Studia i Materiały. Miscellanea Oeconomicae
Rok 21, Nr 4/2017, tom I
Wydział Prawa, Administracji i Zarządzania
Uniwersytetu Jana Kochanowskiego w Kielcach

Zarządzanie kryzysowe i bezpieczeństwo

Marek Kisilowski[1], Katarzyna Rostek[2], Michał Wiśniewski[3]

KONCEPCJA METODYKI RAPORTOWANIA ZAGROŻEŃ BEZPIECZEŃSTWA NARODOWEGO

Streszczenie: W artykule przeanalizowano stan aktualny wymagań prawnych oraz sytuacji bieżącej w zakresie przygotowywania Raportu zagrożeń bezpieczeństwa narodowego. Zidentyfikowano słabości tego procesu oraz elementy wymagające doskonalenia. Zaproponowano rozwiązanie naprawcze w postaci koncepcji metodyki, która z jednej strony poprawi efektywność procesu i jakość wyniku końcowego, czyli Raportu, a z drugiej strony pozwoli na szersze wykorzystanie zasobów informacyjnych, które są podstawową jego wartością. Praktyczne zastosowanie proponowanego podejścia będzie jednak wymagało zmiany przepisów prawnych, obowiązujących obecnie, co jest również zgodne z tendencjami obserwowanymi w decyzjach Rady i Komisji Europejskiej.

Słowa kluczowe: raportowanie, metodyka, bezpieczeństwo narodowe, zagrożenia, zarządzanie kryzysowe, planowanie cywilne, podatność zasobów, infrastruktura krytyczna

1. Wprowadzenie

Raportowanie zagrożeń bezpieczeństwa narodowego jest regulowane prawnie przez ustawę o zarządzaniu kryzysowym (Dz.U. z 2017 r. poz. 209). Definiuje ona podstawowe obowiązki podmiotów administracji publicznej w tym zakresie, koncentrując się na potrzebach Krajowego Planu Zarządzania Kryzysowego (KPZK). Z tego też względu głównym celem Raportu zagrożeń bezpieczeństwa narodowego (Raport) jest wskazanie najważniejszych zagrożeń bezpieczeństwa państwa i dokonanie oszacowania ryzyka ich wystąpienia oraz skutków. Raport przyjęty przez Radę

[1] Dr inż. Marek Kisilowski, Politechnika Warszawska, Wydział Zarządzania.
[2] Dr hab inż. Katarzyna Rostek, Politechnika Warszawska, Wydział Zarządzania.
[3] Mgr inż. Michał Wiśniewski, Politechnika Warszawska, Wydział Zarządzania.

Ministrów w dniu 15 września 2015 r. zidentyfikował i dokonał oceny około 50 różnych czynników zagrożenia[4].

Z powyższego wynika, że Raport ma kluczowe znaczenie dla bezpieczeństwa państwa, tak w kontekście jego sprawnego funkcjonowania, jak i w kontekście zapewnienia bezpieczeństwa publicznego. Tymczasem analiza przeprowadzona na potrzeby projektu NCBiR[5] pt. „*Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej Rzeczypospolitej Polskiej oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo Gaśniczego*" wykazała dużą niespójność i brak jednolitości w przygotowywaniu raportów cząstkowych, z których następnie powstaje Raport zagrożeń bezpieczeństwa narodowego. Stąd głównym celem projektu jest przygotowanie narzędzi metodycznych i technicznych, ułatwiających gromadzenie, standaryzację oraz integrację danych i informacji, ale również poprawiających zakres i efektywność ich wykorzystania w toku planowania kryzysowego i cywilnego. Cel niniejszego artykułu wpisuje się w tez zakres, a jest nim: *przedstawienie koncepcji metodyki raportowania zagrożeń bezpieczeństwa narodowego, wspomagającej standaryzację i poprawiającej jakość gromadzenia, integracji i przetwarzania danych i informacji w procesie planowania kryzysowego i cywilnego.*

Struktura artykułu została podporządkowana temu celowi, prezentując kolejno – prawne uwarunkowania raportowania zagrożeń bezpieczeństwa narodowego, analizę potrzeb w tym zakresie, koncepcję metodyki – będącą odpowiedzią na zidentyfikowane potrzeby, określenie zakresu stosowalności metodyki oraz dyskusję uzyskanych wyników.

2. Prawne uwarunkowania raportowania zagrożeń bezpieczeństwa narodowego

Zgodnie z art. 5a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[6], na potrzeby KPZK ministrowie kierujący poszczególnymi działami administracji rządowej, kierownicy urzędów centralnych i wojewodowie są obowiązani sporządzić Raport o zagrożeniach bezpieczeństwa narodowego[7]. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa (RCB), a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogącym doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego. Raport powinien zawierać następujące elementy:

- wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka,
- określenie celów strategicznych,
- określenie priorytetów w reagowaniu na określone zagrożenia,

---

[4] http://rcb.gov.pl/raport-o-zagrozeniach-bezpieczenstwa-narodowego-3/, (27-05-2017).

[5] Projekt realizowany ze środków Narodowego Centrum Badań i Rozwoju. Umowa nr DOB – BIO7/11/02/2015.

[6] Dz.U. z 2007 r. poz. 209. Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007.

[7] Szerzej metodykę sporządzania raportu przedstawia: *Ocena ryzyka na potrzeby zarządzania kryzysowego*, Warszawa 2013, RCB (http://rcb.gov.pl/wp-content/uploads/ocenaryzyka.pdf).

– wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych,
– programowanie zadań w zakresie poprawy bezpieczeństwa przez uwzględnienie regionalnych i lokalnych inicjatyw,
– wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych.

Raport przyjmuje Rada Ministrów w drodze uchwały. Kierunki działania wynikające z wniosków Raportu, stanowią element KPZK oraz są uwzględniane w planach zarządzania kryzysowego.

Sposób, tryb i terminy opracowania Raportu określa Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego[8]. Zgodnie z rozporządzeniem podmioty zobowiązane do sporządzenia raportów, w zakresie zgodnym z ich właściwością, opracowują raporty cząstkowe (w postaci papierowej i elektronicznej). Przy czym raport cząstkowy opracowywany przez kierownika urzędu centralnego jest włączony do raportu cząstkowego ministra, któremu kierownik urzędu centralnego podlega lub przez którego jest nadzorowany. Chyba, że minister ten postanowi inaczej.

Raport cząstkowy powinien wskazywać najważniejsze zagrożenia i skutki ich wystąpienia przez stworzenie mapy ryzyka, obejmującej wyszczególnienie rodzajów i charakterystyki zagrożeń. Winien też określać cele strategiczne jakie należy osiągnąć, aby zminimalizować możliwość wystąpienia zagrożenia lub jego skutku, a także hierarchizację celów według kryterium ważności. W raporcie powinny znaleźć się wnioski oraz wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych. Raport cząstkowy wykonuje się i przekazuje z zachowaniem przepisów o ochronie informacji niejawnych. Wykonawca raportu cząstkowego dokonuje jego systematycznej aktualizacji.

Dyrektor RCB koordynuje opracowanie Raportu na podstawie raportów cząstkowych. W zakresie koordynacji opracowania Raportu w części dotyczącej zagrożeń o charakterze terrorystycznym, mogącym doprowadzić do sytuacji kryzysowej organem koordynującym, jest Szef ABW. Zaktualizowany raport cząstkowy podmioty zobowiązane przedkładają nie rzadziej niż raz na dwa lata dyrektorowi RCB oraz w przypadku zagrożeń terrorystycznych Szefowi ABW. Dyrektor RCB jest zobowiązany przedłożyć Raport Radzie Ministrów raz na dwa lata wraz z informacją o dokonanych zmianach.

3. Analiza potrzeb w zakresie raportowania zagrożeń bezpieczeństwa narodowego

Raport o zagrożeniach bezpieczeństwa narodowego jest jedynym tak przekrojowym dokumentem, opracowywanym cyklicznie na poziomie krajowym. Przykładowo, przyjęty 15 września 2015 roku przez Radę Ministrów Raport o zagrożeniach bezpieczeństwa narodowego, opisywał ok. 50 różnych czynników zagrożenia zidentyfikowanych przez ministrów, kierowników urzędów centralnych oraz wojewodów.

[8] Dz.U. z 2010 r. Nr 83, poz. 540. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego.

Najpoważniejszym problemem dotyczącym prawidłowości raportów jest zagadnienie pozyskiwania i przetwarzania danych tak, aby były one dostarczane terminowo, były wiarygodne i docierały do właściwych odbiorców w odpowiednim czasie.

Grzegorz Świszcz[9], szef Wydziału Analiz zwraca uwagę, że konieczny jest rozwój lokalnych systemów monitorowania zagrożeń, a także automatyzacja przepływu danych w formie platformy integracyjnej. Zdaniem autora korzystna byłaby też parametryzacja ocenianych czynników, co ułatwiłoby ich dalsze monitorowanie.

Informacje niezbędne do prawidłowego sporządzenia raportu na szczeblu wojewódzkim uzyskiwane są z powiatów i gmin[10]. Powiat jest ogniwem, które wykonuje najwięcej zadań w zakresie zarządzania kryzysowego[11]. Organem właściwym w sprawach zarządzania kryzysowego na obszarze powiatu jest starosta jako przewodniczący powiatu[12]. Starosta wykonuje zadania zarządzania kryzysowego przy pomocy powiatowego zespołu zarządzania kryzysowego powołanego przez starostę.

Organem właściwym w sprawach zarządzania kryzysowego na terenie gminy jest wójt, burmistrz lub prezydent miasta[13]. Wójt, burmistrz, prezydent miasta wykonuje zadania w zakresie zarządzania kryzysowego przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego. Organem pomocniczym wójta, burmistrza, prezydenta miasta w zapewnieniu wykonywania zadań zarządzania kryzysowego jest gminny zespół zarządzania kryzysowego powołany przez wójta, burmistrza lub prezydenta miasta[14]. Organy właściwe w sprawach zarządzania kryzysowego oraz dyrektor RCB mają prawo żądania (również od jednostek samorządu terytorialnego) informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań w zakresie raportowania zagrożeń bezpieczeństwa narodowego.

Należy też uwzględnić, że elementami systemu zarządzania kryzysowego są również jednostki interwencyjno-ratownicze, m.in. Państwowa Straż Pożarna, centra powiadomienia ratunkowego, policja, jednostki systemu Państwowego Ratownictwa Medycznego, dyspozytorzy medyczni, jednostki ochrony zdrowia, Straż Graniczna, Morska Służba Poszukiwania i Ratownictwa, Ochotnicze Straże Pożarne, Górskie Ochotnicze Pogotowie Ratunkowe i inne urzędy, agencje, inspekcje i straże zobowiązane do przekazywania określonych informacji o potencjalnych zagrożeniach. Jednostki te integrowane są w podsystemy zarządzania[15] stanowiące uzupełnienie systemu zarządzania kryzysowego.

---

[9] G. Świszcz, *Centralna aplikacja raportująca – rola i zadania*, 2013, rcb.gov.pl/wp-content/uploads/prezentacjaCAR.pptx, (27.05.2017).

[10] P. Ruczkowski, *Zarządzanie kryzysowe* [w:] *Publicznoprawne podstawy bezpieczeństwa wewnętrznego*, M. Zdyb (red.), Warszawa 2014, Lex a Wolters Kluwer Business, s. 207-225.

[11] W. Krzeszowski, K. Malasiewicz, N. Prusiński, *Zarządzanie kryzysowe w polskiej administracji publicznej*, Warszawa 2012.

[12] Dz.U. z 2007 r. poz. 209, art. 17.

[13] Dz.U. z 2007 r. poz. 209, art. 19.

[14] M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni i bezpieczeństwa narodowego*, Akademia Bezpieczeństwa Narodowego, Warszawa 2014, s. 44.

[15] K. Sienkiewicz-Małyjurek, F. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa 2010.

Szczególne wymogi sygnalizowania zagrożeń przewiduje Unijny Mechanizm Ochrony Ludności (UMOL). UMOL opiera się na Traktatach UE, przepisach wykonawczych, a obecnie także na Decyzji Parlamentu Europejskiego i Rady Nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności Dz. U. UE. z dnia 20 grudnia 2013 r.[16] Wspólnotowy Mechanizm Ochrony Ludności (WMOL) został ustanowiony decyzją Rady 2001/792/WE, Euratom, poddaną przekształceniu w decyzji Rady 2007/779/WE, Euratom. Finansowanie tego mechanizmu zagwarantowano decyzją Rady 2007/162/WE, Euratom z dnia 5 marca 2007 r. ustanawiającą Instrument Finansowy Ochrony Ludności. W decyzji tej przewidziano udzielanie unijnej pomocy finansowej, zarówno jako wkładu w zwiększenie skuteczności reagowania na poważne sytuacje kryzysowe, jak i w celu udoskonalenia środków służących zapobieganiu i zapewnieniu gotowości w zakresie wszystkich rodzajów sytuacji kryzysowych, w tym na kontynuację środków uprzednio podjętych na mocy decyzji Rady 1999/847/WE.

WMOL może być aktywowany w sytuacjach zagrożeń (powodzie, trzęsienia ziemi, awarie techniczne, itp.). Aktywacja Mechanizmu następuje w oparciu o prośbę o pomoc państwa poszkodowanego. Jeżeli zagrożenie dotyczy któregoś z 31 państw uczestniczących w WMOL (28 państw członkowskich UE oraz Islandia, Lichtenstein, Norwegia i Chorwacja), państwo poszkodowane może poprosić o pomoc za pośrednictwem całodobowego systemu komunikacji (*Common Emergency Communication Information System – CECIS*). Jeżeli zagrożenie występuje poza terytorium państw uczestniczących, to Komisja Europejska aktywuje Mechanizm po otrzymaniu apelu o pomoc od państwa poszkodowanego. W związku z Traktatem z Lizbony, Komisja niezwłocznie informuje Wysokiego Przedstawiciela ds. Zagranicznych i Polityki Bezpieczeństwa o podejmowanych działaniach w sferze europejskiej ochrony ludności. Centrum operacyjnym Mechanizmu jest Centrum Monitoringu i Informacji (*Monitoring and Information Center – MIC*), struktura funkcjonująca w ramach Komisji Europejskiej.

Mechanizm został wprowadzony decyzją Rady UE z dnia 23 października 2001 r., która ustanowiła mechanizm wspólnotowy ułatwiający wzmocnioną współpracę w interwencjach wspierających ochronę ludności[17]. Definiowała ona cel działania Mechanizmu jako „*pomoc w zapewnieniu lepszej ochrony, przede wszystkim ludzi, ale także środowiska i mienia, włączając dziedzictwo kulturowe, w przypadku poważnej sytuacji krytycznej, np. katastrofy naturalnej, technologicznej, radiologicznej lub środowiskowej występującej wewnątrz albo poza Wspólnotą, włączając zanieczyszczenie mórz*".

Praktyczna implementacja zapisów powyższej decyzji Rady została dokonana decyzją Komisji Europejskiej z dnia 29 grudnia 2003 r., ustanawiając mechanizm wspólnotowy ułatwiający wzmocnioną współpracę w interwencjach wspierających

[16] Dz.U. UE. L. 2013. 347. 924. Decyzja Parlamentu Europejskiego i Rady EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

[17] 2001/792/WE, Euratom. Decyzja Rady UE z dnia 23 października 2001 r. ustanawiająca wspólnotowy mechanizm ochrony ludności.

ochronę ludności[18]. Decyzja ta, między innymi, powołała Centrum Monitoringu i Informacji (Monitoring and Information Center - MIC), działające 24 godziny na dobę. Notyfikowany o wystąpieniu zagrożenia lub poproszony o pomoc MIC, zbiera i potwierdza informacje dotyczące zagrożenia i dystrybuuje je do punktów kontaktowych państw – uczestników Mechanizmu oraz ułatwia mobilizację grup ratowniczych i ekspertów. Decyzja stała się też podstawą stworzenia wspólnego systemu komunikacji i informacji w sytuacjach zagrożeń (CECIS) oraz programu szkoleniowego obejmującego interwencje wspierające ochronę ludności.

W 2007 roku dokonano przekształcenia Mechanizmu. Decyzją Rady UE z dnia 8 listopada 2007 r. ustanowiono przekształcony WMOL[19]. Nowym elementem było stworzenie podstaw prawnych do budowy i funkcjonowania tzw. modułów ochrony ludności. Decyzja Parlamentu Europejskiego i Rady Nr 1313/2013/EU jest dalszym krokiem w kierunku udoskonalenia Mechanizmu w kierunku zapobiegania, przygotowania, planowania operacji oraz kształtowania zdolności do reagowania kryzysowego.

Przedstawione powyżej zmiany w znacznym stopniu poszerzają zakres sprawowanej ochrony, ale również zwiększają różnorodność i zawartość informacyjną generowanych danych. Raportowanie zagrożeń bezpieczeństwa narodowego powinno nadążać za tymi zmianami, gwarantować ich uwzględnienie oraz właściwe ich wykorzystanie. Niniejszy artykuł, prezentuje koncepcję opracowaną w ramach projektu NCBiR „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej Rzeczypospolitej Polskiej oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo Gaśniczego", która wychodzi naprzeciw tym potrzebom.

4. Metodyka raportowania zagrożeń bezpieczeństwa narodowego

Wadą obowiązującego procesu sporządzania Raportu 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 z kolei utrudnia analizę i ocenę ryzyka na poszczególnych poziomach administracyjnych[20]. W konsekwencji obniża to poziom powstających planów zarządzania kryzysowego (PZK). Brak jednolitych standardów metodycznych i narzędziowych, w połączeniu z opcjonalnym udziałem powiatów i gmin oraz pominięciem operatorów infrastruktury krytycznej (IK) w procesie sporządzania Raportu stanowią przesłanki do reorganizacji całego procesu (Rys. 1). Proponowana metodyka raportowania zakłada modyfikację obecnie stosowanego podejścia w zakresie:

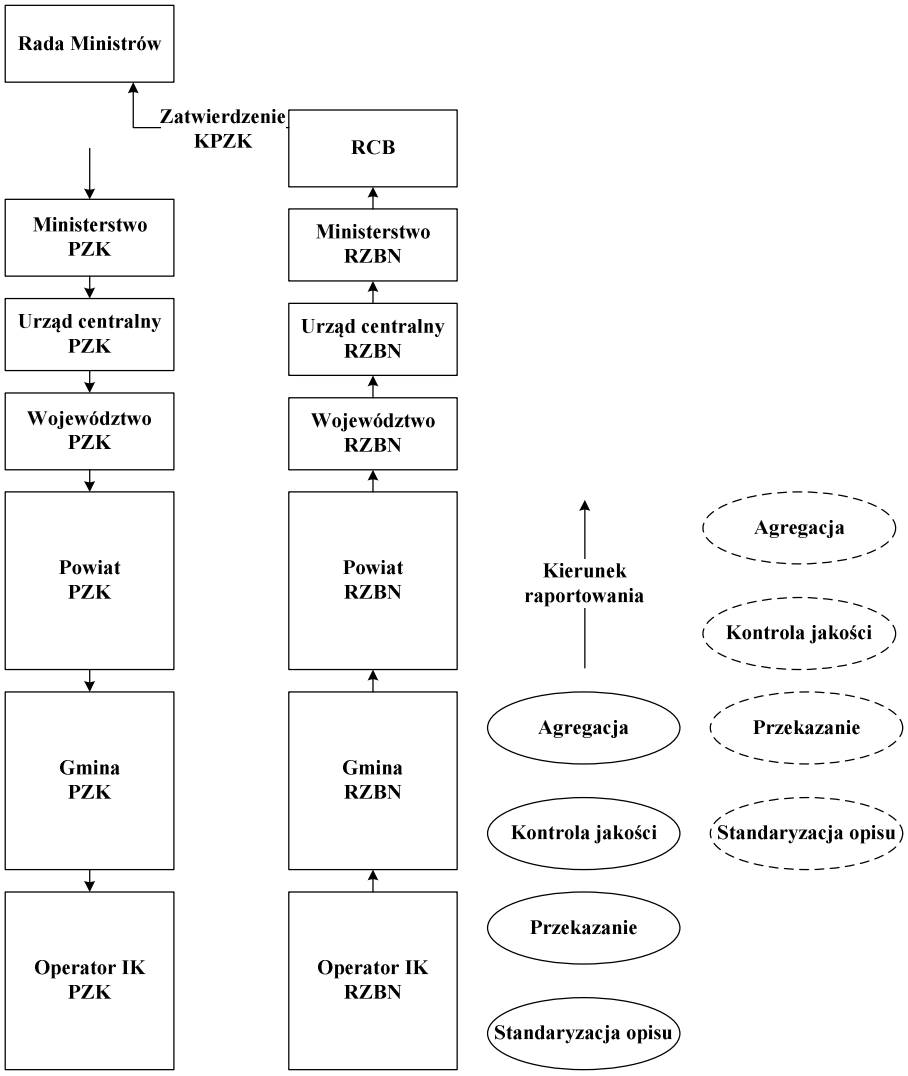
[18] 2004/277/WE, Euratom. Decyzja Komisji UE z dnia 29 grudnia 2003 r. ustanawiająca zasady wykonania decyzji Rady 2001/792/WE, Euratom.

[19] 2007/779/WE, Euratom. Decyzja Rady UE z dnia 8 listopada 2007 r. ustanawiająca wspólnotowy mechanizm ochrony ludności (przekształcenie).

[20] T. Krupa, M. Wiśniewski, *Situational Management of Ctritical Infrastructure Resources Uunder Threat*, Foundations of Management, 2015, vol. 7, an. 15, pp. 93-104.

– uzupełnienia procesu o obligatoryjny, a nie opcjonalny, udział powiatów i gmin w dostarczaniu danych i informacji,
– włączenia do realizacji procesu operatorów IK,
– zastosowania wspólnego sytemu pojęciowego oraz standardu opisu zagrożeń dla wszystkich podmiotów zobowiązanych do opracowania Raportu oraz PZK.

Realizacja dwóch pierwszych postulatów, modyfikujących proces sporządzania Raportu, wymaga zmian w obowiązujących przepisach prawnych i bez takiej zmiany nie będzie mogła być egzekwowana.



Rysunek 1. Metodyka raportowania zagrożeń bezpieczeństwa narodowego
Źródło: opracowanie własne.

Raportowanie zagrożeń bezpieczeństwa narodowego odbywa się w układzie hierarchicznym, co oznacza, że dane i informacje są przekazywane pomiędzy różnymi szczeblami administracji publicznej, pozostającymi w relacjach nadrzędna-podrzędna. Następnie, na podstawie zgromadzonych raportów cząstkowych opracowywany jest Raport, stanowiący podstawę do sporządzenia PZK na poszczególnych poziomach administracyjnych. Prawidłowa realizacja przedstawionej ścieżki postępowania wymaga (Rys. 1):

krok 1: standaryzacji opisu zagrożeń,
krok 2: przekazywania opisu zagrożeń na wyższy poziom,
krok 3: kontroli jakości opisu zagrożeń,
krok 4: agregowania zagrożeń.

Standaryzacja

Standaryzacja opisu zagrożeń oznacza wykorzystanie tych samych metod, procedur, technik oraz narzędzi przez różne jednostki administracyjne oraz operatów IK w procesie sporządzania Raportu. Standaryzacja powinna zapewnić jednolity opis zagrożeń, który umożliwi ich weryfikację oraz agregację na wyższych poziomach administracyjnych.

Wprowadzenie jednolitego standardu opisu zagrożeń dla wszystkich podmiotów procesu sporządzania Raportu wymaga odwołania się do elementu występującego w ramach dowolnego systemu. Tym elementem są zasoby realizujące funkcjonalności. Analiza wymogów prawnych[21] doprowadziła do identyfikacji trzech zasadniczych kategorii opisujących zasoby:

– zagrożenia, na które zasoby są podatne,
– funkcjonalności, które są realizowane dzięki zasobom,
– zabezpieczenia zasobów przed rozpoznanymi zagrożeniami.

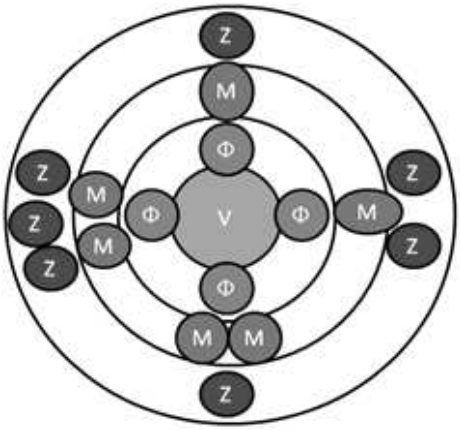
Obserwacja ta umożliwiła opracowanie modelu sytuacji zasobu[22], który może stanowić standard opisu zagrożeń na dowolnym poziomie administracji publicznej oraz dla operatorów IK (Rys. 2).

Przeprowadzona analiza aktów prawnych wykazała również, że nie jest możliwe wskazanie zamkniętego zbioru atrybutów opisujących składowe modelu sytuacji zasobu. Dlatego proponowany standard opisu zagrożeń bezpieczeństwa narodowego musi mieć otwartą strukturę, co pozwoli na jego dostosowanie do zmieniających się przepisów oraz potrzeb różnych podmiotów zaangażowanych w proces sporządzania Raportu. Zaproponowany model sytuacji zasobu umożliwia agregację danych dotyczących zagrożeń rozpoznanych na różnych poziomach administracyjnych, co jest wymagane aby nadrzędny poziom administracyjny mógł opracować własny raport cząstkowy.

---

[21] M. Wiśniewski, T. Ostrowska, *Wyzwania i dobre praktyki zarządzania bezpieczeństwem infrastruktury krytycznej*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, Fundacja GAP, Kraków 2016, s. 111-125.

[22] M. Wiśniewski, *Concept of Situational Management of Safety Critical Infrastructure of State*. Foundations of Management,vol. 8, an.16, Warszawa 2016, pp. 297-310.



gdzie:
V – zasób
Φ – funkcjonalności zasobu
Z – zagrożenia oddziałujące na funkcjonalności
M – modele zabezpieczeń funkcjonalności

Rysunek 2. Model sytuacji zasobu
Źródło: M. Wiśniewski, *Concept of Situational…*, *op.cit.,* s. 301.

Przekazanie

Przekazanie wyników analizy zagrożeń przygotowanych zgodnie z zaproponowanym standardem opisu, wyznaczonym przez model sytuacji zasobu może odbywać się przy zachowaniu obowiązujących procedur przekazywania raportów cząstkowych. Postuluje się jednak rozszerzenie obowiązku przygotowywania raportów cząstkowych na poziom powiatu, gminy oraz włączenie do tego procesu operatorów IK.

Usprawnienie procesu przekazywania wyników analizy zagrożeń może zostać usprawnione przez wdrożenie narzędzia informatycznego, implementującego model sytuacji zasobu. Wdrożenie takiego narzędzia pozwoli na częściową automatyzację procesu agregacji danych, dotyczących zagrożeń na poszczególnych poziomach administracyjnych.

Kontrola

Przez pojęcie kontroli rozumie się, że na podstawie przygotowanych raportów cząstkowych z poziomu niższego, właściwa jednostka ds. bezpieczeństwa na poziomie wyższym będzie w stanie ocenić i wskazać luki w przygotowanym Raporcie.

Logiczne powiązanie zagrożeń z zasobami realizującymi funkcjonalności, których brak lub ograniczona dostępność może stanowić zagrożenie bezpieczeństwa narodowego, zastosowane w modelu sytuacji zasobu, umożliwia weryfikację opracowanych raportów cząstkowych na dowolnym poziomie administracyjnym. Wykryte luki w zbiorze zagrożeń mogą być łatwo uzupełnione, a zasadność ich wprowadzenia wykazana poprzez ich wpływ na sprawność funkcjonowania zasobów.

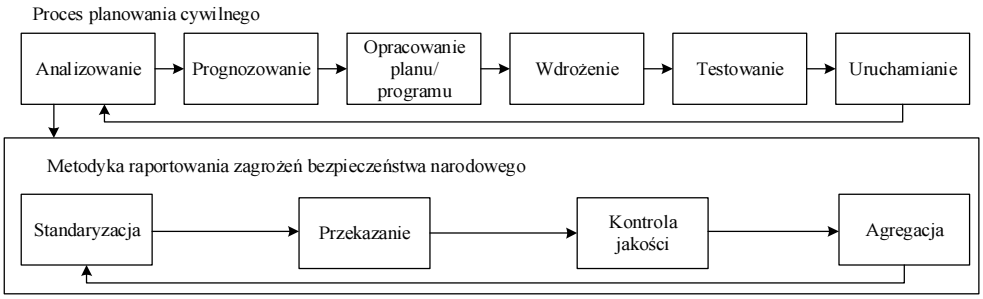
Agregacja

Przez agregację rozumie się, że na podstawie zebranych raportów z poziomów niższych (np. operatora IK), jednostka ds. bezpieczeństwa na poziomie wyższym będzie mogła opracować zbiorczy raport dla własnego poziomu (np. gminy), poprzez zsumowanie zbiorów zagrożeń z poziomów niższych. Wprowadzenie jednolitego standardu opisu zagrożeń umożliwia ich powiązanie ze sobą na zasadzie agregacji zasobów w procesy, dostarczające określone funkcjonalności (np. zagrożenia na które podatna jest elektrownia i zagrożenia na które podatne są linie przesyłowe razem stanowią zbiór zagrożeń dla funkcjonalności dostarczania energii elektrycznej mieszańcom gminy).

Przykładem zastosowania proponowanej metodyki raportowania jest sytuacja, w której na terenie gminy znajdują się dwa zakłady produkcyjne zawarte w wykazie IK (np. elektrownia i oczyszczalnia ścieków). Proponowana metodyka zakłada, że raport cząstkowy gminy powinien zawierać zbiór zagrożeń dla obu działających na jej terenie obiektów IK. Następnie raport cząstkowy gminy może być uzupełniony o inne zagrożenia, stanowiące potencjalne zagrożenia bezpieczeństwa narodowego, a wynikające z materializacji zagrożeń, na które podatne są wskazane IK (np. wystąpienie powodzi, która obejmie oczyszczalnię ścieków, może wywołać skażenie środowiska na terenie gminy. Z kolei pożar na terenie elektrowni może skutkować przerwą w dostawie prądu, co może ograniczyć dostęp społeczności gminy do środków finansowych i usług elektronicznych).

5. Zakres stosowalności metodyki

Zaproponowana koncepcja metodyki raportowania zagrożeń bezpieczeństwa narodowego, podobnie jak obecne procedury w tym zakresie, powinna być częścią procesu planowania cywilnego (Rys. 3).



Rysunek 3. Umiejscowienie metodyki raportowania zagrożeń bezpieczeństwa narodowego w procesie planowania cywilnego
Źródło: opracowanie własne.

Dane zebrane w ramach procedury przygotowywania Raportu wspomagają etap analiz procesu planowania cywilnego, którego celem jest zebranie danych oraz

opracowanie raportów umożliwiających prognozowanie przebiegu zdarzeń niepożądanych. W tym kontekście zebrane dane, dotyczące zagrożeń bezpieczeństwa narodowego, stanowią podstawę do opracowania scenariuszy zdarzeń niekorzystnych[23], których stosowanie nie jest obecnie wymagane polskimi przepisami prawnymi. Niemniej potrzeba ich wprowadzenia jest sygnalizowana m.in. w:

- Dyrektywie Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, art. 2,
- Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, § 2, ust 3,
- Procedurze opracowywania raportu cząstkowego do raportu o zagrożeniach bezpieczeństwa narodowego, s. 10-18.

Gromadzenie danych dotyczących zagrożeń bezpieczeństwa narodowego według przedstawionej metodyki wymaga wdrożenia:

- wspólnego katalogu zagrożeń standaryzującego klasyfikację zagrożeń dla wszystkich podmiotów uczestniczących w przygotowaniu Raportu (jednocześnie dopuszcza się możliwość występowania zagrożeń specyficznych, występujących na określonym terenie. Takie zagrożenie powinno być wprowadzone do systemu informatycznego z możliwością uzupełnienia katalogu głównego, dostępnego dla wszystkich podmiotów przygotowujących Raport),
- systemu informatycznego, który umożliwi cyfrowe gromadzenie danych dotyczących zagrożeń bezpieczeństwa narodowego, ich przetwarzanie, przechowywanie i przekazywanie między szczeblami (wdrożenie takiego systemu usprawni wszystkie kroki proponowanej metodyki raportowania zagrożeń bezpieczeństwa narodowego) oraz:
  - wymusi stosowanie przyjętego standardu opisu zagrożeń,
  - zautomatyzuje przekazywanie raportów cząstkowych między szczeblami administracyjnymi,
  - ułatwi kontrolę raportów np. poprzez automatyczne porównanie sprawozdań z poprzednich okresów lub porównanie ich zawartości ze standardowym wykazem zagrożeń IK,
  - w przypadku pozytywnej weryfikacji RZBN z niższych poziomów, automatycznie przygotuje wstępny RZBN poziomu wyższego,
  - ponadto w systemie można zaszyć mechanizmy wymuszające stosowanie przyjętej klasyfikacji zagrożeń.

Wspólny katalog zagrożeń został wypracowany w ramach projektu badawczo-rozwojowego NCBiR pt.: *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*[24]. Natomiast mechanizm uzupełniania tego katalogu o zagrożenia

[23] M. Wiśniewski, *Concept of Situational Management of Safety Critical Infrastructure of State*, Foundations of Management, vol. 8, an.16, Warszawa 2016, pp. 297-310.

[24] W. Skomra, *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*, Warszawa 2015, Załącznik na płycie CD.

specyficzne opisano w publikacji pt. *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*[25]. Obecnie trwają prace badawcze nad specjalistyczną platformą informacyjno-usługową, której zadaniem jest wspomaganie planowania cywilnego i ratowniczego.

6. Podsumowanie

Zaproponowana koncepcja metodyki RZBN eliminuje niesprawności obecnie stosowanych procedur, tj. brak jednolitych standardów metodycznych i narzędziowych opracowywania Raportu dla wszystkich podmiotów procesu, opcjonalny udział powiatów i gmin, pominięcie operatorów IK.

Odwołanie się w standardzie opisu zagrożeń bezpieczeństwa narodowego do wspólnego elementu, który jest podatny na zagrożenia sprawia, że omawiana koncepcja metodyki RZBN może być stosowana przez wszystkich uczestników tego procesu. Ponadto metodyka znajduje zastosowanie wszędzie, gdzie wymagane jest przygotowanie planów ciągłości działania. Przykładem mogą być przedsiębiorstwa produkcyjne, gdzie sprawność procesów produkcyjnych zależy od maszyn i urządzeń podatnych na zagrożenia. Metodyka może również znaleźć zastosowanie w przedsiębiorstwach usługowych np. świadczących usługi cloud computing, gdzie dostępność usług jest również uzależniona od sprawności posiadanych zasobów. I w wielu innych przypadkach, gdzie kwestia gromadzenia, udostępniania, czy współdzielenia zasobów jest elementem krytycznym realizacji procesu.

Metodyka wymaga jednak wprowadzenia zmian w obowiązujących przepisach prawnych oraz wymusza na podmiotach procesu sporządzania Raportu stosowanie ilościowych metod opisu zagrożeń. Z kolei wprowadzenie ilościowych metod opisu zagrożeń pozwala na dokładniejszą analizę i ocenę ryzyka, jednak wymaga większego wysiłku ze strony osób zajmujących się bezpieczeństwem w ramach danej jednostki administracyjnej. Może to powodować sprzeciw tych osób przeciwko postulowanym zmianom, determinowany obawą o zwiększony zakres koniecznych prac.

Bibliografia:

2001/792/WE, Euratom. Decyzja Rady UE z dnia 23 października 2001 r. ustanawiająca wspólnotowy mechanizm ochrony ludności.

2004/277/WE, Euratom. Decyzja Komisji UE z dnia 29 grudnia 2003 r. ustanawiająca zasady wykonania decyzji Rady 2001/792/WE, Euratom.

2007/779/WE, Euratom. Decyzja Rady UE z dnia 8 listopada 2007 r. ustanawiająca wspólnotowy mechanizm ochrony ludności (przekształcenie).

Dz.U. UE. L. 2013. 347. 924. Decyzja Parlamentu Europejskiego i Rady EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

Dz.U. z 2007 r. poz. 209. Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007.

Dz.U. z 2010 r. Nr 83, poz. 540. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego.

[25] A. Kosieradzka, J. Zawiła-Niedźwiecki (red.), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*, Kraków-Legionowo 2016, ss. 303-305.

Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni i bezpieczeństwa narodowego*, Akademia Bezpieczeństwa Narodowego, Warszawa 2014.
Kosieradzka A., Zawiła-Niedźwiecki J., (red.), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*, Kraków-Legionowo 2016.
Krupa T., Wiśniewski M., *Situational Management of Ctritical Infrastructure Resources Uunder Threat*, Foundations of Management, 2015, vol. 7, an. 15.
Krzeszowski W., Malasiewicz K., Prusiński N., *Zarządzanie kryzysowe w polskiej administracji publicznej*, Warszawa 2012.
Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2015.
Ocena ryzyka na potrzeby zarządzania kryzysowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.
Ruczkowski P., *Zarządzanie kryzysowe*, [w:] M. Zdyb (red.) *Publicznoprawne podstawy bezpieczeństwa wewnętrznego*, Lex a Wolters Kluwer Business, Warszawa 2014.
Sienkiewicz-Małyjurek K., Krynojewski F., *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa 2010.
Skomra W., *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*. Warszawa 2015.
Świszcz G., *Centralna aplikacja raportująca – rola i zadania*, 2013, rcb.gov.pl/wp-content/uploads/prezentacjaCAR.pptx, (27.05.2017).
Wiśniewski M., *Concept of Situational Management of Safety Critical Infrastructure of State*, Foundations of Management, vol. 8, an.16, Warszawa 2016.
Wiśniewski M., Ostrowska T., *Wyzwania i dobre praktyki zarządzania bezpieczeństwem infrastruktury krytycznej*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, Fundacja GAP, Kraków 2016.

Abstract

Conception of methodology for reporting threats of national security

The article analyzed the current state of legal requirements and the current situation in the preparation of the Report of national security threats. The weaknesses of this process and the elements that require improvement have been identified. A corrective solution has been proposed in the form of a methodology that will improve on the one hand the efficiency of the process and the quality of the final result ie the Report, and on the other hand will allow a wider use of the information resources that are fundamental to its value. However, the practical application of the proposed approach will, however, require a revision of the legislation currently in force, which is also in line with the trends observed in the decisions of the European Council and the European Commission.

Keywords: reporting, methodology, national security, threats, crisis management, civil planning, resources vulnerability, critical infrastructure