



SENAT
RZECZYPOSPOLITEJ
POLSKIEJ

ADMINISTRACJA PUBLICZNA W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA

Kancelaria Senatu

ADMINISTRACJA
PUBLICZNA
W SYSTEMIE
BEZPIECZEŃSTWA
PAŃSTWA

Redakcja naukowa

Prof. nzw. dr hab. Anna Gołębiowska

Dr Piotr Benedykt Zientarski

Warszawa 2017

Recenzenci

Prof. dr hab. Marek Chmaj – Uniwersytet SWPS

Dr hab. prof. nzw. Andrzej Bisztyga – Uniwersytet Zielonogórski

Prof. nzw. dr hab. Paweł Kępa – Szkoła Główna Służby Pożarniczej
w Warszawie

Korekta

MAGDALENA NAROŻNA

Projekt okładki

ALICJA NOWACZYK

Redakcja techniczna

PAWEŁ WOJCIECHOWSKI

ISBN 978-83-65711-10-6

CIP – Biblioteka Narodowa

Administracja publiczna w systemie bezpieczeństwa
państwa / redakcja naukowa Anna Gołębiowska, Piotr
Benedykt Zientarski ; [Senat Rzeczypospolitej
Polskiej]. – Warszawa : Kancelaria Senatu, 2017

Centrum Informacyjne Senatu

Dział Edycji i Poligrafii

Warszawa 2017 r.

Nakład 120 egz.

Spis treści

Anna Gołębiowska, Piotr Benedykt Zientarski	
Przedmowa	5
Anna Gołębiowska, Piotr Benedykt Zientarski	
Rozdział I.	
Organy administracji rządowej i samorządowej w sferze	
bezpieczeństwa i porządku publicznego.	9
Marek Lisiecki	
Rozdział II.	
Organizacja i zarządzanie bezpieczeństwem w przyszłości	29
Jerzy Wolanin	
Rozdział III.	
Jak mierzyć odporność społeczności lokalnej?	43
Bogdan Kosowski	
Rozdział IV.	
Stan bezpieczeństwa państwa pochodną procesu podejmowania decyzji	
w administracji publicznej	69
Marcin M. Smolarkiewicz	
Rozdział V.	
Nowoczesne techniki w służbie zarządzania kryzysowego –	
nauka, dydaktyka, praktyka.	85
Paweł Gromek	
Rozdział VI.	
Ciężkość działania administracji publicznej w obliczu	
zagrożeń bezpieczeństwa powszechnego	107
Marek Woch	
Rozdział VII.	
Bezpieczeństwo zdrowotne w działaniach organów	
władzy publicznej w Polsce	123

Aneta Kułakowska/ Ewa Frankowska	
<i>Rozdział VIII.</i>	
<i>Rola monitoringu ekonomicznego w organizacji</i>	139
Barbara Stefaniuk	
<i>Rozdział IX.</i>	
<i>Współczesne uwarunkowania systemu zarządzania kryzysowego</i>	159
Dariusz Prokopowicz	
<i>Rozdział X.</i>	
<i>Wzrost znaczenia bezpieczeństwa elektronicznego transferu danych</i>	
<i>w Internecie w kontekście bezpieczeństwa</i>	
<i>administracji publicznej państwa</i>	173
Załączniki do publikacji:	
Anna Gołębiowska, Piotr Benedykt Zientarski	
<i>Słowo wstępne</i>	195
Głosy w dyskusji na temat roli administracji publicznej	
w systemie bezpieczeństwa państwa podczas konferencji zorganizowanej	
przez Komisję Samorządu Terytorialnego i Administracji Państwowej Senatu RP	
we współpracy z Wydziałem Inżynierii Bezpieczeństwa Cywilnego Szkoły Głównej	
Służby Pożarniczej w Warszawie w dniu 12 grudnia 2016 r.	197

Przedmowa

Rola administracji publicznej w systemie bezpieczeństwa państwa jest tą sferą administrowania, w której dążenie do celu może przekroczyć granice wyznaczone przez powszechnie obowiązujące normy prawne. W związku z tym zasadne wydaje się precyzyjne określenie celu tworzenia struktur i podejmowania działań. Ponadto istotne jest wskazanie metod działania i stworzenie instrumentów pozwalających na zapewnienie sprawności i legalności realizowanych przedsięwzięć.

Z uwagi na to nasuwa się pytanie: czy jest możliwe takie współdziałanie przedstawicieli różnych dyscyplin naukowych, które doprowadzi do wspólnych wniosków pomimo odrębnych punktów widzenia zagadnienia, czy też innych metod badawczych i stosowania w ramach tych metod odmiennych instrumentów? Problematyka dotycząca roli administracji publicznej w systemie bezpieczeństwa państwa dopuszcza takie współdziałanie, podobnie jak wiele innych kwestii związanych z organizacją i funkcjonowaniem administracji publicznej. Dlatego też pozostaje problem koordynacji badań w omawianym zakresie.

Podnosząc kwestie legalności działania administracji publicznej w sferze systemu bezpieczeństwa państwa, należy mieć na uwadze fakt, że administracja publiczna funkcjonuje w ramach państwa, a więc istotne jest to, jakie cele dane państwo sobie obiera. Z tego względu zasada legalizmu oraz zasada sprawności stanowią główny wyznacznik działania administracji publicznej w warunkach demokratycznego państwa prawnego. Administracja publiczna, działając w zakresie dotyczącym sfery systemu bezpieczeństwa państwa, co do zasady czyni to w sferze *imperium*. Wynika to ze specyfiki celu tych działań, a jest nim konieczność ochrony wartości umożliwiających życie w społeczności. I właśnie w tym zakresie niezbędną jest ścieżka władcza w celu wyegzekwowania od wszystkich podmiotów prawa nakazanego lub zakazanego działania. Jednakże, niezależnie od tego, czy mamy do czynienia z aktywnością w sferze *imperium*, czy też w sferze *dominium*, należy uwzględnić fakt, że działania administracji publicznej muszą opierać się na normach prawnych.

Zasada legalizmu to jedna z podstawowych zasad ustrojowych, która przenika administrację publiczną i tym samym determinuje jej działanie. Zgodnie z tą zasadą możliwe jest związanie administracji publicznej prawem, a także określenie jej zadań i kompetencji, co ma znaczenie w sferze, jaką jest kreacja oraz ochrona

bezpieczeństwa państwa. Przepis art. 7 Konstytucji RP zobowiązuje organy władzy publicznej do działania na podstawie i w granicach prawa. Takie ujęcie zasady legalizmu, z której wynika zasada związania prawem administracji publicznej, posiada charakter tylko formalny. W związku z tym należy ją odczytywać z uwzględnieniem innych przepisów konstytucyjnych, zwłaszcza art. 2. Podejście to jest konieczne, aby działania administracji publicznej wpisywały się w naturę demokratycznego państwa prawnego i społeczeństwa obywatelskiego. Fundamentalne znaczenie zasady legalizmu polega na tym, że eliminuje się dowolność i samowolę w relacjach zachodzących pomiędzy organami władzy publicznej a obywatelami.

Warto również podkreślić, iż działanie na podstawie prawa oznacza, że musi istnieć norma prawna, która upoważnia dany organ do działania w sytuacji, w której występuje on jako dzierżyciel władztwa publicznego. Oznacza to, iż norma prawna musi określać jego kompetencję, nawet gdy czyni to w sposób ogólny. Można zatem powiedzieć, iż kompetencji organu administracji publicznej nie można swobodnie domniemywać, bowiem musi ona wynikać z przyjętego porządku prawnego. W przypadku działania w granicach prawa należy rozumieć, iż organy administracji publicznej mają konstytucyjny obowiązek działania zgodnie z ustanowionymi przez prawodawcę zakazami i nakazami. I pomimo tego, iż w działaniach administracji publicznej istnieje pewien tzw. luz, który dotyczy swobodnego uznania, to tego uznania nie należy mylić z dowolnością działania. Tak więc zawsze jego podstawą będzie dana norma prawna, natomiast działania administracji publicznej w tym zakresie podlegać będą kontroli niezależnych organów – sądów administracyjnych. Podkreślenia wymaga fakt, iż zasada legalizmu wynika z koncepcji państwa prawnego, która głosi, że państwo nie stoi ponad prawem, czyli podlega mu na równi z innymi podmiotami, do których adresowane są normy prawne.

Autorzy publikacji zatytułowanej *Administracja publiczna w systemie bezpieczeństwa państwa* podjęli się trudnego zadania zidentyfikowania podstawowych zagadnień dotyczących bezpieczeństwa państwa i wskazania na tej podstawie instrumentów działania administracji publicznej. Niezmiernie istotną kwestią, która znalazła swoje odzwierciedlenie w publikacji, są zagadnienia łączące się z rozwojem nowych technologii, wzrostem znaczenia Internetu i telekomunikacji w życiu wszystkich grup społecznych. Zastosowanie innowacyjnych technik przeobraziło współczesne społeczeństwo, które jest społeczeństwem informacyjnym. I chociaż z jednej strony stwarza to zagrożenia w zakresie bezpieczeństwa i porządku publicznego, to z drugiej strony daje zarówno administracji publicznej, jak i wszystkim służbom publicznym nowe instrumenty działania. Doprowadza to do analizy technologicznych aspektów w zakresie bezpieczeństwa i porządku publicznego. Niemniej jednak technologiczne aspekty nie mogą przesłaniać w tym zakresie elementów o charakterze prawnym, szczególnie związanych

z zapewnieniem legalności działania administracji publicznej w kwestii związanej z bezpieczeństwem państwa.

Na uwagę zasługują przedstawione w publikacji elementy o charakterze prawoporównawczym, bowiem pozwalają na obiektywną ocenę działań administracji publicznej w systemie bezpieczeństwa państwa. Poza tym należy podkreślić interdyscyplinarność prowadzonych rozważań. Publikacja zatytułowana *Administracja publiczna w systemie bezpieczeństwa państwa* ukazuje w jednoznaczny sposób, iż ciągle szuka się rozwiązań mogących podnieść efektywność oraz sprawność działania administracji publicznej w sferze bezpieczeństwa państwa. To dążenie, jak wskazują Autorzy publikacji, nie może spowodować przekroczenia legalności działania. Z tego względu ogromną rolę w tym zakresie powinna odgrywać działalność legislacyjna Sejmu i Senatu Rzeczypospolitej Polskiej, orzecznictwo organów wymiaru sprawiedliwości, jak również współdziałanie organów administracji publicznej ze społeczeństwem na szczeblu zarówno lokalnym, regionalnym, jak i centralnym.

*Prof. nzw. dr hab. Anna Gołębiowska
Dr Piotr Benedykt Zientarski*

Rozdział I.

Organy administracji rządowej i samorządowej w sferze bezpieczeństwa i porządku publicznego

1. Wprowadzenie

Administracja rządowa oraz administracja samorządowa¹ na szczeblu gminnym², powiatowym³ i wojewódzkim⁴ realizuje określone zadania publicz-

Prof. nzw. dr hab. Anna Gołębiowska – Zakład Prawa, Wydział Inżynierii Bezpieczeństwa Cywilnego, Szkoła Główna Służby Pożarniczej w Warszawie.

Dr Piotr Benedykt Zientarski – przewodniczący Komisji Samorządu Terytorialnego i Administracji Państwowej Senatu RP.

¹ Por. A. Gołębiowska, *Prawo miejscowe samorządu terytorialnego w okresie drugiej Rzeczypospolitej*, „Cogitatus” nr 7, Wydawnictwo Collegium Varsoviense, Warszawa 2009, s. 53–68; H. Szczechowicz, *Samorząd terytorialny w społeczeństwie obywatelskim*, [w:] *Samorząd terytorialny na przełomie XX/XXI wieku*, (red.) A. Lutrzykowski, R. Gawłowski, M. Popławski, Toruń 2010, s. 90.

² Por. Ustawa z dnia 8 marca 1990 r. o samorządzie terytorialnym (tekst pierwotny: Dz. U. z 2001 r. nr 142, poz. 1591; obecnie ustawa o samorządzie gminnym); A. Gołębiowska, *Istota samorządu terytorialnego w świetle postanowień Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, [w:] *Administracja publiczna – uwarunkowania prawne, organizacyjne i społeczne*, (red.) A. Gołębiowska, Powszechne Wydawnictwo Prawnicze, Warszawa 2015, s. 15–32.

³ A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego i jego koncepcje prawno-organizacyjne*, [w:] *Rzeczpospolita w koncepcjach transformacji ustrojowej 1989 r.*, (red.) A. Gołębiowska, Powszechne Wydawnictwo Prawnicze, Warszawa 2015, s. 59–80.

⁴ Por. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. nr 142, poz. 1592 ze zm.); Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. nr 142, poz. 1590 ze zm.); Ustawa z dnia 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz. U. z 1998 r. nr 96, poz. 603 ze zm.); A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 25–29.

ne⁵, w tym porządek i bezpieczeństwo publiczne⁶. Pojęcie „bezpieczeństwo i porządek publiczny” ma charakter wieloznaczny. W doktrynie podkreśla się niejasność tych terminów. W związku z tym powstają trudności w ich zdefiniowaniu. I chociaż terminy te występują łącznie, to w sensie znaczeniowym są niejednoznaczne. Pojęcie „bezpieczeństwo” można rozpatrywać w aspekcie bezpieczeństwa państwa i bezpieczeństwa publicznego⁷.

Zapewnienie bezpieczeństwa państwa związane jest z przeciwdziałaniem niebezpieczeństwom zewnętrznym i wewnętrznym. Bezpieczeństwo publiczne to stan, w którym obywatelom nie grozi żadne niebezpieczeństwo, natomiast instytucje państwa mogą funkcjonować w normalnym trybie. W związku z tym zapewnienie bezpieczeństwa publicznego związane będzie m.in. z klęskami żywiołowymi oraz napadami. Ponadto porządek publiczny zdefiniować można jako system urządzeń prawno-publicznych i stosunków społecznych. Ich celem zaś jest ochrona mienia, zdrowia, usuwanie uciążliwości niebezpiecznych itp. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.⁸ posługuje się następującymi pojęciami:

⁵ Por. A. Gołębiowska, *Decentralizacja administracji publicznej na przykładzie samorządu gminnego. Zarys problematyki*, „Opere et Studio pro Oeconomia” No 6, Warszawa 2009, s. 63–87; H. Izdebski, M. Kulesza, *Administracja publiczna. Zagadnienia ogólne*, Warszawa 2004, s. 135; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 26–29.

⁶ A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu terytorialnego w zakresie ochrony bezpieczeństwa i porządku publicznego*, [w:] *Zrównoważony rozwój gospodarczy jednostek samorządu terytorialnego*, (red.) E. Sobczak, Warszawa 2015, s. 7–21.

⁷ A. Gołębiowska, *Prawo do wolności i bezpieczeństwa osobistego w prawie międzynarodowym oraz Konstytucji Rzeczypospolitej Polskiej*, [w:] *Paradygmaty badań nad bezpieczeństwem. Jednostki, grupy i społeczeństwa*, (red.) M. Kopczeński, A. Kurkowska, S. Mikołajczak, Poznań 2015, s. 643–667.

⁸ Por. A. Gołębiowska, *Konstytucja Rzeczypospolitej Polskiej a samorząd terytorialny*, [w:] *Funkcjonowanie samorządu terytorialnego – uwarunkowania prawne i społeczne*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 13–32; Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. nr 89, poz. 555 ze zm.); Por. B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009; A. Gołębiowska, *Prawo do dobrej administracji jako prawo podstawowe o randze konstytucyjnej*, [w:] *Efektywność działania administracji publicznej w Polsce*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 11–29; A. Gołębiowska, *Prawo do wolności i bezpieczeństwa...*, s. 662; Podstawy prawne działania samorządu terytorialnego znajdują się w Konstytucji RP w art. 15 i 16 w Rozdziale I „Rzeczypospolita” oraz w art. 163–172 w Rozdziale VII „Samorząd terytorialny”. Samorząd terytorialny jest podstawowym ogniwem zdecentralizowanej administracji publicznej, a art. 15 Konstytucji RP zapewnia decentralizację władzy publicznej. Zatem bez przekazania samorządowi terytorialnemu istotnej części zadań publicznych trudno byłoby mówić o faktycznej decentralizacji władzy publicznej, której istotą jest ustawowe przekazanie części istotnych zadań i kompetencji władzy publicznej jednostkom niższego szczebla (administracji samorządowej), przy zapewnieniu im samodzielności w realizowaniu przekazanych zadań. Jednostki samorządu terytorialnego występują jako samodzielne podmioty prawa publicznego wykonujące zdania publiczne i ponoszące odpowiedzialność za ich realizację; A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu terytorialnego...*, s. 17–19.

- bezpieczeństwo obywateli⁹;
- bezpieczeństwo i porządek publiczny¹⁰;
- bezpieczeństwo konsumentów, użytkowników i najemców¹¹;
- bezpieczeństwo państwa¹².

Podmiotami wykonującymi zadania w zakresie porządku i bezpieczeństwa publicznego są:

- Prezydent RP;
- organy administracji rządowej¹³;
- organy jednostek samorządu terytorialnego;
- organy i instytucje pozarządowe;
- podmioty prywatne.

Podmioty te posiadają przypisane zadania własne, jak również realizują je samodzielnie we własnym imieniu i na własną odpowiedzialność¹⁴. Pomiędzy

⁹ Por. Art. 35 Konstytucji RP; A. Gołębiowska, *Konstytucja Rzeczypospolitej Polskiej...*, s. 16–23.

¹⁰ Por. Art. 31 Konstytucji RP; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 27–31.

¹¹ Por. Art. 76 Konstytucji RP; A. Gołębiowska, *Konstytucja Rzeczypospolitej Polskiej...*, s. 24–28; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 16–21.

¹² Art. 146 Konstytucji RP.

¹³ Por. A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa obywatela do informacji o działaniach organów samorządu terytorialnego*, [w:] *Funkcjonowanie samorządu terytorialnego – uwarunkowania prawne i społeczne*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 45–62; Zasadnym jest wskazanie art. 4 ustawy o samorządzie województwa, z którego wynika zakres działania samorządu województwa, ale który nie narusza samodzielności powiatu i gminy. Warto wyjaśnić, że organy samorządu województwa wobec powiatu i gminy nie stanowią organów kontroli i nadzoru. Wobec tego samorząd terytorialny, wykonując administrację publiczną, działa w sposób samodzielny zgodny z zasadą decentralizacji. Poza tym samodzielność nie wyklucza możliwości sprawowania nadzoru nad działalnością jednostek samorządu terytorialnego przez organy administracji rządowej. W związku z tym samodzielności jednostek samorządu terytorialnego nie można utożsamiać z suwerennością, ponieważ jako element ładu publicznego w państwie nie może być rozpatrywana w oderwaniu od państwa. Odmienny pogląd w tej kwestii prowadziłby do destrukcji państwa i anarchizacji w sferze realizowania zadań publicznych. Warto również zwrócić uwagę na wyrok Trybunału Konstytucyjnego z dnia 27 września 1994 r. (sygn. akt W 10/93, OTK 1994, nr 2, poz. 46), w którym podkreślono, że: „Gwarantując samorządowi terytorialnemu udział w sprawowaniu władzy oraz powierzając *implicite* organom państwa określenie rozmiarów i form tego udziału, polski ustawodawca konstytucyjny ustanowił prawno pozytywne podstawy działania samorządu terytorialnego i włączył go do struktury sprawowania władzy (...) a tym samym odmówił mu przymiotu władzy suwerennej, o innym niż prawo stanowione przez to państwo źródle władzy publicznej”.

¹⁴ Por. A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 12–16; M. Stec, *Podział zadań i kompetencji w nowym ustroju terytorialnym Polski (kryteria i normatywna realizacja)*, „Samorząd Terytorialny” nr 11 (1998), s. 24–29; H. Izdebski, *Samorząd terytorialny. Podstawy ustroju i działalności*, Warszawa 2006, s. 117–121; Z. Bukowski, T. Jędrzejewski, P. Rączka, *Ustrój samorządu terytorialnego*, Toruń 2005, s. 79–92; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 18–22.

administracją rządową a samorządową występują powiązania w zakresie bezpieczeństwa i porządku publicznego¹⁵.

Jednakże, powracając jeszcze do interpretacji pojęcia „bezpieczeństwo”¹⁶, należy podkreślić, iż odnosi się ono do poczucia zabezpieczenia i pewności¹⁷. Z kolei działania ochronne w zakresie bezpieczeństwa i porządku publicznego ukierunkowane są na zaspokojenie istotnych potrzeb¹⁸. Realizacja zadań w dziedzinie „bezpieczeństwa publicznego” ma zaspokoić takie potrzeby jak np.:

- przetrwanie;
- istnienie;
- niezależność;
- spokój;
- posiadanie.

Termin „porządek publiczny” jest słabszy od terminu „bezpieczeństwo” i oznacza sumę działań o charakterze reglamentacyjnym, które koncentrować się będą na wymuszeniu od obywatela pewnego postępowania. Pojęcie „porządek

¹⁵ Por. A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 9–16; Art. 10 ustawy o samorządzie gminnym i art. 7a ustawy o samorządzie powiatowym oraz art. 8–8b ustawy o samorządzie województwa. Jednocześnie należy podkreślić, iż zrzeszanie się jednostek samorządu terytorialnego zapewnia art. 172 Konstytucji RP oraz art. 10 Europejskiej Karty Samorządu Lokalnego z dnia 15 października 1985 r. (Dz. U. z 1994 r. nr 124, poz. 607, wraz ze sprostowaniem Dz. U. z 2006 r. nr 154, poz. 1107), którą ratyfikowano w Polsce w dniu 26 kwietnia 1993 r. Poza tym należy zaznaczyć, iż z przepisu art. 91 w związku z art. 241 ust. 1 Konstytucji RP wynika, że Europejska Karta Samorządu Lokalnego, będąca umową międzynarodową, stanowi źródło prawa powszechnie obowiązującego w Polsce o mocy ponadustawowej. Zasadnym jest podkreślenie, iż dokument ten uznaje rolę samorządu lokalnego jako instrumentu uczestnictwa obywateli w kierowaniu sprawami publicznymi na podstawie zasad demokracji i decentralizacji władzy, jak również konieczność uznania zasady samorządności lokalnej w ustawodawstwie oraz w miarę możliwości w ustawie zasadniczej. Zatem odnosi się do samorządu lokalnego, przez który w myśl prawa polskiego należy rozumieć samorząd gminny i powiatowy. Do samorządu województwa odnosi się Europejska Karta Samorządu Regionalnego z dnia 5 czerwca 1997 r. przyjęta w ramach Rady Europy.

¹⁶ A. Gołębiowska, *Prawo do wolności i bezpieczeństwa osobistego...*, s. 669–674.

¹⁷ A. Gołębiowska, *Europeanization of administrative law and public administration in Poland*, [w:] *Problemy i uwarunkowania samorządności terytorialnej*, (red.) I. Kłóska, Bielsko-Biała 2015, s. 11–39.

¹⁸ A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 47–51; Odnosi się to do ochrony porządku publicznego i trybu życia zbiorowego ustalonego we wspólnocie przez zaspokojenie i zwalczanie zjawisk przeszkadzających lub utrudniających osiągnięcie celów wspólnoty. Jednocześnie należy podkreślić, iż działania te muszą być ukierunkowane w zakresie ochrony członków wspólnoty przed niebezpieczeństwami wynikającymi z zewnątrz, czyli naturalnymi (żywność, kataklizmy) oraz spowodowanymi przez inne jednostki lub zbiorowości ludzkie. Ponadto należy uwzględnić działania ukierunkowane na ochronę członków wspólnoty przed samymi sobą przez regulowanie uzewnętrzniających się napięć emocjonalnych we wspólnocie, jak również poprzez skuteczną kontrolę dewiacji społecznych oraz działania prewencyjno-informacyjne itp. Dlatego też działania te powinny być ukierunkowane na ochronę dóbr materialnych i intelektualnych, szczególnie przez wymuszanie poszanowania praw własności.

publiczny” oznacza zaś stan przestrzegania ustalonych norm postępowania, zasad współżycia i standardów życia społecznego. Jednocześnie należy zaznaczyć, iż pomiędzy organami administracji rządowej i samorządowej istnieją powiązania wynikające z aktów normatywnych z zakresu ustrojowego i materialnego prawa administracyjnego.

2. Ochrona bezpieczeństwa i porządku publicznego w świetle Konstytucji RP

Konstytucja RP stwierdza istnienie „wspólnot samorządowych”¹⁹ oraz utworzenie „wspólnot” na poziomie gminnym²⁰ i ponadgminnym²¹. Jednostki samorządu terytorialnego mają odrębną od państwa osobowość prawną. Ich funkcjonowanie opiera się na zasadzie samodzielności oraz braku hierarchicznego podporządkowania względem administracji rządowej²². Konstytucja RP podkreśla, iż samorząd terytorialny uczestniczy w sprawowaniu władzy publicznej²³. Z kolei z innego przepisu prawnego wynikają domniemane kompetencje jednostek samorządu terytorialnego²⁴, który wykonuje zadania publiczne niezastreżone przez ustawę zasadniczą oraz ustawy dla organów innych władz publicznych, zwłaszcza administracji rządowej. Preambuła Konstytucji RP zawiera zasadę subsydiarności i zasadę pomocniczości. W przepisach Konstytucji RP przedstawiono pojęcie zadań własnych wykonywanych przez jednostki samo-

¹⁹ Por. Art. 16 ust. 1 Konstytucji RP; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 19–25.

²⁰ Art. 164 ust. 1 Konstytucji RP.

²¹ Art. 164 ust. 2 Konstytucji RP.

²² A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 14–29; Jednocześnie należy podkreślić, iż istotne znaczenie ma zasada samodzielności, która wyraża się w powierzeniu wyłączności w realizowaniu zadań własnych, jak również nadaniu odrębnej struktury organizacyjnej, czy też zapewnieniu samodzielności budżetowo-finansowej oraz ograniczeniu ingerencji władzy centralnej do procedur nadzorczych i zapewnieniu sądowej ochrony praw i interesów podmiotów samorządowych. Wskazana zasada zawarta jest w Konstytucji RP w przepisie art. 165 ust. 2, w którym podkreślono, że samodzielność jednostek samorządu terytorialnego podlega ochronie sądowej, natomiast reguluje ją przepis art. 2 ust. 3 ustawy o samorządzie gminnym, art. 2 ust. 3 ustawy o samorządzie powiatowym oraz art. 6 ust. 3 ustawy o samorządzie województwa; Por. Z. Niewiadomski, *Samorząd terytorialny w Konstytucji RP (komentarz do art. 15. art. 16 oraz art. 163–172)*, „Samorząd Terytorialny” nr 3 (2002), s. 3–30; A. Gołębiowska, *Europeanization of administrative law...*, s. 28–31; A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 49–53; H. Izdebski, *Samorząd terytorialny...*, s. 67–72; A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 8–12.

²³ Art. 16 ust. 2 zd. 1 Konstytucji RP.

²⁴ Por. Art. 164 Konstytucji RP; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 17–24.

rządu terytorialnego²⁵. Zadaniem tymi są działania polegające na zaspokajaniu potrzeb wspólnoty samorządowej²⁶.

Zgodnie z Konstytucją RP Rada Ministrów wykonuje zadania polityki państwa, które nie są zastrzeżone dla innych organów państwowych i samorządu terytorialnego. Rozważania nad tą problematyką doprowadzają do postawienia pytania, a mianowicie, czy z punktu widzenia przepisów konstytucyjnych w zakresie bezpieczeństwa i porządku publicznego można znaleźć miejsce na kompetencje organów administracji samorządowej.

W Konstytucji RP ustrojodawca ustanowił, iż do obowiązków Rzeczypospolitej Polskiej należy zapewnienie bezpieczeństwa obywateli²⁷. Poza tym Konstytucja RP podkreśla, iż do Rady Ministrów należy zapewnienie bezpieczeństwa wewnętrznego państwa i porządku publicznego oraz zapewnienie bezpieczeństwa zewnętrznego państwa, a także ogólne kierowanie w dziedzinie obronności²⁸. W związku z tym, jeśli ust. 4 art. 146 Konstytucji RP ma charakter przykładowego wyliczenia zadań Rady Ministrów, to nie należy traktować tego jako enumeracji dziedzin, które w sposób wyłączny zostały przyporządkowane do realizacji przez rząd i administrację rządową²⁹. Z uwagi na to przepis ten powinien być interpretowany łącznie z ust. 2 art. 146 Konstytucji RP. Uzasadnienie tego twierdzenia należy poprzeć tym, iż zgodnie z jego dyspozycją sprawy polityki państwa należą do Rady Ministrów tylko wtedy, gdy nie są zastrzeżone dla innych organów państwowych albo samorządu terytorialnego. Wobec tego zasadnym jest podkreślenie, że Konstytucja RP, wyznaczając zakres zadań Radzie Ministrów i administracji rządowej, uwzględniła zakres zadań przypisanych jednostkom samorządu terytorialnego³⁰.

²⁵ Art. 166 ust. 1 Konstytucji RP.

²⁶ Por. A. Gołębiowska, *Geneza i formy współdziałania podmiotów samorządowych z podmiotami wyznaniowymi*, [w:] *Współpraca organizacji pozarządowych z samorządem terytorialnym*, (red.) A. Gołębiowska, Powszechne Wydawnictwo Prawnicze, Warszawa 2015, s. 27–40; Warto zwrócić uwagę na uchwałę Trybunału Konstytucyjnego z dnia 27 września 1994 r. (sygn. akt W 10/93, OTK z 1994 r., cz. II, s. 192), w której wskazano, iż wszystkie zadania samorządu terytorialnego mają charakter zadań publicznych. Ponadto podkreślono, że jest to niezależne od tego, czy służą zaspokajaniu zbiorowych potrzeb społeczności lokalnej, czy całego społeczeństwa zorganizowanego w państwo. Poza tym zaspokajanie zbiorowych potrzeb społeczności lokalnej zaliczono do zadań własnych samorządu, a zaspokajanie potrzeb całego społeczeństwa zaliczono do zadań zleconych.

²⁷ Art. 5 Konstytucji RP.

²⁸ Art. 146 ust. 4 pkt 7–8 oraz pkt 11 Konstytucji RP.

²⁹ Por. Art. 146 ust. 4 Konstytucji RP; A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 14–18.

³⁰ Por. A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 18–27; A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 37–42; Jednocześnie należy wyjaśnić, że jednolity charakter państwa w myśl przepisu art. 3 Konstytucji RP i zasady, że: „Rzeczpospolita Polska jest dobrem wspólnym wszystkich obywateli” oznacza, iż samorząd terytorialny nie ma i nie może mieć własnych

3. Ochrona bezpieczeństwa i porządku publicznego przez organy administracji rządowej

Uregulowania związane z działaniem organów administracji rządowej w zakresie zagwarantowania porządku i bezpieczeństwa publicznego zawarte są w ustawach zwykłych. Zaliczyć można do nich m.in. następujące ustawy:

- ustawę z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej³¹;
- ustawę z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych³²;
- ustawę z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej³³;
- ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym³⁴;
- ustawę z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej³⁵.

Konstytucja RP określa podstawy prawne funkcjonowania państwa w okresie wprowadzania stanów nadzwyczajnych na podstawie ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej³⁶. Rada Ministrów wykonuje własne kompetencje. Poza tym współdziała z Prezydentem Rzeczypospolitej Polskiej, jeżeli wystąpi konieczność obrony państwa. Pewne kompetencje w tym zakresie ma również minister obrony na-

suwerennych zadań. Zgodnie z postanowieniem Trybunału Konstytucyjnego z dnia 30 listopada 1999 r. (sygn. akt Ts 104/99, OTK ZU 2000, nr 1, poz. 21), istota samorządu terytorialnego upatrywana jest w tym, że pewne dziedziny spraw, wydzielonych z zakresu władzy państwa, powierza się wspólnotom samorządowym do samodzielnego rozwiązywania. Zadania te są częścią zadań administracji publicznej. Poza tym realizowane są przez organy samorządowe podporządkowane wspólnocie i reprezentujące jej interesy. W związku z tym Konstytucja RP, przyznając samorządowi terytorialnemu kompetencje do uczestniczenia w sprawowaniu władzy publicznej, wskazuje, że uczestniczenie to polega na wykonywaniu zadań publicznych, których przepisy konstytucyjne oraz ustawy ustrojowe nie zastrzegły na rzecz administracji rządowej w myśl art. 163. Poza tym, zgodnie z art. 166 ust. 1 Konstytucji RP, określono wykonywanie zadań polegających na zaspokajaniu zbiorowych potrzeb społeczności lokalnych. Zasadnicze znaczenie ma wykonywanie zadań publicznych zleconych w drodze ustawy, jeżeli wynika to z uzasadnienia potrzeb państwa (art. 166 ust. 2). Wobec tego konsekwencją wykonywania zadań publicznych jest posiadanie władztwa samorządowego, które w istocie jest władztwem publicznym; A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 15–18; A. Gołębiowska, *Geneza i formy współdziałania podmiotów samorządowych...*, s. 29–33.

³¹ Tekst jedn. Dz. U. z 2012 r. nr 461.

³² Dz. U. z 2009 r. nr 62, poz. 504 ze zm.

³³ Tekst jedn. Dz. U. z 2009 r. nr 178, poz. 1380 ze zm.

³⁴ Dz. U. z 2007 r. nr 89, poz. 590 ze zm.

³⁵ Tekst jedn. Dz. U. z 2009 r. nr 12, poz. 68 ze zm.

³⁶ Por. Dz. U. z 2002 r. nr 156, poz. 1301 ze zm.; A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 37–41.

rodowej oraz wojewoda³⁷. W myśl ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym³⁸, działania przywracające konstytucyjny ustrój państwa, bezpieczeństwo obywateli albo porządek publiczny wykonują Prezes Rady Ministrów w sytuacji wprowadzenia stanu wyjątkowego na obszarze większym niż obszar jednego województwa, natomiast na obszarze lub części obszaru jednego województwa właściwy wojewoda. Z kolei zgodnie z ustawą z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej³⁹ organami administracji rządowej działającymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia są wojewoda i właściwy minister. Jednocześnie należy zaznaczyć, iż podczas wykonywania zadań z zakresu porządku i bezpieczeństwa publicznego organy administracji rządowej współpracują ze służbami i strażami⁴⁰.

Istotną kwestią jest zwrócenie uwagi na to, że organy administracji rządowej mogą nałożyć na powiat obowiązek wykonywania określonych czynności w zakresie należącym do zadań powiatu, np. związanych z usuwaniem bezpośrednich zagrożeń dla bezpieczeństwa i porządku publicznego oraz z obronnością. Poza tym należy dodać, że jeżeli działania dotyczące usuwania zagrożeń dla bezpieczeństwa i porządku publicznego, a także związane z obronnością przeprowadza się w ramach zorganizowanej akcji, to nałożenie obowiązku może dotyczyć wykonania czynności także poza terenem powiatu⁴¹. Zasadnym wydaje się zwrócenie uwagi na to, iż w sferze bezpieczeństwa i porządku publicznego ustawodawca przekazał organom administracji rządowej prawo do kierowania organami administracji samorządowej⁴². Ustawodawca posługuje się również zasadą jednoosobowego kierownictwa⁴³, która doprowadza do osiągnięcia dwóch celów. Pierwszym celem jest ponoszenie odpowiedzialności, czyli wyposażenie

³⁷ A. Gołębiowska, *Rozstrzygnięcia nadzorcze i kontrolne wojewody oraz orzecznictwo sądów administracyjnych a stosowanie prawa przez jednostki samorządu terytorialnego*, [w:] *Instytucje kontroli i nadzoru w działaniach organów władzy publicznej w Polsce*, (red.) A. Gołębiowska, M. Woch, P.B. Zientarski, Warszawa 2016, s. 61–83.

³⁸ Por. Dz. U. z 2002 r. nr 113, poz. 985 ze zm.; A. Gołębiowska, *Konstytucja Rzeczypospolitej Polskiej...*, s. 23–27.

³⁹ Dz. U. z 2002 r. nr 62, poz. 558 ze zm.

⁴⁰ Por. A. Gołębiowska, *Geneza i formy współdziałania podmiotów samorządowych...*, s. 34–38; A. Szymonik, *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Warszawa 2011, s. 180–210; A. Gołębiowska, *Europeanization of administrative law...*, s. 17–13.

⁴¹ Art. 7 ustawy o samorządzie powiatowym.

⁴² Por. A. Gołębiowska, *Rozstrzygnięcia nadzorcze i kontrolne wojewody...*, s. 86–91; Warto zwrócić uwagę na rozdział 2 ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, rozdział 2 ustawy o stanie wyjątkowym, rozdział 2 ustawy o stanie klęski żywiołowej, art. 14 ust. 3 ustawy o ochronie przeciwpożarowej oraz art. 20 ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej; A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 39–43.

⁴³ Art. 11 ustawy o stanie klęski żywiołowej oraz art. 14 ustawy o zarządzaniu kryzysowym.

konkretnego organu w określone prawem kompetencje, które ułatwiają rozliczenia organu z realizacji powierzonych zadań. Drugim celem jest osiągnięcie konkretnych rezultatów, a więc usuwanie zagrożeń albo skutków.

Rozważania nad zagadnieniami bezpieczeństwa i porządku publicznego nasuwają pytanie, a mianowicie: co oznacza pojęcie „współdziałanie”? Posłużenie się przez ustawodawcę pojęciem „współdziałanie” obejmuje wiele zadań o różnym charakterze i to władczym oraz niewładczym. Ich celem zaś ma być zapobieganie zagrożeniom i ich usuwanie w sytuacji wystąpienia. Termin „współdziałanie” to współpraca pomiędzy organami administracji rządowej i samorządowej. Niemniej jednak skuteczne współdziałanie powinno być wynikiem podziału kompetencji odpowiadających możliwościom działania organów i ich dostosowanie do danej struktury. Poza tym współdziałanie może polegać na włączaniu organów samorządowych do działań administracji rządowej, jak również łagodzenia podziałów kompetencyjnych. Analiza aktów prawnych doprowadza do wniosku, że zakres kompetencji kierowniczych wykonywanych przez organy administracji rządowej w stosunku do organów administracji samorządowej jest dość szeroki.

Warto zwrócić uwagę na to, że w pojęciu bezpieczeństwa mieści się pojęcie ochrony. Funkcję ochrony realizuje Biuro Ochrony Rządu (BOR), czyli umundurowana i uzbrojona formacja, która wykonuje zadania z zakresu ochrony osób, obiektów i urządzeń⁴⁴. Biuro Ochrony Rządu współpracuje z centralnymi organami administracji rządowej, które podległe są ministrowi właściwemu do spraw wewnętrznych. Ponadto współdziała z jednostkami organizacyjnymi podporządkowanymi, podległymi oraz nadzorowanymi przez ministra właściwego do spraw wewnętrznych lub ministra obrony narodowej oraz innymi organami administracji rządowej i samorządu terytorialnego w zakresie zadań realizowanych przez Biuro Ochrony Rządu i te organy⁴⁵. Centralnymi organami administracji rządowej zajmującymi się sprawami bezpieczeństwa są:

- Agencja Bezpieczeństwa Wewnętrznego;
- Agencja Wywiadu⁴⁶.

Zgodnie z przepisami prawa Agencja Bezpieczeństwa Wewnętrznego zajmuje się ochroną bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego, natomiast Agencja Wywiadu zajmuje się ochroną bezpieczeństwa

⁴⁴ Art. 1 ustawy z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (tekst jedn. Dz. U. z 2004 r. nr 163, poz. 1712 ze zm.).

⁴⁵ Art. 7 ustawy o Biurze Ochrony Rządu.

⁴⁶ Por. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz. U. z 2010 r. nr 29, poz. 154 ze zm.); A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 48–55.

zewnątrznego państwa⁴⁷. Funkcjonariusze tych instytucji mają prawo do żądania niezbędnej pomocy od organów administracji rządowej i samorządu terytorialnego w ramach obowiązujących przepisów prawa⁴⁸.

Poza tym ustawodawca nakłada na organy administracji rządowej obowiązek współdziałania z organami Straży Granicznej⁴⁹, jak również obowiązek zapewnienia im niezbędnych warunków do wykonywania zadań określonych w ustawie⁵⁰. Ponadto Komendant Główny Straży Granicznej współdziała w zakresie realizowanych zadań z właściwymi organami państwowymi oraz jednostkami samorządu terytorialnego⁵¹. Rozważania nad kompetencjami w zakresie porządku i bezpieczeństwa publicznego doprowadzają do wskazania, że skoncentrowane zostały na organach jednoosobowych, co wydaje się słuszne z uwagi na zapewnienie szybkości działania. Poza tym kompetencje te związane są z jednoznacznym przypisaniem odpowiedzialności. Jednocześnie należy zaznaczyć, iż kompetencje w zakresie porządku i bezpieczeństwa publicznego zostały rozproszone na wyspecjalizowane służby, co może powodować trudności w przepływie informacji i jest istotne w sytuacji bezpośredniego zagrożenia i podjęcia natychmiastowych działań. Z pewnością trudności te mogą wynikać z unormowań prawnych i niejasnych procedur, a także rozbudowanej struktury organów działających w sferze porządku i bezpieczeństwa. Z tego względu postuluje się o weryfikację i dostosowanie przepisów do zmieniających się procedur.

4. Ochrona bezpieczeństwa i porządku publicznego przez organy administracji samorządowej

Konstytucja RP określa zakres zadań gminy, która wykonuje zadania samorządu terytorialnego niezastrzeżone dla innych jednostek samorządowych⁵². W związku z tym, jeśli ustawa nie przekáže ich do załatwienia na szczebel powiatowy albo wojewódzki, to wówczas będą załatwiane przez gminy. Usta-

⁴⁷ Por. Art. 1–3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; A. Gołębiowska, *Konstytucja Rzeczypospolitej Polskiej...*, s. 16–20.

⁴⁸ Art. 23 ust. 1 pkt 7 oraz art. 24 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

⁴⁹ Art. 1 ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. nr 116, poz. 675 ze zm.).

⁵⁰ Art. 2 ustawy o Straży Granicznej.

⁵¹ Art. 3a pkt 7 oraz 9c ustawy o Straży Granicznej.

⁵² Por. Art. 164 ust. 3 Konstytucji RP; A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 9–14.

wa o samorządzie gminnym wskazuje⁵³, że do zakresu zadań gminy należą wszystkie sprawy publiczne o znaczeniu lokalnym, które nie są zastrzeżone ustawami na rzecz innych podmiotów⁵⁴. Ponadto podkreślono, iż w sprawach dotyczących realizacji potrzeb danej zbiorowości lokalnej gmina rozstrzyga zawsze wtedy, gdy ustawy nie upoważniają innych organów władzy publicznej⁵⁵. Wskazane kompetencyjne świadczą o woli ustawodawcy nakładającego na gminy odpowiednie działania i odpowiedzialność związaną z zaspakajaniem potrzeb społeczności lokalnej. Wydaje się to właściwe z racji tego, że gminy, jako jednostki „najbliższe” danej społeczności, najbardziej orientują się w jej bieżących sprawach⁵⁶. Z uwagi na to zasadnym jest zwrócenie uwagi na Europejską Kartę Samorządu Terytorialnego⁵⁷, w której podkreślono, że odpowiedzialność za sprawy publiczne powinny ponosić te organy władzy, które znajdują się najbliżej obywateli⁵⁸. Dotyczy to także spraw związanych z ochroną bezpieczeństwa i porządku publicznego, ponieważ zadania własne gmin związane są również z ochroną przeciwpowodziową i przeciwpożarową⁵⁹. Jednocześnie należy zaznaczyć, że jednostki samorządu terytorialnego powinny zapewnić stały monitoring zagrożeń i problemów, które będą rozwiązywane samodzielnie lub we współpracy z innymi jednostkami samorządu terytorialnego albo organami administracji rządowej⁶⁰.

W przepisach ustawy o samorządzie powiatowym wymieniono zadania związane z ochroną bezpieczeństwa i porządku publicznego⁶¹ przeznaczoną dla powiatu⁶². Zgodnie z przepisami ustawowymi powiat jest organem właściwym do tych zadań w sytuacji, gdy dana sprawa posiada charakter ponadgminny. Dotyczy to spraw wykraczających poza bieżące zaspakajanie podstawowych potrzeb wspólnoty terytorialnej⁶³. Chodzi o uzupełnianie się w relacjach pomiędzy gminami a powiatem, który uzupełnia gminy. Z tego

⁵³ Por. Art. 6 ust. 1 ustawy o samorządzie gminnym; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 27–29.

⁵⁴ Por. A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 54–59; *Komentarz do ustawy o samorządzie gminnym*, (red.) P. Chmielnicki, Warszawa 2006, s. 97–100.

⁵⁵ Por. Art. 6 ust. 2 ustawy o samorządzie gminnym; A. Gołębiowska, *Konstytucja Rzeczypospolitej Polskiej...*, s. 19–25.

⁵⁶ A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 52–59.

⁵⁷ A. Gołębiowska, *Prawo do wolności bezpieczeństwa osobistego...*, s. 669–673.

⁵⁸ Art. 4 ust. 3 zd. 2 Europejskiej Karty Samorządu Terytorialnego.

⁵⁹ Art. 7 ust. 1 pkt 14 ustawy o samorządzie gminnym.

⁶⁰ A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 53–55.

⁶¹ Art. 4 ust. 1 pkt 15 ustawy o samorządzie powiatowym.

⁶² A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego...*, s. 61–67.

⁶³ A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 53–56.

względem zadania przechodzą na poziom powiatu w sytuacji, gdy przekroczą zakres terytorialny gminy i będą wymagały zsynchronizowania na poziomie ponadgminnym⁶⁴. W związku z tym zasadnym jest podkreślenie, iż w dziedzinie ochrony bezpieczeństwa i porządku publicznego rola powiatu polega na zapewnieniu koordynacji działań prewencyjnych i reaktywnych. Powiat odpowiedzialny jest za organizację kooperacji gmin i podmiotów administracji rządowej. W związku z tym warto zauważyć rozwiązanie prawne dotyczące koordynacji działań wynikających z powiązania administracji samorządowej (starosta) z systemem powiatowych służb. Dotyczy to spraw związanych z zapewnieniem poczucia braku zagrożenia i spokoju oraz wykluczenia obaw o życie i zdrowie, a także zagwarantowania rozwoju i posiadania. Gminom i powiatom przypisano ochronę mienia przed wandalizmem i kradzieżą oraz likwidację przestępczości i chuligaństwa.

Zgodnie z przepisami ustawy o samorządzie gminnym⁶⁵ oraz ustawy o samorządzie powiatowym⁶⁶ do ich zadań własnych należą ochrona przeciwpożarowa i ochrona przeciwpowodziowa oraz utrzymanie gminnych (powiatowych) magazynów przeciwpowodziowych. Ustawa o ochronie przeciwpożarowej⁶⁷ określa zakres zadań własnych powiatu w sprawach ochrony przeciwpożarowej. Poza tym należy dodać, że ustawa o samorządzie powiatowym wymienia nadzwyczajne zagrożenia dla życia i zdrowia ludzi⁶⁸. Wskazuje na sprawy dotyczące obronności, gdzie zadania wykonywane przez powiat w tym zakresie należą do kompetencji starosty i są przez niego wykonywane, jako zadania zlecone przez administrację rządową⁶⁹.

Przepisy ustawy o samorządzie województwa wskazują na obowiązek opracowania strategii rozwoju województwa⁷⁰. Ponadto zakreślają ramy polityki rozwoju województwa. Obowiązek strategii realizowany jest przez regionalne plany operacyjne i programy wojewódzkie. Ustawa o samorządzie województwa nie wymienia zadań dotyczących ochrony bezpieczeństwa i porządku pu-

⁶⁴ A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego...*, s. 60–63.

⁶⁵ Art. 7 ust. 1 pkt 14 ustawy o samorządzie gminnym.

⁶⁶ Por. Art. 4 ust. 1 pkt 16 ustawy o samorządzie powiatowym; A. Gołębiowska, tamże, s. 59–61.

⁶⁷ Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2002 r. nr 147, poz. 1229 ze zm.).

⁶⁸ Por. Art. 4 ust. 1 pkt 20 ustawy o samorządzie powiatowym; A. Gołębiowska, tamże, s. 63–67.

⁶⁹ Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2004 r. nr 241, poz. 2416 ze zm.). Istotne znaczenie mają m.in. następujące przepisy: art. 2, art. 17 ust. 6 i 7, art. 18 ust. 4 i art. 25 oraz art. 35 ust. 2 i inne; Por. A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 49–59; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 17–19.

⁷⁰ Art. 11 ustawy o samorządzie województwa; Por. A. Gołębiowska, *Rozstrzygnięcia nadzorcze i kontrolne wojewody...*, s. 89–92.

blicznego jako zadań własnych, to z pewnością nie przekreśla, że mogą w tym zakresie powstać różne strategie działania⁷¹. W innych przepisach ustawowych przedstawiono funkcje jednostek samorządu województwa ze wskazaniem na obronność i bezpieczeństwo publiczne⁷². W związku z tym, jeśli ustawodawca nie uwzględnił zadań dotyczących porządku publicznego, to z pewnością można domniemywać, że poza zakresem zainteresowania województwa będą sprawy dotyczące zapewnienia przestrzegania norm codziennego współżycia danej społeczności. Do zakresu zainteresowań województwa należeć będą sprawy dotyczące ochrony życia i zdrowia obywateli przed zagrożeniami militarnymi, terrorystycznymi, a także zwłaszcza niebezpiecznymi, związanymi z przestępczością zorganizowaną.

Wobec tego powstaje pytanie: co należy do kompetencji samorządu województwa? Odpowiadając na postawione pytanie, należy podkreślić, że w dziedzinie obronności i bezpieczeństwa publicznego uprawnienia samorządu województwa są niewielkie. Realizacja tych zadań została wpisana do kompetencji wojewódzkiej administracji rządowej reprezentowanej przez wojewodę⁷³.

Ustawodawca w przepisach zawartych w ustawach samorządowych podkreślił rolę poszczególnych szczebli samorządu w zakresie ochrony bezpieczeństwa i porządku publicznego⁷⁴. Z analizy tych przepisów wynika, iż nie istnieją prawne definicje bezpieczeństwa publicznego i porządku publicznego. Tym samym niemożliwa jest ocena wymienionych zadań. W przepisach ustawowych nie można dopatrzeć się granicy między zadaniami gmin i powiatów w sprawach zapewnienia ochrony bezpieczeństwa i porządku publicznego. Jednocześnie warto zauważyć, iż nie ma szczególnego wskazania, czym miałyby zajmować się powiaty i województwa w zakresie obronności. Przepisy ustaw samorządowych przedstawiają tylko podstawy do ich interpretowania w realizacji zadań z zakresu ochrony bezpieczeństwa i porządku publicznego. Z uwagi na to niejasności pojęć z pewnością mogą utrudniać ich stosowanie przez sądy administracyjne w sytuacji sporów kompetencyjnych. Poza tym mogą budzić wątpliwości w stosowaniu przez organy jednostek samorządu terytorialnego⁷⁵.

⁷¹ A. Gołębiowska, tamże, s. 87–89.

⁷² Por. Art. 14 ust. 1 pkt 13 oraz 14 ustawy o samorządzie województwa; A. Gołębiowska, tamże, s. 90–92.

⁷³ A. Gołębiowska, tamże, s. 72–78.

⁷⁴ A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 16–19.

⁷⁵ A. Gołębiowska, *Rozstrzygnięcia nadzorcze i kontrolne wojewody...*, s. 74–77.

5. Realizacja zadań w zakresie bezpieczeństwa i porządku publicznego

Obszarem rozważań nad jednostkami samorządu terytorialnego są zadania dotyczące zakresu ochrony bezpieczeństwa i porządku publicznego realizowane poprzez kompetencje prawotwórcze oraz kwestie związane z wydawaniem indywidualnych aktów administracyjnych. Jeśli chodzi o rozstrzygnięcia administracyjne, to takim przykładem może być wydanie zakazu dotyczącego zgromadzenia publicznego, gdy zagraża ono bezpieczeństwu i porządkowi publicznemu w myśl ustawy – Prawo o zgromadzeniach⁷⁶, albo cofnięcie pozwolenia na sprzedaż napojów alkoholowych w sytuacji, gdy w miejscu sprzedaży dochodzi do naruszenia porządku publicznego zgodnie z przepisami ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi⁷⁷.

Ustawy samorządowe nie wypowiadają się na temat instrumentów służących do rozwiązywania problemów związanych z ochroną bezpieczeństwa i porządku publicznego. Dlatego też zastosowanie mają ogólne formy działania wspólne dla wszystkich dziedzin podległych właściwości jednostek samorządu terytorialnego. W tym przypadku przykładem może być ustalanie przez gminę kierunków działania wójta w myśl przepisów ustawy o samorządzie gminnym, jak również preliminowanie wydatków w budżecie oraz zawieranie porozumień międzygminnych, czy też rozstrzygnięcie spraw z zakresu ochrony bezpieczeństwa i porządku publicznego w drodze referendum. Tak więc wyjątkiem są tutaj regulacje związane z uchwalaniem przepisów porządkowych. Z kolei dodatkowe instrumenty wynikają z ustaw materialnoprawnych. W związku z tym, iż trudno jest przedstawić wszystkie środki, należy wymienić tylko najbardziej charakterystyczne instrumenty dotyczące rozwiązywania problemów z dziedziny ochrony bezpieczeństwa i porządku publicznego.

Jednocześnie należy wyjaśnić, że realizacja zadań w sferze ochrony bezpieczeństwa i porządku publicznego poprzedzona jest rozpoznawaniem problemów na szczeblu komisji stałych lub doraźnych, szczególnie komisji stałej do spraw bezpieczeństwa i porządku publicznego. Z uwagi na to niezbędne jest współdziałanie z odpowiednimi służbami oraz z organizacjami społecznymi. Ogromne znaczenie ma współpraca samorządu terytorialnego z Policją, bowiem, zgodnie z przepisami ustawy o Policji⁷⁸, komendanci składają roczne sprawozdania ze swojej działalności oraz przedstawiają

⁷⁶ Art. 8 ustawy z dnia 5 lipca 1990 r. – Prawo o zgromadzeniach (Dz. U. nr 51, poz. 297 ze zm.).

⁷⁷ Art. 18 ust. 10 pkt. 3 ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2007 r. nr 70, poz. 473 ze zm.).

⁷⁸ Ustawa z dnia 6 lipca 1990 r. o Policji (Dz. U. z 2007 r. nr 43, poz. 277 ze zm.).

informacje o stanie bezpieczeństwa i porządku publicznego właściwym wojewodom, starostom, wójtom (burmistrzom, prezydentom miast), jak również radom powiatu i gmin⁷⁹. W sytuacji zagrożenia bezpieczeństwa publicznego i zakłócenia porządku publicznego sprawozdanie oraz informację składa się tym organom niezwłocznie na ich żądanie. Z ustawy o Policji wynika, że komendanci powiatowi (miejscy) Policji obowiązani są udostępnić komisji bezpieczeństwa i porządku publicznego na żądanie jej przewodniczącego stosowne dokumenty i informacje związane z pracą Policji na terenie powiatu⁸⁰. Przekazane dane posłużą w przygotowaniu strategii poprawy bezpieczeństwa i porządku publicznego. Ponadto ustawa o Policji wskazuje, iż rady powiatów (miast) i rady gmin mogą w drodze uchwały określić wszelkie zagrożenia bezpieczeństwa i porządku publicznego⁸¹. W związku z tym w tej sytuacji znaczenie mają przepisy znowelizowanej ustawy o samorządzie powiatowym z 2001 r. Nakładają one na radę powiatu obowiązek uchwalenia powiatowego programu zapobiegania przestępczości oraz ochrony bezpieczeństwa obywateli i porządku publicznego⁸².

Dalsze rozważania nad problematyką instrumentów realizacji zadań w sferze ochrony bezpieczeństwa i porządku publicznego doprowadzają do wskazania rozwiązań na poziomie powiatu, które związane są z ochroną przeciwpożarową. Zagadnienie to wyjaśniają przepisy ustawy o Państwowej Straży Pożarnej⁸³. Wskazano w nich, żeby rada powiatu (miasta) przynajmniej raz w roku rozpatrywała informacje komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej o stanie bezpieczeństwa powiatu (miasta) w zakresie ochrony przeciwpożarowej. Z kolei na polecenie starosty taką informację właściwy komendant jest obowiązany przedłożyć w każdym czasie. Rada powiatu (miasta) zaś może określić w drodze uchwały kierunki działań, które zmierzają do usunięcia ewentualnych zagrożeń.

Jednostki samorządu terytorialnego uchwalają akty prawa miejscowego. W Konstytucji RP zaznaczono, że uchwalanie aktów prawa miejscowego jest źródłem prawa powszechnie obowiązującego⁸⁴. W związku z tym ustawa o samorządzie gminnym, o samorządzie powiatowym oraz o samorządzie województwa wyraźnie wskazują na możliwość stanowienia aktów prawa miejscowego. Z uwagi

⁷⁹ Art. 10 ust. 1 ustawy o Policji.

⁸⁰ Art. 10 ust. 5 ustawy o Policji.

⁸¹ Art. 10 ust. 3 ustawy o Policji.

⁸² Nowelizacja ustawy z dnia 11 kwietnia 2001 r. o samorządzie powiatowym (Dz. U. nr 45, poz. 497); Por. A. Gołębiowska, *Konstytucyjne i ustawowe podstawy prawa...*, s. 52–59; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 18–21; A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu terytorialnego...*, s. 66–68.

⁸³ Art. 14 ust. 1 i 2 ustawy z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2006 r. nr 96, poz. 667 ze zm.).

⁸⁴ Por. A. Gołębiowska, *Konstytucyjno-prawne aspekty kompetencji samorządu...*, s. 10–17; A. Gołębiowska, *Istota samorządu terytorialnego...*, s. 21–25.

na to upoważnieniem do wydawania aktów normatywnych w dziedzinie ochrony bezpieczeństwa i porządku publicznego, wynikającym wprost z przepisów ustrojowych ustaw samorządowych, jest upoważnienie do uchwalenia przepisów porządkowych. Jednakże uprawnienia te nie przysługują jednostkom szczebla wojewódzkiego. Nie ulega wątpliwości, iż jest to słuszne z racji niepowierzania im zadań w zakresie porządku publicznego. Rada gminy (powiatu)⁸⁵ może w formie uchwały wydać przepisy porządkowe. Staje się to możliwe w sytuacji, gdy jest to konieczne dla ochrony życia i zdrowia obywateli oraz dla ochrony bezpieczeństwa i porządku publicznego⁸⁶. Przepisy porządkowe są instrumentem do rozwiązywania nagłych sytuacji kryzysowych⁸⁷.

Jednostki samorządu terytorialnego w sytuacjach nagłych mogą skorzystać z interwencji właściwych służb mundurowych. Ustawa o Policji wyraźnie wskazuje na wójta (burmistrza, prezydenta miasta) albo starostę, którzy są uprawnieni do żądania od właściwego komendanta Policji przywrócenia stanu zgodnego z porządkiem, podjęcia działań zapobiegających naruszeniu prawa oraz zmierzających do usunięcia zagrożenia bezpieczeństwa i porządku publicznego⁸⁸. Wskazane uprawnienie nie może być związane z czynnościami operacyjno-rozpoznawczymi, dochodzeniowo-śledczymi oraz czynnościami dotyczącymi ścigania wykroczeń. Jednocześnie warto zaznaczyć, iż żądanie to nie może dotyczyć wykonania konkretnych czynności służbowych i określać sposobu wykonania zadania. W przepisach ustawy o Państwowej Straży Pożarnej podkreślono, że w sytuacji bezpośredniego zagrożenia bezpieczeństwa wspólnoty samorządowej, czyli życia lub zdrowia, wójt (burmistrz, prezydent miasta) albo starosta może

⁸⁵ Por. A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego...*, s. 64–68; Naczelny Sąd Administracyjny w wyroku z dnia 19 czerwca 1991 r. (sygn. akt SA/Ka362/91, POP 1993, nr 2, s. 39) stwierdził, że gminne przepisy porządkowe niezbędne dla ochrony życia i zdrowia obywateli oraz zapewnienia porządku, spokoju i bezpieczeństwa publicznego można wydawać dopiero po stwierdzeniu, że w odrębnych ustawach lub innych przepisach powszechnie obowiązujących nie ma już takiej regulacji prawnej; Por. A. Gołębiowska, *Rozstrzyganie sporów kompetencyjnych przez Naczelny Sąd Administracyjny*, [w:] *Efektywność działania administracji publicznej w Polsce*, s. 36–41.

⁸⁶ Art. 40 ust. 3 ustawy o samorządzie gminnym oraz art. 41 ust. 1 ustawy o samorządzie powiatowym.

⁸⁷ Por. art. 40 ust. 4 ustawy o samorządzie gminnym i art. 41 ust. 2 ustawy o samorządzie powiatowym. Kontrola przepisów jednostek samorządu terytorialnego z racji legalności dokonywana jest przez wojewodę. Przepisy ustaw o samorządzie gminnym i o samorządzie powiatowym przewidują skrócony termin na przedstawienie przepisów porządkowych wojewodzie; A. Gołębiowska, *Rozstrzygnięcia nadzorcze i kontrolne wojewody...*, s. 89–91; A. Gołębiowska, *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego...*, s. 67–71.

⁸⁸ Art. 11 ustawy o Policji.

wydać komendantowi powiatowemu (miejskiemu) Państwowej Straży Pożarnej polecenie podjęcia działań, które zmierzają do usunięcia zagrożenia⁸⁹.

W sferze bezpieczeństwa i porządku publicznego istotne znaczenie ma straż gminna. Zgodnie z przepisami ustawy o strażach gminnych⁹⁰ jest ona powoływana odpowiednią uchwałą rady gminy (miasta), po uprzednim zasięgnięciu opinii właściwego komendanta wojewódzkiego Policji. Powoływanie straży gminnej należy do podstawowych kompetencji organizacyjno-kreacyjnych gminy. W sytuacji, gdy samorząd powiatowy albo wojewódzki nie mają możliwości powoływania straży, to wówczas zgodnie z ustawą⁹¹ jest ona jednostką organizacyjną gminy, którą kieruje komendant powoływany i odwoływany przez wójta (burmistrza, prezydenta miasta)⁹².

6. Podsumowanie

Przedstawione rozważania dotyczą roli organów administracji rządowej i samorządowej w sferze ochrony bezpieczeństwa i porządku publicznego. Celem analizy problematyki ochrony bezpieczeństwa i porządku publicznego było przedstawienie zakresu obowiązków administracji rządowej i samorządowej. Konstytucja RP oraz przepisy ustawowe potwierdzają podział obowiązków pomiędzy poszczególnymi szczeblami samorządu i wymieniają je precyzyjnie. Rozważania nad problematyką ochrony bezpieczeństwa i porządku publicznego pozwalają stwierdzić, że organy administracji rządowej i samorządowej posiadają instrumenty prawne do działania w tym zakresie. Zarówno przepisy konstytucyjne, jak i ustawowe, gwarantują elastyczność systemu zaspokajania potrzeb społeczeństwa w zakresie ochrony bezpieczeństwa i porządku publicznego. Statuuje także konkretne środki kooperacji zachodzące pomiędzy administracją rządową a samorządową.

Bibliografia

Akty prawne:

Europejska Karta Samorządu Lokalnego z dnia 15 października 1985 r. (Dz. U. z 1994 r. nr 124, poz. 607 wraz ze sprostowaniem Dz. U. z 2006 r. nr 154, poz. 1107).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. nr 89, poz. 555 ze zm.).

Ustawa z dnia 11 kwietnia 2001 r. o samorządzie powiatowym (Dz. U. nr 45, poz. 497).

⁸⁹ Art. 14 ust. 3–8 ustawy o Państwowej Straży Pożarnej.

⁹⁰ Art. 2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. nr 123, poz. 779 ze zm.).

⁹¹ Art. 6 ustawy o strażach gminnych.

⁹² Zgodnie z art. 9 ustawy o strażach gminnych nadzór sprawuje Komendant Główny Policji za pośrednictwem właściwego terytorialnie komendanta wojewódzkiego Policji.

Ustawa z dnia 21 listopada 1997 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2004 r. nr 241, poz. 2416 ze zm.).

Ustawa z dnia 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz. U. z 1998 r. nr 96, poz. 603 ze zm.).

Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2002 r. nr 147, poz. 1229 ze zm.).

Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2006 r. nr 96, poz. 667 ze zm.).

Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2007 r. nr 70, poz. 473 ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. nr 123, poz. 779 ze zm.).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. nr 142, poz. 1592 ze zm.).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2001 r. nr 142, poz. 1590 ze zm.).

Ustawa z dnia 5 lipca 1990 r. – Prawo o zgromadzeniach (Dz. U. nr 51, poz. 297 ze zm.).

Ustawa z dnia 6 lipca 1990 r. o Policji (Dz. U. z 2007 r. nr 43, poz. 277 ze zm.).

Ustawa z dnia 8 marca 1990 r. o samorządzie terytorialnym (tekst pierwotny: Dz. U. z 2001 r. nr 142, poz. 1591; obecnie ustawa o samorządzie gminnym).

Orzecznictwo:

Postanowienie Trybunału Konstytucyjnego z dnia 30 listopada 1999 r. (sygn. akt Ts 104/99, OTK ZU 2000, nr 1, poz. 21).

Uchwała Trybunału Konstytucyjnego z dnia 27 września 1994 r. (sygn. akt W 10/93, OTK 1994, nr 2, poz. 46).

Wyrok Naczelnego Sądu Administracyjnego z dnia 19 listopada 1991 r. (sygn. akt SA/a362/91, POP 1993, nr 2, s. 39).

Literatura:

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.

Bukowski Z., Jędrzejewski T., Rączka P., *Ustrój samorządu terytorialnego*, Toruń 2005.

Chmielnicki P. (red.), *Komentarz do ustawy o samorządzie gminnym*, Warszawa 2006.

Gołębiowska A., *Decentralizacja administracji publicznej na przykładzie samorządu gminnego. Zarys problematyki*, „Opere et Studio pro Oeconomia” No 6, Warszawa 2009, s. 63–87.

Gołębiowska A., *Europeanization of administrative law and public administration in Poland*, [w:] *Problemy i uwarunkowania samorządności terytorialnej*, (red.) I. Kłóska, Bielsko-Biała 2015, s. 11–39.

Gołębiowska A., *Geneza i formy współdziałania podmiotów samorządowych z podmiotami wyznaniowymi*, [w:] *Współpraca organizacji pozarządowych z samorządem terytorialnym*, (red.) A. Gołębiowska, Powszechne Wydawnictwo Prawnicze, Warszawa 2015, s. 27–40.

Gołębiowska A., *Geneza oraz konstytucyjno-prawne aspekty samorządu powiatowego i jego koncepcje prawno-organizacyjne*, [w:] *Rzeczpospolita w koncepcjach transformacji ustrojowej 1989 r.*, (red.) A. Gołębiowska, Powszechne Wydawnictwo Prawnicze, Warszawa 2015, s. 59–80.

- Gołębiowska A., *Istota samorządu terytorialnego w świetle postanowień Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, [w:] *Administracja publiczna – uwarunkowania prawne, organizacyjne i społeczne*, (red.) A. Gołębiowska, Powszechnie Wydawnictwo Prawnicze, Warszawa 2015, s. 15–32.
- Gołębiowska A., *Konstytucja Rzeczypospolitej Polskiej a samorząd terytorialny*, [w:] *Funkcjonowanie samorządu terytorialnego – uwarunkowania prawne i społeczne*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 13–32.
- Gołębiowska A., *Konstytucyjne i ustawowe podstawy prawa obywatela do informacji o działalności organów samorządu terytorialnego*, [w:] *Funkcjonowanie samorządu terytorialnego – uwarunkowania prawne i społeczne*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 37–62.
- Gołębiowska A., *Konstytucyjno-prawne aspekty kompetencji samorządu terytorialnego w zakresie bezpieczeństwa i porządku publicznego*, [w:] *Zrównoważony rozwój gospodarczy jednostek samorządu terytorialnego*, (red.) E. Sobczak, Warszawa 2015, s. 7–29.
- Gołębiowska A., *Prawo do dobrej administracji jako prawo podstawowe o randze konstytucyjnej*, [w:] *Efektywność działania administracji publicznej w Polsce*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 11–29.
- Gołębiowska A., *Prawo do wolności i bezpieczeństwa osobistego w prawie międzynarodowym oraz Konstytucji Rzeczypospolitej Polskiej*, [w:] *Paradygmaty badań nad bezpieczeństwem. Jednostki, grupy i społeczeństwa*, (red.) M. Kopczeński, A. Kurkowska, S. Mikołajczak, Poznań 2015, s. 643–674.
- Gołębiowska A., *Prawo miejscowe samorządu terytorialnego w okresie drugiej Rzeczypospolitej*, „Cogitatus” nr 7, Wydawnictwo Collegium Varsoviense, Warszawa 2009, s. 53–68.
- Gołębiowska A., *Rozstrzyganie sporów kompetencyjnych przez Naczelny Sąd Administracyjny*, [w:] *Efektywność działania administracji publicznej w Polsce*, (red.) A. Gołębiowska, P.B. Zientarski, Kancelaria Senatu, Warszawa 2016, s. 31–48.
- Gołębiowska A., *Rozstrzygnięcia nadzorcze i kontrolne wojewody oraz orzecznictwo sądów administracyjnych a stosowanie prawa przez jednostki samorządu terytorialnego*, [w:] *Instytucje kontroli i nadzoru w działaniach organów władzy publicznej w Polsce*, (red.) A. Gołębiowska, M. Woch, P.B. Zientarski, Warszawa 2016, s. 61–93.
- Izdebski H., *Samorząd terytorialny. Podstawy ustroju i działalności*, Warszawa 2006.
- Izdebski H., Kulesza M., *Administracja publiczna. Zagadnienia ogólne*, Warszawa 2004.
- Niewiadomski Z., *Samorząd terytorialny w Konstytucji RP (komentarz do art. 15, art. 16 oraz art. 163–172)*, „Samorząd Terytorialny” nr 3 (2002), s. 3–30.
- Stec M., *Podział zadań i kompetencji w nowym ustroju terytorialnym Polski (kryteria i normatywna realizacja)*, „Samorząd Terytorialny” nr 11 (1998).
- Szczechowicz H., *Samorząd terytorialny w społeczeństwie obywatelskim*, [w:] *Samorząd terytorialny na przełomie XX/XXI wieku*, (red.) A. Lutrzynowski, R. Gawłowski, M. Póławski, Toruń 2010.
- Szymonik A., *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Warszawa 2011, s. 180–210.
- Zimmermann J., *Prawo administracyjne*, Warszawa 2006.

Streszczenie

Organy administracji rządowej i samorządowej mają obowiązek zapewnić porządek i bezpieczeństwo publiczne. Związane jest to z wykonywaniem odpowiednich i przeznaczonych tym organom specjalnych kompetencji. Organy te, działając, wykorzystują kompetencje kontrolne, nadzorcze i koordynacyjne. Realizują zadania publiczne w ramach współdziałania.

Słowa kluczowe: bezpieczeństwo, porządek publiczny, administracja samorządowa, administracja publiczna.

Summary

Organ of government administration and local government in the sphere of security and public order

The state administration bodies and local authorities have a duty to ensure public order and safety. This is connected with the exercise of appropriate and designated the bodies of special competence. Those authorities acting utilize powers of control, supervision and coordination. They carry out public functions in the framework of cooperation.

Key words: safety, public order, local government, public administration.

Rozdział II.

Organizacja i zarządzanie bezpieczeństwem w przyszłości

1. Wprowadzenie

Zagadnienia związane z bezpieczeństwem państwa, bezpieczeństwem obywateli są przedmiotem zainteresowania wielu dyscyplin naukowych. Są i powinny być przedmiotem badań także nauk o zarządzaniu. Szczególnym przedmiotem zainteresowania nauk o zarządzaniu są organizacje przyszłości oraz zarządzanie nimi. Literatura przedmiotu wskazuje na pewne pożądane cechy organizacji przyszłości. Są to m.in.: szybkie reagowanie na zmiany w otoczeniu (jak kameleon), spłaszczanie struktur organizacyjnych, inwestowanie w ludzi i ich kompetencje, orientowanie na cele, tworzenie zespołów zadaniowo-wirtualnych. Nowoczesne organizacje cenią doświadczonych pracowników. Dążą do coraz wyższej sprawności, jakości, innowacyjności działań.

Czy takimi cechami powinny charakteryzować się organizacje przyszłości funkcjonujące na rzecz bezpieczeństwa?

2. Bezpieczeństwo jako przedmiot zarządzania

W badaniach, publikacjach, opiniach społecznych wyraźnie odczuwa się brak kompleksowego spojrzenia na bezpieczeństwo państwa jako na zbiór obejmujący w sposób wieloaspektowy co najmniej takie elementy jak: terytorium, obywatele,

władze, struktury karne, relacje międzynarodowe – czyli to wszystko, co stanowi podstawę do funkcjonowania suwerennego państwa.

Wychodząc od podstawowych elementów państwa, można uznać, że państwo jest bezpieczne tylko wtedy, gdy będą spełnione łącznie następujące warunki:

- nie będzie zagrożone jego terytorium;
- ludzie (obywatele, mieszkańcy tego terytorium, a także przybysze czasowi) będą czyli się bezpiecznie (wszędzie tam, gdzie przebywają, będzie zapewniony ich byt i rozwój, będą zabezpieczone ich prawa i wolności);
- władze będą funkcjonowały suwerennie – zgodnie z obowiązującym porządkiem konstytucyjnym;
- będzie funkcjonował spójny, sprawiedliwy system karny obejmujący wszystkich obywateli;
- będą poprawne relacje międzynarodowe w układzie bilateralnym i multilateralnym.

Wynika z tego, że tych pięć elementów łącznie – ludność, terytorium, władza, system karny, relacje międzynarodowe – powinno być przedmiotem szczególnej ochrony państwa, jednocześnie punktem wyjścia przy poszukiwaniu konceptualnych, przyszłościowych modeli bezpieczeństwa państwa¹. Słuszność takiego podejścia potwierdza między innymi art. 5 Konstytucji RP, w którym stwierdza się „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju”.

Państwo powinno spełniać służebną rolę przede wszystkim wobec swoich obywateli (swojego narodu). We współczesnym ujęciu bezpieczeństwo narodowe to oczekiwanie społeczne zapewnienia możliwości korzystania z dobrobytu ekonomicznego, autonomii społecznej oraz określonego statusu politycznego. Wartość, jaką jest fizyczne przetrwanie, widziana jest przez pryzmat zwiększania pewności.

Zdaniem Z. Traczyka, problematyka bezpieczeństwa obejmuje bardzo szeroki obszar dziedzin życia – od losowych czynników fizykochemicznych poczynając (obejmujących zagrożenia klimatyczne, tektoniczne, pożarowe), poprzez zagrożenia biologiczno-egzystencjalne właściwe dla przetrwania w świecie organizmów

¹ Tak definiowane jest państwo w prawie międzynarodowym publicznym. Zob. art. 1 Konwencji przyjętej w Montevideo w 1933 r.; Por. R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa, PWN, 1994, s. 113–114; W. Góralczyk, *Prawo międzynarodowe publiczne w zarysie*, Warszawa, PWN, 1983, s. 117–118.

żywych (zapewnienie żywności, energii technicznej, zdrowotności), a na czynnikach wynikających z wzajemnej inwazyjności ludzi w życiu społecznym kończąc².

Jak zauważa J. Świniarski, we współczesnych skłonnościach do pluralistycznego pojmowania bezpieczeństwa i jego polisemantycznego definiowania często wskazywanymi różnicami gatunkowymi bezpieczeństwa bywają: niezawodność (nauki techniczne i technologiczne), stabilność i pewność istnienia (nauki społeczno-humanistyczne) oraz trwanie i istnienie (nauki przyrodnicze); albo wolność, spokój i komfort oraz „niczym niezakłócone współistnienie człowieka z innymi ludźmi i środowiskiem przyrodniczym”, tudzież zdrowie, mienie i dobre samopoczucie oraz pewność jutra itp.³

W ujęciu aksjologicznym bezpieczeństwo można zdefiniować jako czynienie rzeczy tak, aby zapewnić: przetrwanie i rozwój przez prokreację oraz edukację, przetrwanie i rozwój przez dostatek oraz dobrobyt, sprawiedliwość i rozwój przez właściwe prawo (praworządność) oraz zorganizowanie życia społecznego (aktywny udział w tym życiu), doskonalenie i wzrost jakości poszanowania wolności oraz odpowiedzialność za siebie, innych i przyrodę (tabela 1).

Tabela 1. Filary, wymiary i atrybuty holistycznie ujmowanego bezpieczeństwa

Filary szeroko pojętego bezpieczeństwa	Wymiary szeroko pojętego bezpieczeństwa	Atrybuty szeroko pojętego bezpieczeństwa
Prokreacja i edukacja	Demograficzny	Przetrwanie, rozwój
Dostatek i dobrobyt	Ekonomiczny	Przetrwanie, rozwój
Prawo i ustrój	Polityczno-społeczny	Sprawiedliwość, rozwój
Wolność i odpowiedzialność	Kulturowo-cywilizacyjny	Doskonalenie, jakość

Źródło: na podstawie J. Świniarski, *Bezpieczeństwo w ujęciu aksjologicznym*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, WSZiP, Warszawa 2008, s. 76 (tabela zmodyfikowana przez autora)

Zdaniem J. Świniarskiego, zarządzanie bezpieczeństwem w czasach globalizacji i dominacji liberalnej demokracji w perspektywie aksjologicznej powinno polegać na trosce o przetrwanie, trwanie, rozwój i doskonalenie rodzaju ludzkiego.

W społeczeństwach najwyżej rozwiniętych, dostrzegając wielość zagrożeń, największą wagę przywiązuje się do bezpieczeństwa ekologicznego i zdrowotnego.

² Z. Traczyk, *Sektor obywatelski i inne obszary bezpieczeństwa*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, WSZiP, Warszawa 2008, s. 293.

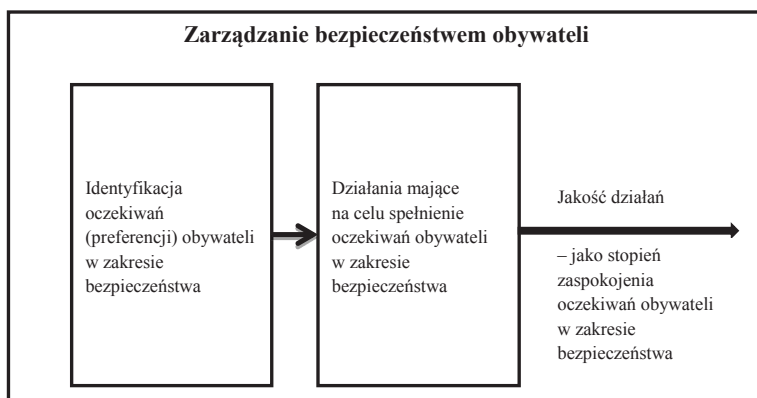
³ J. Świniarski, *Bezpieczeństwo w ujęciu aksjologicznym*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, s. 62–63.

go, bezpieczeństwa ekonomiczno-gospodarczego i socjalnego, bezpieczeństwa politycznego, ochrony wolności i praw obywateli. Jak zauważa M. Cieślarczyk, w społeczeństwach najwyżej rozwiniętych, dostrzegając wielość zagrożeń, największą wagę przywiązuje się do bezpieczeństwa ekologicznego i zdrowotnego, bezpieczeństwa ekonomiczno-gospodarczego i socjalnego, bezpieczeństwa politycznego, ochrony wolności i praw obywateli.

Podsumowując różne poglądy na temat pojęcia zarządzania bezpieczeństwem, można stwierdzić, że jego celem jest przede wszystkim zapewnienie godnego bytu, możliwości rozwoju, zapewnienie swobód obywatelskich. Przy czym to zapewnienie nie może mieć tylko charakteru doraźnego – musi mieć charakter ciągły, odporny na zakłócenia i dotyczyć przede wszystkim przyszłości. Szczególnej ochronie powinny podlegać systemy, w tym infrastruktura krytyczna, funkcjonujące na rzecz realizacji tych celów.

Zarządzanie bezpieczeństwem obywateli obejmuje dwa podstawowe elementy: identyfikację oczekiwań (preferencji) obywateli w zakresie bezpieczeństwa oraz organizowanie działań mających na celu spełnienie tych oczekiwań. Mówiąc o organizowaniu działań, trzeba mieć na myśli ich planowanie (strategiczne, operacyjne), tworzenie odpowiednich struktur organizacyjnych, zapewnienie właściwych ludzi we właściwym miejscu i czasie, umiejętne przewodzenie ludźmi poprzez odpowiedni system motywowania do pracy, dobór stylów kierowania, kontrolowanie (zarówno klasyczne, jak i współczesne oparte na idei kontrolingu menedżerskiego). O jakości działań świadczy stopień zaspokojenia oczekiwań obywateli w zakresie bezpieczeństwa (rys. 1).

Rys. 1. Zarządzanie bezpieczeństwem obywateli



Źródło: Opracowanie własne

Obok jakości, należy także oceniać działania z punktu widzenia ich sprawności oraz innowacyjności. Współcześnie sprawność działań na rzecz bezpieczeństwa obywateli to trafne, wynikające z rzeczywistych potrzeb, formułowanie celów działania (strategicznych i wynikających z nich operacyjnych), ich realizacja i jednocześnie racjonalne wykorzystywanie zawsze ograniczonych zasobów (ludzkich, rzeczowych, finansowych, informacyjnych). Wykorzystywanie nadmiernych zasobów do realizacji konkretnych działań skutkuje niemożnością realizacji innych działań w tym samym czasie, powoduje więc bezpowrotne straty. Zaś innowacyjność działań pozwala nam nadążać za zmianami, za najnowszymi wyzwaniem w zakresie bezpieczeństwa. Przy czym zmiany te powinny dotyczyć zarówno działań w aspekcie czynnościowym (procesowym), jak i rzeczowym (zasobowym).

3. Oczekiwania obywateli w zakresie bezpieczeństwa

W dokumentach Wspólnoty Europejskiej stwierdza się, że bezpieczeństwo Europy jest koniecznym warunkiem dobrobytu i wolności. Europejska Strategia Bezpieczeństwa przyjęta przez Radę Europejską obejmuje dwa obszary – bezpieczeństwa cywilnego oraz obronny (militarny).

Jako szczególnie ważne obszary dla bezpieczeństwa Europy wymienia się:

- Ochronę przed terroryzmem i przestępczością – dostarczanie rozwiązań technologicznych w celu rozpoznawania zagrożeń, wykrywanie, zapobieganie, identyfikację, ochronę, neutralizowanie i powstrzymywanie skutków ataków terrorystycznych i przestępczości;
- Bezpieczeństwo infrastruktury i obiektów użyteczności publicznej – analizę i zabezpieczanie istniejącej i przyszłej publicznej oraz prywatnej infrastruktury o decydującym znaczeniu;
- Bezpieczeństwo granic – skupianie się na technologiach i zdolnościach mających na celu wzmocnienie sprawności wszystkich systemów, wyposażenia, narzędzi i procesów koniecznych do poprawy bezpieczeństwa europejskich granic lądowych i morskich, łącznie z kwestiami kontroli i obserwacji granic;
- Przywracanie bezpieczeństwa w stanie kryzysu – skupianie się na technologiach wspierających różne operacje zarządzania w sytuacjach kryzysowych (takie jak ochrona ludności, zadania ratownicze i akcje humanitarne, wspieranie wspólnej polityki zagranicznej i bezpieczeństwa) oraz na kwestiach takich, jak koordynacja i komunikacja między organizacjami, rozproszona architektura i czynnik ludzki⁴.

⁴ M. Lisiecki, *Jakość w zarządzaniu bezpieczeństwem obywateli*, KUL, Lublin 2009, s. 6–7.

Analizując przedstawione wyżej obszary zagrożeń, można stwierdzić, że nie obejmują one wszystkich istotnych elementów składających się na system bezpieczeństwa państwa, obejmują one jedynie wybrane obszary, choć bardzo istotne obecnie, jak i w przyszłości.

Według opinii społeczności lokalnych – bezpieczeństwo rozumiane jest jako:

- stan świadomości człowieka, w którym czuje się on wolny od jakichkolwiek zagrożeń, pociągający za sobą uczucie spokoju i komfortu;
- życie bez zagrożenia, niczym niezakłócone współistnienie człowieka z innymi ludźmi i środowiskiem przyrodniczym;
- stan bez lęku i niepokoju o siebie i innych;
- pewność jutra;
- brak zagrożenia utraty zdrowia, mienia i życia; pełny komfort psychiczny umożliwiający realizację życiowych marzeń i celów;
- sytuację, w której człowiekowi nic nie zagraża, a w nagłych, nieprzewidywanych sytuacjach może liczyć na pomoc i wsparcie innych;
- określone czynniki i działania powołanych do tego instytucji, które gwarantują przeciętnemu obywatelowi dobre samopoczucie i pewność jutra⁵.

Z racji funkcjonowania Polski w strukturze Unii Europejskiej warto przedstawić opinie Europejczyków na temat zagrożeń dla ich bezpieczeństwa, a na ich tle hierarchię zagrożeń dla społeczności lokalnej w Polsce. Zbiór zagrożeń z lat 2012–2015, z uwzględnieniem ich wagi w Europie i Polsce, przedstawiono w tabeli 2.

Tabela 2. Zbiór zagrożeń dla bezpieczeństwa obywateli Unii Europejskiej i Polski z uwzględnieniem ich wagi (wiosna 2012–2015 r.)

Lp.	Zagrożenia	Waga zagrożeń w UE (w procentach)				Waga zagrożeń w Polsce (w procentach)
		2012	2013	2014	2015	2015
1	Wzrost cen/inflacja/ koszty utrzymania	45	41	32	27	26
2	Bezrobocie	21	22	21	16	19

⁵ Zob. B. Kwiatkowska, *Problemy bezpieczeństwa w samorządowej kampanii wyborczej*, „Zeszyty Naukowe SGSP” nr 22 (1999); M. Lisiecki, B. Kwiatkowska-Basała, *Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia*, [w:] *Zarządzanie bezpieczeństwem*, (red.) P. Tyrała, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, s. 53–60.

3	Sytuacja gospodarcza w kraju	19	18	15	10	8
4	Podatki	14	16	17	14	10
5	Sytuacja finansowa gospodarstwa domowego	15	16	16	15	15
6	Zdrowie i opieka społeczna	15	15	15	16	19
7	Emerytura/renta	14	14	15	15	18
8	System oświaty (edukacji)	10	9	10	11	4
9	Klimat, środowisko, energetyka	5	5	7	5	2
10	Przestępczość	5	6	5	5	3
11	Warunki mieszkaniowe	5	5	6	6	4
12	Imigracja	3	3	4	6	3
13	Terroryzm	1	1	1	2	2
14	Warunki pracy	-	-	-	9	11
15	Warunki życia	-	-	-	8	16

Źródło: Standard Eurobarometer 83, Spring 2015, Public Opinion in the European Union, Report, s. 27–29

Przedstawiony zbiór zagrożeń, z określoną ich wagą dla ludzi, wskazuje, że w dzisiejszych i przyszłych czasach najważniejsze zagrożenia mają i będą miały charakter społeczno-ekonomiczny. Mają one podobny rozkład w Europie i Polsce. Największe obawy dotyczą: wzrostu cen, inflacji, kosztów utrzymania, bezrobocia, zdrowia i opieki społecznej, emerytur, rent, warunków życia, sytuacji finansowej gospodarstw domowych. Tradycyjne zagrożenia (militarne, przestępczość, pożary itd.) nie są najważniejsze dla społeczności lokalnych.

Analizując wyniki badań cyklicznie powtarzanych przez różne ośrodki, można zauważyć, że tendencje w zakresie odczuwanych przez obywateli zagrożeń w ostatnich 10–20 lat są podobne (pomimo wystąpienia kryzysu gospodarczego, zwiększonych w ostatnim okresie zagrożeń migracyjnych, terrorystycznych)⁶.

⁶ Zob. M. Lisiecki, *Jakość w zarządzaniu bezpieczeństwem...*, s. 119–126.

4. Działania na rzecz bezpieczeństwa obywateli w przyszłości

Wielość zagrożeń i wynikających z nich potrzeb obywateli wymusza konstruowanie właściwej strategii działania, projektów nowych rozwiązań organizacyjnych, doskonalenie istniejących już rozwiązań, projektowanie i doskonalenie zarządzania. Jak sugeruje P. Drucker, zarządzanie organizacjami w XXI wieku powinno przede wszystkim opierać się na odpowiednim współdziałaniu pomiędzy organizacjami, częściami organizacji, ludźmi (pracownikami) oraz wykorzystywaniu w jak najwyższym stopniu potencjału, możliwości najważniejszego i najcenniejszego zasobu każdej organizacji, jakim są ludzie⁷. Dotyczy to także zarządzania bezpieczeństwem.

Najważniejszymi podmiotami z punktu widzenia bezpieczeństwa państwa, obywateli są:

- organy władzy ustawodawczej (Sejm, Senat);
- wykonawczej (prezydent, administracja rządowa, samorządowa);
- sądy i trybunały;
- podmioty gospodarcze;
- obywatele.

Od stopnia ich współdziałania będzie zależała jakość, sprawność, innowacyjność działań, która powinna mieć wymiar rzeczywisty – a nie pozorny (papierowy) w postaci niedopracowanych aktów normatywnych. To nie ustawy – lecz konkretni ludzie są w stanie zapewnić wysoki poziom bezpieczeństwa obywateli. Oczywiście formalizacja działań jest potrzebna, lecz jako końcowy element dyskusji nad możliwymi rozwiązaniami, które jak wspomniano wcześniej muszą zapewnić wysoką jakość, sprawność i innowacyjność działań ukierunkowaną na zmieniające się potrzeby obywateli.

Poziom sprawności, jakości, innowacyjności zarządzania bezpieczeństwem obywateli w przyszłości będzie zależał od:

- trafności doboru źródeł informacji oraz metod i technik identyfikowania i prognozowania zagrożeń;
- sposobów komunikowania z podstawowymi odbiorcami usług na rzecz bezpieczeństwa, czyli obywatelami, w zakresie informowania o potencjalnych przyszłych zagrożeniach oraz wsłuchiwanie się w ich rzeczywiste potrzeby w tym zakresie. Komunikowanie z podstawowym odbiorcą usług w zakresie bezpieczeństwa jest też istotne z tego powodu, że to opinia obywateli decyduje o rzeczywistej ocenie organizacji funkcjonujących na

⁷ P. Drucker, *Management and world's*, "Harvard Business Review", September-October 1988, s. 65–76.

rzecz bezpieczeństwa. Opinia ta powinna wpływać na koncepcje i wynikające z nich projekty przyszłych działań, a także na bieżące korekty w tym zakresie. To podatnicy powinni określać, czego chcą;

- organizacji działań, które mogą mieć różną postać. Coraz wyższy poziom wykształcenia najważniejszego zasobu każdej organizacji, jakim są ludzie, wzbogacony dodatkowo praktycznym doświadczeniem, pozwala na coraz większą decentralizację struktur organizacyjnych. Oczywiście konieczne jest zachowanie pomocniczości państwa – w sprawach niemożliwych do załatwienia na niższych szczeblach we własnym zakresie. Wynikający z bardzo szybkiego postępu technologicznego coraz wyższy poziom instrumentalizacji działań powinien ułatwiać współdziałanie wielu podmiotów. W zbiorze działań na rzecz bezpieczeństwa powinny dominować działania prewencyjne. Bardziej powinien nas cieszyć brak zdarzeń niż duża liczba zdarzeń zakończonych doraźnym sukcesem (zatrzymaniem i osądzeniem sprawcy czynu zabronionego, ugaszeniem pożaru itd.).

Wielość zagrożeń potwierdza potrzebę integracji działań na różnych poziomach: gminnym, powiatowym, wojewódzkim, państwowym, międzynarodowym. Te funkcje integracyjne powinni pełnić, idąc od dołu, od obywatela, przede wszystkim wójt, burmistrz, prezydent miasta, starosta – wszyscy z dużymi uprawnieniami w zakresie określania celów strategicznych i operacyjnych, finansowania działań, określania struktur organizacyjnych, zarządzania zasobami ludzkimi.

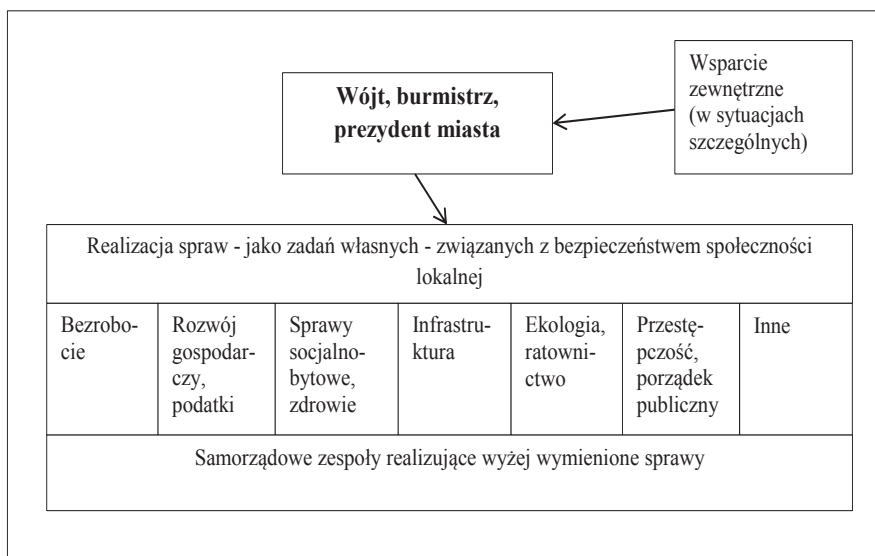
Obecnie trudno powiedzieć, kto na szczeblu gminnym, powiatowym, a nawet wojewódzkim odpowiada za bezpieczeństwo obywateli. Zgodnie z zapisami ustaw dotyczących funkcjonowania administracji publicznej – odpowiadają wójtowie, burmistrzowie, prezydenci miast, starostowie, wojewodowie, w rzeczywistości zaś poszczególne służby, należy dodać rządowe, za swój wycinek działania.

Porównując zalety i wady systemu scentralizowanego i zdecentralizowanego, można stwierdzić, że bardziej sprawnym z punktu widzenia współczesnego zarządzania jest system zdecentralizowany, że wszelkie potrzeby społeczności lokalnej powinny być zaspakajane przez organizacje znajdujące się jak najbliżej obywatela. Stąd podstawowym elementem w systemie zapewnienia bezpiecznego bytu obywateli powinien być pierwszy poziom administracji publicznej, czyli gminy. Od trafności sformułowanej strategii zapewniającej rozwój gminy, od jej realizacji, będzie zależał ten byt. Wójt powinien być koordynatorem działań na rzecz bezpieczeństwa społeczności lokalnej realizowanych przez własne zespoły samorządowe⁸ – w razie potrzeby wspierane przez powiatowe, wojewódzkie

⁸ W tym policję lokalną, której obecnie w Polsce nie ma. Czy ponad 60 tys. funkcjonariuszy pionu prewencji Policji (dzielnicowi, patrole, ruch drogowy) musi funkcjonować w układzie scen-

zespoły samorządowe lub też rządowe. Na zasadzie porozumień mogą to też być wyspecjalizowane zespoły międzygminne. Decentralizacja wiąże się też z reguły z niższymi kosztami funkcjonowania.

Rys. 2. Schemat organizacji i zarządzania bezpieczeństwem społeczności lokalnej w gminie, mieście – w aspekcie zadaniowo-instytucjonalnym



Źródło: Opracowanie własne

Polskie organizacje, zarówno biznesowe, jak i non profit (w tym administracja publiczna), nie należą do liderów podnoszących w sposób znaczący sprawność, jakość i innowacyjność działań. Badania wskazują, że do najbardziej pro sprawnościowych, projakościowych, proinnowacyjnych państw można zaliczyć: Szwajcarię, USA, Izrael, Finlandię i Japonię. Liderem w tym zakresie w Europie Centralnej i Wschodniej są Czechy⁹. Warto śledzić zachodzące w tych państwach zmiany i przenosić najlepsze rozwiązania do naszego kraju – w tym także w zakresie organizacji i zarządzania bezpieczeństwem obywateli. Poziom bezpieczeństwa

tralizowanym? Czy nie można przekształcić tego pionu w policję lokalną (samorządową)? Dałoby to średnio na gminę ok. 25 funkcjonariuszy.

⁹ *The Global Competitiveness Report 2012–2013*, ed. Klaus Schwab, World Economic Forum, Geneva 2012, s. 529–536; *The Global Competitiveness Report 2014–2015*, ed. Klaus Schwab, World Economic Forum, Geneva 2014, s. 529–536; M. Lisiecki, *Uwarunkowania projakościowego zarządzania bezpieczeństwem obywateli*, „Zeszyty Naukowe SGSP”, nr 50(2), 2014.

obywateli będzie zależał od szybkości i skali wprowadzanych zmian, od stopnia podążania za najlepszymi.

Biorąc pod uwagę doświadczenia państw o utrwalonej demokracji oraz tendencje w zakresie tworzenia organizacji przyszłości, można stwierdzić, że:

- większość potrzeb społeczności lokalnej w zakresie zapewnienia bezpieczeństwa obywateli powinna być zaspakajana przez wyspecjalizowane organizacje samorządowe;
- administracja rządowa powinna wspierać administrację samorządową jedynie w sytuacji, gdy zadania nie są możliwe do samodzielnego zrealizowania przez samorządy (zasada pomocniczości państwa);
- administracja rządowa powinna sprawować funkcję nadzorczą w zakresie przestrzegania prawa przez samorządy – nie wnikając jednak w treść merytorycznych decyzji podjętych zgodnie z uprawnieniami ustawowymi.

Organizacja i zarządzanie bezpieczeństwem w przyszłości powinno charakteryzować się dużą szybkością reagowania na zmiany w otoczeniu, inwestowaniem w ludzi (ich wiedzę, kompetencje), orientowaniem na cele wynikające z rzeczywistych potrzeb otoczenia, tworzeniem zespołów zadaniowo-wirtualnych na potrzeby realizacji tych celów, dążeniem do coraz wyższej sprawności, jakości i innowacyjności działań. Jednak nie osiągnie się tego bez właściwych ludzi we właściwym miejscu i czasie. Ludzie byli, są i będą najważniejszym zasobem każdej organizacji.

Bibliografia

Literatura:

- Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne*, PWN, Warszawa, 1994.
- Cieślarczyk M., *Teoretyczne, metodologiczne i praktyczne aspekty zarządzania bezpieczeństwem w pierwszej dekadzie XXI wieku*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, WSZIP, Warszawa 2008.
- Drucker P., *Management and world's*, "Harvard Business Review", September-October 1988.
- Góralczyk W., *Prawo międzynarodowe publiczne w zarysie*, PWN, Warszawa 1983.
- Kwiatkowska B., *Problemy bezpieczeństwa w samorządowej kampanii wyborczej*, „Zeszyty Naukowe SGSP” nr 22 (1999).
- Lisiecki M., *Jakość w zarządzaniu bezpieczeństwem obywateli*, KUL, Lublin 2009.
- Lisiecki M., Kwiatkowska-Basałaj B., *Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia*, [w:] *Zarządzanie bezpieczeństwem*, (red.) P. Tyrała, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.
- Lisiecki M., *Uwarunkowania pro jakościowego zarządzania bezpieczeństwem obywateli*, „Zeszyty Naukowe SGSP”, nr 50(2), 2014.

- Lisiecki M., *Zagrożenia społeczno-ekonomiczne bezpiecznego bytu oraz rozwoju obywateli. Sposoby przeciwdziałania*, [w:] *Nierówności społeczne we współczesnym świecie* (red.) A. Wołk, A. Potasińska, UKSW, Warszawa 2015.
- Standard Eurobarometer 83, Spring 2015, Public Opinion in the European Union, Report.
- Świniarski J., *Bezpieczeństwo w ujęciu aksjologicznym*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, WSZiP, Warszawa 2008.
- The Global Competitiveness Report 2012–2013, ed. Klaus Schwab, World Economic Forum, Geneva 2012.
- The Global Competitiveness Report 2014–2015, ed. Klaus Schwab, World Economic Forum, Geneva 2014.
- Traczyk Z., *Sektor obywatelski i inne obszary bezpieczeństwa*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, WSZiP, Warszawa 2008.

Wykaz rysunków:

- Rys. 1. Zarządzanie bezpieczeństwem obywateli
- Rys. 2. Schemat organizacji i zarządzania bezpieczeństwem społeczności lokalnej w gminie, mieście – w aspekcie zadaniowo-instytucjonalnym

Wykaz tabel:

- Tabela 1. Filary, wymiary i atrybuty holistycznie ujmowanego bezpieczeństwa
- Tabela 2. Zbiór zagrożeń dla bezpieczeństwa obywateli Unii Europejskiej i Polski z uwzględnieniem ich wagi (wiosna 2012–2015 r.)

Streszczenie

W artykule przedstawiono kierunki doskonalenia zarządzania bezpieczeństwem obywateli. Zwrócono uwagę na potrzebę ciągłego identyfikowania oczekiwań obywateli w zakresie bezpieczeństwa, podejmowanie działań mających na celu spełnienie tych oczekiwań zapewniających wysoką sprawność, jakość i innowacyjność. Wskazano na potrzebę dalszej decentralizacji działań.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo obywateli, zarządzanie bezpieczeństwem.

Summary

The organization and the safety management in the future

The article presents the directions of improving the management of public safety. Highlighted the need for continuous monitoring of citizens' expectations in terms of security, to take measures to fulfill these expectations to ensure high efficiency, quality and innovation. The need for further decentralization of activities.

Keywords: safety, safety of citizens, safety management.

Rozdział III.

Jak mierzyć odporność społeczności lokalnej?

Publikacja powstała w wyniku realizacji następujących projektów:

1. Projektu „Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP”, realizowanego na rzecz bezpieczeństwa i obronności państwa na podstawie umowy nr DOBR/0077/R/ID3/2013/03; projekt finansowany ze środków NCBiR,
2. Risk Management Capability Based on Gaps Identification in the BSR. “From Gaps to Caps”. Starting date: 2015-01-01; Ending date: 2016-12-31,
3. Baltic Sea Region EUSBSR flagship project 14.3 (January 2012 – June 2013).

1. Wstęp

Problematyka związana z zagadnieniami dotyczącymi odporności społeczeństwa, w tym w szczególności społeczności lokalnej, stanowi obecnie obszar intensywnych badań^{1,2}. Wynika to między innymi z faktu, że badania nad bezpieczeństwem ściśle związane są z dwoma aktualnie rozwiązywanymi problemami badawczymi. Pierwszym z nich jest poszukiwanie uniwersalnych metodyk szacowania ryzyka, mogących mieć zastosowanie dla dowolnego szczebla administracji publicznej, a nawet mieć charakter ponadpaństwowy, tj. regionalny. Drugim

Prof. dr hab. Jerzy Wolanin – Szkoła Główna Służby Pożarniczej w Warszawie.

¹ R.M. Cretney, *Local responses to disaster. The value of community led post disaster response action in a resilience framework*, [w:] “Disaster Prevention and Management” Vol. 25, No. 1, 2016, s. 27–40.

² A. Sharifi, *A critical review of selected tools assessing community resilience*, [w:] “Ecological Indicators” Volume 69, October 2016, s. 629–647.

wspomnianym wyżej problemem jest poszukiwanie metod zarządzania tym ryzykiem. W niniejszych rozważaniach przyjęto następującą definicję bezpieczeństwa:

Bezpieczeństwo jest to stan przestrzeni cywilizacyjnej i środowiska naturalnego lub/i procesy w nich zachodzące określone przez wartość występującego ryzyka wraz ze zdolnością zarządzania nim.

Przez ryzyko rozumie się możliwość (mierzoną ilościowo lub jakościowo) wystąpienia zagrożenia wraz z jego skutkami (również mierzonymi jakościowo lub ilościowo).

Należy nadmienić, że w przypadku kilku rodzajów ryzyka, co na ogół występuje, poszczególne jego rodzaje można zsumować i rozważać ryzyko zagregowane. W tym miejscu należy poczynić istotną uwagę. Mianowicie zarówno możliwość wystąpienia zagrożenia, jak i jego skutki, mogą być i są nie tylko „obiektywnie” oszacowane przez ekspertów (ryzyko eksperckie), ale również subiektywnie przez tych, których to zagrożenie dotyczy. Ta ostatnia ocena związana jest ze stanem emocjonalnym oceniającego. Ten stan nazywa się społecznym wzburzeniem³. Społeczne wzburzenie jest rzeczywiste, mierzalne i poddaje się zarządzaniu. Jest ponadto, obok oszacowań eksperckich, nieodłączną częścią ryzyka i „musi” być uwzględniane przy jego szacowaniu.

Poznanie ryzyka i „stopnia” możliwości zarządzania nim (pojęcie to zostanie wyjaśnione w dalszej części rozważań) pozwala na oszacowanie odporności społeczności. Tak więc odporność społeczności lokalnej definiuje się następująco:

Odporność społeczności lokalnej na zagrożenia jest to zdolność radzenia sobie (stopień możliwości zarządzania) ze zidentyfikowanym i oszacowanym ryzykiem, związanym z tymi zagrożeniami.

Z powyższej definicji wynika, że aby określić (ocenić) odporność danej społeczności lokalnej, należy w pierwszej kolejności zidentyfikować i oszacować ryzyko występujące na terenie tej społeczności oraz ocenić zdolność radzenia sobie z tym ryzykiem lub, ściślej rzecz ujmując, ocenić efektywność zarządzania tym ryzykiem.

2. Procedura szacowania ryzyka

Przedstawiona poniżej procedura szacowania ryzyka jest wynikiem dwóch opracowań naukowych i jest stosowana w większości państw europejskich^{4, 5}.

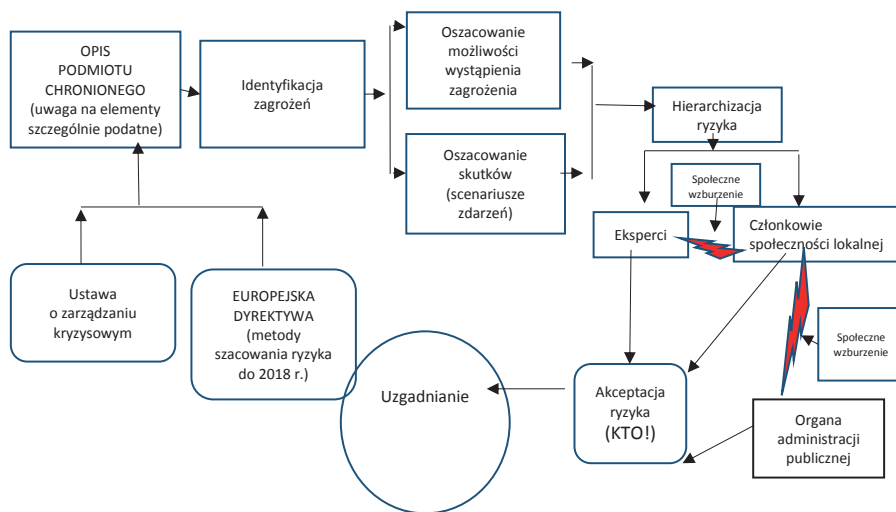
³ P.M. Sandman, *Responding to community Outrage: Strategies for effective Risk Communication*, American Industrial Hygiene Association Fairfax, Va. Fourth Printing 1997.

⁴ *Guiding and Tailoring Risk Assessment for the Baltic Sea Region* (praca zbiorowa), [w:] 14.3 Project implemented under EU Strategy for Baltic Sea Region (EUSBSR Action Plan) RED BOOK 2013.

⁵ W. Skomra (red.), *Metodyka analizy ryzyka do stosowania na różnych poziomach zarządzania kryzysowego*, [w:] *Metodyka oceny ryzyka na potrzeby zarządzania kryzysowego RP*, SGSP, Bell Studio 2015, s. 121–215.

Poniżej znajduje się ogólny schemat szacowania ryzyka zgodnie z przytoczonymi wyżej pracami.

Rys. 1. Ogólny schemat szacowania ryzyka



2.1. Opis podmiotu chronionego

Krok pierwszy, zaznaczony na rys. 1 jako opis podmiotu chronionego, w metodyce szacowania ryzyka nosi nazwę kontekstu. W praktyce sprowadza się do zawierającej szereg elementów charakterystyki społeczności lokalnej. Przez podmiot chroniony w tej metodyce rozumie się wszelkie dobra, jakie podlegają ochronie, w tym w szczególności życie i zdrowie człowieka, mienie, środowisko, funkcjonowanie społeczności lokalnej (społeczeństwa) z uwzględnieniem infrastruktury krytycznej, procesy zapewniające przetrwanie ludności, w tym funkcjonowanie administracji państwowej na każdym jej szczeblu, oraz wszelkie inne wartości ważne dla tej społeczności, np. z kulturowego, gospodarczego punktu widzenia itp. Opis ten na ogół dzieli się na kilka części (ze względu na brak miejsca wybrano tylko te elementy charakterystyki, na które niezbędne jest zwrócenie szczególnej uwagi).

Po pierwsze należy podać pełną nazwę podmiotu podlegającego analizie, nazwę urzędu oraz sposoby kontaktowania się.

Po drugie, chociaż ogólny cel analizy ryzyka jest znany, to jednak, ze względu na specyfikę poszczególnych społeczności lokalnych, cele takiej analizy mogą się różnić. Różne cele analizy ryzyka mogą wynikać również z różnic polityki bezpie-

czeństwa władz lokalnych na obszarze im podległym. Analiza ryzyka polega na jego oszacowaniu, dokonaniu jego ewaluacji poprzez hierarchizację. Ta ostatnia z kolei umożliwia określenie priorytetów działań, pozwalających na obniżenie poziomu ryzyka do poziomu akceptowalnego.

Na koniec, sposób zarządzania ryzykiem opisany powinien być poprzez opisanie kompetencji i funkcji elementów tworzących na danym terenie system bezpieczeństwa. W związku z tym opis podmiotu chronionego powinien zawierać następujące informacje:

1. związane z aspektem prawnym, uwzględniające prawo miejscowe oraz wewnętrzne uregulowania prawne, co oczywiście ściśle związane jest z polityką bezpieczeństwa. Obowiązuje tutaj bezwzględna zasada spójności lokalnej polityki bezpieczeństwa z rządową polityką bezpieczeństwa z uwzględnieniem wspomnianej specyfiki tej ostatniej;
2. charakterystykę podmiotu w przypadku administracji terytorialnej, obejmującą w szczególności:
 - położenie geograficzne;
 - podział administracyjny (gminy na sołectwa, starostwa na gminy itp.);
 - charakterystykę geograficzną, w szczególności uwzględniającą: powierzchnię, charakterystykę terenu (obszary rolnicze, miejskie, aglomeracja), możliwość osunięć lub tąpnięć ziemi, wzniesienia, doliny (ze względu na rozprzestrzenianie się np. obłoków toksycznych), ponadto należy określić te obszary środowiska naturalnego, które są ekspozowane na zagrożenia (np. lasy iglaste ze względu na możliwość zagrożenia pożarowego itp.);
 - charakterystykę lokalnej infrastruktury: cieków wodnych, dróg wodnych, przebieg linii kolejowych, przebieg dróg z podziałem na kategorie, z uwzględnieniem węzłów, z określeniem ich długości, wraz z charakterystyką transportu we wszystkich rodzajach transportu, podmioty gospodarcze, zakłady przemysłowe, przetwarzające, magazynujące lub/i transportujące substancje niebezpieczne (tj. takie, które są toksyczne, palne, wybuchowe, a w przypadku awarii ich wyciek zagraża sąsiadującym mieszkańcom, ich mieniu lub/i środowisku naturalnemu).

Powyższy opis należy nanieść na mapy (plany) analizowanego obszaru. Mapa taka obrazuje położenia źródeł zagrożeń i stanowi mapę źródeł zagrożeń:

- charakterystykę klimatyczną, w szczególności dotyczącą opadów deszczu, śniegu i gradu, temperatur sezonowych, wiatrów, gołoledzi, mgieł i innych szczególnych zjawisk klimatycznych. Należy również w opisie uwzględnić możliwość blokady dróg w wyniku działania sił natury, powodujące utrudnienia w funkcjonowaniu części lub całej jednostki administracyjnej. Opis powinien zawierać również inne zdarzenia niekorzystne zakłócające

funkcjonowanie obszaru administracyjnego (np. możliwe uszkodzenia sieci energetycznych w wyniku działania sił natury – m.in. zamarzająca na przewodach energetycznych mżawka);

- charakterystykę populacji – liczbę mieszkańców i ich charakterystykę ze względu na podatność, w tym rozmieszczenie siedzib, średnią wieku populacji, ze szczególnym uwzględnieniem w charakterystyce ludności takich grup jak: dzieci, ludzie starsi, niepełnosprawni, bezdomni, bezrobotni, wymagający opieki społecznej lub grupy ludności eksponowanych na jakiegokolwiek zagrożenie. Ta charakterystyka populacji wskazuje w szczególności na podatność poszczególnych grup społecznych. W wielu przypadkach pozwala również na ustalenie taktyki działań ratowniczych oraz szczególnych wymagań, dotyczących sił i środków, np. możliwość zapewnienia ewakuacji dla osób niepełnosprawnych w przypadku zmaterializowania się ryzyka. Jedną z istotniejszych cech charakterystyki populacji jest ocena świadomości społecznej związanej z zagrożeniami, a także poziom edukacji społecznej w tym zakresie. Zarówno świadomość społeczna, jak i edukacja, mają decydujący wpływ na taki element ryzyka, jak społeczne wzburzenie;
- charakterystykę powiązań społecznych (mieszkańcy o długiej wspólnej tradycji, społeczność posiadająca doświadczenie w pokonywaniu skutków katastrof (wspólne pokonanie skutków poprzednich katastrof obniża wartość społecznego wzburzenia), luźne powiązania społeczne, powiązania ekonomiczne, zmiany sezonowe liczby ludności narażonej na jakiegokolwiek zagrożenie;
- opis obiektów szczególnych (w aspekcie ich podatności na zagrożenie), między innymi: szpitali, domów opieki społecznej, domów komunalnych, sanatoriów, obiektów kultu religijnego, obiektów kultury narodowej, obiektów takich jak np. magazyny, w których znajdują się substancje niebezpieczne (toksyczne, wybuchowe, zanieczyszczające środowisko itp.);
- opis obowiązujących procesów kluczowych i krytycznych, pozwalających jednostce administracyjnej realizować jej zadania, a które mogą zostać zakłócone w wyniku zagrożenia (np. w wyniku powodzi i zanieczyszczenia środowiska zakłócona jest dostawa wody pitnej), określonych w ustawach kompetencyjnych i innych aktach prawnych, oraz wykaz zasobów do realizacji swoich celów, umożliwiających ograniczanie skutków zagrożenia;
- stwierdzenia na temat bieżącego uaktualniania planów zarządzania kryzysowego, przeprowadzania ćwiczeń na obiektach;
- opis infrastruktury krytycznej (lokalnej), np. wodociągi, ujęcia wodne, kanalizacja, obiekty telekomunikacyjne itp., a także opis infrastruktury krytycznej „cudzej” (gazociągi, ropociągi, linie przesyłu energii), obiekty opieki medycznej, służb ratowniczych, w tym OSP;

- zdolność do reagowania – o dużym lub małym doświadczeniu w reagowaniu, dostępność do służb;
- charakterystykę sąsiadów ze względu na możliwość transferu zagrożeń;
- inne przedsięwzięcia, stany i procesy w zarządzaniu bezpieczeństwem;
- niewiadome.

Niestety, ten ostatni punkt jest czysto intuicyjny, gdyż umieszcza się w nim hipotetyczne zdarzenia niekorzystne losowe (losowość oznacza nieprzewidywalność), ale o określonej wiarygodności wystąpienia. Warto w tym miejscu podkreślić, że wszelkie zdarzenia o poważnych skutkach, które zalicza się do kategorii katastrof, można podzielić na dwie umowne grupy: katastrofy „rutynowe” oraz katastrofy „niespodzianki”^{6,7}. Wśród tych ostatnich można wyróżnić następujące grupy katastrof:

- 1) katastrofy jedyne w swoim rodzaju,
- 2) katastrofy pierwsze danego rodzaju,
- 3) katastrofy o najgorszych skutkach.

Kategoria katastrof „niespodzianek” jest o tyle ważna, że ze względu na swój charakter, zdarzenia je wywołujące nie występują w katalogu zagrożeń. Można je zidentyfikować dzięki wiedzy eksperckiej, gdyż na ogół ukryte są w nowych technologiach lub zwiększającej się skali technologii już istniejących.

2.2. Identyfikacja zagrożeń

Ostatnia uwaga z poprzedniego podrozdziału w zasadzie dotyczy ważnej czynności analizy ryzyka, jaką jest identyfikacja zagrożeń. Nie ulega najmniejszej wątpliwości, że właśnie tutaj następuje największe zróżnicowanie związane z lokalnością zagrożeń.

Identyfikacja zagrożeń jest niezbędna do dalszej analizy ryzyka z nimi związanego. Identyfikacja zagrożeń jest również niezbędna do stworzenia opisowego scenariusza zagrożeń dynamicznych, to jest takich, które po zmaterializowaniu się rozprzestrzeniają się z określoną dynamiką. Dynamika rozprzestrzeniania się zagrożenia z kolei wpływa na rozmiar skutków. Zjawiska o dużej dynamice uniemożliwiają np. ostrzeżenie w porę ludności, gdyż bardzo ściśle powiązane są ze skutkami zagrożenia dynamicznego. Celem identyfikacji zagrożeń jest poszukanie odpowiedzi na pytanie kanoniczne (pytanie, na które oczekuje się odpowiedzi w przypadku każdej analizy ryzyka, niezależnie od tego, jakiego podmiotu dotyczy i w związku z jakim zagrożeniem jest dokonywana):

⁶ J.K. Mitchell, P.S. Showalter (1998), *Long road to recovery*, [w:] *Community responses to industrial disaster*, edited by James K. Mitchell, The United Nation University, 1996.

⁷ P.S. Showalter, *Responding to “unconventional” millennial prediction*, [w:] *“Disaster Prevention and Management”* Vol. 7, No 4, 1998, s. 273–280.

Co złego może się stać?

Identyfikacji zagrożeń można dokonać na kilka sposobów. Po pierwsze, sięgnąć do historii zdarzeń zapisanych w dokumentach lub zapamiętanych. Po drugie, sięgnąć do statystyk służb i zespołów odpowiedzialnych na danym terenie za bezpieczeństwo obywateli. Po trzecie, sięgnąć do ekspertyz sporządzonych przez specjalistów określonych dziedzin. Sięganie do opinii ekspertów na tym etapie dotyczy głównie tych zagrożeń, których występowanie jest bardzo rzadkie lub które nie wystąpiły w ogóle na danym terenie.

Często w praktyce używa się określenia „zagrożenie” w podwójnym znaczeniu. Z jednej strony mówimy, że dany zakład przemysłowy stwarza zagrożenie dla zdrowia ludzi i środowiska, z drugiej zaś strony obliguje się służby ratownicze do natychmiastowej likwidacji zagrożeń lokalnych. W przytoczonym przykładzie zakład stwarza zagrożenie i na pewno zagrożenie to jest lokalne. Jednak nie jest to zagrożenie, które musi likwidować służba ratownicza. Tak więc w tym wypadku mowa jest o dwóch różnych zagrożeniach. Stosowanie pojęcia „zagrożenie” do wszystkich jego typów może prowadzić do poważnych nieporozumień. Do zagrożeń, na które powinny reagować służby ratownicze, zalicza się między innymi wyciek toksycznej substancji z instalacji chemicznej w wyniku awarii technicznej lub wyciek tej substancji z cysterny, która uległa wypadkowi, a utworzony obłok zagraża bezpośrednio zdrowiu ludzi i środowisku. Do nich można zaliczyć pożar mieszkania czy też lasu lub skutki powodzi, chociaż w tym ostatnim wypadku ze względu na rozległość często jest trudno mówić o lokalnym charakterze zagrożeń.

Tak więc z jednej strony mamy do czynienia z zagrożeniami o charakterze potencjalnym i stałym, z drugiej zaś strony z zagrożeniami, które ekspandują w czasie i przestrzeni. Do pierwszej grupy zaliczane są zagrożenia, które wynikają z normalnej eksploatacji urządzeń, linii technologicznych, procesów itp. i znajdują się pod kontrolą do chwili wystąpienia zdarzenia niekorzystnego rozumianego w niniejszej metodyce jako przekształcenie się zagrożenia potencjalnego w dynamiczne, na ogół powodującego niekontrolowany wyciek masy i/lub energii lub powodującego dysfunkcję systemów.

Grupę zagrożeń o charakterze potencjalnym i stałym, mającą możliwości negatywnego oddziaływania na ludzi, otoczenie cywilizacyjne lub/i środowisko naturalne, nazywamy zagrożeniami potencjalnymi. Często zamiast pojęcia „zagrożenie potencjalne” używa się określenia „źródło ryzyka”, które są tożsame.

Tak więc zagrożenia potencjalne to jest ta kategoria zagrożeń, do zarządzania którymi wymagane są działania profilaktyczne, ściśle powiązane z polityką bezpieczeństwa.

Z punktu widzenia analizy ryzyka działania te ściśle powiązane są z całym zespołem przedsięwzięć obniżających prawdopodobieństwo wystąpienia zagrożenia dynamicznego.

Natomiast przesuwający się toksyczny obłok, pożar czy też przepływ fali podwodzowej należą do kategorii zagrożeń rozprzestrzeniających się i równocześnie zagrażających życiu, mieniu i środowisku. Zagrożenia tego typu charakteryzują się tym, że do ich likwidacji wymagane są natychmiastowe działania ograniczające skutki ich wystąpienia. Istotą tych zagrożeń jest niekontrolowane rozprzestrzenianie się uwolnionej masy lub energii. Ponieważ mają one charakter dynamiczny, nazywa się je zagrożeniami dynamicznymi.

Wystąpienie zagrożenia dynamicznego wymaga podjęcia akcji ratowniczej. Jest to fundamentalna różnica między zagrożeniami potencjalnymi a zagrożeniami dynamicznymi.

Zagrożenia można również podzielić ze względu na częstotliwość ich występowania. Na rys. 2 schematycznie przedstawiono taki podział. Wszystkie zagrożenia zostały podzielone na zagrożenia stałe i zagrożenia sporadyczne⁸.

Porównując na rysunku obie kwalifikacje zagrożeń, należy zauważyć, że zagrożenia stałe ciągłe to nic innego jak zagrożenia potencjalne. Natomiast zagrożenia stałe dyskretne i zagrożenia sporadyczne są to zagrożenia dynamiczne.

Analiza ryzyka ściśle związana jest z analizą zagrożeń obu rodzajów. Wymaga ona, zgodnie z definicją ryzyka, określenia prawdopodobieństwa wystąpienia zdarzenia niekorzystnego oraz określenia skutków tego zdarzenia. Ale, żeby to uczynić, należy najpierw rozpoznać zagrożenia, tj. zidentyfikować źródła ryzyka. To, z czym na ogół spotyka się przeprowadzający takie analizy, to bardzo duża liczba potencjalnych zagrożeń występujących na danym terenie.

Rys. 2. Podział zagrożeń ze względu na częstotliwość pojawienia się zdarzeń niekorzystnych⁸



⁸ T. Szopa, *Koncepcja graficznego przedstawiania terytorialnego rozkładu ryzyka i zagrożeń*, [w:] *Mapy terytorialnego rozkładu ryzyka* (oprac.), Politechnika Warszawska, Szkoła Główna Służby Pożarniczej, 2004.

Wszystkie zagrożenia można podzielić na trzy zasadnicze grupy: zagrożenia techniczne, zagrożenia naturalne i zagrożenia militarne. Identyfikacji zagrożeń można dokonać na trzy sposoby.

Jeśli chodzi o zagrożenia techniczne, to, po pierwsze, można skorzystać z dokumentów archiwalnych opisujących historycznie występujące zagrożenia. Po drugie, można skorzystać z katalogu zagrożeń będącego załącznikiem do metodyki⁹. Po trzecie, można wykorzystać wiedzę ekspercką w szczególności dotyczącą nowo pojawiających się zagrożeń. Wszystkie te techniki identyfikacji można stosować rozdzielnie lub łącznie w dowolnych kombinacjach.

Zagrożenia techniczne związane są z awarią sprzętu służącego do magazynowania, transportu, sieci przesyłowych i prowadzenia procesów substancji niebezpiecznych.

Do identyfikacji zagrożeń technicznych może być przydatna poniższa tabela. Spośród wszystkich podanych w niej źródeł ryzyka (źródeł zagrożeń) należy wybrać te, które występują na analizowanym terenie i przyporządkować mu konkretne zagrożenie z katalogu, bądź poprzez zastosowanie jednej z metod eksperckich. Jeśli zidentyfikowane źródło zagrożenia technicznego występuje na danym terenie, a nie jest wymienione w tabeli, należy je uwzględnić i przyporządkować odpowiedniemu zagrożeniu, tak jak w pozostałych przypadkach.

Poszukujemy tutaj odpowiedzi na następujące pytanie kanoniczne:

Czy na rozważanym terenie występuje jedno z niżej wymienionych źródeł ryzyka?

Tabela 1. Przykładowy wykaz źródeł zagrożeń⁹

Obiekt	Najczęstsze zagrożenia
doki, terminale, stacje przeładunkowe, magazyny	duża i różnorodna liczba wielu rodzajów substancji niebezpiecznych (palnych, wybuchowych, trujących); dźwigi i pojazdy
statki, stacje rozrządowe, kanały	materiały niebezpieczne, ropa
lotniska, samoloty transportowe	paliwo, materiały niebezpieczne

⁹ UNEP-APELL Hazard identification and evaluation in a community, UNEP-APELL, Technical Report, 12 12 (with support of Swedish government), 1988.

przemysł (technologia), rafinerie, petrochemia, technologie chemii nieorganicznej, farmaceutyczny, tekstylny, celulozowy itp.	zawory ciśnieniowe, zbiorniki, magazyny, kontenery, linie technologiczne zawierające substancje niebezpieczne w formie surowców, katalizatorów, produktów, produktów przejściowych, odpadów, linii wysokiego napięcia itp
inny rodzaj przemysłu tworzyw sztucznych, gumowych, drzewnych (tartaki) itp.	zawory ciśnieniowe, magazyny, zbiorniki z substancjami trującymi, palnymi itp
wodne elektrownie	spiętrzona woda, linie wysokiego napięcia
elektrownie węglowe	materiały palne, zawory ciśnieniowe, strumienie pary o wysokim ciśnieniu, gorąca woda, linie wysokiego napięcia
elektrownie atomowe	radioaktywne i trujące materiały, zawory ciśnieniowe, para pod wysokim ciśnieniem, gorąca woda, linie wysokiego napięcia
rurociągi gazowe	gaz palny, przepływ pod zwiększonym ciśnieniem
inne rurociągi	palne, trujące i groźne dla środowiska substancje, przepływ pod zwiększonym ciśnieniem
stacje benzynowe, stacje paliw	palne, trujące i stwarzające zagrożenie dla środowiska substancje
magazyny towarowe	palne i trujące substancje zawarte w aerozolah
handel materiałami budowlanymi (drewnem)	duża ilość nagromadzonego drzewa
magazyny towarowe	palne, trujące, wybuchowe substancje
lokalne przedsięwzięcia, ujęcie wodne, pływalnie, punkty uzdatniania wody itp.	substancje niebezpieczne
Szpitala, szkoły	niebezpieczne chemikalia
hotele	wysokie budynki
silosy	palny, wybuchowy pył
kamieniołomy i inne miejsca związane z górami lub umiejscowione pod ziemią; grunty ulegające zalaniom, obsunięcia ziemi, zaważenia się budynków	lawiny kamieni, gruntu, wody podziemne, pojazdy, gaz; warunki geologiczne
tunele	ryzyko zaważenia, utrudnienia w ratowaniu
drogi	pojazdy, materiały niebezpieczne

Po zidentyfikowaniu źródeł zagrożeń należy każdemu z nich przyporządkować zagrożenie.

Poniżej zilustrowano w formie przykładowej tabeli (tabela 2) przyporządkowanie określonej kategorii substancji niebezpiecznej do określonych skutków, do których może prowadzić jej niekontrolowany wyciek.

Tabela 2. Przykładowe skutki uwolnienia substancji niebezpiecznej

Kategoria substancji	Skutki uwolnienia
ciecze palne	pożary powierzchniowe; eksplozja chmury par VCE (<i>Vapour Cloud Explosion</i>)
gazy palne – skroplone pod ciśnieniem	BLEVE, rozgorzenie (<i>Flash Fire</i>)
gazy palne – skroplone termicznie (przez ochłodzenie)	pożary powierzchniowe
gazy palne – pod ciśnieniem	pożar – zapalenie się chmury gazu (<i>Fireball</i>)
organiczne i wybuchowe nadtlenki	wybuch; wybuch fazy skondensowanej
ciecze toksyczne	chmura par z rozlewiska
gazy toksyczne – skroplone pod ciśnieniem	toksyczna chmura, ciągły wpływ
gazy toksyczne – skroplone przez wchłanianie	toksyczna chmura
gazy toksyczne – pod ciśnieniem	toksyczna chmura
toksyczny proszek	toksyczna chmura
toksyczne produkty spalania	toksyczna chmura

2.3. Oszacowanie skutków – scenariusz opisowy

Scenariusz opisowy tworzy się po to, aby, po pierwsze, dane niezbędne do szacowania ryzyka zebrać w jednym miejscu. Po drugie, opisać ciąg zdarzeń wynikających z rozprzestrzeniania się zagrożenia dynamicznego wraz z jego skutkami. Scenariusz opisowy pozwala też szacującemu ryzyko nie tylko na plastyczne uzmysłowienie sobie obrazu zagrożenia dynamicznego oraz jego skutków, ale także na wzajemne powiązanie następstw zdarzeń, wykrycie zjawiska domina (kaskadowego). Ponadto scenariusz opisowy może służyć do identyfikacji tych wielkości skutków, które niezbędne są do dalszych obliczeń i to zarówno w sposób jakościowy, jak i ilościowy.

Scenariusz opisowy bezwzględnie powinien mieć ścisły związek z kontekstem. W zależności od rodzaju zagrożenia, a w szczególności jego skutków, scenariusze opisowe będą różnić się między sobą. I tak na przykład, jeżeli zagrożenie tworzy niekontrolowany wyciek substancji niebezpiecznej z pojazdu poruszającego się po drogach jednostki administracyjnej, wówczas w scenariuszu powinno znaleźć się nawiązanie do kontekstu, opisującego długość dróg, po których poruszają się pojazdy. W takim przypadku scenariusz opisowy również powinien uwzględniać liczbę mieszkańców osiedlonych w pasie o szerokości kilkuset metrów wzdłuż tych dróg, a także rodzaj zabudowy. W ten sposób można oszacować liczbę mieszkańców narażonych na skutki ewentualnego wycieku. Natomiast rodzaj zabudowy jest ważną charakterystyką w przypadku wycieku substancji palnej, która może ulec zapaleniu (wybuchowi), powodując pożary, a tym samym poważne straty w mieniu. Do oceny tych strat niezbędne jest także oszacowanie wartości mienia po obu stronach drogi na odcinkach, na których to mienie jest zlokalizowane.

Z punktu widzenia ryzyka powstania sytuacji kryzysowej, w scenariuszu opisowym nie tylko zagrożenie ludzi, mienia i środowiska stanowią elementy decydujące o jej powstaniu, ale także zakłócenia w funkcjonowaniu jednostki lub jednostek administracji publicznej oraz zakłócenia w codziennym funkcjonowaniu obywateli, czyli niezbędna staje się analiza wpływu zagrożenia na fundamentalne procesy funkcjonujące w społeczności lokalnej. Podczas tej analizy szczególnej staranności wymaga opis tych elementów i procesów, które są nadzwyczaj podatne na zagrożenie. Oczywiście opis ten powinien być spójny z kontekstem. Zagrożenie takie jak powódź lub rozpatrywany tutaj wyciek może doprowadzić do skażenia środowiska, w tym ujęć wodnych, powodując przerwy w jej dostawie. Również obywatele mogą spotkać się z trudnościami w zaopatrzeniu w rzeczy niezbędne lub mieć trudności w dostaniu się do pracy. Taki opis bezwzględnie powinien znaleźć się w scenariuszu opisowym. Przedstawiony powyżej scenariusz należy uzupełnić o następujący opis ewentualnego efektu kaskadowego: np. zalanie jednostki straży pożarnej w czasie spowoduje znaczne opóźnienie dojazdu do pożaru, co z kolei narazi ludzi na utratę życia. Skutki drugiego zdarzenia przewyższą skutki pierwszego z nich. Jest to typowe zjawisko dla efektu kaskadowego.

W tym miejscu należy podkreślić, że wszystkie dane liczbowe podane w opisie scenariuszowym, jeżeli występują, muszą pokrywać się z odpowiedziami do pytań kanonicznych, zadanych w dalszej części metodologii szacowania ryzyka.

Scenariusz opisowy związany z siłami natury konstruowany jest w inny sposób. Jako pierwszy przykład można rozważyć powódź.

Przede wszystkim dla najgroźniejszych rozlań (jako powódź traktowane jest każde wystąpienie wody z brzegów) przy tworzeniu scenariusza opisowego na-

leży odwołać się do map stworzonych w ramach ISOK, na których zaznaczono zasięgi rozlanej wody. Mapy te stworzono dla dwóch przypadków: wody stuletniej o prawdopodobieństwie 0,01 oraz wody pięćsetletniej o prawdopodobieństwie 0,002. Ponieważ ryzyko z definicji jest to iloczyn prawdopodobieństwa i skutków, to dla naszych dwóch przypadków należy określić liczbę osób zamieszkałych na zagrożonym terenie oraz oszacować wartość strat materialnych w obydwu przypadkach – te dane również można odczytać z tych map.

W przypadku, gdy możliwa jest powódź, a nie uwzględniono danego terenu w mapach powodziowych ISOK lub w ogóle w celu dokonania szacowania ryzyka związanego z zagrożeniem powodzią dla dowolnego zbiornika lub cieków wodnego, wystarczy w opisie podać średnią częstotliwość powodzi oraz średni jej zasięg. Dane te posłużą potem do obliczeń, dlatego też w dalszym postępowaniu, w odpowiedziach na pytania kanoniczne trzeba sięgnąć właśnie do nich.

W tym miejscu należy wyjaśnić, że zdarzeniom związanym w szczególności z siłami natury, to jest z tymi siłami lub przyczynami, które powodują pewną cykliczność ich występowania, przyporządkowuje się pojęcie „okresu nawrotu”. Okres nawrotu jest to średni czas nawrotu zdarzenia, np. powodzi. Stwierdzenie, że powódź powtarza się raz na cztery lata, oznacza, że okres nawrotu wynosi cztery lata. Można wykazać, że okres nawrotu danego zdarzenia (zjawiska) jest ściśle przyporządkowany prawdopodobieństwu jego wystąpienia, jeśli, a tak jest w naszym przypadku, prawdopodobieństwo odnosi się do jednego roku. Wówczas odwrotność prawdopodobieństwa jest równa okresowi nawrotu. I tak wspomniane już prawdopodobieństwa 0,01 oraz 0,002 wystąpienia powodzi oznaczają odpowiednio wystąpienie powodzi raz na sto lat i raz na pięćset lat. Tak więc, wracając do przykładu powodzi w gminie Y, stwierdzając, że rzeka wylewa raz na cztery lata, mówimy o pewnym średnim prawdopodobieństwie, mając za sobą wiele wylań tej rzeki. To średnie prawdopodobieństwo wynosi w tym wypadku $\frac{1}{4} = 0,25$. Wówczas pytanie jest następujące: jakie jest prawdopodobieństwo, że rzeka spowoduje chociaż jedną powódź w ciągu najbliższego roku? Odpowiedź znajduje się w tablicach, pokazujących wartości prawdopodobieństw wystąpienia zdarzenia dla przedziału średnich od wartości 0,1 do 10. Tablice te ilustrują rozkład Poissona. Znając prawdopodobieństwo oraz opisane skutki i mnożąc jedno przez drugie otrzymujemy ryzyko związane z powodzią, a dotyczące ewentualnej ewakuacji ludzi, zniszczenia mienia, środowiska, a także ewentualnie uszkodzenia infrastruktury krytycznej, jakim może być np. zablokowanie drogi.

Scenariusz opisowy związany z uszkodzeniem infrastruktury krytycznej najlepiej jest omówić właśnie na przykładzie blokady drogi. Droga należy do infrastruktury krytycznej. Istnieje cały szereg zdarzeń inicjujących taką blokadę.

Mogą to być powódź, zasy śnieżne, uszkodzenie drogi w wyniku osunięć ziemi lub błota z kamieniami, katastrofa budowlana, np. mostu, a nawet wypadek drogowy uniemożliwiający przejazd karetki do wymagającego natychmiastowej pomocy.

We wszystkich tych przypadkach mamy do czynienia z alternatywą zdarzeń (choć nie zawsze można wykluczyć koniunkcję niektórych z nich, np. powódź i lawinę błotną). Alternatywę zdarzeń w przypadku szacowania ryzyka należy rozumieć w ten sposób, że jeden skutek, w naszym przypadku blokada drogi, wywołany może być kilkoma niezależnymi przyczynami. Wówczas w scenariuszu opisowym stosujemy operator „lub”. Tak więc do blokady drogi może dojść, gdy wystąpi powódź lub powstaną zasy śnieżne lub nastąpi katastrofa budowlana mostu lub zdarzy się wypadek blokujący drogę i jednocześnie (koniunkcja) trzeba będzie komuś natychmiast udzielić pomocy. Zresztą zdarzenie „wymagana natychmiastowa pomoc” może być koniunkcją dla każdego z wymienionych zdarzeń inicjujących blokadę drogi. Mamy wówczas ponownie do czynienia ze zdarzeniem kaskadowym – blokada drogi uniemożliwia przejazd karetki, co powoduje śmiertelne zagrożenie dla osoby (osób) wymagających natychmiastowej pomocy. Scenariusz ten można jeszcze uzupełnić o inne skutki długotrwałej blokady drogi, takie jak przerwanie dostaw zaopatrzenia, niemożność dotarcia do pracy i szkoły, niemożność dotarcia służb do miejsc awarii, przerwa w usługach, handlu, a nawet produkcji.

Szacowanie prawdopodobieństwa zakłócenia tych procesów odbywa się poprzez metody eksperckie. Zdarzenia te mogą stanowić koniunkcję lub alternatywę. Opis ten powinien być dokonany przez ekspertów. Do analizy ryzyka w takich przypadkach stosujemy następującą zasadę: rozpatrujemy największe, ale jeszcze w zgodzie z rozsądkiem, możliwe zagrożenie (AHARP – *As High As Reasonably Practicable*). Zresztą podobna zasada obowiązuje, jeżeli chodzi o najmniejszą wartość szacowanego ryzyka – rozpatruje się ryzyko najmniejsze z możliwych, ale jeszcze rozsądnie praktyczne (ALARP – *As Low As Reasonably Practicable*). W praktyce oznacza to, że na ogół nie rozpatruje się rodzajów ryzyka, których koszt sprowadzenia do poziomu akceptowalnego jest wyższy od wartości podmiotu chronionego. Wyjątek stanowi ochrona ludzi, chociaż i tutaj istnieje granica ALARP.

Warto pamiętać, że jeżeli zdarzenia inicjujące stanowiące alternatywę mają różne prawdopodobieństwa wystąpienia, a tak na ogół jest, to wówczas prawdopodobieństwo wystąpienia zdarzenia krytycznego (w tym przypadku blokady drogi) jest wyższe od najwyższego prawdopodobieństwa zdarzenia inicjującego. Wynika to z faktu, że prawdopodobieństwo każdego zdarzenia inicjującego ma wkład w powstanie zdarzenia krytycznego. Można powiedzieć, że prawdopo-

dobieństwa te „sumują” się. Nie jest to jednak dosłownie suma w potocznym rozumieniu i co do zasady nie należy tych prawdopodobieństw wprost sumować.

Nie zawsze jest oczywiste, w którym momencie dany scenariusz bierze swój początek i kiedy się kończy. Dla zagrożeń dynamicznych należy przeanalizować zdarzenie lub sytuację prowadzące do sekwencji zdarzeń o negatywnych skutkach. Te zdarzenia lub sytuacje nazywa się „wyzwalaczami” (*triggers*) i w szczególności one powinny być analizowane.

Aby nadać praktyczny sens konstruowaniu scenariuszy, powinny być one tworzone z punktu widzenia aktualnych trendów i długoterminowych planów rozwoju danej społeczności lokalnej.

Na zakończenie rozważań dotyczących budowy scenariuszy należy wziąć pod uwagę stopień niepewności ich realizacji. Każdy scenariusz obciążony jest niepewnością, wynikającą chociażby z braku wiedzy na temat rozwoju dynamicznych zagrożeń lub też możliwości wystąpienia zdarzenia niespodzianki.

Cały problem polega na tym, że obecne decyzje, na ogół o skutkach finansowych, dotyczą zdarzeń przyszłych, które w ogóle mogą nie wystąpić.

2.4. Hierarchizacja ryzyka

Mając ocenione prawdopodobieństwa wystąpienia poszczególnych scenariuszy opisujących skutki zagrożenia dynamicznego, można przystąpić do jego hierarchizacji. Wydawać by się mogło, że sprawa jest oczywista. Ale niestety ten krok w ocenie ryzyka jest jednym z najtrudniejszych do realizacji. Wynika to z faktu braku miary bezwzględnej akceptacji ryzyka, do której można by odnieść skalę hierarchizacji. Rozwiązania tego problemu nie ułatwia również fakt, że hierarchizacja ryzyka jest inna dla różnych osób lub grup oceniających.

Badania wspomnianego tutaj już Sandmana¹⁰ wskazują, że korelacja między poszczególnymi hierarchizacjami, np. pomiędzy decydentami a grupami społecznymi, wynosi zaledwie 4%. Oznacza to, że mamy do czynienia z dwoma zupełnie różnymi wartościami wielkości ryzyka. Konsekwencją takich rozbieżności jest konflikt stron, przekształcający wydawałoby się czysto eksperckie analizy w problem społeczno-polityczny. Jak już wcześniej wspomniano, ta społeczna percepcja ryzyka nosi nazwę społecznego wzburzenia, które w analizie ryzyka jest równoprawne z analizą ekspercką. Zresztą, jak pokazuje praktyka, decydent dysponuje nie tylko wynikami wiedzy eksperckiej i zna opinię społeczną na temat różnego rodzaju ryzyka, ale sam postrzega te ryzyka

¹⁰ P.M. Sandman, *Responding to community outrage...*

w sposób subiektywny. Tak więc problem szacowania ryzyka i jego hierarchizacji nie tylko staje się problemem politycznym, ale w ten proces w sposób immanentny wpisany jest konflikt.

Hierarchizacja ryzyka wiąże się z jego wizualizacją. Jedną z metod wizualizacji jest przedstawienie ryzyka w postaci specjalnej matrycy zwanej Matrycą Ryzyka. Konstrukcja matrycy polega na tym, że na osi poziomej odkłada się wartości skutków (bądź w postaci liczbowej, bądź też w postaci opisowej), zaś na osi pionowej – prawdopodobieństwa (bądź też opis możliwości wystąpienia danych skutków). Przy opisowej konstrukcji Matrycy Ryzyka ważne, aby dokładnie wyjaśnić poszczególne określenia, np. znikoma możliwość wystąpienia to możliwość wystąpienia powyżej 1000 lat. Na rys. 3 przedstawiono przykład Matrycy Ryzyka. Kolorami zaznaczono jego hierarchię. Problem polega na sporze dotyczącym odpowiedzi na pytania, co to znaczy skutki małe, średnie, duże, bardzo duże i w końcu od kiedy można uznać skutki za katastrofalne. Niestety nie ma standardów w tym zakresie. Te same skutki widziane z różnego poziomu administracji mogą być oceniane w różny sposób. Zniszczenie kilku domów w rezultacie działania wiatru dla gminy może stanowić skutki zakwalifikowane jako duże, zaś z punktu widzenia województwa jako małe. Dlatego każdy, kto sporządza Matrycę Ryzyka, musi opisać, co kryje się pod danym określeniem. Można np. zastosować kryterium finansowe, tj. oznaczać skutki według procentu całkowitego budżetu danej jednostki administracyjnej.

Oznaczenie kolorów z kolei dotyczy wielkości ryzyka i stanowi wizualizację hierarchii ryzyka. Tak więc można ryzyka pogrupować w sześć następujących kategorii: ryzyko zaniedbywalne (niepotrzebne żadne nakłady finansowe), ryzyko małe, ryzyko średnie, ryzyko duże, ryzyko ekstremalne i wreszcie najgorsze scenariusze (przypadki). Do każdej kategorii ryzyka można przypisać określone środki na zarządzanie nim, a także wyspecyfikować działania pozwalające na panowanie nad ryzykiem. Na przykład rodzaje ryzyka zakwalifikowane do ekstremalnych wymagają natychmiastowych działań obniżających ich wartość do tolerowalnego lub akceptowalnego poziomu. Na rys. 3 widać, że ryzyko rośnie, poczynając od lewego dolnego rogu w kierunku prawego górnego rogu. Natomiast w prawym dolnym rogu umiejscowione zostało ryzyko zwane najgorszym scenariuszem lub najgorszym przypadkiem. Ten rodzaj ryzyka jest szczególnym przypadkiem ryzyka ekstremalnego i obejmuje zdarzenia wyjątkowo rzadko występujące, ale o katastrofalnych skutkach. Tutaj mieszczą się również katastrofy niespodzianki (czarne łabędzie).

Rys. 3. Przykładowa Matryca Ryzyka

Możliwość wystąpienia zdarzenia

bardzo częste					
częste					
średnia możliwość wystąpienia					
rzadko występujące					
znikoma możliwość wystąpienia					
	bardzo małe	małe	duże	bardzo duże	katastrofalne

Skutki

	ryzyko zaniedbywalne
	ryzyko małe
	ryzyko średnie
	ryzyko duże
	ryzyko ekstremalne
	najgorszy scenariusz

3. Zarządzanie oszacowanym ryzykiem

Poniższe rozważania opierają się na wynikach europejskiego projektu “From Gaps to Caps”. Przedstawiona metoda oceny zarządzania ryzykiem nosi nazwę Metody Zarządzania Ryzykiem Krajów Morza Bałtyckiego (BSR Method)¹¹.

W Polsce przeprowadzanie analizy ryzyka wynika z obowiązku ustawowego. Jednak w praktyce w wielu wypadkach wykonujący taką analizę, po

¹¹ Risk Management Capability Based on Gaps Identification in the BSR, “From Gaps to Caps”. The project was implemented in the following countries: Denmark, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, Norway, Poland and Sweden. Starting date: 2015-01-01; Ending date: 2016-12-31.

pierwsze, nie widzą ostatecznego celu jej przeprowadzania. Po drugie, nie bardzo wiadomo, jak poprawnie taką analizę przeprowadzić, gdyż nie wprowadzono jednolitej, określającej w sposób jednoznaczny metodyki. Jednak jeśli by przyjąć wyżej opisany zarys metodyki, to zgodnie z definicją bezpieczeństwa oszacowanie ryzyka stanowi ważny, ale tylko jeden element bezpieczeństwa. Drugim elementem niezbędnym do określenia wartości bezpieczeństwa jest zdolność zarządzania oszacowanym ryzykiem. Ocena zdolności zarządzania ryzykiem stanowi procedurę, która do momentu budowy scenariusza jest identyczna jak opisana wyżej procedura szacowania ryzyka. Scenariusz więc stanowi podstawę do oceny możliwości zarządzania danym, konkretnym ryzykiem.

Procedura oceny zarządzania ryzykiem składa się z następujących elementów:

- a. planowania,
- b. opisu zdarzenia krytycznego,
- c. budowy scenariusza,
- d. opisu wpływu na krytyczne, dla danej społeczności, procesy (*vital societal functions*),
- e. opisu skutków, oceny podatności i potencjalnej możliwości reagowania.

Od razu widać, że procedura ta przenika się z procedurą szacowania ryzyka. Dlatego też, nie tracąc nic z głównej myśli, poniżej omówione zostaną niektóre tylko elementy oceny możliwości zarządzania oszacowanym ryzykiem¹².

3.1. Planowanie

Rozpoczyna się na ogół od posiedzenia grupy osób odpowiedzialnych za bezpieczeństwo na danym terenie. Decydują one między innymi o tym, kto powinien się zająć problematyką ryzyka i jakie zasoby są niezbędne do budowy scenariuszy dla poszczególnych zagrożeń oraz jakie informacje są niezbędne do wykonania prawidłowo analizy i w jaki sposób należy je gromadzić (należy tutaj podkreślić, że rodzaj danych i sposób ich gromadzenia jest obecnie rozwiązywanym problemem). W tej fazie procesu określa się również, jacy eksperci i inni specjaliści o szczególnych umiejętnościach (np. komunikacyjnych) powinny znaleźć się w grupie oceniającej zdolności porażenia sobie z ryzykiem.

¹² Określenie „możliwości zarządzania oszacowanym ryzykiem” wskazuje, że mimo swojej ogólności procedury, dotyczącej zarządzania ryzykiem, zawsze taką możliwość zarządzania określa się dla konkretnego oszacowanego ryzyka.

3.2. Opis zdarzenia krytycznego

Zdarzenie krytyczne powinno być zdefiniowane. Przy czym mogą tu być zastosowane definicje naukowe, operacyjne lub też prawne. W tym miejscu dokonuje się również identyfikacji zdarzeń inicjujących, tj. prowadzących do zdarzenia krytycznego. Takiej analizy dokonuje się, przede wszystkim wykorzystując drzewo błędów. W tym kroku szacuje się możliwość wystąpienia zdarzenia krytycznego (w opisie jakościowym) lub prawdopodobieństwo (w opisie ilościowym) jego wystąpienia. Ważne jest też określenie ogólnych skutków, takich jak wpływ na infrastrukturę, fizycznych, społecznych, ekonomicznych, środowiskowych, zdrowotnych, kulturowych, organizacyjnych lub też technicznych.

W celu realizacji dalszych kroków opis zdarzenia krytycznego powinien zawierać również analizę planów reagowania, a także przedsięwzięć prewencyjnych dotyczących tego typu zdarzeń, w szczególności planów związanych z utrzymaniem ciągłości funkcjonowania danej społeczności lokalnej.

3.3. Budowa scenariusza

Identyfikacja zdarzenia krytycznego i ogólny opis jego skutków pozwalają na wybór scenariusza umożliwiającego reprezentacyjny dla danego zagrożenia scenariusz przebiegu zdarzeń. Wybór opiera się na zasadzie „scenariusz najgorszego, ale jeszcze wiarygodnego zdarzenia” (*worst credible*) lub „taki najgorszy scenariusz, który jest jeszcze rozsądnie praktyczny lub wiarygodny” (*as high as reasonably practical / credible*). Wyboru takiego scenariusza co do zasady dokonują eksperci, ale mogą zaistnieć przesłanki powodujące, że wyboru dokonują decydenci. Przy budowie scenariusza ważne jest określenie początku zdarzenia (chwila zerowa), efektów kaskadowych (jeżeli są) oraz końca zdarzenia. Na ogół przyjmuje się, że zdarzenie kończy się w chwili, gdy przestaje „produkować” swoje skutki. To ostateczne stwierdzenie oczywiście nie oznacza końca fazy reagowania. Dotyczy tylko zdarzenia. Przy budowie scenariusza należy również uwzględnić zmienne i ich wartości. Uwzględnia się przy tym skutki krótko- i długoterminowe. Na podstawie podanego wyżej opisu tworzy się całkowitą narrację scenariusza.

3.4. Opis wpływu zdarzenia na procesy krytyczne

Ten krok identyfikuje procesy, które w wyniku wystąpienia zdarzenia mogą ulec zakłóceniu. Sens tego kroku ilustruje poniższa tabela.

Tabela 3. Przykłady możliwych zakłóceń procesów funkcjonowania społeczności lokalnej.

sektor	przykłady funkcji społecznych
energetyka	produkcja i dystrybucja
obsługa finansowa	płatności, dostęp do gotówki, centralny system płatniczy, ciepłownictwo, paliwo itp.
handel i przemysł	budownictwo, sprzedaż detaliczna, produkowanie
zdrowie i opieka medyczna	serwis karetek pogotowia, dostawa leków i sprzętu medycznego, opieka nad dziećmi, niepełnosprawnymi i osobami starszymi, dostęp do lekarzy, opieka nad zwierzętami itp.
informacja i komunikacja	dostęp do: łączności telefonicznej, internetowej, radiowej, poczty elektronicznej, druk i dystrybucja dzienników, stron web, mediów socjalnych
lokalne techniczne serwisy	dostarczanie świeżej wody, sprawność kanalizacji, sprawność urządzeń sanitarnych, przejezdność dróg itp.
dostawa żywności	dystrybucja, produkcja, inspekcja, wytwarzanie itp.
administracja publiczna: – zarządzanie – wspomaganie	lokalna, regionalna, rządowa, serwis pogrzebowy, dyplomacja i obsługa konsulatów
ochrona, bezpieczeństwo	zakłócenia funkcjonowania sądownictwa, prokuratury, obrony, więziennictwa, straży granicznej, policji, straży pożarnej, kontrola emigrantów, służb i straży innego typu itp.
bezpieczeństwo społeczne	zakłócenia systemu emerytalnego, zakłócenia systemu ubezpieczeń (zdrowotnych i związanych z bezrobociem)
transport	zakłócenia ruchu lotniczego, kolejowego, morskiego, transportu drogowego i publicznego

Również w tym kroku można poszukiwać odpowiedzi na dodatkowe pytania, takie jak np.:

- Czy system alarmowania jest sprawny?
- Ile podmiotów i które uruchomione są podczas alarmowania?
- Czy istnieje plan współdziałania podmiotów i ich koordynacji?
- Kto współpracuje z kim?
- Kto pełni rolę wiodącą? itd.

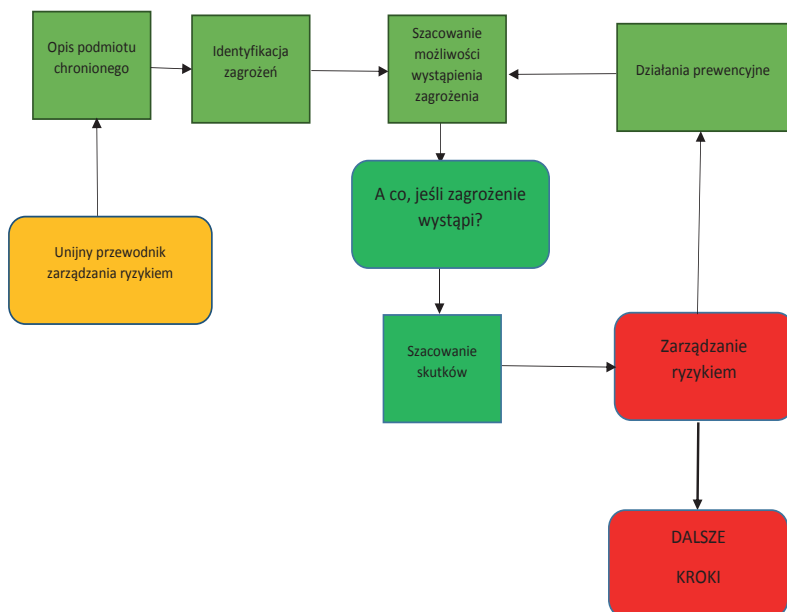
3.5. Opis skutków i oceny podatności wraz z oceną możliwości reagowania

W zasadzie krok ten służy do uszczegółowienia scenariusza o takie kwestie, jak to, jakie są wzajemne zależności poszczególnych struktur i funkcji. W tym właśnie kroku określa się również czułość poszczególnych systemów funkcjonowania społeczności na dane zagrożenie. Sprawdza się, czy wszystkie wartości, które powinny być chronione, zostały uwzględnione w scenariuszu. Dokonuje się również oceny możliwości reagowania na dane zagrożenie, ze względu na skutki. Ponadto ocenia się, czy te możliwości ze względu na skutki są akceptowalne, czy też nie. Ta ocena powinna dotyczyć nie tylko możliwości reagowania, ale również działań prewencyjnych. O ile szacując ryzyko, mowa jest o skutkach jednego z możliwych rodzajów ryzyka, o tyle przy rozpatrywaniu określonego ryzyka, związanego z danym zagrożeniem, analizuje się podatność poszczególnych elementów systemu chronionego na dany rodzaj zagrożenia. Dlatego też przy budowie „scenariusza najgorszego przypadku” należy określić właśnie podatność na ten rozważany przypadek i dokonać hierarchizacji.

W praktyce oceny możliwości zarządzania ryzykiem dokonuje się dla scenariusza najgorszego przypadku dla każdego zagrożenia oddzielnie.

Podsumowując dotychczasowe rozważania, można skonstruować schemat zilustrowany na rys. 4.

Rys. 4. Schemat zarządzania ryzykiem



W opisywanej koncepcji zarządzania ryzykiem jako dalsze kroki proponuje się procedurę pozwalającą na określenie mierników efektywności zarządzania. Mierniki te odnosi się do skutków zdarzenia. Poniżej zilustrowano przykładowo zdarzenie, które pociągnęło za sobą następujące skutki:

1. ofiary śmiertelne,
2. ranni,
3. duże zniszczenia,
4. zakłócenia w funkcjonowaniu niektórych instytucji,
5. trudności dotarcia do pracy.

Z punktu widzenia reagowania, każdy z tych skutków mógł powstać i często w rzeczywistości powstaje w wyniku niedoskonałości zarządzania ryzykiem. W tym konkretnym przypadku oznacza to, że nie odniesiono stuprocentowego sukcesu. W metodzie BSR przyjmuje się pięć wymiarów, względem których mierzy się efektywność działań. Są to: PRZYWÓDZTWO, WSPÓŁPRACA, ŁĄCZNOŚĆ, ZASOBY i WIEDZA. Ponieważ każdy z tych wymiarów ma inny wpływ na wielkość skutków, każdemu z nich można przypisać inną wagę. Aby tego dokonać, proponuje się zbudowanie matrycy zwanej CODI MATRIX (od angielskiego **C**onsequences **D**imensions), tj. skutki versus wymiary.

Tabela 4. Przykład CODI Matrix¹³

	Ofiary śmiertelne	Ranni	Duże zniszczenia	Zakłócenia w funkcjonowaniu instytucji	Trudności w dotarciu do pracy
przywództwo				X	
współpraca	X		X	X	
łączność	X	X			
zasoby		X	X		
wiedza					X

Analiza Matrycy CODI pokazuje, że w tym przypadku największym, można by rzec, ciężarem gatunkowym (wagą) obarczony jest wymiar „współpraca”. Nie tylko miał (lub może mieć) wpływ na liczbę ofiar śmiertelnych, ale również ma wpływ na dwa inne rodzaje skutków, mianowicie na: „duże zniszczenia” i „zakłócenia w funkcjonowaniu instytucji” (łącznie na trzy rodzaje spośród 9

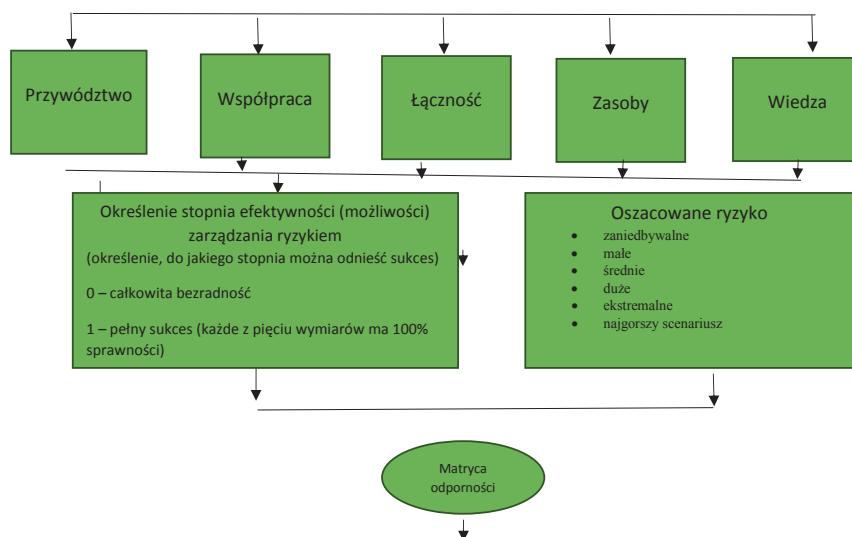
¹³ Risk Management Capability Based on Gaps Identification...

zaznaczonych na matrycy). Tak więc waga tego wymiaru wynosi $3/9 = 1/3$. Postępując podobnie z innymi wymiarami, otrzymujemy następujące wagi: „łączność” i „zasoby” mają wagi $2/9$, natomiast „wiedza” i „przywództwo” – po $1/9$. Analizując jednak ważność wymiarów, wyraźnie widać, że wkład w najpoważniejsze skutki mają wymiary „współpraca” i „łączność”.

Po przypisaniu wag eksperci (stosując jedną z metod eksperckich) określają efektywność poszczególnych wymiarów. Należy podkreślić, że opisane powyżej wagi wskazują na „wkład” poszczególnych wymiarów w zaostrenie skutków, ale nie charakteryzują efektywności zarządzania, a właśnie tę ostatnią oceniają eksperci w skali od 1 – gdy efektywność zarządzania jest 100%, do 0 – gdy występuje całkowity brak efektywności. I tak, niech wymiar „przywództwo” oceniony zostanie na 95%, „współpraca” na 85%, „łączność” na 65%, „zasoby” na 80%, „wiedza” na 70%. Wówczas można obliczyć średnią ważoną wszystkich wymiarów: $95\% \times (1/9) + 85\% \times (1/3) + 65\% \times (2/9) + 80\% \times (2/9) + 70\% \times (1/9) = 96\%$. Wynik oznacza, że efektywność (zdolność) zarządzania ryzykiem została w tym przypadku oceniona na 96%.

Przeprowadzając podobną analizę dla każdego zagrożenia, otrzymuje się efektywność zarządzania ryzykiem związaną z konkretnym zagrożeniem. Z tym konkretnym zagrożeniem związane jest ryzyko, które powinno być oszacowane zgodnie z przedstawioną tutaj metodyką. Na rys. 5 przedstawiono schematycznie omówioną powyżej procedurę.

Rys. 5. Procedura oceny efektywności zarządzania wraz z Matrycą Odporności (Matryca Sytuacji Kryzysowej)



1.0	bardzo duża odporność			średnia odporność		
0.8	(brak możliwości wystąpienia sytuacji kryzysowej)					
0.6		duża odporność		mała odporność		
0.4	w	(mała możliwość wystąpienia sytuacji kryzysowej)	(możliwość wystąpienia sytuacji kryzysowej)	(duża możliwość wystąpienia sytuacji kryzysowej)	zawsze sytuacja kryzysowa	
0.2						
	zaniedbywalne	małe	średnie	duże	ekstremalne	najgorszy scenariusz

Jak widać z powyższego rysunku, znając wielkość ryzyka i efektywność zarządzania, można określić wielkość odporności dla każdego zagrożenia.

Warto przy okazji poczynić kilka uwag. Scenariusze opisowe służące do oceny ryzyka sytuacji kryzysowej na każdym szczeblu jednostki administracyjnej, co do swojej konstrukcji, nie różnią się w sposób istotny. Różna jest tylko skala. Stąd wynika, po pierwsze, że istnieją sytuacje kryzysowe obejmujące dany szczebel administracji publicznej, a nie będące sytuacją kryzysową na szczeblu wyższym. Po drugie, na każdym szczeblu administracji powinno się tworzyć scenariusze opisowe na podstawie już zagregowanych danych zgromadzonych we własnych bazach. Wreszcie, czym wyższy szczebel, tym bardziej szacowanie ryzyka jest bliższe „najgorszemu scenariuszowi”. Np. województwa szacują ryzyko związane z powodzią tylko dla dużych zlewni.

Jeżeli chodzi o szacowanie ryzyka związanego z zagrożeniem narodowym, dokonywane w poszczególnych resortach, to ze względu na skalę zagrożeń opisane tutaj metody określania prawdopodobieństw i skutków nie mają zastosowania, chociaż sam scenariusz opisowy, co do swojej konstrukcji, nie powinien się różnić. Opis np. pandemii również powinien zawierać opis skutków. Metoda określania zagrożenia narodowego nie obejmuje szacowania prawdopodobieństwa wystąpienia zagrożenia, lecz przy nieznanym prawdopodobieństwie rozpatruje się różne możliwe scenariusze z nim związane, wykorzystując teorię gier, w szczególności gry z naturą.

Bibliografia

Literatura:

- Cretney R.M., *Local responses to disaster. The value of community led post disaster response action in a resilience framework*, [w:] "Disaster Prevention and Management" Vol. 25, No. 1, 2016, s. 27–40.
- Guiding and Tailoring Risk Assessment for the Baltic Sea Region* (praca zbiorowa), [w:] 14.3 Project implemented under EU Strategy for Baltic Sea Region (EUSBSR Action Plan) RED BOOK 2013.
- Mitchell J.K., Showalter P.S. (1998), *Long road to recovery*, [w:] *Community responses to industrial disaster*, edited by James K. Mitchell, The United Nation University 1996.
- Sandman P.M., *Responding to community outrage: Strategies for effective Risk Communication*, American Industrial Hygiene Association Fairfax, Va. Fourth Printing 1997.
- Sharifi A., *A critical review of selected tools assessing community resilience*, [w:] "Ecological Indicators" Volume 69, October 2016, s. 629–647.
- Showalter P.S., *Responding to "unconventional" millennial prediction*, [w:] "Disaster Prevention and Management" Vol. 7, No 4, 1998, s. 273–280.
- Skomra W. (red.), *Metodyka analizy ryzyka do stosowania na różnych poziomach zarządzania kryzysowego*, [w:] *Metodyka oceny ryzyka na potrzeby zarządzania kryzysowego RP*, SGSP, Bell Studio 2015, s. 121–215.
- Szopa T., *Koncepcja graficznego przedstawiania terytorialnego rozkładu ryzyka i zagrożeń*, [w:] *Mapy terytorialnego rozkładu ryzyka* (oprac.), Politechnika Warszawska, Szkoła Główna Służby Pożarniczej, 2004.
- UNEP-APELL *Hazard identification and evaluation in a community*, UNEP-APELL, Technical Report, 12 12 (with support of Swedish government), 1988.
- Risk Management Capability Based on Gaps Identification in the BSR*, "From Gaps to Caps". The project was implemented in the following countries: Denmark, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, Norway, Poland and Sweden. Starting date: 2015-01-01; Ending date: 2016-12-31.

Wykaz tabel:

- Tabela 1. Przykładowy wykaz źródeł zagrożeń.
- Tabela 2. Przykładowe skutki uwolnienia substancji niebezpiecznej.
- Tabela 3. Przykłady możliwych zakłóceń procesów funkcjonowania społeczności lokalnej.
- Tabela 4. Przykład CODI Matrix.

Wykaz rysunków:

- Rys. 1. Ogólny schemat szacowania ryzyka.
- Rys. 2. Podział zagrożeń ze względu na częstotliwość pojawienia się zdarzeń niekorzystnych.
- Rys. 3. Przykładowa Matryca Ryzyka.
- Rys. 4. Schemat zarządzania ryzykiem.
- Rys. 5. Procedura oceny efektywności zarządzania wraz z Matrycą Odporności (Matryca Sytuacji Kryzysowej).

Streszczenie

W artykule na podstawie rezultatów trzech projektów badawczych przedstawiono koncepcję szacowania ryzyka. Wskazano sposób konstruowania Matrycy Ryzyka na podstawie metody scenariuszowej. Opisano procedurę oceny możliwości zarządzania oszacowanym ryzykiem. Podano sposoby pomiaru odporności i konstrukcji Matrycy Odporności.

Słowa kluczowe: ryzyko, szacowanie ryzyka, zarządzanie ryzykiem, matryca ryzyka, matryca odporności.

Summary

How to measure the resilience of the local society

At the article a concept of risk assessment based on three international projects is presented. Taking into account scenario method the way of Risk Matrix creation is considered. Procedure of assessing of risk management possibility is described. The resilience measurement methods and Resilience Matrix designing are illustrated.

Key words: risk, risk assessment, risk management, risk matrix, resilience matrix.

Rozdział IV.

Stan bezpieczeństwa państwa pochodną procesu podejmowania decyzji w administracji publicznej

1. Wprowadzenie

W pierwszej połowie XX wieku rozmiar, liczba pełnionych funkcji i zakres władzy państwa rosły, a przyrost i nieefektywność wykonywanych procesów i ich skutki zrodziły żywiołową reakcję w postaci thatcheryzmu i reaganizmu. Zwiększająca się niewydolność sektora publicznego doprowadziła do reorientacji liberalnej doktryny gospodarczej, a jej zasady przeniesiono także na sferę dóbr i usług publicznych. Podstawowe cechy reorientowanej doktryny to:

- przejście przez władze publiczne odpowiedzialności za kluczowe dziedziny życia publicznego;
- przyjęcie odpowiedzialności formalnej za funkcjonowanie przejętych dziedzin publicznych, polegające na stworzeniu przez władze publiczne efektywnego i elastycznego systemu wytwarzania oraz dostarczania określonych usług zaspakajających potrzeby społeczne;
- odpowiedzialność materialna władzy publicznej w zakresie dostarczania określonych usług publicznych, wiążąca się z koniecznością ich finansowania ze środków publicznych, pochodzących głównie z podatków¹.

Dr hab. inż. Bogdan Kosowski – Uniwersytet Jagielloński w Krakowie.

¹ S. Owsiak, *Finanse publiczne. Teoria i praktyka*, PWN, Warszawa 1999, s. 29.

Stąd też w artykule rozważana jest problematyka odnoszącą się do państwa jako suwerennej organizacji politycznej, społeczeństwa zamieszkującego terytorium o określonych granicach, którego głównym składnikiem jest władza publiczna. Rząd konstytucyjny natomiast jest wynikiem świadomego zamysłu ograniczenia uprawnień władzy sprawowanej przez państwo. Streszcza to zasada „rządy prawa, nie ludzi” powszechnie przypisywana Arystotelesowi, na co w obecnym ustroju Polski między innymi zwraca uwagę Konstytucja RP, w której art. 7 wskazuje się: „Organy władzy publicznej działają na podstawie i w granicach prawa”. Ma to zasadnicze znaczenie z punktu widzenia efektywności funkcjonowania nie tylko administracji publicznej, lecz przede wszystkim poszczególnych podmiotów prawnych i fizycznych działających w państwie, co niestety w wielu przypadkach jest ignorowane przez pracowników administracji publicznej. Prawo bowiem „nie rządzi” samo. Rządzą, chociaż obecnie bardziej odpowiednim słowem jest „zarządzają”, ludzie, którzy zajmują określone pozycje w strukturze państwa, jako organizacji uwzględniającej podział w zależności od funkcji genotypowej. Zgodnie bowiem z rolą, jaką spełniają organizacje w zaspokajaniu potrzeb społecznych, dzielimy je na:

- gospodarcze, działające na podstawie zasady ekonomiczności;
- służące zaspokajaniu niematerialnych potrzeb społeczeństwa;
- administracyjne ogólnopaństwowe i lokalne;
- społeczne i religijne².

Źródłem prawa i wartości jest więc społeczeństwo, a wpływ na nie wywierają elementy struktury społecznej. Na poziomie państwa jako organizacji społeczno-politycznej prawo jest aktywnie kształtowane przez hierarchiczną strukturę władzy. Stąd też rolę przywódcy w sensie instytucjonalnym należy wyraźnie oddzielić od roli przywódcy w sensie interpersonalnym, co sprawia, że organizacja powinna działać sprawnie i efektywnie³. W instytucjach publicznych bowiem wykonywane są zadania przez osoby wyposażone w uprawnienia, zajmujące określone pozycje w administracji rządowej i samorządowej, z zachowaniem zasady: „Samorząd terytorialny uczestniczy w sprawowaniu władzy publicznej, a przysługującą mu w ramach ustaw istotną część zadań publicznych, samorząd wykonuje w imieniu własnym i na własną odpowiedzialność”⁴.

² M. Bielecki, *Organizacja. Istota, struktury, procesy*, Wyd. UŁ, Łódź 1992, s. 96.

³ F. Fukuyama, *Budowanie państwa. Władza i ład międzynarodowy w XXI wieku*, Dom Wydawniczy REBIS, Poznań 2005, s. 98.

⁴ Konstytucja Rzeczypospolitej Polskiej z dnia 6 kwietnia 1997 r., art. 16.

2. Teoretyczne podstawy zarządzania w administracji

Za twórcę zarządzania w administracji uważa się powszechnie H. Fayola, który pogrupował czynności administracyjne w takie funkcje jak:

- przewidywanie, badanie przyszłości i ustalenie odpowiedniego do niej programu działania;
- organizowanie, tworzenie materialnego i społecznego organizmu podmiotu;
- rozkazywanie, oddziaływanie na jednostki;
- koordynowanie, jednoczenie i harmonizowanie wszystkich czynności i wysiłków;
- kontrolowanie, czuwanie nad tym, aby wszystko odbywało się w zgodzie z przyjętym wzorcem.

Ustalił ponadto, że każda grupa czynności wykonywana w organizacji wymaga specyficznych uzdolnień, które w instytucjach mają zasadnicze znaczenie dla kierowników wysokiego szczebla. Kierować bowiem to znaczy przewidywać i wskazywać przyszłe cele, nie zawsze pewne, co warunkuje, że dobry menedżer stojący na czele organizacji musi mieć odwagę podejmowania ryzyka i ponoszenia odpowiedzialności. W innym przypadku może on być jedynie urzędnikiem, który sprawuje władzę kierowniczą, zubażając przy tym siebie i podwładnych⁵.

Kierunek administracyjny w teorii organizacji i zarządzania wiąże się także z badaniami niemieckiego uczonego, socjologa, ekonomisty i metodologa nauk społecznych M. Webera, którego powszechnie kojarzy się z koncepcją idealnego typu organizacji biurokratycznej. Za typ idealny uważa on celowo obmyśloną, abstrakcyjną konstrukcję, opisującą strukturę i zasady funkcjonowania instytucji „doskonale racjonalnej”, do których zalicza się między innymi:

- czynność urzędową, która jest działalnością stałą, a jej zakres jest określony stosownymi uregulowaniami prawnymi;
- kompetencję, która oznacza wyraźne rozgraniczenie sfer uprawnień i obowiązków urzędowych;
- hierarchię urzędową, która wyraża się w odpowiedzialności urzędników niższych instancji wobec urzędników wyższych instancji;
- działalność urzędową opartą na dokumentowaniu wszystkich czynności realizowanych na podstawie utrwalonych pisemnie formalnych przepisów;
- oddzielenie urzędników od własności środków administracji i środków utrzymania.

⁵ Zob.: H. Fayol, *Administracja przemysłowa i ogólna*, INOik, Poznań 1947, s. 37 i nast.

Weber założył sprawne i wolne od zakłóceń funkcjonowanie administracji, do której mniej lub bardziej mogą zbliżyć się organizacje realnie funkcjonujące⁶. Każde odchylenie od założonego modelu jest niesprawnością działania. W tym przypadku biurokracja jest nie tylko typem idealnej instytucji, ale także sposobem sprawowania władzy organizacyjnej, a jedynie władza racjonalna może być stosowana elastycznie. Tylko ją można bez większych komplikacji nadawać, przekazywać, odbierać, zwiększać i uszczuplać. Pojawia się zatem sens odróżnienia zakresu aktywności państwa obejmującego zbiór rozmaitych funkcji i celów, począwszy od siły władzy państwowej, tzn. zdolności państwa od planowania i realizowania polityki do egzekwowania prawa w sposób jasny, dla wszystkich zrozumiały⁷, co nazywane jest potencjałem państwa i jego instytucji.

Obecnie w wielu krajach zagadnienia te rozpatrywane są w ramach tzw. subdyscypliny: zarządzanie bezpieczeństwem publicznym, które zapoczątkowane zostało przez Amerykańskie Stowarzyszenie Administracji Publicznej (ASPA) oraz pracowników i przedstawicieli uczelni i wydziałów w dziedzinie zarządzania. Podkreślają oni adekwatność metod zarządzania ogólnego w administracji publicznej, między innymi w odniesieniu do projektowania organizacji, motywowania, wydajności, przywództwa i zarządzania strategicznego.

Rozwój teorii i praktyki zarządzania w administracji publicznej, niewątpliwie powiązanego z zarządzaniem bezpieczeństwem, wiąże się z działaniami, które powinny zapewnić efektywność systemu, jako rezultat podjętych działań opisanych relacją uzyskanych efektów do poniesionych nakładów. Efektywność należy rozpatrywać w dwóch aspektach:

- sprawności, co oznacza „robienie rzeczy we właściwy sposób”. Umiejętność właściwego działania, która związana jest z nakładami i efektami. Sprawne działanie to minimalizowanie kosztów nakładów zużytych do osiągniętych celów;
- skuteczności, co oznacza „robienie właściwych rzeczy”. Umiejętność wyboru właściwych celów.

Można tego dokonać, modyfikując istniejące struktury organizacyjne oraz nowe rozwiązania prawne. Obowiązek ten spoczywa na administracji publicznej, co wynika bezpośrednio z przyjętej koncepcji funkcjonowania państwa. Wypełniając to zadanie, państwo powinno posiadać dobre, transparentne i właściwe dla każdej sytuacji prawo, sprawną administrację współpracującą z wszelkimi podmiotami oraz sprawnie działające służby. Podejście takie wskazuje na podsta-

⁶ Zob.: R. Bendix, *Max Weber. Portret uczonego*, PWN, Warszawa 1975, s. 378 i nast.

⁷ B. Kosowski, *Sprawne i elastyczne zarządzanie w kryzysie*, Difin, Warszawa 2008, s. 48.

wową zasadę, jaką jest cykl działania zorganizowanego wszystkich niezależnych podmiotów systemu.

Zasada ta nie ma sobie przeciwstawnej w odniesieniu do antynomii sprawnego działania, gdzie wyróżnia się pary⁸: specjalizacja – uniwersalizacja, aktywizacja – ograniczenie działań, oczekiwanie właściwej chwili (kunktacja) – antycypacja, utrzymywanie określonego poziomu zasobów – pełne wykorzystanie zasobów, koncentracja sił – zabezpieczenie wszystkich kierunków działania. Specjalizacja w pewnych sytuacjach (według podziału zadań) usprawnia działanie w czasie i przestrzeni, w innych zaś usprawnia kumulowanie działań na mniejszej przestrzeni i rozszerzonej specjalizacji. Nadmierna specjalizacja wiąże się często z brakiem uniwersalnej wiedzy, czym charakteryzują się wybitni specjaliści w konkretnej dziedzinie, co czasami powoduje obniżenie sprawności działania pracy zespołowej. Nadmierna uniwersalizacja jest również niebezpieczna, bowiem często staje się formą wszechstronnego dyletantyzmu.

Z kolei aktywizacja działań polega na jak najbardziej czynnym zachowaniu się z wykorzystaniem całej swojej energii. Przeciwstawnym aktywizacji są ograniczenia przyjmujące różne formy działań. Odwrotnością oczekiwania właściwej chwili jest antycypacja polegająca na uprzedzaniu okoliczności, które wpływają na sprawność działania w przyszłości. Podobnie zresztą jak posiadanie rezerw czy też wybranie pola działania i skoncentrowanie na nim całej uwagi i zasobów, związane z zabezpieczeniem kierunków działania.

Przedstawione zasady sprawnego działania są ogólnymi i uniwersalnymi. Stanowią normatywną część prakseologii stosowaną przy wszelkich rodzajach działań, adaptowaną przez nauki organizacji i zarządzania. W każdym przypadku stosowania antynomii sprawnego działania trzeba ocenić, która z zasad dominuje, i ustalić sposób działania leżący między dwoma skrajnościami, jak to się stosuje np. w administracji publicznej funkcjonującej w systemie scentralizowanym bądź zdecentralizowanym.

W społeczeństwie scentralizowanym prawdopodobieństwo ryzyka systemowego jest równe prawdopodobieństwu błędnej decyzji podejmowanej przez władzę publiczną. Każda błędna decyzja dotyczy nie tylko jednej sfery, a co najmniej kilku podsystemów, a jeśli poszczególne etapy kontroluje jeden biurokrata, to pomyłka staje się bardziej prawdopodobna. Wówczas przedstawiciele państwa nie rozdzielają ryzyka, tylko je kumulują. Nie tworzą warunków do samoregulacji, lecz dążą do administrowania wszystkim, przenosząc przy tym swoje decyzje na podwładnych. Wtedy efektywność zarządzania

⁸ W. Kieżun, *Sprawne zarządzanie organizacją*, SGH, Warszawa 1997, s. 23.

zdecydowanie maleje, a tym samym maleje także poziom bezpieczeństwa, będącego jednym z zasadniczych działań państwa. Bezpieczeństwa, które od transformacji ustrojowej nabrało nowego znaczenia, a które obecnie nie może być postrzegane jedynie jako ochrona przed klasycznymi zagrożeniami. Na globalny poziom bezpieczeństwa mają bowiem wpływ zagrożenia⁹ technologiczne, społeczne, ekonomiczne i inne (rys. 1) bezpośrednio odczuwane przez społeczeństwo, którego rola jest znacząca. Systemy bezpieczeństwa bowiem bez zaangażowania społeczności lokalnych nigdy nie będą efektywne, a niestety w wielu przypadkach władza i administracja publiczna uważa, iż lepiej zna potrzeby i pragnienia społeczeństwa.

Rys. 1. Współczesne zagrożenia



Źródło: opracowanie własne

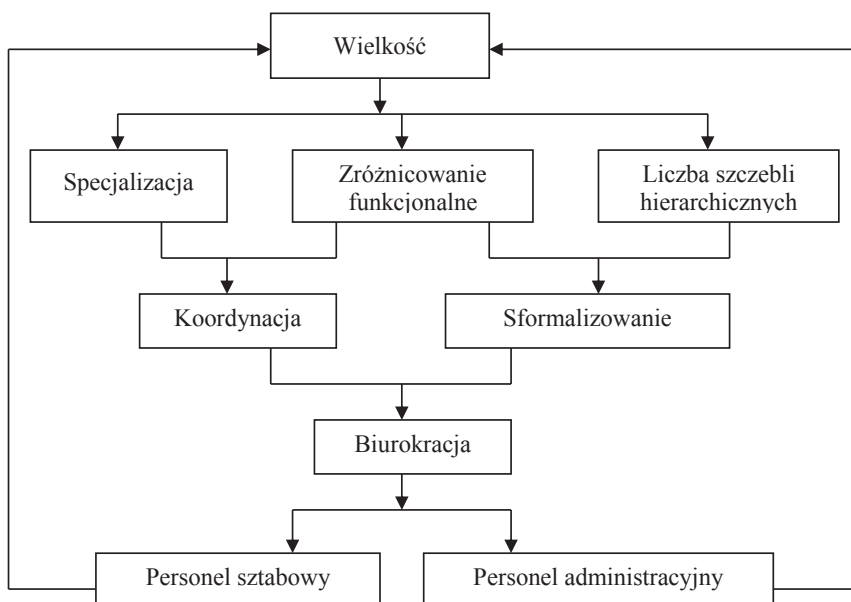
Ta sytuacja stawia przed administracją publiczną i wszystkimi podmiotami uczestniczącymi w systemie bezpieczeństwa nowe szczególne wymagania, zwrócone na spójność i przejrzystość na poziomie planowania i podejmowania działań. Sytuacje zagrożeń w jednym podsystemie powodują bowiem reperkusje niebezpieczeństw w innych podsystemach. Tym samym istnieje bezwzględna potrzeba integrowania wszystkich wyodrębnionych podsystemów funkcjonujących w państwie. Tak ważna dziedzina współczesnego życia nie może przecież być pozostawiona działaniu intuicyjnemu.

⁹ Badania ankietowe przeprowadzone zostały z wykorzystaniem techniki internetowej wśród społeczeństwa oraz ankiet dostarczonych do poszczególnych jednostek administracji publicznej szczebla gminnego, powiatowego i wojewódzkiego. Przy opracowywaniu wyników autor zastosował normalny rozkład prawdopodobieństwa.

3. System zarządzania w administracji publicznej

Z historycznego punktu widzenia reformowanie instytucji publicznych zazwyczaj owocowało sukcesem, kiedy w społeczeństwie istniał silny wewnętrzny popyt na te instytucje. Tworzono je wtedy na nowo, importowano lub adaptowano z obcych wzorców¹⁰. Tak też było i w Polsce, kiedy to w latach 90. ubiegłego wieku rozpoczął się proces decentralizacji władzy, a tym samym wprowadzenia wyższego poziomu uczestnictwa publicznego we władzy i szerszej kontroli nad nią. Niemniej jednak warto pamiętać, iż jednym z zasadniczych argumentów za centralizacją władzy politycznej jest konieczność istnienia ośrodka władzy, egzekwującego minimalne normy. Przyznanie większych uprawnień samorządom nieuchronnie prowadzi do lokalnego zróżnicowania efektów zarządzania. W wielu przypadkach administracja zdolna jest do osiągnięcia celów różnymi sposobami, co powoduje, że wzrasta rola procesów zarządzania, a wraz z nimi pojawia się biurokratyzowanie (rys. 2).

Rys. 2. Mechanizm biurokratyzowania



Źródło: opracowanie na podstawie: S. Galata, *Podstawy zarządzania nowoczesną organizacją. Ekonomia, kultura bezpieczeństwa, etyka*. Wydawnictwo Difin, Warszawa 2007

¹⁰ F. Fukuyama, *Budowanie państwa. Władza i ład...*, s. 50.

Większe uprawnienia związane są z kontekstowym charakterem każdej decyzji oraz większym stopniem zaufania, jakim zdecentralizowana organizacja musi obdarzyć podległe sobie jednostki, co bezpośrednio wpływa na proces podejmowania decyzji. W takim przypadku decyzje podejmowane są bliżej źródeł informacji i zazwyczaj lepiej rozwiązują sprawy lokalne, a organy władzy są bardziej wrażliwe i skuteczniejsze w reakcji na zmiany w otoczeniu. Efektywność działania nabiera szczególnego znaczenia zwłaszcza, gdy zmiany mają wyspecjalizowany charakter, bowiem proces podejmowania decyzji jest krótszy. Dodatkowo w przypadku, kiedy proces decentralizacji objął szereg jednostek, których uprawnienia poniekąd się pokrywają, to współzawodnictwo między jednostkami może dodatkowo sprzyjać sprawności oraz wysokiej jakości świadczonych usług publicznych¹¹.

Z cechami tymi wiąże się jednak bezpośrednio pomiar rezultatów funkcjonowania administracji, który jest bardzo istotny z punktu widzenia nieracjonalnego wydawania środków publicznych, bowiem ocena rezultatów działalności instytucji daje możliwość poprawy efektywności jej funkcjonowania. W przypadku kiedy decydent (władza) dysponuje niewielką ilością informacji o wynikach pracy, wtedy zazwyczaj wynagradza zatrudnionych pracowników na podstawie kryteriów: stażu pracy, wysokości budżetu i liczby pracowników danej instytucji. Członkowie tych organizacji nagradzani są za zachowania, które tak naprawdę należy uznać za nieudolne. Wykonują bowiem zadania tylko i wyłącznie sformalizowane, objęte narzuconymi odgórnie instrukcjami i ustaloną procedurą, choćby nawet miała zająć rozbieżność z interesem społecznym.

Takie zachowania odnoszą się zazwyczaj do personelu średniego, który wytrwale broni swoich posad, a z racji finansowania przez władzę ustawodawczą, domaga się większego budżetu, większej liczby pracowników i większych uprawnień. Ci pracownicy nie zastanawiają się, jak najlepiej realizować cele i poprawiać jakość i efektywność usług administracji publicznej¹². Postrzegają swoje zadania bardzo wąsko. Często czekają, aż problem, z którym powinni się uporać, nabrzmieje tak bardzo, że sytuacja stanie się kryzysowa, po czym oferują pomoc osobom dotkniętym już skutkami kryzysu. Wydają duże sumy pieniędzy na nowy rodzaj usług, nie obmyślając strategii zapobiegania problemom¹³. Reagują na sytuacje kryzysowe, czekając, aż zrobi się bałagan. Społeczeństwo będące klientem ma natomiast ograniczoną swobodę ruchu, jako że w dziedzinach,

¹¹ Tamże, s. 8.

¹² K. Opolski, *Służby i organy reagowania kryzysowego a zarządzanie jakością*, [w:] M. Jabłonowski, L. Smolak, *Zarządzanie kryzysowe w Polsce*, AH, Pułtusk 2007, s. 65.

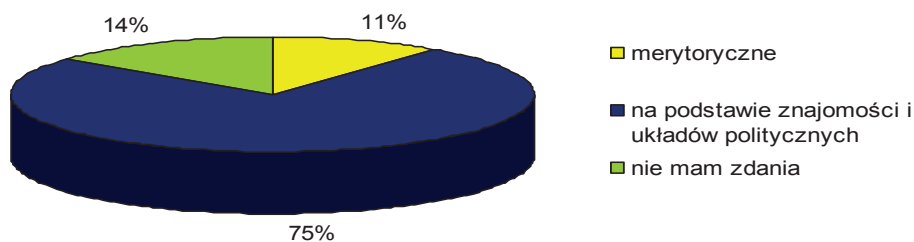
¹³ D. Osborne, T. Gaebler, *Rządzić inaczej. Jak duch przedsiębiorczości przenika i przekształca administrację publiczną*, Media Rodzina, Poznań 2005, s. 316.

w których administracja publiczna świadczy usługi, nie ma możliwości wyboru usługodawcy. Powoduje to, że administracja publiczna uczy się lekceważyć klienta, dbając jedynie o organy ustawodawcze, gdyż stamtąd otrzymuje fundusze.

Tak więc, podczas gdy instytucje prywatne starają się zadowolić klientów, administracja publiczna w wielu przypadkach stara się zadowolić grupy interesu¹⁴, funkcjonując w ramach tzw. błędnego koła biurokracji, mającego charakter sprzężenia zwrotnego. Przejawia się to potęgującymi się odchyleniami od wzorca, tym znacześniejszymi, im bardziej kierownictwo instytucji, typowymi biurokratycznymi narzędziami, przeciwdziałają negatywnym skutkom. Zjawisko takie występuje często w zhierarchizowanej strukturze, w sytuacji braku merytorycznych pracowników (rys. 3). Urzędnicy wykonują wtedy tylko te zadania, które otrzymują, i rzadko robią coś ponad nie. Zanika komunikacja pozioma. Pracownicy niższych szczebli nie są nagradzani za swoje osiągnięcia. Karani są za postępowanie wykraczające poza przestarzałe normy, mimo że ich działania znacznie lepiej służą interesom społecznym. Brak samorealizacji i perspektywicznego rozwoju powoduje obojętność, a często zmianę miejsca pracy najbardziej wartościowych pracowników.

Rys. 3. Merytoryczność w działaniu

Czy w administracji publicznej zatrudnione są osoby?



Źródło: opracowanie własne

Natomiast w komunikacji pionowej przełożeni stosują zasadę przekłamania oraz pozostawiania informacji dla samych siebie, co wpływa na nieracjonalność podejmowanych decyzji. Tym samym pojawiają się rozbieżności pomiędzy zadaniami i wynikami urzędników oraz celami i osiągnięciami organizacji, potęgując niezadowolenie usługobiorców, którzy coraz częściej oczekują dużej sprawności działania instytucji publicznych. Jesteśmy społeczeństwem coraz bardziej

¹⁴ Tamże, s. 236.

wykształconym, dzielimy się na coraz więcej podkultur. Różnimy się systemami wartości i stylem życia. Ze społeczeństwa masowego przekształciliśmy się w społeczeństwo będące mozaiką różniących się kulturowo warstw. Interesują nas usługi dostosowane do obecnego stylu życia i gustu, czego w wielu przypadkach nie oferują instytucje publiczne. Stąd też zanika obywatelskość, władza przez wielu jest ignorowana, a kiedy przychodzi z konieczności zetknąć się z sektorem publicznym, dochodzi do konfliktów i nieporozumień. W kontaktach z władzą najbardziej bowiem irytuje ludzi arogancja biurokracji, gdyż chcą być traktowani jak klienci, w sposób podmiotowy a nie przedmiotowy. Poziom zadowolenia jest jednak inny w różnych grupach społecznych, a wysoki poziom zadowolenia często bywa rezultatem małych oczekiwań¹⁵ i odwrotnie, niski poziom satysfakcji z usług publicznych może być spowodowany zbyt wygórowanymi, nierealistycznymi oczekiwaniami.

Społeczeństwo będące użytkownikiem usług publicznych nie stanowi jednolitej grupy, która oczekuje od administracji publicznej identycznego produktu. Przeciwnie, usługi publiczne dostarczane są różnym odbiorcom, w różnych obszarach i w różnych okolicznościach. Stąd zarówno menedżer instytucji publicznej, jak i polityk powinien posiadać zdolność rozróżnienia potrzeby i pragnień społeczeństwa, z pełną świadomością, że są one inne dla poszczególnych grup społecznych i różne niż oficjalnie przyjęte. Takie podejście prowadzi do ustalenia fundamentalnych potrzeb, określając, co jest pragnieniem, a co potrzebą priorytetową. Rodzą się postawy, które D. Champion i T. Cowdell zestawili w relacje, jakie zachodzą pomiędzy państwem, społeczeństwem i obywatelem.

Relacje te mogą być aktywne, bierno lub restrykcyjne. Kiedy administracja jest bierna, a odbiorca usług aktywny, to można zauważyć próby wymuszenia na administracji publicznej określonych działań ze strony usługobiorcy. W przypadku kiedy administracja jest aktywna, a użytkownik bierny, to państwo próbuje przekonać obywateli do proponowanego rozwiązania¹⁶. Zdarza się czasami, że bierny jest zarówno obywatel, jak również i państwo. Relacje te jednak w społecznościach rozwiniętych zachodzą rzadko i raczej krótkotrwale. Trudno jest w takim przypadku wyobrazić sobie funkcjonowanie państwa, z uwagi na występujące powiązanie społeczeństwa z państwem i władzą go reprezentującą. Tym bardziej że sektor publiczny posiada zobowiązania wobec społeczeństwa i w przypadku usług publicznych nie wystarczy wyjść naprzeciw wyrażonym pragnieniom, ale również należy znaleźć potrzeby nieartykułowane, ustalić priorytety, alokować

¹⁵ K. Opolski, *Służby i organy reagowania...*, s. 63.

¹⁶ K. Elefalk, *The Balanced Scorecard of the Swedish Police Service: 7000 officers in total quality management project*, "Total Quality Management" 2001, Vol. 12, no. 7 & 8, s. 959.

zasoby w sposób społecznie uzasadniony i wreszcie konieczne staje się rozliczenie z tego, co zostało zrobione¹⁷, a to zależy w dużej mierze od decydenta.

Stwierdzono, że „statystyczny decydent wykazuje istotne przejawy niesprawności, do których zalicza się: zbyt centralistyczny styl pracy, nieplanowość, spontaniczność, zbyt długie rozczłonowanie zdań, koncentrację na pracy operatywnej lub też konferencyjny styl pracy”¹⁸. Efektywnie działający decydent charakteryzuje się koncentracją na zagadnieniach strategicznych i pracy koncepcyjnej, korzystając z dużego zakresu przyznanych uprawnień, w niewielkim stopniu ograniczony jest aparatem formalnej kontroli. Właściwej decyzji nie da się sformalizować, gdyż u jej podstaw spoczywa zdolność oceny złożonej sytuacji, wiedza i doświadczenie. Dobry decydent, poza kształtowaniem pozytywnej atmosfery, a także poprawnym przepływem informacji, musi wiedzieć o tym, że czynnikiem, który przywiązuje pracownika do miejsca pracy i pozwala na poprawę wyników, jest również delegowanie na niego uprawnień, a także praca zespołowa w mało zhierarchizowanej strukturze. Zatwierdzanie każdej decyzji przez decydenta może prowadzić do spowolnienia pracy instytucji publicznej lub do całkowitego paraliżu, a odbiór społeczny takiej instytucji staje się wtedy niekorzystny. Pracownicy natomiast posiadający szerokie uprawnienia mają poczucie ważności pełnionych przez siebie funkcji i są w stanie zapewnić wysoką jakość obsłużenia interesantów.

Z racji faktu, że w instytucjach publicznych praktycznie nie istnieją sankcje za „niedobre praktyki”, suboptymalne układy administracyjne bardzo długo trwają nienaruszone i to między innymi staje się przyczynkiem do dyskusji nad alternatywnymi modelami administracyjnymi¹⁹. Być może warto się zastanowić nad stworzeniem innego systemu motywacyjnego w instytucjach publicznych. Systemu opartego na świadomości skracania czasu rozpatrywania spraw i podejmowania decyzji z uwzględnieniem interesu społeczeństwa. Przecież w państwie wolnorynkowym byt administracji publicznej, będącej sektorem nieprodukcyjnym, uzależniony jest od społeczeństwa, które nie powinno być zniechęcane do instytucji publicznych przez władze ją reprezentujące. Uważać bowiem będzie, że podejmowane decyzje nie mają na względzie uzyskania jak najlepszych rezultatów, ale zaspokojenie potrzeb określonych zorganizowanych grup społecznych. Działania władzy i administracji traktowane są wtedy jako zaspokajanie interesów grup²⁰, które zorganizowały się po to, by utrzymać to, co już zdobyły, ignorując

¹⁷ K. Opolski, *Służby i organy reagowania...*, s. 64.

¹⁸ W. Kieżun, *Sprawne zarządzanie...*, s. 225.

¹⁹ F. Fukuyama, *Budowanie państwa. Władza i ład...*, s. 101.

²⁰ D. Osborne, T. Gaebler, *Rządź inaczej. Jak duch przedsiębiorczości...*, s. 435.

przy tym interesy niezorganizowanych obywateli, którzy odnieśliby korzyści z wprowadzenia zmian. Tendencje takie umacniają środki masowego przekazu, koncentrując się bardziej na widowiskach politycznych, konfliktach, wyścigach do władzy, skandalach niż na istocie zarządzania. W wyniku takiego sposobu pojmowania władzy tworzy się sytuacja, w której ryzykowne jest przeprowadzenie jakichkolwiek zmian, a menedżerów administracji publicznej karze się bardziej za próby zmian niż za błędne decyzje przynoszące szkodę społeczeństwu i państwu.

4. Konkluzje

Zazwyczaj w instytucjach publicznych cele organizacji bywają mało wyraziste, wewnętrznie sprzeczne i słabo skonkretyzowane, co jest wynikiem wykonywania zadań tylko w jednym kierunku: „z góry w dół”. Taka organizacja działań rodzi problemy w postaci nadużycia władzy, korupcję, biurokratyczną inercję będącą efektem zachowań kierującego się własnym interesem przedstawiciela określonego szczebla administracji. W wielu przypadkach motywacja pracownika jest inna lub też inaczej rozumiana niż intencja mocodawcy, przez co następuje sprzeniewierzenie się władzy²¹. Organizacje kierujące się poczuciem misji i jasno sprecyzowanymi celami zostawiają natomiast swym pracownikom swobodę wyboru metod służących wypełnianiu misji i celów, co jest pożyteczne²² między innymi dlatego, że:

- organizacje kierujące się poczuciem misji są bardziej sprawne, skuteczne i pracują wydajniej niż te organizacje, które kierują się tylko przepisami;
- w organizacjach tych panuje wyższe morale, są skłonne do nowatorskich rozwiązań i są bardziej elastyczne.

Jak już wspomiano, administracja tradycyjna koncentruje się na zwalczaniu problemów. Dla przykładu, aby zwalczać przestępczość, zatrudnia się coraz więcej policjantów, aby uporać się z pożarami, kupuje się coraz więcej sprzętu strażackiego. Rzadko koncentruje się na prewencji, przyjmując misję świadczenia usług reagowania na zdarzenie. Jest to typowe działanie dla funkcjonowania administracji w tzw. modelu biurokratycznym, którego charakterystyczną cechą jest koncentracja na świadczeniu usług. Stąd też zdaniem autora warto podejmować próby przedyskutowania zmiany dotychczasowego modelu zarządzania admini-

²¹ F. Fukuyama, *Budowanie państwa. Władza i ład...*, s. 68.

²² D. Osborne, T. Gaebler, *Rządź inaczej. Jak duch przedsiębiorczości...*, s. 165.

stracją, wykonującą zadania określone przez władze publiczną, lecz świadcząca usługi dla społeczeństwa.

W tym celu niezbędne staje się stworzenie teoretycznych ram refleksji, czyli nowego sposobu myślenia o władzy, a tym samym stworzenie nowego paradygmatu²³ w nowoczesnej rzeczywistości społecznej²⁴, uwzględniającego zwiększenie odpowiedzialności pracowników administracji publicznej za podejmowane decyzje. Wtedy merytoryka działania nie ulegnie naciskom politycznym, które przecież zmierzają do ograniczenia uprawnień przedstawicieli sektora publicznego i stanowią sztywne oraz częstokroć irracjonalne przepisy powszechnie kojarzone z biurokracją. Pracownik ulegający naciskom zazwyczaj posiada małą wiedzę, a zasłaniając się przepisami, twierdzi, że uniemożliwiają mu one reagowanie w szybko zmieniających się okolicznościach, co doprowadza do marnotrawstwa czasu i wysiłku innych. Stąd też najślabszym ogniwem systemu jest człowiek. Tym bardziej że z jednej strony jesteśmy zwolennikami przepisów w takiej mierze, w jakiej zapobiegają one przykrym zdarzeniom, a z drugiej strony te same przepisy w wielu przypadkach uniemożliwiają rozsądne działania na rzecz zwiększenia efektywności i zwiększania poczucia bezpieczeństwa obywateli.

Bibliografia

Literatura:

- Bendix R., *Max Weber. Portret uczonego*, PWN, Warszawa 1975.
Bielecki M., *Organizacja. Istota, struktury, procesy*, Wyd. UŁ, Łódź 1992.
Elefalk K., *The Balanced Scorecard of the Swedish Police Service: 7000 officers in total quality management project*, "Total Quality Management" 2001, Vol. 12 no. 7 & 8.
Fayol H., *Administracja przemysłowa i ogólna*, INOIK, Poznań 1947.
Fukuyama F., *Budowanie państwa. Władza i ład międzynarodowy w XXI wieku*, Dom Wydawniczy REBIS, Poznań 2005.
Galata S., *Podstawy zarządzania nowoczesną organizacją. Ekonomia, kultura bezpieczeństwa, etyka*, Difin, Warszawa 2007.

²³ Paradygmat naukowy według Kuhana to zbiór założeń dotyczących rzeczywistości, tworzących ogólnie przyjęty jej model. Każdy paradygmat obejmuje zbiór praw i wyjaśnia pewien zbiór faktów. Dopóki wyjaśnia on większość obserwowanych zjawisk i pomaga w rozwiązywaniu problemów, które większość ludzi chce rozwiązać, jest modelem dominującym. Kiedy jednak pojawiają się nowe zjawiska, które stoją w sprzeczności z przyjętym paradygmatem, zaczyna on budzić coraz więcej wątpliwości. Gdy zjawisk niemożliwych do wyjaśnienia i traktowanych jako anomalie w ramach dotychczas obowiązującego paradygmatu przybywa, wchodzi on w fazę kryzysu. W końcu ktoś formułuje nowy paradygmat.

²⁴ S. Galata, *Podstawy zarządzania nowoczesną...*, s. 113.

- Kieżun W., *Sprawne zarządzanie organizacją*, SGH, Warszawa 1997.
- Konstytucja Rzeczypospolitej Polskiej z dnia 6 kwietnia 1997 r.
- Kosowski B., *Sprawne i elastyczne zarządzanie w kryzysie*, Difin, Warszawa 2008.
- Kuhn, Thomas S., *The Structure of Scientific Revolutions*, wyd. II, University of Chicago Press, Chicago 1970.
- Opolski K., *Służby i organy reagowania kryzysowego a zarządzanie jakością*, [w]: M. Jabłonowski, L. Smolak (red.), *Zarządzanie kryzysowe w Polsce*, AH, Pułtusk 2007.
- Osborne D., Gaebler T., *Rządzić inaczej. Jak duch przedsiębiorczości przenika i przekształca administrację publiczną*, Media Rodzina, Poznań 2005.
- Owsiak S., *Finanse publiczne. Teoria i praktyka*, PWN, Warszawa 1999.
- Strzelecki M., Zubrzycki W., Jurczak D., *Jaka administracja? Rozważania nad teorią i praktyką administracji polskiej po 1989 roku*, Wydawnictwo Uczelniane WSZiE TWP w Olsztynie.

Streszczenie

W artykule przedstawione zostały teoretyczne i praktyczne aspekty zarządzania w administracji publicznej, traktując państwo jako suwerenną organizację polityczną społeczeństwa zamieszkującego określone terytorium. Zwrócono uwagę na bardzo ważny element funkcjonowania administracji będącej aparatem władzy publicznej, jakim jest efektywność zarządzania i zadowolenie społeczeństwa z usług wykonywanych przez te instytucje. Określone zostały relacje między władzą a obywatelem w aspekcie teoretycznym oraz empirycznym, co pozwoliło na przedstawienie ogólnych trendów panujących obecnie w instytucjach publicznych, z równoczesnym wskazaniem na potrzebę sformułowania nowego naukowego paradygmatu funkcjonowania administracji, wykonującej zadania władzy publicznej.

Słowa kluczowe: władza, administracja, społeczeństwo, usługi, efektywność, zadowolenie.

Summary

State of the state security derivatives decision-making in public administration

The article presents the theoretical and practical aspects of management in public administration, treating the state as a sovereign political society, which inhabits the set territory. Attention is drawn to a very important element in the operation of the public administration, which is the effective management and public satisfaction with the services provided by these institutions. The relationships between authority and the citizen were set in theoretical and empirical aspect, which allowed to present the general trends, both in public institutions, while also indicating the need for formulation of a new scientific paradigm of the functioning of the administration which carrying out the public power tasks.

Key words: authority, public power, administration, public services, efficiency, satisfaction.

Rozdział V.

Nowoczesne techniki w służbie zarządzania kryzysowego – nauka, dydaktyka, praktyka

1. Pojęcie zarządzania kryzysowego w zarysie

W świecie, w którym zagrożenia naturalne przeplatają się z zagrożeniami technicznymi, będącymi konsekwencją rozwoju cywilizacyjnego¹, podlegamy oddziaływaniu szerokiej gamy zagrożeń. Decydenci odpowiedzialni za zapewnienie szeroko rozumianego bezpieczeństwa do najtrudniejszych sytuacji zaliczają te o charakterze kryzysowym. Kryzys jest zjawiskiem szczególnym, występującym w ramach ogólnego, czasami bardzo długiego procesu zmian występujących wokół nas. Mimo że w literaturze przedmiotowej można odnaleźć wiele definicji kryzysu², każdy zawiera załamanie funkcjonującego systemu – przestają sprawdzać się dotychczas istniejące zasady i procedury – jak również silną presję czasu i nieoznaczoność alternatywnych scenariuszy rozwoju zdarzeń, będących konsekwencją podejmowanych działań. Zarządzanie bezpieczeństwem obywateli w aspekcie ciągłego wzrostu liczby i intensywności występujących zagrożeń stało się nie lada wyzwaniem na początku XXI stulecia i w chwili obecnej jest

Prof. nzw. dr hab. Marcin M. Smolarkiewicz – Wydział Inżynierii Bezpieczeństwa Cywilnego, Szkoła Główna Służby Pożarniczej w Warszawie.

¹ J. Wojnarski, *Kryzys konsekwencją zagrożeń cywilizacyjnych*, [w:] *Zarządzanie kryzysowe w Polsce*, (red.) M. Jabłonowski, L. Smolak, Akademia Humanistyczna im. A. Gieysztora, Pułtusk 2007, s. 301–331.

² J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego. Cz. I. Zarządzanie kryzysowe w administracji publicznej*, Krakowska Akademia im. A. Frycza Modrzejewskiego, Krakowskie Towarzystwo Edukacyjne – Oficyna Wydawnicza AFM, Kraków 2010, s. 73–75.

typem zarządzania strategicznego³. W teorii zarządzania kryzysowego odchodzi się powoli od czterofazowego, ciągłego procesu zarządzania (w skład którego wchodzi zapobieganie, przygotowanie, reagowanie i odbudowa) na rzecz podejścia progresywnego⁴, polegającego m.in. na podejmowaniu szerszych działań w fazie przygotowania i zapobiegania, a nie poleganiu przede wszystkim na przeciwdziałaniu skutkom zdarzeń niekorzystnych, które już wystąpiły. Utrzymanie akceptowalnego poziomu ryzyka i wystarczającego poziomu bezpieczeństwa wymaga koordynacji działań wielu podmiotów zaangażowanych w proces niesienia pomocy w sytuacji wystąpienia zdarzenia niekorzystnego.

Każda klęska, katastrofa lub stan zagrożenia, które możemy określić mianem sytuacji kryzysowej, bez względu na przyczynę powstania dezorganizuje normalne życie, powoduje załamanie lub przeciążenie administracji i infrastruktury państwa lub jego części. Stan przygotowania państwa i jego obywateli na takie sytuacje można określić stopniem, w jakim wykazują oni gotowość do podjęcia kroków zmierzających do ochrony życia i mienia zarówno przed spodziewanym kataklizmem, jak i bezpośrednio po nim. W ujęciu analizy systemowej⁵ bezpieczeństwo można rozpatrywać jako własność obiektu charakteryzująca jego odporność na powstanie sytuacji niebezpiecznej. W takim ujęciu można mówić o zawodności bezpieczeństwa obiektu, czyli jego podatności na powstanie sytuacji niebezpiecznych. Zgodnie z przedmiotową literaturą zarządzanie kryzysowe jest jednym z bardziej złożonych rodzajów zarządzania. Zarządzanie kryzysowe w odróżnieniu od typowego zarządzania (w skład którego wchodzi fazy planowania, organizowania, motywowania i kontroli) charakteryzuje się tym, że⁶:

- jest integralną częścią zarządzania systemem,
- realizowane jest pod presją,
- związane jest z rozwiązywaniem napięć,
- stanowi przeciwdziałanie eskalacji kłopotliwych zjawisk,
- przeciwdziała konfliktom,
- dąży do przywrócenia stanu „normalnego”, odrzucając problemy marginalne.

³ A. Dawidczyk, J. Gryz, S. Koziej, *Zarządzanie strategiczne bezpieczeństwem. Teoria – Praktyka – Dydaktyka*, Wydawnictwo Wyższej Szkoły Humanistyczno-Ekonomicznej, Łódź 2006, s. 7–54.

⁴ P. Żebrowski, P. Abramowicz, A. Filipowska, D. Wróblewski, M.M. Smolarkiewicz, J. Wolanin, M. Wiśniewski, A. Bassara, *Progresive crisis management system*, [w:] The 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, USA, 2005, s. 419–424.

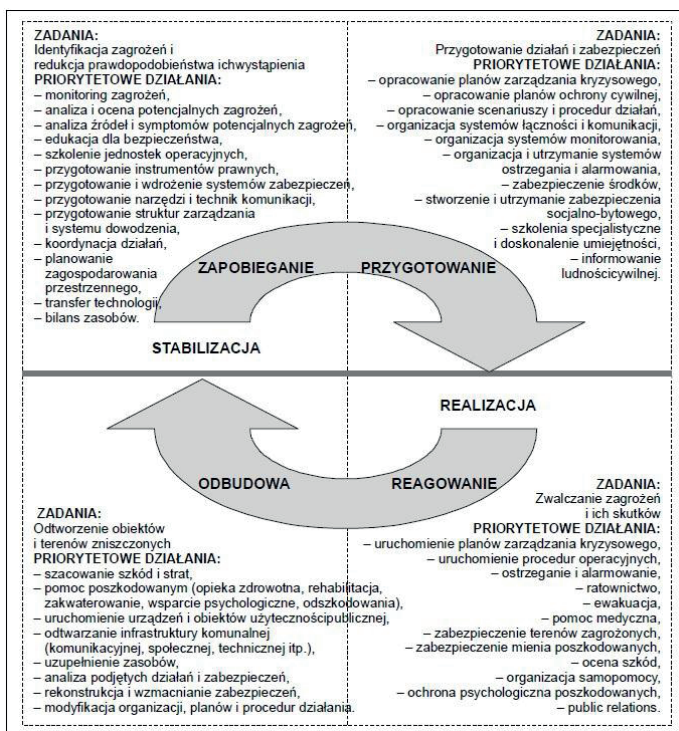
⁵ P. Sienkiewicz, *Badania naukowe bezpieczeństwa systemów*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżynieria działań w obszarze nauki, dydaktyki i praktyki*, (red.) B. Kosowski, A. Włodarski, Fundacja Edukacja i Technika Ratownictwa, Warszawa 2007, s. 41–52.

⁶ W. Lidwa, W. Krzeszowski, W. Więcek, *Zarządzanie w sytuacjach kryzysowych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2010, s. 31.

Mimo że sytuacje kryzysowe nie są powszechne, nie da się im całkowicie zapobiec. W razie ich wystąpienia szczególnie istotne staje się zapewnienie funkcjonowania najważniejszych elementów infrastruktury krytycznej państwa⁷.

W prawodawstwie polskim sytuacją kryzysową, zgodnie z art. 3 pkt 1 ustawy o zarządzaniu kryzysowym⁸ z dnia 26 kwietnia 2007 r., nazywa się „sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków”.

Rys. 1. Cykl 4-fazowego zarządzania kryzysowego



Źródło: M.M. Smolarkiewicz, *Teoria macryc stowarzyszonych i N-wymiarowa macryca bezpieczeństwa – nowe metody macrycowe na potrzeby zarządzania kryzysowego*, WSZiP, Warszawa 2013, s. 9, za: K. Sienkiewicz-Małyjurek. i F.R. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Wydawnictwo Difin, Warszawa 2010, s. 21

⁷ W. Wójtowicz, *Bezpieczeństwo infrastruktury krytycznej*, Ministerstwo Obrony Narodowej, Departament Polityki Obronnej, Warszawa 2006, s. 63–68.

⁸ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. nr 89, poz. 590 z późn. zm.).

Zgodnie z art. 2 tej ustawy „Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, które polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowania w przypadku wystąpienia sytuacji kryzysowych, usuwania ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej”. Z zapisu tego jasno wynika, że ustawodawca określa zarządzanie kryzysowe jako proces cykliczny złożony z czterech faz: zapobiegania, przygotowania, reagowania i odbudowy. Na rysunku (rys. 1) przedstawiono schemat 4-fazowego zarządzania kryzysowego⁹, wraz z opisem zadań realizowanych w ramach poszczególnych faz.

W literaturze przedmiotu niejednokrotnie przytaczano już i zbierano w jednym zestawieniu wiele różnych, aczkolwiek zwykle bardzo bliskoznacznych definicji pojęcia zarządzania kryzysowego¹⁰. Niezależnie od przyjętej definicji semantycznej, wartym i godnym podkreślenia jest tutaj fakt, że ustawa o zarządzaniu kryzysowym wprowadza do obszaru zarządzania kryzysowego i ochrony ludności zasady szczególnie istotne dla uporządkowania tego procesu¹¹:

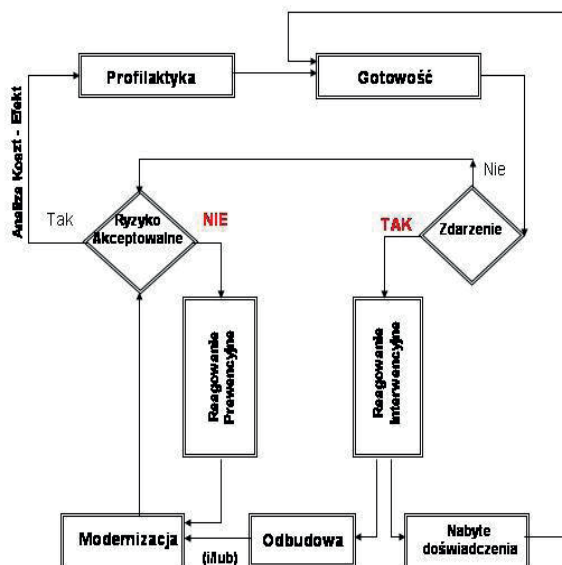
- prymatu układu terytorialnego;
- jednoosobowego kierownictwa i odpowiedzialności;
- kierowania i ponoszenia odpowiedzialności przez jednoosobowe organy sprawujące władzę administracji ogólnej;
- adekwatności w zakresie reakcji właściwego szczebla administracyjnego;
- powszechności;
- oddzielenia systemu gotowości cywilnej od gotowości militarnej.

⁹ K. Sienkiewicz-Małyjurek, F.R. Krynojewski, *Zarządzanie kryzysowe...*, s. 21.

¹⁰ Tamże, s. 11–12.

¹¹ W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, PRESSCOM, Wrocław 2010, s. 12.

Rys. 2. Fazy zarządzania kryzysowego – zarządzanie progresywne



Źródło: P. Żebrowski, P. Abramowicz, A. Filipowska, D. Wróblewski, M.M. Smolarkiewicz, J. Wolanin, M. Wiśniewski, A. Bassara, *Progressive crisis management system*, [w:] The 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, USA, 2005, s. 422

Wszystkie publikacje dziedzinowe podkreślają, że zarządzanie kryzysowe jest procesem ciągłym. W każdej z faz zarządzania kryzysowego podejmowane są decyzje, które w mniejszym lub większym stopniu wpływają na podatność na zagrożenia systemu podlegającego ochronie (zwykle w zarządzaniu bezpieczeństwem obywateli system taki sprowadza się do pojęcia społeczności lokalnej). Zarządzanie kryzysowe odbywa się zatem na szczeblach od lokalnego (gmina), przez pośredni (powiat, województwo) aż do centralnego (kraj). Wraz ze wzrostem szczebla zarządzania zmniejsza się rola bezpośredniego kierowania (dowodzenia), rośnie zaś rola koordynacji działań. Dzieje się tak, gdyż od działań na poziomie operacyjnym przechodzi się do działań na poziomie taktycznym i strategicznym. Uwzględnienie obu wyżej opisanych strategii w obszarze zarządzania kryzysowego nosi miano wspomnianego wcześniej zarządzania progresywnego (rys. 2), które to podejście stanowi kolejną alternatywę jego opisu.

2. Ujęcie naukowe wspomaganie zarządzania kryzysowego

Komputerowe wspomaganie procesu podejmowania decyzji jest jednym z elementów zarządzania bezpieczeństwem¹². Podejmowanie decyzji w sytuacjach, w których liczba czynników znanych i mierzalnych jest znacznie mniejsza od liczby czynników nieznanych lub niemierzalnych, wymaga zastosowania narzędzi wspierających zarządzanie informacją oraz jej ewaluację i agregację. Faktem jest, że rzeczywisty proces decyzyjny w swojej istocie z trudem podlega opisowi ilościowemu. Można określić pewne reguły decyzyjne i, działając zgodnie z nimi, wspomagać proces decyzyjny przez wybór najlepszych alternatyw z punktu widzenia wybranych kryteriów. Jednakże całkowicie matematyczny opis rzeczywistego procesu decyzyjnego jest praktycznie niemożliwy. Szczególnie trudno jest opisać proces decyzyjny w złożonych, wieloaspektowych sytuacjach, z jakimi mamy do czynienia podczas sytuacji kryzysowych.

Kolejnym czynnikiem wpływającym na trudność opisu rzeczywistego procesu decyzyjnego jest fakt, że osoba podejmująca decyzje w sytuacjach realnych bardzo często musi działać w warunkach niedoboru (lub chaosu) informacji oraz zwykle nie ma ona wystarczającej ilości czasu na przeprowadzanie dokładnych analiz lub przygotowanie się. Wreszcie wieloaspektowość sytuacji rzeczywistych, w szczególności sytuacji kryzysowych, podczas których wpływ na podejmowane decyzje mają inne czynniki, m.in. gospodarcze, polityczne, społeczne, ekologiczne i medialne, uniemożliwia skonkretyzowanie wzorca symulacyjnego procesu decyzyjnego oraz utrudnia ewaluację i prognozę konsekwencji (skutków) podejmowanych decyzji¹³. Zaistnienie sytuacji, w której grożą decydentowi negatywne i trudne do przewidzenia konsekwencje, może prowadzić do utraty racjonalności decyzji. Wpływ na to ma również istnienie tzw. „pułapek decyzyjnych” odnoszących się do sytuacji o charakterze kryzysowym w obszarze zarządzania bezpieczeństwem obywateli.

Za jedno z istotnych osiągnięć na drodze opisu procesu decyzyjnego można uznać teorię perspektywy¹⁴ (ang. *prospect theory*), która została sformułowana przez Daniela Kahnemana i Amosa Tversky'ego. Wnieśli oni do ekonomii dwa waż-

¹² M.M. Smolarkiewicz, *Koncepcje baz danych niezbędnych dla funkcjonowania struktur zarządzania kryzysowego (CPR, GCR)*, Elektroniczna Administracja, VI edycja konferencji „Teleinformatyczne standardy i procedury w zarządzaniu kryzysowym – narzędzia GIS-owskie oraz programy symulacyjne”, nr 3, maj–czerwiec 2006, s. 39–60.

¹³ T. Tyszka, *Psychologiczne pułapki oceniania i podejmowania decyzji*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1999, s. 51.

¹⁴ P. Kahneman, A. Tversky, *A Prospect Theory: An Analysis of Decision Under Risk*, „Econometrica”, tom 47, 1979, s. 263–292.

ne wątki dotyczące kontrolowania ryzyka i awersji do strat. Kahneman i Tversky pokazali w swoich badaniach, że ludzie w ocenach swoich szans zwykle nie kierują się zasadami logiki i rachunku prawdopodobieństwa. Najczęściej korzystają z łatwych w użyciu reguł – nierzadko okazują się one być wystarczające, chociaż mogą też w szczególnych sytuacjach prowadzić do poważnych błędów¹⁵. Okazuje się, że przy ocenie swoich szans ludzie chętnie kierują się zasadą dostępności psychicznej.

Zasada ta polega na tym, że ludzie wnioskuje o prawdopodobieństwach na podstawie własnego doświadczenia. Czynniki wpływającymi na dostępność zdarzeń w pamięci człowieka są przede wszystkim czas, który upłynął od wystąpienia, oraz sposób interpretacji wydarzeń przez środki masowego przekazu. Oprócz tego w procesie podejmowania decyzji istotne znaczenie ma sposób sformułowania pytania, czyli przyjęta perspektywa. Kahneman i Tversky przeanalizowali kształt funkcji wartości dla potencjalnych strat i dla możliwych zysków. Dzięki ich badaniom wiadome jest, że w sytuacji decyzji wielokryterialnej sposób przedstawienia problemu oraz jego ujęcie może wpływać na podejmowaną decyzję, co staje się istotnym aspektem w szczególności opisu procesu decyzyjnego w sytuacji kryzysowej.

Aby wspomagać proces decyzyjny w zarządzaniu kryzysowym, jako jedną z nielicznych inżynierskich metod wykorzystuje się analizę ryzyka. Istnieje wiele definicji ryzyka. Większość z nich można odnaleźć w pracach dotyczących zarządzania i ekonomii. W zarządzaniu bezpieczeństwem najczęściej korzysta się z ilościowej, inżynierskiej definicji ryzyka, określanego jako iloczyn prawdopodobieństwa wystąpienia zdarzenia niekorzystnego i jego spodziewanych skutków¹⁶. Ryzyko definiuje się również jako wartości oczekiwanej zmiennej losowej reprezentującej straty powstałe w wyniku realizacji zdarzenia niekorzystnego¹⁷. Ryzyko w rozumieniu zarządzania bezpieczeństwem obywateli ma zawsze dwa aspekty. Z jednej strony mówi się o tzw. ryzyku eksperckim¹⁸ – obliczeniowym, wymiernym aspekcie ryzyka, policzalnym w sensie inżynierskim, którego wartość jest funkcją prawdopodobieństwa wystąpienia zagrożenia oraz jego potencjalnych skutków. Z drugiej strony, ze względu na konieczność „osadzenia” analizy

¹⁵ T. Tyszka, *Psychologiczne pułapki...*, s. 65–76.

¹⁶ J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Wydawnictwo Danmar, Warszawa 2005, s. 23 i nast.

¹⁷ M.M. Smolarkiewicz, *Metodyka wyznaczania niepewności określenia ryzyka na potrzeby zarządzania kryzysowego*, [w:] *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej na tle innych państw Unii Europejskiej. Stan obecny oraz perspektywy zmian*, (red.) M. Lisiecki, M. Raczkowska-Lipińska, B. Sitek, W. Pokruszyński, Wydawnictwo WSGE, Józefów k. Otwocka 2009, s. 495–502.

¹⁸ P.M. Sandman, *Responding to Community Outrage: Strategies for effective Risk Communication*, Va. Fourth Printing, American Industrial Hygiene Association Fairfax, 1997, s. 3–5.

ryzyka w realiach określonego obszaru (systemu), zwykle unikalnego pod względem istniejącej infrastruktury, jak również struktury społecznej, konieczne staje się uwzględnienie zwykle niepoliczalnego w sposób inżynierski aspektu ryzyka, zwanego w literaturze społecznym wzburzeniem¹⁹. Społeczne wzburzenie reprezentuje socjologiczny aspekt ryzyka związany przede wszystkim z poczuciem bezpieczeństwa społeczności lokalnej oraz jej indywidualną akceptowalnością danego rodzaju ryzyka.

Kolejnym istotnym elementem sprawnego zarządzania kryzysowego jest zarządzanie informacją²⁰. Na każdym szczeblu decyzyjnym istnieje potrzeba pozyskiwania rzetelnych, aktualnych i jasno sformułowanych informacji, które pozwalają na podjęcie najbardziej efektywnej w danym momencie decyzji. Ponieważ każda sytuacja nadzwyczajna charakteryzuje się niedoborem lub nadmiarem informacji (mówi się o zjawisku chaosu informacyjnego), zapewnienie wszystkim – służbom ratowniczym, administracji rządowej i samorządowej, jak również poszkodowanym i całemu społeczeństwu – dostępu do właściwej dla danego podmiotu, jednolitej (spójnej na wszelkich poziomach) i aktualnej informacji staje się jednym z kluczowych zadań zarządzania w takich sytuacjach.

W zakresie zarządzania kryzysowego i zarządzania bezpieczeństwem istotne jest wspieranie procesu decyzyjnego poprzez wykorzystanie kompletnych i spójnych dziedzinowych baz danych²¹. Rozwój systemów komputerowych i bazodanowych w aspekcie ich użyteczności w zarządzaniu informacją, wprowadzenie logiki rozproszonej oraz badania nad jej wykorzystaniem pokazały, że w obszarze zarządzania kryzysowego winno dążyć się do tworzenia dziedzinowych systemów baz danych rozproszonych (ang. *distributed database*)²². Sieci komputerowych baz danych, zarządzające bardzo dużymi zbiorami danych zwykle konstruuje się na bazie technologii baz rozproszonych, aby uniknąć niepotrzebnego powielania informacji i zaoszczędzić zasoby pamięci masowej, jednocześnie zachowując łatwość dostępu do informacji. Rozproszony system baz danych to taki system, w którym występuje rozłożenie danych przez ich fragmentaryzację (podział) lub replikację (powielenie) do różnych konfiguracji sprzętowych i programistycznych. Rozproszone systemy baz danych są przeciwieństwem systemów lokalnych, tzn. takich, gdzie zarówno dane, jak i oprogramowanie do ich zarządzania są zlokalizowane w jednym miejscu, np. w tym samym komputerze. Rozproszenie danych – ich fragmentaryzacja lub replikacja, dotyczy informacji przechowy-

¹⁹ Tamże, s. 7.

²⁰ B. Deltor, *Information management*, [w:] *Understanding information retrieval systems: management, types, and standards*, CRC Press, Los Angeles, CA, USA, 2011, s. 125–134.

²¹ M.M. Smolarkiewicz, *Koncepcje baz danych niezbędnych dla funkcjonowania...*, s. 39–60.

²² Tamże.

wanych w systemie. Głównym celem rozproszonej bazy danych jest to, aby dla użytkownika wyglądała ona jak jedna, scentralizowana baza. Zastosowanie logiki rozproszonych baz danych w procesie wspomaganie decyzji niesie ze sobą wiele korzyści. Z zalet takiego systemu baz danych należy podkreślić przede wszystkim łatwość tworzenia zapasowych serwerów i kopii zapasowych danych z bazy lokalnej oraz możliwość narzucenia lokalnej odpowiedzialności za dane.

3. Wybrane narzędzia użyteczne w kształceniu kadr na potrzeby zarządzania kryzysowego

Bezpieczeństwo lub też poczucie bezpieczeństwa jest jedną z podstawowych potrzeb człowieka zgodnie z piramidą potrzeb Masłowa²³. Niezależnie od pryzmatu spojrzenia na daną społeczność, każda – bez względu na rozmiar, genezę powstania i wzajemne powiązania – stara się stworzyć warunki do własnej bezpiecznej egzystencji. Dzieje się tak zarówno w małych społecznościach (lokalnych), jak również w większych, wynikających z organizacji administracyjnej – gminnych, powiatowych lub wojewódzkich. Na wszystkich szczeblach podziału administracyjnego państwa budowane są **systemy bezpieczeństwa** – zbiory unormowań prawnych, organizacyjnych, strukturalnych, społecznych, mające na celu obniżenie szansy (prawdopodobieństwa) występowania, jak również skutków zdarzeń niekorzystnych. Budowa tego typu systemów nierozdzielnie powiązanych (dedykowanych) z daną społecznością jest podstawowym zadaniem strategii zapewnienia bezpieczeństwa obywateli. Każdy istniejący system bezpieczeństwa buduje się na podstawie jednej z dwóch strategii – reagowania i/lub zapobiegania.

Strategia reagowania nastawiona jest przede wszystkim na zlokalizowanie wystąpienia zagrożenia w jak najkrótszym czasie i minimalizację jego skutków. Strategia zapobiegania ma na celu niedopuszczenie do wystąpienia zagrożenia oraz takie dostosowanie systemu podlegającego ochronie, by w razie wystąpienia zagrożenia jego wpływ na ludzi, mienie i środowisko był jak najmniejszy. Jedną z możliwości działania w obszarze strategii zapobiegania jest edukacja²⁴. Edukacja rozumiana szeroko – zarówno powszechna edukacja społeczeństwa w zakresie zwiększania świadomości na temat występujących zagrożeń²⁵, jak rów-

²³ A. Maslow, *Motywacja i osobowość*, Biblioteka klasyków psychologii, Wydawnictwo Naukowe PWN, Warszawa 2005, s. 47 i nast.

²⁴ A. Dawidczyk, J. Gryz, S. Koziej, *Zarządzanie strategiczne bezpieczeństwem...*, s. 91–135.

²⁵ R. Jakubczak, A. Skrabacz, *Społeczeństwo w tworzeniu bezpieczeństwa narodowego Polski w XXI wieku*, Wydawnictwo Akademii Podlaskiej, Siedlce 2006, s. 146–148.

niez odpowiednie przygotowanie służb odpowiedzialnych za niesienie pomocy i usuwanie skutków zdarzeń niekorzystnych oraz przedstawiciele administracji rządowej i samorządowej odpowiedzialnych za koordynację i wspomaganie działań ratowniczych. Złożoność i skala problemów występujących podczas każdej sytuacji kryzysowej uniemożliwiają nauczanie poprzez wskazanie ściśle określonych dróg i procedur działania. Proces edukacji (przygotowywania decydentów) powinien być ukierunkowany na interdyscyplinarne przygotowanie oraz naukę współdziałania²⁶ w sytuacjach trudnych i nietypowych. Aby osiągnąć tak sprecyzowane cele, należy skorzystać z możliwości, jakie dają dydaktyczne gry decyzyjne.

Jedną z form dydaktycznych zwiększających efektywność procesu nauczania decydentów odpowiedzialnych za podejmowanie decyzji w sytuacjach kryzysowych jest Multimedialny Trening Decyzyjny (MTD)^{27, 28}. Trening taki jest grą celową przeznaczoną dla wyselekcjonowanego odbiorcy dorosłego. Kategorię tę można zaliczyć do tzw. gier poważnych (ang. *serious games*). Symulacyjne **gry poważne** realizowane są na podstawie określonego modelu symulacji, zaś ich cele dydaktyczne są ściśle określone. Gry takie wymagają zazwyczaj wysokiej mocy obliczeniowej komputerów, specjalistycznych szkieletowych programów eksperckich oraz umiejętności wykorzystywania rozproszonych baz danych, jak również efektywnego zarządzania informacją. Wykorzystanie w procesie edukacji gier poważnych, w szczególności MTD, pozwala przeprowadzić analizę właściwych procedur, ocenić ryzyko oraz proces podejmowania decyzji. MTD stanowi efektywną, skuteczną i uniwersalną metodę dydaktyczną, która pozwala przygotować decydentów wszystkich szczebli do racjonalnego podejmowania decyzji i działania w razie wystąpienia sytuacji kryzysowej. Treningi takie budowane są na bazie unikatowych scenariuszy sytuacji kryzysowych, z wykorzystaniem nowoczesnych narzędzi dydaktycznych. Scenariusze wykorzystywane w procesie dydaktycznym opierają się głównie na wiedzy z zakresu zarządzania kryzysowego, ochrony przeciwpożarowej, funkcjonowania organów administracji rządowej i samorządowej, a także organizacji i prowadzenia akcji ratowniczych.

²⁶ M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wydawnictwo Akademii Podlaskiej, Siedlce 2009, s. 71.

²⁷ M.M. Smolarkiewicz, *Zastosowanie Multimedialnych Treningów Decyzyjnych w edukacji dla bezpieczeństwa*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżynieria działań w obszarach nauki, dydaktyki i praktyki*, (red.) B. Kosowski, A. Włodarski, Fundacja Edukacja i Technika Ratownictwa, Warszawa 2007, s. 213–220.

²⁸ M.M. Smolarkiewicz, *Gra decyzyjna „WODA” – symulacja powodzi na potrzeby szkoleniowe Centrów Zarządzania Kryzysowego*, „Bezpieczeństwo i Technika Pożarnicza – Safety & Fire Technique”, nr 2011/4, Józefów k. Otwocka 2011, s. 45–51.

U podstaw realizacji MTD leży założenie, że decydent, osadzony w realiach symulowanej sytuacji kryzysowej, na podstawie posiadanej wiedzy i doświadczenia jest w stanie sam wypracować najlepsze w danej sytuacji rozwiązanie, m.in. dzięki możliwości szerszego spojrzenia na skalę i rozmiar zagrożenia, z którym przyjdzie mu się zmierzyć. Stworzenie wiernej symulacji rzeczywistości – sytuacji kryzysowej – w ramach Multimedialnych Treningów Decyzyjnych wymaga wykorzystania wszelkich dostępnych środków komunikacji oraz form multimedialnego odwzorowania rzeczywistości. Dzięki temu Multimedialny Trening Decyzyjny jest formą trenażera, pozwalającego na ćwiczenie umiejętności zarządzania informacją, analizy sytuacji oraz procesu podejmowania decyzji w sytuacji kryzysowej. Stosowanie technik multimedialnych pozwala na osiągnięcie lepszych wyników dydaktycznych niż przy wykorzystaniu tradycyjnych metody przekazywania wiedzy. Kształcenie multimedialne powoduje pobudzenie aktywności spostrzeżeniowej, manualnej, intelektualnej i emocjonalnej. Stymulowanie zaangażowania emocjonalnego wpływa korzystnie na przyswajanie wiedzy i przyspiesza ten proces, jak również uczy kreatywnego myślenia.

Jednym z ciekawszych narzędzi technicznych, które można wykorzystać na potrzeby budowy MTD, jest środowisko „rzeczywistości wzbogaconej” (ang. *Augmented Reality – AR*)²⁹. Koncepcja implementacji obrazu rzeczywistego do środowiska aplikacyjnego, poszerzonego o markery reprezentujące określone obiekty lub zachowania, jest motywem przewodnim prac nad wykorzystaniem technik cyfrowej wirtualnej rzeczywistości w grach decyzyjnych. Przykładem takiej gry jest program ARES^{30,31}, odwzorowujący działania ratowniczo-gaśnicze funkcjonariuszy Państwowej Straży Pożarnej (PSP) na poziomie interwencyjnym. Gra decyzyjna ARES stanowi jądro stanowiska badawczego do analizy procesu podejmowania decyzji na poziomie interwencyjnym. Idea funkcjonowania programu polega na pobieraniu poprzez urządzenie wejściowe (kamerę cyfrową) rzeczywistego obrazu. Odpowiedzialny za pobieranie, analizę, przetwarzanie i wyświetlanie obrazu jest menadżer rzeczywistości wzbogaconej. Korzysta on z bibliotek, które pozwalają śledzić pozycję kamery w przestrzeni trójwymiarowej względem znaczników umieszczonych w rzeczywistej przestrzeni. Obraz

²⁹ I.E. Sutherland, *A head-mounted three dimensional display*, Proceeding AFIPS '68 (Fall, part I) Proceedings of the December 9-11, 1968, fall joint computer conference, part I, s. 757–764.

³⁰ R. Mazur, J. Szewczyk, M.M. Smolarkiewicz, *Dydaktyczne gry decyzyjne w środowisku „rzeczywistości wzbogaconej” na przykładzie systemu ARES. Metodologia badań*, „Bezpieczeństwo i Technika Pożarnicza – Safety & Fire Technique”, Wydawnictwo CNBOP, nr 2012/1, s. 57–66.

³¹ M.M. Smolarkiewicz, J. Szewczyk, *Symulacja zdarzeń na poziomie interwencyjnym z wykorzystaniem rzeczywistości wzbogaconej (program ARES) – analiza czasów podejmowania decyzji*, „Zeszyty Naukowe SGSP”, nr 39, Warszawa 2009, s. 43–52.

pobrano przez kamerę analizowany jest przez odpowiednią funkcję znajdującą się w menadżerze. Jeżeli wraz z obrazem rzeczywistym pobrano zostanie obraz markera znajdującego się w bibliotece, wówczas menadżer przekazuje, za pośrednictwem urządzenia wyjściowego, np. hełmu wirtualnego, rzutnika, monitora itp., rzeczywisty obraz wraz ze sztucznie wygenerowanym obrazem dwu- lub trójwymiarowym.

4. Narzędzia wspomagania zarządzania kryzysowego – od nauki do praktyki

Praktyczne zastosowanie osiągnięć naukowych przyczynia się do szybszego rozwoju i lepszej konkurencyjności na rynkach międzynarodowych. W obszarze zarządzania kryzysowego, w szczególności w zakresie wspomagania procesu decyzyjnego, w ostatnich latach daje się zaobserwować szybki wzrost liczby zastosowań systemów wspomagania decyzji (SWD) i systemów eksperckich (SE)^{32, 33}, jak również rozwiązań opartych na systemach informacji geograficznej GIS (ang. *Geographic Information System*), często budowanych wspólnie z modułami dyspozytorskimi (aplikacjami służącymi zarządzaniu siłami i środkami)^{34, 35}.

Systemem wspomagania decyzji (SWD) nazywamy system informatyczny, który dostarcza informacje w danej dziedzinie z wykorzystaniem analitycznych modeli decyzyjnych z dostępem do baz danych w celu wspomagania decydentów w skutecznym działaniu w kompleksowym i źle ustrukturalizowanym środowisku. SWD to systemy komputerowe wyposażone w interaktywny dostęp do danych i modeli, które wspomagają rozwiązanie specyficznych sytuacji decyzyjnych, nie dających się rozwiązać automatycznie przy użyciu samego komputera³⁶. Z uwagi na istotne zalety SWD, który pozwala decydentowi m.in. na projektowanie lub poszukiwanie stosownych wariantów rozwiązań, wzbogacenie umiejętności

³² M.M. Smolarkiewicz, *Systemy wspomagania decyzji i systemy ekspertowe w zarządzaniu kryzysowym – ich rola, zadania i ograniczenia*, „Journal of Modern Science – Zeszyty Naukowo-Dydaktyczne WSGE”, nr 1/6/2009, s. 371–384.

³³ P. Sienkiewicz, H. Świeboda, R. Wieleba, K. Żwirek, *Wspomaganie decyzji w systemie zarządzania kryzysowego w środowisku sieciocentrycznym*, „Studia i Materiały Stowarzyszenia Zarządzania Wiedzą”, nr 33, 2010, s. 48–57.

³⁴ M.M. Smolarkiewicz, *Rola GIS w zarządzaniu bezpieczeństwem*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, Wydawnictwo WSZiP, Warszawa 2008, s. 135–145.

³⁵ J. Ryzenko, M.M. Smolarkiewicz, *Space-enabled information environment for crisis management. Scenario-based analysis and evaluation in an operational environment*, „Acta Astronautica”, nr 66, 2010, s. 33–39.

³⁶ J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Agencja Wydawnicza Placet, Warszawa 2005, s. 239.

w podejmowaniu decyzji, planowanie i wdrożenie decyzji oraz adaptację, zastosowanie systemu tego typu w znacznym stopniu może podnieść efektywność podejmowanych decyzji. Oczywiście jest, że nie da się wyeliminować czynnika ludzkiego, jednakże decydent korzystający z SWD także się uczy. Rozwija w sobie zdolności w obszarze podniesienia skuteczności osobistej, rozszerzenia obszaru poszukiwania rozwiązania problemu, ułatwienia komunikacji międzyosobowej.

Inną rolę w zarządzaniu kryzysowym pełnią systemy eksperckie. W podejmowaniu decyzji podczas zaistnienia sytuacji kryzysowej często istnieje potrzeba skorzystania z wiedzy ekspertów. W skrajnie trudnych sytuacjach, w obszarze głębokiej niepewności, gdy nie można polegać na źródłach informacji (z uwagi na chaos informacyjny), często jedynym rozwiązaniem pozostaje powierzenie decyzji ich doświadczeniu i wiedzy. W tym obszarze pojawia się możliwość zastosowania dedykowanych systemów eksperckich, których rola polega na przeniesieniu wiedzy eksperta do komputera, który jest wyposażony w specjalne reguły wnioskowania i język, dzięki któremu może komunikować się z użytkownikiem (decydentem)³⁷. System ekspercki zawiera wyspecjalizowaną wiedzę na temat specyficznego obszaru ludzkiej działalności. Wiedza ta zorganizowana jest w taki sposób, że umożliwia systemowi wejście w interakcyjny dialog z użytkownikiem, w wyniku którego system może oferować rozsądne rady lub proponować rozsądne decyzje oraz objaśniać sposób rozumowania leżący u podstaw tych rad lub propozycji. Systemy te mogą samodzielnie tworzyć różne modele sytuacji decyzyjnej, uwidaczniać otrzymywane rozwiązanie i objaśniać je. Aby rozstrzygnąć problem, muszą posługiwać się specjalistycznymi programami zawierającymi reguły heurystyczne, które odzwierciedlają wiedzę ekspertów dziedzinowych.

Aby móc koordynować działania wielu podmiotów działających na rozległym obszarze, nie wystarcza w obecnych realiach zapewnienie łączności radiowej oraz dostępu do baz danych. Wraz z rozwojem technik cyfrowych wprowadzone są coraz powszechniejsze rozwiązania oparte na systemach GIS. Zarządzanie kryzysowe jest wspierane, oprócz technologii GIS, również przez inne techniki satelitarne i okołosatelitarne. Wykorzystanie szerzej rozumianych technik satelitarnych staje się efektywne (mając na myśli relację koszt–efekt) dopiero w momencie, gdy sytuacja wymyka się poza ramy ratowniczych działań proceduralnych, czyli w momencie wystąpienia kryzysu (bądź gdy sytuacja zaczyna nosić znamiona sytuacji kryzysowej), w przypadku działania na obszarach ubogich w infrastrukturę techniczną (gdy występują trudności w określeniu położenia) lub w przypadku zagrożeń rozległych w czasie i przestrzeni.

³⁷ M. Szmit, *Informatyka w zarządzaniu*, Centrum Doradztwa i Informacji Difin, Warszawa 2003, s. 41–42.

W przypadku rozległych zagrożeń powodujących dysfunkcję naziemnych systemów komunikacji (takich jak powódzie, pożary lasów) łączność satelitarna staje się niezbędna, gdyż naziemne stacje przekaźnikowe mogą przestać funkcjonować. Łączność satelitarna staje się w dzisiejszych czasach niezbędna jako alternatywny środek komunikacji na poziomie taktycznym i strategicznym (tzn. w obszarze dowodzenia w strukturze powyżej pojedynczego odcinka bojowego). Kolejną i niezaprzeczalną zaletą wykorzystania technik satelitarnych w zakresie łączności i nawigacji są możliwości, jakie niosą ze sobą tzw. terminale satelitarne. Terminale takie znacznie skracają czas niezbędny do koordynacji działań w miejscach o ubogiej infrastrukturze komunikacyjnej oraz wymagających zgrania działań w przestrzeni (na przykład poszukiwań osób zaginionych w lasach). Dzięki temu, że terminale takie stają się coraz bardziej dostępne, nie tylko dla służb odpowiedzialnych za bezpieczeństwo i niesienie pomocy, ale także dla zwykłych obywateli, w niedalekiej przyszłości wszyscy, którzy znajdą się w obszarze wystąpienia określonego zdarzenia niekorzystnego, otrzymają dostęp do jednoznacznej informacji, identycznego obrazu sytuacji. Wykorzystanie systemów takich jak GPS (ang. *Global Positioning System*) pozwala na określenie z dużą dokładnością położenia prawie w każdym miejscu na świecie.

W obszarze zarządzania kryzysowego nawigacja satelitarna jest wykorzystywana przede wszystkim w transporcie materiałów niebezpiecznych. W momencie wypadku z udziałem pojazdu przewożącego tego typu środki zawsze istnieje możliwość uwolnienia substancji, co stanowi poważne zagrożenie dla zdrowia i życia. W takich sytuacjach natychmiastowe ustalenie miejsca zdarzenia staje się zadaniem priorytetowym, gdyż im dłuższy czas uwalniania substancji, tym większy może być obszar zagrożony. Monitorowanie ruchu pojazdów pozwala na wcześniejsze udrażnianie dróg i uniemożliwianie wystąpienia zatorów poprzez wcześniejsze reagowanie na zaistniałą sytuację. W przypadku długotrwałych zagrożeń wielkoobszarowych (takich jak powódzie, pożary lasów) tylko obraz satelitarny jest w stanie pokazać rozległość obszaru zaburzenia. Dzięki wykorzystaniu otwartych modeli obliczeniowych, pozwalających na wprowadzanie poprawek do warunków brzegowych w trakcie trwania symulacji oraz dających możliwość startu obliczeń od zadanej sytuacji, obraz satelitarny umożliwi uzyskiwanie bieżących poprawek do modeli, a co za tym idzie, zwiększenie dokładności obliczeniowej.

Analiza ryzyka z wykorzystaniem informacji ze zobrażeń satelitarnych i modelowych obliczeń numerycznych umożliwia podejmowanie decyzji na podstawie rzeczywistego ryzyka a nie jedynie prognozą rozwoju zagrożenia (wnoszone również dzięki korekcie modeli w czasie rzeczywistym). Dzięki takiej analizie dowodzący jest w stanie skoncentrować dostępne siły i środki (których liczba

w sytuacji kryzysowej jest zwykle niewystarczająca) w miejscu, gdzie istnieje realna potrzeba i szansa obniżenia skutków zaistniałego zagrożenia.

Podsumowując powyższe rozważania, można stwierdzić, że z punktu widzenia teorii decyzji i informacyjnych systemów zarządzania najbardziej słusznym środowiskiem do rozwoju praktycznych narzędzi wspomagania decyzji na potrzeby zarządzania kryzysowego wydaje się hybryda systemu wspomagania decyzji (SWD) i rodziny systemów eksperckich (SE), działająca na podstawie rozproszonych baz danych, w koncepcji hurtowni danych współpracująca z systemami informacji geograficznej³⁸. Systemy takie mogą być budowane na podstawie wielokryterialnych koncepcji modelowych. Do koncepcji takich można zaliczyć m.in. wielowymiarowe systemy matrycowe.

Jedną z koncepcji systemu matrycowego jest Teoria matryc stowarzyszonych (TMS)³⁹, która uwzględnia m.in. matryce zagrożeń i matryce bezpieczeństwa, ale ze względu na wykorzystanie szeroko rozumianego zarządzania ryzykiem, jako narzędzia optymalizującego podejmowane decyzje, ma ona zastosowanie głównie w obszarze zapobiegania i przygotowania, natomiast jej wykorzystanie w obszarze reagowania jest raczej hipotetyczne z powodu dynamiki zmian sytuacji w czasie w tej fazie. Teoria matryc stowarzyszonych wprowadza do obszaru zarządzania kryzysowego nowe narzędzia, tj. w fazie reagowania matrycę R-decyzji, łączącą rodzaj zdarzenia niekorzystnego z najczęściej występującymi problemami decyzyjnymi, zaś w fazie przygotowania i zapobiegania matrycę Z-decyzji, łączącą czynniki charakteryzujące ryzyko związane z realizacją określonego zagrożenia oraz wpływem poszczególnych decyzji na redukcję siły oddziaływania tego zagrożenia na całkowitą wartość ryzyka. Matryce R-decyzji i Z-decyzji prowadzą do skonstruowania Wielowymiarowej Matrycy Decyzji (WMD), przy pomocy której poprzez poszukiwanie ekstremów (minimów) wartości ryzyka dochodzi się do najlepszego w danym momencie wariantu decyzji.

Inną koncepcją systemu matrycowego jest N-wymiarowa matryca bezpieczeństwa^{40, 41}. Pozwala ona na wspomaganie procesu podejmowania decyzji

³⁸ M.M. Smolarkiewicz, *Teoria matryc stowarzyszonych i N-wymiarowa matryca bezpieczeństwa...*, s. 92.

³⁹ M.M. Smolarkiewicz, *Teoria matryc stowarzyszonych w zarządzaniu kryzysowym*, [w:] *Wymiary bezpieczeństwa na progu XXI wieku. Między teorią a praktyką*, (red.) A. Zaręba, B. Zapała, Polskie Towarzystwo Nauk Politycznych, Wydawnictwo Adam Marszałek, Toruń, 2010, s. 83–93.

⁴⁰ M.M. Smolarkiewicz, *Metody matrycowe w zarządzaniu bezpieczeństwem publicznym na potrzeby centrów powiadamiania ratunkowego – podejście funkcyjne do konstruowania N-wymiarowej matrycy bezpieczeństwa*, [w:] *Infrastruktura bezpieczeństwa publicznego. Ogólnokrajowe i lokalne wyzwania cywilizacyjne*, (red.) Z. Ciekankowski, Wydawnictwo WSZiP, Warszawa 2010, s. 365–377.

⁴¹ M.M. Smolarkiewicz, *Wykorzystanie metodyki N-wymiarowej Matrycy Bezpieczeństwa na potrzeby Centrów Powiadamiania Ratunkowego – studium przypadku*, [w:] *Bezpieczeństwo w ad-*

w fazie reagowania poprzez określenie relacji pomiędzy zbiorami informacji, decyzji i działań w obszarze koordynacji aktywności wielu podmiotów zaangażowanych w akcję ratowniczą po wystąpieniu zdarzenia niekorzystnego. Została ona opracowana na potrzeby koncepcji funkcjonalnej Centrum Powiadamiania Ratunkowego (CPR). Wspomniana metoda matrycowa wprowadza dwuwymiarowe dyskretne zależności funkcyjne (tzw. funkcje relacji) do opisu relacji pomiędzy zbiorami: możliwych zdarzeń niekorzystnych, wszystkich możliwych i realnych klas zagrożeń, możliwych miejsc zdarzenia, uwzględniających przede wszystkim rodzaj miejsca lub obiektu, najbardziej istotnych z punktu widzenia prowadzenia działań ratowniczych cech miejsca zdarzenia, podmiotów zaangażowanych w reagowanie, wspomaganie lub koordynację działań, możliwych decyzji pozaproceduralnych (innych niż dysponowanie sił i środków określonego podmiotu, takich jak informowanie mediów, alarmowanie ludności o zagrożeniach, prośba o pomoc spoza powiatu i inne), możliwych działań (w rozumieniu realizacji zadań), wszystkich możliwych do wykorzystania sił i środków będących w posiadaniu podmiotów zaangażowanych.

Na podstawie wymienionych zbiorów i relacji pomiędzy ich elementami zdefiniowano 11 dwuwymiarowych matryc, które, razem połączone, tworzą N-wymiarową matrycę bezpieczeństwa. Każda z matryc stanowiących element N-wymiarowej matrycy bezpieczeństwa opisuje jeden z aspektów, który staje się istotny na różnych etapach działań przy zaistnieniu zdarzenia niekorzystnego. Metoda N-wymiarowej matrycy bezpieczeństwa sama w sobie stanowi jedną z prób rozwiązania problemu koordynacji działań służb, inspekcji, straży oraz innych podmiotów zaangażowanych w niesienie pomocy i minimalizację skutków takich zdarzeń. Ze względu na konieczność podejmowania decyzji głównie w sytuacji niedoboru czasu i informacji ta metoda matrycowa staje się potencjalnym narzędziem wspomaganie operatora CPR.

Wymienione powyżej wielowymiarowe systemy matrycowe są przykładami narzędzi, które znajdują realne i praktyczne zastosowanie w procesie zarządzania kryzysowego. Teoria matryc stowarzyszonych wplata w sposób systemowy narzędzia analizy ryzyka w procedury wspomaganie procesu decyzyjnego. Jej zaletą jest możliwość funkcjonalnego podejścia do analizy koszt–efekt w każdej fazie procesu zarządzania kryzysowego, dzięki czemu podejmowane decyzje mogą być optymalizowane w ujęciu redukcji potencjalnego ryzyka. Niestety słabością takiego podejścia jest konieczność ciągłego napływu wiarygodnej

ministracji i biznesie we współczesnym świecie, (red.) M. Chrabowski, C. Tatarczuk, J. Tomaszewski, Wydawnictwo WSAiB, Gdynia 2011, s. 106–115.

i bardzo szczegółowej informacji sytuacyjnej, co często stanowi duży problem w zdarzeniach o charakterze kryzysowym.

Biorąc powyższe pod rozwagę, wydaje się słusznym stwierdzenie, że metoda ta może stać się nieocenionym narzędziem wspomagania decyzji, jeżeli udałoby się stworzyć narzędzia, które w sposób ciągły są w stanie tworzyć przestrzenne, poszerzone o propagację czasową, mapy ryzyka dla zagrożonych obszarów. Do podstawowych użytkowników (odbiorców) narzędzi budowanych na podstawie teorii macryc stowarzyszonych można zaliczyć przede wszystkim centra zarządzania kryzysowego szczebla powiatowego, wojewódzkiego i centralnego, jak również Rządowe Centrum Bezpieczeństwa. W przypadku działań o charakterze rutynowym, gdzie priorytetem staje się przede wszystkim optymalizacja zarządzania siłami i środkami, z pomocą przychodzi metoda N-wymiarowej macrycy bezpieczeństwa. Metoda ta może być również wykorzystywana na potrzeby sytuacji kryzysowych, jednakże tylko w obszarze dobrze ustrukturalizowanych decyzji w zakresie działań wymagających koordynacji wielu podmiotów. W przypadku takich wspólnych i złożonych działań służb, inspekcji, straży oraz podmiotów administracji rządowej i samorządowej niezbędne jest ustalenie priorytetów i celów, jakie mają być poprzez nie osiągnięte.

W takiej sytuacji najlepszym rozwiązaniem stają się procedury, które w sposób elastyczny pozwalają na zaangażowanie do działania sił i środków tych podmiotów, które w danym momencie są niezbędne. N-wymiarowa macryca bezpieczeństwa jest *de facto* strukturą łączącą w logiczny sposób poprzez zależności funkcyjne tysiące prostych procedur ułatwiających udzielenie odpowiedzi m.in. na pytania: których sił i środków należy użyć w danym momencie, kto jest odpowiedzialny za koordynację działań, a kto za ich wspomaganie, gdzie poszukiwać zasobów, w których posiadaniu się nie jest w danej chwili, jakie konsekwencje zdarzenia niekorzystnego są najbardziej prawdopodobne, czy w istniejącej sytuacji grozi eskalacja skutków itd. W tym miejscu należy zwrócić uwagę, że zarówno jedna, jak i druga metoda macrycowa nie jest narzędziem będącym w stanie samodzielnie podejmować decyzje (w przeciwieństwie do istotniej zaawansowanych metod opartych np. na sieciach neuronowych⁴²), a jedynie wspomagającym ocenę sytuacji i wybór najlepszej z punktu widzenia przyjętych kryteriów decyzji. Do podstawowych użytkowników (odbiorców) narzędzi budowanych na podstawie N-wymiarowej macrycy bezpieczeństwa można zaliczyć przede wszystkim centra powiadamiania ratunkowego (CPR) i stanowiska dyspozytorskie służb, inspekcji i straży.

⁴² S. Biedugnis., M.M. Smolarkiewicz, M.Z. Smolarkiewicz, *Sieci neuronowe w zagadnieniach bezpieczeństwa zaopatrzenia w wodę*, „Zeszyty Naukowe SGSP”, nr 41, 2011, s. 81–93.

Bibliografia

Literatura:

- Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wydawnictwo Akademii Podlaskiej, Siedlce 2009.
- Dawidczyk A., Gryz J., Koziej S., *Zarządzanie strategiczne bezpieczeństwem. Teoria – Praktyka – Dydaktyka*, Wydawnictwo Wyższej Szkoły Humanistyczno-Ekonomicznej, Łódź 2006.
- Deltor B., *Information management*, [w:] *Understanding information retrieval systems: management, types, and standards*, CRC Press, Los Angeles, CA, USA, 2011.
- Jakubczak R., Skrabacz A., *Społeczeństwo w tworzeniu bezpieczeństwa narodowego Polski w XXI wieku*, Wydawnictwo Akademii Podlaskiej, Siedlce 2006.
- Kahneman P., Tversky A., *A Prospect Theory: An Analysis of Decision Under Risk*, "Econometrica" tom 47, 1979.
- Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Agencja Wydawnicza Placet, Warszawa 2005.
- Lidwa W., Krzeszowski W., Więcek W., *Zarządzanie w sytuacjach kryzysowych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2010.
- Maslow A., *Motywacja i osobowość*, Biblioteka klasyków psychologii, Wydawnictwo Naukowe PWN, Warszawa 2005.
- Mazur R., Szewczyk J., Smolarkiewicz M.M., *Dydaktyczne gry decyzyjne w środowisku „rzeczywistości wzbogaconej” na przykładzie systemu ARES. Metodologia badań, „Bezpieczeństwo i Technika Pożarnicza – Safety & Fire Technique”*, Wydawnictwo CNBOP, nr 2012/1.
- Ryzenko J., Smolarkiewicz M.M., *Space-enabled information environment for crisis management. Scenario-based analysis and evaluation in an operational environment*, "Acta Astronautica" nr 66, 2010.
- Sandman P.M., *Responding to Community Outrage: Strategies for effective Risk Communication*, Va. Fourth Printing, American Industrial Hygiene Association Fairfax, 1997.
- Sienkiewicz P., *Badania naukowe bezpieczeństwa systemów*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżynieria działań w obszarze nauki, dydaktyki i praktyki*, (red.) B. Kosowski, A. Włodarski, Fundacja Edukacja i Technika Ratownictwa, Warszawa 2007.
- Sienkiewicz P., Świeboda H., Wieleba R., Żwirek K., *Wspomaganie decyzji w systemie zarządzania kryzysowego w środowisku sieciocentrycznym*, „Studia i Materiały Stowarzyszenia Zarządzania Wiedzą”, Nr 33, 2010.
- Sienkiewicz-Małyjurek K., Krynojewski F.R., *Zarządzanie kryzysowe w administracji publicznej*, Wydawnictwo Difin, Warszawa 2010.
- Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, PRESSCOM, Wrocław 2010.
- Smolarkiewicz M.M., *Gra decyzyjna „WODA” – symulacja powodzi na potrzeby szkoleniowe Centrów Zarządzania Kryzysowego*, „Bezpieczeństwo i Technika Pożarnicza – Safety & Fire Technique”, nr 2011/4, Józefów k. Otwocka 2011.
- Smolarkiewicz M.M., *Koncepcje baz danych niezbędnych dla funkcjonowania struktur zarządzania kryzysowego (CPR, GCR)*, Elektroniczna Administracja, VI edycja konferencji

- „Teleinformatyczne standardy i procedury w zarządzaniu kryzysowym – narzędzia GIS-owskie oraz programy symulacyjne”, nr 3, maj–czerwiec 2006.
- Smolarkiewicz M.M., *Metody matrycowe w zarządzaniu bezpieczeństwem publicznym na potrzeby centrów powiadamiania ratunkowego – podejście funkcyjne do konstruowania N-wymiarowej matrycy bezpieczeństwa*, [w:] *Infrastruktura bezpieczeństwa publicznego. Ogólnokrajowe i lokalne wyzwania cywilizacyjne*, (red.) Z. Czekanowski, Wydawnictwo WSZiP, Warszawa 2010.
- Smolarkiewicz M.M., *Metodyka wyznaczania niepewności określenia ryzyka na potrzeby zarządzania kryzysowego*, [w:] *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej na tle innych państw Unii Europejskiej. Stan obecny oraz perspektywy zmian*, (red.) M. Lisiecki, M. Raczkowska-Lipińska, B. Sitek, W. Pokruszyński, Wydawnictwo WSGE, Józefów k. Otwocka 2009.
- Smolarkiewicz M.M., *Rola GIS w zarządzaniu bezpieczeństwem*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, (red.) M. Lisiecki, Wydawnictwo WSZiP, Warszawa 2008.
- Smolarkiewicz M.M., *Systemy wspomaganie decyzji i systemy ekspertowe w zarządzaniu kryzysowym – ich rola, zadania i ograniczenia*, “*Journal of Modern Science – Zeszyty Naukowo-Dydaktyczne WSGE*”, nr 1/6/2009.
- Smolarkiewicz M.M., *Teoria matryc stowarzyszonych i N-wymiarowa matryca bezpieczeństwa – nowe metody matrycowe na potrzeby zarządzania kryzysowego*, WSZiP, Warszawa 2013.
- Smolarkiewicz M.M., *Teoria matryc stowarzyszonych w zarządzaniu kryzysowym*, [w:] *Wymiary bezpieczeństwa na progu XXI wieku. Między teorią a praktyką*, (red.) A. Zaręba, B. Zapała, Polskie Towarzystwo Nauk Politycznych, Wydawnictwo Adam Marszałek, Toruń, 2010.
- Smolarkiewicz M.M., *Wykorzystanie metodyki N-wymiarowej Matrycy Bezpieczeństwa na potrzeby Centrów Powiadamiania Ratunkowego – studium przypadku*, [w:] *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, (red.) M. Chabowski, C. Tatarczuk, J. Tomaszewski, Wydawnictwo WSAiB, Gdynia 2011.
- Smolarkiewicz M.M., *Zastosowanie Multimedialnych Treningów Decyzyjnych w edukacji dla bezpieczeństwa*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – Inżynieria działań w obszarach nauki, dydaktyki i praktyki*, (red.) B. Kosowski, A. Włodarski, Fundacja Edukacja i Technika Ratownictwa, Warszawa 2007.
- Smolarkiewicz M.M., Szewczyk J., *Symulacja zdarzeń na poziomie interwencyjnym z wykorzystaniem rzeczywistości wzbogaconej (program ARES) – analiza czasów podejmowania decyzji*, „*Zeszyty Naukowe SGSP*”, nr 39, Warszawa 2009.
- Sutherland I.E., *A head-mounted three dimensional display*, *Proceeding AFIPS '68 (Fall, part I) Proceedings of the December 9-11, 1968, fall joint computer conference, part I*.
- Szmit M., *Informatyka w zarządzaniu*, Centrum Doradztwa i Informacji Difin, Warszawa 2003.
- Tyszka T., *Psychologiczne pułapki oceniania i podejmowania decyzji*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1999.
- Wojnarski J., *Kryzys konsekwencją zagrożeń cywilizacyjnych*, [w:] *Zarządzanie kryzysowe w Polsce*, (red.) M. Jabłonowski, L. Smolak, Akademia Humanistyczna im. A. Gieysztor, Pułtusk 2007.

Wolanin J., *Zarys teorii bezpieczeństwa obywateli*, Wydawnictwo Danmar, Warszawa 2005.

Wójtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, Ministerstwo Obrony Narodowej, Departament Polityki Obronnej, Warszawa 2006.

Ziarko J., Walas-Trębacz J., *Podstawy zarządzania kryzysowego. Cz. I. Zarządzanie kryzysowe w administracji publicznej*, Krakowka Akademia im. A. Frycza Modrzejewskiego, Krakowskie Towarzystwo Edukacyjne – Oficyna Wydawnicza AFM, Kraków 2010.

Żebrowski P., Abramowicz P., Filipowska A., Wróblewski D., Smolarkiewicz M.M., Wolanin J., Wiśniewski M., Bassara A., *Progresive crisis management system*, [w:] The 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, USA, 2005.

Akty prawne:

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. nr 89, poz. 590 z późn. zm.).

Wykaz rysunków:

Rys. 1. Cykl 4-fazowego zarządzania kryzysowego.

Rys. 2. Fazy zarządzania kryzysowego – zarządzanie progresywne.

Streszczenie

W niniejszym artykule przeprowadzono analizę wybranych teorii, systemów i narzędzi, które są wykorzystywane na potrzeby wspomagania procesu zarządzania kryzysowego. Omawiane zagadnienia podzielono z uwagi na nowe teorie naukowe opisujące m.in. proces podejmowania decyzji, narzędzia użyteczne w procesie edukacji decydentów odpowiedzialnych za zapewnienie bezpieczeństwa obywateli oraz systemy praktyczne wspomagające zarządzanie kryzysowe. Z systemów tych w szczególności opisano wielowymiarowe metody matrycowe: Teorię matryc stowarzyszonych oraz N-wymiarową matrycę bezpieczeństwa. Przedstawione zagadnienia ukazują powiązanie pomiędzy nauką, dydaktyką i praktyką w procesie budowania nowych narzędzi na potrzeby optymalizacji procesu zarządzania kryzysowego.

Słowa kluczowe: zarządzanie kryzysowe, ryzyko, teoria perspektywy, N-wymiarowa matryca bezpieczeństwa, Teoria matryc stowarzyszonych, system wspomagania decyzji, system ekspercki.

Summary

Modern techniques for crisis management – science, didactics, practice

In this article, an analysis was made of chosen theories, systems and tools use for supporting of the crisis management process. The topics were divided into new scientific theories that describe, among others, decision-making process, tools useful in education of decision-makers responsible for ensuring the safety of citizens, and practical systems supporting the crisis management. Among these systems, in particular, multi-dimensional matrix methods were described: Theory of associated matrices and N-dimensional safety matrix. Presented issues show the link among science, didactics and practice in the process of developing new tools for optimization of the of crisis management process.

Key words: crisis management, risk, prospect theory, N-dimension safety matrix, Theory of associated matrices, decision support system, expert system.

Rozdział VI.

Ciągłość działania administracji publicznej w obliczu zagrożeń bezpieczeństwa powszechnego

1. Wprowadzenie do problematyki ciągłości działania

Problematyka ciągłości działania zdaje się coraz mocniej determinować współczesne postrzeganie bezpieczeństwa powszechnego, a także funkcjonowania podmiotów dedykowanych do jego zapewniania. W przedmiotowym kontekście stawiane im oczekiwania są dwojakiego rodzaju. Po pierwsze, ukie-runkowanie na zapewnienie bezpieczeństwa (rozumianego jako wolność od zagrożeń, a także niezakłócone byt i rozwój) ludności cywilnej wymusza permanentne dostosowywanie działalności do nierzadko dynamicznie zmieniających się uwarunkowań materialno-energetycznych, społecznych i kulturowych. Po drugie, wspomniane podmioty nierzadko same stają w obliczu zagrożeń, przed którymi są obowiązane chronić. Zachowanie ciągłości działania dotyczy więc kreowania warunków do utrzymania bezpieczeństwa powszechnego na minimalnym akceptowalnym dla państwa i ogółu jego obywateli poziomie (wymiar zewnętrzny). Jest ono także rozumiane przez pryzmat zapewnienia, by organizacja chroniąca przed właściwymi zagrożeniami była zdolna utrzymać świadczenie swoich usług na właściwym sobie, minimalnym akceptowalnym poziomie jakości (wymiar wewnętrzny).

Dr Paweł Gromek – Wydział Inżynierii Bezpieczeństwa Cywilnego, Szkoła Główna Służby Po-
żarniczej.

Powyższe założenia korespondują z syntetyczną definicją ciągłości działania, która została zawarta w międzynarodowym dokumencie normatywnym¹. Zgodnie z jej treścią to zdolność organizacji do kontynuowania swojej działalności (dostarczania produktów i/lub świadczenia usług) po wystąpieniu zdarzenia zakłócającego jej funkcjonowanie na poziomie jakości określonym uprzednio jako minimalny akceptowalny². Organizacyjny kontekst pozwala implementować taki sposób rozumienia na grunt pojedynczych organizacji, jak też ich sieci (w tym tych stanowiących sformalizowane i niesformalizowane systemy działań ludzkich).

Ciągłość działania jest bezsprzecznie związana z zagrożeniami, które poddawane są ocenie z perspektywy ryzyka (zarządzania ryzykiem) oraz wpływu na działalność (z ang. *Business Impact Analysis*, BIA). W pierwszym przypadku mowa o procesowym ujęciu identyfikacji, analizy i oceny zagrożeń pod kątem prawdopodobieństwa (częstości, częstotliwości) ich wystąpienia w świetle właściwych skutków dla organizacji. BIA odnosi się natomiast do rozkładu czasowego strat powstałych wskutek oddziaływania zagrożeń na najważniejsze procesy organizacyjne (procesy kluczowe, w tym krytyczne). Uwypukla się w ten sposób konieczność prawidłowego wyznaczenia odpowiednich buforów czasowych, a także czynności pozwalających przywrócić w określonych rygorach czasowych jakość najważniejszych procesów organizacyjnych do poziomu przyjętego za akceptowalny³.

Zarządzanie ryzykiem oraz BIA to dwa główne fundamenty zarządzania ciągłością działania. Na nich jest budowany ten całościowy proces zarządczy, w ramach którego dokonuje się identyfikacji potencjalnych zagrożeń organizacyjnych i ich skutków, zapewniający ramowe struktury budowania odporności organizacji na wspomniane zagrożenia, umożliwiającą również skuteczne reagowanie w obliczu ich materializacji, celem ochrony interesów kluczowych interesariuszy, reputacji, marki i eksponowanych wartości⁴.

Na zarządzanie ciągłością działania składa się wiele złożonych aspektów. Na najwyższym poziomie ogólności bierze się tu pod uwagę struktury organizacyjne (statyczne i dynamiczne), układ priorytetów działań zorganizowanych (politykę organizacyjną), planowanie, zakresy odpowiedzialności, procesy, procedury, a także zasoby przeznaczone do zapewnienia ciągłości działania (dedykowane i/lub funkcjonujące codziennie w innych strukturach organizacyjnych, zmieniające jednak swoją przynależność w momencie aktywizacji

¹ ISO 22301:2012 Societal security. Business continuity management systems. Requirements.

² Tamże, 3.3.

³ Zob. R. Kaszubski, D. Romańczuk (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania. Business Continuity Management*, Warszawa 2011, s. 77–86.

⁴ Zob. ISO 22301:2012..., 3.4.

poszczególnych procedur awaryjnych). Ukazana w ten sposób wieloaspektowość zdaje się wymuszać konieczność stosowania holistycznego podejścia w niniejszym zakresie. W praktyce przedmiotu poznania wykorzystuje się podejście systemowe, dbając o to, aby system zarządzania ciągłością działania był integralną częścią ogólnego systemu zarządzania organizacją, dotyczył zaś ustanawiania, wdrażania, funkcjonowania, monitorowania, przeglądów, utrzymywania oraz doskonalenia działań ukierunkowanych na zapewnianie ciągłości działania⁵.

Ponadto omawiane czynności zarządcze o charakterze systemowym powinny być wykonywane nieprzerwanie. Zgodnie z regulacjami normatywnymi wpisuje się je w modelowe ujęcie procesu ciągłego doskonalenia organizacyjnego (z ang. *Plan-Do-Act-Check*, PDCA). Oznacza to ich przydział do czterech cyklicznie następujących po sobie faz⁶:

- ustanawiania systemu zarządzania ciągłością działania – w ramach którego tworzy się przedmiotową politykę, określa cele, formułuje mechanizmy nadzoru, a także opisuje procesy i procedury pozwalające na doskonalenie systemowe;
- wdrożenia i eksploatacji systemu – utożsamianego z praktyczną implementacją założeń systemowych na grunt codziennej działalności organizacji;
- monitoringu i przeglądu – dotyczących efektywności systemu, związanych z raportowaniem bieżącego stanu systemu zarządzania ciągłością działania wraz z podejmowaniem ewentualnych czynności naprawczych i/lub doskonalących;
- utrzymania i doskonalenia – mocno powiązanych z działaniami składającymi się na poprzednią fazę, uwzględniających jednak możliwości weryfikacji ustanowionych pierwotnie celów i polityki ciągłości działania.

Ponadto analizowana problematyka dotyczy bardzo charakterystycznych kwestii związanych z funkcjonowaniem, wręcz przetrwaniem organizacji. Biorąc pod uwagę wyniki analizy literatury przedmiotu, wymienić należy, również normatywnie opisane⁷:

- kontekst działania organizacji (środowisko wewnętrzne i otoczenie, wymagania, oczekiwania i ograniczenia, zakres systemu zarządzania ciągłością działania);
- przywództwo (zaangażowanie naczelnego kierownictwa, politykę bezpieczeństwa, przypisane role, uprawnienia i zakresy odpowiedzialności);

⁵ Tamże, 3.5.

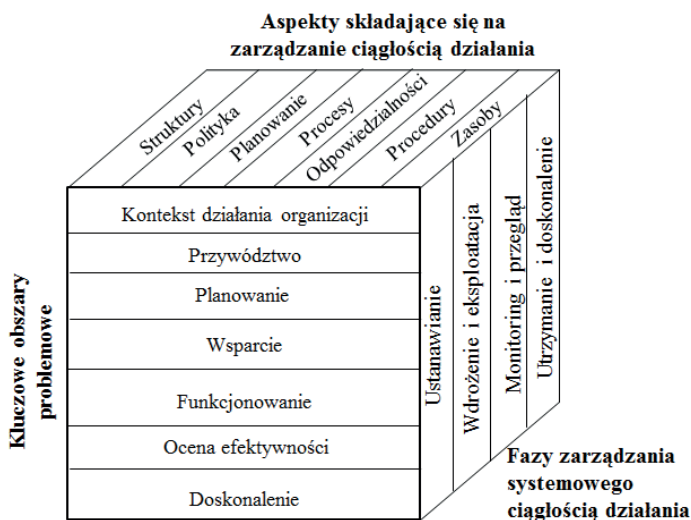
⁶ Zob. ISO 22301:2012..., 0.2.

⁷ Tamże, 4–10.

- planowanie (szanse i zagrożenia, cele służące zapewnianiu ciągłości działania);
- wsparcie (zasoby, kompetencje, świadomość personelu, komunikację wewnętrzną i zewnętrzną, dokumentowanie informacji);
- funkcjonowanie (planowanie i nadzór operacyjny, BIA i ocenę ryzyka, strategię ciągłości działania, procedury ciągłości działania);
- ocenę efektywności (monitorowanie, pomiary, analizę i ocenę właściwą, audyty, przeglądy);
- doskonalenie (identyfikację niezgodności i opracowywanie działań korygujących, ukierunkowanie na ciągłe doskonalenie systemowe).

Na rysunku 1 ukazano morfologiczne zrelatywizowanie opisanych powyżej kluczowych elementów problematyki ciągłości działania oraz systemowego podejścia do przedmiotowego zarządzania.

Rysunek 1. Morfologiczne ujęcie najważniejszych elementów problematyki systemowego zarządzania ciągłością działania



Źródło: opracowanie własne

2. Ciągłość działania a funkcjonowanie administracji publicznej

Istnieje wiele sposobów definiowania administracji publicznej⁸. Jedno z właściwych określeń traktuje o zespole działań, czynności i przedsięwzięć organi-

⁸ Szerzej: E. Ochendowski, *Prawo administracyjne. Część ogólna*, Toruń 2006, s. 19–24.

zatorskich i wykonawczych, które są prowadzone celem realizacji interesu publicznego przez różne podmioty, organy oraz instytucje na podstawie regulacji prawnych⁹. W przedstawionym sposobie rozumienia przejawia się systemowy charakter przedmiotu rozważań, do czego nawiązuje wprost kolejna definicja. Mówi ona o tym, że administracja to system złożony z ludzi zorganizowanych z ukierunkowaniem na stałą, systematyczną i perspektywiczną realizację dobra wspólnego ujmowanego w świetle misji publicznej, która polega głównie na praktycznym wdrażaniu w życie regulacji ustawowych, przy czym ludzie współtworzący omawiany system są wyposażeni we władztwo państwowe oraz środki materialno-techniczne niezbędne z punktu widzenia realizacji swoich zadań¹⁰.

W nawiązaniu do powyższego, wyróżnić można następujące cechy administracji publicznej (m.in.)¹¹:

- złożoność ilościowo-jakościową,
- prowadzenie działalności w imieniu państwa oraz w interesie publicznym,
- posiadanie władztwa administracyjnego,
- prowadzenie działalności na podstawie regulacji prawnych,
- ciągłość i stabilność działań,
- organizacyjne oddziaływanie na życie społeczne w odniesieniu do właściwości terytorialnej,
- monopolistyczność.

Wymienione cechy nakreślają kontekst organizacyjny administracji publicznej. Świadczą o jej istotnym udziale w perspektywie materializacji najważniejszych potrzeb publicznych. Z oczywistych przyczyn jedną z takich potrzeb oraz konstytucyjnym obowiązkiem państwa (w tym administracji publicznej działającej w imieniu państwa) jest zapewnienie bezpieczeństwa jego obywatelom. Stąd też nie powinna dziwić najwyższa ranga organów administracji publicznej w zarządzaniu bezpieczeństwem (państwa, narodowym, wewnętrznym, publicznym, społecznym, powszechnym, ekonomicznym, militarnym itd.). Na uwagę zasługuje chociażby fakt, że system zarządzania kryzysowego składa się wyłącznie z tego rodzaju podmiotów¹².

W świetle przedstawionej roli administracji publicznej jeszcze jedna jej cecha zdaje się wyróżniać na tle pozostałych. To ciągłość i stabilność działań. Skoro

⁹ Por. H. Izdebski, M. Kulesza, *Administracja publiczna. Zagadnienia ogólne*, Warszawa 1999, s. 79.

¹⁰ Por. Z. Niewiadomski (red.), *Prawo administracyjne. Część ogólna*, Warszawa 2007, s. 29.

¹¹ Por. J. Zimmermann, *Prawo administracyjne*, Warszawa 2010, s. 29; E. Ura, *Prawo administracyjne*, Warszawa 2010, s. 86.

¹² Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn.: Dz. U. z 2013 r. poz. 1166 z późn. zm.), art. 2.

bowiem organy administracji publicznej są wykonawcami zadań publicznych, to na najwyższym poziomie ogólności od ciągłości ich działań zależy ciągłość funkcjonowania całego państwa. Uwidaczniają się w tym miejscu dwa wymiary ciągłości działania administracji publicznej. Właściwe organy powinny bowiem zapewniać ciągłość funkcjonowania państwa jako instytucji (wymiar zewnętrzny), przy równoczesnym zachowywaniu ciągłości działań własnych (wymiar wewnętrzny).

Na tej podstawie można podjąć próbę zdefiniowania ciągłości działania administracji publicznej. Pod terminem tym należy rozumieć zdolność organów administracji publicznej do kontynuowania swojej działalności (świadczenia usług publicznych) po wystąpieniu zdarzenia zakłócającego ich funkcjonowanie, na poziomie jakości określonym uprzednio jako minimalny akceptowalny w odniesieniu do stanu funkcjonowania państwa oraz stanu funkcjonowania tych podmiotów.

Sformułowana definicja może posłużyć za punkt odniesienia w toku badania zależności zachodzących pomiędzy działalnością administracji publicznej a problematyką ciągłości działania. Nawiązując do wyników zastosowania intuicyjnej odmiany analizy morfologicznej tego zagadnienia, wpierając się przy tym zasygnalizowaną dualnością wymiarów przedmiotu rozważań, wyróżnia się następujące podejścia do omawianego zagadnienia wraz z charakteryzującymi je założeniami:

1. Podejście teoretyczne:

- W szerokim ujęciu cechy administracji publicznej jednoznacznie wskazują na jej powiązanie z aparatem władczym (kierowniczym, zarządczym) państwa. Z tego powodu właściwe organy mają realne przełożenie na funkcjonowanie całego narodu oraz współkonstytuowanej przez niego jednostki instytucjonalnej. Ciągłość działania administracji publicznej jest w tym kontekście równoznaczna z ciągłością działania państwa.
- W wąskim ujęciu świadomość istotnej roli organów administracji publicznej skłania ku stwierdzeniu, że do katalogu interesów narodowych należy zaliczyć ciągłość ich działania. W niniejszej perspektywie ciągłość działania administracji publicznej jest utożsamiana z ciągłością działania jej organów.

2. Podejście praktyczne:

- W szerokim ujęciu należy nawiązać do bezpośredniego przełożenia oddziaływania organów administracji publicznej na bezpieczeństwo systemów, obiektów, urządzeń, instalacji i usług kluczowych z punktu widzenia niezakłócalności funkcjonowania całego państwa. Mowa o infrastrukturze krytycznej. W przedmiotowym świetle ciągłość działania administracji publicznej wiąże się nierozzerwanie z kreowaniem i utrzymywaniem warunków zapewniania ciągłości działania infrastruktury krytycznej.

- W wąskim ujęciu systemy zapewniające ciągłość działania administracji publicznej są wymieniane wprost jako te wpisujące się do ogólnego katalogu elementów infrastruktury krytycznej. Szerzej, organy administracji publicznej również można traktować jako zasób infrastruktury krytycznej. Pomimo zdecydowanego przekroczenia ram interpretacyjnych ustalonych w ustawie o zarządzaniu kryzysowym, taki sposób rozumienia zdaje się wychodzić naprzeciw aktualnym trendom rozwoju problematyki ciągłości działania w Polsce i na całym świecie¹³.

Na rysunku 2 zobrazowano ideę badania relacji zachodzących w obrębie problematyki ciągłości działania w funkcjonowaniu administracji publicznej, uwzględniającą wskazane perspektywy i ujęcia badawcze.

Rysunek 2. Idea badania relacji zachodzących w obrębie problematyki ciągłości działania w funkcjonowaniu administracji publicznej

		Perspektywa	
		Teoretyczna	Praktyczna
Ujęcie	Szerokie	Ciągłość działania administracji publicznej to ciągłość działania państwa	Kreowanie i moderowanie warunków ochrony infrastruktury krytycznej
	Wąskie	Ciągłość działania administracji publicznej to ciągłość działania jej organów	Administracja publiczna jako zasób infrastruktury krytycznej

Źródło: opracowanie własne

¹³ Konkluzje po międzynarodowym seminarium na temat ciągłości działania administracji publicznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2016 r.

Niezwykle trudno określić, które z zaprezentowanych wypadkowych podejść i ujęć są cenniejsze poznawczo na tle pozostałych. Nie budzi jednak wątpliwości spostrzeżenie, iż branie pod uwagę wszystkich czterech pozwala na wieloaspektowe podejście, szczególnie istotne w odniesieniu do niezwykle zróżnicowanych zagrożeń bezpieczeństwa narodowego, w tym bezpieczeństwa powszechnego.

3. Zapewnianie ciągłości działania w kontekście bezpieczeństwa powszechnego

Praktycy zarządzania ciągłością działania niejednokrotnie wskazują na zagrożenia bezpieczeństwa powszechnego jako znacząco rzutujące na zdolność organizacji do kontynuowania swojej działalności (dostarczania produktów i/lub świadczenia usług) na poziomie jakości określonym uprzednio jako minimalny akceptowalny¹⁴.

Do zagrożeń bezpieczeństwa powszechnego, czyli czynników negatywnie wpływających na bezpieczeństwo (wolność od zagrożeń, a także niezakłócone byt i rozwój) ludności cywilnej w wymiarach egzystencjalnym oraz bytowo-kulturowym zalicza się¹⁵:

- pożary;
- powodzie i podtopienia;
- upały i susze;
- skażenia chemiczne;
- zakłócenia w dostawach energii elektrycznej;
- zakłócenia w dostawach paliw płynnych;
- zakłócenia w dostawach gazu;
- silne mrozy;
- intensywne opady śniegu;
- huragany;
- epidemie;
- epizootie;
- epifitozy;
- katastrofy budowlane;
- skażenia radiacyjne.

¹⁴ P. Gromek, *Współpraca z Państwową Strażą Pożarną w ramach zarządzania kryzysowego w świetle Business Continuity Management*, seminarium zamknięte, Związek Banków Polskich, Warszawa 2015.

¹⁵ Por. Krajowy Plan Zarządzania Kryzysowego 2013/2015, RCB, Warszawa.

Biorąc pod uwagę perspektywy i ujęcia wspólnego traktowania problematyki ciągłości działania oraz funkcjonowania administracji publicznej, truizmem jest stwierdzenie, że zagrożenia bezpieczeństwa powszechnego wpływają również na kluczowe obszary działalności organów administracji publicznej. Dokładne zbadanie tego oddziaływania jest możliwe dopiero po zidentyfikowaniu właściwych procesów kluczowych. Uwzględniając wrażliwość przedmiotowych informacji, warto przyjąć stosunkowo wysoki poziom ogólności, sprowadzający rozważania na grunt identyfikacji wspomnianych procesów na podstawie zadań własnych administracji publicznej. W tabeli 1 przedstawiono przykładowe procesy kluczowe przypisane do wybranych zadań własnych administracji publicznej.

Tabela 1. Przykładowe procesy kluczowe w funkcjonowaniu administracji publicznej w Polsce (wysoki poziom ogólności)

Lp.	nazwa grupy zadań własnych	szczebel administracji publicznej	przykładowe procesy krytyczne (wysoki poziom ogólności)
1	sprawowanie władzy ustawodawczej	centralny	dostęp do infrastruktury; minimalny skład osobowy
2	zarządzanie kryzysowe	centralny	dostęp do wiedzy eksperckiej; dostęp do sprawdzonych informacji na temat sytuacji kryzysowej
3	alarmowanie przeciwpowodziowe	wojewódzki	warunki techniczne na potrzeby alarmowania ludności
4	zarządzanie kryzysowe	wojewódzki	kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa
5	edukacja publiczna	powiatowy	dostęp do edukacji publicznej
6	sprawy ochrony przeciwpożarowej	powiatowy	funkcjonowanie krajowego systemu ratowniczo-gaśniczego
7	sprawy ochrony zdrowia	gminny	dostęp do świadczeń z zakresu podstawowej opieki zdrowotnej, położnictwa i ginekologii oraz stomatologii
8	sprawy ochrony przeciwpowodziowej	gminny	monitoring powodziowy; zapewnienie warunków do ewakuacji ludzi, zwierząt i mienia

Źródło: opracowanie własne

Analizując charakter zidentyfikowanych procesów kluczowych, można zauważyć zróżnicowany stopień ich wpływu na bezpieczeństwo narodowe, w tym zarządzanie kryzysowe ujmowane w myśl właściwych regulacji ustawowych. Jednakże oczywistym pozostaje fakt, że ich zakłócenie może przekładać się na realną i odczuwalną wolność od zagrożeń, a także zakłócone byt i rozwój społeczności gmin, powiatów, województw, a nawet całego państwa. Istotnymi źródłami zakłóceń są natomiast zagrożenia bezpieczeństwa powszechnego.

W tabeli 2 zestawiono przykłady wpływu zagrożeń bezpieczeństwa powszechnego na procesy kluczowe w funkcjonowaniu administracji publicznej w Polsce.

Tabela 2. Przykłady wpływu zagrożeń bezpieczeństwa powszechnego na procesy kluczowe w funkcjonowaniu administracji publicznej w Polsce

Lp.	przykładowe procesy kluczowe (wysoki poziom ogólności)	przykłady wpływu zagrożeń bezpieczeństwa powszechnego
1	dostęp do infrastruktury niezbędnej do kierowania bezpieczeństwem narodowym	zniszczenie lub znaczne uszkodzenie podstawowej lokalizacji władzy ustawodawczej wskutek pożaru wewnętrznego
2	minimalny skład osobowy na potrzeby stanowienia ustaw	trudności w zebraniu minimalnego składu osobowego podczas całkowitego zaniku dostępu do energii elektrycznej (<i>blackout</i>)
3	dostęp do wiedzy eksperckiej na potrzeby zarządzania kryzysowego na szczeblu centralnym	bezpośrednie zaangażowanie ekspertów w działania operacyjne w strefie zagrożenia radiologicznego podczas powodzi
4	dostęp do sprawdzonych informacji na temat sytuacji kryzysowej	chaos informacyjny spowodowany kaskadowym wpływem wiatrów huraganowych na powstawanie w skali masowej pożarów, uszkodzeń konstrukcji budowlanych oraz utratę dostępu do energii elektrycznej (<i>blackout</i>)
5	warunki techniczne na potrzeby alarmowania ludności na poziomie województwa	uszkodzenia fizyczne systemu syren alarmowych wskutek oddziaływania silnych mrozów i intensywnych opadów śniegu
6	kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa	katastrofa budowlana podstawowej lokalizacji centrum zarządzania kryzysowego obsługującego wojewodę

7	dostęp do edukacji publicznej w powiecie	skażenie chemiczne placówki oświatowej zlokalizowanej w pobliżu trasy transportu drogowego substancji niebezpiecznych (ADR)
8	funkcjonowanie krajowego systemu ratowniczo-gaśniczego na poziomie powiatu	dysponowanie zasobów odwodu operacyjnego do wsparcia działań ratowniczo-gaśniczych w obliczu wielkoobszarowego pożaru lasu w sąsiednim województwie
9	dostęp do świadczeń z zakresu podstawowej opieki zdrowotnej, położnictwa i ginekologii oraz stomatologii na poziomie gminy	utrata dostępu do energii elektrycznej w placówkach publicznych zakładów opieki zdrowotnej wskutek zerwania oblodzonych linii energetycznych
10	monitoring powodziowy w gminie	zniszczenie przez falę powodziową systemu monitoringu powodziowego na terenie gminy
11	zapewnienie warunków do ewakuacji ludzi, zwierząt i mienia na terenie gminy	wyłączenie stacji paliw płynnych zlokalizowanych na terenie gminy jako konsekwencja zakłóceń w dostawach energii elektrycznej

Źródło: opracowanie własne

Wyniki analizy wpływu wybranych zagrożeń bezpieczeństwa powszechnego na przykładowe procesy kluczowe pozwalają na konkluzję, że badany rodzaj zagrożeń rzutuje w znacznej mierze na dostępność zasobów, których wykorzystanie jest niezbędne z punktu widzenia ciągłości działania administracji publicznej. Dotyczy to głównie zasobów ludzkich, rzeczowych i informacyjnych. Oczywistym jest, że pośredni wpływ będzie można zaobserwować także w przypadku zasobów finansowych. Dlatego głównym kierunkiem zapewniania przedmiotowej ciągłości działania powinna być dbałość o wyznaczenie i utrzymanie zasobów alternatywnych, możliwych do uruchomienia w obliczu zakłóceń w postaci pożarów, powodzi, katastrofalnych w skutkach zjawisk pogodowych i chorobowych, uwolnienia niebezpiecznych czynników chemicznych i radiologicznych, utraty dostępu do energii elektrycznej, paliw, gazu itp.

4. Rekomendacje dla administracji publicznej

Formułując rekomendacje z zakresu ciągłości działania administracji publicznej w kontekście zagrożeń bezpieczeństwa powszechnego, warto wziąć pod uwagę dwa wzajemnie uzupełniające się podejścia – konceptualne i praktyczne.

Z założenia stworzy to możliwości elastycznego dopasowywania wytycznych i wskazówek do uwarunkowań funkcjonowania na poszczególnych szczeblach administracji publicznej w Polsce, a także w odniesieniu do konkretnych jednostek terytorialnych.

Ujęcie konceptualne dotyczy ciągłości działania rozumianej jako atrybut administracji publicznej. Z praktycznego punktu widzenia zaprzestanie jej działania to bezpośredni krok ku bezprawiu, anarchii i rozpadowi instytucji państwa. W niniejszym świetle warto rozważyć pozytywne ustosunkowanie się do następujących zaleceń:

1. Ciągłość działania należy uznać za jeden z najważniejszych wskaźników potencjału sprawnego państwa i organów władczych stojących na straży jego niepodległości. Oznacza to konieczność głębokiego zakorzenienia przedmiotowej problematyki w świadomości podmiotów kierujących bezpieczeństwem narodowym, czyli głównie organów administracji publicznej. Aktualnie ciągłość działania zdaje się być nad wyraz oczywistym, aczkolwiek niepodkreślanym aspektem bezpieczeństwa narodowego. Zmiana tego podejścia pozwoli na stworzenie fundamentów pod predyktywne projektowanie przyszłości państwa i narodu.
2. Istotą ciągłości działania administracji publicznej powinno być zapewnianie zdolności do kontynuowania swojej działalności rozumianej w świetle świadczenia usług publicznych po wystąpieniu wszelkiego rodzaju zdarzeń zakłócających jej funkcjonowanie, na poziomie jakości określonym uprzednio jako minimalny akceptowalny. W tym kontekście należy podkreślić, że administracja publiczna powinna być przygotowana na pojawianie się przedmiotowych zagrożeń we wszystkich stanach funkcjonowania państwa, a nawet w czasie wojny.
3. Z uwagi na ściśle zrelatywizowanie ciągłości działania administracji publicznej ze względu na aparat zarządczy państwa, zaleca się traktować o niej w sposób systemowy. Pozwoli to wykorzystać analogie funkcjonalne występujące pomiędzy systemem zarządzania ciągłością działania a systemem kierowania bezpieczeństwem narodowym, w tym system zarządzania kryzysowego.
4. Zapewnianie ciągłości działania administracji publicznej należy brać pod uwagę przy projektowaniu i wprowadzaniu wszelkich zmian o systemowym lub niesystemowym charakterze w odniesieniu do obszarów prawa korespondujących z zadaniami stawianymi na poszczególnych szczeblach zarządzania państwem.
5. Przedsięwzięcia ukierunkowane na zapewnianie ciągłości działania powinny dotyczyć nie tylko administracji publicznej jako organizacyjnej całości, lecz również odnosić się do jej poszczególnych jednostek (organów, urzędów itp.).

Wdrożenie rekomendacji sformułowanych w świetle ujęcia konceptualnego to zasadniczy etap budowania swoistej kultury ciągłości działania poprzez stopniowe zwiększanie właściwej świadomości.

Ujęcie praktyczne wyraża się w bezpośrednim czerpaniu ze sprawdzonych, międzynarodowych standardów ciągłości działania. Istnieje bowiem wiele rekomendacji stosowanych w pragmatyce funkcjonowania organizacji *for profit*, które mogą stanowić inspirację w zapewnianiu ciągłości działania administracji publicznej. Implementując część z nich na grunt przedmiotu poznania, sformułowano następujące rekomendacje dla administracji publicznej:

1. Procesy kluczowe i procesy krytyczne należy wyznaczać na podstawie zadań własnych oraz innych zadań przypisanych regulacjami prawnymi do poszczególnych rodzajów i szczebli administracji publicznej. Z uwagi na ich wrażliwość zaleca się rozważenie ustalenia poziomu szczegółowości, powyżej którego będą obowiązywały klauzule informacji niejawnych.
2. Plany zarządzania kryzysowego powinny dotyczyć zdecydowanie szerszego katalogu zagrożeń niż jedynie tych rzutuujących na bezpieczeństwo powszechne i bezpieczeństwo publiczne. Zaleca się, aby wykorzystać je do integracji dokumentów, które stanowią o planowaniu cywilnym w Polsce. Ich formułowanie na wzór planów ciągłości działania pozwoli uwypuklić kwestie nie tylko zapobiegania, przygotowania, reagowania i odbudowy, lecz także konieczności utrzymania usług publicznych świadczonych przez państwo i poszczególne jednostki administracji publicznej na minimalnym poziomie jakości bez względu na aktualną fazę zarządzania kryzysowego w rozpatrywanym kontekście.
3. Procesy komunikacyjne powinny przebiegać zgodnie z założeniami komunikacji kryzysowej. Oznacza to konieczność sformułowania procedur awaryjnych stosowanych w kontaktach z mediami w obliczu predefiniowanych okoliczności, a także merytoryczne i metodyczne przygotowanie osób piastujących stanowiska lub funkcje rzeczników prasowych oraz specjalistów z zakresu public relations. Samą komunikację kryzysową należy postrzegać również z dwóch perspektyw – zewnętrznej (rozumianej jako wymiana informacji podmiotu administracji publicznej z otoczeniem) oraz wewnętrznej (utożsamianej z przepływami informacyjnymi wewnątrz tego podmiotu).
4. Osoby piastujące istotne z punktu widzenia ciągłości działania funkcje powinny być bezwzględnie zastępowalne. Związane z tym aspektem przerywanie łańcucha kierowania powinno zostać opisane proceduralnie.
5. Najważniejsze elementy infrastruktury administracji publicznej powinny zostać powielone i zlokalizowane w odległości zapewniającej izolacyjność

względem zagrożeń, które mogą dotyczyć ich lokalizacji pierwotnych. Oznacza to konieczność przygotowania się na ewentualność ewakuacji wybranych personelu i mienia (dokumentów, baz danych, aparatury itp.) do lokalizacji alternatywnych.

6. Ochrona istotnych informacji powinna się wyrażać w powieleniu zasobów informacyjnych na elektronicznych nośnikach informacji. Zapasowe serwery i bazy danych należy zintegrować funkcjonalnie z lokalizacjami alternatywnymi.
7. Operatorzy wybranych rodzajów infrastruktury krytycznej od wielu lat funkcjonują na podstawie standardów ciągłości działania. Wynika to wręcz z regulacji prawnych (np. sektor bankowy, sektor energetyczny, sektor ubezpieczeń społecznych). Administracja publiczna powinna cechować się otwartością na współpracę w zakresie ochrony infrastruktury krytycznej, a także wymianę przedmiotowych doświadczeń.
8. Ćwiczenia z zakresu obronności, zarządzania kryzysowego i obrony cywilnej można zorganizować tak, aby sprawdzały one, niejako przy okazji, opracowane i wdrożone procedury ciągłości działania.

Wyszczególnione rekomendacje z oczywistych przyczyn nie stanowią katalogów zamkniętych. Zostały sformułowane na relatywnie wysokim poziomie ogólności. Starano się dzięki temu zachować ich uniwersalność. Należy pamiętać, że ciągłość działania administracji publicznej w obliczu zagrożeń bezpieczeństwa powszechnego to złożona problematyka. Niemniej jednak przytoczone wskazówki pozwolą niejako wyjść naprzeciw aktualnym trendom zmian w sposobach zapewniania bezpieczeństwa narodowego.

Bibliografia

Literatura:

- Gromek P., *Współpraca z Państwową Strażą Pożarną w ramach zarządzania kryzysowego w świetle Business Continuity Management*, seminarium zamknięte, Związek Banków Polskich, Warszawa 2015
- Izdębski H., Kulesza M., *Administracja publiczna. Zagadnienia ogólne*, Warszawa 1999.
- Kaszubski R. W., Romańczuk D. (red.), *Księga dobrych praktyk w zakresie zarządzania ciągłością działania. Business Continuity Management*, Warszawa 2011.
- Niewiadomski Z. (red.), *Prawo administracyjne. Część ogólna*, Warszawa 2007.
- Ochendowski E., *Prawo administracyjne. Część ogólna*, Toruń 2006.
- Ura E., *Prawo administracyjne*, Warszawa 2010.
- Zimmermann J., *Prawo administracyjne*, Warszawa 2010.

Akty prawne:

ISO 22301:2012 Societal security. Business continuity management systems. Requirements.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz. U. z 1997 r. nr 78, poz. 483 z późn. zm.).

Krajowy Plan Zarządzania Kryzysowego 2013/2015, RCB, Warszawa.

Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (tekst jedn. Dz. U. z 2015 r. poz. 525 z późn. zm.).

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

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tekst jedn. Dz. U. z 2016 r. poz. 814, z późn. zm.).

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (tekst jedn. Dz. U. z 2016 r. poz. 446, z późn. zm.).

Wykaz wykresów:

Rysunek 1. Morfologiczne ujęcie najważniejszych elementów problematyki systemowego zarządzania ciągłością działania.

Rysunek 2. Idea badania relacji zachodzących w obrębie problematyki ciągłości działania w funkcjonowaniu administracji publicznej.

Wykaz tabel:

Tabela 1. Przykładowe procesy kluczowe w funkcjonowaniu administracji publicznej w Polsce (wysoki poziom ogólności).

Tabela 2. Przykłady wpływu zagrożeń bezpieczeństwa powszechnego na procesy kluczowe w funkcjonowaniu administracji publicznej w Polsce.

Streszczenie

Ciągłość działania administracji publicznej nabiera szczególnie na znaczeniu w obliczu zagrożeń bezpieczeństwa powszechnego. Pożary, powodzie, niszczy-cielskie zjawiska pogodowe, zagrożenia chemiczne, zagrożenia radiologiczne, a także przerwanie dostępu do paliw płynnych, gazu i energii elektrycznej stano-wią wybrane czynniki rzutujące na bezpieczeństwo podmiotów odpowiedzial-nych za zapewnianie bezpieczeństwa narodowego.

Problematykę ciągłości działania w funkcjonowaniu administracji publicznej można badać w dwóch ujęciach (wewnętrznym i zewnętrznym) oraz dwóch perspektywach (teoretycznej i praktycznej). Dzięki tak unikalnemu połączeniu podejść badawczych możliwa jest implementacja międzynarodowych standardów ciągłości działania. W głównej mierze dotyczą one zwiększania świadomości, alternatywności zasobów oraz tworzenia procedur. W tym kontekście ciągłość działania administracji publicznej może być rozumiana jako integrator wielu obszarów kierowania bezpieczeństwem narodowym.

Słowa kluczowe: administracja publiczna, ciągłość, ciągłość działania, bez-pieczestwo.

Summary

Continuity of public administration in a face of general security threats

Continuity of public administration gains in importance in a face of general se-curity threats. Fires, floods, destructive weather phenomenon, chemical threats, radiological threats as well as breaks in fuel, gas and energy supply constitute chosen factors affecting security of entities responsible for national security.

Problematic aspects of continuity in public administration operations can be analyzed in two approaches (internal one and external one) and two perspectives (theoretical one and practical one). Owing to such kind of unique connection of research directions, implementation of international continuity standards is pos-sible. In main realm, the standards concern awareness raising, alternativeness of resources and procedural obtaining. In this context public administration continuity can be understood as an integrator of many fields in national security management.

Key words: public administration, continuity, business continuity, security.

Rozdział VII.

Bezpieczeństwo zdrowotne w działaniach organów władzy publicznej w Polsce

1. Zapewnienie bezpieczeństwa zdrowotnego

W Sprawozdaniu z ogólnopolskiej konferencji naukowej pt. *Przedsiębiorczość w służbie zdrowia: „Podmioty niepubliczne w publicznej służbie zdrowia”*, pod red. Anny Gołębiowskiej oraz Marka Wocha, która odbyła się 12 maja 2016 r. w Sejmie RP, wspólnie ze Zbigniewem Teterem wskazaliśmy, że: „każda żywa istota dąży do zapewnienia sobie bezpieczeństwa. Bezpieczeństwa dającego szansę na przeżycie swoje i swojego potomstwa. Przeżycie w optymalnych warunkach, dla zachowania ciągłości gatunku. Człowiek w dążeniu do optymalnego bezpieczeństwa nie wyróżnia się zbyt wiele spośród innych gatunków. Pierwotne osobniki zapewniały sobie bezpieczeństwo we własnym zakresie. W rozwiniętych społeczeństwach odpowiedzialność za organizację systemów bezpieczeństwa powierzono władzy. To władza opowiada za poczucie bezpieczeństwa swoich obywateli. W naszych aktualnych polskich warunkach jest to demokratycznie wybrany rząd, reprezentujący państwo oraz jego mieszkańców. Rząd ma zapewnić również jeden z najważniejszych elementów bezpieczeństwa, jakim jest bezpieczeństwo zdrowotne. Obowiązkiem państwa jest zorganizowanie systemu opieki zdrowotnej w taki sposób, by zapewnić w sposób optymalny poczucie bezpieczeństwa zdrowotnego obywateli”.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r.¹, przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., w przepisie art. 5 wskazuje, że Rzeczpospolita Polska strzeże niepodległości swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju.

W mojej ocenie przywołane w przepisie art. 5 Konstytucji RP z dnia 2 kwietnia 1997 r. bezpieczeństwo obywateli również obejmuje bezpieczeństwo zdrowotne, które powinno podlegać ochronie przez organy władzy publicznej².

System ochrony zdrowotnej może bezpośrednio podlegać zarządzaniu przez państwo lub podlegać silnym regulacjom prawnym. Stosunki własnościowe realizatorów zadań systemu powinny być z punktu widzenia klienta (świadczeniobiorcy, pacjenta) obojętne. Istotą jest zapewnienie bezpieczeństwa zdrowotnego na wysokim poziomie. Widać to doskonale na przykładzie jednego z segmentów ochrony zdrowia, jakim jest lecznictwo uzdrowiskowe od lat regulowane przez ustawę uzdrowiskową. Właścicielami uzdrowisk i sanatoriów są zarówno Skarb Państwa, jednostki samorządu terytorialnego, jak i podmioty niepubliczne. Sytuacja finansowa i jakość świadczonych usług zależne są głównie od zarządzających i sposobów zarządzania³.

Jakość usług ze względu na dominację w uzdrowiskach medycyny uniwersalistycznej jest szczególnie ważna, należy ją poprawiać poprzez:

- wypracowanie standardów postępowania leczniczego;
- tworzenie i wdrażanie programów ukierunkowanych na potrzeby zdrowotne stale rosnącej populacji ludzi starszych;
- ściślejsze łączenie leczenia szpitalnego z wczesną rehabilitacją w warunkach uzdrowiskowych⁴.

¹ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz. U. z 1997 r. nr 78, poz. 483 z późn. zm.), dalej: Konstytucja RP z dnia 2 kwietnia 1997 r.

² Por. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. z 2010 r. nr 83, poz. 540), RCB, *Ocena ryzyka na potrzeby zarządzania kryzysowego Raport o zagrożeniach bezpieczeństwa narodowego*, Warszawa 2013. Raport o zagrożeniach bezpieczeństwa narodowego stanowi podstawę dla procesu planowania cywilnego. Wnioski z raportu stanowią element Krajowego Planu Zarządzania Kryzysowego oraz są uwzględniane w planach zarządzania kryzysowego.

³ Por. Z. Teter, A. Kosowski, B. Jabłońska, K. Kiefert, *Lecznictwo uzdrowiskowe w Polsce w latach 2005–2015*, Warszawa 2016.

⁴ A. Gołębiowska, M. Woch (red.), *Sprawozdanie z ogólnopolskiej konferencji naukowej. Przedsiębiorczość w służbie zdrowia: „Podmioty niepubliczne w publicznej służbie zdrowia”*, Warszawa 2016.

2. Bezpieczeństwo zdrowotne w państwie demokratycznym

Zapewnienie prawa do ochrony zdrowia⁵ w państwie demokratycznym jest zagadnieniem wielopłaszczyznowym i wielopoziomowym⁶. Chciałbym natomiast poruszyć w niniejszym podrozdziale problematykę tego uprawnienia, przysługującego każdemu człowiekowi w Polsce. Termin wielopłaszczyznowości używany był przez Kazimierza Dąbrowskiego do określania m.in. wybranych struktur i funkcji społecznych i politycznych⁷. Natomiast uważam, że termin ten również idealnie pasuje do opisywania systemu finansowania opieki zdrowotnej⁸ i próby wykazania, że nie jest to linearny ciąg poszczególnych uczestników i zdarzeń w nim występujących, a zorganizowanie i usystematyzowanie instytucji w nim występujących wymaga skoordynowanych wielopoziomowych działań.

Zanim jednak przejdę do zagadnień ochrony zdrowia⁹, proszę zwrócić uwagę na kryteria demokratycznego państwa prawa, które Bronisław Jastrzębski przedstawił w następujący sposób: „podstawą państwa demokratycznego przede wszystkim są: wolność, równość, sprawiedliwość, praworządność i demokracja. Państwo prawa jest pojęciem pragmatycznym opartym na związku z rzeczywistością społeczną, bo integruje ustrojowe zasady państwa na gruncie prawa, jeśli jest oczywiście tworzone na podłożu społeczno-ekonomicznym i obywatelskim, i jego norm konstytucyjnych, zalegalizowanych przez ustawodawcę i władzę zwierzchnią, jaką jest Naród, w formie referendum”¹⁰.

Już sama definicja demokratycznego państwa prawa zdaniem Jerzego Jaskierni nastrocza trudności w precyzyjnym ustaleniu modelu tego terminu. Jego zdaniem, wątpliwość istnieje już na etapie ustalania, czy właściwsze jest ujęcie

⁵ Maria Szyszkowska wskazuje, że: „Życie i zdrowie człowieka to jedna z wartości, którą można uznać za niemal uniwersalną”; M. Szyszkowska, *Każdy bywa pacjentem. Zarys filozofii farmacji*, Warszawa 2010, s. 7.

⁶ Szerzej zob. J. Kornai, K. Eggleston, *Solidarność w procesie transformacji*, Warszawa 2002, s. 99–165, A. Czupryna, S. Poździejch, A. Ryś, C. Włodarczyk (red.), *Zdrowie publiczne*, tom I, Kraków 2000, s. 167–212; W.C. Włodarczyk, *Reforma opieki zdrowotnej w Polsce*, Kraków 1998, s. 13–43.

⁷ K. Dąbrowski, *Moralność w polityce. Wielopoziomowość funkcji uczuciowych i popędowych w życiu społecznym i politycznym oraz instytucjach*, Warszawa 1991, *passim*.

⁸ W mojej opinii system finansowania opieki zdrowotnej jest tylko jednym z elementów tzw. systemu ochrony zdrowia. Jednak ze względu na kwestie finansowe jest powszechnie przyjmowany, jako dominujący pogląd.

⁹ Szerzej zob. M. Dercz, H. Izdebski, *Organizacja ochrony zdrowia w Rzeczypospolitej Polskiej w świetle obowiązującego ustawodawstwa*, Warszawa – Poznań 2001, s. 9 i nast., gdzie autorzy przedstawiają dylematy terminologiczne pojęcia „ochrona zdrowia”; Także: M. Woch, *Instytucje kształtujące system opieki zdrowotnej w Polsce. (Analiza prawno-porównawcza lat 1918–2004)*, Warszawa 2012, s. 11.

¹⁰ B. Jastrzębski, *Polska – czy jest państwem prawa*, Płock 2009, s. 24–25.

demokratycznego państwa prawnego jako z a s a d y ustroju czy jako z a s a d ustroju. Podobnie z regułą tą wiąże się dylemat dotyczący zakresu egzekwowania zasad z niej płynących. Zwraca przy tym uwagę, że zbyt ni aktywizm wydobywania z demokratycznego państwa prawnego nowych reguł i norm może podważyć pewność prawa. Należy także wyraźnie odróżnić konstytucjonalizację tej zasady od procesu jej urzeczywistnienia¹¹.

Natomiast na temat Narodu John S. Mill pisał: „można powiedzieć, że narodowość jest tam, gdzie są ludzie połączeni wzajemnymi sympatiami, które nie są im pobudką do tego, że chętniej działają wspólnie ze sobą aniżeli z innymi, że aby ten rząd sprawowany był wyłącznie przez nich, albo przynajmniej przez jakąś część. Uczucie narodowości z rozmaitych przyczyn powstać może; czasami wspólnoty języka i religii, a nawet granice geograficzne przyczyniają się do jego powstania i rozwoju. Ale najważniejszą ze wszystkich jest tu wspólność przeszłości politycznej, wspólność historii narodowej, a więc wspólność wspomnień, powiązanych przez wspólną dumę i upokorzenie, smutki i radości wspólne. Jednakże żaden z tych warunków nie jest ani niezbędnie potrzebnym, ani sam jeden wystarczającym do utworzenia narodowości”¹².

¹¹ Szerzej zob. A. Chmielarz, J. Sułkowski, *Sprawozdanie z międzynarodowej konferencji naukowej „Demokratyczne państwo prawne w teorii i w praktyce w państwach Europy Środkowej i Wschodniej”*, Łódź, 4–6 września 2008 r., „Przegląd Sejmowy” 2009, nr 2, s. 236 i nast.; J. Zajadło, *Demokratyczne państwo prawne w teorii i w praktyce w państwach Europy Środkowej i Wschodniej*, K. Skotnicki (red.), „Przegląd Sejmowy” 2011, nr 3, s. 196–197; Także: M. Pietrzak, *Demokratyczne świeckie państwo prawne*, Warszawa 1999, s. 27 i nast.; A. Rost, *Instytucje prawa konstytucyjnego*, Poznań 2003, s. 39 i nast.; S. Wronkowska (red.), *Zasada demokratycznego państwa prawnego w Konstytucji RP*, Warszawa 2006; H. Suchocka (red.), *Tworzenie prawa w demokratycznym państwie prawnym*, Warszawa 1992; E. Morawska, *Klauzula państwa prawnego w Konstytucji RP na tle orzecznictwa Trybunału Konstytucyjnego*, Toruń 2003, s. 19 i nast.; T. Kozłowski, *Spór o obecne pojęcie prawa*, [w:] *Teoretycznoprawne problemy integracji europejskiej*, L. Leszczyński (red.), Lublin 2004, s. 11 i nast.; W. Staśkiewicz, *Demokratyczne państwo prawne w Polsce lat dziewięćdziesiątych: eufunkcjonalność teorii i dysfunkcjonalność praktyki*, [w:] *Prawo i ład społeczny*, Księga Jubileuszowa dedykowana Profesor Annie Turskiej, Warszawa 2000, s. 110–140.

¹² John S. Mill, *O rządzie reprezentatywnym. Poddaństwo kobiet*, Kraków – Warszawa 1995, s. 245. Szerzej zob. K. Grzybowski, *Historia doktryn politycznych i prawnych*, Warszawa 1968, s. 370 i nast.; C. Strzeszewski, *Katolicka Nauka Społeczna*, Warszawa 1985, s. 503 i nast.; W. Lutosławski, *Ludzkość Odrodzona. Wizje przyszłości*, Warszawa 1910, s. 214 i nast.; A. Rossmannith, *Antropologiczna perspektywa rozważań o demokracji w ujęciu Wincentego Lutosławskiego*, [w:] *Wincenty Lutosławski (1863–1954). Materiały z posiedzenia Naukowego PAU w dniu 19 XI 2004 r.*, Polska Akademia Umiejętności Archiwum Nauki PAN i PAU w Służbie Nauki nr 16, Kraków 2010, s. 127–139; C. Znamierowski, *Szkoła prawa: Rozważania o państwie*, Warszawa 1999, s. 72 i nast.; A. Kryniecka-Piotrak, *Koncepcja demokracji w poglądach filozoficznych Czesława Znamierowskiego*, praca doktorska napisana pod kierunkiem prof. dr hab. Marii Szyzkowskiej, Warszawa 2003 (niepublikowana); M. Oakeshott, *O postępowaniu człowieka*, Warszawa 2008, s. 313 – gdzie autorzy podjęli próbę zdefiniowania pojęcia „Naród”.

Mając na względzie terminy „demokratyczne państwo prawa” oraz „Naród”, biorę za punkt wyjścia do moich dalszych rozważań Konstytucję RP z dnia 2 kwietnia 1997 r., która stanowi w przepisie art. 2, iż: „Rzeczpospolita Polska jest demokratycznym państwem prawnym¹³, urzeczywistniającym zasady sprawiedliwości społecznej”, w art. 38: „Rzeczpospolita Polska zapewnia każdemu człowiekowi prawną ochronę życia”, a w art. 68:

- „1. Każdy ma prawo do ochrony zdrowia.
2. Obywatelom, niezależnie od ich sytuacji materialnej, władze publiczne zapewniają równy dostęp do świadczeń opieki zdrowotnej finansowanej ze środków publicznych. Warunki i zakres udzielania świadczeń określa ustawa.
3. Władze publiczne są obowiązane do zapewnienia szczególnej opieki zdrowotnej dzieciom, kobietom ciężarnym, osobom niepełnosprawnym i osobom w podeszłym wieku.
4. Władze publiczne są obowiązane do zwalczania chorób epidemicznych i zapobiegania negatywnym dla zdrowia skutkom degradacji środowiska.
5. Władze publiczne popierają rozwój kultury fizycznej, zwłaszcza wśród dzieci i młodzieży”.

3. Odpowiedzialność władz publicznych za bezpieczeństwo zdrowotne

Wydawałoby się, że sprawa jest oczywista – prawo do ochrony zdrowia, a w tym kontekście i życia, przysługuje każdemu ze środków publicznych. Natomiast wykonanie uprawnień leży w gestii władz publicznych. W tym momencie pojawia się jednak problem z taką interpretacją, ponieważ podczas rozmów w różnych środowiskach zajmujących się tą tematyką, ale również z ust każdego człowieka, który wcześniej czy później będzie osobą potrzebującą

¹³ W orzecznictwie Trybunału Konstytucyjnego utrwalony jest pogląd, iż ogólne zasady, wynikające z art. 2 Konstytucji, powinny być przestrzegane szczególnie restryktywnie, jeśli chodzi o akty prawne odnoszące się do fundamentalnych wartości chronionych przez Konstytucję. Szczególnie doniosłe znaczenie winny one mieć na płaszczyźnie wolności i praw człowieka i obywatela (K 33/00, OTK ZU nr 7/2001, poz. 217) – także w odniesieniu do wolności i praw ekonomicznych, socjalnych i kulturalnych, wśród których jest gwarantowane przez art. 68 ust. 1 Konstytucji prawo do ochrony zdrowia. Starannej realizacji dyrektyw, wynikających z zasad przyzwoitej legislacji, należy wymagać od ustawodawcy zwykłego zwłaszcza przy reglamentacji prawnej tych sfer, które zostały uznane za szczególnie newralgiczne przez samego ustrojodawcę; Wyrok TK z dnia 7 stycznia 2004 r., sygn. akt (K 14/03), OTK – A 2004, nr 1A, poz. 1. (Dz. U. z 2004 r. nr 5, poz. 37); (dalej: Wyrok TK z dnia 7 stycznia 2004 r.); Zob. także: J. Galster, W. Szyszkowski, Z. Wasik, Z. Witkowski, *Prawo konstytucyjne*, Toruń 1995, s. 68 i nast.; W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2007, s. 12–13.

pomocy lub już był beneficjentem systemu ochrony zdrowotnej, pada pytanie: Co obligatoryjnie powinno być publiczne, a co może być prywatne w systemie opieki zdrowotnej?¹⁴

Pozostaje również kwestia odpowiedzialności władz publicznych¹⁵, które mają zapewnić równy dostęp do świadczeń opieki zdrowotnej finansowanej ze środków publicznych. Już na tym polu pojawia się kolejna kwestia niedookreślona, ponieważ władze publiczne mają je tylko „zapewnić”¹⁶, a nie np. „zagwarantować”¹⁷.

Natomiast między „zapewnić”, jak to jest zapisane w Konstytucji RP, a „zagwarantować”, jak postulują inni, różnica jest subtelna, ale moim zdaniem bardzo istotna. Chodzi mianowicie o odpowiedzialność, która spoczywać ma tylko na

¹⁴ M. Biardzki, *Publiczne czy prywatne – dylemat na nową kadencję*, „Służba Zdrowia”, dziennik ogólnopolski z dnia 17 października 2011 r., s. 7–9 i nast.

¹⁵ Por. Wyrok TK z dnia 7 stycznia 2004 r.; Wyrok TK z dnia 27 czerwca 2000 r., sygn. akt (K 20/99), OTK – A 2000, nr 5, poz. 140; „Poprzez określenie zakładów opieki zdrowotnej mianem „publiczny” ustawodawca uznał, że ich znaczenie jest doniosłe z punktu widzenia interesu publicznego. Na tyle ważne, aby uznać konieczność ich podporządkowania rządowym lub samorządowym organom państwa, chociaż przez nadanie im osobowości prawnej uzyskały one duży stopień samodzielności oraz niezależną od Skarbu Państwa i jednostek samorządu terytorialnego podmiotowość prawną (w sferze stosunków majątkowych). Okoliczność, iż w odniesieniu do publicznych, samodzielnych zakładów opieki zdrowotnej organami tworzącymi są organy administracji rządowej lub jednostki samorządu terytorialnego, stwarza gwarancję i zabezpieczenie, że zakłady te będą mogły realizować cele, dla których je utworzono. Wiąże się z tym – w określonych ustawowo sytuacjach – zobowiązanie do ponoszenia konsekwencji majątkowych związanych z ich działalnością. Ani organ administracji rządowej, ani jednostka samorządu terytorialnego nie może uwolnić się od tego rodzaju obowiązków bez stosownego ustawowego przyzwolenia. W ten sposób zabezpiecza się możliwość realizowania celów publicznych związanych z ochroną zdrowia, o których mowa w art. 68 Konstytucji”. Sąd Najwyższy w wyroku z dnia 8 października 2009 r. (sygn. akt II PK 110/09) zauważył, że „Samodzielne Publiczne Zakłady Opieki Zdrowotnej, jakkolwiek odrębne od Skarbu Państwa organizacyjnie i niezależne finansowo, stanowią jednak emanację państwa z uwagi na celowość ich tworzenia i likwidowania (zwłaszcza w kontekście prawa równego dostępu do świadczeń opieki zdrowotnej – art. 68 ust. 2 zd. 1 Konstytucji RP) oraz sposobu finansowania (swoista zależność od środków publicznych), jak również w ramach systemu opieki zdrowotnej finansowanej ze środków publicznych przez NFZ”. Z pisma z dnia 4 stycznia 2010 r. Izby Skarbowej w Warszawie (IPPP1/443-1019/09-2/MP) wynika, że gmina również jest organem władzy publicznej. Jeżeli tak szeroko ujmijemy ten termin, to należy określić katalog działań na rzecz mieszkańców w kwestii ochrony zdrowia na danym terenie.

¹⁶ J. Bralczyk (red.), *Słownik 100 tysięcy potrzebnych słów*, Warszawa 2008, s. 979: „zapewnić” – 1. oświadczyć komuś, że coś jest lub będzie na pewno, 2. sprawić, że coś się stanie lub ktoś uzyska coś.

¹⁷ Tamże, s. 221. „gwarancja” – to inaczej poręczenie, zobowiązanie, które ktoś nam daje, biorąc tym samym odpowiedzialność za coś lub za kogoś. Staje się wtedy gwarantem. Kiedyś mówiono o gwarantach naszej niezależności: jeśli mi ktoś gwarantuje niezależność, jestem jednak zależny – właśnie od niego.

gwarantującym, a na zapewniającym już nie (dlatego w przypisach zamieściłem definicje tych znaczeń)¹⁸.

Pozostaje również kwestia władz publicznych, które mają zapewniać równy dostęp do świadczeń opieki zdrowotnej, czy szerzej – ochrony zdrowia. Należy zadać pytanie, czy nie podjąć próby enumeratywnego wymienienia w jednym akcie prawnym organów i instytucji władz publicznych, które realizują poszczególne zadania z zakresu ochrony zdrowia. Należy zauważyć, że władza publiczna to organy i instytucje wchodzące w skład państwa polskiego i wykonujące zadania na rzecz jego i obywateli (ale nie tylko obywateli). Pozostaje jednak trudność, na co wskazuje Trybunał Konstytucyjny, który określił, iż chodzi o organy państwa i organy samorządu terytorialnego, jednocześnie jednak nie wymienił, co to za organy¹⁹.

Ponadto „w polskiej literaturze przedmiotu niestety od wielu lat rozróżnienie terminów „władza publiczna” i „władza państwowa” jest najczęściej pomijane lub stosowane bywa zazwyczaj na korzyść tej drugiej, o której się mówi więcej i z większym zaangażowaniem, a którą traktuje się jako władzę „rzeczywistą”, czy też władzę w znaczeniu organizatorskim bez związków z wolą powszechną (rozumianą za J.J. Rousseau jako odzwierciedlenie umowy społecznej, przy czym wola powszechna nie mogła być w tej koncepcji utożsamiana z wolą większości)”²⁰.

¹⁸ Wyrok TK z dnia 7 stycznia 2004 r. Trybunał Konstytucyjny, dostrzegając tę różnicę, stwierdził, iż dostęp do świadczeń ma być rzeczywisty a nie o charakterze programowym. Sformułowanie Konstytucji RP (*verba legis*: „władze publiczne [...] zapewniają...”) jest kategoryczne i ma charakter gwarancyjny. Pytanie: jak i kto ma to wyegzekwować? – pomimo iż art. 190 ust. 1 Konstytucji RP stanowi, iż orzeczenia Trybunału Konstytucyjnego mają moc powszechnie obowiązującą i są ostateczne; Szerzej. zob. M. Safjan, *Skutki prawne orzeczeń Trybunału Konstytucyjnego*. Tekst wystąpienia wygłoszonego przez Prezesa Trybunału Konstytucyjnego prof. M. Safjana w Komitecie Nauk Prawnych Polskiej Akademii Nauk 6 stycznia 2003 r.; Art. 1 pkt 3 Uchwały Senatu Rzeczypospolitej Polskiej z dnia 9 listopada 2007 r. (MP z 2007 r. nr 86, poz. 925), który stanowi, iż po dziale IX dodaje się IXa w brzmieniu: Wykonywanie orzeczeń Trybunału Konstytucyjnego. Obwieszczenie Marszałka Senatu Rzeczypospolitej Polskiej z dnia 13 maja 2010 r. w sprawie ogłoszenia jednolitego tekstu uchwały Senatu Rzeczypospolitej Polskiej – Regulamin Senatu (MP z 2010 r. nr 39, poz. 542).

¹⁹ Wyrok TK z dnia 7 stycznia 2004 r. Na temat różnego określenia terminu „władza publiczna”, „organy władzy publicznej” i konsekwencji ustrojowych z tym związanych szerzej zob. M. Konarski, M. Woch (red.), *Z zagadnień nadzoru i kontroli organów władzy publicznej w Polsce*, tom 1, Warszawa 2012, *passim*; Szerzej zob. M. Dercz, *Samorząd, likwidując szpital, nie zapewni opieki pacjentom*, „Gazeta Prawna” 31 maja 2011 r., http://praca.gazetaprawna.pl/wywiady/518907,samorząd_likwidując_szpital_nie_zapewni_opieki_pacjentom.html, dostęp: 3.04.2017 r., gdzie autor wskazuje, że „...jednym z głównych problemów związanych z funkcjonowaniem ochrony zdrowia w Polsce jest brak ustawowego określenia, które podmioty władzy publicznej ponoszą prawną odpowiedzialność za poszczególne rodzaje i poziomy świadczeń”.

²⁰ M. Konarski, M. Woch, *Z zagadnień nadzoru i kontroli organów władzy publicznej w Polsce*, [w:] *Z zagadnień nadzoru i kontroli organów władzy publicznej w Polsce*, tom 5, M. Konarski, M. Woch (red.), Warszawa 2015, s. 13.

Trybunał Konstytucyjny stwierdził, iż: „pojęcie «władzy publicznej» w rozumieniu art. 77 ust. 1 Konstytucji obejmuje wszystkie władze w sensie konstytucyjnym – ustawodawczą, wykonawczą i sędziowską. Należy ponownie podkreślić, że pojęcia organu państwa oraz organu władzy publicznej nie są tożsame. W pojęciu władzy publicznej mieszczą się bowiem także inne instytucje niż państwowe lub samorządowe, o ile wykonują funkcje władzy publicznej w wyniku powierzenia czy przekazania im tych funkcji przez organ władzy państwowej lub samorządowej. Wykonywanie władzy publicznej dotyczy wszelkich form działalności państwa, samorządu terytorialnego i innych instytucji publicznych, które obejmują bardzo zróżnicowane formy aktywności. Wykonywanie takich funkcji łączy się z reguły, chociaż nie zawsze, z możliwością władczego kształtowania sytuacji jednostki. Dotyczy to obszaru, na którym może dojść do naruszenia praw i wolności jednostki ze strony władzy publicznej.

Nazwa «organ» władzy publicznej, użyta w art. 77 ust. 1 Konstytucji, oznacza instytucję, strukturę organizacyjną, jednostkę władzy publicznej, z której działalnością wiąże się wyrządzenie szkody, nie zaś organ osoby prawnej w kategoriach prawa cywilnego. Odpowiedzialność oparta na tym przepisie obciąża strukturę (instytucję), a nie osoby z nią związane (jej funkcjonariuszy). Podstawowe znaczenie ma ustalenie, czy działanie organu władzy publicznej związane jest z realizacją jego prerogatyw. Formalny charakter powiązań pomiędzy bezpośrednim sprawcą szkody a władzą publiczną jest mniej istotny. Ustalenie statusu osoby, która jest bezpośrednim sprawcą szkody, ułatwia jednak przypisanie danego działania organowi władzy publicznej²¹.

Andrzej Zoll²² zajął stanowisko, iż „pewien podstawowy zarys odpowiedzialności władzy publicznej za wyrządzone szkody można zrekonstruować wprost z normy konstytucyjnej”. Jeśli przepis – art. 77 ust. 1 Konstytucji – mówi o wynagrodzeniu szkody wyrządzonej przez organ władzy publicznej, to, w ocenie Rzecznika Praw Obywatelskich, należy przez to rozumieć wszystkie władze w sensie konstytucyjnym: ustawodawczą, wykonawczą i sędziowską. Pod pojęciem organu władzy publicznej, zdaniem rzecznika, ustawodawca konstytucyjny rozumiał działalność instytucji władzy publicznej jako takiej, a odpowiedzialność jest zlokalizowana po stronie struktury tejże władzy, a nie osób związanych z tą strukturą. Przepis konstytucyjny odpersonalizowuje odpowiedzialność władzy publicznej.

Sławomira Wronkowska zauważa natomiast, że „...państwo prawne to państwo, które chroni jednostkę przed naruszeniami jej praw przez osoby będące funkcjonariuszami państwowymi i przed wyrządzanymi przez tych ostatnich

²¹ Zob. także: Wyrok TK z dnia 4 grudnia 2001 r. (sygn. akt (K 18/00), OTK – A 2001, nr 8, poz. 256).

²² Rzecznik Praw Obywatelskich od 30 czerwca 2000 r. do 30 czerwca 2005 r.

szkodami. Dlatego też w państwie prawnym istnieje odpowiedzialność odszkodowawcza państwa za działania jego funkcjonariuszy”²³.

Z kolei Janusz Trzcziński, czytając art. 68 Konstytucji RP, stawia pytanie: czy prawo do zdrowia jest prawem człowieka w takim sensie, że obywatel może się na to prawo powołać i żądać jego realizacji? Czy też może jest to przepis adresowany do władz publicznych – po prostu apel, deklaracja intencji, określenie celu, który władza publiczna ma spełnić?²⁴ Również należy odpowiedzieć na pytanie: czy artykuł 68 Konstytucji RP posiada normatywny charakter, czyli czy stwarza prawo podmiotowe obywatelowi, czy są to tylko normy programowe?²⁵

Przez prawo podmiotowe J. Trzcziński rozumie powszechnie taką normę, która po pierwsze, wskazuje ściśle określonego adresata (obywatel, inny podmiot), po drugie, daje adresatowi normy możliwość wyboru zachowania się (tzn. spełnienia lub niespełnienia tej normy), który może zależnie od tego, czy chce dochodzić swoich praw, czy nie, odpowiednio się zachować i, po trzecie, gdy przepis ten kształtuje sytuację prawną adresata normy. Jeżeli te trzy cechy występują: jest wyraźny adresat, jest ukształtowanie sytuacji prawnej tego podmiotu i podmiot ma prawo wyboru zachowania się, to możemy powiedzieć, że mamy do czynienia z prawem podmiotowym²⁶.

Natomiast za normy programowe uznaje się takie normy, które nakazują realizację lub dążenie do osiągnięcia pewnego celu. Chodzi tu o cele normodawcy, cele i zadania kierowane pod adresem władzy publicznej, a nie prawo po stronie obywatela. Norma programowa nie wykazuje zatem, jak należy się zachować po to, aby zrealizować pewien cel, lecz określa, jaki cel powinien być zrealizowany. Często mówi, jaki cel może być zrealizowany ze względu na możliwości, jakie ma

²³ S. Wronkowska, *Zarys koncepcji państwa prawnego...*, s. 76.

²⁴ J. Trzcziński, *Konstytucyjne prawo do zdrowia na tle art. 35 karty podstawowych praw Unii Europejskiej*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje 1997–2003. Profesorowi Kazimierzowi Działosze prace dedykowane na siedemdziesięciolecie*, L. Garlicki, A. Szymt (red.), Warszawa 2003, s. 302.

²⁵ Na temat norm szerzej zob. K. Opałek, *Zagadnienia teorii prawa i teorii polityki*, Warszawa 1986, s. 197 i nast.; C. Znamierowski, *Oceny i normy*, Warszawa 1957, s. 496 i nast.

²⁶ J. Wróblewski, *Zasady tworzenia prawa*, Warszawa 1989, s. 137, gdzie Autor wskazuje, że: „Adresat aktu prawnego powinien móc go zrozumieć. Znajomość ta jest zróżnicowana w stosunku do rozmaitych rodzajów informacji o przepisach prawnych i ze względu na różne grupy adresatów tych przepisów. Jest oczywiste, że znajomość prawa zakłada zrozumienie sformułowań tekstów prawnych, a więc aktów prawnych zawierających przepisy obowiązujące”; Także: H. Rot, *Elementy teorii prawa*, Wrocław 1980, s. 71, gdzie Autor wskazuje, aby przez „akt prawotwórczy» (normatywny, normodawczy) jako podstawowy składnik strukturalny systemu prawa stanowionego (ustawowego, „zamkniętego”) rozumieć akt wydany przez organ państwa (lub inny uprawniony podmiot) na podstawie upoważnienia zawartego w konstytucji lub innej ustawie, w formie przez ustawę przewidzianej i zawierający normy, które określonego rodzaju podmiotom wyznaczają określonego rodzaju zachowania się ilekroć wystąpią przewidziane w tych normach okoliczności”.

władza publiczna. Zdaniem J. Trzczińskiego art. 68 ze względu na swoją redakcję przypomina (w ust. 2–5) normę programową a nie prawo podmiotowe i jest klasyfikowany wśród norm programowych. Podkreśla również, że nie można jednak bez dyskusji godzić się na taką interpretację art. 68 Konstytucji i odmówić mu normatywnego charakteru w takim sensie, że nie może być podstawą dochodzenia przez jednostkę jej praw²⁷. Chociażby składając do Trybunału Konstytucyjnego skargę konstytucyjną²⁸.

Krystian Complak wskazuje natomiast, że: „jeśli polska doktryna i praktyka konstytucyjna nie zrezygnują z poglądu o programowym charakterze norm ustawy zasadniczej o celach państwa – zwłaszcza w kontekście praw społeczno-gospodarczych jednostki – ich realizację w naszym porządku prawnym wymuszają międzynarodowe instancje i organy. Co więcej, normy te zostaną zastosowane ze znacznie abstrakcyjniejszego poziomu niż przewiduje to Konstytucja Rzeczypospolitej”²⁹.

4. Wnioski

Należy zauważyć, że za bezpieczeństwo zdrowotne obywateli, ale i cudzoziemców odpowiada nie tylko jeden organ władzy wykonawczej, którym jest minister właściwy do spraw zdrowia. Prawa i obowiązki przenikają się na wielu poziomach różnych organów władzy i instytucji.

W tekście pt. *Finansowanie świadczeń opieki zdrowotnej przez jednostki samorządu terytorialnego w Polsce* zwróciłem uwagę, że jednostki samorządu tery-

²⁷ J. Trzcziński, *Konstytucyjne prawo do zdrowia...*, s. 303.

²⁸ Szerzej zob. M. Woch, *Indywidualna skarga konstytucyjna jako środek ochrony wolności lub praw*, Warszawa 2011, passim; J. Trzcziński, *Glosa do wyroku Trybunału Konstytucyjnego z dnia 2 lipca 2002 r. (sygn. akt U 7/01)*, „Przegląd Sejmowy” 2002, nr 5, s. 132, gdzie Autor stwierdził, że „... przepisy, które niesłusznie nazywa się normami programowymi, także po stronie obywatela stwarzają prawa podmiotowe co najmniej w takim zakresie, w jakim prawa te są odzwierciedleniem obowiązków władzy publicznej, a więc na poziomie minimum tych praw lub – jak kto woli – na poziomie ich istoty”.

²⁹ Szerzej zob. K. Complak, *Konstytucyjne postanowienia programowe czy normy o celach państwa*, [w:] *Sześć lat Konstytucji...*, s. 46–61; K. Działocha, *Wewnętrzna hierarchia norm konstytucji w orzecznictwie Trybunału Konstytucyjnego*, [w:] *Państwo–ustrój–konstytucja. Księga pamiątkowa poświęcona profesorowi Wiesławowi Skrzydle*, Z. Mańkowski (red.), Lublin 1991, s. 55–56; T. Glibert-Studnicki, A. Grabowski, *Normy programowe w konstytucji*, [w:] *Charakter i struktura norm konstytucji*, J. Trzcziński (red.), Warszawa 1997, s. 112; M. Zieliński, *Wykładnia prawa. Zasady. Reguły. Wskazówki*, Warszawa 2002, s. 39–40; P. Sarnecki, *Normy programowe w konstytucji i odpowiadające im wolności obywatelskie*, [w:] *Sześć lat Konstytucji...*, s. 252–262.

torialnego³⁰ w celu zaspokajania potrzeb wspólnoty samorządowej w zakresie ochrony zdrowia, uwzględniając w szczególności regionalną mapę potrzeb zdrowotnych, priorytety dla regionalnej polityki zdrowotnej oraz stan dostępności do świadczeń opieki zdrowotnej na obszarze województwa, mogą finansować dla mieszkańców tej wspólnoty świadczenia gwarantowane³¹. Jak również, że było to możliwe przed zmianą przepisów ustawą z dnia 10 czerwca 2016 r. o zmianie ustawy o działalności leczniczej oraz niektórych innych ustaw³².

Przykładowo należy również zwrócić uwagę, że Biuro Bezpieczeństwa Narodowego, przy pomocy którego Prezydent Rzeczypospolitej Polskiej³³ wykonuje zadania w zakresie bezpieczeństwa i obronności, wskazuje, że służba zdrowia kwalifikuje się do systemu bezpieczeństwa narodowego. Pomimo że Ministerstwo Zdrowia odpowiada m.in. za organizację systemu ochrony zdrowia, politykę zdrowotną i lekową, to jednak w obowiązujących ramach prawnych, wykonując konstytucyjny obowiązek zapewnienia dostępu do świadczeń medycznych, również w sytuacjach kryzysowych, należy mieć na uwadze, że wszystkie działania podmiotów uprawnionych do udzielania świadczeń medycznych i wsparcia organizacyjno-logistycznego wynikają wyłącznie z umocowanych w prawie właściwości organów, zaś skuteczna, w pełni nowoczesna i kompetentna pomoc medyczna powinna być wypadkową współpracy i współdziałania wszystkich jednostek oraz służb porządkowych, technicznych, medycznych i administracyjnych. Mówiąc o właściwości organów państwa odpowiedzialnych za zapewnienie na wymaganym poziomie opieki zdrowotnej należy mieć na uwadze, że właściwość ta leży nie tylko w gestii ministra zdrowia, ale również organów administracji rządowej w terenie i samorządowej³⁴.

Biuro jest także merytoryczno-organizacyjnym zapleczem Rady Bezpieczeństwa Narodowego powoływanej przez Prezydenta RP. Prezydent RP, na podstawie ustawowego upoważnienia, określa organizację oraz zakres działania Biura Bezpieczeństwa Narodowego³⁵. W strukturze biura funkcjonuje Departament Prawa

³⁰ Szerzej zob. M. Konarski, M. Woch, *Ewolucja prawa miejscowego jednostek samorządu terytorialnego w Polsce*, Warszawa 2014, *passim*.

³¹ M. Woch, *Podstawowa opieka zdrowotna jako filar funkcjonowania organów jednostek samorządu terytorialnego w Polsce*, [w:] *Funkcjonowanie samorządu terytorialnego – uwarunkowania prawne i społeczne*, A. Gołębiowska, P.B. Zientarski (red.), Warszawa 2016, s. 177–201; Szerzej: M. Woch, *Ochrona zdrowia w Polsce z punktu widzenia filozoficzno-prawnego*, Warszawa 2015, s. 89 i nast.

³² Dz. U. z 2016 r. poz. 960.

³³ Dalej: Prezydent RP.

³⁴ Por. BBN, *Biała Księga Bezpieczeństwa Narodowego RP*, Warszawa 2013, s. 88 i nast.

³⁵ Por. Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2012 r. poz. 461 z późn. zm.); Zarządzenie nr 2 Prezydenta Rzeczypospolitej Polskiej z dnia 11 sierpnia 2010 r. w sprawie organizacji oraz zakresu działania Biura Bezpieczeństwa Narodowego.

i Bezpieczeństwa Pozamilitarnego, który w zadaniach ma m.in. udział w pracach nad przygotowywaniem koncepcji strategicznej oraz zakresów zadań struktur państwa w pozamilitarnych dziedzinach bezpieczeństwa narodowego (w szczególności: bezpieczeństwo publiczne, zdrowotne, informacyjne, społeczne, ekonomiczne, gospodarcze oraz inne na polecenie szefa biura lub zastępców szefa biura).

Ponadto w strukturach państwa polskiego funkcjonuje Rządowe Centrum Bezpieczeństwa, będące państwową jednostką budżetową podległą Prezesowi Rady Ministrów. Do zadań centrum należy opracowywanie i aktualizowanie Krajowego Planu Zarządzania Kryzysowego, we współpracy z właściwymi komórkami organizacyjnymi urzędów obsługujących ministrów oraz kierowników urzędów centralnych, w tym również Ministra Zdrowia³⁶.

Natomiast poprzez infrastrukturę krytyczną, która obejmuje systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urzędnia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, rozumie się również systemy ochrony zdrowia³⁷.

Biorąc powyższe pod uwagę, należy stwierdzić, że zagadnienia dotyczące ochrony zdrowia w Polsce to nie tylko finansowanie świadczeń opieki zdrowotnej przez jednego płatnika publicznego, a przeważnie w debatach publicznych do tego sprowadzają się wnioski.

Bibliografia

Literatura:

- Biardzki M., *Publiczne czy prywatne – dylemat na nową kadencję*, „Służba Zdrowia”, dziennik ogólnopolski z dnia 17 października 2011 r.
- Bralczyk J. (red.), *Słownik 100 tysięcy potrzebnych słów*, Warszawa 2008.
- Chmielarz A., Sułkowski J., *Sprawozdanie z międzynarodowej konferencji naukowej „Demokratyczne państwo prawne w teorii i w praktyce w państwach Europy Środkowej i Wschodniej”*, Łódź, 4–6 września 2008 r., „Przegląd Sejmowy” 2009, nr 2.
- Complak K., *Konstytucyjne postanowienia programowe czy normy o celach państwa*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje 1997–2003. Profesorowi Kazimierzowi Działosze prace dedykowane na siedemdziesięciolecie*, L. Garlicki, A. Szmyt (red.), Warszawa 2003.

³⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. nr 89, poz. 590 z późn. zm., dalej: ustawa o zarządzaniu kryzysowym); Por. RCB, *Krajowy Plan Zarządzania Kryzysowego 2013/2015*, s. 576–595, rozdział pt. „Organizacja ratownictwa, opieki medycznej, pomocy społecznej oraz pomocy psychologicznej”.

³⁷ Przepis art. 3 ustawy o zarządzaniu kryzysowym.

- Czupryna A., Poździej S., Ryś A., Włodarczyk C., (red.), *Zdrowie publiczne*, tom I, Kraków 2000.
- Dąbrowski K., *Moralność w polityce. Wielopoziomowość funkcji uczuciowych i popędowych w życiu społecznym i politycznym oraz instytucjach*, Warszawa 1991.
- Dercz M., *Samorząd, likwidując szpital, nie zapewni opieki pacjentom*, „Gazeta Prawna” 31 maja 2011 r., http://praca.gazetaprawna.pl/wywiady/518907,samorząd_likwidujac_szpital_nie_zapewni_opieki_pacjentom.html, dostęp: 3.04.2017 r.
- Dercz M., Izdebski H., *Organizacja ochrony zdrowia w Rzeczypospolitej Polskiej w świetle obowiązującego ustawodawstwa*, Warszawa – Poznań 2001.
- Działocha K., *Wewnętrzna hierarchia norm konstytucji w orzecznictwie Trybunału Konstytucyjnego*, [w:] *Państwo–ustrój–konstytucja. Księga pamiątkowa poświęcona profesorowi Wiesławowi Skrzydle*, Z. Mańkowski (red.), Lublin 1991.
- Galster J., Szyszkowski W., Wasik Z., Witkowski Z., *Prawo konstytucyjne*, Toruń 1995.
- Gizbert-Studnicki T., Grabowski A., *Normy programowe w konstytucji*, [w:] *Charakter i struktura norm konstytucji*, J. Trzciniński (red.), Warszawa 1997.
- Gołębiowska A., Woch M., (red.), *Sprawozdanie z ogólnopolskiej konferencji naukowej. Przedsiębiorczość w służbie zdrowia: „Podmioty niepubliczne w publicznej służbie zdrowia”*, Warszawa 2016.
- Grzybowski K., *Historia doktryn politycznych i prawnych*, Warszawa 1968.
- Jastrzębski B., *Polska – czy jest państwem prawa*, Płock 2009.
- Konarski M., Woch M., *Ewolucja prawa miejscowego jednostek samorządu terytorialnego w Polsce*, Warszawa 2014.
- Konarski M., Woch M., *Z zagadnień nadzoru i kontroli organów władzy publicznej w Polsce*, [w:] *Z zagadnień nadzoru i kontroli organów władzy publicznej w Polsce*, tom 5, M. Konarski, M. Woch (red.), Warszawa 2015.
- Kornai J., Eggleston K., *Solidarność w procesie transformacji*, Warszawa 2002.
- Kozłowski T., *Spór o obecne pojęcie prawa*, [w:] *Teoretycznoprawne problemy integracji europejskiej*, L. Leszczyński (red.), Lublin 2004.
- Kryniecka-Piotrak A., *Koncepcja demokracji w poglądach filozoficznych Czesława Znamierowskiego*, praca doktorska napisana pod kierunkiem prof. dr hab. Marii Szyszkowskiej, Warszawa 2003, (niepublikowana).
- Lutosławski W., *Ludzkość Odrodzona. Wizje przyszłości*, Warszawa 1910.
- Mill, John S., *O rządzie reprezentatywnym. Poddaństwo kobiet*, Kraków – Warszawa 1995.
- Morawska E., *Klauzula państwa prawnego w Konstytucji RP na tle orzecznictwa Trybunału Konstytucyjnego*, Toruń 2003.
- Oakeshott M., *O postępowaniu człowieka*, Warszawa 2008.
- Opalek K., *Zagadnienia teorii prawa i teorii polityki*, Warszawa 1986.
- Pietrzak M., *Demokratyczne świeckie państwo prawne*, Warszawa 1999.
- Rossmann A., *Antropologiczna perspektywa rozważań o demokracji w ujęciu Wincentego Lutosławskiego*, [w:] *Wincenty Lutosławski (1863–1954). Materiały z posiedzenia Naukowego PAU w dniu 19 XI 2004 r.*, „Polska Akademia Umiejętności Archiwum Nauki PAN i PAU w Służbie Nauki” nr 16, Kraków 2010.
- Rost A., *Instytucje prawa konstytucyjnego*, Poznań 2003.
- Rot H., *Elementy teorii prawa*, Wrocław 1980.

- Safjan M., *Skutki prawne orzeczeń Trybunału Konstytucyjnego*. Tekst wystąpienia wygłoszonego przez Prezesa Trybunału Konstytucyjnego prof. M. Safjana w Komitecie Nauk Prawnych Polskiej Akademii Nauk 6 stycznia 2003 r.
- Sarnecki P., *Normy programowe w konstytucji i odpowiadające im wolności obywatelskie*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje 1997–2003*. Profesorowi Kazimierzowi Działosze prace dedykowane na siedemdziesięciolecie, L. Garlicki, A. Szmyt (red.), Warszawa 2003.
- Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2007.
- Staśkiewicz W., *Demokratyczne państwo prawne w Polsce lat dziewięćdziesiątych: eu-funkcjonalność teorii i dysfunkcjonalność praktyki*, [w:] *Prawo i ład społeczny*, Księga Jubileuszowa dedykowana Profesor Annie Turskiej, Warszawa 2000.
- Strzeszewski C., *Katolicka Nauka Społeczna*, Warszawa 1985.
- Suchocka H. (red.), *Tworzenie prawa w demokratycznym państwie prawnym*, Warszawa 1992.
- Szyszkowska M., *Każdy bywa pacjentem. Zarys filozofii farmacji*, Warszawa 2010.
- Teter Z., Kosowski A., Jabłońska B., Kifert K., *Lecznictwo uzdrowiskowe w Polsce w latach 2005–2015*, Warszawa 2016.
- Trzciański J., *Glosa do wyroku Trybunału Konstytucyjnego z dnia 2 lipca 2002 r. (sygn. akt U 7/01), „Przegląd Sejmowy” 2002, nr 5*.
- Trzciański J., *Konstytucyjne prawo do zdrowia na tle art. 35 karty podstawowych praw Unii Europejskiej*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje 1997–2003*. Profesorowi Kazimierzowi Działosze prace dedykowane na siedemdziesięciolecie, L. Garlicki, A. Szmyt (red.), Warszawa 2003.
- Włodarczyk W.C., *Reforma opieki zdrowotnej w Polsce*, Kraków 1998.
- Woch M., *Indywidualna skarga konstytucyjna jako środek ochrony wolności lub praw*, Warszawa 2011.
- Woch M., *Instytucje kształtujące system opieki zdrowotnej w Polsce. (Analiza prawno-porównawcza lat 1918–2004)*, Warszawa 2012.
- Woch M., *Ochrona zdrowia w Polsce z punktu widzenia filozoficzno-prawnego*, Warszawa 2015.
- Woch M., *Podstawowa opieka zdrowotna jako filar funkcjonowania organów jednostek samorządu terytorialnego w Polsce*, [w:] *Funkcjonowanie samorządu terytorialnego – uwarunkowania prawne i społeczne*, A. Gołębiowska, P.B. Zientarski (red.), Warszawa 2016.
- Wronkowska S., *Zarys koncepcji państwa prawnego w polskiej literaturze politycznej i prawnej*, [w:] *Polskie dyskusje o państwie prawa*, S. Wronkowska (red.), Warszawa 1995.
- Wronkowska S. (red.), *Zasada demokratycznego państwa prawnego w Konstytucji RP*, Warszawa 2006.
- Wróblewski J., *Zasady tworzenia prawa*, Warszawa 1989.
- Zajadło J., *Demokratyczne państwo prawne w teorii i w praktyce w państwach Europy Środkowej i Wschodniej*, K. Skotnicki (red.), „Przegląd Sejmowy” 2011, nr 3.
- Zieliński M., *Wykładnia prawa. Zasady. Reguły. Wskazówki*, Warszawa 2002.
- Znamierowski C., *Oceny i normy*, Warszawa 1957.
- Znamierowski C., *Szkółka prawa: Rozważania o państwie*, Warszawa 1999.

Streszczenie

Pojęcie bezpieczeństwa obywateli obejmuje również bezpieczeństwo zdrowotne, które powinno podlegać ochronie przez organy władzy publicznej. Jednak w strukturze państwa funkcjonuje wiele organów i instytucji władzy publicznej, które mają w swych zadaniach zagadnienia odnoszące się do ochrony zdrowia, co czasami nie ułatwia ich realizacji.

Słowa kluczowe: bezpieczeństwo obywateli, bezpieczeństwo zdrowotne, organy władzy publicznej.

Summary

Health security in the activities of public authorities in Poland

The concept of the security of citizens also includes health security, which should be protected by public authorities. But in the structure of the state are many organs and institutions of public authority, which are in their tasks, issues relating to health, which sometimes does not facilitate their implementation.

Key words: public security, health security, public authorities.

Rozdział VIII.

Rola monitoringu ekonomicznego w organizacji

1. Wstęp

Celem niniejszego artykułu jest zaprezentowanie fundamentalnego znaczenia informacji ekonomicznej, która ma kluczowy wpływ na funkcjonowanie wszystkich podmiotów działających w gospodarce. Dynamiczne tempo procesu globalizacji gospodarowania, wyrażające się nagłymi i radykalnymi zmianami występującymi we wszystkich obszarach życia podmiotów (rynkami, technologiami, innowacjami, konkurencją, środowiskiem), prowadzi do zmian w wielkości i strukturze popytu i podaży. Współczesna działalność organizacji określana jest coraz bardziej przez wartości intelektualne i niematerialne, a także przez środki informacyjne, technologiczne, informatyczne. O poziomie rozwoju społeczno-gospodarczego państwa, a tym samym stopie życiowej jego mieszkańców, w ostatecznej mierze decydują podmioty gospodarcze kreujące wartość¹.

Każda organizacja, chcąc się utrzymać na rynku oraz być konkurencyjna wobec innych podmiotów, powinna nieustannie obserwować swoje otoczenie i szybko reagować na zachodzące w nim zmiany. System informacji w organizacji powinien funkcjonować sprawnie przede wszystkim na etapie wczesnego ostrzegania o możliwych zagrożeniach. Powinien umożliwiać organizacji identyfikację (ocenę)

St. kpt. dr Aneta Kułakowska, Dr Ewa Frankowska – Zakład Podstaw Ekonomii i Nauk o Zarządzaniu, Wydział Inżynierii Bezpieczeństwa Cywilnego, Szkoła Główna Służby Pożarniczej w Warszawie.

¹ K. Janasz, W. Janasz, K. Koziół, K. Szopik-Depczyńska, *Zarządzanie strategiczne, Koncepcje, Metody, Strategie*, wydanie drugie, Wydawnictwo Difin, Warszawa 2010, s. 18.

przyszłych szans i zagrożeń. Długofalowe decyzje rozwojowe organizacji wymagają zapotrzebowania na informację i wiedzę o prawdopodobnych zachowaniach konkurentów, odbiorców i dostawców. Sukcesy współczesnych organizacji powiązane są ściśle z informacją i zasobami informacyjnymi, którymi dysponują przedsiębiorstwa².

Z punktu widzenia ekonomii informację możemy traktować jako dobro, ponieważ zaspokaja określone potrzeby podmiotu gospodarującego. Charakteryzuje się pewnymi szczególnymi właściwościami, które odróżniają ją od innych typów dóbr. Podstawową cechą charakterystyczną informacji jest to, że jej konsumpcja, czyli wdrożenie jej do swych zasobów wiedzy, lub wykorzystanie jej do podjęcia optymalnej decyzji nie powoduje jej zużycia. Wskutek tego nie ma potrzeby ponownego ubiegania się o pozyskanie informacji, którą już pozyskaliśmy. Kolejną znaczącą cechą specyficzną informacji jest możliwość jej powielania i przekazywania różnym komórkom i użytkownikom w organizacji. Optymalizacja procesów w organizacji nie jest możliwa bez szybkiej i wiarygodnej informacji. Dla zrozumienia funkcji, jaką pełni informacja, konieczne staje się uświadomienie tego, że obecnie funkcjonujemy w czasach ukształtowanych przez informacje.

2. Istota informacji i procesy informacyjne w organizacji

Informacja stanowi wskaźnik poziomu i jakości rozwoju cywilizacyjnego. Jej zdefiniowanie sprawia wiele trudności. Próbuąc określić pojęcie informacji, należy zaznaczyć, że jest to termin, który charakteryzuje się dużą złożonością. W literaturze przedmiotu autorzy próbują określić, czym jest informacja, dostosowując definicję do potrzeb danej dziedziny, lub posługują się tym pojęciem bez próby zdefiniowania, ponieważ nie widzą potrzeby definiowania tego terminu, informacja jest bowiem pojęciem pierwotnym, naturalnym, które istnieje i jest rozumiane przez ogół. Informacja jest także opisywana za pomocą cech, własności lub spełnianych przez nią funkcji. Jest ona przedmiotem zainteresowania środowiska naukowego, które dąży do poznania i zbadania natury informacji. W nauce termin informacji uważa się powszechnie za ogólny, interdyscyplinarny, powiązany ze wszystkimi dyscyplinami naukowymi.

Pojęcie informacji związane jest ze wszelkiego rodzaju wiadomością. Informację jako termin w literaturze fachowej określa się także jako:

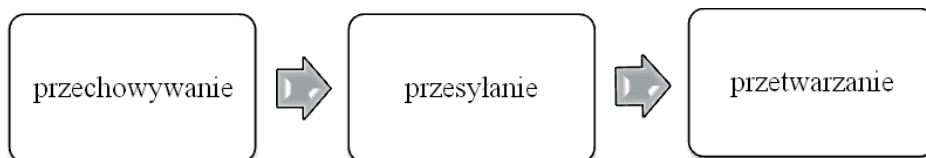
- wszystko, co można zużytkować do bardziej sprawnego wyboru działań prowadzących do realizacji celów i zadań organizacji;

² Tamże, s. 38.

- odzwierciedlenie rzeczywistości, które zmienia zachowania odbiorcy;
- dowolną wiadomość, na podstawie której odbiorca podejmuje określone działanie;
- każdy rodzaj wiadomości, której można przypisać określone znaczenie;
- wiadomość uzyskiwaną przez człowieka poprzez obserwację lub czynność umysłową podlegającą przekazowi nadawca–odbiorca;
- wiadomość o rzeczach, przedmiotach, zjawiskach lub procesach;
- czynniki, na podstawie których ludzie, żywe organizmy oraz urządzenia automatyczne mogą w sprawny sposób przeprowadzić celowe działanie;
- doniesienie o otaczającym nas świecie i odbywających się w nim procesach;
- specyficzne dobro niematerialne, które nabiera coraz większego znaczenia, przeobrażając świat i społeczeństwa;
- fundamentalna własność stanów i procesów fizycznych, biologicznych, psychologicznych oraz społecznych;
- dane uświadomione i zinterpretowane przez człowieka³.

Zgodnie z przytoczonymi powyżej definicjami informacji, należy wyróżnić trzy główne rodzaje działalności informacyjnej, które prezentuje poniższy rysunek.

Rysunek 1. Rodzaje działalności informacyjnej



Źródło: opracowanie własne na podstawie S. Forlicz, *Informacja w biznesie*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2008, s. 15

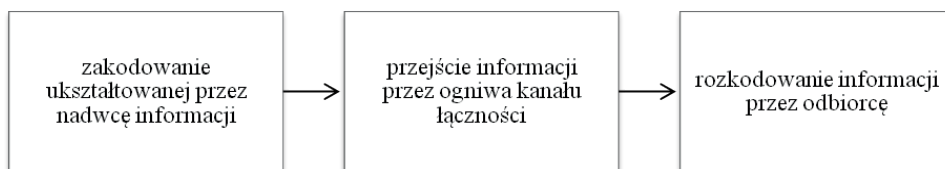
1. Przechowywanie informacji jest działaniem statycznym, w czasie którego informacja nie powinna ulegać zmianom, i odbywa się przy wykorzystaniu pewnego obiektu mającego charakter materialny. Urządzenie służące do przechowywania informacji umożliwia zapisywanie w nim informacji, przechowywanie jej i odtwarzanie. Przykładem magazynu informacji jest np. dysk twardy komputera itp.

³ W.K. Roman, *Podstawy zarządzania informacją*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2012, s. 16–17.

2. Przetwarzanie informacji dotyczy przekształcania zbioru informacji w inny zbiór informacji, najczęściej według określonego z góry algorytmu. Przetworzenie informacji daje możliwość wyciągania pewnych wniosków lub sklasyfikowania i uporządkowania informacji.
3. Przesyłanie informacji to wszelkiego rodzaju przemieszczanie informacji od nadawcy do odbiorcy przez złożony z ogniw kanał łączności. Ogniwa kanału łączności są to wszelkie obiekty fizyczne umożliwiające przesyłanie informacji od nadawcy do odbiorcy. Sygnały (informacje) dochodzące do danego ogniwa nazywają się sygnałami (informacjami) wejściowymi, a sygnały (informacje) wychodzące z danego ogniwa – odpowiednio – sygnałami (informacjami) wyjściowymi.

Proces przepływu informacji składa się z następujących elementów, które przedstawia poniższy rysunek.

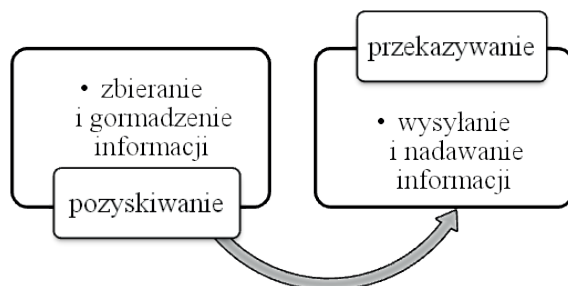
Rysunek 2. Proces przepływu informacji



Źródło: opracowanie własne na podstawie S. Forlicz, *Informacja w biznesie...*, s. 15

Przepływ informacji może zostać zainicjowany przede wszystkim przez ewentualnego odbiorcę informacji, który uznaje (czasem intuicyjnie) możliwość poprawy jakości lub podejmowanej decyzji dzięki poszerzeniu swojej wiedzy przez zdobycie nowych informacji. Należy jednak zaznaczyć, że pozyskiwanie nowych informacji (np. drogą obserwacji rzeczywistości, zbierania informacji od innych podmiotów) jest tylko jedną stroną możliwej aktywności informacyjnej podmiotu. Inną stroną aktywności informacyjnej podmiotów jest także przekazywanie informacji (np. transmisja danych lub sygnalizowanie). Przepływ informacji może zostać zainicjowany przez nadawcę informacji, który odczuwa chęć poprawy własnej sytuacji dzięki zmianie decyzji podjętej przez ten drugi podmiot na skutek otrzymanych informacji. W takiej działalności informacyjnej, jaką jest przesyłanie informacji, należy wyróżnić dwie formy aktywności podmiotów, które przedstawia rysunek 3.

Rysunek 3. Formy aktywności w przesyłaniu informacji



Źródło: opracowanie własne na podstawie S. Forlicz, *Informacja w biznesie...*, s. 16

Przykładami pozyskiwania informacji przez podmioty gospodarcze mogą być np.:

- badania rynku;
- badania konsumentów i konkurencji;
- zbieranie informacji przez konsumentów na temat oferentów, cen, jakości świadczonych usług lub towarów;
- zbieranie informacji przez pracodawcę na temat potencjalnych pracowników;
- badania nad rozwojem technologii i innowacjami;
- badania marketingowe itp.

Z punktu widzenia ekonomii informację możemy traktować jako dobro, ponieważ zaspakaja określone potrzeby człowieka. Jednak dysponuje ona pewnymi szczególnymi właściwościami, które odróżniają ją od innych dóbr. Pierwszą cechą charakterystyczną informacji jest to, że konsumpcja informacji, czyli wprowadzenie jej do zasobu wiedzy jednostki lub wykorzystania jej w celu podjęcia optymalnej decyzji, nie powoduje jej zużycia. Kolejną ważną cechą informacji jest możliwość jej powielania, teoretycznie nieskończoną liczbę razy, najczęściej przy znikom niskich kosztach i bez utraty jej użyteczności dla powielającego, np. użyteczność dla osoby prowadzącej szkolenia informacja zawarta w materiałach szkoleniowych pozostaje niezmienną, niezależnie od tego, ile razy zostanie przekazana⁴.

Zapotrzebowanie informacyjne związane jest przede wszystkim w podejmowaniem optymalnych decyzji gospodarczych w organizacji. Współczesność otoczenia dalszego i bliższego przedsiębiorstwa wymaga od organów kierowniczych szybkich, efektywnych wyników działalności gospodarczej. Wykonywanie zadań związanych ze sprawnym podejmowaniem decyzji możliwe jest w sytuacji

⁴ Tamże, s. 16.

zapewnienia wsparcia procesu decyzyjnego przez odpowiedni poziom i jakość informacji, przede wszystkim ekonomicznych⁵.

3. Monitoring ekonomiczny jako mechanizm dostarczania informacji ekonomicznej w organizacji

W praktyce gospodarczej występuje kilka technik dokonywania bezpośrednich pomiarów działalności gospodarczej. Przyjmując za kryterium użyteczność w bezpośrednim dostarczaniu informacji ekonomicznych, należy stwierdzić, że metodą najbardziej pomocną jest obserwacja, która dostarcza badaczowi rzetelnej i prawdziwej wiedzy o obserwowanych obiektach. Tok postępowania obserwacyjnego polega na ukierunkowanym, zmierzonym i systematycznym postrzeganiu badanych obiektów w ich naturalnych warunkach. Działania obserwacyjne w znacznym stopniu przyczyniają się do poznania i zrozumienia przepływu działań i procesów gospodarczych⁶. Zaobserwowane prawidłowości statyczne z określonym prawdopodobieństwem wpływają na rozpoznanie zjawisk i obiektów przez obserwatora, są źródłem pogłębiania jego wiedzy o obserwowanych obiektach. Stała obserwacja i kontrola procesów lub zjawisk w Słowniku języka polskiego jest zdefiniowana jako monitoring⁷, a zatem monitoring to ciągłe obserwowanie przebiegu funkcjonowania badanego obiektu.

Monitoring to mechanizm informacyjny, który systematycznie dozoruje ilościowe i jakościowe zmiany pewnych ustalonych wcześniej obiektów obserwacji, wykorzystując określone techniki rejestracji. W literaturze przedmiotu występuje zróżnicowane rozumienie monitoringu, traktowanego jako:

- obserwacja i odpowiednio zorganizowana rejestracja wszystkich zdarzeń, parametrów oraz sytuacji związanych z funkcjonowaniem obiektu, mogących mieć wpływ na działania całości obiektu lub kluczowej jego części⁸;
- działalność badawcza, która pozwala ocenić skuteczność i efektywność decyzji i możliwość jej korekty;
- tok postępowania dotyczący powiadamiania decydentów o możliwych zagrożeniach i możliwościach interwencji⁹.

⁵ A. Mytlewski, *Monitoring ekonomiczny przedsiębiorstw*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2007, s. 7.

⁶ H. Gabrusiewicz, M. Hamrol, E. Kurtys, H. Sobolewski, *Analiza wartości jako narzędzie optymalizacji kosztów własnych przedsiębiorstwa*, Akademia Ekonomiczna, Poznań 1998, s. 66.

⁷ Słownik języka polskiego, Polskie Wydawnictwo Naukowe.

⁸ R. Cegieła, A. Zalewski, *Racjonalne zarządzanie przedsięwzięciami informatycznymi i systemami komputerowymi*, Nakom, Poznań 2000, s. 314.

⁹ Tamże, s. 12.

Jednym z fundamentalnych obszarów zastosowania monitoringu jest działalność gospodarcza. Wdrożenie koncepcji monitoringu do działalności gospodarczej określa się mianem monitoringu ekonomicznego. W literaturze przedmiotu spotyka się określone rozumienie monitoringu ekonomicznego:

1. jest rozpatrywany jako systematyczne, metodyczne obserwowanie oraz rejestrowanie zmian zachodzących w organizacji i jej otoczeniu bliższym i dalszym, dla celów diagnozy, sterowania i przewidywania postępu sytuacji gospodarczej¹⁰;
2. to mechanizm dostarczania względnie stałych co do struktury treści i form organizacyjnych określonych stanów systemu gospodarczego, w wybranych momentach lub przedziałach czasowych, bez dokonania ich głębszej analizy i oceny¹¹;
3. to metoda wspomagania zarządzania organizacją, która ma na celu nadzorowanie kluczowych i najbardziej strategicznych składników, które mają wpływ na funkcjonowanie organizacji i przygotowanie ewentualnych decyzji niwelujących zagrożenie;
4. to zespół elementów, który wykorzystuje narzędzia do rejestracji zdarzeń i procesów gospodarczych oraz ustalania bieżących stanów obserwowanego zjawiska.

Po rozważeniu powyższych definicji monitoringu ekonomicznego można stwierdzić, że ten mechanizm jest tokiem działań i postępowania o charakterze organizatorskim, których zasadniczym zadaniem jest zrealizowanie celu w odniesieniu do wyraźnie określonych obiektów i zjawisk oraz ich atrybutów. Organizacja czynności w zakresie monitoringu ekonomicznego dotyczy przede wszystkim określonego toku postępowania, który opisany jest przez rysunek 5.

Rysunek 4. Tok postępowania w działania organizacyjnych w zakresie monitoringu ekonomicznego



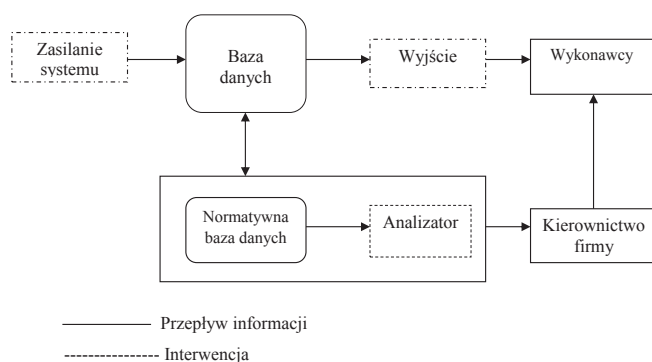
Źródło: A. Mytlewski, *Monitoring ekonomiczny...*, s. 12.

¹⁰ Z. Leszczyński, *Monitoring finansowy w zarządzaniu małym i średnim przedsiębiorstwem*, [w:] *Zarządzanie małym i średnim przedsiębiorstwem, Uwarunkowania europejskie*, (red.) M. Strużycki, Difin, Warszawa 2002, s. 274.

¹¹ W. Flakiewicz, *Systemy informacyjne w zarządzaniu*, Wydawnictwo Beck, Warszawa 2002, s. 43.

Monitoring ekonomiczny należy rozpatrywać jako metodę badań gospodarczych, która polega na długookresowej, ciągłej lub odpowiednio częstotliwej obserwacji odpowiednio wyselekcjonowanych obiektów i procesów, opisywaniu tych obiektów i procesów za pomocą przyjętych wzorców oraz na czynnościach porządkujących dopływ informacji o tych obiektach i procesach do użytkowników lub odbiorców informacji. Organizowanie funkcji i zadań monitoringowych prowadzi do ukształtowania stabilnych i trwałych mechanizmów zaopatrzenia informacyjnego dla potrzeb kadry zarządczej i decydentów. Poniższy rysunek prezentuje miejsce kierownictwa w organizacji w systemie monitorowania.

Rysunek 5. System monitorowania w organizacji



Źródło: J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 1999, s. 178

Przedstawiony na rysunku model systemu monitoringu ekonomicznego w organizacji, opisany przez J. Kisielnickiego, zasila podmiot gospodarujący w informacje wynikowe, dokonując jednocześnie porównań z wartościami normatywnymi (wzorcowymi) określonymi dla danej kategorii obiektów. Analizator w modelu ma za zadanie ustawiczne porównywanie wyników z właściwymi wielkościami wzorcowymi. Model monitoringu ekonomicznego może być wykorzystywany w różnorodnych koncepcjach zarządzania w organizacji, tj. np. logistycznych, marketingowych, procesowych oraz kontrolingowych. W zakresie wczesnego ostrzegania monitoring ekonomiczny ma wyznaczone zadania, do których należy zaliczyć¹²:

¹² W. Radzikowski, J. Wierzbński, *Controlling, Koncepcje – metody – zastosowania*, Toruńska Szkoła Zarządzania, Toruń 1999, s. 88–89.

- ustalenie działań pozwalających na wcześniejsze zaobserwowanie i przeanalizowanie symptomów niebezpieczeństwa przed jego wystąpieniem;
- przekazywanie charakterystycznych informacji wczesnego ostrzegania w przypadku zmian sytuacji, procesów, gdy odbiegają one od założonych norm w organizacji;
- przekazywanie informacji z określonym wyprzedzeniem, aby użytkownicy lub decydenci w organizacji dysponowali czasem na wprowadzenie działań likwidujących lub zmniejszających zagrożenia;
- musi być mechanizmem, który w sposób zindywidualizowany i uwzględniający specyfikę danej organizacji będzie dostarczał informacji o otoczeniu sektorowym lub makroekonomicznym.

Podmiotem monitorującym jest organizacja lub właściciel podmiotu gospodarującego. W węższym znaczeniu podmiotami monitorującymi mogą być komórki organizacyjne organizacji lub pojedyncze stanowiska do tego ustanowione. Przedmiotem pracy podmiotu monitorującego jest informacja ekonomiczna. Z kolei pomiotami monitorowanymi są obiekty oraz zdarzenia, które zachodzą we wnętrzu podmiotu lub w jego otoczeniu. Należy pamiętać, że efektami zachowywania się obiektu są zdarzenia gospodarcze. Zdarzenia te w obszarze monitoringu ekonomicznego powinny spełniać warunek mierzalności, to znaczy, że obserwator powinien nadać obiektowi miarę zdarzenia lub stanu.

Różnorodność doboru metod, technik i struktur monitoringu ekonomicznego wpływa bezpośrednio na jego różnorodność typologiczną. Klasyfikując monitoring ekonomiczny w organizacji, należy wykazać wiele czynników kształtujących jego podział, do których przede wszystkim zaliczamy:

1. Kryterium częstotliwości przeprowadzania obserwacji:
 - monitoring ciągły – nadzorujący i dokonujący obserwacji w czasie rzeczywistym;
 - monitoring periodyczny – dokonujący obserwacji z określoną częstotliwością (o stałej i zmiennej periodyczności).
2. Kryterium zakresu monitoringu:
 - monitoring wewnętrzny – skierowany na obserwację zdarzeń gospodarczych zachodzących we wnętrzu przedsiębiorstwa;
 - monitoring zewnętrzny – skierowany na otoczenie organizacji lub realizowany z otoczenia w stosunku do przedsiębiorstwa;
 - monitoring mieszany – realizujący obserwację otoczenia, jak i wnętrza organizacji.

3. Kryterium pola obserwacji:

- monitoring marketingowy – polegający na obserwacji makrootoczenia i otoczenia sektorowego;
- monitoring finansowy – polegający na obserwacji kategorii finansowych kwantyfikujących wszystkie sfery działalności organizacji;
- monitoring zasobów ludzkich – nadzorujący gospodarowanie i przepływy zasobów ludzkich;
- monitoring produkcyjno-technologiczny – realizujący funkcje ciągłej kontroli (często automatycznej) nad procesami technologicznymi;
- monitoring ekologiczny – prowadzący nadzór nad emisją czynników szkodliwych przez przedsiębiorstwo.

4. Kryterium podmiotowe:

- monitoring obligatoryjny – zinstytucjonalizowany, nakazany prawem przez zewnętrznych audytorów przedsiębiorstwa;
- monitoring własny – fakultatywny, najczęściej menedżerski, wynikający z potrzeb zarządczych.

Znaczącą cechą wskazanej powyżej klasyfikacji monitoringu ekonomicznego jest fakt, że poszczególne jego rodzaje służą dostarczaniu informacji dla potrzeb określonych grup użytkowników lub decydentów organizacji¹³.

Struktury i zadania monitoringu ekonomicznego w organizacji wymagają zbudowania trwałych mechanizmów zapewniających odpowiednio częstotliwe uzyskiwanie informacji ekonomicznych o określonych atrybutach jakościowych. Odpowiednio zbudowany monitoring ekonomiczny wymaga jednoznacznego wyznaczenia:

- podmiotu monitorującego, uprawnionego do przeprowadzenia obserwacji i dalszego wykorzystania wyników;
- podmiotu monitorowanego, który podlega obserwacji;
- przedmiotu monitorowania, tj. zadań podlegających obserwacji i ich mierników;
- terminów i częstotliwości dokonywania obserwacji;
- źródła pozyskiwania informacji o przebiegu realizacji zadania;
- sposobów gromadzenia i przetwarzania informacji;
- sposobów prezentowania, w tym wizualizacji, informacji o przebiegu realizacji zadań.

Powyższe mechanizmy służą realizacji określonych celów monitoringu ekonomicznego.

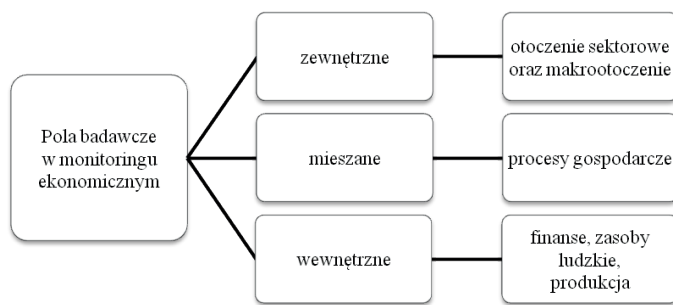
¹³ R. Borowiecki, M. Romanowska, *System informacji strategicznej, Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Wydawnictwo Difin, Warszawa 2001, s. 127–129.

Monitoring ekonomiczny może dotyczyć różnorodnych obszarów działalności organizacji. Znaczącą kwestią w tym obszarze jest opis pól badawczych i ich różniczenie, dlatego należy wskazać następujące zakresy badawcze w monitoringu ekonomicznym:

- pola znajdujące się we wnętrzu organizacji;
- pola znajdujące się w otoczeniu organizacji;
- pola mieszane, gdzie obiekt obserwacji wychodzi poza granice organizacji.

Zawartość pól badawczych w monitoringu ekonomicznym prezentuje poniższy rysunek¹⁴.

Rysunek 6. Zakres pól badawczych w monitoringu ekonomicznym



Źródło: A. Mytlewski, *Monitoring ekonomiczny...*, s. 29

Rozpoznanie pól badawczych w monitoringu ekonomicznym daje możliwości pozyskania wszechstronnych informacji, które pozwalają na kompleksowe planowanie oraz ocenę różnych zjawisk i procesów.

4. Zarządzanie zasobami informacyjnymi w organizacji

Procesy globalizacji sprawiają, że do zarządzania każdą organizacją niezbędne staje się dysponowanie i pozyskiwanie coraz większej ilości informacji. Przyczyną zwiększonego popytu informacyjnego w organizacji jest wiele. Do zasadniczych czynników należy zaliczyć przede wszystkim rozwój technologii informacyjnych, który powoduje powstanie nowych struktur informacyjnych o zasięgu globalnym oraz narzędzi do zarządzania nimi, czyli instrumentów do pozyskiwania, selekcjonowania, analizowania, przetwarzania, zarządzania i przekazywania informacji. Do innych bodźców zaliczyć powinno się także coraz bardziej złożo-

¹⁴ Tamże, s. 29.

ne warunki funkcjonowania organizacji wszystkich typów, a przede wszystkim gospodarczych. Wzrastające potrzeby podyktowane są tworzeniem nowych zasobów wiedzy w organizacjach, czyli traktowaniem informacji jako kapitału podmiotu gospodarującego i jako zasobu kreującego wartość organizacji oraz postrzeganiem zasobu informacyjnego jako czynnika, który powoduje przewagę nad konkurencją organizacji¹⁵.

Biorąc powyższe pod uwagę, jednym z kluczowych wyzwań stojących przed współczesną organizacją jest konieczność nieustannego dopasowywania się do szybkich zmian zachodzących w otoczeniu organizacji. Fundamentalnym celem teraźniejszych organizacji jest maksymalizacja zysków. Funkcjonujące organizacje nastawione na osiąganie zysków wykorzystują kombinację zasobów, które posiadają w swojej dyspozycji. Do tradycyjnych nakładów, jakie są wykorzystywane w procesach gospodarczych, należy zaliczyć ziemię, pracę i kapitał.

Obecnie czwartym kluczowym czynnikiem, który odgrywa dużą rolę w procesach gospodarczych, jest informacja i zasoby informacyjne będące w dyspozycji organizacji. W organizacji należy szczegółowo wymienić zasoby materialne pod postacią środków finansowych, technicznych i kapitału ludzkiego oraz zasoby niematerialne, do których należy jak najbardziej zaliczyć informację, wiedzę, kwalifikacje, doświadczenie, zdolności i kulturę organizacyjną. Wszystkie powyższe czynniki są przedmiotem planowania, kontroli i koordynacji w zakresie zarządzania jednostką gospodarującą¹⁶. Informacja i zasoby informacyjne są jednym z najbardziej znaczących nakładów, jakie współcześnie biorą udział w procesach gospodarczych. Odgrywają znaczącą rolę w procesach produkcyjnych, zarządczych i komunikowania oraz wymiany dóbr i usług. Wobec powyższego bez odpowiedniego zasobu informacyjnego niemożliwe jest efektywne i optymalne funkcjonowanie jakiegokolwiek organizacji¹⁷.

Wyjaśniając pojęcie „zasób informacyjny”, należy stwierdzić, że jest to pewna ilość danego dobra, które zostało zgromadzone po to, aby mogło być wykorzystane w przyszłości przez podmiot gospodarujący. Zasób informacyjny to przede wszystkim uporządkowany zestaw danych, wiadomości i wiedzy w postaci zbiorów zebranych w celu ich przetwarzania i otrzymania nowej jakościowo informacji o wyznaczonym zakresie funkcjonalnym w strukturze podmiotu gospodarującego¹⁸.

¹⁵ R. Zygała, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wydanie UE, wydanie I, Wrocław 2007, s. 43.

¹⁶ Tamże, s. 30.

¹⁷ Tamże, s. 60.

¹⁸ M. Adamczyk, A. Jurga, J. Kałkowska i inni, *Projektowanie systemów informacyjnych zarządzania*, Poznań 2010, s. 34.

Definiując zakres zarządzania informacją, należy przez to rozumieć organizowanie i kontrolowanie obiegu informacji w organizacji w celu zapewnienia optymalnych warunków dla osiągnięcia założonych celów, czyli realizacji misji organizacji¹⁹.

Gromadzenie zasobów informacji jest związane z rozwojem społeczno-gospodarczym, któremu towarzyszy szybki rozwój narzędzi i technologii informacyjnych. Fundamentalną rolą zasobu informacyjnego jest zaspokajanie wszystkich potrzeb informacyjnych organizacji i jej poszczególnych komórek i uczestników. Przyjmując powyższe przesłanki odnoszące się do zasobów, które są w dyspozycji organizacji, należy stwierdzić, że warunkują one realizację celów przedsiębiorstwa oraz warunkują skuteczne zarządzanie podmiotem. Zarządzanie zasobami informacyjnymi jest współcześnie niezbędnym działaniem w ramach kompleksowego zarządzania każdą jednostką gospodarującą. Potrzeba zarządzania informacją zrodziła się w warunkach społeczeństwa informacyjnego, dysponującego, wytwarzającego i potrzebującego ogromnej ilości informacji. Zarządzanie informacją jest skutkiem konieczności przechowywania zasobów informacji, ich przetwarzania oraz udostępniania.

Kluczowym celem zarządzania zasobami informacyjnymi jest identyfikacja sytuacji wewnętrznej i zewnętrznej organizacji oraz dostarczenie informacji zgodnych z potrzebami i niezbędnych do podejmowania decyzji i rozwiązywania zaistniałych sytuacji problematycznych. Zarządzanie zasobami informacyjnymi jest procesem złożonym, ponieważ dynamiczne zmiany techniczne i technologiczne oraz stale powiększające się zasoby informacyjne wymagają skoordynowania współistnienia i współdziałania wielu czynników. Każda organizacja dysponuje własnymi zasobami informacyjnymi, ale również pozyskuje informacje z otoczenia bliższego i dalszego. Biorąc powyższe pod uwagę, każda organizacja powinna przeszkolić swój personel, zatrudniać specjalistów oraz mieć w swoich zasobach urządzenia przetwarzające dane, a nierzadko nawiązywać współpracę z profesjonalnymi instytucjami zewnętrznymi. Równie istotnym argumentem przesądzającym o konieczności zarządzania informacją jest postrzeganie informacji jako poszukiwanego i cenionego towaru będącego przedmiotem wymiany i handlu. Wzrost roli informacji w życiu podmiotów gospodarujących jest czynnikiem determinującym rozwój i pojawianie się innowacji²⁰.

¹⁹ Tamże, s. 87.

²⁰ Tamże, s. 78.

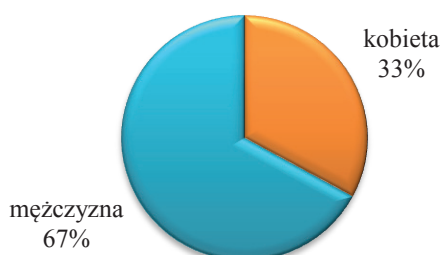
5. Obserwacja ekonomiczna jako narzędzie wspomagające podejmowanie optymalnych decyzji i zarządzanie zasobami podmiotów w skali mikroekonomicznej – badania empiryczne

Podstawowym celem i założeniem badań przeprowadzonych w listopadzie i grudniu 2016 roku było uzyskanie opinii na temat zastosowania obserwacji ekonomicznej jako narzędzia wspomagającego podejmowanie racjonalnych i efektywnych decyzji gospodarczych oraz wpływ na zarządzanie zasobami podmiotów mikroekonomicznych. W celu pozyskania danych wykorzystano metodę badawczą za pośrednictwem ankiety. Metoda ta należy do najbardziej popularnych metod badawczych i polega na uzyskaniu informacji i danych od określonej zbiorowości oraz weryfikacji założeń badania. Kwestionariusz jako instrument badawczy stanowił podstawę do opracowania szczegółowej analizy opinii badanych podmiotów. Badania ankietowe umożliwiły pozyskanie od określonych respondentów informacji dotyczących tego, jak dana osoba ankietowana ocenia i postrzega badane zjawisko. Badania opierały się na metodach jakościowych w celu poznania wewnętrznych zachowań odnośnie do wykorzystania obserwacji ekonomicznej w swojej działalności. Kwestionariusz dostarczony do respondentów miał formę anonimową. Badania przeprowadzone były wśród gospodarstw domowych i podmiotów gospodarczych, obejmując 182 respondentów. Badania ankietowe zweryfikowały opinie i wskazały tendencje dotyczące zastosowania obserwacji ekonomicznej.

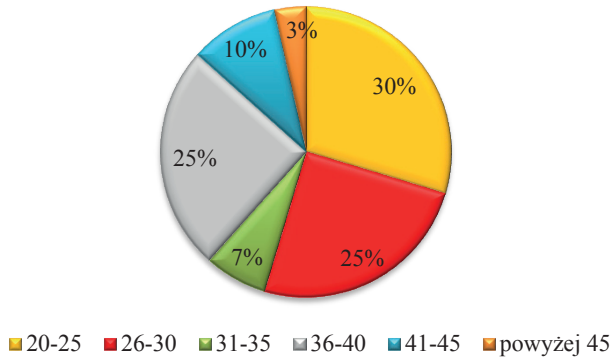
Pytania dotyczyły:

- typologii badanych podmiotów: miejsca zamieszkania, wieku oraz płci;
- zagadnień związanych z obserwacją zjawisk ekonomicznych w otoczeniu mikroekonomicznym i makroekonomicznym oraz kategorii i zjawisk ekonomicznych podlegających obserwacji;
- źródeł pozyskiwania informacji ekonomicznej;
- wpływu obserwacji ekonomicznej na decyzje gospodarcze.

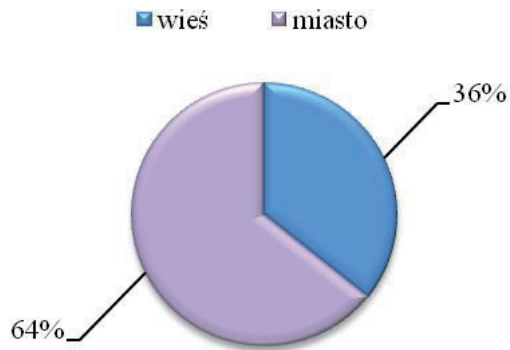
Wykres 1. Płeć respondentów



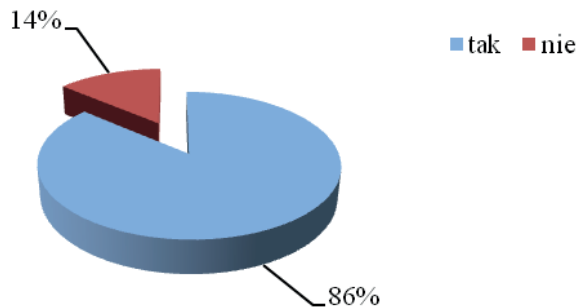
Wykres 2. Wiek respondentów



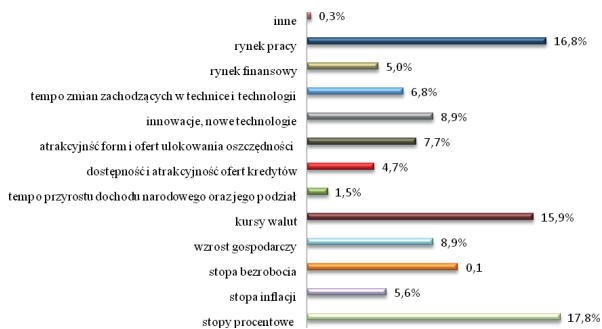
Wykres 3. Miejsce zamieszkania



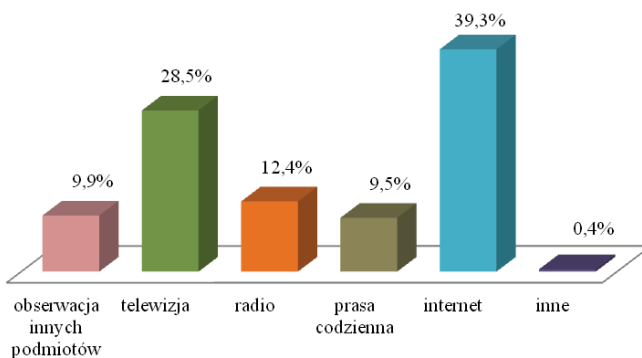
Wykres 4. Obserwacja zjawisk ekonomicznych w otoczeniu mikroekonomicznym i makroekonomicznym



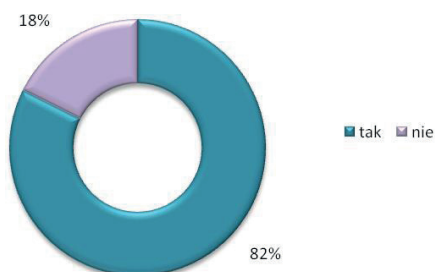
Wykres 5. Kategorie i zjawiska ekonomiczne podlegające obserwacji



Wykres 6. Źródła pozyskiwania informacji ekonomicznej



Wykres 7. Wpływ obserwacji ekonomicznej na decyzje gospodarcze



Wykresy 1–7. Źródło: opracowanie własne na podstawie badań ankietowych: „Obserwacja ekonomiczna – narzędzie wspomagające podejmowanie optymalnych decyzji i zarządzanie zasobami podmiotów w skali mikroekonomicznej”

6. Wnioski

Przeprowadzone badania pozwoliły uzyskać odpowiedzi na zadane pytania w kwestionariuszu ankietowym oraz poznać opinie badanych respondentów w zakresie stosowania obserwacji ekonomicznej do rzeczywistości gospodarczej w otoczeniu makroekonomicznym i mikroekonomicznym. Zebrane dane posłużyły do sformułowania wniosków na temat wpływu obserwacji ekonomicznej na podejmowanie decyzji gospodarczych i zarządzanie zasobami. Uzyskane informacje i wiedza o zachowaniach oraz potrzebach informacyjnych respondentów pozwoliły ocenić zastosowanie monitoringu ekonomicznego w działalności podmiotów gospodarujących. Badania ankietowe zweryfikowały opinie i wskazały tendencje dotyczące źródeł pozyskiwania informacji ekonomicznych. Uzyskano także informacje dotyczące rodzajów obserwowanych kategorii i zjawisk ekonomicznych w otoczeniu respondentów. Przeprowadzone badania ukazały znaczący wpływ obserwacji rzeczywistości gospodarczej na decyzje ekonomiczne.

7. Zakończenie

Szybki rozwój gospodarczy, techniczny i kulturalny we współczesnym świecie wywołuje wzrost zapotrzebowania na wszechstronną informację. Jest ona propagatorem wiadomości, czyli stanowi jeden z najbardziej kluczowych elementów rozwoju organizacji. Zapotrzebowanie informacyjne związane jest przede wszystkim z podejmowaniem optymalnych i racjonalnych decyzji i zarządzaniem zasobami organizacji. Efektywność i sprawne funkcjonowanie systemów informacyjnych wpływa bezpośrednio na jakość informacji, a to z kolei wpływa na decyzje oraz na zarządzanie organizacją. Szczególnym wyzwaniem stojącym przed współczesnymi organizacjami i decydentami jest jakość i rzetelność informacji oraz szybkość jej pozyskania.

Podstawowym mechanizmem informacyjnym wykorzystywanym w organizacji jest monitoring ekonomiczny, który dostarcza informacji niezbędnych do sprawnego jej funkcjonowania. Koncepcja monitoringu ekonomicznego jest odpowiedzią na rosnące problemy związane z informacją ekonomiczną ważną z punktu widzenia zarządzania organizacją. Monitoring ekonomiczny systematycznie nadzoruje ilościowe i jakościowe zmiany pewnych ustalonych wcześniej obiektów lub zjawisk obserwacji, wykorzystując określone techniki rejestracji. Mechanizm ten charakteryzuje się odpowiednio zorganizowaną rejestracją wszystkich zdarzeń gospodarczych oraz sytuacji związanych z funkcjonowaniem organizacji, które mogą mieć wpływ na jej działanie lub na istotną jej część. To także zespół działań, który ma wpływ na ocenę trafności decyzji i ewentualne jej skorygowanie.

Sprawnie zbudowany i funkcjonujący monitoring ekonomicznych powinien prowadzić do porządkowania przepływów i zasobów informacyjnych. Uporządkowanie zasobów informacyjnych jest czynnikiem służącym użyteczności informacji i dostosowania jej do wymogów decydentów, odbiorców i użytkowników. Usługi monitoringu ekonomicznego mogą być realizowane samodzielnie przez organizację, jednak coraz częściej realizowanie tych usług przekazywane jest wyspecjalizowanym jednostkom (outsourcing).

Współczesna organizacja, wykorzystując mechanizm monitoringu ekonomicznego, zapewnia sobie informację ekonomiczną, która staje się niezbędna do rozwoju i sprawnego funkcjonowania oraz zapewnienia sobie bezpieczeństwa ekonomicznego.

Bibliografia

Literatura:

- Adamczyk M., Jurga A., Kałkowska J. i inni, *Projektowanie systemów informacyjnych zarządzania*, Poznań 2010.
- Borowiecki R., Romanowska M., *System informacji strategicznej, Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Wydawnictwo Difin, Warszawa 2001.
- Cegieła R., Zalewski A., *Racjonalne zarządzanie przedsiębiorstwami informatycznymi i systemami komputerowymi*, Nakom, Poznań 2000.
- Flakiewicz W., *Systemy informacyjne w zarządzaniu*, Wydawnictwo Beck, Warszawa 2002.
- Forlicz S., *Informacja w biznesie*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2008.
- Gabusiewicz H., Hamrol M., Kurtys E., Sobolewski H., *Analiza wartości jako narzędzie optymalizacji kosztów własnych przedsiębiorstwa*, Akademia Ekonomiczna, Poznań 1998.
- Janasz K., Janasz W., Kozioł K., Szopik-Depczyńska K., *Zarządzanie strategiczne, Koncepcje, Metody, Strategie*, wydanie drugie, Wydawnictwo Difin, Warszawa 2010.
- Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 1999.
- Leszczyński Z., *Monitoring finansowy w zarządzaniu małym i średnim przedsiębiorstwem*, [w:] *Zarządzanie małym i średnim przedsiębiorstwem, Uwarunkowania europejskie*, Strużycki M. (red.), Wydawnictwo Difin, Warszawa 2002.
- Mytlewski A., *Monitoring ekonomiczny przedsiębiorstw*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2007.
- Radzikowski W., Wierzbiński J., *Controlling, Koncepcje – metody – zastosowania*, Toruńska Szkoła Zarządzania, Toruń 1999.
- Roman W.K., *Podstawy zarządzania informacją*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2012.
- Słownik języka polskiego, Polskie Wydawnictwo Naukowe.
- Zygała R., *Podstawy zarządzania informacją w przedsiębiorstwie*, Wydanie UE, wydanie I, Wrocław 2007.

Wykaz wykresów:

Wykres 1. Płeć respondentów.

Wykres 2. Wiek respondentów.

Wykres 3. Miejsce zamieszkania.

Wykres 4. Obserwacja zjawisk ekonomicznych w otoczeniu mikroekonomicznym i makroekonomicznym.

Wykres 5. Kategorie i zjawiska ekonomiczne podlegające obserwacji.

Wykres 6. Źródła pozyskiwania informacji ekonomicznej.

Wykres 7. Wpływ obserwacji ekonomicznej na decyzje gospodarcze.

Wykaz rysunków:

Rysunek 1. Rodzaje działalności informacyjnej.

Rysunek 2. Proces przepływu informacji.

Rysunek 3. Formy aktywności w przesyłaniu informacji.

Rysunek 4. Tok postępowania w działaniach organizacyjnych w zakresie monitoringu ekonomicznego.

Rysunek 5. System monitorowania w organizacji.

Rysunek 6. Zakres pól badawczych w monitoringu ekonomicznym.

Streszczenie

Artykuł poświęcony jest problematyce związanej z informacją w organizacji. Przedstawiono w nim znaczenie informacji i zasobów informacyjnych w procesach gospodarczych. Zaprezentowano i omówiono podstawowy mechanizm informacyjny w postaci monitoringu ekonomicznego, który wykorzystywany jest w organizacji do podejmowania najkorzystniejszych ekonomicznie decyzji oraz do zarządzania zasobami przedsiębiorstwa. Omówiono istotę zarządzania zasobami informacyjnymi. Zaprezentowano wyniki badań w zakresie wykorzystania obserwacji do rzeczywistości gospodarczej przez podmioty skali mikroekonomicznej.

Słowa kluczowe: informacja, zasoby informacyjne, procesy informacyjne, informacja ekonomiczna, monitoring ekonomiczny, zarządzanie informacjami.

Summary

Economic monitoring in the organization

The article is devoted to issues associated with information in activity of organization. In it meaning of information and information stores was presented in economic processes. An information basic mechanism was expressed in the form of the economic monitoring which is being used in the organization for taking most beneficial economically of decision and to the enterprise resource planning. Nature of the resource management was discussed information. They presented research results in using observation of the economic reality by entities of the microeconomic scale.

Key words: information, information stores, information processes, trading information, economic monitoring, information management.

Rozdział IX.

Współczesne uwarunkowania systemu zarządzania kryzysowego

1. Wstęp

W dobie ewolucji współczesnych zagrożeń bezpieczeństwa nadrzędnym celem systemu bezpieczeństwa narodowego jest zapewnienie jak najbardziej korzystnych i sprzyjających warunków realizacji interesów narodowych poprzez eliminację wewnętrznych i zewnętrznych zagrożeń, redukcję ryzyka oraz odpowiednie podejmowanie wyzwań i umiejętne wykorzystywanie pojawiających się szans¹. Jednym z istotnych podsystemów wykonawczych w systemie bezpieczeństwa narodowego, zapewniającym skuteczną ochronę ludności i bezpieczeństwa, jest system zarządzania kryzysowego, który odgrywa główną rolę w rozwiązywaniu sytuacji kryzysowych wiążących się bezpośrednio z ryzykiem.

W Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej widnieje zapis, zgodnie z którym nadrzędnym celem działań państwa w zakresie zarządzania kryzysowego jest „utrzymanie zdolności do reagowania – odpowiednio do zaistniałej sytuacji – w przypadku wystąpienia zagrożeń bezpieczeństwa publicznego oraz bezpieczeństwa powszechnego, związanych z ochroną porządku prawnego, życia i zdrowia obywateli oraz majątku narodowego przed bezprawnymi działaniami oraz skutkami klęsk żywiołowych, katastrof naturalnych i awarii technicznych”². Państwo powinno spełniać ową rolę przede wszystkim wobec

Dr Barbara Stefaniuk – Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej.

¹ B. Stefaniuk, *Udział elementów krajowego systemu ratowniczo-gaśniczego w zarządzaniu kryzysowym na przykładzie powiatu bialskiego*, Akademia Obrony Narodowej, Warszawa 2013, s. 72.

² Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 45.

swoich obywateli, a więc poprzez zapewnienie bezpieczeństwa wewnętrznego – zapewniać bezpieczeństwo powszechne i publiczne. We współczesnym ujęciu bezpieczeństwo publiczne to „oczekiwanie społeczne na zapewnienie możliwości korzystania z dobrobytu ekonomicznego, autonomii społecznej oraz określonego statusu politycznego”³. Podstawą efektywności działań podejmowanych na rzecz bezpieczeństwa powszechnego i publicznego w zarządzaniu kryzysowym jest współpraca podstawowych instytucji bezpieczeństwa powszechnego i publicznego, samorządów lokalnych z formacjami działającymi w tym zakresie, organizacjami pozarządowymi, sektorem prywatnym i obszarem obywatelskim. Głównymi podmiotami wykonawczymi w systemie zarządzania kryzysowego wobec społeczeństwa i państwa w zakresie bezpieczeństwa jest administracja samorządowa oraz służby porządku publicznego – Państwowe Ratownictwo Medyczne, Policja i Krajowy System Ratowniczo-Gaśniczy (KSRG) zbudowany na fundamencie Państwowej Straży Pożarnej⁴. Jednostki te tworzą triadę ochrony ludności w zarządzaniu kryzysowym, której podstawowym celem jest zaspokojenie jednej z podstawowych potrzeb społecznych – potrzeby bezpieczeństwa w zakresie ochrony życia i zdrowia obywateli.

2. Otoczenie systemu zarządzania kryzysowego

Otoczenie systemu zarządzania kryzysowego są to wszelkie procesy i zjawiska zachodzące wewnątrz i na zewnątrz systemu⁵. Otoczenie systemu zarządzania kryzysowego jest to zewnętrzne środowisko bezpieczeństwa, w którym zachodzą wszelkie zmiany i procesy oddziałujące na system. Na stan bezpieczeństwa otoczenia systemu zarządzania kryzysowego ma wpływ rodzaj wygenerowanych zagrożeń wewnątrz i na zewnątrz systemu⁶. W literaturze przedmiotu wyróżniamy środowisko bezpieczeństwa: zewnętrzne i wewnętrzne, militarne i niemilitarne (cywilne), które tworzą warunki bezpieczeństwa i realizacji interesów danego podmiotu w dziedzinie bezpieczeństwa oraz osiągnięcia wyznaczonych celów strategicznych w tym zakresie. Otoczenie systemu zarządzania kryzysowego charakteryzowane jest przy pomocy czterech podstawowych kategorii, do których zalicza się:

³ W. Lis, *Bezpieczeństwo państwa. Zagadnienia podstawowe*, Wydawnictwo Katolicki Uniwersytet Lubelski, Lublin 2014, s. 19.

⁴ B. Stefaniuk, *Udział elementów...*, s. 71.

⁵ B. Stefaniuk – definicja autorska.

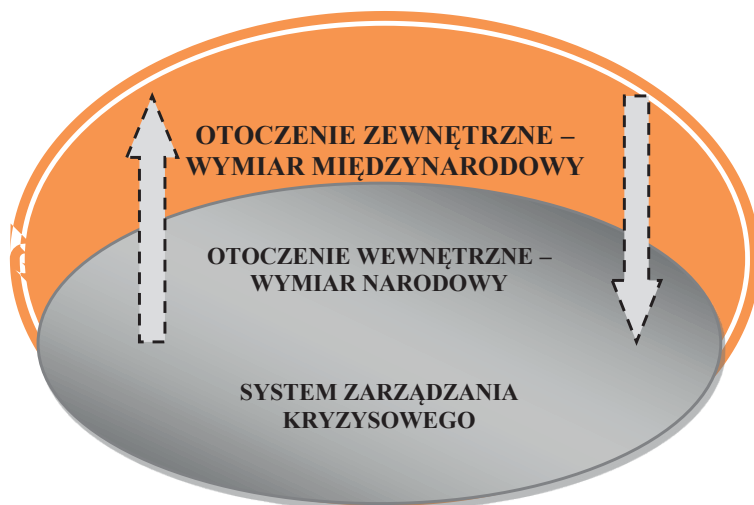
⁶ J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego w administracji publicznej*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2010, s. 65.

- szanse;
- wyzwania;
- ryzyka;
- zagrożenia.

Do najważniejszych wartości chronionych przez państwo należą⁷: przetrwanie państwa jako instytucji, narodu, grupy etnicznej, biologiczne przeżycie ludności, integralność terytorialna państwa, jego niezależność polityczna, swoboda działania międzynarodowego, spokój, ochrona własności i komfort życia obywateli.

Poniższy rysunek 1 przedstawia w sposób graficzny otoczenie systemu zarządzania kryzysowego.

Rysunek 1. Otoczenie systemu zarządzania kryzysowego



Źródło: opracowanie własne

Istotnym wyzwaniem dla bezpieczeństwa Polski będzie działalność zorganizowanych grup przestępczych, zwłaszcza transnarodowych. Zjawisko to będzie się nasilać wraz z rosnącą atrakcyjnością Polski dla grup przestępczych w związku z jej tranzytowym położeniem, postępującą integracją europejską, otwartością granic oraz wzrostem zamożności obywateli⁸. Do wyzwań dla polskiej polityki bezpieczeństwa w zakresie zarządzania kryzysowego w najbliższym czasie bę-

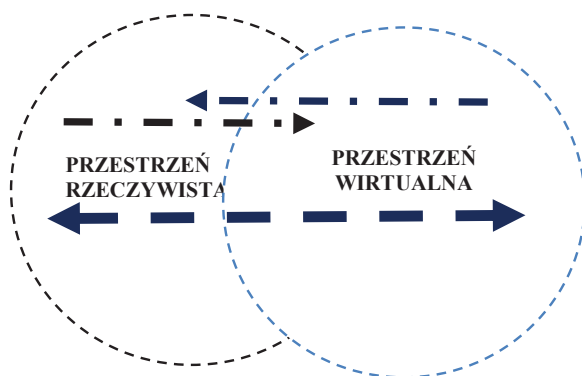
⁷ W. Kitler, *Zarządzanie kryzysowe w Polsce, stan obecny i perspektywy*, [w:] *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, G. Sobolewski, D. Majchrzak (red.), Akademia Obrony Narodowej, Warszawa 2011, s. 124.

⁸ *Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022*, Warszawa 2013, s. 31.

dzie należy dywersyfikacja źródeł energii, jej dostawców oraz kanałów przesyłowych, a także zwiększenie w tym wymiarze odporności kraju na sytuacje kryzysowe⁹. W erze rozwoju technologii informacyjnej istotnym wyzwaniem instytucji zarządzania kryzysowego jest walka z cyberterroryzmem. Cyberterroryzm to wszelkie działania terrorystyczne w cyberprzestrzeni. Cyberprzestrzeń obejmuje kluczowe dla systemu zarządzania kryzysowego systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj.: systemy łączności, transportu, infrastruktury energetycznej, wodociągowej, gazowej i ochrony zdrowia¹⁰.

Poniższy rysunek 2 przedstawia graficzną przestrzeń systemu zarządzania kryzysowego.

Rysunek 2. Przestrzeń systemu zarządzania kryzysowego



Źródło: opracowanie własne

Wyzwaniem dla bezpieczeństwa państwa pozostanie możliwość wystąpienia sytuacji kryzysowych w następstwie katastrof naturalnych lub wywołanych działalnością człowieka lub będących konsekwencją rozmaitych procesów i zjawisk globalnych. Wśród tych zagrożeń należy wymienić:

- suszę atmosferyczną;
- susze glebową;
- klęski geologiczne.

Dlatego też konieczne jest utrzymanie jak najwyższego poziomu zdolności do reakcji na tego typu wydarzenia, szybkiej minimalizacji ich skutków, a także zapobiegania im, gdy okaże się to możliwe. Szczególne znaczenie ma w tym

⁹ R. Grodzki, *Zarządzanie kryzysowe. Dobre praktyki*, Wydawnictwo Difin, s. 46.

¹⁰ W. Lis, *Bezpieczeństwo państwa...*, s. 163.

względzie zapewnienie należytej odporności na sytuacje kryzysowe infrastruktury krytycznej¹¹. Zasadniczymi czynnikami kształtującymi współczesny system zarządzania kryzysowego jest polityka bezpieczeństwa państwa, uwarunkowania zewnętrzne i wewnętrzne, współczesne wyzwania i zagrożenia oraz ewolucja zintegrowanego systemu bezpieczeństwa narodowego w obszarze ratownictwa i ochrony ludności¹².

3. Zarządzanie kryzysowe w administracji publicznej

Teoretyczny aspekt zarządzania kryzysowego polega na wyjaśnieniu pojęć „kryzys” i „sytuacja kryzysowa” oraz powiązanie tych pojęć z zarządzaniem kryzysowym. W literaturze przedmiotu kryzys definiowany jest jako sytuacja, której skutki zagrażają życiu lub zdrowiu, a zapobieganie jej i likwidacja jej skutków jest podejmowana z zastosowaniem zwykłych lub nadzwyczajnych środków, we współdziałaniu różnych organów administracji publicznej i instytucji oraz specjalistycznych formacji ratowniczych¹³. Kryzys to sytuacja, w której istnieje zagrożenie dla podstawowych wartości, celów i interesów organizacji lub zagrożone są prawa i swobody obywateli, ich życie i mienie¹⁴. Z kolei sytuacja kryzysowa to stan rzeczy lub okoliczność, w której załamuje się dotychczasowy proces rozwoju i zakłócone zostaje funkcjonowanie danego podmiotu¹⁵. System zarządzania kryzysowego jest głównym filarem ochrony ludności i bezpieczeństwa państwa w Polsce¹⁶.

Zarządzanie kryzysowe, w świetle literatury przedmiotu, definiuje się jako system, w którym poszczególne, zależne funkcje są zharmonizowane, zaś sama organizacja określana jest jako sieć dynamicznych procesów¹⁷. Zarządzanie kryzysowe to zestaw działań polegających na sterowaniu procesami i powiązaniem między nimi dla uzyskania wymaganych właściwości materiałów i wyrobów oraz zaspokojenia wymagań kolejnych klientów w łańcuchu procesów, a także na zbie-

¹¹ Strategia rozwoju systemu bezpieczeństwa..., s. 31.

¹² Tamże.

¹³ J. Stawicka, B. Wiśniewski, R. Socha, *Zarządzanie kryzysowe. Teoria. Praktyka. Konteksty. Badania*, Wyższa Szkoła Policji, Szczytno 2011, s. 52.

¹⁴ R. Grodzki, *Zarządzanie kryzysowe...*, Wydawnictwo Difin, s. 17.

¹⁵ W. Kitler, *Zarządzanie kryzysowe w Polsce...*, s. 33.

¹⁶ Materiały z konferencji naukowej z cyklu „Zarządzanie kryzysowe w systemie bezpieczeństwa państwa. Podmioty wykonawcze w zarządzaniu kryzysowym”, Akademia Obrony Narodowej, Warszawa, 4 grudnia 2012 roku, s. 3.

¹⁷ K. Graczyk, G. Nakielski, T. Tabacznik, *Elementy zarządzania kryzysowego w administracji terytorialnej*, Uniwersytet Zielonogórski, Zielona Góra 2015, s. 54.

raniu informacji dla potrzeb zarządzania. Istotą funkcji zarządzania kryzysowego jest konstruowanie celu działania i organizowanie toku czynności, pozyskiwanie i wykorzystanie potrzebnych zasobów ludzkich i rzeczowych przeznaczonych do realizacji założonych celów, wynikających z dokumentów strategicznych.

Zarządzanie kryzysowe to działalność organów władzy na wszystkich szczeblach organizacji państwa angażująca wyspecjalizowane organizacje, inspekcje, straże oraz społeczeństwo. Misją systemu zarządzania kryzysowego jest ochrona ludności i ratownictwo. Rolę organów kierowania spełniają organy właściwe w sprawach zarządzania kryzysowego na poszczególnych szczeblach organizacji państwa, zaś jednostek wykonawczych systemu – Państwowa Straż Pożarna, Policja, jednostki systemu Państwowego Ratownictwa Medycznego, Centra Powiadamiania Ratunkowego, inne jednostki ochrony przeciwpożarowej, dyspozytorzy medyczni, jednostki ochrony zdrowia, instytucje wspierające, tj.: Straż Graniczna, Morska Służba Poszukiwania i Ratownictwa oraz inne właściwe w tych sprawach państwowe urzędy, agencje, inspekcje, straże i służby¹⁸.

Zadania realizowane w zakresie zarządzania kryzysowego wymagają koordynacji działań wielu niezależnych merytorycznie podmiotów, konsolidacji procedur działania i wykorzystywanych technologii. Wymagają również podejmowania trafnych i racjonalnych decyzji. Niezbędna w tym zakresie jest szeroka wiedza, ciągłe doskonalenie, podnoszenie kompetencji, świadomości oraz nieustanne uzupełnianie informacji. Zarządzania kryzysowego nie da się ująć w sztywne ramy, gdyż każda sytuacja kryzysowa jest odmienna, zróżnicowana i złożona¹⁹. Dynamizm sytuacji kryzysowych stanowi źródło ciągłych zmian w zakresie ustawicznego doskonalenia mechanizmów działań, procedur i zasad współpracy²⁰. Istotą zarządzania procesowego jest zapewnienie sprawnych i logicznych działań. W praktyce zarządzania kryzysowego polega to na oddelegowaniu uprawnień i odpowiedzialności na organy właściwe w poszczególnych jednostkach samorządowych oraz orientacji na szereg funkcji realizowanych na rzecz społeczeństwa w tych jednostkach. Samorząd znajduje się najbliżej obywateli, ma więc bezpośrednią możliwość oceny lokalnych zagrożeń i jest w stanie podjąć bezwzględną reakcję w przypadku ich wystąpienia.

W funkcjonowaniu systemu zarządzania kryzysowego zakłada się kompleksowość i spójność podejmowanych działań w celu skutecznego przeciwstawienia się wszelkim zagrożeniom i efektywną integrację potencjału militarnego z administracją, gospodarką oraz społeczeństwem. Ponieważ żaden z elementów

¹⁸ B. Stefaniuk, *Udział elementów krajowego systemu ratowniczo-gaśniczego...*, s. 74.

¹⁹ Tamże, s. 45.

²⁰ Tamże, s. 80.

systemu bezpieczeństwa narodowego nie jest zdolny do samodzielnego wykonywania zadań związanych z bezpieczeństwem państwa, wymaga to współdziałania struktur organizacyjnych właściwych do spraw zarządzania kryzysowego i reagowania obronnego, funkcjonujących w okresie pokoju, kryzysu i wojny, na każdym szczeblu kierowania²¹. Zarządzanie to system działań regulujący sposób oraz zasady funkcjonowania określonej organizacji zgodnie z wytyczonymi celami²², które obejmują funkcje planowania, organizowania, motywowania i kontroli. Funkcje te powiązane są ściśle z funkcjonowaniem organizacji, dysponowaniem zasobami i władzą mającą prawo nimi rozporządzać tak, aby osiągać wyznaczone zadania, stosując przy tym optymalną strategię jej funkcjonowania²³.

Zarządzanie kryzysowe odnosi się do zagrożeń, które ze względu na swoją specyfikę mogą doprowadzić do ograniczenia możliwości przeciwdziałania nim ze względu na niewystarczającą ilość środków pozwalających zapobiec dalszemu rozwojowi niekorzystnej sytuacji. System zarządzania kryzysowego jest systemem likwidującym zagrożenia poprzez zapobieganie, przygotowanie, reagowanie i odbudowę. Zarządzanie kryzysowe umożliwia ocenę, klasyfikację i analizę nowych zagrożeń, które dotychczas nie były zdefiniowane lub miały inne znaczenie i wymiar. Czas zaistnienia kryzysu uwarunkowany jest koniecznością szybkiego podejmowania decyzji, małą przewidywalnością i wysokim stopniem niepewności²⁴.

W literaturze z zakresu nauk o bezpieczeństwie, zarządzaniu organizacjami i ratownictwie zarządzanie kryzysowe utożsamiane jest z integralną częścią bezpieczeństwa narodowego, które spełnia zasadniczą rolę w rozwiązywaniu sytuacji kryzysowych, wiążących się z ryzykiem polegającym na przeciwdziałaniu zagrożeniom, przygotowaniu się na wypadek ich wystąpienia oraz utrzymaniu lub przywracaniu stanu stabilizacji²⁵. Współczesne zagrożenia trzeba wykrywać, weryfikować, poznawać i przede wszystkim badać. Wymaga tego sprawność i jakość zarządzania kryzysowego. Najogólniej zagrożenie można zdefiniować jako możliwość poniesienia straty, utraty zdrowia, życia, zniszczenia mienia, skażenia środowiska w wyniku zdarzenia niepożądanego, tj. pożaru, wypadku drogowego, emisji substancji toksycznej do środowiska²⁶. Wczesne rozpoznanie zagrożenia

²¹ Tamże.

²² B. Stefaniuk, *Organizacja Państwowej Straży Pożarnej w powiecie*, Akademia Obrony Narodowej, s. 8.

²³ Tamże, s. 8.

²⁴ A. Warmiński, *Zadania i środki działania rządowych organów administracji ochrony bezpieczeństwa państwa i porządku publicznego*, Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej, Biała Podlaska 2012, 23.

²⁵ B. Stefaniuk, *Udział elementów krajowego systemu ratowniczo-gaśniczego...*, s. 74.

²⁶ Tamże, s. 9.

pozwała identyfikować obszary, które wiążą się z największym ryzykiem wystąpienia sytuacji kryzysowej.

4. Źródła zagrożeń kryzysowych – uwarunkowania

W literaturze przedmiotu współcześnie przyjmuje się, że zagrożenia godzące w bezpieczeństwo człowieka, jego mienia i środowiska, w którym egzystuje, wynikają z dwóch głównych źródeł²⁷. Pierwsze źródło stanowi działalność człowieka przeciwko człowiekowi lub prawom przyrody. Drugie źródło to z działania sił natury. Sytuacje wywołane działaniem sił przyrody prowadzą do katastrof naturalnych, tj.: powodzi, długotrwałych susz i powstałych w ich wyniku lokalnych deficytów wody, wielkoobszarowych pożarów, huraganowych wiatrów, osuwisk ziemi i splotów błotnych, epidemii chorób zakaźnych. Sytuacje wywołane działalnością człowieka²⁸ to m.in. awarie techniczne i katastrofy komunikacyjne.

Do zagrożeń, które kształtują otoczenie zewnętrzne systemu zarządzania kryzysowego, zalicza się m.in.:

- proliferację broni masowego rażenia;
- międzynarodowy terrorizm;
- cyberterrorizm;
- osłabienie systemu organizacji międzynarodowych, np. Unii Europejskiej, w walce z kryzysem migracyjnym;
- dominację zagrożeń asymetrycznych;
- negatywne zjawiska w cyberprzestrzeni;
- zagrożenia bezpieczeństwa żywnościowego.

Do obecnych zagrożeń systemu można zaliczyć zagrożenia bezpieczeństwa energetycznego, a więc uzależnienie od dostaw gazu ziemnego i ropy naftowej z jednego źródła oraz ograniczone zdolności transportowania i magazynowania nośników energetycznych, które wymiennie obniżają odporność naszego kraju na sytuacje kryzysowe związane z bezpieczeństwem energetycznym i wywołane przez czynniki natury politycznej lub technicznej²⁹. Różnice w postrzeganiu wyzwań i zagrożeń bezpieczeństwa oraz własnych korzyści przez członków Paktu Północnoatlantyckiego i Unii Europejskiej w połączeniu z niejasnym i nieprzewi-

²⁷ J. Ziarko, J. Walas-Trębacz, *Podstawy zarządzania kryzysowego, cz. I: Zarządzanie kryzysowe w administracji...*, s. 30.

²⁸ Zob. Krajowy Plan Zarządzania Kryzysowego na lata 2013/2015.

²⁹ R. Wróblewski, *Zarządzanie kryzysowe jako element zarządzania bezpieczeństwem narodowym*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2013, s. 498.

dywalnym rozwojem środowiska bezpieczeństwa mogą stanowić poważne wyzwanie dla międzynarodowej wspólnoty w obszarze zarządzania kryzysowego.

5. Międzynarodowy aspekt zarządzania kryzysowego

Bezpieczeństwo zewnętrzne państwa to zapewnienie bezpieczeństwa państwa na zewnątrz poprzez wszelkie działania dyplomatyczne, rozwijanie stosunków politycznych, gospodarczych i kulturalnych z innymi państwami, a także rozwijanie przepływu informacji i kontaktów międzyludzkich. Współczesny system zarządzania kryzysowego i bezpieczeństwa narodowego jest uwarunkowany dynamicznym procesem identyfikacji zagrożeń, podejmowanych wyzwań, definiowania celów i sposobów ich realizacji. Nowa jakość bezpieczeństwa przejawia się w takich cechach jak:

- informacyjność;
- powszechność informacji, która wpływa na nastroje i wywołuje presję opinii publicznej na określone działania;
- asymetryczność w doborze sił i środków;
- sieć instytucji międzynarodowych i narodowych odpowiedzialnych za bezpieczeństwo;
- zintegrowanie działań reagowania kryzysowego³⁰.

Poniższy rysunek 3 przedstawia uwarunkowania systemu zarządzania kryzysowego.

Rysunek 3. Uwarunkowania systemu zarządzania kryzysowego



Źródło: opracowanie własne

³⁰ Strategia rozwoju systemu bezpieczeństwa narodowego..., s. 33.

System zarządzania kryzysowego Rzeczypospolitej Polskiej zintegrowany jest z systemem zarządzania kryzysowego Unii Europejskiej (UE) i Paktu Północnoatlantyckiego (NATO)³¹. System zarządzania Paktu Północnoatlantyckiego tworzą takie podsystemy jak:

- wywiadowczy i wczesnego ostrzegania;
- planowania operacyjnego;
- planowania cywilnego w sytuacjach nadzwyczajnych;
- reagowania kryzysowego.

Podstawę funkcjonowania systemu tworzą reguły prawa międzynarodowego, prawa narodowego, strategia NATO i doktryny. Operacje reagowania kryzysowego obejmują:

- operacje, prowadzenie działań związanych z wycofaniem sił;
- operacje humanitarne;
- poszukiwanie i ratownictwo;
- wsparcie operacji ewakuacyjnych;
- wsparcie działań stabilizacyjnych poza granicami kraju³².

Współpraca systemu zarządzania kryzysowego w wymiarze międzynarodowym uwarunkowana jest dominacją współczesnych zagrożeń bezpieczeństwa międzynarodowego, która ukierunkowana jest na realizację działań podejmowanych na rzecz zapewnienia bezpieczeństwa kooperatywnego (zbiorowego).

5. Zakończenie

Rozwój cywilizacyjny stworzył dobra ułatwiające życie, podnosząc przy tym jego standard. Obok zagrożeń naturalnych pojawiły się nowe problemy – efekty uboczne postępu technologicznego, zagospodarowania przestrzennego, rozwoju zagrożeń asymetrycznych i coraz to nowszych rozwiązań technologicznych. Zagrożenia takie są nieprzewidywalne i mogą mieć szeroki zasięg oddziaływania.

Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego spełnia zasadniczą rolę w rozwiązywaniu sytuacji kryzysowych, wiążących się z ryzykiem. Zarządzanie kryzysowe to nowa, dynamiczna dziedzina wiedzy. Wymaga stałego dostosowywania sił i środków do wciąż zmieniającego się stanu bezpieczeństwa w wymiarze narodowym i międzynarodowym w celu utrzymania zdolności do reagowania na zagrożenia. Z tego względu instytucje zarządzania

³¹ L. Wojnicz, *Polityka Unii Europejskiej wobec terroryzmu*, Wydawnictwo Adam Marszałek, Toruń 2011, s.74.

³² M. Marszałek, *Operacje reagowania kryzysowego NATO. Istota. Uwarunkowanie. Planowanie*, Wydawnictwo Difin 2013, s. 42.

kryzysowego, narodowe i międzynarodowe, największy nacisk kładą się na proces planowania, przygotowania i organizowania funkcji, struktur i zdań w systemie. W ogólnym ujęciu podejście procesowe pozwala zarządzać sferami łączącymi elementy systemu, które tworzą strukturę organizacji, oraz pozwala integrować elementy. Zadania realizowane w zakresie zarządzania kryzysowego wymagają koordynacji działań wielu niezależnych merytorycznie podmiotów. Wynikiem procesowego zarządzania kryzysowego jest wypracowanie zasad skutecznej pracy zespołowej, kanałów komunikacji i sprawne prowadzenie działań w przypadku wystąpienia sytuacji kryzysowej. Elementem kierowania bezpieczeństwem narodowym jest i będzie zarządzanie kryzysowe, definiowane jako działalność organów administracji publicznej polegająca na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzania zasobów i infrastruktury krytycznej.

Współczesne wyzwania i zagrożenia obligują do podjęcia długofalowych działań doraźnych i zapobiegawczych w dziedzinie bezpieczeństwa narodowego. Konieczne w tym zakresie jest stworzenie właściwych instytucjonalnych mechanizmów działania, które będą sprawnie funkcjonować w razie wystąpienia bezpośredniego zagrożenia, a także umożliwią podjęcie efektywnych działań, minimalizujących prawdopodobieństwo wystąpienia niepożądanych zjawisk i zagrożeń wtórnych.

Bibliografia

Literatura:

- Graczyk K., Nakielski G., Tabacznik T., *Elementy zarządzania kryzysowego w administracji terytorialnej*, Uniwersytet Zielonogórski, Zielona Góra 2015.
- Grodzki R., *Zarządzanie kryzysowe. Dobre praktyki*, Wydawnictwo Difin, Warszawa 2012.
- Kitler W., *Zarządzanie kryzysowe w Polsce, stan obecny i perspektywy*, [w:] *Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego*, G. Sobolewski, D. Majchrzak (red.), Akademia Obrony Narodowej, Warszawa 2011.
- Lis W., *Bezpieczeństwo państwa. Zagadnienia podstawowe*, Wydawnictwo Katolicki Uniwersytet Lubelski, Lublin 2014.
- Krajowy Plan Zarządzania Kryzysowego na lata 2013/2015.
- Marszałek M., *Operacje reagowania kryzysowego NATO. Istota. Uwarunkowanie. Planowanie*, Wydawnictwo Difin 2013.
- Stefaniuk B., *Organizacja Państwowej Straży Pożarnej w powiecie*, Akademia Obrony Narodowej, Warszawa 2009.

- Stefaniuk B., *Udział elementów krajowego systemu ratowniczo-gaśniczego w zarządzaniu kryzysowym na przykładzie powiatu bialskiego*, Akademia Obrony Narodowej, Warszawa 2013.
- Sobolewski G., *Organizacja i funkcjonowanie Centrum Zarządzania Kryzysowego*, Akademia Obrony Narodowej, Warszawa 2012.
- Stawicka J., Wiśniewski B., Socha R., *Zarządzanie kryzysowe. Teoria. Praktyka. Konteksty. Badania*, Wyższa Szkoła Policji, Szczytno 2011.
- Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022, Warszawa 2013.
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.
- Warmiński A., *Zadania i środki działania rządowych organów administracji ochrony bezpieczeństwa państwa i porządku publicznego*, Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej, Biała Podlaska 2012.
- Wojnicz L., *Polityka Unii Europejskiej wobec terroryzmu*, Wydawnictwo Adam Marszałek, Toruń 2011.
- Wróblewski R., *Zarządzanie kryzysowe jako element zarządzania bezpieczeństwem narodowym*, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2013.
- Ziarko J., Walas-Trębacz J., *Podstawy zarządzania kryzysowego w administracji publicznej*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2010.

Streszczenie

Celem artykułu pt. *Współczesne uwarunkowania systemu zarządzania kryzysowego* jest ukazanie współczesnych wewnętrznych, jak i międzynarodowych uwarunkowań systemu zarządzania kryzysowego w Polsce. Zmiany, jakie zachodzą w środowisku bezpieczeństwa w wymiarze globalnym, powodują ewolucję pojęcia bezpieczeństwa i zagrożenia. Uwarunkowania systemu zarządzania kryzysowego to wszelkie czynniki wewnętrzne i zewnętrzne, które mają wpływ na poziom bezpieczeństwa narodowego i efektywność zarządzania kryzysowego. Współcześnie można skonstruować szeroki katalog zagrożeń, którym przeciwdziałają system zarządzania kryzysowego. Do katalogu zdarzeń dopisywane są coraz to nowe zagrożenia, na podstawie których system jest ciągle doskonalony, weryfikowany i modyfikowany na wszystkich szczeblach administracji publicznej.

Słowa kluczowe: zagrożenie, bezpieczeństwo, otoczenie, system, zarządzanie kryzysowe.

Summary

The aim of the article on. *Contemporary conditions of crisis management system* is to show the contemporary internal and international conditions of the crisis management system in Poland. The changes taking place in the security environment on a global scale, causing evolution of the concept of safety and security. Conditions crisis management system, any internal and external factors, that have an impact on the level of national security and the effectiveness of crisis management. Today, you can construct a broad spectrum of threats, which counteracts the crisis management system. To the event directory, credited for ever new threats based on which the system is constantly improved, revised and modified at all levels of public administration.

Key words: risk, security, environment, system, crisis management.

Rozdział X.

Wzrost znaczenia bezpieczeństwa elektronicznego transferu danych w Internecie w kontekście bezpieczeństwa administracji publicznej państwa

1. Wprowadzenie

Dynamiczny rozwój technologii elektronicznego transferu danych w globalnej sieci Internetu znacząco przyspieszył już od pierwszej połowy lat 90. W Polsce ten proces znacząco przyspiesza pod koniec ubiegłego wieku, co związane jest z rozwojem elektronicznej bankowości oferowanej za pośrednictwem Internetu dla różnych segmentów klientów. Od 1998 roku, kiedy Powszechny Bank Gospodarczy uruchomił Oddział Elektroniczny, zaczęła się rozwijać internetowa bankowość elektroniczna w Polsce z ofertą skierowaną także dla klientów indywidualnych.

Praktycznie od początku rozwoju usługi zdalnego dostępu do oferty banku pojawiają się nowe kategorie ryzyka, instrumenty zabezpieczeń oraz problematyka bezpieczeństwa dostępu do oferty instytucji finansowych poprzez Internet. Powszechnie dominuje pogląd, że z sukcesywnym rozwojem elektronicznej bankowości rośnie znaczenie kwestii bezpieczeństwa elektronicznego transferu danych, w tym doskonalenia instrumentów zarządzania ryzykiem systemów informatycznych. Ponieważ rozwój elektronicznej bankowości internetowej

Dr Dariusz Prokopowicz – Wydział Nauk Historycznych i Społecznych, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.

dotyczy już praktycznie każdej instytucji finansowej, więc bezustanny proces doskonalenia systemów bezpieczeństwa elektronicznego transferu danych stał się składową rynkowej konkurencji¹. W wyniku tych systemowych i rynkowych procesów system finansowy w Polsce staje się w coraz większym stopniu dostosowany do analogicznych systemów innych krajów, przede wszystkim krajów Europy Zachodniej należących do Unii Europejskiej².

Ponad 10 lat temu dokonany został istotny proces determinujący kolejny etap przyśpieszenia globalizacji ekonomicznej i wpływający na makroekonomiczny rozwój polskiej gospodarki. W 2004 roku Polska wstąpiła w struktury rynkowe Unii Europejskiej, co miało istotne znaczenie także dla dalszego rozwoju bankowości komercyjnej. Otóż, ponieważ Polska jest częścią Unii Europejskiej, niektóre aspekty umiędzynarodowienia polskiego systemu finansowego, w tym w zakresie technologii teleinformatycznej, były nieuniknione, np. w kwestii ujednoczenia standardów elektronicznego transferu danych w systemach informatycznych banków i dostosowania technicznych narzędzi bezpieczeństwa transferu danych w systemach bankowości elektronicznej, jak również dostosowania normatywów prawa i struktury systemu bankowego w Polsce do wytycznych Komitetu Bazylejskiego ds. Nadzoru Bankowego, tj. centralnego organu nadzoru bankowego w Unii Europejskiej³. Jednak mimo tego, że instytucje rynkowego systemu finansowego w ostatnich latach zwykle wyznaczają kluczowe trendy w zakresie rozwoju technologii teleinformatycznej, to jednak problematyka elektronicznego transferu danych dotyczy także w coraz większym stopniu instytucji publicznych i przedsiębiorstw niefinansowych. Dzieje się tak w związku z coraz powszechniej realizowaną cyfryzacją urzędów i instytucji publicznych.

Od kilkunastu lat cyfryzacja urzędów i instytucji publicznych przeprowadzana jest także w Polsce. Dokonujący się proces informatyzacji infrastruktury przedsiębiorstw i urzędów zwiększa skalę zaangażowania technologii informatycznej w celu elektronicznego gromadzenia, przetwarzania oraz udostępniania informacji niejawnych między podmiotami funkcjonującymi w gospodarce. Kwestia ta dotyczy również informatyzacji procesów, które operują na zasobach danych osobowych klientów podmiotów gospodarczych i obywateli wobec urzędów

¹ B. Domańska-Szaruga, *Financial Instability and the New Architecture of Financial Supervision in European Union*, [w:] B. Domańska-Szaruga, T. Stefaniuk (red.), *Organization in changing environment. Conditions, methods and management practices*, Wydawnictwo Studio Emka, Warszawa 2014, s. 23.

² M. Wiśniewska, *Finanse w dobie kryzysu*, Seria „Prace Naukowe Wyższej Szkoły Bankowej w Gdańsku”, Wydawnictwo CeDeWu, Warszawa 2013.

³ B. Domańska-Szaruga, *Common banking supervision within the financial safety net*, [w:] *The Economic Security of Business Transactions. Management in business*, Wydawnictwo Chartridge Books Oxford, Oxford 2013, s. 265.

i instytucji publicznych⁴. Poza tym sukcesywnie realizujący się postęp w zakresie technologii informatycznej wymusza permanentne doskonalenie technik ochrony informacji niejawnych przetwarzanych w bazach danych przedsiębiorstw, instytucji finansowych i publicznych oraz transferowanych poprzez sieć Internet.

W związku z wymienionymi procesami w ostatnich latach zwiększa się także rola bezpieczeństwa systemów informatycznych i ochrony stale rosnących zasobów danych osobowych w bazach danych internetowych portali społecznościowych, w których obywatele dzielą się informacjami niekiedy nawet bardzo osobistymi. Poza tym rośnie liczba firm, które zbierają dane osobowe w celach marketingowych, a następnie je odsprzedają innym firmom, bankom lub instytucjom. Coraz powszechniej zbieranie danych osobowych nie ogranicza się już tylko do podstawowych informacji typu imię, nazwisko, płeć i wiek, ale związane jest także z innymi kategoriami – prywatnymi informacjami dotyczącymi poszczególnych obywateli, jak np. preferencje zakupowe, zainteresowania, miejsce pracy, poziom dochodów itd. W ten sposób przedsiębiorstwa, instytucje finansowe i publiczne tworzą ogromne zbiory danych niejawnych stanowiące wartościową informację na potrzeby podejmowanych przedsięwzięć marketingowych.

Doskonalona w ten sposób segmentacja potencjalnych odbiorców oferty znacząco zwiększa efektywność prowadzonych działań marketingowych. Poprzez kierowanie stosownie sprofilowanej oferty produktowej lub usługowej do ściśle wyselekcjonowanej grupy odbiorców, kontrahentów, segmentu docelowego potencjalnych klientów uzyskuje się większą skuteczność zastosowanej strategii marketingowej podczas kampanii reklamowych.

Przeprowadzane w ten sposób przedsięwzięcia kampanii reklamowych generują znaczącą redukcję kosztów niezbędnych działań marketingowych w sytuacji skierowania oferty do ściśle określonego segmentu potencjalnych nabywców. W związku z tym budowane w instytucjach, przedsiębiorstwach, w tym także w internetowych portalach społecznościowych, rozbudowane wieloaspektowo i informacyjnie bazy danych osobowych stają się cennym zasobem informacji wykorzystywanej na potrzeby marketingu. Rosnące informacyjnie i wymiennie wartościowo bazy danych osobowych wymuszają na utrzymujących je podmiotach ponoszenie nakładów na zapewnienie wymaganego poziomu bezpieczeństwa⁵. W wypadku funkcjonujących w Internecie firm, w tym internetowych portali społecznościowych, działających w Internecie firm oferujących hosting, usługi zakładania witryn WWW i poczty elektronicznej, telekomów, instytucji

⁴ A. Gołębiowska, *Local government in the Constitution of the Republic of Poland of 1997*, "Ius Novum", nr 2 (2015), s. 29.

⁵ M. Muchacki, *Cywilizacja informatyczna i Internet. Konteksty współczesnego konsumenta TI*, Wydawnictwo Impuls, Warszawa 2014.

publicznych z elektronicznym dostępem do sprofilowanych usług oraz oddziałów elektronicznych banków i innych instytucji finansowych, występuje znaczące ryzyko nieuprawnionego dostępu do danych osobowych przez hakerów działających np. na zlecenie firm i instytucji konkurencyjnych⁶.

Permanently rosnąca liczba tego typu baz danych niejawnych tworzonych przez podmioty działające także w Internecie i stale powiększany zakres gromadzonych w nich informacji może generować wzrost ryzyka upublicznienia danych osobowych obywateli w sieci Internet. W związku z tym podmioty utrzymujące i rozbudowujące tego typu bazy danych zmuszone są do ponoszenia coraz większych nakładów na doskonalenie technicznych zabezpieczeń zgromadzonych zasobów danych niejawnych celem ograniczenia potencjalnego uaktywnienia się wymienionych powyżej kategorii ryzyka utraty, kradzieży lub upublicznienia danych osobowych obywateli w Internecie⁷.

W związku z przedstawionymi powyżej obiektywnie realizującymi się procesami w ostatnich latach powstają nowe kategorie internetowego ryzyka systemów teleinformatycznych, jako pochodna dynamicznie rozwijających się i stale rozbudowywanych dużych zbiorów danych osobowych tworzonych przez firmy oferujące określone produkty lub usługi użytkownikom Internetu. Od kilku lat tego typu hurtownie danych coraz częściej funkcjonują jako zbiory informacji określane jako Big Data oraz w tzw. chmurach obliczeniowych. Do firm, które obecnie posiadają największe tego typu zbiory danych o użytkownikach Internetu, należą przede wszystkim Google, Facebook, Twitter, Instagram, YouTube i inne. Ponieważ każdy z tych komercyjnie działających podmiotów tworzy własne bazy danych o użytkownikach Internetu, więc tzw. wrażliwe dane osobowe są obecnie przechowywane w wielu miejscach globalnej sieci⁸.

Ponadnarodowo działające korporacje internetowe oferujące użytkownikom Internetu darmowe korzystanie z oferowanych usług, w tym także na platformach portali społecznościowych, tworzą specjalne programy zwane robotami, dzięki którym przeprowadzają analizę dostępnych w Internecie informacji na temat poszczególnych użytkowników i zbierają dane osobowe na potrzeby prowadzonej działalności marketingowej. Prawdopodobnie niewielka część użytkowników Internetu wie, jak daleko zaszła już ta skomercjonalizowana inwigilacja prowadzona przez firmy internetowe. Działalność tych podmiotów

⁶ S. Dolecki, *Brutalna cyberrzeczywistość*, „Bank. Miesięcznik finansowy”, raport specjalny „Cyberbezpieczeństwo”, Warszawa 2016, nr 4/276, s. 51.

⁷ S. Gwoździewicz, *The European Union Towards the Threats in Cyberspace*, International Scientific Journal „Verejna Sprava a Spolocnost”, Rocznik XV, No 2/2014, Słowacja, Koszyce 2014, s. 52.

⁸ M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014, s. 93.

podwyższa potencjalną skalę ryzyka związanego z możliwym spadkiem bezpieczeństwa informacji niejawniej gromadzonej w elektronicznych bazach danych i transferowanej poprzez systemy teleinformatyczne podłączone do Internetu⁹.

We współczesnych gospodarkach krajów wysokorozwiniętych i rozwijających się instytucje sektora publicznego, zarówno urzędy krajowe, jak i jednostki samorządu terytorialnego, pełnią szczególnie istotną rolę w zaspokajaniu potrzeb społeczeństwa i pośrednio całej gospodarki. Po ponad ćwierćwieczu rozwoju polskiej gospodarki w warunkach rynkowych i procesach dostosowawczych do systemowych standardów Unii Europejskiej także w Polsce jedną ze sfer oferowanych usług publicznych jest zaspokajanie potrzeb informacyjnych obywateli¹⁰. Procesy decyzyjne zapadające w instytucjach sektora publicznego dotyczące np. gospodarki finansowej pośrednio wpływają na tempo rozwoju społeczno-gospodarczego kraju¹¹.

Od lat 90. w Polsce rośnie znaczenie kwestii racjonalizacji prowadzonej gospodarki finansowej, ponieważ działania te mają skłonić do wzrostu efektywności ekonomicznej procesu gospodarowania zasobami pieniężnymi. Przedsięwzięcia te powinny przyczyniać się do aktywizacji procesów gospodarczych i tym samym przyczyniać się do poprawy funkcjonowania w zakresie efektywności ekonomicznej zarówno poszczególnych podmiotów sektora publicznego, jak i całego sektora finansów publicznych i pośrednio całej gospodarki.

W kluczowych obszarach działalności instytucji publicznych istotną kwestią jest pozyskiwanie, przetwarzanie, gromadzenie, archiwizowanie oraz udostępnianie dla innych podmiotów różnego rodzaju informacji, w tym informacji jawnych oraz niejawnych, także danych osobowych obywateli. Kluczową kwestią w tym obiegu i udostępnianiu informacji jest bezpieczeństwo archiwizowania i transferu danych w teleinformatycznych systemach instytucji sektora publicznego oraz w sieci Internet¹².

Analogicznie jak podmioty sektorów komercyjnych, tak i instytucje sektora publicznego, aby sprawnie funkcjonować, muszą bezustannie dostosowywać się do zmieniających się realiów otoczenia społeczno-gospodarczego i postępu technologicznego w zakresie nowoczesnych rozwiązań informatycznych bezpiecznego archiwizowania, przetwarzania i udostępniania informacji.

⁹ P. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologii*, „Prokuratura i Prawo”, nr 1/2011, s. 27.

¹⁰ D. Wociór (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Wydawnictwo C.H. Beck, Warszawa 2016, s. 48.

¹¹ M. Muchacki, *Cywilizacja informatyczna i Internet...*, s. 27.

¹² M. Górka (red.), *Cyberbezpieczeństwo jako podstawa...*, s. 148.

2. Uwarunkowania ekonomiczne i cywilizacyjne technologicznego postępu w zakresie transferu i udostępniania danych w Internecie

Polska gospodarka w okresie ostatniego ćwierćwiecza przeszła gruntowną wieloaspektową transformację systemową. W tym okresie zaszły istotne zmiany w polskiej gospodarce, w tym w przedsiębiorstwach oraz podmiotach sektora publicznego, tj. jednostkach samorządu terytorialnego. Ponadto sukcesywnie realizowane są procesy integracyjne struktur gospodarczych poszczególnych krajów, szczególnie w obszarze Unii Europejskiej. Podstawą tych procesów była liberalizacja transgranicznych przepływów kapitałowych wsparta harmonizacją regulacji prawnych. Tymczasem rozwój nowoczesnych technologii generuje doskonalenie, innowacje i udogodnienia elektronicznego transferu danych i udostępniania informacji oraz upraszcza kanały dystrybucji produktów i usług, co przyczynia się do zwiększenia wzrostu gospodarczego¹³. W podmiotach gospodarczych natomiast obserwuje się wzrost standaryzacji stosowanych procedur, wypracowanych technik sprzedaży i prowadzonej działalności gospodarczej. Wpływa to pośrednio także na doskonalenie technik gromadzenia, przetwarzania danych i udostępniania informacji przez instytucje sektora publicznego. Odgórnie zachodzące procesy ujednolicania i homogenizacji struktur rynkowych oraz oddolnie – upowszechniania standardów technologii informatycznej, są podstawą realizowanego transnarodowo zjawiska integracji rynków, globalizacji procesów gospodarczych i technik elektronicznego udostępniania informacji w globalnej sieci Internet¹⁴.

Wzrost innowacji technologicznych elektronicznego udostępniania informacji w sektorze przedsiębiorstw i instytucji sektora publicznego znacząco wpływa na rozwój przedsiębiorczości w gospodarkach rynkowych. Niestety pod względem szeroko ujętych innowacji w produkcji i gospodarce działające w Polsce przedsiębiorstwa i podmioty sektora publicznego należą do najmniej aktywnych w Unii Europejskiej¹⁵.

Szczególnie istotną kwestią, którą należy uwzględnić przy kształtowaniu polityki gospodarczej w Polsce na kolejne lata, jest aktywizacja instytucji sekto-

¹³ M. Dutko, M. Karciarz, *Informacja w Internecie*, Wydawnictwo Naukowe PWN, Warszawa 2011, s. 31.

¹⁴ M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytet Śląski, Katowice 2015, s. 78.

¹⁵ A. Żołnierski, *Znaczenie kapitału społecznego w procesach zarządzania innowacjami*, [w:] Raport o innowacyjności gospodarki Polski w 2011 roku, T. Baczek (red.), Wydawnictwo INE PAN, Warszawa 2012, s. 36.

ra publicznego do poprawy standardów udostępniania informacji, tak aby poziom technologiczny i w zakresie bezpieczeństwa transferu danych w Internecie dorównywał standardom rozwiniętych krajów Europy Zachodniej. Znaczącym udogodnieniem w procesie doskonalenia technik elektronicznego udostępniania informacji przez podmioty sektora publicznego oraz poprawy działania instrumentów bezpieczeństwa jest możliwość realizacji tych procesów w przedsięwzięciach inwestycyjnych współfinansowanych z udziałem środków finansowych, dotacji z Unii Europejskiej. Obecnie powszechnie przyjmuje się, że w kolejnej, rozpoczętej już perspektywie finansowej przewidzianej na lata 2015–2020 kluczowe aspekty, jakie są wymieniane przy określaniu celów systemowych do osiągnięcia, tj. takich, które powinny być aktywizowane i rozwijane w polskiej gospodarce, to także innowacyjność technologiczna, rozwój gospodarki elektronicznej, cyfryzacja instytucji sektora publicznego i poprawa bezpieczeństwa transferu danych w Internecie.

Pozytywną pochodną tych procesów powinna być w kolejnych latach znacząca aktywizacja wzrostu gospodarczego, w tym poprawa sytuacji na rynku pracy w wyniku generowania nowych miejsc zatrudnienia specjalistów od bezpieczeństwa systemów teleinformatycznych, internetowych i innych obszarów IT⁶. W dalszej perspektywie, także po roku 2020, pochodną tych procesów powinna być także poprawa stanu finansów publicznych państwa. Podstawą powyżej przedstawionych celów strategicznych rozwoju gospodarki elektronicznej i społeczeństwa informacyjnego w Polsce są doświadczenia w finansowaniu technologicznych przedsięwzięć inwestycyjnych realizowanych w ramach poprzedniej perspektywy finansowania z udziałem środków finansowych UE w latach 2007–2013. Otóż na podstawie tych doświadczeń zauważono, że efektywne wykorzystanie dostępnych funduszy UE z poprzedniej perspektywy finansowej zdeterminowane było innowacyjnością i przedsiębiorczością działających już efektywnie w warunkach rynkowych podmiotów gospodarczych w Polsce.

W zakresie procesu ekonomicznej globalizacji od pewnego czasu zachodzą istotne globalnie działające zmiany we współczesnych gospodarkach, w tym także w instytucjach krajowych i samorządowych sektorów publicznych. Instytucje sektora publicznego, w tym jednostki samorządu terytorialnego, doskonałą swe funkcjonowanie także w zakresie gromadzenia, przetwarzania i udostępniania danych innym podmiotom, w tym obywatelom i przedsiębiorstwom. Sukcesywnie realizowane są procesy poprawy bezpieczeństwa transferu danych w Internecie. Procesy te realizowane są celem aktywizacji rozwoju gospodarki elektronicznej i społeczeństwa informacyjnego oraz dostosowywania procedur i technik zapew-

¹⁶ M. Dutko, M. Karciarz, *Informacja w Internecie...*, s. 58.

nienia bezpieczeństwa do standardów rozwiniętych krajów Europy Zachodniej, w tym także obowiązujących regulacji Unii Europejskiej¹⁷.

Procesy te dotyczą także działających międzynarodowo instytucji i podmiotów gospodarczych, których dynamiczny rozwój zdeterminowany jest między innymi kwestią efektywnej implementacji innowacji technologicznych w poszczególnych korporacjach, podmiotach sektora MSP i instytucjach sektora publicznego. Podstawą tych procesów jest liberalizacja przepływów kapitałowych wsparta harmonizacją przepisów prawa. Oprócz tego rozwój nowoczesnych technologii skorelowany jest z kwestią aktywizacji postępu technologicznego także w zakresie elektronicznego przetwarzania i składowania danych oraz udostępniania informacji w sieci Internet. Rozwój ten upraszcza kanały dystrybucji produktów i usług przedsiębiorstw oraz usług informacyjnych podmiotów sektora publicznego i przyczynia się do wzrostu innowacyjności, standaryzacji stosowanych procedur, wypracowanych technik dystrybucji produktów i realizowanych usług informacyjnych. Odgórnie zachodzące procesy scalania i ujednociania struktur rynkowych oraz oddolnie – aktywizacji innowacyjności technologicznej, upowszechniania standardów technologii informatycznej są podstawą zjawiska globalizacji systemów finansowych, w tym także w sektorze publicznym¹⁸.

Wykazana w ostatnich latach przewaga pozytywnych aspektów tych procesów sugeruje ich kontynuację w najbliższej przyszłości¹⁹. W zakresie głównych determinantów sprzyjających doskonaleniu technik elektronicznego transferu danych i udostępniania informacji zainteresowanym beneficjentom poprzez sieć Internet wymienia się²⁰:

- doskonalenie technik i powstające innowacje w zakresie dystrybucji produktów, usług finansowych sektora finansowego oraz usług informacyjnych instytucji sektora publicznego,
- redukcję barier proceduralnych, udogodnienia technologiczne dla klientów podmiotów gospodarczych i beneficjentów instytucji sektora publicznego, m.in. w zakresie prowadzonej działalności gospodarczej, zawierania transakcji finansowych z udziałem elektronicznej bankowości, elektronicznego rozliczania prowadzonej działalności gospodarczej z urzędami,

¹⁷ M. Wiśniewska, *Finanse w dobie kryzysu...*, s. 78.

¹⁸ S. Bukowski (red.), *Globalizacja i integracja regionalna a wzrost gospodarczy*, Wydawnictwo CeDeWu, Warszawa 2010, s. 54.

¹⁹ T.T. Kaczmarek, *Globalna gospodarka i globalny kryzys*, Wydawnictwo Difin, Warszawa 2009, s. 38.

²⁰ G. Szpor, W. Wiewiórowski, *Internet. Prawno-informatyczne problemy sieci portali i e-usług*, Wydawnictwo C.H. Beck, Warszawa 2012, s. 163.

- celowe działania wpisane w politykę społeczno-gospodarczą kraju, np. poprzez rządowe programy wspierania rozwoju krajowej i lokalnej gospodarki elektronicznej celem zwiększenia poziomu cyfryzacji działalności instytucji sektora publicznego,
- aktywizowany prorozwojową polityką społeczno-gospodarczą, postępem technicznym w zakresie informatyki i technik elektronicznego transferu danych generuje poprawę standardów współpracy i wymiany informacji między przedsiębiorstwami a instytucjami sektora publicznego, w tym jednostkami samorządowymi.

Pochodną tych procesów powinna być także aktywizacja przedsiębiorczości i innowacyjności technologicznej, co w konsekwencji powinno pozytywnie wpływać na rozwój działalności gospodarczej. W dalszej perspektywie powinno się to przełożyć na przyspieszenie tempa rozwoju gospodarczego, zwiększenie PKB i poprawę sytuacji na rynku pracy.

Wobec powyższego w niniejszym podrozdziale wskazano na znaczące rozwijające się korelacje i sprzężenia zwrotne w zakresie innowacyjności technologicznej w sektorze podmiotów gospodarczych oraz współpracy tych podmiotów z instytucjami sektora publicznego. Od początku lat 90. ubiegłego wieku wzrost gospodarczy w Polsce jest zdeterminowany głównie rozwojem przedsiębiorczości, komercjalizacją procesów gospodarczych, implementacją nowoczesnych rozwiązań technologicznych, dostosowywaniem standardów proceduralnych do uregulowań normatywnych Unii Europejskiej. Znaczący jest w tym zakresie udział kreatywności i innowacyjności działających w Polsce podmiotów gospodarczych oraz funkcjonujących w ujęciu lokalnym i krajowym podmiotów sektora publicznego, w tym samorządowych. Tych pozytywnych tendencji w poważnym stopniu nie zakłócił nawet niedawny globalny kryzys finansowy. Ponadto poziom innowacyjności technologicznej w Polsce jest jeszcze znacząco niższy w kontekście standardów krajów wysokorozwiniętych²¹. W związku z tym istnieje w polityce społeczno-gospodarczej potrzeba dalszego systemowego inspirowania do tworzenia innowacji technologicznych powstających w przedsiębiorstwach i ich implementacji w instytucjach sektora publicznego. Przełoży się to na poprawę gospodarki finansowej tych podmiotów, a tym samym także proces ten może być istotnym czynnikiem poprawy finansów instytucji publicznych, także jednostek samorządowych, niektórych już wysoko zadłużonych. Poza tym na tle tego procesu powinny także rozwijać się korelacje i sprzężenia zwrotne poprawiających współpracę podmiotów gospodarczych z instytucjami sektora publicznego.

²¹ A. Borcuch, *Bankowość elektroniczna w Polsce*, wydanie II zmienione, Wydawnictwo CeDeWu, Warszawa 2012, s. 92.

3. Wzrost ryzyka utraty danych w systemach elektronicznego składowania i transferu informacji niejawnych

Niestety w warunkach polskich niewiele jest zweryfikowanych i potwierdzonych przez określone instytucje danych ilościowych w zakresie skutecznych ataków hakerskich dokonywanych na systemy informatyczne innych podmiotów poprzez Internet. P. Wróbel podaje, że kwestia odpowiedzialności prawej związanej z problematyką bezpieczeństwa systemów informatycznych i zawartych w nich zasobów informacyjnych została już znacząco opisana przez badaczy amerykańskich. Natomiast w Polsce problematyka ta nadal jest w niewielkim stopniu podejmowana w badaniach, z czym wiąże się ograniczony zasób danych analitycznych²².

Na podstawie przeprowadzonych w krajach zachodnich badań wykazano relatywnie wysoki poziom „nieszczelności” informacyjnej systemów teleinformatycznych. Według raportu Websense Research z 2011 roku, sporządzonego na podstawie przebadania dwóch tysięcy różnego typu podmiotów gospodarczych i instytucji działających w USA, Kanadzie, Wielkiej Brytanii i Australii zatrudniających minimum 250 użytkowników komputerów, w okresie jednego roku doszło do wielu niepokojących zdarzeń, które sugerować mogą istnienie wielu luk w systemach bezpieczeństwa oraz błędnie opracowanych procedur. Otóż w 37% spośród przebadanych podmiotów pracownik przyczynił się do utraty określonych informacji niejawnych oraz danych, co mogło doprowadzić lub doprowadziło do wystąpienia niekorzystnych dla funkcjonowania danego podmiotu zdarzeń.

W 20% spośród przebadanych organizacji informacje niejawne zostały świadomie przez zatrudnionych pracowników w sposób nieuprawniony skopiowane i wyniesione, wykradzione z wewnętrznych systemów informatycznych firm i instytucji. Także w 20% badanych podmiotów dane niejawne trafiły do internetowych portali społecznościowych. Poza tym w 35% przebadanych podmiotów w ich wewnętrznych systemach informatycznych pojawiły się „konie trojańskie”, złośliwe programy typu *malware* lub innego rodzaju wirusy²³.

Dynamiczny rozwój usług internetowych przyspieszył proces informacyjnej globalizacji, ale również stworzył szersze pole dla działania hakerów oraz organizacji terrorystycznych. Codziennie w ujęciu globalnym powstaje wiele nowych wirusów, które niejednokrotnie zdolne są atakować systemy informatyczne wielu

²² P. Wróbel, *Komunikacja elektroniczna. Zagrożenia i ich skutki dla organizacji*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2014, s. 186–187.

²³ Websense Research Report, 2011, s. 11 (www.websense.com).

firm, instytucji publicznych, banków oraz komputery użytkowników domowych. Poza tym także codziennie tworzone są nowe zabezpieczenia dla atakowanych systemów informatycznych. Tego typu rywalizacja nie zawsze przyjmuje formę gry z wynikiem zerowym. Obecnie przyjmuje się, że funkcjonujące w Unii Europejskiej normatywy prawne nie są w pełni adekwatne względem panujących standardów cyfryzacji urzędów i przedsiębiorstw oraz tworzonej przez te podmioty infrastruktury newralgicznych gałęzi w gospodarce narodowej. Do tego typu szczególnie zagrożonych atakiem ze strony cyberterrorystów gałęzi w gospodarce zalicza się:

- energetykę;
- transport;
- centra zarządzania kryzysowego;
- urzędy;
- system finansowy²⁴.

W związku z kryzysem imigracyjnym w Europie i wojną w Syrii w mediach europejskich przeważają relacje sugerujące, że za zamachami stoją obecnie głównie fundamentaliści islamscy. Jednak w ujęciu globalnym źródła zamachów terrorystycznych są jednak bardziej zróżnicowane, biorąc pod uwagę narodowość, kulturę i religię sprawców zamachów. Ponieważ terroryzm coraz częściej dotyczy globalnego medium, jakim jest Internet, a zjawisko cyberterrorizmu może wyrządzić nie mniejsze negatywne skutki niż „tradycyjne” akty terroru, więc globalne ujęcie tej problematyki jest także istotne. Analizy dotyczące globalnego ujęcia terroryzmu wskazują, że fundamentalizm islamski może być związany jedynie z co piątym zamachem terrorystycznym dokonywanym w ostatnich miesiącach. Poza fundamentalizmem islamskim nadal zamachy terrorystyczne są dokonywane przez różnego typu organizacje neonazistowskie, skrajnie lewicowe, grupy separatystyczne oraz fundamentalistyczne związane z różnymi nurtami religijnymi.

Podczas Forum Bezpieczeństwa Banków, które odbyło się 10 maja 2016 roku w Warszawie, dr Krzysztof Cieślak, ekspert Centrum Badań nad Terroryzmem Collegium Civitas, wskazywał, że cyberterrorizm, który na celownik obrał sektor finansowy, nie musi ograniczać się już jedynie do włamań hakerskich na konta klientów banków. Zagrożenia ze strony cyberterrorizmu względem banków mogą przybierać inny charakter. Dotychczas funkcjonujące w strukturach odpowiednich służb publicznych zespoły powoływane celem bieżącego monitoringu potencjalnych zagrożeń, w tym zespoły ds. zarządzania kryzysowego, w ostatnich latach zmieniają charakter procesu kontroli i zarządzania potencjalnymi

²⁴ A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wydawnictwo Wolters Kluwer Polska, Warszawa 2010, s. 19–20.

zagrożeniami. Dotychczasowe zagrożenia wywoływane siłami natury, awarie instalacji energetycznych, wodociągowych i innych ustępują miejsca względem potencjalnych zagrożeń terrorystycznych lub nawet cyberterrorystycznych²⁵.

Według Dariusza Wojtasa, project managera zajmującego się aplikacjami oferowanymi przez IMPAQ Sp. z o.o. dla banków komercyjnych, ataki hakerskie w ostatnich latach nasilają się także w Polsce. Obecnie licealista potrafiący tworzyć i konfigurować strony internetowe ma możliwość stworzenia programów hakerskich, które będą o tyle skuteczne jako narzędzia ataku na systemy elektronicznej bankowości, o ile zostaną rozpowszechnione wśród użytkowników sieci Internet²⁶. Do stworzenia złośliwego lub szpiegującego oprogramowania nie trzeba już dysponować zaawansowaną wiedzą informatyczną i wyrafinowaną technologią. Kluczową kwestią z punktu widzenia działalności hakerów jest dystrybucja stworzonych programów typu *malware*²⁷.

Banki komercyjne, celem ograniczenia ryzyka podatności na tego typu ataki, zmuszone zostają do bezustannego monitorowania dokonywanych w ich systemach operacji finansowych, permanentnego doskonalenia posiadanych systemów informatycznych oraz informowania klientów o nowych technikach ataków hakerskich wymierzonych bezpośrednio w wewnętrzne teleinformatyczne systemy bankowe oraz w komputery lub urządzenia mobilne klientów banków. Edukowanie klientów obecnie dotyczy głównie wskazania na potencjalne zagrożenia wynikające z możliwości zainfekowania komputera oprogramowaniem stworzonym przez hakerów, dystrybuowanym poprzez technikę *fishingu* celem przejęcia kontroli nad systemem elektronicznej bankowości internetowej z poziomu platformy transakcyjnej klienta banku²⁸.

Jedną z najpopularniejszych w ostatnich latach technik *fishingowych* jest rozsyłanie w załącznikach e-maili plików, które pozornie wyglądają jak zdjęcia, dokumenty w plikach wordowych lub PDF-ach, a w rzeczywistości zawierają spreparowane przez hakerów ukryte programy szpiegujące lub wirusy przejmujące kontrolę nad internetowym rachunkiem klienta banku. Zdarzały się sytuacje, że do skrzynek mailowych klientów banków wpadały maile od dostawców usług, np. energii elektrycznej, informujące o zbliżającym się terminie płatności, do

²⁵ K. Machowski, *Hakerzy i terroryści, czyli kto zagraża współczesnym bankom* [w:] „Bank. Miesięcznik Finansowy”, nr 6 (278), czerwiec 2016, s. 14.

²⁶ K.J. Móraski, *Zarządzanie informacją skutecznym sposobem na fraudy* [w:] „Bank. Miesięcznik Finansowy”, temat numeru: „Bezpieczeństwo banków”, nr 4 (265), kwiecień 2015, s. 50.

²⁷ M. Górka (red.), *Cyberbezpieczeństwo jako podstawa...*, s. 64.

²⁸ J. Gąsiorowski, P. Podsiadlik, *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Wydawnictwo Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015, s. 75.

których załączone formularze rachunków w postaci plików PDF zawierały ukryte programy szpiegujące. Kliknięcie na taki plik PDF w celu otwarcia dokumentu powodował uruchomienie programu szpiegującego i zawirusowanie komputera użytkownika, który coraz częściej jest także klientem bankowości elektronicznej²⁹. Hakerski program szpiegujący działa „w tle” operacji wykonywanych przez użytkownika komputera, w trybie ukrytym, tj. w taki sposób, aby użytkownik elektronicznej bankowości internetowej nie zorientował się, że program ten umożliwił hakerowi dostęp do konta bankowego. Inną wersją programów hakerskich typu *malware* są działające „w tle” wirusy, które po zainfekowaniu komputera użytkownika bankowości internetowej przeprowadzają transakcje finansowe w imieniu klienta banku, do którego konta bankowego uzyskiwały dostęp.

Do jednych z popularniejszych hakerskich technik wykradania informacji niejawnych i nieupoważnionej ingerencji w systemy bankowości elektronicznej należą odmiany *fishingu* bazujące na technikach spamowych, tj. rozsyłania wiadomości spamowych kierowanych do dużej liczby potencjalnych odbiorców, użytkowników Internetu korzystających z poczty elektronicznej. W ostatnich latach odnotowuje się tendencję wzrostową ilości spamu trafiającego do skrzynek mailowych użytkowników Internetu, którzy przeglądają prywatną pocztę zwykle na komputerach domowych lub coraz częściej także na urządzeniach mobilnych typu smartfony i tablety.

Rosnąca ilość spamu rozsyłanego w sieci Internet polega zwykle na wysłaniu ograniczonej ilości spamu na możliwie największą liczbę adresów IP, tj. według formuły tzw. *snow-shoe spam*, tak aby zmniejszyć prawdopodobieństwo odfiltrowania tych spamowych maili przez antyspamowe programy zabezpieczające komunikację mailową. Hakerzy rozsyłają programy szpiegujące, których zadaniem jest m.in. uzyskanie dostępu do jak największej liczby kont pocztowych. Złamanie haseł dostępu do kont pocztowych części użytkowników Internetu pozwala hakerom na zdobycie adresów mailowych wielokrotnie większej liczby użytkowników globalnej sieci. W sytuacji posiadania milionów adresów mailowych hakerzy już jako spamery rozsyłają maile spamowe. Dostawcy oprogramowania pocztowego i antywirusowego stale udoskonalają aplikacje antyspamowe.

W odpowiedzi na te udoskonalenia mające za zadanie podnoszenie poziomu bezpieczeństwa komunikacji mailowej spamery tworzą wiele wersji tych samych wiadomości spamowych. W 2015 roku zdarzały się sytuacje, że spamery tworzyli nawet do 95 różnych wersji tych samych wiadomości spamowych, tj. maili zawierających spam tej samej treści, ale w mailach różniących się np. tematem

²⁹ T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Wydawnictwo Eneteia, Warszawa 2013, s. 47.

wiadomości lub formatem załączonego pliku³⁰. Celem zwiększenia skuteczności włamywania się spamerów do kolejnych kont pocztowych oraz przejmowania haseł dostępu do kont zakładanych na portalach dostawców różnych usług internetowych wykorzystywane są luki systemowe odnajdywane w przeglądarkach internetowych powszechnie stosowanych przez internautów. W 2015 roku w skali globalnej najbardziej podatne na skuteczne ataki hakerskie były przeglądarki Adobe oraz Internet Explorer. Otóż aż 31% zarejestrowanych ataków dotyczyło przeglądarek Internet Explorer oraz 19% marki Adobe³¹. W związku z tym standardem stosowanym już od wielu lat przez znaczną część banków jest brak możliwości udostępniania usług bankowości elektronicznej w sytuacji zdalnego kontaktowania się klienta z bankiem za pomocą przeglądarki Internet Explorer.

W wyniku sukcesywnie postępującego udoskonalania bankowych systemów informatycznych działalność hakerów starających się przejąć kontrolę nad kontami klientów banków zmienia swój charakter. W ostatnich latach ataki hakerskie nie są głównie kierowane na bankowe systemy informatyczne, ponieważ one są zwykle zabezpieczone wielopoziomowo i z zastosowaniem najnowszych technologicznych rozwiązań w zakresie bezpieczeństwa. Zamiast bezpośrednich ataków na informatyczne systemy bankowe cyberprzestępcy relatywnie zwiększają swe zaangażowanie w zakresie prób ingerencji w stacjonarnych lub przenośnych urządzeniach informatycznych klientów banków, ponieważ zwykle komputery domowe oraz prywatne smartfony i tablety są najslabiej zabezpieczone. Coraz popularniejszą techniką w tym zakresie jest zawirusowywanie urządzeń z dostępem do Internetu złośliwym oprogramowaniem typu *malware*. Użytkownik sieci Internet, nie zauważając pojawienia się w komputerze lub smartfonie programów szpiegujących, uaktywnia je poprzez np. otwieranie maili zawierających niezamawiane oferty różnych firm. Cyberprzestępcy zwiększają prawdopodobieństwo skutecznego ataku, tworząc m.in. złośliwe programy *malware* atakujące najbardziej popularne globalnie systemy operacyjne zainstalowane w domowych komputerach i innych urządzeniach wyposażonych w dostęp do Internetu. Prawdopodobieństwo to dodatkowo zwiększa się, jeżeli użytkownicy Internetu nie aktualizują na bieżąco zainstalowanego oprogramowania, a szczególnie systemu operacyjnego i programów antywirusowych³².

Od kilku lat nasilają się ataki hakerskie w formie *malvertising*, tj. infekowanie złośliwym oprogramowaniem rozsyłanych w Internecie reklam. Nazwa *malvertising* powstała z połączenia słów *malicious advertising*, co oznacza złośliwą

³⁰ J. Kosiński, *Paradygmaty cyberprzestępczości*, Wydawnictwo Difin, Warszawa 2015, s. 142.

³¹ A. Król, *Cybernetyczna siła*, „Bank. Miesięcznik Finansowy”, temat numeru: „Bezpieczeństwo banków”, nr 4 (265), kwiecień 2015, s. 38.

³² M. Górka (red.), *Cyberbezpieczeństwo jako podstawa...*, s. 131.

reklamę, tj. sytuację, kiedy do skrzynki mailowej trafiają maile z reklamami zainfekowane złośliwym programem, który zawierać może program wykorzystujący luki w przeglądarkach internetowych. W momencie otwarcia takiego maila z reklamą uaktywnia się program *malware*, który poprzez luki w przeglądarce otwiera dostęp do bankowości elektronicznej użytkownika danego komputera. Niekiedy uaktywnienie programu infekującego nie wymaga nawet kliknięcia myszką, ponieważ samo najechanie wskaźnikiem myszki na dany plik czy grafikę z reklamą powoduje uwolnienie programu *malware*. Cyberprzestępcy łączą technikę *malvertisingu* z socjotechniką. Przykładem jest sytuacja, gdy etap rozsyłania zainfekowanych reklam poprzedzony jest rozsyłaniem reklam niezainfekowanych, tak aby stworzyć poczucie zaufania użytkowników Internetu względem reklamowego spamu.

Z danych analityków badających stosowane przez cyberprzestępców metody nieupoważnionej ingerencji w komputery i systemy informatyczne innych użytkowników Internetu, firm i instytucji wynika, że liczba tych metod nadal rośnie. Wśród tych metod nadal są stosowane „stare”, znane już sprzed kilkunastu i więcej lat, jak np. ataki, których efektem jest odmowa dla użytkownika w systemie dostępu do usługi, tj. tzw. DoS (z ang. *Denial of Service*). Ataki hakerskie tego typu należą do metod paraliżowania infrastruktury sieci komputerowych w firmach i instytucjach oraz ograniczania dostępu do określonych aplikacji w komputerach domowych³³. Oprócz tego nadal generowane są także nowe metody infekowania komputerów złośliwym oprogramowaniem. Wśród tych najnowszych wymienia się np. rozsyłanie programów *malware* poprzez wymuszanie w komputerach użytkowników Internetu instalowania lub uruchamiania aktualizacji programu antywirusowego, który to antywirus jest oprogramowaniem fałszywym, stworzonym na podobieństwo innych stosowanych przez znaczną część użytkowników globalnej sieci. Otóż w znacznej części komputerów osobistych są instalowane darmowe, dostępne w Internecie do pobrania programy antywirusowe³⁴.

Niektórzy użytkownicy urządzeń z dostępem do Internetu ułatwiają cyberprzestępcom opanowanie użytkowanego sprzętu informatycznego, nie instalując żadnych dodatkowych antywirusów i firewallów, ufając tylko tym, które stanowią integralne części systemów operacyjnych. Obecnie liczba urządzeń z dostępem do Internetu sukcesywnie rośnie i nie tylko jest to związane z rozwojem rynku komputerów stacjonarnych i przenośnych, tj. laptopów, palmtopów i notebooków. Stale postępuje miniaturyzacja i łączenie funkcji różnych urządzeń

³³ A. Król, *Cybernetyczna siła...*, s. 38.

³⁴ T. Trejderowski, *Kradzież tożsamości...*, s. 51.

mobilnych, co w ostatnich kilku latach szczególnie zauważalne było w ewolucji poszczególnych generacji smartfonów. Poza tym rośnie także rynek innych urządzeń typowych dla wyposażenia gospodarstw domowych, jak np. inteligentne, tj. wyposażone w mikroprocesory i dodatkowe funkcje informacyjne i komunikacyjne, telewizory i lodówki. Te urządzenia mogą być także celem ataków hakerskich, szczególnie w sytuacji, gdy zainstalowane w nich systemy operacyjne nie zostały w pełni udoskonalone w kwestii zabezpieczeń lub użytkownicy nieświadomi problemu użytkują te urządzenia bez zachowania minimalnych standardów bezpieczeństwa³⁵. Niekiedy tego typu nowinki technologiczne wyprzedzają rozwój odpowiednich metod i programów antywirusowych.

4. Zakończenie

Przeprowadzona w Polsce w latach 90. ubiegłego wieku odbudowa rynku finansowego była istotnym czynnikiem w kontekście efektywnego rozwoju gospodarki rynkowej w Polsce. Rozwój internetowej bankowości elektronicznej determinuje potrzebę ciągłego dopracowywania regulacji kształtujących bezpieczeństwo elektronicznego transferu danych i ochrony danych osobowych. W sytuacji szybko rosnącej liczby użytkowników bankowych systemów elektronicznej bankowości rośnie na znaczeniu kwestia poprawy funkcjonowania systemów informatycznych w zakresie bezpieczeństwa dokonywanych transakcji, analizy podejmowanego ryzyka i ponoszenia kosztów na tworzenie systemowych rozwiązań utrzymania wysokiego poziomu bezpieczeństwa i ochrony danych niejawnych. Problematyka poprawy systemowych rozwiązań bezpieczeństwa jest szczególnie istotna w sytuacji nagminnie pojawiających się ataków hakerskich na systemy internetowej bankowości elektronicznej.

W związku ze wzrostem transnarodowych przepływów kapitałowych i wymiany handlowej rośnie także udział transakcji finansowych rozliczanych elektronicznie. Poza tym w związku z tym, że Polska jest członkiem Unii Europejskiej, polskie regulacje odnośnie do bezpieczeństwa elektronicznego transferu danych i ochrony informacji niejawnych są dostosowywane do normatywnych standardów unijnych. Proces ten jest także zaliczany do składowych doskonalenia zewnętrznych regulacji prawnych i wiązany z obecnie postępującą globalizacją systemów finansowych³⁶.

³⁵ M. Górka (red.), *Cyberbezpieczeństwo jako podstawa...*, s. 164.

³⁶ J. Kosiński, *Paradygmaty cyberprzestępczości...*, s. 143.

Dokonująca się globalizacja ekonomiczna i w związku z tym stale rosnące powiązania polskiej gospodarki ze światem powodują, że doskonalenie krajowych regulacji prawnych dotyczących utrzymania określonego poziomu bezpieczeństwa systemów informatycznych i ochrony danych niejawnych odbywa się, między innymi, jako proces dostosowywania polskiej legislacji do regulacji Unii Europejskiej. Nie jest to jednak czynnikiem zapewniającym pełną adekwatność dostosowania normatywów prawnych względem dynamicznie rozwijającej się oferty bankowości elektronicznej instytucji finansowych, jak i usług ze strony firm internetowych³⁷. Obecnie przyjmuje się, że obowiązujące regulacje prawne zapewniają jedynie najbardziej elementarny poziom ochrony danych niejawnych podczas realizacji określonych zamówień handlowych i transakcji finansowych, jednak mogą być niewystarczające wobec dokonującego się bezustannie postępu technologii teleinformatycznej wykorzystywanej poprzez dostawców usług internetowych, a szczególnie firm oferujących zwykle bezkosztowe korzystanie z portali społecznościowych.

Wobec dokonującego się procesu cyfryzacji firm, urzędów i instytucji obecnie przyjmuje się, że zgodnie z potrzebami większości użytkowników Internetu ochrona danych osobowych jest tą dziedziną egzystencji ludzi, która powinna być zapewniona przez podmioty działające w Internecie. Zgodnie z treścią zapisów Konstytucji ochrona danych osobowych jest jednym z elementarnych praw każdego obywatela, a więc także użytkownika Internetu. Dokonujący się bezustannie postęp technologiczny w zakresie oferty usług firm internetowych spowodował po stronie użytkowników Internetu częściową erozję realnego działania tego prawa³⁸. Dzieje się tak, ponieważ albo użytkownicy Internetu nie mają pełniej świadomości budowanych awatarów w hurtowniach danych koncernów internetowych, albo nowe technologie teleinformatyczne nie pozwalają już na zachowanie pełnej prywatności obywateli funkcjonujących w społeczeństwach informacyjnych. Wspomniane powyżej koncerny internetowe, takie jak Google, Facebook, Twitter, Instagram i YouTube, codziennie zbierają kolejne dane o użytkownikach ich portali społecznościowych, bezustannie rozbudowują informacyjnie istniejące już awatary, tj. elektroniczne odpowiedniki poszczególnych obywateli, użytkowników Internetu. W jaki sposób i kiedy będą te dane wykorzystane, oprócz obecnej działalności reklamowej tych koncernów, tego niestety użytkownicy Internetu nie wiedzą. Nie mogą tego wiedzieć, jeżeli nawet te właśnie firmy, internetowe koncerny będące właścicielami portali społeczno-

³⁷ M. Dutko, M. Karciarz, *Informacja w Internecie...*, s. 87.

³⁸ A. Gałach, A. Jędruszczak, B. Nowakowski, *Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 127.

ściowych, także nie wiedzą, do czego te bezustannie rozbudowywane informacje, gromadzone w hurtowniach danych, wykorzystają za 10 lat.

Bibliografia

Literatura:

- Borcuch A., *Bankowość elektroniczna w Polsce*, wydanie II zmienione, Wydawnictwo CeDeWu, Warszawa 2012.
- Bukowski S. (red.), *Globalizacja i integracja regionalna a wzrost gospodarczy*, Wydawnictwo CeDeWu, Warszawa 2010.
- Dolecki S., *Brutalna cyberzeczywistość*, „Bank. Miesięcznik finansowy”, raport specjalny „Cyberbezpieczeństwo”, nr 4/276, Warszawa 2016.
- Domańska-Szaruga B., *Common banking supervision within the financial safety net*, [w:] *The Economic Security of Business Transactions. Management in business*, Wydawnictwo Chartridge Books Oxford, Oxford 2013.
- Domańska-Szaruga B., *Financial Instability and the New Architecture of Financial Supervision in European Union*, [w:] B. Domańska-Szaruga, T. Stefaniuk (red.), *Organization in changing environment. Conditions, methods and management practices*, Wydawnictwo Studio Emka, Warszawa 2014.
- Dutko M., Karciarz M., *Informacja w Internecie*, Wydawnictwo Naukowe PWN, Warszawa 2011.
- Gałąch A., Jędruszczak A., Nowakowski B., *Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym*, Wydawnictwo C.H. Beck, Warszawa 2013.
- Gołębiowska A., *Local government in the Constitution of the Republic of Poland of 1997*, „Ius Novum”, nr 2 (2015).
- Gąsiorowski J., Podsiadlik P., *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej*, Wydawnictwo Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza 2015.
- Górka M. (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa 2014.
- Gwoździewicz, S., *The European Union Towards the Threats in Cyberspace*, *International Scientific Journal „Verejna Sprava a Spolocnost”*, Rocznik XV, No 2/2014, Słowacja, Koszyce 2014.
- Hołyst P., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologii*, „Prokuratura i Prawo”, nr 1/2011.
- Kaczmarek T.T., *Globalna gospodarka i globalny kryzys*, Wydawnictwo Difin, Warszawa 2009.
- Kosiński J., *Paradygmaty cyberprzestępczości*, Wydawnictwo Difin, Warszawa 2015.
- Krasuski A., *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy*, Wydawnictwo Wolters Kluwer, Warszawa 2012.
- Król A., *Cybernetyczna siła*, „Bank. Miesięcznik Finansowy”, temat numeru: „Bezpieczeństwo banków”, nr 4 (265), kwiecień 2015.

- Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytet Śląski, Katowice 2015.
- Machowski K., *Hakerzy i terroryści, czyli kto zagraża współczesnym bankom*, „Bank. Miesięcznik Finansowy”, nr 6 (278), czerwiec 2016.
- Mórawski K.J., *Zarządzanie informacją skutecznym sposobem na fraudy*, „Bank. Miesięcznik Finansowy”, temat numeru: „Bezpieczeństwo banków”, nr 4 (265), kwiecień 2015.
- Muchacki M., *Cywilizacja informatyczna i Internet. Konteksty współczesnego konsumenta TI*, Wydawnictwo Impuls, Warszawa 2014.
- Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wydawnictwo Wolters Kluwer Polska, Warszawa 2010.
- Szpor G., Wiewiórowski W., *Internet. Prawno-informatyczne problemy sieci portali i e-usług*, Wydawnictwo C.H. Beck, Warszawa 2012.
- Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny*, Wydawnictwo Eneteia, Warszawa 2013.
- Websense Research Report, 2011 (www.websense.com).
- Wiśniewska M., *Finanse w dobie kryzysu*, Seria „Prace Naukowe Wyższej Szkoły Bankowej w Gdańsku”, Wydawnictwo CeDeWu, Warszawa 2013.
- Wociór D. (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Wydawnictwo C.H. Beck, Warszawa 2016.
- Wróbel P., *Komunikacja elektroniczna. Zagrożenia i ich skutki dla organizacji*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2014.
- Żołnierski A., *Znaczenie kapitału społecznego w procesach zarządzania innowacjami*, [w:] Raport o innowacyjności gospodarki Polski w 2011 roku, T. Baczko (red.), Wydawnictwo INE PAN, Warszawa 2012.

Streszczenie

Procesy globalizacyjne i postęp technologiczny przyniosły nowe wyzwania dla ochrony, elektronicznego przesyłania i przetwarzania danych, w tym informacji niejawnych. Rozwój technik udostępniania informacji poprzez Internet zdeterminowany jest przede wszystkim wieloma udogodnieniami dla beneficjentów, klientów i osób korzystających z usług informacyjnych oferowanych przez firmy, instytucje finansowe i publiczne. Natomiast dla podmiotów udostępniających elektronicznie informacje poprzez Internet pojawia się możliwość znaczącej redukcji kosztów transakcyjnych przeprowadzanych operacji finansowych oraz elektronicznego transferu danych. Występują jednak także negatywne aspekty elektronicznego transferu danych w Internecie. Z rozwojem technologii informacyjnych funkcjonujących w Internecie wiąże się bowiem także ryzyko utraty lub kradzieży informacji przez podmioty nieuprawnione.

Proces udostępniania informacji poprzez Internet generuje także wiele zagrożeń związanych z przestępstwami kradzieży tożsamości, elektronicznego przechwytywania przez hakerów danych niejawnych oraz dokonywania malwersacji środków pieniężnych w systemach elektronicznej bankowości. Celem ograniczenia ryzyka utraty danych oraz innych zagrożeń elektronicznego transferu danych niejawnych poszczególne podmioty, w tym instytucje sektora publicznego, rozbudowują systemy bezpieczeństwa zdalnego udostępniania informacji oraz dokonywanych transakcji realizowanych za pośrednictwem Internetu. Bezustannie dokonuje się kontynuacja procesu doskonalenia technik zapewniających określony poziom bezpieczeństwa internetowego transferu danych. Stale doskonalone są procedury bezpiecznego przetwarzania, składowania i udostępniania informacji. W kontekście rozwoju teleinformatycznych technologii informacyjnych rośnie znaczenie doskonalenia technik bezpiecznego transferu danych niejawnych w sieci Internet, w tym przede wszystkim danych osobowych.

Słowa kluczowe: udostępnianie informacji, bezpieczeństwo w cyberprzestrzeni, bezpieczeństwo transferu danych, sektor publiczny, Internet, bezpieczeństwo usług bankowych, bankowość internetowa, ochrona danych osobowych.

Summary

Determinants of security electronic transfer of personal data on the Internet in Poland

The processes of globalization and technological advances have brought new challenges for the protection of electronic transmission and processing of data, including classified information. The development of techniques for sharing information through the Internet is determined primarily convenient for beneficiaries, clients and beneficiaries of information services offered by companies, financial institutions and public. But for providers of electronic information through the Internet there is the possibility of a significant reduction in transaction costs of the operations of financial and electronic data transfer. However, there are also negative aspects of the electronic transfer of data on the Internet. On the other hand, the development of information technology operating on the Internet involves the risk of loss or theft of information by unauthorized entities.

The process of sharing information through the Internet also generates a lot of risks associated with the crime of identity theft, electronic interception by hackers classified data and making the embezzlement of funds in the system of electronic banking. To mitigate the risk of data loss and other threats to electronic transfer of classified data the individual entities in the public sector is developing safety systems for remote sharing of information and of transactions carried out via the Internet. Constantly made the continuation of the process improvement techniques to ensure a certain level of security online data transfer. Continually improved procedures for safe handling, storage and sharing of information. In the context of the development of ICT information technology is becoming increasingly important to improve techniques for the safe transfer of classified data on the Internet, including in particular personal data.

Key words: sharing of information, security in cyberspace, security, data transfer, the public sector, the Internet, online banking, personal data protection.

Słowo wstępne

W dniu 12 grudnia 2016 roku w Senacie Rzeczypospolitej Polskiej odbyła się ogólnopolska konferencja naukowa pod tytułem *Rola administracji publicznej w systemie bezpieczeństwa państwa*. Jej organizatorem była Komisja Samorządu Terytorialnego i Administracji Państwowej Senatu Rzeczypospolitej Polskiej we współpracy z Zakładem Prawa Wydziału Inżynierii Bezpieczeństwa Cywilnego Szkoły Głównej Służby Pożarniczej w Warszawie.

Celem konferencji była refleksja na temat prawnych, organizacyjnych oraz społecznych aspektów konsekwencji wynikających z roli, jaką pełni administracja publiczna w systemie bezpieczeństwa państwa.

Ogólnopolska konferencja naukowa pod tytułem *Rola administracji publicznej w systemie bezpieczeństwa państwa* skupiła wybitnych ekspertów z czołowych ośrodków naukowych, m.in. Uniwersytetu Jagiellońskiego, Uniwersytetu Kardynała Stefana Wyszyńskiego, Politechniki Warszawskiej, Szkoły Głównej Służby Pożarniczej w Warszawie i Uniwersytetu Jana Kochanowskiego.

Konferencja stała się platformą do wymiany poglądów na temat przyszłych konsekwencji dotyczących roli administracji publicznej w systemie bezpieczeństwa państwa. Wystąpieniom prelegentów towarzyszyła ożywiona dyskusja, stanowiąca idealny przyczynek do dalszych rozważań nad tytułową problematyką.

Zagadnieniem fundamentalnym w demokratycznym państwie prawnym jest sprawne i legalne działanie administracji publicznej. Sprawność i legalność są pojęciami wywodzącymi się z dwóch różnych dyscyplin. Sprawność działania związana jest z naukami o zarządzaniu, natomiast legalność nierozzerwalnie łączy się z naukami prawnymi. Niemniej jednak istnieje wiele płaszczyzn, w ramach których oba te pojęcia mogą, a nawet powinny być rozpatrywane razem. Taką płaszczyzną jest kwestia funkcjonowania administracji publicznej, ponieważ wszelkie dziedziny administrowania państwem wymagają podejmowania działań, które będą skuteczne, ekonomiczne, a także korzystne ze społecznego punktu widzenia, czyli będą posiadały atrybut sprawności.

Prof. nzw. dr hab. Anna Gołębiowska
Dr Piotr Benedykt Zientarski

Głosy w dyskusji
na temat roli administracji publicznej
w systemie bezpieczeństwa państwa
podczas konferencji zorganizowanej przez
Komisję Samorządu Terytorialnego
i Administracji Państwowej Senatu RP
we współpracy z Wydziałem Inżynierii
Bezpieczeństwa Cywilnego Szkoły Głównej
Służby Pożarniczej w Warszawie
w dniu 12 grudnia 2016 r.

Mirosław Wawrzyński

Odniosę się do jednego aspektu: podczas konferencji jeden z referentów mówił o przyszłości i pewnych sprawach, które jej dotyczą. Niestety, w jego wypowiedzi nic nie było na temat wyzwań przyszłości. W związku z tym chciałem zwrócić uwagę na trzy istotne elementy, które w najbliższym czasie będą nas dotyczyły.

Pierwszy to jest generalnie duży spadek populacji Polski. W okresie 30–40 lat z naszego kraju zniknie około 3–4 milionów osób. W tej chwili już znikło 2 miliony, które wyjechały za pracę. Skorelowany z tym jest wzrost średniej mediany wieku, czyli w populacji będzie więcej ludzi starszych, w okresie najbliższych 30–40 lat będzie mieszkać w Polsce więcej osób starszych, mniej młodzieży. Ma to bezpośredni wpływ na zapewnienie bezpieczeństwa, bo trudno mi sobie wyobrazić strażaka, który pełni służbę i jest wydolny w wieku 60–70 lat.

Druga sprawa, która bezpośrednio wiąże się z ryzykiem dotyczącym bezpieczeństwa, to fakt, że w tej chwili mamy do czynienia z trendem przyrostu masy ciała, czyli coraz więcej ludzi młodych, również osób w wieku średnim i dorosłym, jest otyła, ma otyłość, nadwagę. Chcę państwu uzmysłowić, że coraz więcej osób jest też słabych fizycznie, zwłaszcza młodych, są po prostu wiotcy. Nie można oczekiwać, że bezpieczeństwo zapewnią ludzie, którzy nie potrafią przebiec nawet krótkiego dystansu lub wejść na czwarte piętro. Różnego rodzaju badania pokazują, że w Warszawie ludzie młodzi mają problemy z wejściem o własnych siłach na czwarte piętro.

Trzecia rzecz. Bardzo mnie czasami dziwi, że mówimy o bezpieczeństwie, zakładając, że może ono powstać jako analiza różnych badań wynikających z analizy średniej krzywej Gaussa. Są takie zjawiska jak „czarne łabędzie”. Pan przewodniczący, senator mówił o tym, że miał do czynienia ze zdarzeniami, które w ogóle nie sądził, że się wydarzą. Co kilkadziesiąt lat pojawiają się niespodziewane zdarzenia. Przykład: 1997 rok – wielka powódź. Kilka lat później była ogromna susza, która spustoszyła duże obszary Europy, w tym Polski. Doszło do zanieczyszczenia różnego rodzaju gazami olbrzymich obszarów. Tego rodzaju zdarzenia zwane czarnymi łabędziami są często pomijane i nieanalizowane w ekspertyzach. Niestety do nich dochodzi i system musi być przygotowany na pojawienie się tego typu niespodziewanych zdarzeń. My sobie popatrzymy na krzywej osi, matrycę sobie zbudujemy, a potem się dziwimy, że pojawia się gigantyczna powódź raz na stulecie albo gigantyczna susza, co było notowane.

Dr Marek Woch

Moim zdaniem dzisiaj, jeżeli nie zaczniemy mówić w kategoriach właśnie bezpieczeństwa zdrowotnego, narodowego, to my nie znajdziemy rozwiązania. Dlaczego? Kwestia zaczyna się już na poziomie terminologii. Ja będę mówił jako dogmatyk prawa i filozof prawa, bo takie mam stopnie. Sam system ochrony zdrowia jest często mylony z systemem opieki zdrowotnej. System opieki zdrowotnej jest węższą formą systemu ochrony zdrowia i zazwyczaj jest osadzony tylko *stricte* w finansowaniu świadczeń. Ja, mówiąc o organach władzy publicznej i zadaniach własnych gminy, powiatu i województwa, stałem na stanowisku (to można odczytać w moich publikacjach sprzed wielu lat, to nie jest kwestia ostatnich zmian ustawowych tego rządu), że samorządy mają kompetencje do finansowania świadczeń zdrowotnych, bo jeżeli mają to w zadaniach własnych, to powinny. Natomiast samorządy – tutaj ukłon w stronę pana profesora – że tego nie czyniły, tylko postawiły na profilaktykę zdrowotną, na programy różne i na finansowanie bazy medycznej, to jest jedna rzecz.

Dругa rzecz. Znamienny jest tutaj 1999 rok, kiedy samorządy dostały bazę leczniczą, natomiast odebrano im finansowanie. Finansowanie pozostawiono na poziomie rządowym. Kwestia jest jednak inna: jeżeli pan podnosi temat izb obrachunkowych, bo o tym pan mówił, to ja powiem wprost, że dzisiaj uchwała rady gminy, powiatu lub sejmiku moim zdaniem jest nie do podważenia, jeżeliby została taka podjęta, że ochrona zdrowia jako zadanie własne będzie finansowana ze środków samorządu. Chciałbym zobaczyć taką opinię, że ktoś by to podważył. Czym innym jest argumentacja, i to jest niuans, że samorządy twierdzą, iż nie otrzymały z pozycji rządowej finansowania na to zadanie, bo ono nie jest zadaniem zleconym, tylko jest zadaniem własnym.

Obecnie jesteśmy przed dyskusją, która w Polsce na poziomie ogólnokrajowym nie wybrzmiała. Ona wybrzmiała tutaj przed wakacjami na poziomie parlamentarnym, legislacyjnym, natomiast na poziomie dyskusji ogólnonarodowej nie. Chodzi o ten rozkład. Przykład – miasto stołeczne. W Warszawie, w której obradujemy w Senacie, jest siedem podmiotów założycielskich, różnych podmiotów leczniczych. Wszyscy zerkają na administrację rządową, czy będzie finansowanie, czy nie będzie. To jest tylko przykład, jak skomplikowana jest to materia.

Natomiast jeśli chodzi o podejście do placówek medycznych i ich miejsca w zabezpieczeniu bezpieczeństwa zdrowotnego, to tutaj doktryna i orzecznictwo różnie mówią. Jednak w kategoriach gospodarczych *stricte* liberalizmu ekonomicznego i *stricte* podaż–popyt nie możemy iść w tym kierunku. Działania obecnej władzy zwracają ten kierunek, który ja wyznaczyłem w 1989 roku, w lutym, marcu. Odbywały się liczne posiedzenia podstolika Okrągłego Stołu.

Wydałem na ten temat publikację. Chętnie ją przekażę, Panie Profesorze. Jakie były dyskusje? Otóż odcięcie było radykalne, wszystko, co było przed 1989 rokiem w kategoriach właśnie służby zdrowia, sprawiedliwości społecznej, zostało podważone. Wybitne osoby, które dzisiaj uchodzą za ekspertów w różnych mediach, tego typu stanowiska wyrażały i to, co mówię, jest do potwierdzenia, znajduje się w protokołach ze zgrupowań komisji konstytucyjnej, które się odbywały od 1990 do 1997 roku. Art. 68 konstytucji był bardzo mocno dyskutowany: czy my mamy iść już normatywnie w kierunku *stricte* gospodarki rynkowej w służbie zdrowia, czy jednak postawimy na sprawiedliwość społeczną. Proszę mi wierzyć, że zanegowałem liberalizm ekonomiczny, gospodarkę rynkową w służbie zdrowia. Z tej racji, że służba zdrowia, dostęp do opieki zdrowotnej znajduje się na drugim miejscu listy czynników najważniejszych dla bezpieczeństwa, wbrew temu, co tutaj też było przywoływane, że drugi jest strach o pracę. Strach o pracę, moim zdaniem, w Polsce jest mniejszy niż kwestia rodziny, bo to faktycznie jest osiemdziesiąt kilka procent. Na drugim miejscu jest strach, bojaźń związane z niemożnością dostępu do lekarza, bo to już nie jest kwestia (to jest następny stopień skomplikowania), że nas lekarze nie wyleczą, bo oni bardzo dobrze leczą, tylko tego, że nie możemy się w czasie, w którym potrzebujemy, do niego dostać. To jest wyzwanie, *à propos* tego, co pan tutaj podnosił. To jest wyzwanie i ryzyko na przyszłość, z którymi musimy się zmierzyć.

Natomiast ja protestuję przy każdej okazji przeciwko stwierdzeniu, że obecnie Minister Zdrowia jako jeden z organów wykonawczych jest w stanie to zabezpieczyć. Dzisiaj, jeżeli nie podejmiemy tego tematu z pozycji Senatu, jako jednego z organów władzy ustawodawczej, lub Sejmu, czy prezydenta, czy w ogóle członków Rady Ministrów jako organów władzy wykonawczej, czy nawet z pozycji sądownictwa, bo też odgrywa bardzo dużą rolę w systemie ochrony zdrowia, wbrew pozorom odgrywa ją nawet policja i prokuratura, już nie mówiąc o uczelniach wyższych, to nie rozwiążemy problemu narzędzia finansowania.

Andrzej Pająk

Zastępca przewodniczącego Komisji Samorządu Terytorialnego
i Administracji Państwowej

Proszę państwa, jak pokazała dyskusja i różnorodność poruszanych tematów, na problem bezpieczeństwa składa się wiele czynników, w ramach bezpieczeństwa istotnym czynnikiem jest na przykład bezrobocie oraz jakość spożywanych pokarmów, żywność. Kwestia rodziny też jest bardzo ważnym elementem. Myślę, że dzisiejsza konferencja pokazała, jak wiele, praktycznie każdy element naszego życia wpływa na nasze bezpieczeństwo.

Odnośnie do dzisiejszego spotkania, to wszystkie materiały zostaną zebrane i zostaną opublikowane. Jeśli chodzi o propozycje zmian w aktach prawnych, które padły, to za Senat mogę powiedzieć, że na pewno jest na nie otwarty. Jeśli pojawią się pewne wnioski, to Senat ma możliwość inicjatywy ustawodawczej, przy wspólnym działaniu zwłaszcza z Państwową Strażą Pożarną. Pragnę podkreślić, że z perspektywy starosty, wójta ta służba to jest centralne narzędzie, centralna instytucja, którą można się posługiwać przy zapewnieniu bezpieczeństwa. W sytuacjach głównie zagrożeń powodzią, wypadków drogowych lub osuwisk, na straży zawsze można polegać. Takie jest moje doświadczenie z gminy, z powiatu. Myślę, że jeszcze długo, długo tak będzie, że w zakresie podstawowego bezpieczeństwa straż pożarna będzie odgrywała wiodącą rolę. Element zaufania, o którym pani wcześniej mówiła, odgrywa tutaj dużą rolę.

Proszę państwa, pragnę podziękować zwłaszcza tym, którzy przyczynili się do zorganizowania tej konferencji. Tak więc składam podziękowanie na ręce pana rektora, na ręce pani dziekan. Bardzo pragnę podziękować pani profesor Annie Gołębiowskiej, która jest przewodniczącą rady programowej, a więc wszystko, co tutaj było wygłaszane, wcześniej zostało przez nią zaakceptowane i to dzięki niej znalazło się na wokandzie.

Pragnę również podziękować pracowniczkom senackiej Komisji Samorządu Terytorialnego i Administracji Państwowej, które z wielkim zaangażowaniem i oddaniem pracują, żeby wszystko odbyło się należycie.

Wszystkim bardzo serdecznie dziękuję i do następnego spotkania. Możliwe, że poruszoną dzisiaj problematykę trzeba by było dalej kontynuować i tematów na pewno jeszcze będzie wiele, a jeśli nie, to na pewno pojawią się nowe. Do bezpieczeństwa chyba jednak wszystko będzie się sprowadzało – jak widzę po wielości tematów, które dzisiaj na tej konferencji były poruszane.

ISBN 978-83-65711-10-6