbiór aktualnie przypisanych do zasobu mechanizmów bezpieczeństwa – zabezpieczeń (Z).

Na podstawie powyższych zbiorów realizacje produktu kartezjańskiego $\langle WS, \mathbb{P}, \mathbb{Z} \rangle$ odzwierciedlają potencjalne stany (sytuacje) zasobu informacyjnego z punktu widzenia możliwości utraty przypisanych mu atrybutów bezpieczeństwa.

Jako model ryzyka przyjmuje się odwzorowanie:

$$\mathcal{R} : \langle WS, \mathbb{P}, \mathbb{Z} \rangle \rightarrow \mathcal{N}, \tag{3}$$

gdzie: N jest zbiorem dopuszczalnych wartości oceny ryzyka zasobu informacyjnego. Przykładowy zbiór potencjalnych wartości ryzyka przedstawia poniższa tabela.

Tabela 1. Tabela ryzyka

Tabela ryzyka	Możliwość zagrożenia	Niskie(N)			Średnie (Ś)			Wysokie(W)		
	Łatwość wykorzystania	N	S	W	N	S	W	N	S	W
Wartość zasobu (poziom strat)	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9
	6	6	7	8	7	8	9	8	9	10
	7	7	8	9	8	9	10	9	10	11
	8	8	9	10	9	10	11	10	11	12
	9	9	10	11	10	11	12	11	12	13

Źródło: opracowanie własne.

Sposób wyznaczania oceny ryzyka odzwierciedla rysunek 5, składający się z czterech tabel.

Przykład wyceny zagrożeń przez ekspertów w stosunku do zasobu

Zasób informacyjny XXX Nazwa zagrożenia dla zasobu	Wpływ zagrożenia na atrybut bezpieczeństwa	Ocena eksperta 1	Ocena eksperta 2	Ocena eksperta 3	Ocena eksperta 4	Ocena eksperta 5	Ocena średnia dla danego zagrożenia
Naruszenie prawa/ustaw	Poufność	W	W	S	W	W	W
Kradzież nośnika z danymi	Poufność, dostępność, integralność	W	S	S	S	W	S
Zniszczenie danych	Poufność, niezaprzeczalność	N	S	S	S	S	S
Odtworzenie z wyrzuconych danych	Poufność, dostępność, integralność	W	S	S	S	W	W
Dane z niewiarygodnych źródeł	Poufność, dostępność, integralność, niezaprzeczalność	N	S	N	N	S	N
Ocena zagrożenia dla zasobu informacyjnego							S

Przykład wyceny podatności przez ekspertów w stosunku do zasobu

Zasób informacyjny XXX Nazwa podatności dla zasobu	Ocena eksperta 1	Ocena eksperta 2	Ocena eksperta 3	Ocena eksperta 4	Ocena eksperta 5	Ocena średnia dla danej podatności
Niezabezpieczone urządzenia do przechowywania danych	S	W	S	W	S	W
Brak procedur niszczenia nośników danych	W	S	S	S	W	S
Niekontrolowane kopiowanie	W	S	W	W	S	W
Brak wylogowania przy opuszczaniu stacji roboczej	W	S	S	S	W	S
Zastosowanie programów aplikacyjnych do nieaktualnych danych	W	S	W	W	S	W
Ocena podatności dla zasobu informacyjnego						W

Przykład mapy ryzyka

Tabela ryzyka	Możliwość zagrożenia	Niskie(N)			Średnie (Ś)			Wysokie(W)		
	Łatwość wykorzystania	N	S	W	N	S	W	N	S	W
Wartość zasobu (poziom strat)	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9
	6	6	7	8	7	8	9	8	9	10
	7	7	8	9	8	9	10	9	10	11
	8	8	9	10	9	10	11	10	11	12
	9	9	10	11	10	11	12	11	12	13

Przykład wartościowania zasobu

Nazwa zasobu XXX	Koszty finansowe		Koszty pozafinansowe			
Atrybut bezpieczeństwa zasobu	Strata finansowa	Pogorszenie wydajności działalności finansowej	Naruszenie przepisów prawa	Naruszenie ochrony danych osobowych	Utrata wizerunku	Inne
Poufność	0	0	0,5	1	0,5	0
Dostępność	0,5	0,5	0	0	0,5	0
Integralność	0,5	0	0	0	0	0
Niezaprzeczalność	0	0,5	0	0	0	0,5
Suma według kryterium	1	1	0,5	1	1	1
Wartość aktywu	5					

Rysunek 5. Schemat wyznaczania wartości ryzyka dla zasobu informacyjnego

Źródło: opracowanie własne.

W praktyce uważa się, że zasób informacyjny jest bezpieczny, gdy ma zachowane/spełnione następujące atrybuty bezpieczeństwa:

- Poufność – właściwość zapewniająca, że informacja nie jest udostępniana nieautoryzowanym osobom, podmiotom lub procesom.
- Dostępność – właściwość zapewniająca, że zasób jest osiągalny i może być wykorzystany na żądanie.
- Integralność – właściwość zapewniająca, że zasób informacyjny nie został zmieniony lub zniszczony w sposób nieautoryzowany lub własność zasobu informacyjnego wykluczająca wprowadzenie do niego zmian w nieautoryzowany sposób.
- Niezaprzeczalność/adresowalność – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w wymianie.
- Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być jednoznacznie przypisane tylko temu podmiotowi.

Podstawowym procesem kontrolującym atrybuty bezpieczeństwa jest audyt: powtarzalny, obiektywny, oparty na jasnych metrykach. Do stwierdzenia, czy przypisany do zasobu informacyjnego atrybut bezpieczeństwa jest zachowany, należy wykorzystać dwie wielkości: wartość ryzyka szczątkowego[7] oraz wartość ryzyka akceptowalnego[8]. Jeśli wartość ryzyka szczątkowego jest mniejsza od wartości ryzyka akceptowalnego, to uważa się, że atrybut bezpieczeństwa jest zachowany/spełniony.

4. Wieloaspektowy model oceny ryzyka

Podstawowymi elementami wieloaspektowego modelu oceny ryzyka są:

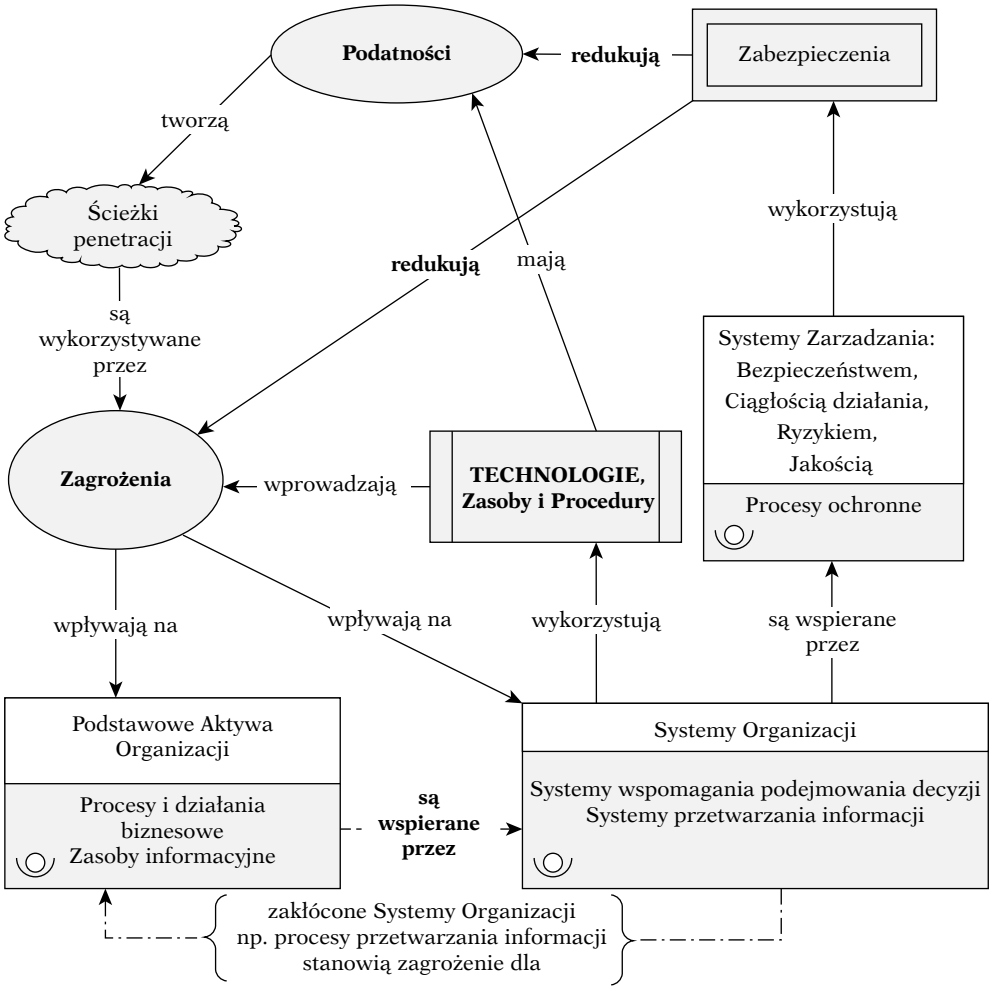
1. Rejestr zasobów informacyjnych podlegających ochronie,
2. Podstawowe obszary działania, w których organizacja narażona jest na zagrożenia (rysunek 1),
3. Rejestry: czynników zagrożeń jakości zasobów informacyjnych w myśl normy ISO 9001:2015; czynników zagrożeń bezpieczeństwa informacji w myśl

[7] Ryzyko szczątkowe (rezydualne, reliktowe, ang. *residual risk*) – pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem. Źródło: ISO Guide 73:2009 Risk Managment – Vocabulary, definicja 3.8.1.6.

[8] Ryzyko akceptowalne – wielkość ryzyka, którą organizacja może zaakceptować bez żadnych dodatkowych działań zaradczych bądź zmian w funkcjonowaniu.

normy ISO serii 27000:2015; czynników zagrożeń ryzyka w myśl normy ISO 31000 w zakresie zarządzania ryzykiem; czynników zagrożeń ciągłości działania w myśl normy ISO 22301 dotyczącej ciągłości działania organizacji, innych czynników zagrożeń,

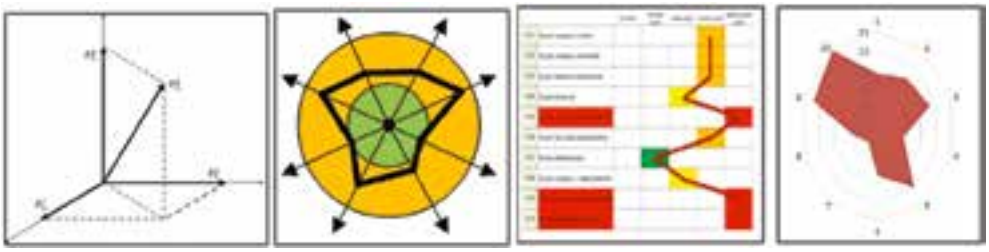
4. Podstawowe elementy bezpieczeństwa informacji (rysunek 6),
5. Sposoby wizualizacji wartości ryzyka (rysunek 7).



Rysunek 6. Podstawowe elementy bezpieczeństwa zasobów informacyjnych i powiązania między nimi

Źródło: opracowanie własne.

Do pozyskania wyżej wymienionych grup informacji wykorzystywane są różnorodne modele, metody, techniki i narzędzia, bazujące na wiedzy i doświadczeniu osób zarządzających. W tym miejscu warto podkreślić dość niski poziom zaangażowania i wiedzy w organizacjach z zakresu modelowania, gdzie wynikiem tego procesu są wieloaspektowe/wielowymiarowe modele oceny ryzyka oraz innowacyjne instrumenty zarządzania ryzykiem. Stanowi ono również dla wielu organizacji nie lada wyzwanie.



Rysunek 7. Podstawowe sposoby wizualizacji wartości ryzyka
Źródło: opracowanie własne.

Konstrukcja modelu składa się z dwóch etapów: najpierw dokonywana jest **identyfikacja czynników ryzyka** występujących we wszystkich podstawowych elementach organizacji (rysunek 1), a dopiero **później stopnia ich** oddziaływania. Istotnym jest, by na etapie identyfikacji ryzyka nie brać pod uwagę miar dla oceny poszczególnych zdarzeń – czynników ryzyka ani prawdopodobieństwa ich wystąpienia. Określenie stopnia niepewności winno być następnym etapem. Tak wyraźne oddzielenie czynności poznawczej, jaką jest identyfikacja zagrożeń oraz technicznej, jaką jest ich pomiar ma swój bardzo głęboki sens.

Jako model ryzyka zasobu informacyjnego, proponowany w niniejszej pracy, przyjmujemy wektor $\overrightarrow{R_{Z_i}}$ określony następująco:

$$\overrightarrow{R_{Z_i}} = \left\langle \overrightarrow{R^1_{Z_i}},\ \ldots, \overrightarrow{R^j_{Z_i}},\ \ldots,\ \overrightarrow{R^J_{Z_i}} \right\rangle \in M_{\mathrm{m\times n}} \ldots \times M_{\mathrm{m\times n}} \ldots \times M_{\mathrm{m\times n}}, \tag{4}$$

gdzie: $\overrightarrow{R^j_{Z_i}} \in M_{\mathrm{m\times n}}$ – współrzędna wektora $\overrightarrow{R_{Z_i}}$ charakteryzująca wybrany aspekt bezpieczeństwa zasobu informacyjnego Z_i, będąca kombinacją liniową

$$\overrightarrow{R^j_{Z_i}} = \xi_{\alpha^1}\left(\alpha^1_{Z_i}\right)\cdot\overrightarrow{\alpha^1} + \xi_{\alpha^2}\left(\alpha^2_{Z_i}\right)\cdot\overrightarrow{\alpha^2} + \ldots + \xi_{\alpha^j}\left(\alpha^{M^j}_{Z_i}\right)\cdot\overrightarrow{\alpha^{M^j}} \tag{5}$$

czynników ryzyka zasobu informacyjnego Z_i w bazie przestrzeni liniowej $(M_{\mathrm{m\times n}}, R, +, \cdot)$.

Mając na uwadze wymagania dotyczące objętości artykułu dalsze rozważania zostaną ograniczone do pięciu składowych, rozumianych jako przykładowe. Prezentowane podejście bierze pod uwagę następujące kategorie czynników ryzyka: bezpieczeństwa (B), ciągłości działania (C), technologii informacyjnej (T), złożoności (S) oraz jakości (J). Zatem jako model ryzyka zasobu informacyjnego przyjmujemy:

$$\overrightarrow{R_{Z_i}} = \left\langle \overrightarrow{R^B_{Z_i}},\ \overrightarrow{R^C_{Z_i}},\ \overrightarrow{R^T_{Z_i}},\ \overrightarrow{R^S_{Z_i}},\ \overrightarrow{R^J_{Z_i}} \right\rangle \in M_{\mathrm{m\times n}} \times M_{\mathrm{m\times n}} \times M_{\mathrm{m\times n}}, \times M_{\mathrm{m\times n}} M_{\mathrm{m\times n}}, \tag{6}$$

gdzie:

- $\mathrm{M_{m\times n}}$ – macierz o rozmiarach m x n, w niniejszym artykule przyjęto macierze kwadratowe 2 × 2, czyli m=2 i n=2,
- $\overrightarrow{R^B_{Z_i}}$ – współrzędna wektora $\overrightarrow{R_{Z_i}}$ charakteryzująca aspekt bezpieczeństwa informacji dla zasobu informacyjnego Z_i, będąca kombinacją liniową czynników ryzyka zasobu informacyjnego Z_i w bazie przestrzeni liniowej $(M_{2\times 2}, \boldsymbol{R}, +, \cdot)$,
- $\overrightarrow{\mathrm{R}^{\mathrm{C}}_{\mathrm{Z_i}}}$ – współrzędna wektora $\overrightarrow{\mathrm{R}_{\mathrm{Z_i}}}$ charakteryzująca aspekt ciągłości działania zasobu informacyjnego Z_i, będąca kombinacją liniową czynników ryzyka zasobu informacyjnego Z_i w bazie przestrzeni liniowej $(M_{2\times 2}, \boldsymbol{R}, +, \cdot)$,
- $\overrightarrow{\mathrm{R}^{\mathrm{T}}_{\mathrm{Z_i}}}$ – współrzędna wektora $\overrightarrow{\mathrm{R}_{\mathrm{Z_i}}}$ charakteryzująca aspekt technologii informatycznej procesów przetwarzania zasobu informacyjnego Z_i, będąca kombinacją liniową czynników ryzyka zasobu informacyjnego Z_i w bazie przestrzeni liniowej $(\mathrm{M}_{2\times 3}, \mathrm{R}, +, \cdot)$,
- $\overrightarrow{\mathrm{R}^{\mathrm{S}}_{\mathrm{Z_i}}}$ – współrzędna wektora $\overrightarrow{\mathrm{R}_{\mathrm{Z_i}}}$ charakteryzująca aspekt złożoności zasobu informacyjnego Z_i, będąca kombinacją liniową czynników ryzyka zasobu informacyjnego Z_i w bazie przestrzeni liniowej $(\mathrm{M}_{2\times 3}, \mathrm{R}, +, \cdot)$,
- $\overrightarrow{\mathrm{R}^{\mathrm{J}}_{\mathrm{Z_i}}}$ – współrzędna wektora $\overrightarrow{\mathrm{R}_{\mathrm{Z_i}}}$ charakteryzująca aspekt jakości zasobu informacyjnego Z_i, będąca kombinacją liniową czynników ryzyka zasobu informacyjnego Z_i w bazie przestrzeni liniowej $(\mathrm{M}_{2\times 3}, \mathrm{R}, +, \cdot)$.

$(\mathrm{M_{m\times n}}, \mathrm{R}, +, \cdot)$ – przestrzeń wektorowa określona jako zbiór macierzy $\mathrm{M^{m\times n}}$ z operatorem dodawania macierzy + i operatorem zewnętrznym · jest przestrzenią wektorową nad ciałem liczb rzeczywistych R, przy czym:

$$\overrightarrow{R^B_{z_i}} = \xi_\lambda\left(\lambda_{z_i}\right)\cdot\vec{\lambda} + \xi_\alpha\left(\alpha_{z_i}\right)\cdot\vec{\alpha} + \xi^B_\eta\left(\eta^B_{z_i}\right)\cdot\overrightarrow{\eta^B} + \xi^B_\beta\left(\beta^B_{z_i}\right)\cdot\overrightarrow{\beta^B}, \tag{7}$$

$$\overrightarrow{R^C_{z_i}} = \xi_\kappa\left(\kappa_{z_i}\right)\cdot\vec{\kappa} + \xi_\pi\left(\pi_{z_i}\right)\cdot\vec{\pi} + \xi^C_\eta\left(\eta^C_{z_i}\right)\cdot\overrightarrow{\eta^C} + \xi^C_\beta\left(\beta^C_{z_i}\right)\cdot\overrightarrow{\beta^C}, \tag{8}$$

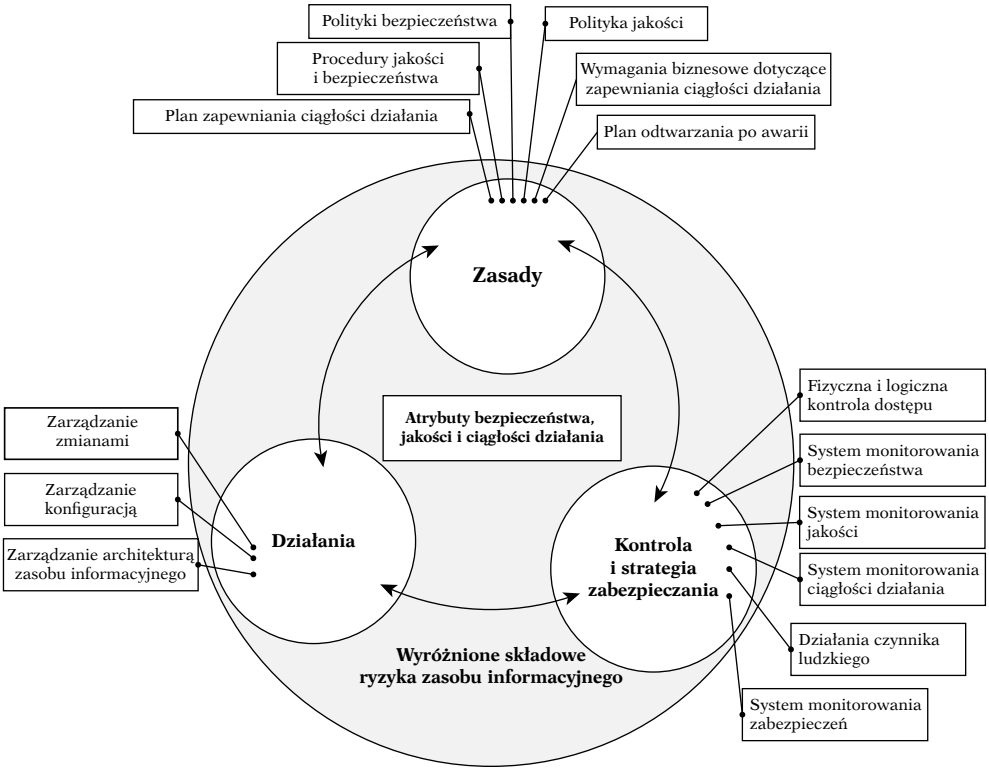
$$\overrightarrow{R^T_{z_i}} = \xi_\vartheta\left(\vartheta_{z_i}\right)\cdot\vec{\vartheta} + \xi_\zeta\left(\zeta_{z_i}\right)\cdot\vec{\zeta} + \xi^T_\eta\left(\eta^T_{z_i}\right)\cdot\overrightarrow{\eta^T} + \xi^T_\beta\left(\beta^T_{z_i}\right)\cdot\overrightarrow{\beta^T}, \tag{9}$$

$$\overrightarrow{R^S_{z_i}} = \xi_\mu\left(\mu_{z_i}\right)\cdot\vec{\mu} + \xi_\rho\left(\rho_{z_i}\right)\cdot\vec{\rho} + \xi^S_\eta\left(\eta^S_{z_i}\right)\cdot\overrightarrow{\eta^S} + \xi^S_\beta\left(\beta^S_{z_i}\right)\cdot\overrightarrow{\beta^S}, \tag{10}$$

$$\overrightarrow{R^J_{z_i}} = \xi_\sigma\left(\sigma_{z_i}\right)\cdot\vec{\sigma} + \xi_\varrho\left(\varrho_{z_i}\right)\cdot\vec{\varrho} + \xi^J_\eta\left(\eta^J_{z_i}\right)\cdot\overrightarrow{\eta^J} + \xi^J_\beta\left(\beta^J_{z_i}\right)\cdot\overrightarrow{\beta^J}, \tag{11}$$

gdzie:

- $\xi_\lambda\left(\lambda_{z_i}\right),\ldots,\ \xi^J_\beta\left(\beta^J_{z_i}\right)$ – wielkości odzwierciedlające wpływ poszczególnych czynników ryzyka na wartość ryzyka zasobu informacyjnego Z_i w danym obszarze. Punktem wyjścia do opracowania wymaganego zbioru funkcji normalizacji jest przyjęty model bezpieczeństwa zasobów informacyjnych (rysunek 8). Przykładowe postacie tych funkcji zawiera tabela 2.
- $\vec{\lambda}, \vec{\alpha}, \overrightarrow{\eta^B}, \overrightarrow{\eta^C}, \overrightarrow{\eta^T}, \overrightarrow{\eta^S}, \overrightarrow{\eta^J}, \overrightarrow{\beta^B}, \overrightarrow{\beta^C}, \overrightarrow{\beta^T}, \overrightarrow{\beta^S}, \overrightarrow{\beta^J}, \vec{\kappa}, \vec{\pi}, \vec{\vartheta}, \vec{\zeta}, \vec{\mu}, \vec{\sigma}, \vec{\rho}, \vec{\varrho}$ – wektory bazowe przestrzeni wektorowej $(M_{2\times2}, \boldsymbol{R}, +, \cdot)$ z algebry $(M_{m\times n}, \boldsymbol{R}, +, \cdot, \otimes)$.



Rysunek 8. Model bezpieczeństwa zasobów informacyjnych

Źródło: opracowanie własne na podstawie: M. Ryba, J. Sulwiński, *„Siedem grzechów głównych" – analizy stanu infrastruktury teleinformatycznej z perspektywy bezpieczeństwa*, „TeleInfo" 2005, vol. 26.

Ponieważ wymiar algebry $(M_{2\times2}, \boldsymbol{R}, +, \cdot, \otimes)$[9] wynosi: dim $(M_{2\times2}, \boldsymbol{R}, +, \cdot, \otimes) = 4$, zatem dla określenia składowych $(\overrightarrow{R^B_{Z_i}}, \overrightarrow{R^C_{Z_i}}, \overrightarrow{R^T_{Z_i}}, \overrightarrow{R^S_{Z_i}}, \overrightarrow{R^J_{Z_i}})$ istnieje 20 wektorów bazowych zdefiniowanych następująco:

$$\vec{\lambda} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};\ \vec{\alpha} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ \overrightarrow{\eta^B} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix};\ \overrightarrow{\beta^B} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\vec{\kappa} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};\ \vec{\pi} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ \overrightarrow{\eta^C} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix};\ \overrightarrow{\beta^C} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\vec{\upsilon} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};\ \vec{\zeta} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ \overrightarrow{\eta^T} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix};\ \overrightarrow{\beta^T} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\vec{\mu} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};\ \vec{\rho} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ \overrightarrow{\eta^S} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix};\ \overrightarrow{\beta^S} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\vec{\sigma} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};\ \vec{\varrho} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ \overrightarrow{\eta^J} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix};\ \overrightarrow{\beta^J} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Tabela 3. Przykładowe postacie funkcji normalizacji

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

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

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.

Postać wyżej przedstawionych w tabeli funkcji normalizacji z rodziny Ξ określona została w taki sposób, aby odwzorować ich wartości na odpowiednie przedziały oraz aby zachować właściwe proporcje ich wpływu na ryzyko systemu informacyjnego.

Z kombinacji liniowej powyższych wzorów wynika, że wpływ wszystkich, wyróżnionych wymiarów/czynników analizy ryzyka zasobu informacyjnego Z_i na poszczególne współrzędne ($\overrightarrow{R_{Z_i}^B}$, $\overrightarrow{R_{Z_i}^C}$, $\overrightarrow{R_{Z_i}^T}$, $\overrightarrow{R_{Z_i}^S}$, $\overrightarrow{R_{Z_i}^J}$) wektora ryzyka $\overrightarrow{R_{Z_i}}$ jest jednakowy. W celu uszczegółowienia oszacowania poziomu ryzyka zasobu informacyjnego Z_i może być konieczne przypisanie zarówno poszczególnym współrzędnych wektora, jak i i składowym ryzyka wag ich wpływu na końcowy poziom ryzyka zasobu informacyjnego Z_i oraz modyfikacja współrzędnych wektora ryzyka $\overrightarrow{R_{Z_i}} \in M_{m\times n} \times M_{m\times n} \times M_{m\times n}$ z wykorzystaniem tych wag wpływu. W artykule to zagadnienie zostało pominięte.

Wielkość ryzyka systemu informacyjnego można określić jako moduł wektora:

$$\overrightarrow{R_{Z_i}} = \sqrt[2]{R_{Z_i}^{B2} + R_{Z_i}^{C2} + R_{Z_i}^{T2}}. \tag{12}$$

Poniżej przywołano przykładową legendę do oceny istotności ryzyka $\left|\overrightarrow{R_{Z_i}}\right|$.

- ryzyko akceptowalne (1–16 pkt) – to ryzyko niskie, nieznaczne, które może powodować krótkotrwałe, niewielkie zakłócenia w działalności organizacji, stanowi najniższe zagrożenie dla realizacji celów i zadań organizacji; nie jest wymagane podejmowanie dodatkowych działań przeciwdziałających ryzyku; ryzyko podlega monitorowaniu oraz nadzorowi nad wdrożonymi mechanizmami kontrolnymi i zabezpieczającymi;
- ryzyko warunkowo akceptowalne (17–36 pkt) – to ryzyko średnie, które wywołuje średnie zakłócenia w działalności organizacji, wymaga monitorowania i podjęcia ewentualnych działań mających na celu minimalizację ryzyka, prawdopodobieństwa i/lub skutków jego wystąpienia;
- ryzyko istotne (37–60 pkt) – to ryzyko wysokie, które wywołuje zakłócenia w działalności organizacji, wymaga szczególnego monitorowania; może wymagać zastosowania dodatkowych mechanizmów kontrolnych i zabezpieczających lub przygotowania nowych uregulowań wewnętrznych oraz podjęcia działań tak zwanej reakcji na ryzyko w celu zmniejszenia danego ryzyka do poziomu akceptowalnego;
- ryzyko krytyczne (61–100 pkt) – to ryzyko bardzo wysokie, które charakteryzuje wysokie prawdopodobieństwo jego zmaterializowania się; stanowi najwyższe zagrożenia dla realizacji celów i zadań organizacji, bezwzględnie wymaga podjęcia dodatkowych działań mających na celu minimalizację prawdopodobieństwa albo skutków jego wystąpienia, opracowania metod działania tzw. reakcji na ryzyko i wdrożenia mechanizmów bezpieczeństwa oraz ciągłego monitorowania.

4. Podsumowanie i kierunki dalszych badań

Model oceny ryzyka zasobów informacyjnych jest jednym z najważniejszych etapów całego procesu zarządzania ryzykiem w bezpieczeństwie informacji. Świadomość czynników mogących zakłócić działalność systemu informacyjnego w przedsiębiorstwie stanowi podstawowy element podejścia do problematyki ryzyka. Zastosowanie prawidłowo skonstruowanego wieloaspektowego modelu ryzyka zasobu informacyjnego stanowi duże ułatwienie i wsparcie dla organizacji, które przystępują do tej tematyki inspirowane normą ISO 31000 czy też koniecznością spełnienia wymagań dla systemów zarządzania bezpieczeństwem informacji opisanego w ISO serii 27000:2015, systemów zarządzania ciągłością

działania opisanego w ISO 22301 czy też systemu zarządzania jakością opisanego w znowelizowanej normie ISO 9001:2015. Wiedza o ryzyku występującym w procesie przetwarzania zasobów informacyjnych oraz zastosowanym modelu jego oceny pozwala na odpowiednie kształtowanie tego procesu, tak aby poziom bezpieczeństwa w nim osiągnął akceptowalny poziom. Analizując źródła i kategorie ryzyka w procesach przetwarzania informacji, należy przede wszystkim brać pod uwagę kontekst organizacji, jej charakterystykę, architekturę, cykl życia samej organizacji oraz zasobów intelektualnych.

Rozważania zawarte w niniejszym artykule mają przede wszystkim znaczenie poznawcze i stąd pominięto opis niektórych zagadnień. Zamiarem było pokazanie koncepcji innego niż tradycyjne spojrzenia na problemy kwantyfikacji zagrożenia i ryzyka. Z uwagi na różnorodność czynników i szerokie spektrum ich oddziaływań na procesy przetwarzania informacji, zastosowanie właściwego modelu ryzyka powinno być nieodłącznym elementem systemu zarzadzania ryzykiem oraz procesu podejmowania decyzji i planowania wariantów funkcjonowania każdej jednostki organizacyjnej.

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, 2016, 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.

Griffin R.W., *Podstawy Zarządzania Organizacjami*, WN PWN, Warszawa 2010.

Kaucz A.J., Kiedrowicz M., Skinder-Pik M., *Gromadzenie i przetwarzanie danych mających związek ze zwalczaniem przestępczości finansowej. Zasady dostępu, ograniczenia prawne*, WAT, Warszawa 2016.

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.

Kiedrowicz M., *Objects identification in the information models used by information systems*, w: *Geographic Information Systems Conference And Exhibition – GIS ODYSSEY 2016*, Perugia 2016, s. 129–136.

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

Ryba M., Sulwiński J., *„Siedem grzechów głównych" – analizy stanu infrastruktury teleinformatycznej z perspektywy bezpieczeństwa*, „TeleInfo" 2005, vol. 26.

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., *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., Protasowicki T., *Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego*, w: Kosiuczenko P., Śmiałek M., Swacha J., *Od procesów do oprogramowania: badania i praktyka*, KKIO 2015, PTI, Warszawa 2015, s. 27–44.

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., 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.

Wróblewski D., Połeć B., *Teoria i praktyka zarządzania ryzykiem – normy a regulacje w prawie miejscowym*, w: *Zarządzanie kryzysowe w wymiarze lokalnym. Organizacja, procedury, organy i instytucje*, D. Majchrzak (red.), AON, Warszawa 2014, s. 206.

* * *

Multifaceted Risk Model of Information Resource Assessment

Summary

The subject of the article is the concept of a five-dimensional risk model (BCTSJ) of an information resource system. This model, using the dimensions of Safety (B), Continuity (C), Technology (T), Complexity (S) and Quality (J), takes into account the different categories and types of risk factors that result from the complexity or structure of the information resource itself. It also includes elements of the attractiveness and environment of the processing of information resources in the process of reviewing or measuring the amount of information resource risk. The model presented in this article may be the starting point for developing a risk assessment method for information resources, appropriate policies, such as concerning information security organization or quality, which in turn can be inputs to developing information management, risk management methods or IT systems to support the processing of these information resources.

Keywords: information resource, information system, risk, risk model, risk vector, risk management system.