Michał Wiśniewski[*]

Teresa Ostrowska[**]

8. WYZWANIA I DOBRE PRAKTYKI ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Streszczenie

Opracowanie prezentuje syntezę wiedzy na temat procesu zarządzania bezpieczeństwem infrastruktury krytycznej w świetle teorii zarządzania ryzykiem, przepisów ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. oraz powiązanych aktów prawnych. W tekście zwrócono uwagę na niedoskonałość obecnie przyjętych procedur, konieczność ich ciągłego doskonalenia oraz dostosowywania do panujących warunków politycznych, prawnych, społecznych i gospodarczych. Wynikiem rozdziału jest wykaz wyzwań stojących przed polskim systemem zarządzania bezpieczeństwem infrastruktury krytycznej oraz, opracowany na podstawie analizy zagranicznych metodyk zarządzania kryzysowego, wykaz dobrych praktyk z tego zakresu. Całość została uzupełniona o analizę istniejących ujęć teoretycznych, analitycznych i projektowych możliwych do wykorzystania w procesie zarządzania bezpieczeństwem infrastruktury krytycznej.

Słowa kluczowe

infrastruktura krytyczna, zarządzanie kryzysowe, zdarzenie niekorzystne, scenariusz zdarzeń, efekt domina

Wstęp

Infrastruktura krytyczna (IK) to, według ustawy o **zarządzaniu kryzysowym** (dalej u.z.k.), systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi **kluczowe dla bezpieczeństwa państwa i jego obywateli** oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców (u.z.k.). Z definicji wynika, że IK stanowi fundament sprawnego państwa i funkcjonującego na jego terenie społeczeństwa, w zakresie stabilności rozwoju gospodarczego, bezpieczeństwa narodowego, funkcjonowania administracji oraz podnoszenia standardu życia ludności. Zapewnienie bezpieczeństwa IK, rozumianego niekoniecznie jako fizyczna ochrona obiektu lecz jako ciągły dostęp do usług świadczonych przez systemy IK jest obowiązkiem państwa.

Osiągnięcie tego celu zależy od właściwego rozpoznania zagrożeń, analizy ryzyka, które wyrażają, działań prewencyjnych wobec zagrożeń oraz naprawczych wobec incydentów, kryzysów i katastrof. Narzędziem realizacji tego celu w państwach rozwiniętych są systemy i wspomagające je metodyki zarządzania bezpieczeństwem IK (ZB-IK).

[*] Mgr inż., Wydział Zarządzania, Politechnika Warszawska, Narbutta 85, 02-524 Warszawa, M.Wisniewski@wz.pw.edu.pl.

[**] Dr inż., Wydział Zarządzania, Politechnika Warszawska, Narbutta 85, 02-524 Warszawa, T.Ostrowska@wz.pw.edu.pl.

Celem niniejszego rozdziału jest analiza i wskazanie niesprawności polskiego systemu ZB-IK, dobrych praktyk z tego obszaru oraz propozycja możliwych rozwiązań podnoszących jego efektywność.

W rozdziale przeprowadzono analizę obowiązujących aktów prawnych, warunkujących funkcjonowanie systemu ZB-IK w Polsce, przegląd zagranicznych metodyk, odnoszących się do procesu ZB-IK oraz wskazano możliwe do zastosowania koncepcje teoretyczne z obszaru nauk o zarządzaniu.

Opracowanie jest wynikiem prac przeprowadzonych w ramach uczestnictwa w projekcie rozwojowym NCBiR pt. *Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz jednostkach organizacyjnych KSRG* umowa nr DOB – BIO7/11/02/2015 na wykonanie projektów w zakresie badań naukowych i projektów rozwojowych na rzecz obronności i bezpieczeństwa państwa, przez konsorcjum: Politechnika Warszawska (Wydział Zarządzania), Medcore sp. z o.o.

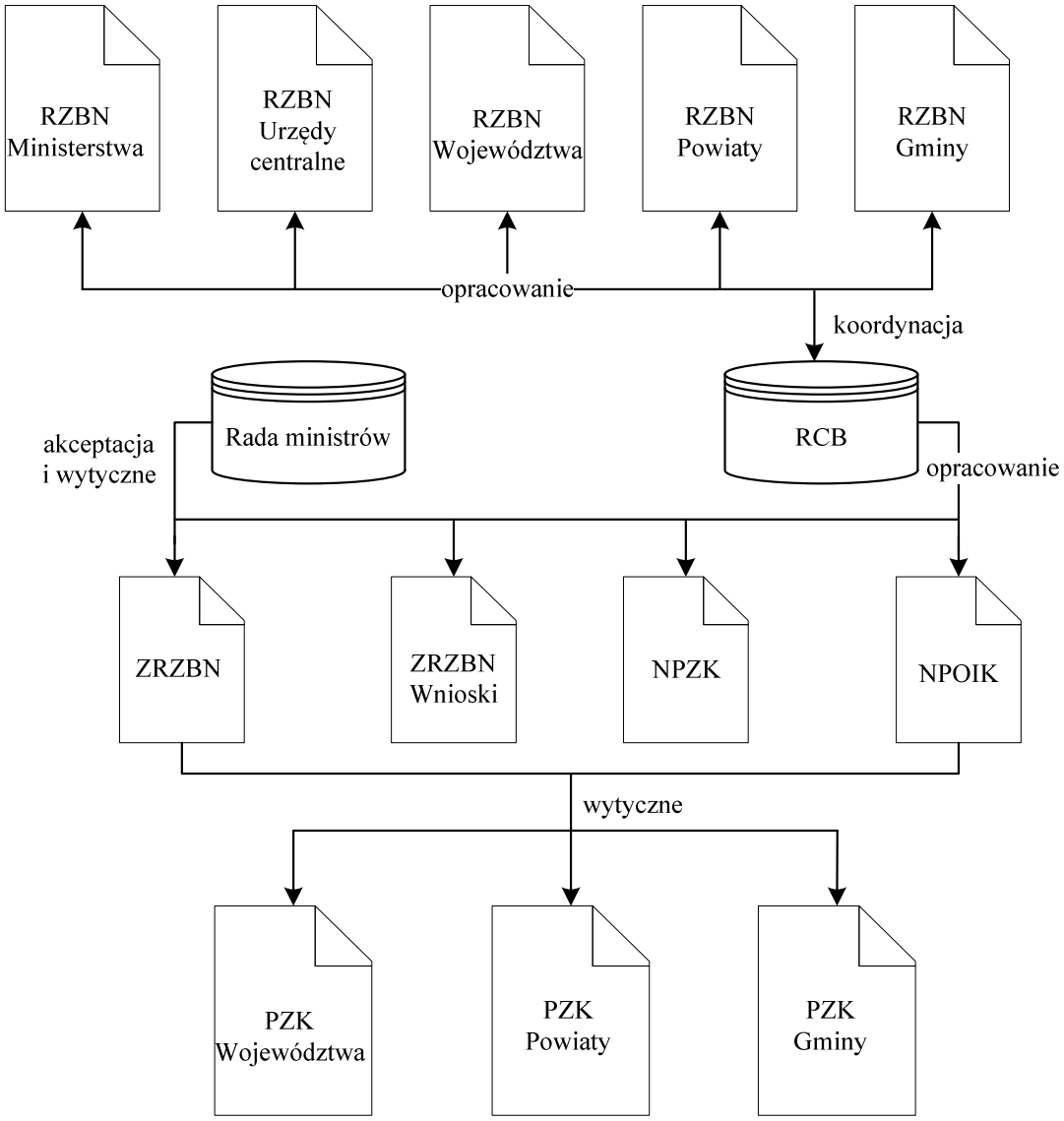
1. Polski system zarządzania bezpieczeństwem IK

Podstawą prawną polskiego systemu ZB-IK jest ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. oraz opublikowany w 2013 roku Narodowy Program Ochrony IK (NPOIK). Ustawa dzieli IK na jedenaście systemów (u.z.k., art. 3, pkt 2), z kolej Unijny Mechanizm Ochrony Ludności, wyróżnia dodatkowo system ochrony dziedzictwa narodowego. Fakt ten wskazuje na konieczność budowania otwartych systemów i metodyk ZB-IK.

Obecny model ZB-IK opiera się na przygotowywanych raz na dwa lata, raportach zagrożeń bezpieczeństwa narodowego (RZBN). Obowiązek sporządzenia raportów mają ministerstwa, urzędy centralne oraz wojewodowie. W procesie tym opcjonalnie mogą uczestniczyć powiaty oraz gminy. Fakt ten utrudnia zbieranie wiarygodnych danych na temat zagrożeń występujących na poszczególnych poziomach administracyjnych oraz ich agregację na poziomy wyższe.

Koordynatorem procesu opracowywania RZBN jest Rządowe Centrum Bezpieczeństwa, które na podstawie zabranych RZBN sporządza Krajowy Plan Zarządzania Kryzysowego (KPZK). Dokument ten jest następnie przedstawiany Radzie ministrów, która przyjmuje go w postaci uchwały. Wnioski z RZBN oraz KPZK stanowią podstawę do opracowania planów zarządzania kryzysowego (PZK) na poziomach województw, powiatów i gmin. W ramach obowiązującej procedury ZB-IK powstaje również NPOIK określający zadania i obowiązki dotyczące ochrony IK (Krupa i Wiśniewski 2015, s. 94). Na rysunku 3 przedstawiono schemat funkcjonowania polskiego systemu ZB-IK.

Ustawa o zarządzaniu kryzysowym jest pierwszym w Polsce aktem prawnym, w którym zdefiniowano pojęcie IK oraz sformułowano cele i zadania związane z jej ochroną. Nie oznacza to jednak, że przed rokiem 2007 nie było w Polsce przepisów definiujących proces ochrony obiektów o szczególnym znaczeniu dla bezpieczeństwa państwa i funkcjonowania społeczeństwa. Wykaz wybranych aktów prawnych związanych z ochroną IK został m.in. wskazany przez K. Steca (Stec 2011, s. 197).



Rysunek 3. Schemat polskiego systemu zarządzania bezpieczeństwem IK
Źródło: (Krupa i Wiśniewski 2015a, s. 95).

Wadą obowiązującego systemu ZB-IK jest fakt, że powstające w jego ramach dokumenty określają zadania, terminy oraz jednostki odpowiedzialne za ich wykonanie, natomiast nie ma wskazanych metod jakimi uczestnicy tego procesu mają się posługiwać. Prowadzi to do rozbieżności metodycznych i jakościowych opracowanych dokumentów, co utrudnia realizację procesu analizy i oceny ryzyka na poszczególnych poziomach administracyjnych. W konsekwencji obniża to poziom powstających PZK.

W związku z dużą dowolnością stosowanych metod efektywność systemu i podejmowanych działań w dużej mierze uzależniona jest od wiedzy i doświadczeń osób wykonujących analizy zagrożeń na jakie podatne są obiekty IK.

Przykładem uzależnienia efektywności wykorzystania elementów systemu IK może być karambol jaki miał miejsce w Krakowie w 2015 r. Ciężarówka typu TIR staranowała dziewiętnaście pojazdów osobowych. W wyniku zdarzenia piętnaście osób zostało poszkodowanych, z czego dziesięć osób wymagało hospitalizacji. Na miejsce zdarzenia dyspozytor pogotowia ratunkowego, w oparciu o uzyskane dane

i własne doświadczenia, zadysponował naziemne zespoły ratownicze i śmigłowiec lotniczego pogotowia ratunkowego. W wyniku późniejszych wypowiedzi lekarzy zajmujących się poszkodowanymi okazało się, że decyzja o niezwłocznym zadysponowaniu śmigłowca pozwoliła na unikniecie ofiar śmiertelnych (tvn24.pl).

W omawianym przypadku decyzja o wysłaniu jednostki lotniczego pogotowia ratunkowego na miejsce zdarzenia okazała się trafna. Jednak podstawą tej decyzji były doświadczenia dyspozytora, które w przypadku pomyłki niepotrzebnie osłabiłyby system ratownictwa zaliczany do systemów IK. W związku z powyższym powinno się dążyć do stanu, w którym efektywność procesu ZB-IK będzie wynikała z przyjętego modelu postępowania i tylko w ograniczony sposób będzie zależna od czynnika ludzkiego.

Na proces ZB-IK wpływa również proces planowania cywilnego. Jednym z najistotniejszych warunków planowania cywilnego jest przestrzeganie wymogu angażowania stosownych zasobów i kompetencji do określonej sytuacji. Gwarantuje to reagowanie na najniższym koniecznym poziomie oraz zapewnia włączenie do systemu wszystkich poziomów władzy, instytucji, organizacji i podmiotów gospodarczych oraz mieszkańców. W tym ujęciu mamy do czynienia z gotowością w zakresie sprostania warunkom zagrożeń, tj. podjęcia w określonym czasie, miejscu i zakresie zorganizowanego, adekwatnego do sytuacji i efektywnego działania zgodnie z przygotowanymi planami lub improwizacji stosownie do zadań wynikających z rzeczywistego zagrożenia. Ma to na celu zapewnienie akceptowanego poziomu bezpieczeństwa przez przygotowanie i utrzymanie adekwatnych do zagrożeń zdolności reagowania.

Odpowiednia reakcja na zaistniały incydent czy sytuację kryzysową wymaga oszacowania wartości ryzyka oraz posiadania wiedzy na temat skuteczności i efektywności działań podejmowanych w celu eliminacji zdarzenia niekorzystnego lub zażegnania kryzysu. Wiąże się to z zagadnieniem gromadzenia i porządkowania wiedzy na temat zdarzeń przeszłych oraz jej przetwarzania w celu doskonalenia umiejętności reagowania w przyszłości. Gromadzona wiedza powinna m.in. uwzględniać zależności i współzależności zagrożeń w ocenie ryzyka wystąpienia zdarzenia niekorzystnego, które mogą wywołać tzw. efekt domina. W literaturze związanej z zagadnieniem zarządzania bezpieczeństwem czy zarządzania ryzykiem można znaleźć wiele przykładów metod identyfikacji zagrożeń, jednak w ramach tych metod pomija się kwestię powiązań między zagrożeniami. W opracowaniach kładzie się nacisk na konieczność identyfikacji i oceny zagrożeń elementarnych. Tymczasem takie zagrożenia najczęściej są przyczyną serii zagrożeń, które należy uwzględnić w ocenie ryzyka.

Wskazanie listy zagrożeń wraz z rozpoznaniem wzajemnych powiązań między zagrożeniami jest podstawą opracowania prognozy rozprzestrzeniania się zdarzeń niepożądanych, która pozwala odpowiednio dobrać siły i środki do zaistniałej sytuacji, realizując tym samym założenia procesu planowania cywilnego.

Najczęściej stosowaną metodą określania wzajemnych powiązań zagrożeń oraz prognozowania rozprzestrzeniania się zagrożeń jest metoda scenariuszowa. Na potrzebę budowania takich prognoz wskazuje m.in. NPOIK (2013 s. 27). Metoda ta jest również stosowana w zagranicznych metodykach ZB-IK Holandii, Szwecja, Irlandii, Niemiec, Kanady i Wielkiej Brytanii.

Budowa scenariuszy zdarzeń niekorzystnych odbywa się zazwyczaj w oparciu o miękkie metody tj. burze mózgów, spotkania seminaryjne, metody eksperckie. Choć uzyskane w ten sposób opracowania są bardzo cenne i niewątpliwie podnoszą

bezpieczeństwo systemów IK, to ich wadą jest brak zapewnienia, że wskazane zostały wszystkie możliwe scenariusze zdarzeń niekorzystnych, jakie w danym systemie i przy danych zasobach wiedzy są możliwe do realizacji. Istnieje tu możliwość pominięcia w analizach części zagrożeń oraz niedocenienie pewnych ryzyk.

Przykładem może być katastrofa elektrowni jądrowej Fukushima I. Obiekt należący do systemu IK Japonii został zabezpieczony przed występującymi na terenie kraju trzęsieniami ziemi. W wyniku wystąpienia takiego zagrożenia żaden element elektrowni nie uległ poważnym uszkodzeniom. Jednak fale tsunami wywołane przez trzęsienie ziemi zdołały doprowadzić do katastrofy (wyborcza.pl).

Innym przykładem niedocenienia zagrożenia dla IK była sytuacja z lata 2015 r., kiedy to w Polsce ze względu na wysokie temperatury i braki wody potrzebnej do chłodzenia bloków energetycznych konieczne było czasowe wstrzymanie prac w dużych zakładach produkcyjnych (hkatowice.tvp.pl).

Przedstawione rozważania dotyczące polskiego systemu ZB-IK wskazują na jego niesprawność przede wszystkim w obszarze braku ogólnie przyjętych metod realizacji wytycznych zawartych w ustawie o zarządzaniu kryzysowym i NPOIK. Niesprawnością jest również zbyt duże uzależnienie systemu od doświadczeń i wiedzy osób prowadzących analizy ryzyk związanych z systemami IK. Słabością systemu jest także koncentracja na pojedynczych zagrożeniach i nieuwzględnianie tzw. efektu domina. W tym obszarze należy jednak zauważyć podejmowane działania w celu zmiany podejścia do procesu analizy i oceny ryzyka w kierunku uwzględniania scenariuszy zdarzeń niekorzystnych zawierające się w zapisach NPOIK.

Eliminacja wymienionych niesprawności w opinii autorów jest podstawowym wyzwaniem stojącym przed praktykami i badaczami procesu ZB-IK.

2. Zagraniczne metodyki zarządzania bezpieczeństwem IK

Jednym z możliwych sposobów eliminacji niesprawności polskiego systemu ZB-IK jest benchmarking najlepszych praktyk polegający na analizie rozwiązań stosowanych za granicą. Proces ZB-IK realizowany jest w wielu krajach Europy i świata. Kraje takie jak Szwecja, Niemcy, Irlandia, Holandia czy Wielka Brytania wykazują się dużym doświadczeniem i dojrzałością rozwiązań w tym zakresie. W związku z tym, że metodyki ww. krajów zostały już szeroko omówione m.in. w takich monografiach, jak Wróblewski (2015), Abgarowicz (2015) czy Kosieradzka i Zawiła-Niedźwiecki (2016), w niniejszym opracowaniu wskazano hasłowo elementy uznawane przez autorów za dobre praktyki warte uwzględnienia w ramach reorganizacji polskiego systemu ZB-IK.

Analizując metodyki wymienionych krajów skupiono się przede wszystkim na organizacji procesu oceny ryzyka, budowy PZK a także na metodach, technikach oraz narzędziach wykorzystywanych w procesie ZB-IK. Wyniki analiz zaprezentowano w tabeli 9.

Implementacja wymienionych w tabeli 9 dobrych praktyk w polskim systemie ZB-IK wymaga jego reorganizacji. Konieczna jest przede wszystkim zmiana optyki nastawionej na rozpoznawanie zagrożeń elementarnych i skupienie się na zagrożeniach złożonych.

Tabela 9. Wykaz dobrych praktyk stosowanych w zagranicznych metodykach ZB-IK

Lp.	Wyszczególnienie	Źródło
1	określenie wpływu na społeczeństwo i badaną organizację	metodyka: Szwecji, Wielkiej Brytanii
2	odniesienie analizy ryzyka do precyzyjnie zdefiniowanego obszaru (obiektu, miejsca)	metodyka: Niemiec, Irlandii, Szwecji, Kanady
3	agregacja wyników analizy ryzyka oparta o arytmetykę (w tym ocena ważona)	metodyka: Niemiec, Holandii, Kanady
4	wizualizacja wyników analizy ryzyka w postaci rozbudowanej matrycy ryzyka uwzględniającej obszary: zapobiegania i redukcji ryzyka, zwiększenia sił reagowania	metodyka: Irlandii, Holandii
5	analizy średnio- i długoterminowe (5-25 lat)	metodyka: Kanady, Wielkiej Brytanii, Holandii
6	budowa i podział opracowanych scenariuszy zagrożeń na grupę scenariuszy realnych (do materializacji tu i teraz) i rozwojowych (możliwych do zrealizowania w przyszłości)	metodyka: Holandii
7	analizy wielokryterialne	metodyka: Holandii, Szwecji, Niemiec, Kanady
8	grupowanie zagrożeń	metodyka: Wielkiej Brytanii, Irlandii
9	podział skutków zagrożeń na kilka kategorii, w tym: ofiary śmiertelne, zranieni i z urazami, zakłócenia społeczne, straty ekonomiczne, brak dostępu do opieki zdrowotnej, brak dostępu do edukacji, przerwy w świadczeniu podstawowych usług (woda, prąd, ścieki), konieczność ewakuacji, wpływ psychologiczny, bezpieczeństwo terytorialne, bezpieczeństwo fizyczne, stabilność polityczna, rządy prawa, niepodległość i suwerenność państwa	metodyka: Wielkiej Brytanii, Holandii, Szwecji, Niemiec, Irlandii, Kanady
10	wykorzystanie modeli numerycznych	metodyka: Wielkiej Brytanii, Kanady
11	wykaz modeli zabezpieczeń, które powinny zostać wzmocnione	metodyka: Holandii
12	wykaz środków kontroli	metodyka: Holandii
13	wykaz zagrożeń inicjujących i wtórnych	metodyka: Holandii, Kanady, Niemiec
14	wykaz ról dla wszystkich uczestników zdarzenia niekorzystnego	metodyka: Holandii
15	wykaz funkcji analizowanego systemu i powiązanie z nim zagrożeń	metodyka: Szwecji
16	podział zagrożeń na wewnętrzne i zewnętrzne	metodyka: Szwecji
17	określenie czasu trwania zdarzenia niekorzystnego	metodyka: Niemiec, Irlandii
18	uwzględnienie trendów zagrożeń (osłabianie, nasilanie, stabilizacja)	metodyka: Irlandii
19	wykaz jednostek mogących dostarczyć wiedzę na temat analizowanych obiektów, systemów	metodyka: Irlandii
20	wprowadzenie podziału na zagrożenia stałe (mogące wystąpić zawsze dla każdego obiektu) i specyficzne	metodyka: Irlandii
21	określenie źródeł informacji, na których oparto analizę	metodyka: Irlandii, Kanady
22	przedziałowa ocena prawdopodobieństwa i skutków	metodyka: Holandii

Źródło: opracowanie własne.

Jednym z możliwych rozwiązań tego problemu jest oparcie procesu analizy i oceny ryzyka o scenariusze zdarzeń niekorzystnych. Takie rozwiązanie jest stosowane we wszystkich przeanalizowanych zagranicznych metodykach ZB-IK. Ponadto umożliwi to wprowadzenie standaryzacji działań, zaproponowanie metod pracy zespołów analityczno-projektowych odpowiedzialnych za bezpieczeństwo IK oraz ograniczenie uzależnienia efektywności procesu ZB-IK od czynnika ludzkiego.

3. Analiza wymogów prawnych

Reorganizacja Polskiego systemu ZB-IK i próba zastosowania w nim podejścia scenariuszowego wymaga przeprowadzenia analizy obowiązujących aktów prawnych. Analiza ma dać odpowiedź na pytania:

1. Jaki jest stan obwiązujących przepisów prawnych z zakresu ZB-IK?
2. Czy obowiązujące przepisy pozwalają na zastosowanie podejścia scenariuszowego?
3. Jakie elementy powinien zawierać scenariusz zdarzenia niekorzystnego?

Stan prawny dotyczący prezentowanej problematyki jest bardzo rozproszony, zróżnicowany i pochodzi z różnych okresów. Wynika to między innymi z faktu, że problematyka ZB-IK leży w gestii różnych centralnych organów administracji oraz innych władz publicznych.

Obowiązujące przepisy pochodzą z aktów wykonawczych – rozporządzeń stanowionych przez różne organy wykonawcze. Powoduje to, że są one nieskoordynowane, a często wręcz sprzeczne, utrudniając w ten sposób działania różnych służb w przypadku wystąpienia sytuacji zagrażającej bezpieczeństwu IK.

Ponadto regulacje prawne dotyczące procesu ZB-IK w Polsce są obarczone tymi samymi błędami, które formułuje się w odniesieniu do całości polskiego ustawodawstwa, tzn. że są nadmiernie obszerne, niestabilne (często nowelizowane) i przesadnie szczegółowe.

Poważny problem stanowi również podejście do problematyki publicznego zarządzania kryzysowego związanego z procesem ZB-IK. Podejście to będące efektem innego spojrzenia na zagadnienie społeczeństwa obywatelskiego wywodzącego się zarówno z ustawodawstwa UE, jak i z przemian ustrojowych w Polsce jest rozbieżne z obowiązującą koncepcją obrony cywilnej wywodzącą się z ustawy z 21 listopada 1967 roku o powszechnym obowiązku obrony RP. W wyniku przemian ustrojowych oraz polskiego członkostwa w UE definicja publicznego zarządzania kryzysowego uległa przemianom zarówno w ustawie o zarządzaniu kryzysowym jak i ustawie o państwowym ratownictwie medycznym oraz ustawie o ochronie przeciwpożarowej.

Prezentowana ocena skłania do przyjęcia stanowiska o konieczności całościowej analizy problematyki obowiązującego ustawodawstwa z uwzględnieniem celów społecznych głównie w aspekcie ZB-IK.

Obowiązujące przepisy formalno-prawne nie wykluczają jednak możliwości modyfikacji systemu ZB-IK i wprowadzenia analiz i oceny ryzyka w oparciu o scenariusze zdarzeń niekorzystnych. Szczególnie istotne dla procesu budowy tych scenariuszy są poniższe akty prawne:

- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,
- Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym,
- Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej,
- Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej,
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego,
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 września 2002 r. w sprawie odbywania służby w obronie cywilnej.

Wymienione dokumenty pośrednio wskazują jakie zestawy danych powinny być uwzględniane przez scenariusz zdarzeń niekorzystnych. Wykaz tych elementów został zawarty w tabeli 10.

Tabela 10. Wykaz elementów scenariusza zdarzeń niekorzystnych wymaganych obowiązującymi przepisami

Lp.	Nazwa elementu obligatoryjnego	Źródło
1	wykaz obiektów, urządzeń, instalacji oraz usług kluczowych dla bezpieczeństwa państwa	art. 3, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
2	zestawienie potencjalnych zagrożeń wraz z ich charakterystyką	art. 3, pkt 8, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. art. 17, pkt 4, Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej art. 1, pkt 1, Ustawa o ochronie przeciwpożarowej z dnia 12 sierpnia 1991 r. § 20, pkt 2, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG § 20, pkt 1, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 września 2002 w sprawie odbywania służby w obronie cywilnej
3	ocena ryzyka wystąpienia zagrożeń	art. 11, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
4	skutki wystąpienia zagrożenia	art. 3, pkt 10, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
5	skala zagrożeń	§ 20, pkt 2, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
6	miejsce występowania zagrożenia	§ 20, pkt 2, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
7	rodzaj zagrożenia	§ 20, pkt 2, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
8	sposoby przeciwdziałania zagrożeniu	§ 20, pkt 2, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
9	stan infrastruktury	§ 20, pkt 9, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
10	warunki terenowe	§ 20, pkt 9, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
11	warunki atmosferyczne	§ 20, pkt 9, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
12	szacunkowy stopień zagrożenia	załącznik 1, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
13	obszar geograficzny objęty zasięgiem zagrożenia	art. 3, pkt 10, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. załącznik 1, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
14	wykaz wariantów zasięgu zagrożeń	art. 3, pkt 9, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
15	wykaz sił i środków potrzebnych do zażegnania zdarzenia niekorzystnego lub	art. 5, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.

Lp.	Nazwa elementu obligatoryjnego	Źródło
	sytuacji kryzysowej	art. 1, pkt 2, Ustawa o ochronie przeciwpożarowej z dnia 12 sierpnia 1991 r. § 20, pkt 3-4, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji KSRG
16	wykaz podmiotów odpowiedzialnych za usuwanie zagrożeń	art. 4, pkt 3, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
17	wykaz podmiotów wykonujących działalność leczniczą w przypadku wystąpienia zdarzenia niekorzystnego lub sytuacji kryzysowej	art. 30, pkt 1, Ustawa o Państwowym Ratownictwie Medycznym z dnia 8 września 2006 r.
18	wykaz struktur uruchamianych w sytuacjach kryzysowych	art. 4, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
19	wykaz szkoleń przygotowujących członków oddziałów obrony cywilnej do reakcji na zdarzenie niekorzystne lub sytuację kryzysową	§ 20, pkt 1, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 września 2002 w sprawie odbywania służby w obronie cywilnej
20	wykaz zadań i obowiązków uczestników zarządzania kryzysowego	art. 5, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
21	wykaz zawartych umów porozumień związanych z realizacją zadań zawartych w planie zarządzania kryzysowego	art. 5, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
22	wykaz zadań dotyczących monitorowania zagrożeń	art. 5, pkt 2, Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.
23	wykaz zabezpieczeń przed zagrożeniami	art. 17, pkt 4, Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej
24	wykaz świadczeń osobistych	dział VII, rozdział 1, Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej
25	wykaz świadczeń rzeczowych	dział VII, rozdział 2, Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej

Źródło: opracowanie własne.

Należy zauważyć, że w polskim ustawodawstwie nie istnieją akty prawne bezpośrednio odnoszące się do zagadnienia budowy scenariuszy zdarzeń niekorzystnych czy sytuacji kryzysowych. Dlatego przedstawiony w tabeli 10 wykaz zestawów danych należy traktować jako punkt wyjściowy i otwartą listę, którą należy monitorować i uzupełniać o nowe elementy wymagane przepisami prawnymi.

4. Istniejące rozwiązania możliwe do wykorzystania w procesie zarządzania bezpieczeństwem IK

Wprowadzenie do procesu ZB-IK scenariuszy zdarzeń niekorzystnych wymaga wskazania podstaw teoretycznych, które umożliwią opracowanie nowej metodyki postępowania. Zaproponowane rekomendacje w tym obszarze powinny uwzględniać:

- koncepcje i podejścia do zarządzania,
- metody i techniki organizatorskie,
- narzędzia informatyczne.

Zarządzanie ryzykiem, a tym samym i bezpieczeństwem, utożsamiane jest z procesami diagnozy i sterowania, których celem jest intencjonalne zapewnienie stabilizacji oraz wykreowanie uwarunkowań dalszego rozwoju organizacji (Zawiła-Niedźwiecki 2013). Współczesne koncepcje zarządzania, wywodzące się głównie

z obszaru organizacji funkcjonowania przedsiębiorstw produkcyjnych, sprawdzają się w obszarach bankowości, ubezpieczeń, handlu itp. Wykorzystując analogię pomiędzy procesem zarządzania ryzykiem w przedsiębiorstwach a procesem ZB-IK można sądzić, że sprawdzą się one również i w tym obszarze. Koncepcjami, które wydają się szczególnie predysponowane do wsparcia omawianego procesu są podejście scenariuszowe i sytuacyjne oraz metody AIDA i *Case Based Reasoning* (CBR).

Podejście scenariuszowe w obszarze zarządzania finansami stanowi podstawę teoretyczną analizy, za pomocą której bada się równoczesny wpływ wielu czynników na wyniki wyceny lub oceny efektywności projektu inwestycyjnego (Pluta 2010, s. 36-38). W tym kontekście podejście scenariuszowe stanowi ciekawe narzędzie służące określaniu czynników ryzyka oraz ustalania obszarów niepewności związanych z funkcjonowaniem przedsiębiorstw. Scenariusze opisujące analizowany system powinny zawierać (Haijden i in. 2002):

- opis stanu rzeczywistości na koniec ustalonego okresu,
- interpretację bieżących zjawisk i ich konsekwencji w przyszłości,
- wewnętrznie spójny obraz przyszłej rzeczywistości.

W kontekście zarządzania ryzykiem podejście scenariuszowe wykorzystuje się jako sposób konwersji zdolności organizacji do uczenia się na konkretny plan działania zaprojektowany w celu reagowania na szok zewnętrzny oraz odzyskania równowagi po jego nastąpieniu (Worthington, Collins i Hitt 2009, s. 444). Przez szok zewnętrzny należy rozumieć wystąpienie zagrożenia, na które podatny jest analizowany system IK: atak terrorystyczny, klęska żywiołowa, absencja kluczowych pracowników itp.

Na podstawie scenariuszy opracowuje się plany reakcji na zdarzenie niekorzystne, plany ciągłości działania oraz plany przywrócenia pełnej sprawności IK. Opracowanie planów przekłada się na możliwość wypracowania swoistych instrukcji stanowiskowych na wypadek zaistnienia zdarzenia niekorzystnego. Dzięki temu szybciej uruchamiane są odpowiednie struktury mające reagować na wystąpienie zdarzenia niekorzystnego, a pracownicy nie ulegają szokowi i wiedzą jak się zachować.

Planowanie w oparciu o podejście scenariuszowe jest dobrym narzędziem do oceny ryzyka, określania obszarów niepewności w otoczeniu i ich wpływu na działalność przedsiębiorstwa, ale w swojej naturze jest narzędziem opisowym. Z tego powodu trudno je stosować do pomiaru ryzyka (Daszyńska-Żygadło 2012, s. 80) gdzie wskazane jest posługiwanie się wskaźnikami ilościowymi. Problem ten można wyeliminować uzupełniając podejście scenariuszowe elementami podejścia sytuacyjnego zarządzania przedsiębiorstwem.

Ujęcie sytuacyjne jest wynikiem prac praktyków i badaczy, którzy próbowali zastosować koncepcje głównych szkół nauk o zarządzaniu w warunkach występujących w organizacjach oraz określić przewidywane zależności między sytuacjami, działaniami i wynikami (Wajda 2003, s. 48). Podstawowym założeniem ujęcia sytuacyjnego jest stwierdzenie, że rzeczywistość jest zbyt złożona aby można było stosować uniwersalne sposoby działania, skuteczne w każdych warunkach. Pogląd ten potwierdza A. Hamrol dodając, że organizacje są systemami złożonymi, probabilistycznymi, spójnymi, o nieograniczonych zbiorach sprzężeń wewnętrznych i zewnętrznych. Nie ma zatem sytuacji identycznych i powtarzalnych, w których można wprost zastosować znane standardy rozwiązań. Dopiero analiza konkretnej sytuacji daje możliwość doboru adekwatnych modeli, metod czy rozwiązań oraz pozwala na

określenie ich jednorazowej skuteczności (Hamrol 1998, s. 68). Zamiast uniwersalnych metod zarządzania w nurcie sytuacyjnym przyjmuje się, że (Kaczmarek i Sikorski 1996, s. 24-25):

- zalecenia szkoły sytuacyjnej mają służyć jako sugestie sprawdzonych rozwiązań w różnych sytuacjach,
- każda organizacja jest jedyna w swoim rodzaju i wymaga, aby zachowania kierownicze warunkować zmiennymi właściwymi w konkretnej sytuacji,
- celowe jest opracowanie zbiorów modelowych rozwiązań dotyczących różnych poziomów i aspektów zarządzania w organizacji, stanowiących zbiór możliwości, z których należy wybrać najlepsze w danej sytuacji.

Opracowanie zbioru modelowych rozwiązań w przypadku procesu ZB-IK wymaga zastosowania mechanizmów gromadzenia wiedzy z zakresu (Krupa i Wiśniewski 2015b, s. 1028):

- obiektów podatnych na zagrożenia,
- funkcjonalności obiektów,
- zagrożeń,
- powiązań między zagrożeniami,
- skutków wystąpienia zdarzeń niekorzystnych,
- procedur i narzędzi wykorzystanych do zażegnania zdarzenia niekorzystnego i przywrócenia stanu z przed jego wystąpienia.

Szczególnie użyteczne podejście do zarządzania sytuacyjnego w kontekście procesu ZB-IK prezentuje Kłykow. Definiuje on sytuację jako (Kłykow i Jurek 1988, s. 71):

- zbiór węzłów związanych ze sobą skierowanymi połączeniami, które odwzorowują zależności między węzłami, tworząc strukturę sytuacji,
- węzły reprezentują elementy modelowanej rzeczywistości,
- węzły mogą reprezentować inne struktury sytuacji, co umożliwia budowę struktur hierarchicznych.

Założenia podejścia sytuacyjnego można wykorzystać do budowy struktury analizowanego systemu IK uwzględniającego obiekty i oddziałujące na nie zagrożenia. Określenie struktury systemu pozwala na wskazanie scenariuszy zdarzeń jakie mogą się w nim rozgrywać, co jest pierwszym krokiem w kierunku wskazania zestawu modeli zabezpieczeń przed rozpoznanymi zagrożeniami. Wskazanie właściwego modelu zabezpieczeń jest procesem decyzyjnym, który może być wspomagany metodami AIDA i CBR.

Wykorzystanie metody AIDA wiąże się z realizacją trzech kroków. Budowany jest model problemu decyzyjnego, w ramach którego (Krupa i Ostrowska 2012, s. 26):

- wydziela się obszary decyzyjne i decyzje elementarne,
- zaznacza pary decyzji elementarnych znajdujących się w relacji pełnej sprzeczności,
- wyznacza wagi względnej istotności Vi obszarów decyzyjnych Di na skali procentowej oraz wagi względnej istotności vji (względnych kosztów do sumy 1 w każdym obszarze decyzyjnym Di) elementarnych decyzji dji na skali (0..1).

Następnie generowany jest zbiór dopuszczalnych decyzji niezawierający par elementarnych decyzji znajdujących się w relacji pełnej sprzeczności. Ostatnim etapem jest przeprowadzenie względnej oceny kosztowej wszystkich poprawnie utworzonych decyzji (bez relacji sprzeczności) i uporządkowanie ich w malejącej kolejności względnych kosztów oraz analiza uzyskanych rozwiązań, wytypowanie grupy najbardziej pożądanych wariantów decyzji, dokonanie wyboru jednej z nich i wykonanie decyzji.

Metoda AIDA może zostać wykorzystana do opracowania modeli zabezpieczeń wykorzystywanych w ramach reakcji na rozpoznane scenariusze. Obszary decyzyjne mogą reprezentować rozpoznane zagrożenia, a decyzje elementarne – zabezpieczenia przed zagrożeniami. Technika ma jednak ograniczenia, z którymi należy się liczyć. Stosując ściśle założenia metody odrzuca się modele zabezpieczeń, w których występuje więcej niż jedno zabezpieczenie z danego obszaru decyzyjnego.

Metoda CBR opiera się na obserwacji rozumowania eksperta, który szukając rozwiązania problemu odwołuje się do doświadczeń z przeszłości i wzoruje swoje działania na wówczas podjętych. Metoda CBR określa przypadek jako parę: problem i jego rozwiązanie. Przypadki są niezależne, nie są regułami, są zapisami rzeczywistych zdarzeń inicjowanymi w konkretnych sytuacjach, które mogą zostać opisane odpowiednim zestawem danych. Istota CBR sprowadza się do stwierdzenia, że możliwe jest rozwiązanie bieżącego problemu przez adaptację rozwiązań zastosowanych w przeszłości (Riesbeck i Schank 1989). W metodzie CBR wyróżnia się następujące etapy realizowane w cyklu (Aamodt i Plaza 1994):

- wyszukanie – w bazie przypadków wyszukuje się przypadek najbardziej podobny do rozpatrywanego,
- wykorzystanie – sposób rozwiązania znalezionego przypadku staje się potencjalnym rozwiązaniem obecnego problemu,
- ocena przydatności – znane rozwiązanie dopasowuje się do rozpatrywanego problemu, możliwa jest modyfikacja rozwiązania,
- zapamiętanie – rozpatrywany problem oraz zastosowane rozwiązanie zapamiętuje się jako nowy przypadek.

Wskazanie kryteriów podobieństwa sytuacji w jakich znajduje się analizowany system da możliwość porównywania określonego scenariusza zdarzeń z przypadkami mającymi miejsce w przeszłości, dzięki czemu możliwe będzie określenie czy przyjęty model zabezpieczeń przyniesie pożądane rezultaty.

Proponowane podejście jest możliwe do realizacji bez wsparcia narzędzi informatycznych, jednak takie działanie wyraźnie wpłynie na efektywność metody. Dlatego rekomenduje się aby proces ZB-IK uwzględniający scenariusze zdarzeń niekorzystnych został wsparty odpowiednimi narzędziami informatycznymi tj.:

- bazy i hurtownie danych – umożliwiające gromadzenie danych i prowadzenie analiz wskazujących na korelację pozornie niezwiązanych zjawisk,
- narzędzia pracy grupowej – dające możliwość opracowywania, gromadzenia, wymiany i prezentacji dokumentów tworzonych przez zespół analityczno-projektowy,
- symulatory procesów biznesowych – pozwalające na budowę struktury systemu IK i automatyczne generowanie scenariuszy zdarzeń niekorzystnych.

Zakończenie

Zapewnienie bezpieczeństwa IK, rozumianego jako ciągły dostęp do usług świadczonych przez systemy IK, jest jednym z podstawowych obowiązków państwa. Osiągnięcie tego celu zależy od właściwego rozpoznania zagrożeń, na które podatne są systemy IK i właściwego doboru zabezpieczeń. Celem niniejszego rozdziału było wskazanie niedociągnięć polskiego systemu ZB-IK, identyfikacja dobrych praktyk z tego obszaru oraz zaproponowanie rozwiązań podnoszących jego efektywność.

W rozdziale przeprowadzono analizę obowiązujących aktów prawnych, warunkujących funkcjonowanie systemu ZB-IK w Polsce, przegląd zagranicznych metodyk, odnoszących się do procesu ZB-IK oraz możliwe do zastosowania koncepcje teoretyczne z obszaru nauk o zarządzaniu.

W obszarze wyzwań stojących przed praktykami i badaczami zajmującymi się zagadnieniami ZB-IK należy wskazać trzy główne problemy:

- brak ogólnie przyjętych metod realizacji wytycznych zawartych w ustawie o zarządzaniu kryzysowym i NPOIK,
- zbyt duże uzależnienie systemu od doświadczeń i wiedzy osób prowadzących analizy ryzyk związanych z systemami IK,
- koncentrację na pojedynczych zagrożeniach i nieuwzględnianie tzw. efektu domina.

Analiza metodyk ZB-IK wiodących w tym obszarze krajów pozwoliła na wskazanie zestawu dobrych praktyk możliwych do zastosowania w kontekście wyeliminowania niesprawności polskiego systemu ZB-IK. Ich wdrożenie wymaga reorganizacji polskiego systemu ZB-IK pod kątem uwzględniania scenariuszy zdarzeń niekorzystnych.

Analiza aktów prawnych dotyczących zarządzania kryzysowego, planowania cywilnego i planowania ratowniczego pozwoliła wskazać wykaz zestawów danych, które powinny być uwzględnione w ramach scenariusza zdarzeń niekorzystnych. Należy tu jednak zaznaczyć, że wskazania te pośrednio wynikają z obowiązujących aktów prawnych, gdyż w polskim prawodawstwie nie istnieje dokument określający strukturę scenariusza zdarzeń niekorzystnych.

Podstawy teoretyczne do opracowania metodyki ZB-IK dają podejście scenariuszowe i sytuacyjne oraz metody AIDA i CBR stosowane w naukach o zarządzaniu. Nowa metodyka postępowania powinna być również wspomagana przez odpowiedni zestaw narzędzi informatycznych w celu zwiększenia jej efektywności.

Propozycja metodyki ZB-IK uwzględniającej scenariusze zdarzeń niekorzystnych została przedstawiona w artykule (Krupa i Wiśniewski 2015, s. 93-104) i jest przedmiotem dalszych prac badawczych autorów.

Literatura

Opracowania zwarte

Aamodt A., Plaza E. (1994). *Case-Based Reasoning: Foundational Issues, Methodological Variation and System Approaches,* Artificial Intelligence Communications, 7(1).

Abgarowicz G. (red.) (2015). *Pamięć przyszłości. Analiza ryzyka dla zarządzania kryzysowego*, CNBOP – PIB, Józefów.

Daszyńska-Żygadło K. (2012). *Podejście scenariuszowe w zarządzaniu ryzykiem*, Annales Unicersitatis Mariae Curie-Skłodowska, vol. XLVI, 4.

Haijden K., Bradfield R., Burt G., Cairns G., Wright G. (2002). *The sixth sense: Acceleration organisational learning with scenarios*, Wiley, Chichester.

Hamrol A. (1998). *Zarządzanie jakością. Teoria i praktyka*, Państwowe Wydawnictwo Naukowe, Warszawa.

Kaczmarek B., Sikorski C. (1996). *Podstawy zarządzania – zachowania organizacyjne*.

Kłykow J., Jurek J. (1988). *Dialogowe semiotyczne systemy podejmowania decyzji*, PWN.

Kosieradzka A., Zawiła-Niedźwiecki J. (red.) (2016). *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*, edu-Libri, Kraków.

Krupa T., Ostrowska T. (2012). *Decision-making in flat and hieratchical decision problems*, Foundations of Manafgement, vol. 4, no. 2.

Krupa T., Wiśniewski M. (2015a). *Situational management of ctritical infrastructure resources under threat*, Foundations of Management, vol. 7, annula 15.

Krupa T., Wiśniewski M. (2015b). *Wykorzystanie wiedzy w zarządzaniu sytuacyjnym bezpieczeństwem infrastruktury krytycznej Polski*, Logistyka, nr 5.

Pluta W. (2010). *Planowanie finansowe w przedsiębiorstwie*, PWE.

Riesbeck C., Schank R. (1989). *Inside Case-Based Reasoning*, Lawrence Erlbaum.

Stec K. (2011). *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, Bezpieczeństwo narodowe, nr 19.

Wajda A. (2003). *Podstawy nauki o zarządzaniu organizacjami*, Warszawa.

Worthington W., Collins J., Hitt M. (2009). *Beyond risk mitigation: Enhancing corporate innovation with scenario planning*, Business Horizons, nr 52.

Wróblewski D. (red.) (2015). *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, CNBOP – BIP, Józefów.

Zawiła-Niedźwiecki J. (2003). *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, Wydawnictwo edu-Libri, Kraków.

Akty prawne

Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (tekst jedn. Dz.U. 2015 poz. 827 ze zm.).

Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (tekst jedn. Dz.U. 2009 nr 178 poz. 1380 ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. Dz.U. 2013 r. poz. 1166 ze zm.).

Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (tekst jedn. Dz.U. 2013 r. poz. 757 ze zm.).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego (Dz.U. 2011 nr 46 poz. 239).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 września 2002 r. w sprawie odbywania służby w obronie cywilnej (Dz.U. 2002 nr 169 poz. 1391).

A Framework for Major Emergrncy Management, A Guide to Risk Assessment In Major Emergency Management, Irlandia, 2010.

All Hazards Risk Assessment Methodology Guidelines, Kanada, 2013.

Guide to Risk and Vulenerability Analyses, Szwecja, 2012.

Method of Risk Analysis for Civil Protection, Niemcy, 2011.
Narodowy Program Ochrony Infrastruktury Krytycznej, RCB, 2013.
National Risk Assessment Method Guide, Holandia, 2008.
National Risk Register, Wielka Brytania, 2008.
Swedish National Risk Assessment, Swedish Civil Contingency Agency, 2012.
Working with scenarios, risk assessment and capabilities In the National Safety and Security Strategy of Netherlands, Holandia, 2009.

Netografia

www.hkatowice.tvp.pl, *Upalne ograniczenia mniej prądu dla zakładów produkcyjnych*, data odczytu: 28.04.2016.
www.tvn24.pl, *Karambol w Krakowie*, data odczytu: 28.04.2016.
www.wyborcza.pl, *Fukushima katastrofa która wciąż trwa*, data odczytu: 28.04.2016.

CHALLENGES AND GOOD PRACTICES OF SECURITY MANAGEMENT OF CRITICAL INFRASTRUCTURE

Abstract

This paper presents a synthesis of knowledge about the process safety management of critical infrastructure in the light of the theory of risk management provisions of the Act on Crisis Management of 26 April 2007 and the related legal acts. The article draws attention to the imperfection of currently accepted procedures, the need for their continuous improvement and adaptation to the prevailing political, legal, social and economic. The result of this article is a list of the challenges facing the Polish system of safety management of critical infrastructure and based on the analysis of foreign methodologies crisis management, the list of good practices in this field. The article is complemented by an analysis of existing theoretical, analytical and project approaches, which are possible for use in the management of security of critical infrastructure.

Keywords

critical infrastructure, crisis management, adverse event, the scenario of events, domino effect