www.noz.ue.wroc.pl

NAUKI O ZARZĄDZANIU
MANAGEMENT
SCIENCES

ISSN 2080-6000
e-ISSN 2449-9803
1 (30) 2017

DOI: 10.15611/noz.2017.1.07 JEL Classification: H12

WSPÓŁPRACA ADMINISTRACJI Z SEKTOREM GOSPODARCZYM NA RZECZ OCHRONY INFRASTRUKTURY KRYTYCZNEJ

COOPERATION BETWEEN BUSINESS AND THE PUBLIC ADMINISTRATION IN THE AREA OF CRITICAL INFRASTRUCTURE PROTECTION

Witold Skomra

Szkoła Główna Służby Pożarniczej, e-mail: witold.skomra@rcb.gov.pl

Streszczenie: Pojawienie się infrastruktury dostarczającej usługi niezbędne do funkcjonowania współczesnego społeczeństwa spowodowało, że wystąpiła współzależność między podmiotami gospodarczymi a administracją publiczną. Podmioty gospodarcze są przede wszystkim zainteresowane osiąganiem zysku, a administracja publiczna – bezpieczeństwem osób, które mogą być danej usługi pozbawione (np. w wyniku awarii). Obie strony mają więc wspólny cel: odpowiedni poziom bezpieczeństwa tej infrastruktury i maksymalne skrócenie czasu jej odtworzenia. Ten podział odpowiedzialności nie jest jednoznaczny. Administracja, a szczególnie e-administracja, sama realizuje procesy mogące, w razie awarii, negatywnie oddziaływać na społeczeństwo i podmioty gospodarcze. Na bazie tego spostrzeżenia sformułowano następujący problem badawczy: jakie powinny być relacje między właścicielami infrastruktury a administracją publiczną, by zapewnić właściwą ochronę tej infrastruktury. Po dokonaniu analizy dostępnej literatury i obowiązujących przepisów prawnych określono wykaz takich relacji.

Słowa kluczowe: infrastruktura krytyczna, logistyka społeczna, logistyka kryzysowa, zarządzanie kryzysowe, ciągłość działania.

Summary: The emergence of infrastructure which provides services that are indispensable for the proper functioning of modern societies created an interdependence between business and the public administration. Enterprises are primarily interested in making profits, while the public administration wants to provide security for people who may be deprived of a given service (e.g., in the event of a breakdown). Therefore, both parties have a common aim, which is to maintain a suitable level of protection of this infrastructure and to minimize the time of its recovery. Basing on this observation, we formulated the following research question: "What kind of relations between business and the public administration provides a proper level of infrastructure protection?" We analyze the available literature and the legal regulations in force, and give a list of such relations.

Keywords: critical infrastructure, social logistics, logistics of crisis situations, crisis management, business continuity.

1. Wstęp

Druga połowa XX wieku i początek wieku XXI to niespotykany w historii ludzkości rozwój techniczny i gospodarczy. Wywarł on wpływ na unowocześnianie infrastruktury[1] zapewniającej funkcjonowanie społeczeństw przez rozbudowę i specjalizację. Cechą uboczną tego procesu jest coraz większa zależność jednostki od współczesnych zdobyczy cywilizacyjnych. W przypadku dysfunkcji infrastruktury to uzależnienie, przybierające niekiedy cechy ubezwłasnowolnienia, prowadzić może nawet do zagrożenia bytu człowieka lub jego wspólnot. Taką infrastrukturę określa się zatem mianem infrastruktury krytycznej (IK). Zasadniczym problemem przy jej ochronie jest fakt, że znaczna część IK pozostaje własnością sektora prywatnego, podczas gdy za bezpieczeństwo ludności odpowiedzialność ponosi administracja publiczna. W efekcie podmiot gospodarczy pozostaje właścicielem rodzajów ryzyka mogących oddziaływać na posiadaną infrastrukturę (i pośrednio na cele działania lub zyski własnej organizacji), zaś administracja publiczna jest właścicielem rodzajów ryzyka związanych ze społecznymi skutkami braku usług dostarczanych przez IK. Na tej podstawie sformułowano następujące pytanie badawcze: jakie powinny być relacje między właścicielami infrastruktury a administracją publiczną, by zapewnić właściwą ochronę tej infrastruktury.

2. Pojęcie infrastruktury krytycznej

Po raz pierwszy termin „infrastruktura krytyczna" pojawił się w obiegu prawnym w USA w 1996 r., jednak od tego momentu był wielokrotnie modyfikowany. Amerykańska ustawa *Patriot Act* (zastąpiona w 2015 r. przez *Freedom Act*) definiowała IK jako „systemy i zasoby fizyczne lub wirtualne tak niezbędne dla Stanów Zjednoczonych, że niesprawność lub zniszczenie tych systemów i zasobów miałoby osłabiający wpływ na bezpieczeństwo, bezpieczeństwo gospodarki narodowej, narodową ochronę zdrowia lub każdą kombinację tych spraw" [Uniting and Strengthening America…, sec. 1016 (e)].

Na gruncie polskim termin ten pojawił się po raz pierwszy w ustawie o zarządzaniu kryzysowym, zgodnie z którą przez infrastrukturę krytyczną rozumie się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [Ustawa z 26 kwietnia 2007 r. …, art. 3, ust. 2]. Ustawa wskazała też 11 systemów, wśród których należy poszukiwać infrastruktury krytycznej. Są to:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Dla każdego z wymienionych systemów określono odrębne kryteria techniczne stosowane w procesie wyłaniania obiektów IK. Wskazano również ministra odpowiedzialnego za dany system.

Do przedstawionej metody wyłaniania obiektów IK można mieć zastrzeżenia, np. nie zdefiniowano infrastruktury krytycznej o znaczeniu lokalnym bądź regionalnym. Przyjmując przynależność do jednego z systemów za podstawowe kryterium wyłaniania obiektów IK, ogranicza się inne parametry, które mogą mieć kluczowe znaczenie dla życia i zdrowia wielu osób jednocześnie [Krupa, Wiśniewski 2015]. Ponadto tytuł ustawy sugeruje bardzo szerokie podejście do problematyki kryzysu i związanego z nim procesu zarządzania. W rzeczywistości treść ustawy została ograniczona głównie do zagadnienia zarządzania sytuacją kryzysową. Została ona zdefiniowana jako „sytuacja wpływająca 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". Przy tak zdefiniowanych celach ustawy definicję infrastruktury krytycznej można by uprościć w sposób następujący. Infrastruktura krytyczna są to obiekty, obiekty, instalacje lub usługi, których zniszczenie lub zakłócenie funkcjonowania spowodowałoby skutki dla bezpieczeństwa państwa i jego obywateli, sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Czym jest to bezpieczeństwo państwa, można pośrednio wywnioskować z treści jednego z aktów wykonawczych do ustawy, gdzie mówi się m.in. o zagrożeniach: „o istotnym wpływie na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji oraz potencjału ekonomicznego i obronnego" [Rozporządzenie Rady Ministrów z 30 kwietnia 2010, par.4, pkt 1a)].

Z zaproponowanej definicji można wyciągnąć następujący wniosek. Całościowe oddziaływanie dysfunkcji IK na społeczeństwo i obszar gospodarczy wymusza równie całościowe podejście do jej ochrony [Pyznar 2010, s. 212].

[1] Zgodnie z internetowym słownikiem języka polskiego PWN infrastruktura to: urządzenia i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki [*Słownik języka polskiego*…].

3. Obowiązki w zakresie ochrony IK

Zgodnie z ustawą o zarządzaniu kryzysowym właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia. Dodatkowym obowiązkiem operatora jest wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej [Ustawa z 26 kwietnia 2007 r. …, art. 6, ust. 5].

Zasady wyłaniania obiektów IK, współpracy w dziedzinie ich ochrony oraz standardy i dobre praktyki zawiera Narodowy Program Ochrony Infrastruktury Krytycznej (w skrócie NPOIK). Słowo „program" w nazwie nie jest przypadkowe. Celowo przyjęto, że nie może to być źródło prawa powszechnie obowiązującego. Podejście nakazowe ma bowiem wadę polegającą na niechęci wykonawców do realizacji narzuconych obowiązków [Pyznar 2010, s. 110]. Zgodnie z NPOIK ochrona IK r odbywa się w sześciu formach; są one następujące [Narodowy Program Ochrony Infrastruktury Krytycznej…, s. 30-31]:

1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia wdrażanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
6) plany ciągłości działania i odtwarzania – rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

Wymienione formy ochrony wymagane są od każdego z operatorów, niezależnie do którego z systemów zaliczono zarządzany przez niego obiekt.

Szczegółowe wymogi planów ochrony IK zawarto w rozporządzeniu wykonawczym. Jednym z istotnych elementów planu w myśl tego rozporządzenia są „warianty zapewnienia ciągłości funkcjonowania infrastruktury krytycznej" [Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. …, par. 2, ust. 3, pkt 4]. Warto też zauważyć, że nie w każdym przypadku sporządzenie planu jest obowiązkowe. W myśl ustawy jest możliwe uznanie, że wymóg posiadania planu jest spełniony, o ile operator przedłoży inny dokument, który jest zgodny z Narodowym Programem Ochrony Infrastruktury Krytycznej i który zapewnienia ciągłość funkcjonowania infrastruktury krytycznej. Odpowiednią decyzję podejmuje dyrektor Rządowego Centrum Bezpieczeństwa. W praktyce ten tryb postępowania dotyczy tych podmiotów, które wdrożyły zarządzanie ciągłością działania.

4. Udział administracji w zapewnianiu bezpieczeństwa IK

Odpowiedzialność operatora za ochronę i ciągłość działania IK nie oznacza, że administracja publiczna nie uwzględnia działań, które mają dodatkowo chronić IK, ale przede wszystkim zabezpieczają ludność przed skutkami dysfunkcji usług dostarczanych przez obiekty IK. To podwójne spojrzenie na bezpieczeństwo IK jest efektem pewnego paradoksu. Z punktu widzenia właściciela (operatora IK) infrastruktura przez niego zarządzana powinna służyć przede wszystkim osiąganiu celów biznesowych. Z punktu widzenia potrzeb odbiorcy usług ta sama infrastruktura powinna, poza celami biznesowymi, odpowiadać potrzebom społecznym. Próby zdefiniowania, czym jest taka infrastruktura biznesowo-społeczna, podejmowane są w ramach badań naukowych nad logistyką społeczną. W ramach nich stwierdzono, że istnieją pewne usługi, np. związane z ratowaniem zagrożonego życia i zapewnieniem bezpieczeństwa (publicznego oraz w przestrzeni publicznej), które nie są realizowane z potrzeby zysku. Jednak grupę podmiotów kierujących się takimi celami ograniczono do organizacji non profit [Szołtysek 2014, s. 5]. Inaczej podeszli do tego zagadnienia twórcy podziału logistyki na wojskową, cywilną i kryzysową. Według tej koncepcji głównym celem działania logistyki cywilnej jest maksymalizacja zysku przedsiębiorstwa, zaś logistyki kryzysowej – zaspokojenie elementarnych potrzeb logistycznych ludności. W tym drugim przypadku rachunek ekonomiczny ma znaczenie trzeciorzędne [Nowak, Nowak 2009]. Oba te nurty badawcze nie opisują poprawnie IK. W rzeczywistości mamy do czynienia z dwoma przypadkami. Operatorem IK możne być administracja publiczna, która swoje wydatki pokrywa bezpośrednio z budżetu państwa, a ewentualne zyski – co do zasady – odprowadza na rachunek dochodów budżetu państwa. Generalnie jej celem nie jest generowanie zysku (jest więc to postawa analogiczna do podejścia sto-

Tabela 1. Wsparcie naukowe systemów infrastruktury krytycznej państwa

Systemy infrastruktury krytycznej	Dyscypliny naukowe	Dziedziny nauki	Obszary wiedzy
Systemy zaopatrzenia w energię, surowce energetyczne i paliwa	dyscyplina wiodąca (DW): energetyka dyscypliny wspierające (DP): elektrotechnika, górnictwo i geologia inżynierska, inżynieria chemiczna, nauki o zarządzaniu	nauki techniczne nauki ekonomiczne	nauki techniczne nauki społeczne
Systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	DW: inżynieria chemiczna, technologia chemiczna DP: nauki o zarządzaniu	nauki techniczne nauki ekonomiczne	nauki techniczne nauki społeczne
Systemy transportowe	DW: transport DP: budownictwo, inżynieria środowiska, nauki o zarządzaniu	nauki techniczne nauki ekonomiczne	nauki techniczne nauki społeczne
Systemy łączności	DW: telekomunikacja DP: informatyka, nauki o administracji, nauki o zarządzaniu	nauki technicznych nauki prawne nauki ekonomiczne	nauki techniczne nauki społeczne
Systemy sieci teleinformatycznych	DW: telekomunikacja DP: nauki o zarządzaniu	nauki techniczne nauki ekonomiczne	nauki techniczne nauki społeczne

Źródło: [Zawiła-Niedźwiecki 2015, s. 8609-8610].

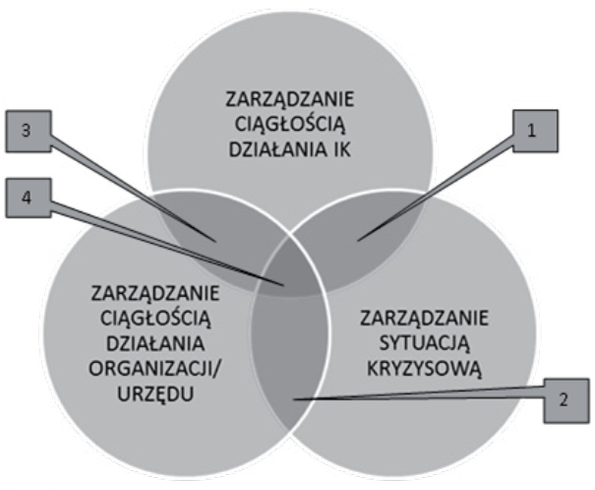
sowanego przez organizacje *non profit* opisywanego w ramach logistyki społecznej). Drugi przypadek to operatorzy będący podmiotami gospodarczymi, którzy jednocześnie muszą dbać o osiąganie zysku i powinni brać pod uwagę aspekty społeczne związane z prowadzoną działalnością. Co ciekawe, odpowiedzialność za skutki społeczne braku usług świadczonych na rzecz ludności przez IK nie pojawiają się w opracowaniach dotyczących społecznej odpowiedzialności biznesu (CSR – *Corporate Social Responsibility*) [Bernatt 2009].

Jak widać, funkcjonowanie IK umyka wszystkim wspomnianym nurtom badawczym. Sytuację dodatkowo komplikuje wielość dyscyplin naukowych, w zainteresowaniu których leżą poszczególne systemy IK. Powiązanie poszczególnych systemów IK z dyscyplinami naukowymi przedstawiono w tab. 1.

5. Zarządzanie ciągłością działania w ochronie IK

Jest jeszcze jeden dodatkowy element wymagający szczegółowych badań. Administracja i przedsiębiorcy stają się współzależni. Powstaje wspólna infrastruktura realizująca procesy na rzecz obydwu stron. Prowadzi to do uzależnienia się w takim stopniu, że dysfunkcja tej infrastruktury może prowadzić do skutków wykraczających poza granice władającej nią organizacji [Narodowy Program Ochrony Infrastruktury Krytycznej…, s. 5]. Konieczność otrzymywania przez administrację usług świadczonych przez IK jest oczywistością (brak prądu, wody czy ogrzewania uniemożliwia pracę urzędów). Natomiast krytyczny wpływ usług świadczących przez administrację na sektor biznesu już tak oczywisty nie jest. Tymczasem wdrażana obecnie e-administracja, w przypadku jej dysfunkcji, bardzo często utrudnia lub wręcz uniemożliwia realizację procesów biznesowych [Skomra 2016, s. 204]. Przykładem takich krytycznych usług jest platforma zaufanej poczty ePUAP, dostęp do rejestrów sądowych (KRS) czy rejestrów państwowych (PESEL).

W działalności biznesowej można się zabezpieczyć przed brakiem dostępności do niezbędnej usługi i zasobów przez zawarcie tzw. umowy *Service Level Agreement* (SLA), zawierającej wskaźniki dotyczące procedur współpracy, terminowości usuwania zgłoszonych błędów jak i sankcji za ich nieusunięcie [Załącznik nr 1…, s. 114]. Zawieranie takich umów z administracją publiczną jest, oczywiście, niemożliwe. Tym samym konieczne staje się uznanie ochrony IK (w tym IK, dla której operatorem jest administracja publiczna) jako procesu ukierunkowanego na ochronę ciągłości świadczenia określonej usługi oraz odtworzenia jej w razie potrzeby [Narodowy Program Ochrony Infrastruktury Krytycznej…, s. 5]. Aby to osiągnąć, wszyscy uczestnicy powinni posługiwać się podobną metodyką identyfikacji kluczowych procesów i usług oraz zasadami ich ochrony. Z tego powodu NPOIK zaleca wdrożenie we wszystkich obiektach IK planów ciągłości działania [Załącznik nr 1…, s. 119] na podstawie wielu norm, w tym normy – System Zarzą-



Rys. 1. Wzajemne relacje między zarządzaniem ciągłością działania a zarządzaniem sytuacją kryzysową

Źródło: opracowanie własne.

dzania Ciągłością Działania (*Business Continuity Management*) [ISO 22301:2012…]. Dodatkowo system zarządzania ciągłością działania powinien objąć urzędy obsługujące ministrów odpowiedzialnych za poszczególne systemy IK [Narodowy Program Ochrony Infrastruktury Krytycznej…, s. 21].

Uwzględniając fakt, że brak usługi świadczonej przez IK może wywołać sytuację kryzysową i konieczność uruchomienia procedur zawartych w planach zarządzania kryzysowego, wzajemne relacje między wszystkimi omawianymi obszarami można przedstawić na diagramie (rys. 1).

Obszary wspólne, zaznaczone na schemacie, można opisać następująco:

1. Zadania realizowane na zasadach współpracy przez operatora IK i administrację publiczną, a związane z minimalizacją skutków dysfunkcji IK.
2. Zdania podejmowane w ramach systemu zarządzania kryzysowego w przypadku awarii systemu decyzyjnego (brak sukcesji, awaria techniczna uniemożliwiająca przekazywanie decyzji itp.).
3. Zadania związane z minimalizacją skutków awarii IK, której operatorem jest sama administracja publiczna (administracja odpowiada za skutki zarówno bezpośrednie, jak i skutki pośrednie – w tym społeczne).
4. Zadania wykonywane w ramach współodpowiedzialności, dotyczące utrzymania usług realizowanych wspólnie (administracja i sektor biznesowy wdrażają procesy współzależne i wspólnie odpowiadają za skutki ich przerwania).

Wspomniane procedury, związane z zarządzaniem sytuacją kryzysową, mające uzupełniać i wspierać procesy ochrony IK, zostały zawarte w Krajowym Planie Zarządzania Kryzysowego oraz w planach zarządzania kryzysowego województwa, powiatu i gminy [Ustawa z 26 kwietnia 2007 r. …, art. 5]. We wszystkich tych dokumentach muszą się znaleźć m.in.:

- procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej,
- priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej.

Niezależnie od tego plany zarządzania kryzysowego poszczególnych ministrów muszą zawierać m.in.:

- analizę i ocenę możliwości wystąpienia zagrożeń, w tym dla infrastruktury krytycznej,
- szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczania i likwidacji ich skutków,
- organizację realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Dodatkowe zadania, których celem jest ochrona obiektów IK, wynikają z ustawy o działaniach antyterrorystycznych. Przykładowo po podniesieniu stopnia alarmowego policja ma obowiązek sprawdzenia zabezpieczeń w obiektach IK [Ustawa z dnia 10 czerwca 2016 r. …., art. 12]. Ważne postanowienia zawiera również jedno z rozporządzeń będące aktem wykonawczym do tej ustawy [Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. …]. Zgodnie z rozporządzeniem administracja publiczna wykonuje przedsięwzięcia w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP (stopień CRP jest prowadzany w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych), we współpracy z operatorami obiektów infrastruktury krytycznej[2] w zakresie ochrony tych obiektów. Jednocześnie operatorzy uwzględniają, na potrzeby tej współpracy, szczegółowe zakresy przedsięwzięć sporządzane przez administrację.

6. Podsumowanie

Wpływ administracji na inne dziedziny życia, w tym na obszar działalności gospodarczej kojarzy się zazwyczaj z procesem regulacyjnym (stanowienie prawa i egzekwowanie jego postanowień). Ochrona infrastruktury jest tu wyjątkiem. Ustawa o zarządzaniu kryzysowym nie przewiduje sankcji za niedopełnienie obowiązków dotyczących zadań i obowiązków związanych z IK, ale równocześnie nie przewiduje bezpośredniego wsparcia operatorów IK z budżetu państwa.

Bazując na przeprowadzonej analizie, relacje między właścicielami infrastruktury a administracją publiczną następujące w celu utrzymania właściwej ochrony tej infrastruktury można określić jako:

- współzależność – wspólna infrastruktura, zasoby bazodanowe i procesy wymagają, by eliminacja zagrożeń, które są z nimi związane, była traktowana jako zadanie wspólne,
- współodpowiedzialność – wspólne dążenie do poprawy bezpieczeństwa IK, wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów IK, społeczeństwa, gospodarki i państwa,
- współpraca – oznacza wykonywanie razem przez uczestników ochrony IK określonych, zbieżnych i wzajemnie uzupełniających się zadań do osiągnięcia wspólnego celu, który wynika z zasady współodpowiedzialności,
- zaufanie – rozumiane jako przekonanie, że motywacją działania uczestników ochrony IK jest dążenie do wspólnego celu – poprawy bezpieczeństwa IK i RP.

Aby to osiągnąć, niezbędne są wspólne standardy bezpieczeństwa i zasady postępowania w sytuacjach kryzysowych.

Literatura

Bernatt M., 2009, *Społeczna odpowiedzialność biznesu. Wymiar konstytucyjny i międzynarodowy*, Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa.

Internetowy słownik języka polskiego PWN, http://sjp.pwn.pl, 6.01.2017.

[1] Rozporządzenie posługuje się definicją: „właściciele, posiadacze samoistni i posiadacze zależni obiektów infrastruktury krytycznej".

ISO 22301:2012 – System Zarządzania Ciągłością Działania (*Business Continuity Management*).

Krupa T., Wiśniewski M., 2015, *Situation management of critical infrastructure resources under threat*, Foundation of Management – International Journal. Faculty of Management WUT, vol. 7.

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) z dnia 2 listopada 2015 r. przyjęty uchwałą Rady Ministrów nr 210/2015, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf, 16.12.2016.

Nowak W., Nowak E., 2009, *Podstawy logistyki w sytuacjach kryzysowych z elementami zarządzania logistycznego*, SWSPiZ, Łódź – Warszawa.

Pyznar M., 2010, *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, [w:] Tyburska A. (red.), *Ochrona infrastruktury krytycznej*, Wydawnictwo WSPol, Szczytno.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, DzU 2010, nr 83, poz. 542.

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

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP, DzU 2016, poz. 1101.

Skomra W., 2010, *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, [w:] Tyburska A. (red.), *Ochrona infrastruktury krytycznej*, Wydawnictwo WSPol, Szczytno.

Skomra W., 2016, *Zarządzanie kryzysowe. Praktyczny przewodnik*, Presscom, Wrocław.

Szołtysek J., 2014, *Przesłanki i założenia koncepcji logistyki społecznej*, Gospodarka Materiałowa i Logistyka, nr 2, s. 2-7.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56, OCT. 26, 2001.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, DzU 2016 r., poz. 904.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, tekst jedn., DzU 2013, poz. 1166 ze zm.

Załącznik nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, http://rcb.gov.pl/wp-content/uploads/Za%C5%82%C4%85cznik-nr-1-Standardy-s%C5%82u%C5%BC%C4%85ce-zapewnieniu-sprawnego-funkcjonowania-infrastruktury-krytycznej-%E2%80%93-dobre-praktyki-i-rekomendacje.pdf, 12.01.2017.

Zawiła-Niedźwiecki J., 2015, *Ryzyko operacyjne z perspektywy logistyki społecznej*, Logistyka – Nauka, nr 4, s. 8606-8613.