Maciej Kiedrowicz[1]

Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych

1. Wstęp

W ostatnim czasie pojęcie oceny ryzyka zyskało na popularności w niemalże wszystkich dziedzinach życia, począwszy od biznesu przez medycynę po bezpieczeństwo informacyjne. Przedmiotem artykułu jest metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych, do przetwarzania których wykorzystywane są technologie informacyjne, szczególnie technologie IT. Celem artykułu jest prezentacja autorskiej metodyki zarządzania ryzykiem zasobów informacyjnych, uwzględniającej różne metody, modele i techniki z zakresu inżynierii ryzyka, istotnych z perspektywy zapewnienia kompletności procesu zarządzania ryzykiem w bezpieczeństwie oraz wyznaczania poziomu ryzyka zasobów informacyjnych. Na etapie opracowywania metodyki zastosowane zostały metody i narzędzia badawcze takie jak: studia literatury fachowej, krytyczna analiza dokumentów i różnych zasobów informacyjnych badanych jednostek organizacyjnych oraz rozmowy z właścicielami zasobów informacyjnych, administratorami baz danych lub systemów informatycznych. Artykuł prezentuje metodykę zarządzania ryzykiem uwzględniającą autorski model ryzyka zasobu informacyjnego oraz autorską metodę analizy i szacowania ryzyka, wiążące je w sposób pozwalający na skuteczne zarządzanie ryzykiem, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia. Elementem obiektywizacji proponowanej w niniejszej pracy metodyki jest odejście od powielania klasycznego procesu zarządzania ryzykiem i wprowadzenie dodatkowych elementów na etapach analizy, szacowania i ewaluacji ryzyka.

W pierwszej części artykułu dokonano przeglądu aktualnie dostępnych metodyk zarządzania ryzykiem, zaczerpniętych zarówno z literatury fachowej, jak i z norm serii ISO. Kolejna część zawiera opis koncepcji metodyki zarządzania ryzykiem zasobów informacyjnych. Podstawowymi elementami składowymi

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

przedstawionej metodyki są zasady, struktura ramowa oraz przegląd procesu zarządzania ryzykiem zasobów informacyjnych. Rozdział ostatni stanowi uszczegółowienie i rozwinięcie koncepcji metodyki zarządzania ryzykiem zasobów informacyjnych.

2. Przegląd metodyk zarządzania ryzykiem

W literaturze fachowej zidentyfikowano wiele metodyk zarządzania ryzykiem (tabela 1)[2]. Metodyki te są opracowane często w formie standardów, na przykład ISO/IEC 31010:2009, ISO 31000, PN-ISO/IEC 27005 lub zbioru dobrych praktyk. Ponadto metodyki opracowane są przez organizacje, niejednokrotnie na własne potrzeby, które zostały następnie zaimplementowane przez wiele instytucji, między innymi M_o_R (British Cabinet Office) czy Risk Management Methodology (European Union Agency for Network and Information Security). Metodyki zarządzania ryzykiem mogą mieć zastosowanie zarówno w stosunku do organizacji o standardowych profilach działalności, jak i o specyficznych profilach działalności. Ponadto mogą być stosowane do zarządzania ryzykiem w odniesieniu do zasobów, procesów, systemów, programów oraz projektów.

Tabela 1. Wybrane metodyki zarządzania ryzykiem i ich charakterystyka

Rodzaj metodyki	Charakterystyka
ISO 31000 Risk Management – Principles and Guidelines on Implementation – IOS	ISO 31000 zawiera podstawowe wskazówki na temat zarządzania ryzykiem. Standard może znajdować zastosowanie w przedsiębiorstwach różnego typu (prywatnych lub publicznych), zarówno w zadaniach grupowych, jak i indywidualnych. Może być stosowany do różnego rodzaju zadań, włączając w to strategie, decyzje, operacje, projekty, produkty lub usługi.
M_o_R (Management of Risk) – British Cabinet Office	Metodyka, którą można stosować na różnych poziomach organizacji – strategicznym, programu, projektu lub poziomie operacyjnym. Celem metodyki jest identyfikacja polityki zarządzania ryzykiem oraz odpowiednich strategii i planów dla programów i projektów, a następnie systematyczna identyfikacja i analiza ryzyka oraz zarządzanie nim.

[2] http://www.e-mentor.edu.pl/artykul/index/numer/64/id/1237 (dostęp: 18.06.2017).

Rodzaj metodyki	Charakterystyka
PN-ISO/IEC 27005 Zarządzanie ryzykiem w bezpieczeństwie informacji	Standard ma zastosowanie do wszystkich typów organizacji (np. przedsiębiorstw, instytucji rządowych, organizacji non-profit), które zamierzają zarządzać ryzykami mogącymi spowodować naruszenie bezpieczeństwa informacji w tych organizacjach.
COSO 2004 – Enterprise Risk Management – Integrated Framework – Committee of Sponsoring Organizations of the Treadway Commission	Standard umożliwia zarządzanie ryzykiem w przedsiębiorstwie i obejmuje następujące aspekty: powiązanie ryzyka ze strategią, ustalenie odpowiednich celów i opracowanie mechanizmów zarządzania wybranym ryzykiem; podejmowanie decyzji z uwzględnieniem ryzyka. Zarządzanie ryzykiem w przedsiębiorstwie wymusza identyfikację oraz wybór ryzyka, które najbardziej może wpłynąć na podejmowanie decyzji. Końcowym etapem zarządzania ryzykiem, zgodnie ze standardem, jest podjęcie decyzji związanej z ryzykiem – uniknięcie, zmniejszenie lub akceptacja ryzyka.
Hierarchical Holographic Modelling – Centre for Risk Management of Engineering Systems at the University of Virginia	Metodyka ukierunkowana jest na badanie różnych charakterystyk z wykorzystaniem różnych kryteriów. Poprzez analizę systemu z wykorzystaniem modeli funkcjonalnych, czasowych, geograficznych, politycznych można opracować listy ryzyka w odniesieniu do różnych części systemu. Zalety metodyki to m.in.: wskazanie ryzyka wewnętrznego i zewnętrznego, określenie ryzyka związanego z całym systemem lub poszczególnymi podsystemami; możliwość rozwiązywania niewielkich problemów różnych podsystemów
COBIT (ang. *Control Objectives for Information and related Technology*)	Jest metodyką utworzoną poprzez zbiór celów kontrolnych dla technologii informacyjnych i powiązanych. Jest to zestawienie dobrych praktyk do zarządzania IT utworzonych w 1992 r. przez stowarzyszenie ISACA oraz IT Governance Institute. Obecnie obowiązuje czwarta edycja tego pakietu.

Źródło: opracowanie własne.

Zidentyfikowano trzy rodzaje metodyk, w których zaznaczono, że jest możliwa do wykorzystania w celu zarządzania ryzykiem zasobów informacyjnych, są to następujące standardy:

- ISO 31000 Risk Management – Principles and Guidelines on Implementation,
- PN-ISO/IEC 27005 Technika informatyczna. Zarządzanie ryzykiem w bezpieczeństwie Informacji,
- COBIT (ang. *Control Objectives for Information and related Technology*).

Metodyka analizy ryzyka zawarta w normie ISO/IEC 31010 Risk Management – Risk Assessment Techniques jest przeznaczona do analizy zdarzeń związanych z awariami i nie można przetransponować ich na potrzeby systemu zarządzania ryzykiem zasobu informacyjnego. Ponadto efektem finalnym tej metodyki – etap ewaluacji – jest 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.

Zdaniem autora standardem, na bazie którego można skonstruować dość dobrą metodykę zarządzania ryzykiem zasobów informacyjnych, jest norma PN-ISO/IEC 27005, Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN 2015. Opisany w niej 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). W standardzie tym bezpieczeństwo informacji jest osiągalne przez wdrożenie właściwego zbioru zabezpieczeń, wyselekcjonowanych w trakcie wybranego procesu zarządzania ryzykiem i zarządzanego przez SZBI (System Zarządzania Bezpieczeństwem Informacji), włączając w to polityki, procesy, procedury, struktury organizacyjne, oprogramowanie i sprzęt do ochrony zidentyfikowanych aktywów informacyjnych. Te zabezpieczenia powinny być określone, wdrożone, monitorowane, przeglądane i doskonalone tam, gdzie jest to konieczne, w celu zapewnienia, że określone cele biznesowe i cele bezpieczeństwa organizacji zostaną osiągnięte. Norma PN-ISO/IEC 27005 zawiera wytyczne do zarządzania ryzykiem dotyczącym bezpieczeństwa informacyjnego i stanowi rozwinięcie ogólnych koncepcji opisanych w PN-ISO/IEC 27001, lecz:

- nie wskazuje rodzajów zasobów, w odniesieniu do których może mieć zastosowanie,
- nie zawiera szczegółowych wytycznych do zarządzania ryzykiem w zakresie bezpieczeństwa informacyjnego.

W metodyce COBIT każde wymaganie biznesowe jest opisane przez siedem biznesowych wymogów informacyjnych. Stanowią one jednocześnie kryteria kontrolne pozwalające zweryfikować stopień spełnienia wymagania. Są to:

- skuteczność – zapewnienie, że informacja wykorzystywana w procesach biznesowych jest dla nich odpowiednia i adekwatna, dostarczona na czas w sposób prawidłowy, spójny i użyteczny;
- wydajność – zapewnienie, że dostarczenie informacji odbywa się w ramach optymalnego zużycia zasobów;

- poufność – zapewnienie, że dostęp do informacji mają tylko osoby uprawnione;
- integralność – zapewnienie, że informacja pozostaje dokładna i kompletna;
- dostępność – zapewnienie, że dostęp do informacji jest możliwy wtedy, gdy jest to wymagane w procesie biznesowym;
- zgodność – zapewnienie, że każdy element systemu informacyjnego pozostaje zgodny z przepisami prawa, regulacjami i umowami, dla których przedmiotem jest proces biznesowy;
- wiarygodność – zapewnienie właściwych informacji dla zarządzania organizacją i dla kierownictwa, aby mogło realizować obowiązki finansowe i sprawozdawcze.

Zatem powstaje pytanie, czy istnieje możliwość, na podstawie dostępnych standardów, stworzenia kompletnej i spójnej metodyki analizy i zarządzania ryzykiem zasobów informacyjnych, uwzględniającej różne kategorie, grupy czynników ryzyka oraz atrybuty bezpieczeństwa zasobów informacyjnych, i wiążącej je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka tych zasobów, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia. Rozdział 3 stanowi próbę odpowiedzi na tak postawione pytanie, prezentując opis podstawowych elementów metodyki zarządzania ryzykiem zasobów informacyjnych i systemów informatycznych wspomagających ich przetwarzanie, która jest taką kompletną i spójną metodyką.

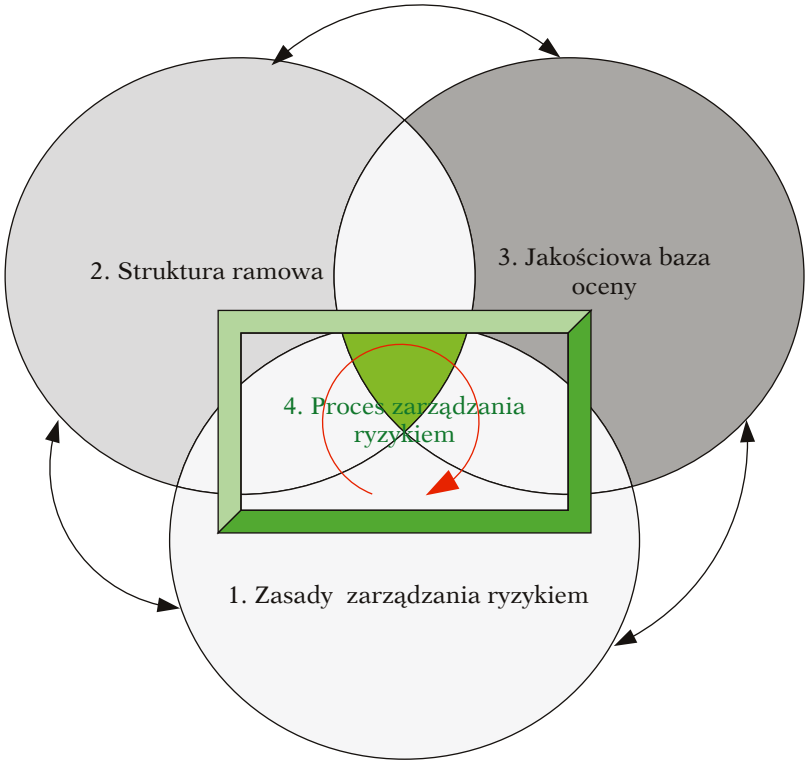
3. Koncepcja metodyki zarządzania ryzykiem zasobów informacyjnych

Podstawowe filary metodyki zarządzania ryzykiem ilustruje rysunek 1, natomiast rozwinięcie (uszczegółowienie) tych filarów – rysunek 2. Na rycinach tych proces zarządzania ryzykiem zasobów informacyjnych jest przedstawiany jako cykl, ponieważ po wdrożeniu odpowiednich środków (planów, procedur i zabezpieczeń), dokonywana jest ponowna ocena, która pozwala określić, czy zamierzony cel (np. poziom bezpieczeństwa zasobów informacyjnych) został osiągnięty.

Metodyka oceny ryzyka prezentowana jest jako czteroetapowe podejście do tej działalności, polegające na:

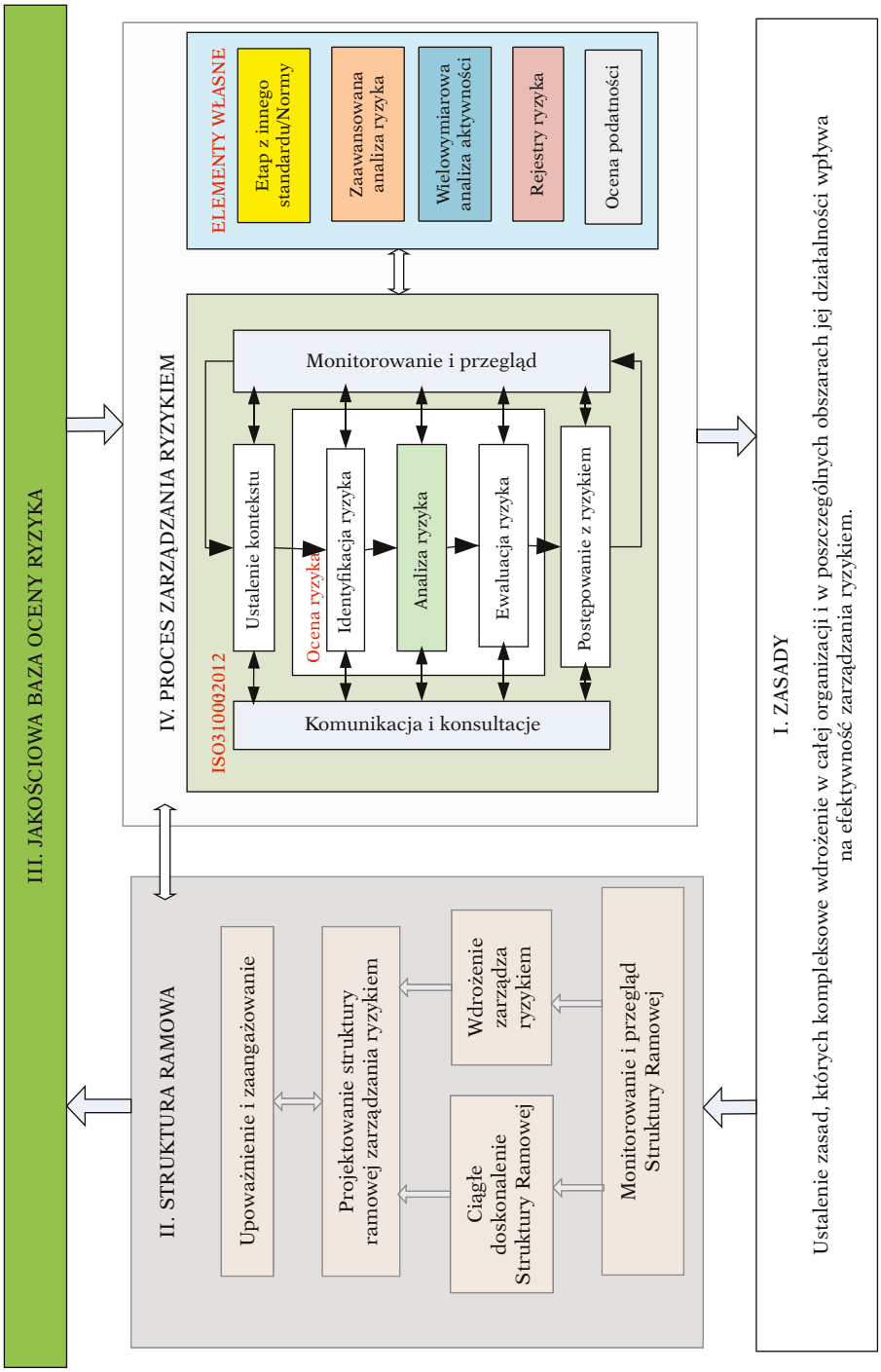
1. Skonstruowaniu **zasad** zarządzania ryzykiem zasobów informacyjnych, uwzględniając aktualnie obowiązujące przepisy prawa. Kompleksowe wdrożenie zbioru tych zasad w całej organizacji i poszczególnych obszarach jej działalności wpływa na efektywność i skuteczność zarządzania ryzykiem.

2. Określeniu skutecznej **struktury ramowej** zarządzania ryzykiem zasobów, obejmującej zestaw elementów zapewniających podstawy i ustalenia organizacyjne w zakresie projektowania, wdrażania, monitorowania, dokonywania przeglądów i ciągłego doskonalenia zarządzania ryzykiem zasobów informacyjnych w systemie informacyjnym lub w całej organizacji.
3. Zbudowaniu **jakościowej bazy (elektronicznego repozytorium)** oceny, która może być uzupełniona analizami różnych szczebli decyzyjnych lub zespołów analizy ryzyka, jeżeli wyniknie taka potrzeba.
4. Ustaleniu i wdrożeniu **procesu zarządzania ryzykiem zasobów informacyjnych**.



Rysunek 1. Podstawowe filary metodyki zarządzania ryzykiem zasobów informacyjnych

Źródło: opracowanie własne na podstawie: *Zarządzanie ryzykiem – przegląd wybranych metodyk*, D. Wróblewski (red.), Wydawnictwo CBBOP-PIB, Józefów 2015, s. 36.



Rysunek 2. Uszczegółowienie podstawowych filarów metodyki zarządzania ryzykiem zasobów informacyjnych

Źródło: opracowanie własne.

Dokonując przeglądu i analizy rysunku 2, można zauważyć, że filar „IV. Proces zarzadzania ryzykiem" został rozszerzony w stosunku do klasycznego procesu zarzadzania o dodatkowe autorskie elementy. Wprowadzone elementy mają charakter dodatkowych działań rozszerzających model podstawowego cyklu życia procesu zarządzania ryzykiem. Odejście od powielania klasycznego procesu zarządzania ryzykiem i wprowadzenie dodatkowych elementów/działań na etapach analizy, szacowania i ewaluacji ryzyka pozwala na skuteczne zarządzanie ryzykiem zasobów informacyjnych, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia. Zmodyfikowany sposób przeglądu procesu zarządzania ryzykiem – leżący w kompetencji kierownictwa i personelu jednostki organizacyjnej. Zaproponowany proces zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych może być iteracyjny. Iteracyjne podejście do przeprowadzenia szacowania ryzyka może polegać na zwiększaniu szczegółowości w każdej iteracji. Iteracyjne podejście zapewnia korzystną równowagę między minimalizowaniem nakładu czasu oraz wysiłku na identyfikowanie zabezpieczeń a pewnością odpowiedniego oszacowania wszystkich ryzyk. Szczegółowy opis wymienionych elementów znajduje się w kolejnym rozdziale[3].

4. Charakterystyka podstawowych filarów metodyki zarządzania ryzykiem zasobów informacyjnych

4.1. Zasady zarządzania ryzykiem

W tym filarze wyodrębnionych zostało kilkanaście zasad, których kompleksowe wdrożenie w systemie informacyjnym organizacji i poszczególnych obszarach wspomaganych technologią informatyczną (IT) wpływa na efektywność

[3] Opis korzyści, jakie można uzyskać w procesie zarzadzania ryzykiem wykorzystując zaproponowany model, można znaleźć w opracowaniach: M. Kiedrowicz, J. Stanik, *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; J. Stanik, T. Protasowicki, *Metodyka kształtowania ryzyka w cyklu rozwojowym systemu informatycznego*, w: *Od procesów do oprogramowania: badania i praktyka*, P. Kosiuczenko, M. Śmiałek, J. Swacha (red. nauk.), Polskie Towarzystwo Informatyczne, Warszawa 2015; J. Stanik, M. Kiedrowicz, *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Ekonomiczne Problemy Usług" 2017, nr 126/1.

zarządzania ryzykiem zasobów informacyjnych. Zasady zarządzania ryzykiem[4] mają charakter polityki zarządzania ryzykiem. Ich kompleksowe wdrożenie w całej organizacji i poszczególnych obszarach jej działalności znacznie wpływa na efektywność zarządzania ryzykiem. W tabeli 2 przytoczono kilka, najczęściej wymienianych zarówno w literaturze fachowej, jak i normach ISO, zasad.

Tabela 2. Przykładowe zasady zarządzania ryzykiem

Nazwa zasady	Opis
Kreowanie i ochrona wartości	Zarządzanie ryzykiem, służąc realizacji przedsięwzięć w obszarze ochrony ludności, pozwala osiągnąć bezpieczny i stabilny poziom życia w przyjaznym środowisku, sprzyjając gospodarce, administracji i infrastrukturze.
Dostępność najlepszych zasobów informacji	Informacje gromadzone są w bazach danych. Gromadzi się i opracowuje dostępne dane o zagrożeniach, podatności, wrażliwości ekspozycji na różne czynniki w ujęciu historycznym i perspektywicznym oraz zmiany i obserwacje z udziałem ekspertów.
Integracja ze wszystkimi procesami biznesowymi	Zarządzanie ryzykiem stanowi główny nurt aktywności, najskuteczniejszy w integracji standardów aktywności organizacji i społeczeństwa.
Dopasowanie	Metodyka zarządzania ryzykiem zapewnia zrównanie potrzeb społecznych w zakresie profilu ryzyka.
Informowanie o podejmowanych decyzjach	Zarządzanie ryzykiem wspiera w świadomym podejmowaniu decyzji i ustaleniu priorytetów względem ograniczonych zasobów dla działań redukujących ryzyko
Dynamika, powtarzalność i reagowanie na zmiany	Zarządzanie ryzykiem zagrożeń reaguje na zmiany profilu ryzyka, informacje o zagrożeniach i wrażliwości ekspozycji. Skuteczny monitoring pozwala te zmiany identyfikować i odpowiednio wcześnie na nie reagować.
Ułatwienie ciągłego doskonalenia	Skuteczne zarządzanie ryzykiem steruje doskonaleniem i wdrażaniem strategii, które podnoszą na wyższy poziom organizację zarządzania ryzykiem w społeczeństwie i organach władzy. Takie podejście zapewnia elastyczność i możliwości adaptacyjne społeczności.

Źródło: opracowanie własne na podstawie: PN-ISO 31000:2012, Zarządzanie ryzykiem. Zasady i wytyczne, PKN 2012.

[4] Źródło: opracowanie własne na podstawie: PN-ISO 31000:2012, Zarządzanie ryzykiem. Zasady i wytyczne, PKN 2012.

4.2. Struktura ramowa zarządzania ryzykiem – dobre praktyki

Skuteczność zarządzania ryzykiem zależy od efektywności ramowej struktury zarządzania, zapewniającej podstawy organizacyjne, które gwarantują sukcesy na wszystkich szczeblach organizacyjnych. Ramy zarządzania ryzykiem określone zostały poprzez pięć atrybutów[5]:

- pełną akceptację odpowiedzialności za własne ryzyko oraz doskonalenie kontroli i strategii postępowania z ryzykiem zasobów informacyjnych;
- zwiększenie nacisku na doskonalenie zarządzania ryzykiem zasobów – konieczne jest opracowanie zestawu celów i przedsięwzięć, a następnie analizowanie i doskonalenie procesów przetwarzania informacji odpowiednio do potrzeb (oznacza to zobowiązanie do prowadzenia przeglądów i modyfikowania systemu informacyjnego, zasobów i zdolności zapewniających permanentne doskonalenie),
- identyfikację każdej osoby w zakresie odpowiedzialności za zarządzanie ryzykiem – wszystkie powinny być odpowiednio przygotowane, dysponować odpowiednimi zasobami, a także prowadzić i doskonalić kontrolę oraz monitorowanie ryzyka i zdolności skutecznej komunikacji z odpowiednimi służbami;
- podejmowanie decyzji – na każdym szczeblu w procesie tym musi być uwzględniane ryzyko, z zastosowaniem odpowiednich procesów zarządzania ryzykiem;
- okresowe raporty dla komórek, zespołów bądź referatów odpowiedzialnych za nadzór oraz kontrolę zarządzania ryzykiem zasobów informacyjnych – powinny zawierać opisy stosowanych procesów, procedur oraz być kompletne i sporządzane terminowo.

Jak sugeruje D. Wróblewski[6], przed rozpoczęciem projektowania struktury ramowej dla organizacji, należy zagwarantować włączenie się w proces zarządzania ryzykiem jej kierownictwa. Jest to etap konieczny i mający wpływ na działania podejmowane w dalszym ciągu procesu zarządzania ryzykiem. Właściwie dopasowana struktura zapewnia poprawność obiegu informacji o ryzyku i wykorzystanie jej w podejmowaniu decyzji na wszystkich etapach procesu zarządzania ryzykiem.

---

[5] *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, Australian Government, August 2010, Fact Sheet*, s. 2, http://www.finance.gov.au/sites/default/files/ A3_23082010_0.pdf (dostęp: 18.06.2017).

[6] *Zarządzanie ryzykiem – przegląd wybranych metodyk*, D. Wróblewski (red.), Wydawnictwo CBBOP-PIB, Józefów 2015.

Struktura ramowa zarządzania ryzykiem jest przeznaczona do wsparcia integracji zarządzania ryzykiem i jego rezultatów z polityką kierownictwa, systemem zarządzania i podejmowanymi działaniami. Struktura ramowa zarządzania ryzykiem obejmuje zestaw elementów zapewniających podstawy i ustalenia organizacyjne w zakresie projektowania, wdrażania, monitorowania, dokonywania przeglądów i ciągłego doskonalenia zarządzania ryzykiem w całej organizacji.

4.3. Proces zarządzania ryzykiem

Punktem wyjścia do ustanowienia, a następnie wdrożenia procesu zarządzania ryzykiem zasobów informacyjnych, jest posiadanie odpowiednio przygotowanej strategii zarządzania tym ryzykiem. Jak sugerują J. Stanik, R. Hoffmann, J. Napiórkowski[7], w zbiorze podstawowych elementów tej strategii powinny się znaleźć także:

- właściwie sprecyzowany model ryzyka zasobu informacyjnego,
- adekwatna metoda analizy i szacowania ryzyka zasobu informacyjnego,
- adekwatna do ustalonej metody struktura organizacyjna zespołu analizy ryzyka wraz z przejrzystym rozpisaniem ról poszczególnych członków zespołu.

Na potrzeby niniejszego rozdziału jako model ryzyka przyjęto wieloaspektowy[8] model oceny ryzyka zasobu informacyjnego. Model ten za pomocą wymiarów: bezpieczeństwa (B), ciągłości działania (C), technologii (T), złożoności (S) oraz jakości (J) uwzględnia różne kategorie lub rodzaje czynników ryzyka, wynikających zarówno ze złożoności lub struktury samego zasobu informacyjnego, jak i elementów dotyczących bezpieczeństwa informacyjnego, bezpieczeństwa ciągłości działania, jakości lub atrakcyjności zasobu informacyjnego, w procesie przeglądu lub wyznaczania wielkości ryzyka zasobu informacyjnego. Podstawowy szkielet procesu jest zgodny z ISO 31000 Risk Management – Principles and Guidelines on Implementation i obejmuje pięć głównych zadań: komunikację i konsultacje[9], ustalenie kontekstu, ocenę ryzyka, postępowanie z ryzykiem oraz monitorowanie i przegląd. Biorąc pod uwagę przyjęte elementy strategii

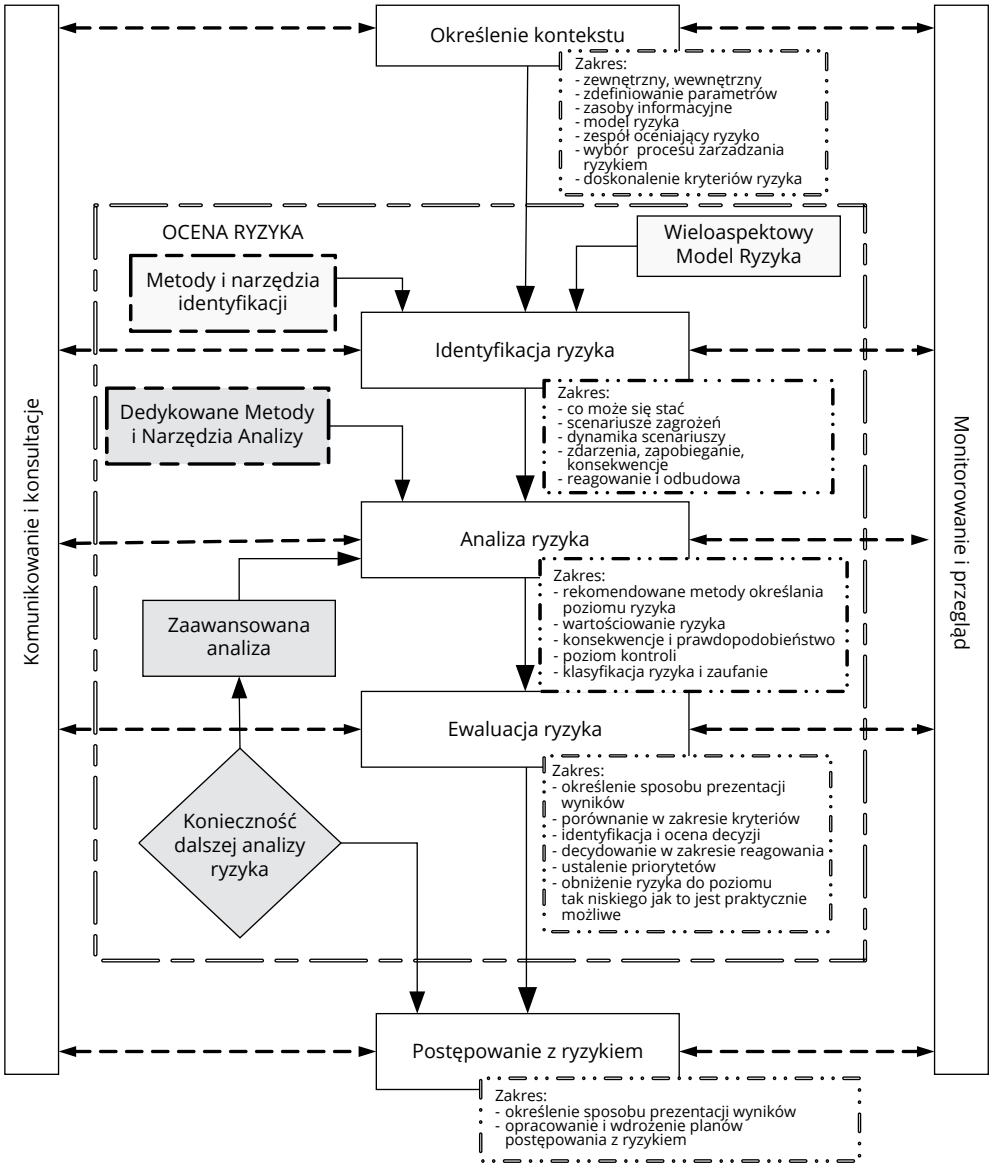
---

[7] J. Stanik, R. Hoffmann, J. Napiórkowski, *Zarządzanie ryzykiem w systemie zarządzania bezpieczeństwem organizacji*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2016, nr 123.

[8] J. Stanik, M. Kiedrowicz, *Model ryzyka procesów biznesowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego Ekonomiczne Problemy Usług" 2017, vol. 126/1, s. 325–338.

[9] Komunikacja i konsultacje – ciągłe i prowadzone w sposób iteracyjny procesy, które są przez organizację wykonywane w celu zapewnienia, przekazywania lub uzyskania informacji, jak również w celu porozumiewania się z interesariuszami, odnoszące się do zarządzaniem ryzykiem. Źródło: *ISO Guide 73:2009 Risk Management – Vocabulary*, definicja 3.3.1.2.

zarządzania ryzykiem, szkielet ten został rozbudowany o cztery pomocnicze elementy (szare elementy na rysunku 3), przyczyniające się do dokładniejszego wyznaczenia poziomu ryzyka zasobów informacyjnych.



Rysunek 3. Uszczegółowienie podstawowych filarów metodyki zarządzania ryzykiem zasobów informacyjnych

Źródło: opracowanie własne na podstawie: PN-ISO/IEC 27005, Technika informatyczna, Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN 2013.

4.3.1. Komunikacja i konsultacje

Zasady komunikacji i konsultacji należy ustalić przed przystąpieniem do realizacji kolejnych elementów procesu. Działania te powinny uwzględniać nie tylko kwestię samego ryzyka zasobu informacyjnego (z jego przyczynami i konsekwencjami), ale także etap postępowania z nim. Jest to istotne, ponieważ element ten jest podstawą właściwego komunikowania się ze wszystkimi zaangażowanymi członkami zespołu analizy i ryzyka (ZAR) oraz z podmiotami zarówno w samej organizacji, jak i z jej interesariuszami. Komunikowanie się i konsultacje nie są przy tym celem same w sobie – to ich właściwe wykorzystanie pozwala na zrozumienie podejmowanych decyzji, ich przyczyn oraz oczekiwanych konsekwencji.

4.3.2. Ustalenie kontekstu

Ustalając kontekst procesu zarządzania ryzykiem zasobu informacyjnego, należy zwrócić uwagę, by odnosił się on między innymi do zdefiniowanych celów, odpowiedzialności, zakresu oraz skali podejmowanych działań, dotyczących systemu informacyjnego oraz technologii informacyjnej. Niezbędne jest również uwzględnienie przyjętej metody oceny ryzyka (zalecane są dedykowane metody i narzędzia analizy), sposobów szacowania jego wyników oraz kryteriów. Uzgadnianie kryteriów ryzyka stanowi ważny element procesu. Proces zarządzania ryzykiem powinien być dopasowany do funkcjonującej struktury organizacji, zrozumiały dla jej otoczenia i prowadzony zgodnie z przyjętą metodyką i prawem. Kompetencje i odpowiedzialność członków ZAR powinny być precyzyjnie rozdzielone, kryteria ryzyka zdefiniowane i zgodne z celami przyjętej strategii zarządzania ryzykiem.

4.3.3. Ocena ryzyka

Kolejnym istotnym działaniem jest ocena ryzyka. 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, na przykład kierownik jednostki organizacyjnej, z uwzględnieniem przyjętej metodyki. Kryteria i kompetencje w zakresie akceptacji ryzyka zatwierdza kierownik podmiotu. Ryzyka, dla których wartość pierwotnego poziomu jest niższa lub równa 20%[10] poziomu

[10] Przy ustalaniu progów poziomów ryzyka, od których zależy sposób postępowania z ryzykiem, można przyjąć np. zasadę Pareto.

maksymalnego, uznaje się *a priori* za ryzyka szczątkowe, które nie podlegają procedurze postępowania z ryzykiem. Ryzyka, dla których poziom przekracza 20% poziomu ryzyka maksymalnego, podlegają procedurze postępowania z ryzykiem. Ryzyka, dla których poziom ryzyka jest większy od 80% poziomu maksymalnego, przedstawiane są do akceptacji kierownictwa podmiotu.

Celem oceny ryzyka jest stworzenie rejestru czynników ryzyka, które będą wpływały na zdefiniowane cele. Sprowadza się to do wytypowania wyczerpującej listy czynników ryzyka[11] i zagrożeń[12].

D. Wróblewski[13] sugeruje, że dokonując identyfikacji, należy pamiętać o efekcie kaskadowym (domina)[14], który wpływa na pojawienie się kolejnych czynników ryzyka. 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 ciągłość realizacji procesu przetwarzania informacji. 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 bądź wybranych obszarów działalności. Podstawą identyfikacji jest informacja, która musi spełniać określone kryteria. Powinna być wiarygodna, terminowa, pełna i – o ile to możliwe – zweryfikowana.

W dalszej kolejności właściwie zagregowane ryzyka należy poddać analizie. Analiza ryzyka służy jego szczegółowemu zrozumieniu. Analizy ryzyk dokonuje osoba lub zespól osób wyznaczonych przez kierownictwo podmiotu (urzędu). Na analizę ryzyka składają się: szacowanie następstw, szacowanie prawdopodobieństwa incydentu, określenie poziomu ryzyka.

Wiedza zdobyta na tym etapie pozwala na podjęcie decyzji o sposobie postępowania z ryzykiem (wybór strategii[15] i dobór metod[16]). Analiza powinna zostać

---

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

[12] Zgodnie z normą ISO Guide 73:2009 przez zagrożenia rozumiemy źródła potencjalnej szkody, natomiast ryzyko wyrażane jest w odniesieniu do możliwych konsekwencji i prawdopodobieństwa ich wystąpienia.

[13] *Zarządzanie ryzykiem – przegląd…*

[14] Efekt domina – teoria zakładająca, że jedno zdarzenie wywołuje ciąg kolejnych wydarzeń. Element ten jest istotny, ponieważ niektóre ryzyka (zagrożenia) mogą występować jedynie jako następstwa innych ryzyk.

[15] Strategia postępowania z ryzykiem – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka.

[16] Metoda postępowania z ryzykiem – sposób modyfikacji ryzyka, do którego można zaliczyć m.in.: unikanie ryzyka, podjęcie lub zwiększenie ryzyka, usunięcie źródła ryzyka, zmianę

przeprowadzona w taki sposób, aby mogła dostarczyć danych wejściowych do ewaluacji ryzyka.

4.3.4. Ewaluacja ryzyka

W praktyce ewaluacja ryzyka to proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane. Ewaluacja ryzyka ma istotny wpływ na proces podejmowania decyzji. Do wizualizacja wyników ryzyka należy wykorzystywać różne sposoby, a mianowicie matryce ryzyka, wektory ryzyka, krzywe ryzyka lub pola ryzyka. Wyniki analizy ryzyka stanowią podstawę do podjęcia decyzji, które ryzyka i w jakim stopniu wymagają wdrożenia przez organizację właściwego algorytmu postępowania z nimi oraz ustalenie priorytetu ich uruchamiania wymaga posiadanie wiarygodnych.

Następnie ustalone poziomy ryzyka powinny zostać porównane z ich kryteriami, z uwzględnieniem ustanowionego na wejściu kontekstu. Ewaluacja umożliwi w tym wypadku określenie, w jaki sposób postąpić z danym ryzykiem. Ewaluacja ryzyka, jako ostatni krok oceny ryzyka, obejmuje porównanie poziomu ryzyka zidentyfikowanego w procesie analizy z przyjętymi kryteriami. To porównanie wymaga dużej dokładności i rzetelności. Ocenia się, czy oczekiwane ryzyko mieści się w granicach akceptacji lub tolerancji, ewentualnie czy jest poza tymi granicami. Ryzyko akceptowane nie wymaga szczególnej uwagi (działania codzienne), a ryzyko w granicach tolerancji powinno już wzmocnić czujność i uruchomić działania mające na celu jego monitorowanie, kontrolę i mechanizmy jego redukowania. Tolerancja w sprawach ryzyka nie jest akceptacją zaistniałego stanu rzeczy i wymaga reakcji. Zanim jednak podejmie się jakiekolwiek działania, ocenia się skuteczność monitoringu, wiarygodność informacji, kompetencje personelu, poprawność analizy, możliwe straty lub korzyści wynikające z wystąpienia ryzyka, przewidywane nakłady na jego redukcję i ekonomiczność całego przedsięwzięcia. Fundamentalnym wymogiem jest skupienie się na sprowadzeniu ryzyka do poziomu akceptowanego. Podczas oceny ryzyka każde ryzyko musi zostać sklasyfikowane i porównane z jego wartością tolerowaną i akceptowaną. Trzeba jednak wcześniej przyjąć kryteria, które pomogą jednoznacznie zidentyfikować ryzyko znaczące, wymagające zdecydowanych działań. Jest to krok w kierunku zdefiniowania ryzyka szczególnej uwagi. Rejestr

następstw, dzielenie ryzyka, retencję ryzyka. Źródło: opracowanie własne na podstawie: *ISO Guide 73:2009*, definicja 3.8.1.

ryzyk, który zostanie sporządzony w wyniku oceny, pomoże zracjonalizować zarządzanie ryzykiem.

4.3.5. Postępowanie z ryzykiem

Ryzyka, które na poziomie oceny nie zostały uznane za ryzyka szczątkowe, podlegają procedurze postępowania z ryzykiem. Postępowanie z ryzykiem może polegać na: wpływaniu na zmianę poziomu ryzyka poprzez zastosowanie zabezpieczenia, unikaniu ryzyka, przeniesieniu ryzyka, akceptacji ryzyka, mimo że jego poziom przekracza poziom ryzyka szczątkowego.

Punktem wyjścia w zakresie postępowania z ryzykiem są dwa jego poziomy: pierwszy – niewymagający innego postępowania niż monitoring, zawsze do zaakceptowania i drugi – nietolerowany, wymagający podjęcia natychmiastowych środków zaradczych, mających sprowadzić je do strefy tolerancji. Ryzyko sytuujące się między tymi poziomami ocenia się w kategoriach ekonomicznych (kosztów i korzyści), na przykład w zarządzaniu ryzykiem szczątkowym[17]. Ryzyko nie jest jednak czymś stałym i może eskalować w stronę granicy nietolerancji. Takie ryzyko wymaga więcej uwagi i musi być monitorowane. Sytuacja upoważnia do zakwalifikowania ryzyka jako „ryzyka nietolerowane". Ocena ryzyka warunkuje sposób postępowania z ryzykiem. Sposób postępowania z ryzykiem powinien zostać wyartykułowany i właściwie opisany. Służą do tego plany postępowania z ryzykiem.

4.3.6. Monitorowanie i przegląd

Ostanie dwa działania to monitorowanie i przegląd. Pierwsze z nich powinno zostać uwzględnione już na etapie sporządzania planów (okresowo), choć norma zaleca także weryfikację procesu *ad hoc*. Planując, należy dążyć do przypisania jednoznacznie odpowiedzialności za to działanie oraz objęcia nim każdego aspektu zarządzania ryzykiem. Monitoring rejestruje zmiany zachodzące w otoczeniu, nie zapobiega zagrożeniom, nie eliminuje ani nie ogranicza ryzyka, ale zapewnia informacje i jest podstawą do prowadzenia działań oraz kontrolowania ryzyka. Tylko stały monitoring daje gwarancję zaufania do informacji. Zmianom podlega wszystko: otoczenie, klimat, wrażliwość, organizacje, prawo, programy

[17] Ryzyko szczątkowe (rezydualne, reliktowe, ang. *residual risk*) – ryzyko, którego poziom nie przekracza akceptowanej wartości, pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem. Źródło: *ISO Guide 73:2009 Risk Managment – Vocabulary*.

i procesy. Te zmiany wpływają na cele, zasady, politykę i praktykę zarządzania ryzykiem. Procesy monitorowania i przeglądu powinny być także we właściwy sposób dokumentowane.

4.3.7. Dokumentowanie zarządzania ryzykiem

Dokumentowanie[18] działań związanych z zarządzaniem ryzykiem to jeden z ostatnich etapów odnoszących się do proponowanej metodyki. Wykorzystywane w organizacjach wytyczne dotyczące dokumentowania ryzyk wskazują co najmniej następujące dokumenty: arkusze identyfikacji bądź identyfikacji i oceny ryzyka, rejestr ryzyk, zgłoszenia ryzyk przez interesariuszy w postaci dokument informacja o ryzyku, aktualny dokument metodyka zarządzania ryzykiem.

Pierwszy stanowią arkusze identyfikacji bądź identyfikacji i oceny ryzyka. Służą one jako podstawowy materiał do analizy ryzyka. Drugim rodzajem dokumentów są tzw. rejestry ryzyka[19]. Zawierają one poszerzoną informację na temat zidentyfikowanych i ocenionych ryzyk wraz z określeniem działania wobec danego ryzyka. Rejestry ryzyka wykorzystywane są najczęściej jako integralne zestawienia do raportów ryzyka, które podlegają weryfikacji oraz analizie na etapie monitorowania i przeglądu.

Podsumowanie i kierunki dalszych badań

Zarządzanie ryzykiem stanowi centralny element zarządzania strategicznego każdej organizacji. Jest to proces, w ramach którego organizacja w sposób metodyczny rozwiązuje problemy związane z ryzykiem, które towarzyszy jej działalności w taki sposób, aby ta działalność – zarówno w poszczególnych dziedzinach, jak i traktowana jako całość – przynosiła trwałe korzyści.

Opracowano wiele metodyk wykorzystywanych do zarządzania ryzykiem, jednakże brakowało odpowiednio dopasowanej dla potrzeb zarządzania zasobami informacyjnymi. Artykuł prezentuje autorską metodykę zarządzania ryzykiem

[18] Norma ISO 31000:2009 nie rekomenduje wzorcowych ani też przykładowych form dokumentowania zarządzania ryzykiem, a przedstawia jedynie ogólne zalecenia dotyczące jego identyfikowania. Ze względu na wagę tego zagadnienia zostało ono rozszerzone w niniejszym rozdziale.

[19] Przykłady rejestrów ryzyka odnajdziemy m.in. w wypartej przez ISO 31000 normie Risk Management Guidelines Companion – AS/NZS 4360:2004.

zasobów informacyjnych, która jest odejściem od stosowania, na etapie ewaluacji ryzyka, tradycyjnych map ryzyka, a proponuje wykorzystanie, jako miary oceny ryzyka, krzywych ryzyka, mających charakter diagramów radialnych, wektorów przestrzennych lub pól ryzyka. Zaproponowana metodyka należy do grupy metodyk semilościowych. Opiera się na wieloaspektowym modelu ryzyka zasobu uwzględniającym różne obszary i czynniki ryzyka odnoszące się do zagrożeń występujących w poszczególnych fazach cyklu życia zasobu informacyjnego i wiążące je w sposób pozwalający na możliwie pełne i jednoznaczne wyznaczenie poziomu ryzyka, przy jednoczesnym zachowaniu praktycznej użyteczność proponowanego podejścia.

Zaproponowana metodyka powinno być nieodłącznym elementem SZR oraz procesu podejmowania decyzji i planowania wariantów funkcjonowania organizacji. Metodyka posiada zarówno zalety, jak i wady. Główne zalety metodyki obejmują: możliwość prowadzenia oceny na różnych etapach i w różnych odstępach czasu; możliwość porównywania uzyskanych wyników badań w czasie; możliwość analizowania wielu grupy zdarzeń; możliwości uzyskania oceny zagregowanej. Pomimo zalet metodyka ma pewne wady: charakteryzuje się wysoką złożonością wynikającą z zastosowania aparatu matematycznego, stosowanie niejednolitych kryteriów oceny; z powodu zastosowania metody półilościowej (metoda ekspercka) – brak możliwości uzyskania pełnego obiektywizmu odnośnie do uzyskanego wyniku.

Poprawność opracowanej metodyki zweryfikowano na prototypie kancelarii typu RFID opracowanym w ramach projektu „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości".

Bibliografia

Hoffmann R., Kiedrowicz M., Stanik J., *Evaluation of information safety as an element of improving the organization's safety management*, „MATEC Web of Conferences" 2016, vol. 76, DOI: 10.1051/matecconf/20167604011.

ISO Guide 73:2009 Risk Management – Vocabulary.

ISO 31000 Risk Management – Principles and Guidelines on Implementation.

ISO/IEC 27001 – Information security management systems.

ISO/IEC 27002 – Code of practice for information security management.

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 2015.

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

PN-ISO/IEC 27005 Technika informatyczna. Zarządzanie ryzykiem w bezpieczeństwie Informacji, 2014.

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. nauk.), Polskie Towarzystwo Informatyczne, Warszawa 2015, s. 27–44.

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., 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.

Zarządzanie ryzykiem – przegląd wybranych metodyk, D. Wróblewski (red.), Wydawnictwo CBBOP-PIB, Józefów 2015.

* * *

Methodology of Risk Management in Information Security

Summary

The article presents a risk management methodology that takes into account the accepted risk model of the information resource, the method for risk analysis and estimation, and exemplary risk areas and risk factors relating to the various phases of the information life cycle and binds them in a way that allows for the full and unambiguous determination of the risk level, while maintaining the practical utility of the proposed approach.

Keywords: information resource, risk, risk vector, risk management methodology.