Ekonomiczne Problemy Usług nr 123

ISSN: 1896-382X | www.wnus.edu.pl/pl/epu/
DOI: 10.18276/epu.2016.123-30 | strony: 321-336

JERZY STANIK, ROMUALD HOFFMANN, JAROSŁAW NAPIÓRKOWSKI
Wojskowa Akademia Techniczna[1]

ZARZĄDZANIE RYZYKIEM W SYSTEMIE ZARZĄDZANIA BEZPIECZEŃSTWEM ORGANIZACJI

Streszczenie

W artykule autorzy podejmują problematykę analizy ryzyka i zarządzania ryzykiem w ogólnie rozumianej organizacji oraz wpływu na jej bezpieczeństwo. Podkreślają wagę i znaczenie prowadzenia ciągłej analizy istotnych czynników ryzyka, ich identyfikacji oraz sposobu postępowania z nimi. Artykuł zawiera także przegląd procesu zarządzania ryzykiem z uwzględnieniem tzw. „dobrych praktyk" mających w nim zastosowanie. Podsumowanie przedstawia pozytywne konsekwencje prowadzenia procesu zarządzania ryzykiem przez organizacje, a także problemy związane z jego praktyczną realizacją.
Słowa kluczowe: analiza ryzyka, zarządzanie ryzykiem, modele zarządzania ryzykiem, zarządzanie ryzykiem w bezpieczeństwie organizacji.

Wprowadzenie

Wraz z nasilaniem się zmian występujących w otoczeniu zarządy przedsiębiorstw i firm wyraźniej dostrzegają różnego rodzaju ryzyka związane z prowadzoną działalnością gospodarczą oraz poświęcają więcej uwagi tematyce zarządzania ryzykiem. Kwestie zarządzania ryzykiem stają się istotną częścią zarządzania strategicznego przedsiębiorstwem i w wielu wypadkach są kluczowe dla zracjonalizowania działalności organizacji oraz ciągłości jego działania.

Częstym błędem w procesie zarządzania organizacją jest odseparowanie systemu/procesu zarządzania ryzykiem i traktowania go jak odrębnej wyspy. Przecież

[1] Wydział Cybernetyki.

w naszych organizacjach funkcjonują już systemy zarządzania procesami, zarządzania jakością, zarządzania projektami, zarządzania celami, kontrola i audyt wewnętrzny, które z jednej strony są doskonałym źródłem danych do analizy ryzyka, a z drugiej strony analiza ryzyka dostarcza nam wiedzy na temat zagrożeń, podatności i potencjałów dla tych obszarów.

Wiele dyskusyjnych nieporozumień w ocenie bezpieczeństwa organizacji jest często skutkiem braku świadomości i niewłaściwego toku rozumowania. W ferworze prowadzonych sporów i udowadniania swoich racji rozmówcy zapominają o tym, że bezpieczeństwo nie jest stanem, ale ciągle zmieniającym się procesem, którego wewnętrzne i zewnętrzne uwarunkowania są, w różnym (czasami dużym) stopniu, zależne od organizacji, której bezpośrednio dotyczą. Dlatego istotnym elementem w procesie zapewnienia bezpieczeństwa wewnętrznego czy też zewnętrznego jest system zarządzania bezpieczeństwem informacji spełniający kluczową rolę w rozwiązywaniu sytuacji krytycznych lub kryzysowych.

1. Konstrukcja modelu Systemu Bezpieczeństwa Organizacji

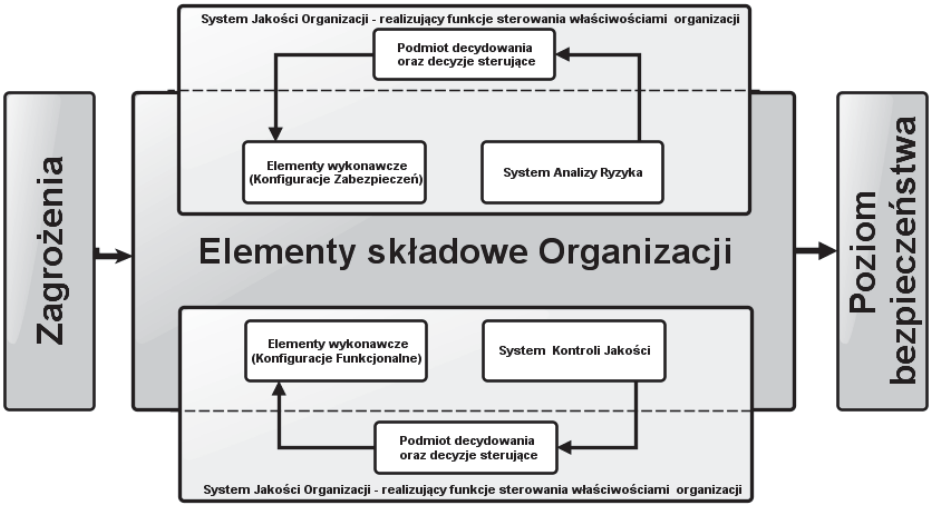
W ujęciu analizy systemowej (Sienkiewicz 2007, s. 47) bezpieczeństwo organizacji można rozpatrywać jako własność obiektu charakteryzującą jego odporność na powstanie sytuacji niebezpiecznej, przy czym uwagę koncentruje się wtedy na zawodności bezpieczeństwa obiektu, czyli jego podatności na powstanie sytuacji niebezpiecznych i jego funkcjonowania w określonym czasie. Z drugiej strony natomiast bezpieczeństwo organizacji należy traktować jako jej zdolność do ochrony wewnętrznych wartości (aktywów wrażliwych) przed zagrożeniami. Następuje wtedy bezpośredni związek z takimi cechami systemowymi jak: jakość, niezawodność, stabilność, równowaga, żywotność. Dlatego też zarządzanie bezpieczeństwem organizacji jest integralną częścią zarządzania systemowego i jest związane z racjonalizacją wyboru środków zapewniających bezpieczne funkcjonowanie organizacji w niebezpiecznym środowisku. Tworzenie systemu bezpieczeństwa (rysunek 1) ma natomiast na celu zmniejszenie ludzkich obaw i strachu przed tym, co niesie przyszłość, przy założeniu, że zapewnienie stuprocentowego stanu bezpieczeństwa jest niemożliwe. Chodzi zatem jedynie o ograniczenie, a nie całkowitą likwidację zagrożeń, które są immanentną stroną ludzkiego życia.

Rys. 1. Łańcuch systemu zarządzania jakością/niezawodnością, ryzykiem i bezpieczeństwem

Źródło: opracowanie własne.

Bezpieczeństwo i niezawodność to dziedzina inżynierii zajmująca się zapobieganiem zagrożeniom poprzez odpowiednio zaprojektowane zabezpieczenia o ściśle określonych funkcjach. Zaprojektowana funkcja musi być precyzyjnie pełniona w ściśle określonych warunkach realnego zagrożenia i w określonym czasie. Bezpieczeństwo i niezawodność kancelarii są uzyskiwane poprzez wbudowanie do elementów składowych kancelarii specjalizowanych konfiguracji bezpieczeństwa i niezawodności, które realizują funkcje zabezpieczania na podstawie sygnałów wejściowych – zagrożeń. Pewność i jakość realizacji funkcji zabezpieczania determinuje wymagany poziom bezpieczeństwa funkcjonalnego oraz poziom redukcji zagrożenia spowodowanego awarią.

Graficzną ilustrację organizacji z punktu widzenia sterowania jej bieżącymi właściwościami użytkowymi i utrzymania bieżącego poziomu bezpieczeństwa przedstawiono na rysunku 2.



Rys. 2. Ilustracja organizacji z punktu widzenia sterowania jej właściwościami użytkowymi i poziomem bezpieczeństwa

Źródło: opracowanie własne.

Na rysunku tym wyróżniono trzy istotne elementy:

1. Elementy składowe organizacji, rozumiane jako zespół sił i środków oraz powiązań pomiędzy nimi, zapewniających dostarczanie produktów/usług biznesowych wyspecyfikowanych w misji lub wizji organizacji;
2. System Bezpieczeństwa Organizacji, rozumiany jako zespół sił i środków oraz powiązań pomiędzy nimi, zapewniających pożądany poziomu bezpieczeństwa organizacji;

3. System Jakości Organizacji, rozumiany jako zespół sił i środków oraz powiązań pomiędzy nimi, zapewniających wymaganą/wysoką jakość/niezawodność dostarczanych produktów/usług poprzez możliwość sterowania jej właściwościami użytkowymi, a w szczególności jej elementów składowych/dziedzinowych organizacji.

Bezpieczeństwo funkcjonowania organizacji jest wypadkową bezpieczeństwa funkcjonowania jej elementów składowych (dziedzinowych), między innymi takich jak np.:

- system produkcyjny/wykonawczy, który stanowią siły i środki realizujące wykonawcze procesy biznesowe;
- system zarządzania, który realizuje procesy informacyjno-decyzyjne, decydujące o sposobie funkcjonowania podsystemu produkcyjnego/ wykonawczego;
- systemy techniczne wspomagające system produkcyjny lub system zarządzania;
- systemy informatyczne wspomagające system produkcyjny lub system zarządzania.

O poziomie bezpieczeństwa funkcjonowania elementów składowych organizacji stanowią poziomy ich bezpieczeństwa dziedzinowego. Funkcjonowanie każdego z elementów składowych organizacji może być zakłócane przez:

- zagrożenia naturalne: powodzie, warunki pogodowe, huragany itp.;
- awarie techniczne urządzeń i systemów, np.: energetycznych, informatycznych itp.;
- zagrożenia cywilizacyjne: chemiczne, radiacyjne, komunikacyjne itp.;
- zagrożenia wynikające z położenia i specyfiki regionalnej, między innymi takie jak np.: przemyt, uwarunkowania narodowościowe, religijne itp.;
- destrukcyjne działanie człowieka.

Poszczególne rodzaje zagrożeń mogą występować jednocześnie i oddziaływać destrukcyjnie na elementy składowe organizacji. Ponadto może występować efekt ich synergii, która w analizie kompleksowego bezpieczeństwa organizacji nie powinna być pomijana. Bezpieczeństwo funkcjonowania organizacji zapewnia się poprzez:

- permanentne zapobieganie powstawaniu poszczególnych rodzajów zagrożeń funkcjonowania elementów składowych organizacji (obiektów);
- stałe przygotowanie obiektów i służb odpowiedzialnych za bezpieczeństwo dziedzinowe organizacji na ewentualność wystąpienia określonych rodzajów zagrożeń;
- prowadzenie skutecznych działań naprawczych w przypadku ich wystąpienia;

– odtwarzanie zdolności funkcjonalnych obiektów dotkniętych zagrożeniami, po ich wyeliminowaniu.

Poziom bezpieczeństwa organizacji, w rozumieniu kompleksowym, zależy od dziedzinowych poziomów bezpieczeństwa. Określony poziom bezpieczeństwa dziedzinowego organizacji możemy uzyskać na wiele sposobów – nie tylko poprzez zapewnienie określonej skuteczności bezpośredniego przeciwdziałania zaistniałym zdarzeniom dzięki systemowi zabezpieczeń. Na jego wartość możemy wpływać również poprzez:

– zapobieganie powstawaniu danego rodzaju zagrożenia bezpieczeństwa;
– przygotowanie podmiotu na wypadek uaktywnienia danego rodzaju zagrożenia bezpieczeństwa w postaci zdarzenia (edukacja, rozmieszczenie i dostępność sił i środków przeciwdziałania);
– zwiększanie skuteczności sił i środków mechanizmów bezpieczeństwa w trakcie przeciwdziałania skutkom danego zdarzenia;
– skuteczność działań w usuwaniu następstw danego zdarzenia.

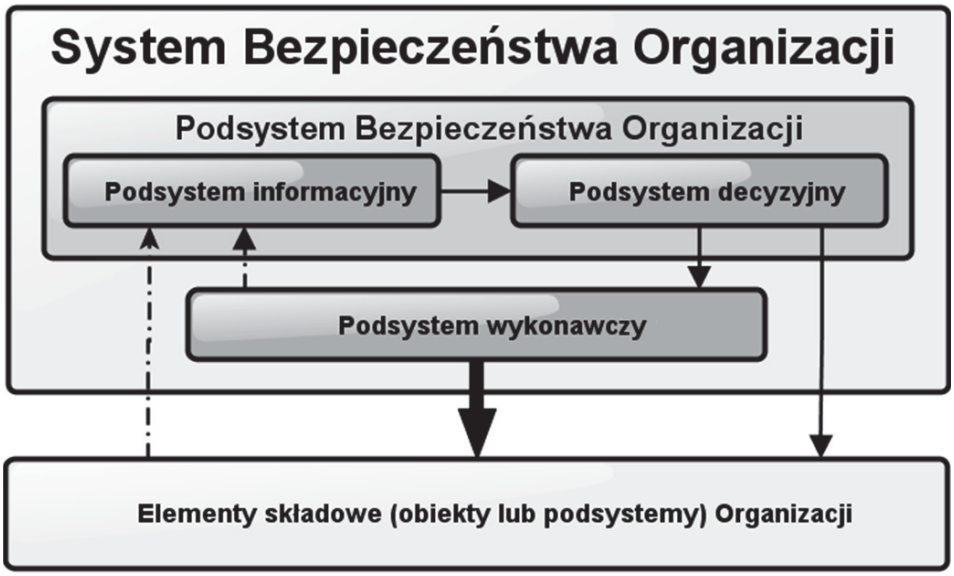
Mamy zatem możliwość kształtowania poziomu bezpieczeństwa dziedzinowego i kompleksowego. Wielkościami sterowalnymi w tym przypadku są parametry charakteryzujące czynniki wpływające na poziom bezpieczeństwa organizacji, to jest związane z:

– zapobieganiem możliwych dla niej zagrożeń bezpieczeństwa;
– przygotowaniem kancelarii na wypadek uaktywnienia tych zagrożeń;
– mechanizmami bezpieczeństwa przeciwdziałającymi tym zagrożeniom;
– usuwaniem następstw danego zdarzenia.

Każda organizacja musi zatem czynić starania o zapewnienie sobie stabilności stanu bezpieczeństwa. W tym celu tworzony jest system bezpieczeństwa organizacji (SBO). W ujęciu modelowym w Systemie Bezpieczeństwa Organizacji wyróżniamy dwa podsystemy (rysunek 3):

– wykonawczy, który stanowią siły i środki realizujące procesy wykonawcze;
– podsystem zarządzania bezpieczeństwem kancelarii, który realizuje procesy informacyjno-decyzyjne decydujące o sposobie zapewniania bezpieczeństwa poszczególnym obiektom kancelarii przez podsystem wykonawczy.

Zakłada się, że celem działania Podsystemu Zarządzania Bezpieczeństwem Organizacji (PZBO) jest utrzymanie wymaganego poziomu bezpieczeństwa organizacji jako całości funkcjonalnej oraz zapewnienie bezpieczeństwa zasobów wrażliwych. Cel ten można osiągnąć poprzez bieżące sterowanie podsystemem wykonawczym użytkowania zabezpieczeń. W skład Podsystemu Zarządzania Bezpieczeństwem Organizacji (PZBO) wchodzą dwa podsystemy (rysunek 3).



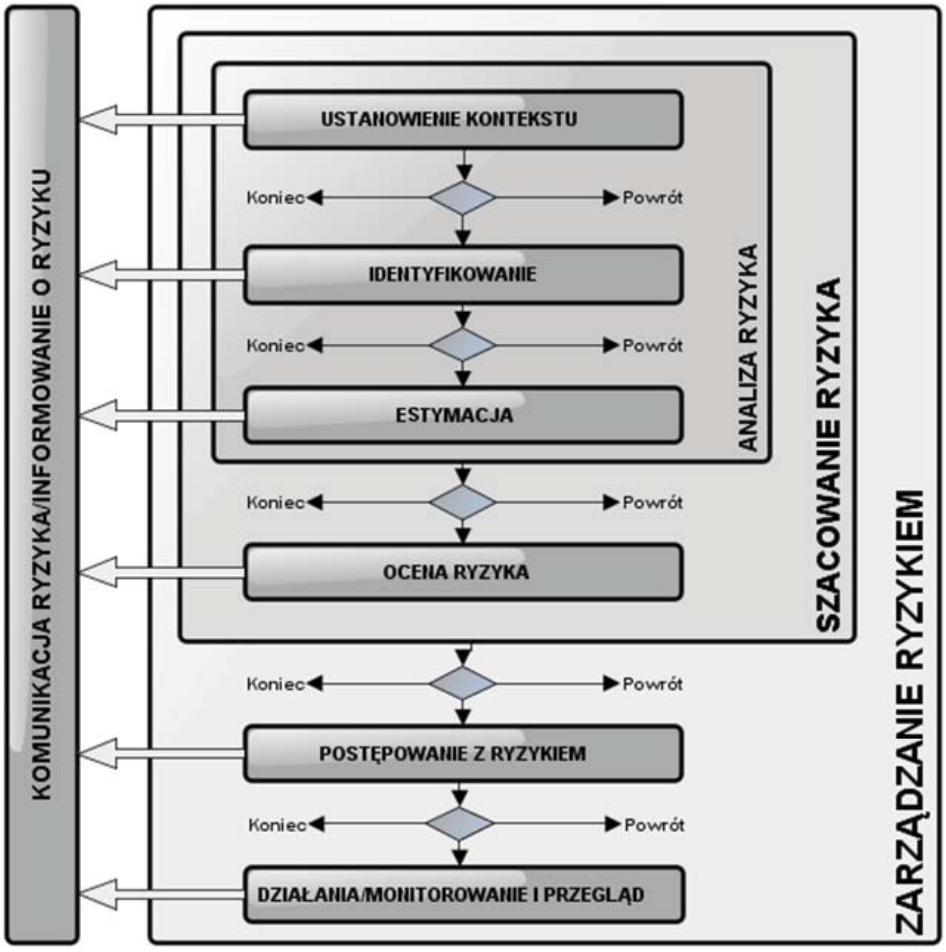
Rys. 3. Struktura funkcjonalna Systemu Bezpieczeństwa Organizacji

Źródło: opracowanie własne.

Zadanie, jakie ma do spełnienia System Bezpieczeństwa Organizacji, to przede wszystkim przygotowanie określonego podmiotu organizacji – służb bezpieczeństwa – na możliwość wystąpienia zagrożeń, radzenia sobie z nimi w odpowiedni sposób oraz przywracanie sytuacji do stanu pierwotnego sprzed wystąpienia tego zagrożenia. Proces zarządzania bezpieczeństwem w organizacji powinien być prowadzony w sposób ciągły, stale udoskonalany i realizowany planowo z jednoczesnym określeniem stopnia ryzyka, jego akceptacji poprzez określenie progu tolerancji, po przekroczeniu którego konieczne będzie zarządzanie tym ryzykiem.

2. Zarządzanie ryzykiem w organizacji

„Zarządzanie ryzykiem" oznacza planowe stosowanie polityki, procedur i praktyk zarządczych w ramach zadań dotyczących analizy, wyceny i nadzoru ryzyka (rysunek 4).



Rys. 4. Model procesu zarządzania ryzykiem w organizacji

Źródło: opracowanie własne.

Zarządzanie ryzykiem wspiera i wpływa na większą efektywność zarządzania organizacją, ponieważ pomaga zrozumieć i ocenić groźne czynniki ryzyka. Dlatego celem zarządzania ryzykiem w organizacji powinno być:

- pozyskanie informacji o możliwych zagrożeniach i ich wpływie na przyszły kształt otoczenia zewnętrznego podmiotu;
- określenie skutków wynikających z bieżących zdarzeń, które mogą mieć jakikolwiek wpływ na funkcjonowanie i wyniki organizacji;
- opracowanie właściwych procedur postępowania (przygotowanie do następstw) w sytuacjach awaryjnych, w szczególności do ryzyk nieprzewidywalnych.

Zarządzanie ryzykiem jest procesem ciągłym i powinno być logicznie uporządkowanym ciągiem następujących po sobie zdarzeń, działań, decyzji, których efektem jest powstanie pewnej wartości dodanej, jaką jest bezpieczeństwo podmiotu. Dlatego też identyfikowanie możliwego ryzyka (kryzysu) jest kluczowym zadaniem mającym na celu uniknięcie zaskoczenia, jakim może być nagła sytuacja kryzysowa. Powinniśmy mieć świadomość, że aby efektywnie zająć się analizą ryzyka, należy to ryzyko w miarę precyzyjny sposób zdefiniować, ustalając jego przyczyny, zakres, granice oraz określić rodzaj możliwych zagrożeń mogących mieć wpływ na realizację celów postawionych przez podmiotem.

Powinniśmy zdawać sobie sprawę, że analiza ryzyka jest podstawowym elementem systemu zarządzania ryzykiem w organizacji, ponieważ w procesie analizy ryzyka tworzy się informacje niezbędne do podejmowania właściwych decyzji w zakresie: strategii postępowania z ryzykiem, efektywnego doboru środków redukcji ryzyka, oceny zasadności transferu, akceptacji lub unikania tegoż ryzyka. Te istotne informacje, z punktu widzenia zarządzania organizacją, a wypracowane w trakcie prowadzonej analizy ryzyka, wskazują także priorytety dla rozwoju systemów bezpieczeństwa, zabezpieczeń i kontroli w organizacji. Zasadne wydaje się zatem stwierdzenie, że analiza ryzyka służy do minimalizacji (optymalizacji) strat związanych z ryzykiem operacyjnym. W tym miejscu możemy postawić sobie pytanie: dlaczego obecnie obserwujemy stale rosnący nacisk na zarządzanie ryzykiem? Odpowiedź jest prosta, ponieważ przykłady z życia pokazały, że w sytuacji niepewności oraz możliwości optymalizacji ryzyka poprzez usunięcie często zbędnych, nieskutecznych, ale kosztownych zabezpieczeń − takie podejście jest poprawne. Bowiem tradycyjne zabezpieczanie wszystkich obszarów działań organizacji okazuje się nadmiernie kosztowne i nieskuteczne − bo zazwyczaj zawsze brakuje zasobów (warianty oszczędne). Konieczne zatem jest nie tylko unikanie i redukowanie ryzyka, ale sprawne zarządzanie tym ryzykiem.

3. Przegląd standardów zarządzania ryzykiem

W zakresie zarządzania ryzykiem nie ma znaczących polskich rozwiązań, ale istnieje kilka obcych standardów utworzonych przez różnego rodzaju organizacje zajmujące się wymienioną problematyką. Międzynarodowym standardem określającym podejście do procesu zarządzania ryzykiem jest norma ISO 31000:2009. Dokument ten zawiera ogólne zasady i wytyczne dotyczące zarządzania ryzykiem, które mogą być stosowane we wszystkich organizacjach, ponieważ nie są one specyficzne dla konkretnej branży czy sektora. W związku z tym, że ISO 31000 nie promuje jednolitego modelu zarządzania ryzykiem, standard ten nie jest przeznaczony do celów certyfikacji. Służy on przede wszystkim do zharmonizowania

i wsparcia innych norm ISO związanych z ujętymi w nich i opisanymi konkretnymi rodzajami zagrożeń.

Według normy ISO 31000 zarządzanie ryzykiem jako element strategicznego zarządzania przedsiębiorstwem musi być poprzedzone silnym i trwałym zaangażowaniem zarządu przedsiębiorstwa oraz pozostałej kadry kierowniczej, odpowiedzialnej za wszystkie poziomy zarządzania. Zaangażowanie to stanowi swego rodzaju wejście w pętlę dodatniego sprzężenia zwrotnego, która obejmuje cały proces zarządzania ryzykiem i przebiega przez wszystkie jego etapy. Na proces ten składają się: projektowanie struktury dla zarządzania ryzykiem, wdrażanie zarządzania ryzykiem, monitorowanie i przegląd istniejącej struktury oraz jej ciągłe doskonalenie. Następnie niezbędne jest sprzężenie zwrotne, dzięki któremu informacja o koniecznych zmianach struktury zarządzania ryzykiem przekazywana jest do etapu ponownego jej projektowania. Standard ISO 31000 zaleca projektowanie struktury ramowej dla zarządzania ryzykiem, która obejmuje analizę strategiczną otoczenia organizacji oraz jej wnętrza, a także system celów przedsiębiorstwa powiązanych wzajemnymi relacjami.

Oprócz międzynarodowej normy ISO istnieje również kilka innych standardów zarządzania ryzykiem, takich jak standard opracowany w Wielkiej Brytanii, opublikowany przez Federację Europejskich Stowarzyszeń Zarządzania Ryzykiem (Federation of European Risk Management Associations, FERMA) czy amerykański Enterprise Risk Management – Integrated Framework (Zarządzanie Ryzykiem Korporacyjnym – zintegrowana struktura ramowa), zwany COSO II, który został opracowany przez Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Wymienione standardy zintegrowanego zarządzania ryzykiem organizacji, wskazują na konieczność identyfikacji czynników wpływających na zdarzenia, które wywierają wpływ na realizację strategii i osiąganie postawionych przez organizację celów. Samo zidentyfikowanie czynników ryzyka i związanych z nimi zdarzeń nie wyczerpuje jednak procesu zarządzania ryzykiem. Przytoczone standardy podkreślają konieczność prowadzenia procesu analizy i oceny ryzyka oraz reakcji na ryzyko, a więc odpowiedniego postępowania wobec ryzyka. Postulują także wybór wspólnych metod oceny bezpieczeństwa (CSM), których celem jest budowanie jednolitego podejścia do kwestii bezpieczeństwa. Jednym z takich narzędzi jest wspólna metoda bezpieczeństwa w zakresie wyceny i oceny ryzyka (CSM) opisana w obowiązującym od 21 maja 2015 r. rozporządzeniu wykonawczym Komisji (UE) nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009.CSM w zakresie wyceny i oceny ryzyka znajduje zastosowanie:

1) jeżeli ocena ryzyka jest wymagana w odpowiednich technicznych specyfikacjach interoperacyjności (TSI); w takim przypadku TSI określają, w razie potrzeby, które elementy CSM mają zastosowanie;

2) aby zapewnić bezpieczną integrację podsystemów strukturalnych, do których mają zastosowanie TSI, z istniejącym systemem, zgodnie z art. 15 ust. 1 dyrektywy 2008/57/WE.

Jednakże, stosowanie CSM w przypadku, o którym mowa w akapicie pierwszym lit. b) nie może prowadzić do wymogów sprzecznych z wymogami, które są określone w odpowiednich TSI i mają charakter obligatoryjny.

Podstawą opracowania wspólnej metody bezpieczeństwa w zakresie wyceny i oceny ryzyka była potrzeba zharmonizowania na poziomie Unii Europejskiej metod stosowanych przez podmioty kolejowe uczestniczące w rozwoju i eksploatacji systemu kolejowego w celu identyfikacji ryzyka i zarządzania nim oraz metod wykazywania zgodności systemu kolejowego z wymogami bezpieczeństwa.

4. Proces zarządzania ryzykiem w bezpieczeństwie informacji – elementy dobrej praktyki

Proces zarządzania ryzykiem rozpoczyna się od ustalenia/wskazania systemu podlegającego ocenie, np. System Bezpieczeństwa Organizacji, i obejmuje następujące działania:

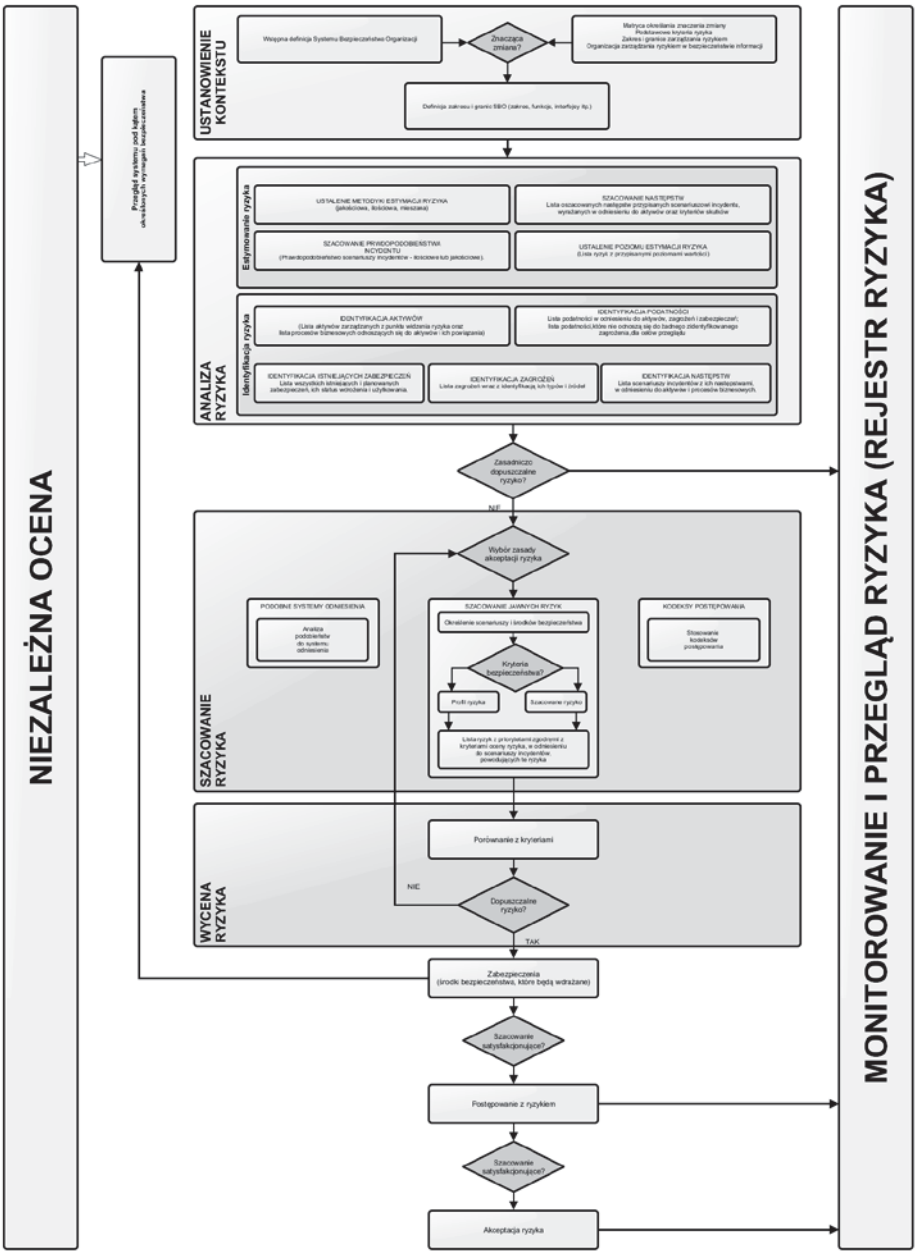
- proces oceny ryzyka obejmujący: definicję systemu i jego granice, analizę ryzyka, w tym identyfikację zagrożeń, ryzyko, związane z nimi środki bezpieczeństwa oraz wymogi bezpieczeństwa, które powinien spełniać oceniany system;
- wykazanie zgodności systemu w zakresie bezpieczeństwa ze zidentyfikowanymi wymogami bezpieczeństwa;
- zarządzenie wszystkimi zidentyfikowanymi zagrożeniami oraz związanymi z nimi środkami bezpieczeństwa.

Proces zarządzania ryzykiem ma charakter wieloetapowy. Jego przebieg przedstawiono na rysunku 5. Proces ten kończy się z chwilą wykazania zgodności systemu ze wszystkimi wymogami bezpieczeństwa koniecznymi do zaakceptowania ryzyka związanego ze zidentyfikowanymi zagrożeniami. Do zbioru podstawowych działań w zakresie zarządzania ryzykiem w bezpieczeństwie informacji między innymi można zaliczyć:

1. Ustanowienie kontekstu – zebranie wszystkich informacji o organizacji mających odniesienie do zarządzania ryzykiem w bezpieczeństwie organizacji.
2. Analiza ryzyka – systematyczne wykorzystywanie wszystkich dostępnych informacji do identyfikowania zagrożeń i szacowania ryzyka; określenie zbioru czynników ryzyka w środowisku wewnętrznym i zewnętrznym organizacji oraz ustalenie zbioru działań skierowanych na obniżenie negatywnego wpływu zidentyfikowanych czynników ryzyka na funkcjonowa-

nie organizacji i podejmowanie odpowiednich działań służących przeciwdziałaniu i ograniczaniu ryzyka.

3. Szacowanie/estymacja ryzyka – polega na przypisaniu wartości prawdopodobieństwu i następstwom ryzyka. Wartościami tymi mogą być: rachunek zysków i strat, obawy uczestników i inne zmienne, odpowiednie do oceny ryzyka. Estymowane ryzyko jest połączeniem prawdopodobieństwa scenariusza incydentu i jego następstw. Przykłady różnych metod i podejść do estymacji ryzyka w bezpieczeństwie informacji można znaleźć w załączniku E normy ISO/IEC 27005:2014 Zarządzanie ryzykiem w bezpieczeństwie informacji. Kodeks postępowania oznacza spisany zbiór zasad, które mogą być wykorzystywane do nadzorowania określonego zagrożenia lub określonych zagrożeń, pod warunkiem ich prawidłowego stosowania; „system odniesienia" oznacza system, który sprawdził się w praktyce jako system o dopuszczalnym poziomie bezpieczeństwa i z którym można porównywać system oceniany pod kątem dopuszczalności ryzyka.
4. Wycena ryzyka – oznacza procedurę opierającą się na analizie ryzyka, która ma na celu ustalenie, czy osiągnięto poziom dopuszczalnego ryzyka – porównanie jego wielkości z założonym, dopuszczalnym progiem tolerancji na ryzyko.
5. Estymacja ryzyka polega na przypisaniu wartości prawdopodobieństwu i następstwom ryzyka. Wartości te mogą być ilościowe lub jakościowe. Estymacja ryzyka jest oparta na oszacowanych następstwach i prawdopodobieństwie. Dodatkowo można brać pod uwagę rachunek zysków i strat, obawy uczestników i inne zmienne, odpowiednie do oceny ryzyka. Estymowane ryzyko jest połączeniem prawdopodobieństwa scenariusza incydentu i jego następstw.
6. Ustalenie zabezpieczeń/„środki bezpieczeństwa" – pakiet działań zmniejszających częstotliwość zagrożeń albo łagodzących ich skutki, który ma na celu osiągnięcie lub utrzymanie dopuszczalnego poziomu ryzyka;



Rys. 5. Elementy dobrej praktyki w procesie zarządzania ryzykiem w bezpieczeństwie organizacji

Źródło: opracowanie własne.

7. Akceptacja ryzyka/kryteria akceptacji ryzyka – zasady, które są stosowane w celu wyciągnięcia wniosku o dopuszczalności lub niedopuszczalności ryzyka związanego z określonym zagrożeniem lub określonymi zagrożeniami. „Kryteria akceptacji ryzyka" – kryteria, na podstawie których oceniana jest dopuszczalność danego ryzyka; kryteria te stosuje się, aby ustalić, czy poziom ryzyka jest na tyle niski, że nie jest konieczne podejmowanie natychmiastowych działań w celu jego zredukowania;
8. Informowanie o ryzyku – prowadzenie rejestru zagrożeń, w którym rejestruje się i opatruje odniesieniami zidentyfikowane zagrożenia, związane z nimi środki i źródło zagrożeń oraz wskazuje organizację, która ma nimi zarządzać;

Zarządzanie ryzykiem jest zakresem działań, które musi podjąć podmiot działania organizacji, aby występujące ryzyko było na poziomie akceptowalnym dla bezpieczeństwa danej organizacji. Jest to proces „prowadzenia" ryzyka pod kontrolą obejmujący zakres działań związanych z analizą tego ryzyka, jego redukcji lub transferem oraz minimalizacją strat, jeśli już wystąpi. Zarządzanie ryzykiem jest procesem ciągłym i powinno być logicznie uporządkowanym ciągiem następujących po sobie zdarzeń, działań, decyzji, których efektem jest powstanie pewnej wartości dodanej, jaką jest bezpieczeństwo podmiotu[2].

Podsumowanie

Procesy zarządzania ryzykiem w bezpieczeństwie powinny być nieodłączną częścią życia każdej organizacji. Aby proces zarządzania ryzykiem mógł być jednak skuteczny, należy zastanowić się, jakie działania, metody, techniki lub narzędzia zarządzania dla organizacji będą najlepsze. Aby skutecznie prowadzić politykę zarządzania ryzykiem w organizacji, należy najpierw określić, jakie są cele i zadania tej jednostki w zakresie zarządzania ryzykiem i uzgodnić je z ogólną strategią organizacji. Jako że ryzyko jest nieodłącznie wpisane w funkcjonowanie każdej organizacji, zarządzanie nim powinno być naturalną czynnością na każdym poziomie kierowania. Często powielane są opinie, że ryzykiem zarządza się zawsze, jednakże nie zawsze w sposób świadomy.

Analiza ryzyka i zarządzanie ryzykiem jest podstawowym elementem zarządzania w organizacji, służącym do minimalizacji strat związanych z wystąpieniem sytuacji kryzysowej i ryzykiem operacyjnym. Jest narzędziem (elementem) wspo-

[2] Zgodnie z przepisami Unii Europejskiej „zarządzanie ryzykiem" oznacza planowane stosowanie polityki, procedur i praktyk zarządczych w ramach analizy ryzyka, oceny i nadzoru (DzU nr 108/4, art. 3.6).

magającym wyznaczanie tych obszarów działalności organizacji, które w pierwszej kolejności powinny być poddane sprawdzeniu i analizie.

Analiza ryzyka i zarządzanie prowadzone systematycznie i w sposób ciągły przyczyniają się do poprawy efektywności oraz uzyskania spójnych, porównywalnych i wiarygodnych rezultatów. Należy sobie uświadomić, że akcyjne podejście do zarządzania ryzykiem może prowadzić do zmaterializowania się poważnych niewykrytych ryzyk. Niestety jest to zagadnienie trudne i wymagające starannego przygotowania i określenia zbioru możliwych czynników ryzyka, budowania świadomości i odpowiedniego merytorycznego przygotowania osób dokonujących analizy ryzyka w procesie zarządzania bezpieczeństwem i jakością organizacji. Konieczne jest stosowanie podejścia obejmującego kompleksowe zarządzanie ryzykiem w organizacji, a nie ocena ryzyka tylko dla poszczególnych obszarów. W tym miejscu warto przeanalizować podstawowe zasady zarządzania ryzykiem w kontekście, jakie ich zastosowanie przynosi korzyści organizacji:

Analiza ryzykiem jest składową procesu podejmowania decyzji, ułatwiającą kierującym podejmowanie świadomych i właściwych wyborów, ustalenia priorytetów działań oraz rozpoznawania alternatywnych kierunków działań w przypadku zaistniałych zagrożeń, zdarzeń i sytuacji kryzysowych. Prawidłowo prowadzona analiza ryzyka bazuje na najlepszych praktykach oraz dostępnych źródłach informacji, takich jak dane historyczne, doświadczenia, informacje zwrotne od wszystkich interesariuszy, obserwacje, prognozy i opinie ekspertów z uwzględnieniem ich różnorodności i ograniczeń, czyli równocześnie przyczynia się do gromadzenia informacji z wielu źródeł z uwzględnieniem i wyraźnym określeniem stopnia tej niepewności.

Analiza ryzyka i zarządzanie nim powinny być dostosowane do zewnętrznych i wewnętrznych uwarunkowań organizacji i profili ryzyk, jakie występują w danej organizacji, bo tylko wtedy przynosi oczekiwane wyniki. Automatyczne przenoszenie metodyk i wyników do innych obszarów skutkuje pomyłkami w konsekwencji prowadzącymi do sytuacji kryzysowych o niewyobrażalnych skutkach.

Analizując ryzyko, musimy brać także pod uwagę czynniki ludzkie i kulturowe, rozpoznając tym samym możliwości, percepcję i intencje osób zarówno wewnątrz, jak i na zewnątrz organizacji, które mogą ułatwić bądź utrudnić osiągnięcie celów organizacji. W ten sposób zmniejszymy ryzyko i niepewność w podejmowaniu decyzji i wyborze możliwości przeciwdziałania.

Przejrzysta oraz kompleksowa analiza ryzyka daje nam gwarancję, dzięki odpowiedniemu określonemu czasowo zaangażowaniu kierujących na wszystkich poziomach zarządzania w organizacji, efektywnego i wczesnego określenia możliwych sytuacji kryzysowych a w efekcie spowoduje minimalizację oczekiwanych w wyniku zdarzenia strat.

Analiza ryzyka powinna być dynamiczna, powtarzalna oraz reagować na zmiany, ponieważ wewnętrzne i zewnętrzne ryzyka zmieniają się, pojawiają się

nowe ryzyka, a niektóre zanikają. Właściwe ich monitorowanie i przegląd zapewnia organizacji stałą aktualną wiedzę co do niepewności i ryzyka działań oraz możliwość podjęcia skutecznych przeciwdziałań.

Dzięki analizie i zarządzaniu ryzykiem można doskonalić zintegrowany system zarządzania bezpieczeństwem i jakością, wskazać kierunki koniecznych zmian w otoczeniu, priorytety podejmowania działań oraz możliwe straty, gdyby te zdarzenia wystąpiły. Analiza umożliwia także podejmowanie działań zapobiegawczych, prowadzących do minimalizacji poniesionych strat.

Analiza i szacowanie ryzyka jest pierwszym elementem w procesie zarządzania ryzykiem. Wyniki tego procesu są pomocne w wyborze odpowiednich systemów lub sposobów zabezpieczeń, pomagają zminimalizować lub wyeliminować zidentyfikowane czynniki ryzyka.

Polityka zarządzania ryzykiem zależy w dużej mierze od charakteru działalności, od jej podejścia i skłonności do podejmowania ryzyka, zwanej również „apetytem" na ryzyko, oraz od uwarunkowań otoczenia. W celu wspomożenia procesu wprowadzania i utrzymania efektywnego zarządzania ryzykiem niezbędne jest ustalenie „wspólnego zrozumienia" dotyczącego ryzyk w skali całej jednostki organizacyjnej i jej otoczenia. Bez ustalenia wspólnej płaszczyzny dyskusji na temat ryzyk towarzyszących działalności organizacji nie jest możliwe zarówno zapewnienie efektywnej komunikacji, jak i wprowadzenie efektywnego procesu zarządzania ryzykiem w skali całej jednostki organizacyjnej, nie można bowiem zarządzać czymś, co nie jest jednoznacznie zdefiniowane i zidentyfikowane oraz w ten sam sposób rozumiane przez pracowników organizacji. Różnie bowiem postrzegane jest ryzyko przez pracowników funkcjonujących na różnych szczeblach struktury organizacyjnej (wyższe kierownictwo, średnie kierownictwo, szeregowi pracownicy), odpowiedzialnych za poszczególne procesy biznesowe (procesy główne, pomocnicze) lub zlokalizowanych w różnych jednostkach organizacyjnych (centrala, oddziały) tej samej organizacji. Praktycznym rozwiązaniem wdrożenia „wspólnego zrozumienia" dotyczącego ryzyk w skali całej organizacji jest wykorzystanie standardowego modelu wyceny i oceny ryzyka.

Literatura

1. Białas A. (2007), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT.
2. Jajuga K. (2009), *Zarządzanie ryzykiem*, PWN, Warszawa.
3. Matkowski P. (2006), *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer Polska.
4. Monkiewicz J., Gąsiorkiewicz L. (2010), *Zarządzanie ryzykiem działalności organizacji*, Uczelnie Techniczne.
5. Patrick O. (2009), *ISO 31000:2009 Risk management – Principles and guidelines*, 06.

6. PKN-ISO GUIDE 73, Zarządzanie ryzykiem – Terminologia.
7. PN ISO/IEC 27005, Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.
8. PN-ISO 31000, Zarządzanie ryzykiem – Zasady i wytyczne.
9. Sienkiewicz P. (2007), *Badania naukowe bezpieczeństwa systemów*, w: *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżyniera działań w obszarach nauki, dydaktyki i praktyki*, red. B. Kosowski, A. Włodarski, Wyd. Fundacja Edukacja i Technika Ratownictwa. Warszawa.
10. Stanik J., Kiedrowicz M., *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 2015*, red. B.F. Kubiak, J. Maślankowski, Chapter 18, s. 231–251.
11. http://software.softblue.pl/content/system-zarzadzania-ryzykiem-1.
12. www.coso.org [dostęp 10.06.2010].
13. www.coso.org/documents/COSO_ERM_ExecutiveSummary_Polish.pdf [dostęp 05.2010].
14. www.ferma.eu/AboutFERMA/ARiskManagementStandard/tabid/195/Default.aspx.
15. www.4pm.pl/upload/artykuly/InLab.pdf.
16. www.ryzyko.biz/standardy_zarzadzania_ryzykiem.pdf.

THE RISK ANALYSIS AND THE RISK MANAGEMENT AS BASIC COMPONENTS OF THE SAFETY MANAGEMENT SYSTEM OF THE ORGANIZATION

Summary

In the article authors are taking issues of the risk analysis and of risk management in the generally understood organization and of the influence on her safety. They are emphasizing the weight and the significance of conducting constant analysis of essential risk factors, their identification and the manner with them. The article contains also an inspection of the process of the risk management with so-called taking into account "best practices" being applicable to it. The summary is showing positive consequences of leading the process of the risk management by organizations, as well as the problems associated with his practical accomplishment.

Keywords: risk analysis, risk management, models of the risk management, risk management in the safety of the organization.

Translated by Jerzy Stanik