ZARZĄDZANIE PUBLICZNE 3 (47) 2019, s. 175–189
doi:10.4467/20843968ZP.19.014.10690
www.ejournals.eu/Zarzadzanie-Publiczne

Mariusz Matysek
e-mail: mariuszmatysek@poczta.onet.pl
ORCID: 0000-0002-6409-3301

HOLISTYCZNE UJĘCIE ZARZĄDZANIA RYZYKIEM BEZPIECZEŃSTWA INFORMACJI W ORGANIZACJACH SEKTORA PUBLICZNEGO

Filozoficznie rzecz ujmując,
zarządzanie ryzykiem ma na celu wprowadzenie
porządku tam, gdzie panuje chaos,
i dążenie do pewności tam,
gdzie panuje niepewność.
Glenn R. Carroll

Abstract

A Holistic Risk Analysis for Information Security Risks in Public Sector

In this work we describe a model of holistic approach to risk management in public organizations. The proposed model incorporates all types of risk, including information security risk. The core of the model is defined by risk identification, its quantitative estimation and management. This paper presents risk management as an integral part of management control.

Keywords: information security, risk management, key risk indicators, management control

Streszczenie

W artykule przedstawiono model holistycznego podejścia do zarządzania ryzykiem w organizacjach publicznych. Zaproponowany model integruje wszelkie rodzaje ryzyka, w tym ryzyka związane z zachowaniem bezpieczeństwa informacji. Istotą modelu jest identyfikacja ryzyk, ich szacowanie i administrowanie w kontekście realizacji celów głównych. Według przyjętej koncepcji proces zarządzania ryzykiem stanowi immanentną składową kontroli zarządczej.

Słowa kluczowe: bezpieczeństwo informacji, zarządzanie ryzykiem, kluczowe wskaźniki ryzyka, kontrola zarządcza

1. Wstęp

Zarządzanie bezpieczeństwem informacji jest aktualnie jednym z kluczowych czynników skuteczności i efektywności funkcjonowania organizacji sektora publicznego. Potrzeba gromadzenia i administrowania rosnącą ilością informacji oraz zjawisko powszechnej informatyzacji generują coraz bardziej złożone zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i liczby czynników ryzyka. Taki stan rzeczy skłania do podjęcia krytycznej analizy dotychczasowych sposobów podejścia do zarządzania ryzykiem bezpieczeństwa informacji oraz poszukiwania nowych metod i technik.

Wieloletnie obserwacje organizacji sektora publicznego pokazują, że powszechnie stosowaną praktyką jest zarządzanie ryzykiem bezpieczeństwa informacji bez dokonywania analizy kontekstowej w odniesieniu do innych obszarów aktywności organizacji (obserwacji dokonano w urzędach celnych i urzędach skarbowych, a także w administracji samorządowej). Analiza ryzyka jako narzędzie wspomagające skuteczną realizację celów jest powszechnie stosowana w odniesieniu do wielu aspektów działania organizacji, takich jak zarządzanie przez cele, zarządzanie projektami czy kontrola zarządcza (wymóg wynikający z ustawy o finansach publicznych, Dz.U. 2009, nr 157, poz. 1240 ze zm.). W ramach każdej z dokonanych analiz ryzyka planowane są odrębne i niezależne działania zaradcze na wypadek zmaterializowania się ryzyka oraz projektowane są mechanizmy kontrolne. Może to doprowadzić do sytuacji, w której zaplanowane działania będą kolidowały ze sobą, a nawet pozostawały ze sobą w sprzeczności. Dla przykładu: realizacja polityki otwartości i transparentności urzędów z jednej strony a polityka zachowania daleko idącej ostrożności w zarządzaniu informacją z drugiej wymagają wielu kompromisów. Dotyczy to również zarządzania ryzykiem w odniesieniu do obu polityk. Do sprawnego zarządzania organizacją sektora publicznego potrzebne jest wieloaspektowe spojrzenie obejmujące całość organizacji, w kontekście realizacji jej zasadniczych celów.

Mając powyższe na uwadze, przyjęto hipotezę, że jedynie całościowe postrzeganie organizacji daje podstawę do opracowania optymalnego sposobu zarządzania ryzykiem bezpieczeństwa informacji.

2. Tradycyjne podejście do zarządzania ryzykiem bezpieczeństwa informacji

Konieczność zintegrowania i zestandaryzowania działań związanych z przetwarzaniem informacji przez podmioty realizujące zadania publiczne spowodowała potrzebę skodyfikowania zasad i trybu postępowania w aktach powszechnie obowiązującego prawa[1]. W rozporządzeniu z dnia 12 kwietnia 2012 r. Rady

[1] Obszary działalności, w których prawnie wymagana jest ochrona danych i informacji, to między innymi: prawo dotyczące ochrony danych osobowych, prawo bankowe, prawo finansowe, prawo

Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej i minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016, poz. 526) w § 20.1 postanowiono, że:

> Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Ponadto ustalono, że zarządzanie to realizowane będzie między innymi poprzez: „(…) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy". Jako wzorzec postępowania prawodawca wskazał Polską Normę PN-ISO/IEC 27005:2014-01. W swej istocie przywołana norma jest zbiorem wytycznych i tzw. dobrych praktyk w zarządzaniu ryzykiem bezpieczeństwa informacji. Jak zastrzegają autorzy: „(…) nie przedstawiono w niej żadnej określonej metody zarządzania ryzykiem (…). Organizacja sama określa swoje podejście do zarzadzania ryzykiem, na przykład w zależności od kontekstu SZBI, kontekstu zarządzania ryzykiem (…)".

Zgodnie z tezą zawartą w motywie 76 preambuły RODO (ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000 ze zm.):

> Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

Wyszczególnione tu kryteria odniesienia, jakie należy uwzględniać przy dokonywaniu analizy ryzyka, wskazują jednoznacznie na potrzebę wieloaspektowego postrzegania organizacji. Podobnie jak w poprzednio omawianym akcie prawnym, prawodawca nie określił konkretnego wzorca odniesienia, pozostawiając wykonawcy swobodę tworzenia własnego modelu zarządzania ryzykiem.

Zarówno według rozporządzenia dotyczącego interoperacyjności, jak i rozporządzenia RODO warunkiem skuteczności zarządzania ryzykiem jest podejście procesowe w organizacji. Według tej koncepcji ryzyka są identyfikowane, kwantyfikowane i zarządzane w odniesieniu do procesów krytycznych. Stanowi to istotną przeszkodę we wdrożeniu tych przepisów, gdyż w krajowych organizacjach sektora publicznego podejście procesowe należy do rzadkości. Dodatkową

---

dotyczące informatyzacji państwa, prawo telekomunikacyjne, prawo dotyczące statystyki publicznej, prawo oświatowe, prawo z zakresu ochrony zdrowia oraz prawo archiwalne.

trudność sprawia hermetyczny język, jaki stosują prawodawcy w obu rozporządzeniach. Jest on trudny do przyswojenia, a przez to nastręcza wielu problemów przy wdrażaniu przepisów.

Niedoprecyzowanie modelu zarządzania ryzykiem oraz brak podejścia procesowego spowodowały ukształtowanie się w organizacjach sektora publicznego specyficznych rozwiązań. Obserwacje dokonane w urzędach skarbowych, urzędach celnych, administracji samorządowej wskazują na kilka charakterystycznych cech wspólnych tych rozwiązań.

Po pierwsze, w praktyce analiza ryzyka w aspekcie bezpieczeństwa informacji odnosi się głównie do zapewnienia bezpieczeństwa danych gromadzonych i przetwarzanych w systemach informatycznych. Obsługujący je pracownicy mają największy wpływ na sposób dokonywania analizy ryzyka oraz projektowanie działań zaradczych. Ryzyka przez nich identyfikowane ograniczają się do działalności przez nich nadzorowanej. Na ogół pomijane są te, które można zidentyfikować, jedynie dokonując analizy przekrojowej organizacji, tj. analizując całe procesy *end-to-end*, a nie tylko wybrane fragmenty. Zjawisko takie obserwowane jest nie tylko w przypadku polskich organów sektora publicznego, lecz także w organizacjach biznesowych [Spears, 2005; Blakley, McDermott, Geer, 2001].

Po drugie, kwantyfikacja atrybutów ryzyka, tj. skutku i prawdopodobieństwa, dokonywana jest często na podstawie subiektywnych wyobrażeń i spekulacji. Dla przykładu – ocena skutków finansowych utraty informacji w przypadku urzędu gminy jest trudna do określenia, gdyż często brakuje historycznych doświadczeń w tym zakresie, a ponadto nieznane są metody ich wyceny, jak ma to miejsce w przypadku sektora bankowego, ubezpieczeniowego czy biznesu.

Po trzecie, aspekt ludzki – związany między innymi z szerzeniem wiedzy o ryzyku, uczulaniem na pewne zjawiska mogące stanowić symptomy pojawienia się ryzyka czy uczeniem zasad reagowania na te symptomy – jest traktowany w sposób drugorzędny, a czasem zupełnie marginalizowany.

Po czwarte, zarządzanie bezpieczeństwem informacji, w tym zarządzanie ryzykiem, stanowi w organizacjach sektora publicznego działalność wyodrębnioną spośród pozostałych procesów biznesowych. Przejawia się to dokonywaniem niezależnej od pozostałej działalności analizy ryzyka. Różny jest także sposób dokonywania tej analizy, na przykład stosowanie odmiennych skal wartości skutku i prawdopodobieństwa ryzyka.

Po piąte, skuteczny i sprawny przepływ informacji o ryzyku stanowi krytyczny element procesu zarządzania ryzykiem. Wiedza o ryzyku dotycząca bezpieczeństwa informacji na ogół pozostaje w komórkach organizacyjnych dokonujących jego analizy. Ryzyka rozpatrywane są w sposób wybiórczy w odniesieniu do ich wewnętrznej działalności i z ich punktu widzenia. Tworzące się w ten sposób funkcjonalne silosy[2] w znacznym stopniu utrudniają przepływ informacji o ryzyku w kontekście całej organizacji. Przyczyn takiego stanu rzeczy należy upatrywać

[2] „Efekt silosu sprawia, że kierownicy wyższych szczebli zmuszeni są do rozwiązywania problemów niższych szczebli. (…) Zwykli pracownicy, którzy mogliby rozwiązać te problemy we włas-

w specyfice organizacji publicznych, jej zwyczajach związanych z zachowaniem drogi służbowej, funkcjonalnej strukturze etc.

3. Holistyczny model zarządzania ryzykiem bezpieczeństwa informacji

W celu przeciwdziałania opisanym zjawiskom i ich skutkom poszukiwane są modele referencyjne dotyczące zarządzania ryzykiem bezpieczeństwa informacji dla organizacji sektora publicznego mających charakter kompleksowy i interdyscyplinarny. Zgodnie z wytycznymi podanymi w Polskiej Normie PN-ISO 31000:2012 zaleca się:

> (…) aby organizacje opracowały, wdrożyły i ciągle doskonaliły strukturę ramową, której celem jest integracja procesu zarządzania ryzykiem z całościowym ładem organizacyjnym, a także z jej strategią i planowaniem, zarządzaniem, procesami raportowania, politykami, wartościami i kulturą.

Na kanwie tego zalecenia warto rozważyć możliwość zbudowania systemu zarządzania ryzykiem bezpieczeństwa informacji zintegrowanego z całościowym systemem zarządzania ryzykiem w organizacji [Kwo-Shing Hong i in., 2003; Spears, 2005; Soomro, Shah, Javed, 2015]. W dalszych rozważaniach, jako model całościowego systemu zarządzania ryzykiem w organizacjach sektora publicznego, przyjęto stanowienie zarządzania ryzykiem w odniesieniu do kontroli zarządczej[3]. Obejmuje ona najszersze spektrum zarządzania organizacją.

W praktyce pożądany jest system mający następujące cechy:

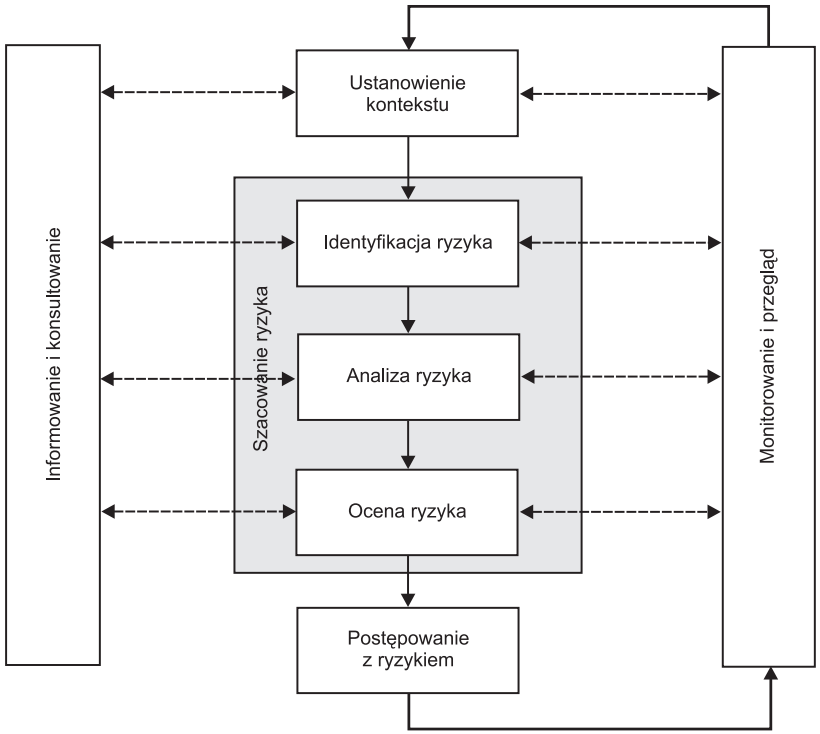
1) jednolity jako narzędzie – obowiązujące w nim reguły postępowania są adekwatne do reguł obowiązujących w całościowym systemie zarządzania ryzykiem;
2) stosunkowo łatwy do przyswojenia przez wszystkich członków organizacji – zarówno kierujących, jak i wykonawców;
3) oferujący jednakowe standardy oceny ryzyka, niezależnie od ocenianego obszaru działalności.

Ogólny schemat **procesu** zarządzania ryzykiem – zarówno w odniesieniu do bezpieczeństwa informacji, jak i kontroli zarządczej – jest co do istoty identyczny (rysunek 1).

---

nym zakresie, w efekcie nie biorą pełnej odpowiedzialności za rezultaty i postrzegają siebie jedynie jako zwykłych wykonawców i dostawców informacji" [Rummler, Brache, 2000].

[3] Kontrola zarządcza wywodzi się z ang. *management control* – panowanie nad organizacją. Zgodnie z def. INTOSAI jest „narzędziem zarządzania wykorzystywanym do uzyskania racjonalnej pewności, że cele zarządzania zostały osiągnięte".



Rysunek 1. Proces zarządzania ryzykiem

Źródło: Polska Norma PN-ISO/IEC 27005:2014-01.

Proces ten składa się z sekwencji działań polegających na identyfikacji, parametryzowaniu i hierarchizacji zjawisk mogących zagrozić organizacji w dążeniu do celów oraz opracowywaniu skutecznych działań zaradczych. Czasem przebiega jednorazowo, a czasem może być iteracyjny, jak to zaleca norma [Polska Norma PN-ISO/IEC 27005:2014-01: 15] w odniesieniu do zarządzania bezpieczeństwem informacji.

3.1. Ustanowienie kontekstu

W praktyce zarządzania ryzykiem bezpieczeństwa informacji w organizacjach sektora publicznego pierwszy etap procesu, tj. ustanowienie kontekstu, sprowadza się do wskazania systemów informacyjnych oraz typów informacji podlegających ochronie. Uwzględnia się przy tym głównie aspekt technologiczny, a więc aktywa takie jak: systemy informatyczne i ich ochronę, przechowywanie i przetwarzanie danych, dokumentację. W holistycznym modelu zarządzania ryzykiem proponuje się rozpocząć analizę kontekstową od zidentyfikowania procesów służących realizacji głównych celów organizacji. Podejście procesowe determinuje

powtarzalność działań i ich systematyczność, co w przypadku zarządzania ryzykiem jest warunkiem koniecznym jego skuteczności [Burlton, 2001]. Rzecz jasna można je zastosować w organizacji, która osiągnęła pod względem kulturowym wystarczający poziom dojrzałości (według CMMI wymagany jest co najmniej czwarty stopień dojrzałości w pięciostopniowej skali, by można było świadomie i skutecznie zarządzać procesami w organizacji) i wdrożyła zarządzanie procesowe. W przeciwnym razie zaleca się dokonywanie analizy w wyodrębnionych obszarach działania.

W tym celu należy zestawić powiązane ze sobą zadania i funkcjonalności ze względu na ich specyfikę rzeczową wynikającą z przepisów prawa lub powiązań strukturalno-organizacyjnych. Pomocnym kryterium może być klasyfikowanie według typu działalności:

- podstawowa – nakierowana bezpośrednio na klienta,
- zarządcza – determinująca skuteczne i efektywne funkcjonowanie organizacji,
- wspomagająca – dostarczająca niezbędnych zasobów do realizacji celów.

Następnie należy zidentyfikować systemy informacyjne stanowiące procesy biznesowe i systemy informacyjne niezbędne do skutecznego funkcjonowania pozostałych procesów oraz ustalić, które z nich są krytyczne ze względu na bezpieczeństwo informacji.

3.2. Identyfikacja ryzyka

Kolejny etap procesu zarządzania ryzykiem bezpieczeństwa informacji w modelu holistycznym to identyfikacja ryzyka. Można jej dokonać, analizując realizowane procesy. Wówczas w przebiegach procesów identyfikowane są działania newralgiczne, zagrożone utratą dostępności, integralności i poufności informacji. W wypadku analizy obszarów działania należy przeanalizować w sposób systematyczny każdy ze zidentyfikowanych obszarów. Można do tego wykorzystać listę kontrolną obejmującą wykaz kategorii potencjalnego ryzyka oraz kryteria ich segregacji. Przykładowe kategorie ryzyka zostały zaprezentowane w tabeli 1. Należy zauważyć, że bezpieczeństwo informacji występuje w tabeli dwukrotnie, tj. w odniesieniu do (1) kwestii organizacyjnych oraz do (2) sprzętu i informacji. W pierwszym przypadku informacja jest postrzegana jako czynnik łączący wszelkie aktywności organizacji, stanowiący jej swoisty krwiobieg, determinujący sprawność. W drugim zostały podniesione kwestie techniczne przekazu informacji.

Ponadto w procesie identyfikacji ryzyka zaleca się uwzględnić przesłanki historyczne:

1) niepowodzenia w osiąganiu celów w przeszłości, na przykład niezrealizowane zadania lub cele, przekroczenie planowanych wydatków itp.,
2) stwierdzone w przeszłości nieprawidłowości, takie jak naruszenie procedur, naruszenie prawa lub regulacji wewnętrznych, nieprawidłowe wydatki i inne.

Warto też tworzyć scenariusze zagrożeń. Daje to sposobność identyfikowania i precyzyjnego definiowania ryzyk rzadkich i niespodziewanych, określanych mianem „czarnych łabędzi”[4]. Taka analiza koncepcyjna stanowi dopełnienie podprocesu identyfikacji ryzyka.

Tabela 1

Przykładowe kategorie ryzyka

	Kategoria ryzyka	Charakterystyka kategorii
Wynikające z kontekstu wewnętrznego	kwestie organizacyjne	procedury, struktura urzędu, jakość usług i produktów tworzonych przez urząd, planowanie, organizacja pracy, charakter wykonywanej działalności, kultura organizacji, ciągłość działania, bezpieczeństwo informacji
	kwestie finansowe	dostępne środki finansowe, liczba, rodzaj i wielkość dokonywanych operacji finansowych, procedury finansowe
	zasoby ludzkie	liczba pracowników i ich kwalifikacje, szkolenia, odpowiedzialność i postawa kierownictwa
	sprzęt i informacja	narzędzia niezbędne do wykonywania zadań, dostęp do informacji, komunikacja, bezpieczeństwo informacji
Wynikające z kontekstu zewnętrznego	kwestie polityczne	cykle polityczne, decyzje polityczne, sposób prowadzenia polityki przez rząd i opozycję
	kwestie prawne	wpływ obecnych i przyszłych przepisów prawa, sprawy sądowe, jakość umów
	interesariusze, klienci, obywatele	wizerunek urzędu, współpraca z interesariuszami, protesty

Źródło: opracowanie własne.

Gromadzeniu i porządkowaniu informacji o ryzykach w organizacji służy rejestr ryzyka. Jego prowadzenie umożliwia kierującym organizacją szybkie zorientowanie się, z jakimi zagrożeniami, w jakich procesach/obszarach i z jakim natężeniem mogą mieć do czynienia przy realizacji celów. Zaleca się prowadzenie rejestru ryzyka w systemie informatycznym. Umożliwia to przede wszystkim

[4] Pojęcie „czarny łabędź” w odniesieniu do ryzyka wymyślił Nassim Nicholas Taleb – amerykański ekonomista, filozof, doktor zarządzania. W ujęciu autora, „czarny łabędź” to zdarzenie rzadkie, które można opisać na trzy sposoby: po pierwsze, jest nietypowe, co sprawia, że nie można go w żaden sposób przewidzieć; po drugie, jego wpływ na rzeczywistość jest ogromny, nieraz katastrofalny; po trzecie, jego wystąpienie, mimo braku możliwości jego przewidzenia, łatwo jesteśmy sobie w stanie wyjaśnić, co sprawia, że po fakcie wydaje nam się, że dane zdarzenie było jednak łatwo przewidzieć.

prowadzenie aktualnego rejestru ryzyka. Aktualność identyfikacji i oszacowania ryzyka jest tu cechą dominującą z punktu widzenia skuteczności zarządzania ryzykiem bezpieczeństwa informacji. Ponadto elektroniczny rejestr ryzyka ułatwia między innymi:

- automatyzację procesu szacowania ryzyka;
- wskazywanie obszarów, w których ryzyko przekracza dopuszczalny poziom, zarówno w formie liczbowej, jak i graficznej, co poprawia percepcję;
- sortowanie ryzyka ze względu na jego istotność;
- powiązanie ryzyka z innymi obszarami działalności poprzez analizę przyczyn i skutków; przykładowo: ryzyko związane z bezpieczeństwem informacji może zagrażać realizacji celu biznesowego, a czasem inne ryzyko może zagrażać bezpieczeństwu informacji.

Rejestr może zawierać dodatkowo jako opcję katalog przykładowych ryzyk występujących w organizacji, ich potencjalnych przyczyn i skutków (tabela 2). Ułatwia to identyfikację ryzyka, jego precyzyjny opis (zgodnie z zasadami dobrych praktyk prawidłowo sformułowane ryzyko powinno zawierać opis samego ryzyka, przyczynę i skutek) oraz ocenę wzajemnych zależności. Rozwiązaniem pożądanym jest prowadzenie rejestru ryzyka wspólnego dla bezpieczeństwa informacji i ogólnego systemu zarządzania organizacją w ramach sprawowanej kontroli zarządczej. Pozwala to powiązać zarządzanie ryzykiem bezpieczeństwa informacji z realizacją konkretnych celów, a także trafniej oszacować ryzyka z punktu widzenia funkcjonowania całej organizacji, a nie tylko wybranych aspektów.

Tabela 2

Przykładowe przyczyny i skutki ryzyka

Ryzyko	Potencjalne przyczyny	Potencjalne skutki
Ujawnienie/utrata informacji niejawnych i informacji prawnie chronionych	nieprzestrzeganie zasad polityki bezpieczeństwa informacji i ochrony danych	utrata poufności informacji
	brak polityki bezpieczeństwa informacji	zagrożenie dla bezpieczeństwa osób/kraju
	nieprawidłowe wykorzystywanie sprzętu komputerowego	pogorszenie wizerunku organizacji
	nieprawidłowa organizacja systemu bezpieczeństwa informacji i ochrony danych	

Źródło: opracowanie własne.

Proponowane holistyczne postrzeganie organizacji na etapie identyfikacji ryzyka:

- pozwala nabrać przekonania, że żaden z obszarów działalności nie został pominięty w procesie identyfikowania ryzyka;

- ułatwia identyfikację wpływu konkretnego ryzyka na inne aspekty funkcjonowania organizacji – to samo ryzyko może oddziaływać z różnym natężeniem na kilka aspektów [Ministerstwo Finansów, 2012: 28];
- pozwala hierarchizować (kaskadować) ryzyka pod kątem zarówno ich ważności realizacji celów, jak i kolejności w logicznym łańcuchu związków przyczynowo-skutkowych;
- dzięki zastosowanej konfiguracji ryzyk w odniesieniu do celów można zbadać wpływ ryzyk zidentyfikowanych do celów podrzędnych na realizację celów nadrzędnych.

3.3. Analiza i ocena ryzyka

Szacowanie ryzyka sprowadza się do ilościowo-jakościowej oceny dwóch zasadniczych parametrów ryzyka, tj. oddziaływania i prawdopodobieństwa. Na ogół szacowanie przeprowadza się z wykorzystaniem metody opisowo-analitycznej, a także doświadczenia i wiedzy pracowników w zakresie funkcjonowania organizacji. Jest to więc w znacznej mierze ocena subiektywna. O ile ocena prawdopodobieństwa niekorzystnego zdarzenia na ogół nie nastręcza trudności, o tyle ocena oddziaływania jest znacznie bardziej skomplikowana, ponieważ jest dokonywana według kilku kategorii, takich jak: finansowa, organizacyjna, wizerunkowa, prawna, ochrony zdrowia i bezpieczeństwa osób itp. Z kolei dobór kategorii dokonywany jest w zależności od ocenianego obszaru działania organizacji. Pojawiają się tu naturalne wątpliwości związane z oceną tego samego ryzyka oddziałującego na różne aspekty funkcjonowania organizacji. Przykładowo: w urzędzie skarbowym ryzyko ujawnienia/utraty informacji prawnie chronionych będzie przypuszczalnie inaczej oceniane w odniesieniu do celów związanych z poborem należności publiczno-prawnych, a inaczej – do ochrony samych informacji. W pierwszym przypadku dominującymi kryteriami oceny będą kryteria finansowe i prawne, w drugim zaś – prawne i wizerunkowe. Dlatego też w proponowanym modelu zarządzania ryzykiem postuluje się jednolite podejście do szacowania ryzyka, polegające na każdorazowym kontekstowym odnoszeniu się do aktualnie realizowanych w organizacji celów.

Innym problemem dotychczasowych rozwiązań jest różnorodność skal ocen stosowanych do oceny ryzyk w różnych aspektach działalności. Proponuje się stosowanie jednej, uniwersalnej skali do oceny zarówno prawdopodobieństwa, jak i skutków zdarzeń. Doboru skali należy dokonać w zależności od poziomu kultury organizacji. Istotne jest, by każdy pracownik – niezależnie od tego, czy jest wykonawcą, czy kierującym, oraz niezależnie od poziomu usytuowania w strukturze organizacyjnej – jednakowo pojmował i stosował zasady szacowania ryzyka.

Takie rozwiązanie ma oczywiste zalety. Po pierwsze, proponowane podejście do szacowania ryzyka umożliwi unifikację i standaryzację zasad oraz metod szacowania ryzyka. Po drugie, zmniejszy się liczba ryzyk podlegających

regularnej ocenie. Co prawda, to samo ryzyko będzie rozpatrywane w różnych kontekstach, co przysporzy więcej pracy związanej z jego analizą, ale wartością dodaną będzie gruntowna analiza zjawisk towarzyszących ryzyku – wieloaspektowe postrzeganie (warto porównać proponowany system z systemem zarządzania ryzykiem operacyjnym w bankach, w szczególności zasad wyznaczania KRI – *key risk indicators*, czyli kluczowych wskaźników ryzyka [Garczyński, 2012]). Tym samym nastąpi wzrost wiedzy na temat mechanizmów funkcjonowania organizacji.

Kolejnym zagadnieniem związanym z szacowaniem ryzyka bezpieczeństwa informacji jest częstotliwość dokonywania pomiaru. Obserwacje pokazują, że w organizacjach sektora publicznego analiza tej kategorii ryzyk dokonywana była nieregularnie. Najczęściej impulsem wymuszającym ponowne szacowanie ryzyka były zmiany przepisów związanych bezpośrednio lub pośrednio z bezpieczeństwem informacji bądź zmiany regulaminów organizacyjnych. Poza tym zaobserwowano, że terminy tych działań na ogół nie były zbieżne z terminami dokonywania analizy ryzyka na potrzeby na przykład kontroli zarządczej. Powodowało to między innymi problemy z harmonizacją działań związanych z kolejnym etapem procesu zarządzania ryzykiem – postępowaniem z ryzykiem. Zaleca się, by oceny ryzyka dokonywać łącznie z okresową oceną stopnia realizacji celów. Wprowadza to regularność i kompleksowość w zakresie czynności związanych z analizą ryzyka, a tym samym przyczynia się do porządkowania organizacji. Poza tym powoduje, że z zarządczego punktu widzenia dla każdego dokonującego analizy ryzyka punktem odniesienia jest rzecz najcenniejsza w organizacji, tj. realizacja założonych celów.

3.4. Postępowanie z ryzykiem

Jak zaznaczono we wstępie, jednym z zasadniczych problemów związanych z prowadzeniem wszelkiego rodzaju analiz ryzyka na potrzeby organizacji sektora publicznego jest ryzyko kolizji planowanych działań zaradczych. Wynika to z tego, że planujący te działania kierują się na ogół wyłącznie dobrem nadzorowanego przez siebie, wyodrębnionego obszaru działalności. Może to prowadzić do sytuacji, w której planujący muszą konkurować o zasoby: techniczne, ludzkie, finansowe i organizacyjne. Może się też zdarzyć, że dwa obszary ryzyka zachodzą na siebie i w ramach postępowania z ryzykiem jeden plan zakłada unikanie ryzyka, a drugi jedynie jego modyfikowanie.

W celu przeciwdziałania tego rodzaju kolizjom proponuje się zintegrowanie planowania działań zaradczych z procesami zarządzania organizacją oraz każdorazową ocenę wpływu planowanych działań na inne obszary funkcjonowania organizacji.

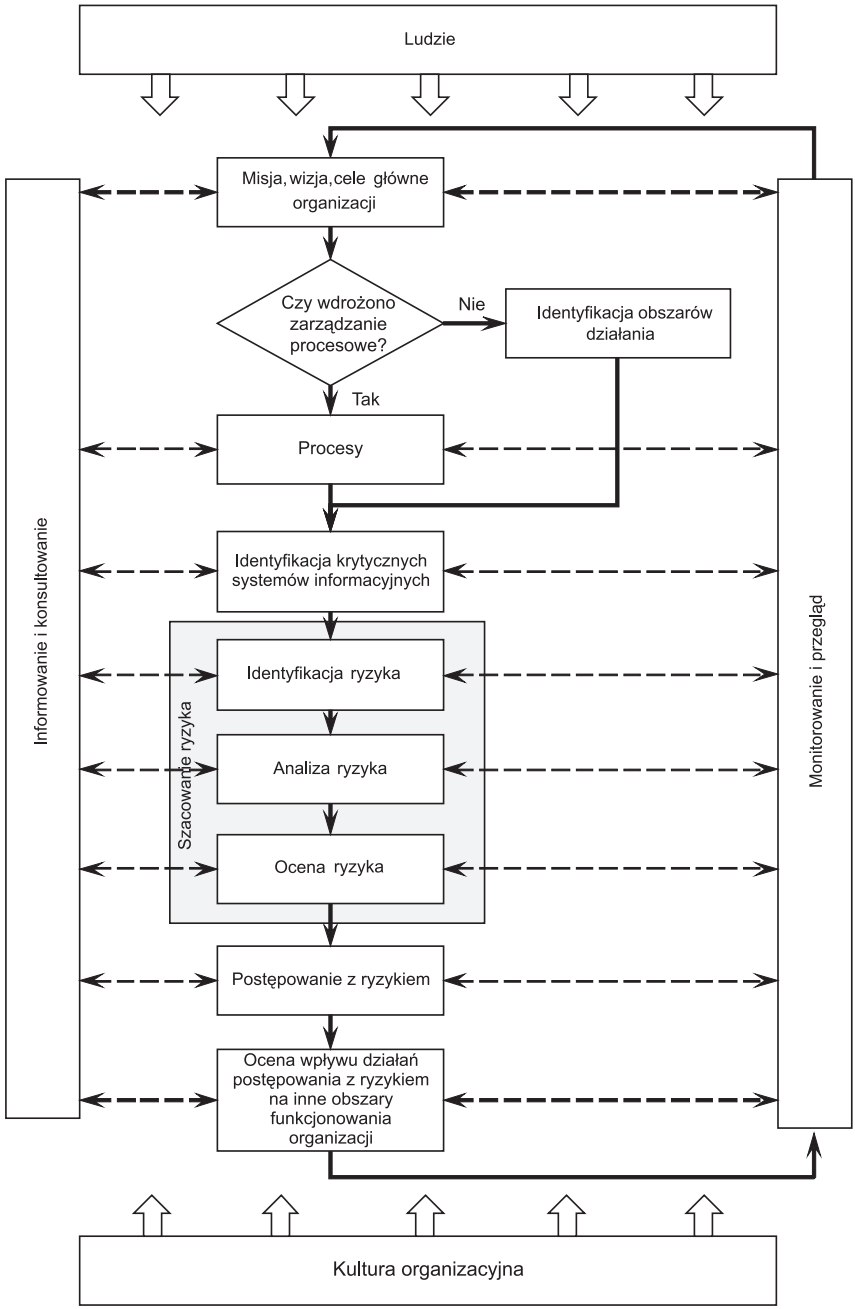
3.5. Informowanie i konsultowanie

Skuteczny i sprawny przepływ informacji o ryzyku pomiędzy pracownikami i zarządzającymi stanowi krytyczny element procesu zarządzania ryzykiem. W normie PN-ISO/IEC 27005:2014-01 zaleca się między innymi: „opracowanie planów informowania o ryzyku (…); utworzenie komitetu, gdzie może mieć miejsce dyskusja o typach ryzyka, ich priorytetach, o odpowiednim z nimi postępowaniu oraz ich akceptowaniu". O ile opracowanie planów informowania o ryzyku ma wymiar praktyczny, o tyle utworzenie komitetu do spraw ryzyka dotyczy raczej dużych organizacji, dysponujących odpowiednimi zasobami ludzkimi. Praktyka pokazuje, że podjęcie nawet takich działań nie gwarantuje sukcesu. Należy uruchomić tu mechanizmy zakorzenione w kulturze organizacji, a więc szerzyć wiedzę na temat rozwijania zdolności rozpoznawania czynników i symptomów ryzyka, tzw. inteligencję ryzyka [Apgar, 2008]. Ponadto trzeba przyjąć jako zasadę tworzenie wszelkiego rodzaju planów działania na podstawie analizy ryzyka i przy współudziale możliwie największej liczby członków organizacji (tryb konsultacyjny). Pogłębia to wiedzę o ryzyku w kontekście wieloaspektowym i pozwala zaplanować optymalne metody radzenia sobie z nim. Poza tym rozpoczęcie procesu zarządzania ryzykiem na wczesnym etapie zarządzania organizacją, tj. na etapie formułowania celów[5], zwiększa prawdopodobieństwo upowszechnienia wiedzy o wszelkich niekorzystnych zjawiskach towarzyszących funkcjonowaniu organizacji i pozwala lepiej dopasować ten proces do realiów.

3.6. Schemat modelu

Biorąc pod uwagę przyjęte założenia, model holistycznego podejścia do zarządzania ryzykiem bezpieczeństwa informacji w organizacjach sektora publicznego przyjmie kształt zaprezentowany na rysunku 2.

[5] W myśl standardów kontroli zarządczej najważniejsze dla organizacji systemy to system wyznaczania celów i zadań oraz system monitorowania ich realizacji. Elementy takie jak struktura organizacji czy zarządzanie ryzykiem są pochodnymi wyznaczonych celów.



Rysunek 2. Holistyczny model zarządzania ryzykiem bezpieczeństwa informacji w organizacjach sektora publicznego

Źródło: opracowanie własne na podstawie Polskiej Normy PN-ISO/IEC 27005:2014-01.

4. Zakończenie

Zaproponowana koncepcja holistycznego postrzegania organizacji każe traktować zarządzanie ryzykiem bezpieczeństwa informacji jako jedno z wielu ryzyk, organicznie związane z osiąganiem przez organizację celów. Takie podejście sprawia, że zarządzanie ryzykiem bezpieczeństwa informacji odbywa się na różnych poziomach i w różnych obszarach organizacji, przez co uzyskujemy pełniejszy obraz mechanizmów jej funkcjonowania. Możliwe jest także skomponowanie zidentyfikowanych ryzyk w logiczne łańcuchy przyczynowo-skutkowe, a przez to można lepiej zaplanować działania zaradcze, tj. skuteczniejsze i efektywniejsze kosztowo. Istotną zaletą jest również angażowanie w cały proces zarządzania ryzykiem bezpieczeństwa informacji szerokiego kręgu pracowników, nawet niezwiązanych bezpośrednio z gromadzeniem i przetwarzaniem informacji. Poszerza to znacznie wiedzę organizacyjną o ryzyku oraz daje większą pewność, że wszelkie niekorzystne zjawiska zostaną na czas dostrzeżone i podejmie się skuteczne kroki zaradcze. Wszystko to sprzyja usprawnieniu funkcjonowania organizacji. Od umiejętności zarządczych kierujących organizacjami publicznymi zależy, na ile uda się ów proces uczynić trwałym elementem kultury organizacji.

Bibliografia

Apgar D. (2008), *Inteligencja ryzyka. Jak nauczyć się zarządzania niewiadomym*, Onepress, Warszawa.

Beasley M., Branson B., Hancock B. (2010), *Developing Key Risk Indicators to Strengthen Enterprise Risk Management*, COSO, www.coso.org [dostęp: 27.09.2017].

Blakley B., McDermott E., Geer D. (2001), *Information Security is Information Risk Management*, New Security Paradigms Workshop.

Burlton R.T. (2001), *Business Process Management: Profiting from Process, Sams Publishing*, Indianapolis.

Chrapko M. (2010), *CMMI – doskonalenie procesów w organizacji*, WN PWN, Warszawa.

Davies J., Finlay M., McLenaghen T., Wilson D. (2006), *Key Risk Indicators – Their Role in Operational Risk Management and Measurement*, „Risk Business International Limited".

Garczyński D. (2012), *Zarządzanie ryzykiem operacyjnym w banku z wykorzystaniem Kluczowych Wskaźników Ryzyka*, „Annales Universitatis Mariae Curie-Skłodowska", sectio H, 46, 4.

Kwo-Shing Hong, Yen-Ping Chi, Louis R. Chao, Jih-Hsing Tang (2003), *An Integrated System Theory of Information Security Management*, „Information Management & Computer Security", 11 (5).

Ministerstwo Finansów (2012), *Zarządzanie ryzykiem w sektorze publicznym*. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce, http://www.mf.gov.pl [dostęp: 27.09.2017].

Pipkin D.L (2002), *Bezpieczeństwo informacji*, Wydawnictwo Naukowo-Techniczne, Warszawa.

Polska Norma PN-ISO 31000:2012, *Zarządzanie ryzykiem. Zasady i wytyczne*.

Polska Norma PN-ISO/IEC 27005:2014-01, *Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji*.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, http://data.europa.eu/eli/reg/2016/679/oj [dostęp: 27.09.2017].

Rummler G.A., Brache A.P. (2000), *Podnoszenie efektywności organizacji*, tłum. T. Ludwicki, PWE, Warszawa.

Soomro Z.A., Shah M.H., Javed A. (2015), *Information Security Management Needs more Holistic Approach: A Literature Review*, „International Journal of Information Management" 36.

Spears J.L. (2005), *A Holistic Risk Analysis Method for Identyfying Information Security Risks* [w:] P. Dowland, S. Furnell, B. Thuraisinngham, X.S. Wang, *Security Management, Integrity, and Internal Control in Information Systems*, IICIS 2004, IFIP International Federation for Information Processing, vol. 193, Springer, Boston.