ZAPEWNIANIE BEZPIECZEŃSTWA KLUCZOWEJ INFRASTRUKTURY PAŃSTWA – PODEJŚCIE BEZSANKCYJNE CZY REGULACYJNE?

Krzysztof SZWARC

Wojskowa Akademia Techniczna

Streszczenie. W artykule scharakteryzowano istotę kluczowej infrastruktury państwa oraz dokonano analizy systemów wchodzących w jej skład. Zwrócono uwagę na wymagania dotyczące zapewniania bezpieczeństwa takich obiektów. Scharakteryzowano istotę podejścia bezsankcyjnego i regulacyjnego oraz dokonano analizy porównawczej obu podejść, przedstawiając ich wady i zalety.
Słowa kluczowe: kluczowa infrastruktura państwa, podejście regulacyjne, podejście bezsankcyjne, zapewnianie bezpieczeństwa kluczowej infrastruktury.

Wstęp

W każdym systemie można wyodrębnić takie elementy, które w szczególnym stopniu determinują zdolność realizacji jego celów. Podobnie w ogólnym zbiorze infrastruktury zlokalizowanej na administrowanym obszarze można wyodrębnić takie, które na podstawie obiektywnych kryteriów uznaje się za kluczowe. Od ich sprawności w znacznej mierze zależy bezpieczeństwo społeczeństwa i państwa. Dlatego ochrona oraz zapewnianie ciągłości działania takich obiektów stanowi szczególne wyzwanie dla organizatorów systemów bezpieczeństwa[1].

Bieżący stan danego obiektu jest pochodną skuteczności systemu bezpieczeństwa, a konkretnie zdolności przeciwdziałania zakłóceniom. Należy dostrzec, że będące przedmiotem badania systemy są od siebie współzależne, a zatem sprawność jednego systemu może poważnie implikować zdolność dostarczania wartości przez inne. Przy redukowaniu ryzyka zakłóceń można zatem rozważać strategie polegające na:

a) współpracy z innymi operatorami w zakresie zapewniania bezpieczeństwa;
b) uniezależnianiu się od dostaw usług przez innych operatorów;
c) utrzymywaniu zapasów newralgicznych zasobów dostarczanych przez otoczenie.

W proces zapewniania bezpieczeństwa kluczowej infrastruktury zlokalizowanej na danym terytorium zaangażowane są państwa oraz inne organizacje, które posiadają kompetencje do regulowania stosunków pomiędzy operatorami takich systemów.

---

[1] K. Szwarc, P. Zaskórski, *Modelowanie procesów zapewniania bezpieczeństwa i ciągłości działania organizacji administracji publicznej*, „Studia Bezpieczeństwa Narodowego" nr 12, WAT, Warszawa 2017, s. 335-361.

Należy zauważyć, że przyjęto dwa różne podejścia do jej ochrony, tj. a) **bezsankcyjne**, dotyczące m.in. infrastruktury krytycznej i szczególnie eksponowane w Narodowym Programie Ochrony Infrastruktury Krytycznej[2]; b) **regulacyjne**, w którym precyzyjnie określa się zadania oraz sankcje związane z brakiem ich realizacji.

Celem artykułu jest ocena wpływu obu podejść na bezpieczeństwo kluczowej infrastruktury zlokalizowanej na terytorium państwa. Podjęto próbę odpowiedzi na pytanie: *W jaki sposób przyjęte przy ustanawianiu przepisów podejście wpływa na zapewnianie bezpieczeństwa systemów kluczowej infrastruktury państwa przez operatorów?* W trakcie badań wykorzystano metody analizy i krytyki źródeł oraz analizy porównawczej.

1. Kluczowa infrastruktura państwa

W temacie artykułu celowo użyto sformułowania „kluczowa infrastruktura", aby wyodrębnić z ogólnego zbioru infrastruktury elementy o newralgicznym znaczeniu, przy jednoczesnym zachowaniu dystynkcji pomiędzy pojęciami wprowadzonymi do języka na podstawie różnych aktów prawnych. Na podstawie słowników można stwierdzić, że określenie „**kluczowy**" może dotyczyć pozycji (roli), osoby lub rzeczy, która kontroluje (reguluje) funkcjonowanie innych obiektów lub może wywierać wpływ na ich działanie. To obiekt podstawowy, istotny, newralgiczny, najważniejszy, wyjściowy czy główny[3].

Drugim składnikiem przyjętego terminu jest **infrastruktura**, która może być rozumiana jako zbiór instytucji i aparatury zapewniających warunki istnienia, przetrwania i rozwoju społeczeństwa oraz jego aktywności gospodarczej i społecznej na danym terytorium[4]. Pomimo pewnych wątpliwości terminologicznych, B. Frischmann przez infrastrukturę rozumie złożone fizyczne systemy tworzone przez ludzi i służące zaspokajaniu społecznych potrzeb. Według wspomnianego autora, do tradycyjnej infrastruktury należy zaliczyć systemy[5]:

- transportowe – infrastruktura drogowa, kolejowa, lotnicza, morska;
- komunikacyjne – sieci teleinformatyczne i usługi pocztowe;

---

[2] Niezmiennie od 2013 r. w Narodowym Programie Ochrony Infrastruktury Krytycznej podkreśla się, że w Ustawie o zarządzaniu kryzysowym nie przewidziano sankcji za niedopełnienie przez operatorów obowiązków dotyczących ochrony infrastruktury krytycznej oraz finansowego wsparcia dla podejmowania takich działań. Zob. *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013, s. 7; *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2015, s. 9; *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2018, s. 9.

[3] *Webster's New English Dictionary and Thesaurus for Home*, REA, Warszawa 2005, s. 775; *Nowy słownik języka polskiego*, PWN, Warszawa 2002, s. 329.

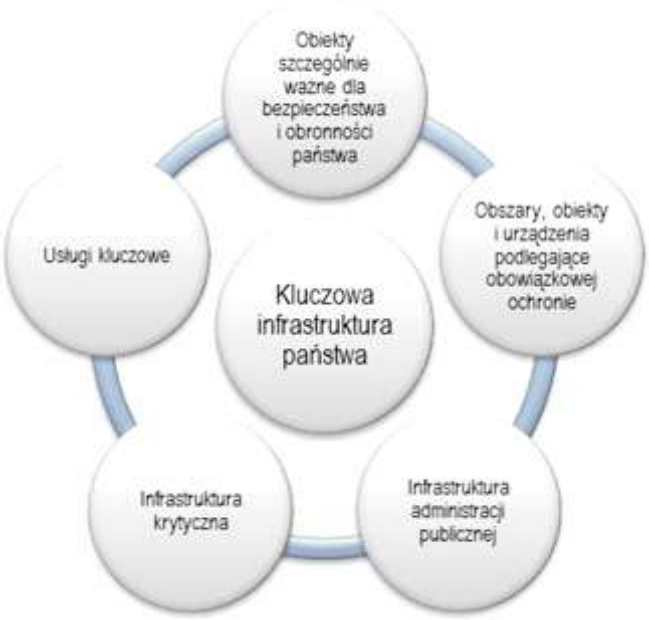
[4] Ibidem, s. 274; T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wrocław, Warszawa, Kraków, Gdańsk 1978, s. 82-83.

[5] B. Frischmann, *Infrastructure. The Social Value of Shared Resources*, Oxford University Press, New York 2012, s. 3-4.

- sprawowania władzy – sądownictwo, administracja publiczna;
- świadczenia usług społecznych – szkoły, kanalizacja, zaopatrzenie w wodę i energię.

Z przeprowadzonych badań wynika, że aktualnie nie ma jednej uniwersalnej definicji pojęcia „infrastruktura". Odmienne jest również postrzeganie tego, z jakich obiektów się składa. Dostrzega się próby podziału ogólnego zbioru infrastruktury na ekonomiczną (w tym techniczną) oraz społeczną. Biorąc pod uwagę kryterium prawa własności, systemy infrastruktury można podzielić na **publiczne** – które stanowią dobra publiczne, są zatem udostępniane bezpłatnie lub częściowo płatnie, pozostające w gestii władz publicznych (rządowych i samorządowych, które odpowiadają za jej tworzenie i utrzymanie) oraz **komercyjne**[6].

W ramach rozważanej problematyki istotne jest określenie zakresu „kluczowej infrastruktury państwa", który ulega rozszerzeniu na podstawie powstawania nowych oraz zmiany dotychczasowych przepisów prawa (rys. 1).



Rys. 1. Kluczowa infrastruktura państwa
Źródło: opracowanie własne

[6] K. Brzozowska, *Finansowanie inwestycji infrastrukturalnych przez kapitał prywatny na zasadzie project finance*, CeDeWu, Warszawa 2009, s. 18.

W ten sposób do kluczowej infrastruktury państwa[7] można zaliczyć coraz to nowe kategorie obiektów, przy których wyodrębnianiu nie spełniono warunku rozłączności zbiorów. Chronologicznie pierwszym zbiorem obiektów w tej kategorii są **obszary, obiekty i urządzenia podlegające obowiązkowej ochronie** typowane na podstawie Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia. Aktualnie do tej kategorii obiektów zalicza się obszary, obiekty i urządzenia, których zakres dotyczy: obronności państwa, ochrony interesu gospodarczego państwa, bezpieczeństwa publicznego, ochrony innych ważnych interesów państwa, oraz systemy infrastruktury krytycznej[8]. Dokument ten reguluje sposób wyznaczania takich obiektów, nakazuje obowiązek fizycznej i technicznej ochrony.

Inną wyżej wymienioną kategorią obiektów, które można zaliczyć do kluczowej infrastruktury państwa, jest **infrastruktura krytyczna**. Pierwotna definicja tego pojęcia została zakwestionowana wyrokiem Trybunału Konstytucyjnego. W efekcie, po nowelizacji ustawy, przyjęto nową definicję, a także zbiór obiektów, spośród których systemy takie można identyfikować, na podstawie niejawnych kryteriów. Ponadto, w analizowanej ustawie[9]:

- sformułowano definicje pojęć: „europejska infrastruktura krytyczna", „ochrona infrastruktury krytycznej", „planowanie cywilne";
- określono zadania planowania cywilnego, w tym dotyczące przygotowania rozwiązań na wypadek zniszczenia lub zakłócenia działania IK;
- nakłada się na dyrektora RCB obowiązek tworzenia i aktualizacji Narodowego Programu Ochrony Infrastruktury Krytycznej, rozpoznaje potencjalną EIK oraz informuje w tej sprawie odpowiednie organa UE;
- określa się zadania organów administracji publicznej i operatorów dotyczące ochrony infrastruktury krytycznej.

Ponadto w dokumencie wykonawczym[10] do ustawy określa się strukturę, a także sposób tworzenia i aktualizacji przez operatorów planu ochrony infrastruktury krytycznej. Zawiera się w nim: a) dane operatora oraz infrastruktury, umożliwiające jej identyfikację; b) analizę ryzyka zagrożeń zabezpieczanego obiektu, ze szczególnym uwzględnieniem istnienia zależności od innych systemów oraz środków (własnych i publicznych) możliwych do wykorzystania w celu ochrony infrastruktury krytycznej; c) warianty przeciwdziałania zakłóceniom, tj. reagowania kryzysowego, zapewniania ciągłości działania oraz odtwarzania zniszczonych / uszkodzonych systemów; d) zasady współpracy z centrami zarządzania kryzysowego i organami administracji publicznej.

---

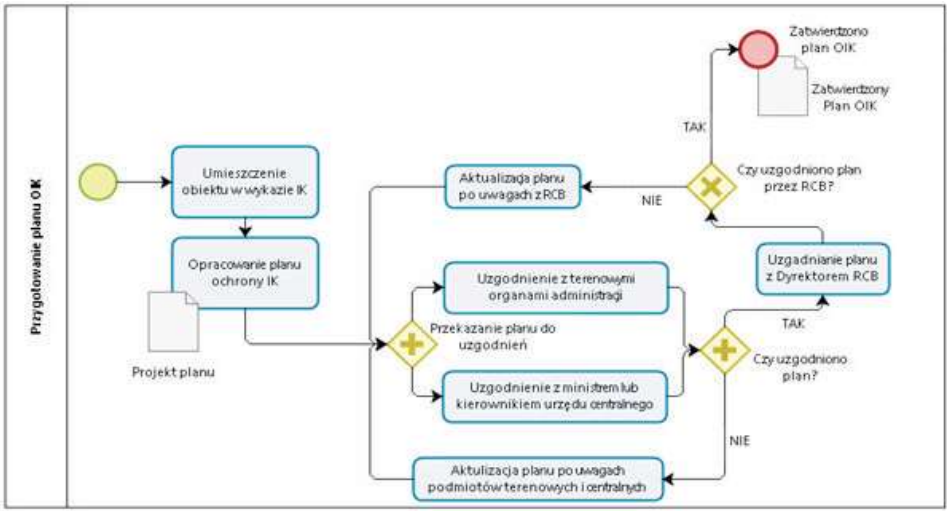
7 Takiego pojęcia dla określenia analizowanego nadsystemu użyto [w:] R. Radziejewski, *Ochrona infrastruktury krytycznej. Teoria a praktyka*, PWN, Warszawa 2014.

8 Dz.U. z 2018 r. poz. 2142, art. 5, ust. 2.

9 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2018 r. poz. 1401.

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

Proces przygotowywania planu przedstawiono na rysunku 2. W rozporządzeniu przyjęto, że dokument ten powinien być aktualizowany co najmniej raz na dwa lata, a każda jego zmiana wymaga uzgodnień przez wojewodę i terenowe organy administracji zespolonej i niezespolonej, właściwego ministra lub kierownika urzędu centralnego, a także dalej dyrektora RCB. Pewnym uproszczeniem jest natomiast możliwość usuwania w planie oczywistych pomyłek przez organ dokonujący uzgodnienia.



Rys. 2. Proces przygotowania planu ochrony infrastruktury krytycznej
Źródło: opracowanie własne

Rys. 3. Zintegrowane podejście do zapewniania bezpieczeństwa infrastruktury krytycznej
Źródło: opracowanie własne

Z zalecanej w rozporządzeniu struktury planu wynika, że przyjęto kompleksowe podejście do zapewniania bezpieczeństwa infrastruktury krytycznej obejmujące mechanizmy oceny zagrożeń i ryzyka, prewencji i reakcji na wystąpienie zakłócenia / zniszczenie obiektu. Założenia tego podejścia zostały sprecyzowane w załączniku 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej, w którym zebrano dobre praktyki i rekomendacje dotyczące zapewniania bezpieczeństwa tych systemów[11]. Z rysunku 3 wynika, że adekwatnym terminem do przedsięwzięć opisywanych w analizowanych dokumentach jest zapewnianie bezpieczeństwa infrastruktury krytycznej, co można interpretować jako poparte analizą ryzyka i zaplanowane działania polegające na ochronie oraz zapewnianiu funkcjonalności i integralności infrastruktury krytycznej, poprzez ograniczanie podatności na zagrożenia, a także reagowanie na incydenty, wznawianie i odtwarzanie pracy.

Z analizy porównawczej tekstów Programu od 2013 wynika, że zarówno jego cele, jak i priorytety w analizowanym okresie nie uległy zmianie. Może to budzić pewne wątpliwości, zwłaszcza w aspekcie priorytetów, gdzie w tekstach z 2015 i 2018 r. wprost deklaruje się, że zdefiniowane priorytety dotyczą okresu „2 lat od przyjęcia przez Radę Ministrów aktualizacji Programu"[12]. Można stąd wnioskować, że albo nie osiągnięto zdefiniowanych wcześniej priorytetów, albo przy przygotowaniu Programu powielono analizowany fragment dokumentu.

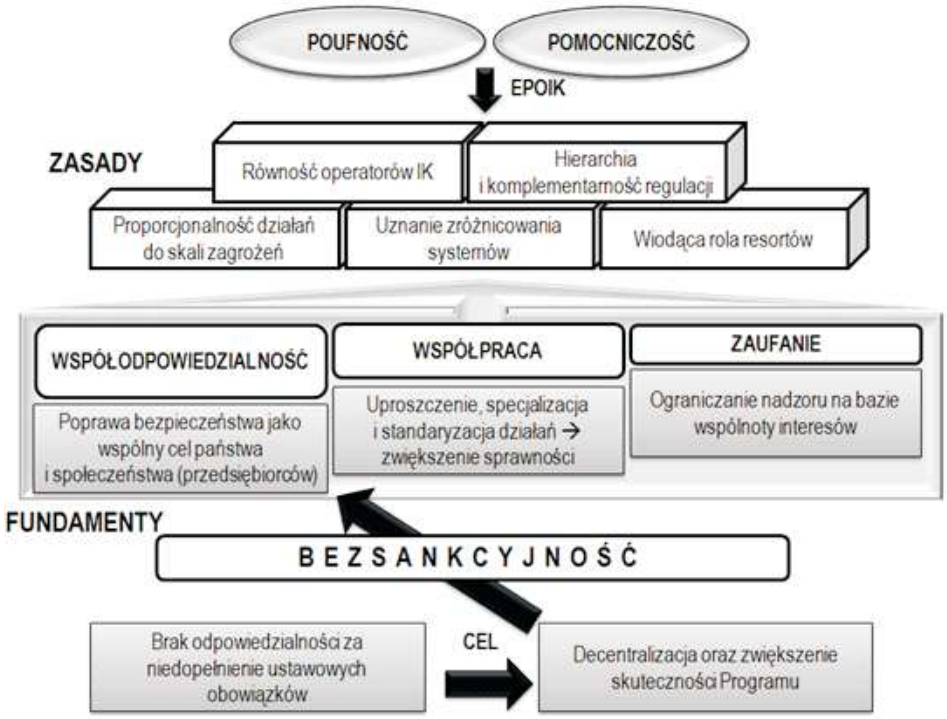
Przy przygotowywaniu NPOIK wzorowano się na zasadach sformułowanych w Europejskim Programie Ochrony IK (rys. 4). Można przyjąć, że inną, naturalną, niewyartykułowaną wprost, wspólną dla obu programów jest zasada poufności, która w pewnym stopniu może utrudniać zaangażowanie w realizację programowych zadań m.in. środowiska naukowego. Jak widać (rys. 4), NPOIK oparto na trzech zasadach tworzących filary, a także pięciu zasadach uzupełniających. Oprócz wspomnianych wcześniej, z regulacji UE wynika zasada pomocniczości, której istota nadaje prymat programom narodowym, w stosunku do których program europejski powinien pełnić funkcję wspierającą i uzupełniającą. W związku z dokonaną wcześniej analizą innego aktu prawnego oraz zaliczeniem do objętych jego jurysdykcją obiektów infrastruktury krytycznej utrzymania w mocy zasady bezsankcyjnego podejścia. Niemniej jest ona spójna z fundamentalnymi zasadami Programu, a zwłaszcza zasadą zaufania, że ustanawiane przez operatorów zabezpieczenia są zgodne z rekomendacjami oraz skuteczne. Stosowanie tej zasady nie oznacza rezygnacji z nadzoru, czego przykładem są prezentowane, ze względu na zachowanie zasady poufności

[11] *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, RCB, Warszawa 2018.

[12] Por. NPOIK 2015, 2018: pkt 2.3.

jedynie w formie komunikatu, wyniki kontroli dokonanej przez NIK. Wynika stąd, że zaniechania dotyczyły[13]:

- ustanawiania mechanizmów ochrony fizycznej, w tym dotyczących wejścia na teren obiektów oraz systemu monitoringu;
- niedostatecznej ochrony prawnej, w tym zwłaszcza zawierania w umowach stosownych klauzul dotyczących poufności oraz sprawdzania oferentów;
- braków w ochronie personalnej w zakresie przygotowania procedur na wypadek sabotażu oraz typowania kluczowych pracowników systemu;
- wad ochrony teleinformatycznej w zakresie audytu sieci informatycznej oraz zabezpieczenia przemysłowego systemu sterowania procesami technologicznymi (SCADA).



Rys. 4. Uniwersalne zasady współpracy na rzecz zapewniania bezpieczeństwa infrastruktury krytycznej

Źródło: K. Szwarc, *Współzależność jako wyzwanie w aspekcie ochrony infrastruktury krytycznej,* [w:] Z. Czachór, A. Chabasińska (red. nauk.), *Bezpieczeństwo narodowe Polski. Zagrożenia i determinanty zmian,* Difin, Warszawa 2016, s. 153

[13] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-obiektow-infrastruktury-krytycznej.html (dostęp 15.07.2018 r.).

W efekcie powyższych zaniechań wymienia się incydenty, które mogły prowadzić do poważnych skutków, w tym wpływu na zdrowie i życie ludzi. NIK wyraziła również zastrzeżenia do realizacji zadań przez organy administracji publicznej dotyczące zwłaszcza współdziałania i informowania przez wojewodów organów niższych szczebli o istnieniu obiektów IK na administrowanych przez nich terenach oraz braku współpracy organów szczebla gminnego z operatorami IK.

Innym źródłem prawa, w którym sformułowano wymagania w analizowanym zakresie, jest **rozporządzenie**[14] do ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony RP, w którym mowa jest o **obiektach szczególnie ważnych dla bezpieczeństwa i obronności państwa**. Na podstawie nowelizacji rozporządzenia nie tylko rozszerzono pierwotny katalog obiektów, lecz także sprecyzowano ich charakterystykę[15]. Można przy tym wnioskować, że:

- wyłączenie z tej kategorii stanowisk kierowania bezpieczeństwem narodowym oznacza, że zabezpieczenia tych obiektów są regulowane przepisami innej normy prawnej[16], co nie wyłącza ich z katalogu kluczowej infrastruktury państwa;
- do tej kategorii można również zaliczyć wyłączone w pkt 1 obiekty[17] **po dokonaniu nowelizacji rozporządzenia** – należy bowiem zauważyć, że po przekształceniu BOR w SOP w ustawie nie wymienia się obiektów i urządzeń o szczególnym znaczeniu.

Na tej podstawie Rada Ministrów ustala wykaz obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa, a za jego prowadzenie i aktualizację odpowiada minister obrony narodowej. Objęte tym wykazem obiekty podlegają szczególnej ochronie (rys. 5).

---

[14] Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2003 r. nr 116, poz. 1090.

[15] Rozporządzenie Rady Ministrów z dnia 16 grudnia 2016 r. zmieniające Rozporządzenie w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2017 r. poz. 42, §1 pkt 1 i 2.

[16] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym, Dz.U. z 2004 r. nr 98, poz. 978.

[17] Zgodnie z brzmieniem ustawy z dnia 16 marca 2001 r. o Biurze Ochrony Rządu z obiektów szczególnie ważnych dla bezpieczeństwa i obronności wyłączono obiekty i urządzenia o szczególnym znaczeniu oraz obiekty służące Prezydentowi RP, Prezesowi Rady Ministrów, ministrowi właściwemu ds. wewnętrznych i zagranicznych. W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa nie wymienia się obiektów i urządzeń o szczególnym znaczeniu. Drugi punkt został natomiast rozszerzony i dotyczy ponadto również wskazanych w decyzji ministra SW innych obiektów stanowiących siedziby członków Rady Ministrów, z wyłączeniem obiektów służących ministrom resortów obrony narodowej i sprawiedliwości. Por. Dz.U. 2001 nr 27, poz. 298 z późn. zm. art. 2 oraz Dz.U. z 2018 r. poz. 138 z późn. zm., art. 3.

Na rysunku 5 nie zaznaczono, że w proces szczególnej ochrony zaangażowani są ministrowie obrony narodowej (obiekty kategorii I) i spraw wewnętrznych (obiekty kategorii II), dla których przewidziano zadania dotyczące[18]:

- opracowania wytycznych do przygotowania i prowadzenia szczególnej ochrony;
- opracowywania i aktualizacji planów ochrony, gdzie w ochronie uczestniczą SZ RP, oraz uzgadniania pozostałych planów (kat. I), a także opracowania procedury przygotowywania, uzgadniania aktualizacji planów (kat. II);
- ewidencjonowania obiektów oraz informowania drugiego ministra o wprowadzaniu zmian w ewidencji;
- opiniowania wniosków o zaliczenie danego obiektu do kategorii obiektu szczególnie ważnego dla bezpieczeństwa i obronności państwa;
- decydowania o użyciu SZ RP, Policji lub PSP w zabezpieczeniu obiektu;
- prowadzenia szkoleń dla podmiotów odpowiedzialnych za przygotowanie i prowadzenie szczególnej ochrony.

Rys. 5. Funkcje i zadania podmiotów odpowiedzialnych za szczególną ochronę

Źródło: opracowanie własne na podstawie Rozporządzenia Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2003 r. nr 116, poz. 1090; Rozporządzenie Rady Ministrów z dnia 16 grudnia 2016 r. zmieniające rozporządzenie w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2017 r. poz. 42

[18] Rozporządzenie Rady Ministrów z dnia 16 grudnia 2016 r. zmieniające Rozporządzenie w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2017 r. poz. 42, §1 pkt 5 i pkt 6.

Kolejną kategorią obiektów, które można zaliczyć do kluczowej infrastruktury państwa, jest **infrastruktura administracji publicznej (IAP)**, czyli „systemy oraz obiekty niezbędne do zapewnienia bezpiecznego i ciągłego funkcjonowania organów administracji publicznej"[19]. W dokumencie tym reguluje się również sposób zabezpieczania obiektów infrastruktury krytycznej w związku z zagrożeniem terrorystycznym. Dominującą rolę w tym procesie przewidziano dla Szefa Agencji Bezpieczeństwa Wewnętrznego, który na podstawie informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego obiektom IK lub IAP może wydawać polecenia organom administracji publicznej, właścicielom i posiadaczom obiektów należących do tych rodzajów infrastruktury.

Adekwatnie do różnego ryzyka zagrożenia zdarzeniem o charakterze terrorystycznym, w ustawie przewidziano możliwość wprowadzenia stopni alarmowych oraz stopni alarmowych CRP. Szczegółowe wytyczne dotyczące zwiększenia rygorów bezpieczeństwa w zależności od typu stopnia alarmowego (CRP) określa rozporządzenie[20]. Wraz z wprowadzaniem kolejnych stopni alarmowych:

- wzmacnia się kontrolę zabezpieczanych obiektów, zarówno wewnątrz, jak i w ich bezpośrednim otoczeniu;
- ogranicza możliwość wstępu na teren chroniony osób postronnych, a także weryfikuje uprawnienia pracowników do wejścia i wnoszenia na teren obiektu;
- wzmacnia obsadę etatową oraz potencjał jednostek interwencyjnych możliwych do wykorzystania w przypadku wystąpienia incydentu, w tym broni i amunicji;
- dokonuje przeglądu procedur uruchamianych w kolejnych stopniach;
- prowadzi akcje informacyjne wśród społeczeństwa oraz personelu;
- weryfikuje systemy rezerwowe oraz zdolność pracy w lokalizacji zapasowej na wypadek wystąpienia zakłócenia;
- ogranicza możliwość wstępu na teren wybranych obiektów.

Z kolei wprowadzanie kolejnych stopni alarmowych CRP oznacza, że należy:

- wzmocnić monitoring stanu bezpieczeństwa systemów teleinformatycznych;
- poinformować i uczulić personel o ryzyku incydentów informatycznych;
- zachować zdolność komunikacji z podmiotami reagowania kryzysowego oraz informować je o podjętych działaniach i stanie bezpieczeństwa systemu;
- dokonywać przeglądu procedur;
- wzmacniać gotowość własnego personelu do reagowania na incydenty bezpieczeństwa, w tym w formie całodobowych dyżurów;

[19] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. z 2018 r. poz. 452, art. 2, pkt 3.

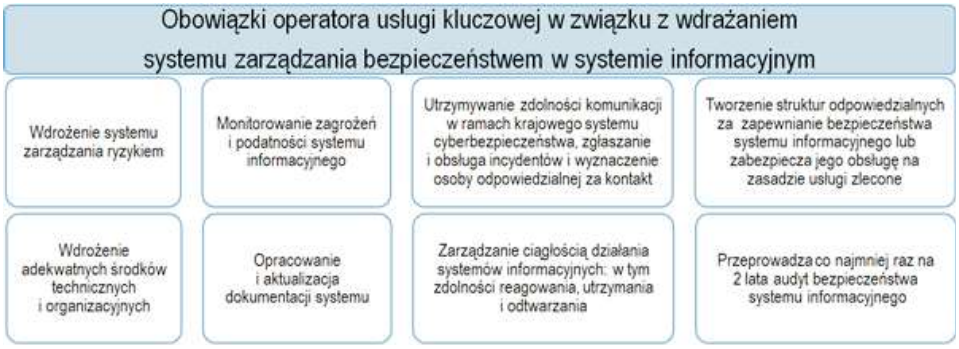
[20] Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP, Dz.U. z 2016 r., poz. 1101.

- dokonywać przeglądu zapasów uruchamianych w sytuacjach kryzysowych;
- dokonywać przeglądu i w razie potrzeby uruchamiać plany ciągłości działania.

Chronologicznie najnowszą kategorią obiektów, które można zaliczyć do kluczowej infrastruktury państwa, są **usługi kluczowe**. Za taką zgodnie z ustawą można uznać usługę, „która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych”[21]. Równie ważna wydaje się dokonana dalej charakterystyka operatora usługi kluczowej, za którego można uznać podmiot[22]:

- scharakteryzowany w ramach załącznika 1 do rozporządzenia, posiadający jednostkę organizacyjną na terytorium RP i uznany przez organ właściwy ds. cyberbezpieczeństwa (wymieniony w rozdziale 8 ustawy) za takiego operatora;
- który świadczy usługę kluczową z wykorzystaniem systemów informatycznych, a incydent bezpieczeństwa istotnie zakłócałby zdolność świadczenia tej usługi.

Wykaz takich operatorów prowadzony jest przez ministra cyfryzacji. Wykaz usług kluczowych wydano w formie rozporządzenia[23]. W rozdziale trzecim ustawy określono obowiązki operatora usług kluczowych dotyczące ustanawiania i wdrażania systemu zarządzania bezpieczeństwem informacyjnym, zestawione syntetycznie na rysunku 6.



Rys. 6. Obowiązki operatora usługi kluczowej związane z ustanawianiem systemu zarządzania bezpieczeństwem dla systemu informacyjnego

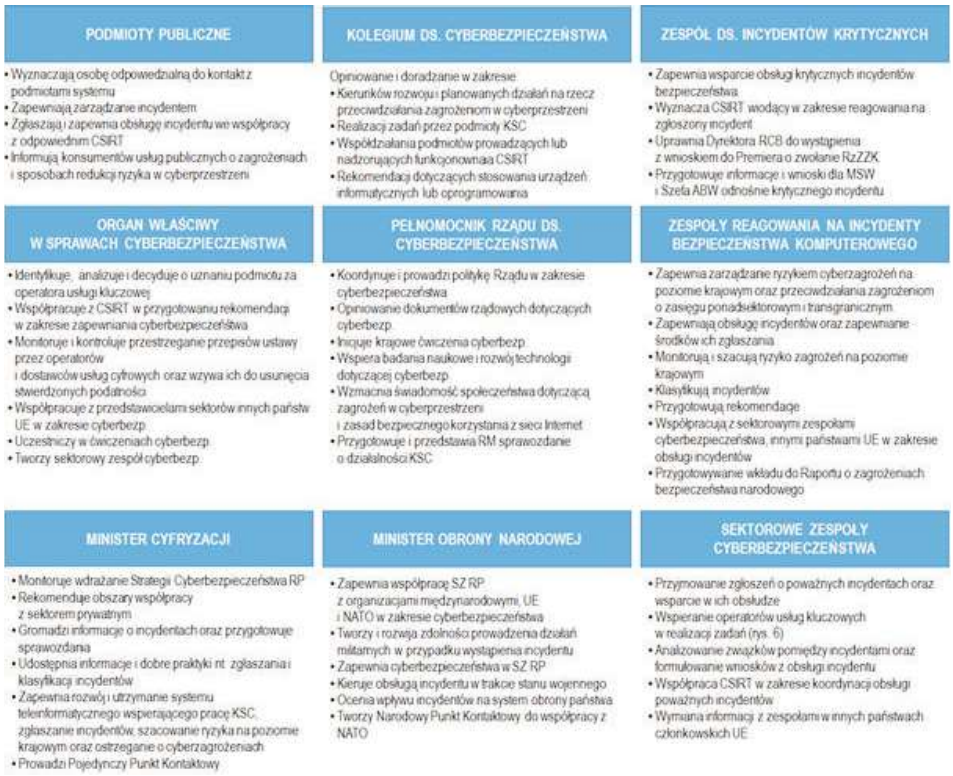
Źródło: opracowanie własne na podstawie: Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r. poz. 1560, art. 2, pkt 16

[21] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r. poz. 1560, art. 2, pkt 16.

[22] Ibidem, art. 5.

[23] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz.U. z 2018 r. poz. 1806.

Na podstawie analizowanych norm prawa operator usługi kluczowej zobowiązany został do wdrożenia kompleksowego systemu zarządzania bezpieczeństwem informacji (rys. 6), obejmującego pełną triadę (rys. 3), z uwzględnieniem specyfiki systemu teleinformatycznego. W formie aktów wykonawczych sprecyzowano wymagania wobec struktur bezpieczeństwa tworzonych przez operatorów usług kluczowych, wymagania organizacyjne i techniczne dla podmiotów świadczących usługi w zakresie cyberbezpieczeństwa[24] oraz dokumentacji SZBI wykorzystywanego do świadczenia usługi kluczowej[25]. W ustawie rozróżnia się usługi cyfrowe oraz dostawcę takich usług i jego obowiązki.



Rys. 7. Obowiązki podmiotów Krajowego Systemu Cyberbezpieczeństwa (KSC)
Źródło: opracowanie własne

[24] Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. z 2018 r. poz. 1780.

[25] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz.U. z 2018 r. poz. 2080.

Operatorzy usług kluczowych oraz dostawcy usług cyfrowych to istotne elementy krajowego systemu cyberbezpieczeństwa (rys. 7), którego skład obejmuje ponadto wybrane podmioty publiczne, Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego organizowane przez ABW, MON oraz Państwowy Instytut Badawczy (NASK), sektorowe zespoły cyberbezpieczeństwa oraz podmioty świadczące usługi w tym zakresie, organy właściwe ds. cyberbezpieczeństwa, Pojedyncze Punkty Kontaktowe, Pełnomocnika Rządu oraz Kolegium ds. Cyberbezpieczeństwa. W ustawie oraz dokumentach wykonawczych opisano zadania tych podmiotów, które syntetycznie zebrano na rysunku 7.

Celem ustawy jest zatem stworzenie wielopoziomowego systemu zapewniania cyberbezpieczeństwa. Najistotniejszą rolę w zapewnianiu ciągłości świadczenia kluczowych usług mają operatorzy kluczowych usług oraz dostawcy cyfrowi (rys. 6). W skład systemu (rys. 7) wchodzą ponadto podmioty koordynujące lub wspierające obsługę incydentów o zasięgu ogólnokrajowym, transgranicznym i ponadsektorowym. W strukturze systemu można również znaleźć podmioty, których zasadniczym zadaniem jest nie tyle bieżące reagowanie, co opiniowanie i kształtowanie kierunków rozwoju, a także formułowanie rekomendacji.

Zaangażowanie podmiotów systemu zależy od rodzaju incydentu. Dlatego w ustawie rozróżnia się incydenty: poważny, krytyczny oraz istotny. Dla uściślenia wydano dwa rozporządzenia, w których definiuje się progi istotności oraz uznawania incydentu za poważny, z podziałem na sektory, podsektory i zdarzenia[26].

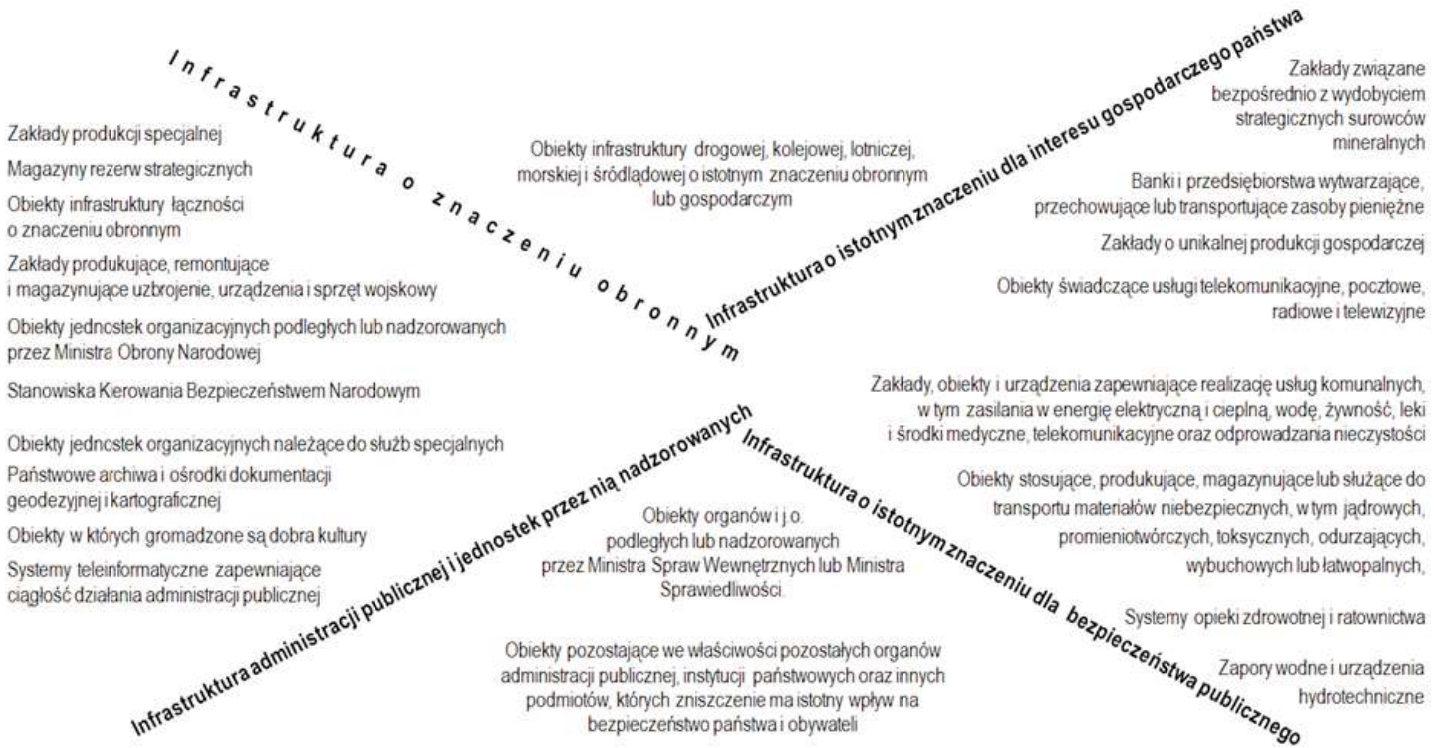
Biorąc pod uwagę zjawisko współzależności oraz transgraniczność systemów kluczowej infrastruktury, starania związane z normalizacją działań w zakresie zapewniania cyberbezpieczeństwa można uznać za zasadne[27]. O wadze cyberbezpieczeństwa mogą również świadczyć przewidziane w ustawie sankcje, będące konsekwencją wybranego w toku procedowania nad dyrektywą podejścia regulacyjnego do ochrony tych systemów.

Jako syntezę omawianych zagadnień dokonano próby klasyfikacji i wymienienia systemów składających się na kluczową infrastrukturę państwa (rys. 8). W praktyce trudno zakładać, aby był to katalog zamknięty. Podział ten nie musi być również kompletny ze względu na niejawny charakter kryteriów identyfikacji niektórych systemów, w tym infrastruktury krytycznej, a co za tym idzie zrozumienia istoty tych obiektów. Symptomatyczna wydaje się zwłaszcza definicja „systemów zapewniających ciągłość działania administracji publicznej", której zakres może w praktyce zawierać

---

[26] Ibidem; Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, Dz.U. z 2018 r. poz. 2180.

[27] P. Zaskórski, K. Szwarc, Ł. Tomaszewski, *Bezpieczeństwo informacyjne determinantą ciągłości działania*, [w:] P. Sienkiewicz, H. Świeboda (red.), *Metodologia badań bezpieczeństwa narodowego. Tom 7*, AON, Warszawa 2014; K. Szwarc, P. Zaskórski, *Zapewnianie bezpieczeństwa informacyjnego w systemach zarządzania kryzysowego*, [w:] B. Jagusiak, K. Karski (red. nauk.), *Praktyczne uwarunkowania bezpieczeństwa europejskiego*, WAT, Warszawa 2017.



Rys. 8. Systemy kluczowej infrastruktury państwa
Źródło: opracowanie własne

np. systemy informatyczne, systemy zasilania w energię, obiekty biurowe, kluczowych pracowników czy łączność. Niewiele pod tym względem wyjaśnia załącznik nr 1 do NPOIK z 2013 r., gdzie w praktyce opisano, czym jest administracja publiczna.

2. Wpływ podejścia regulacyjnego na zapewnianie bezpieczeństwa infrastruktury

Na podstawie analizowanej ustawy do polskiego porządku prawnego zaimplementowano wymagania wynikające z Dyrektywy NIS[28] Parlamentu Europejskiego i Rady UE[29]. Przy jej przygotowywaniu sondowano potrzebę wprowadzania zmian dotyczących zwiększania bezpieczeństwa sieci i informacji w UE. W toku konsultacji ocenie poddano trzy warianty[30]:

- utrzymanie dotychczasowego podejścia;
- wdrożenie podejścia regulacyjnego, polegające na przyjęciu wspólnych unijnych ram prawnych dotyczących bezpieczeństwa sieci i informacji;
- zachowanie zasady dobrowolności przy podejmowaniu inicjatyw przez państwa członkowskie, przygotowywane jednak na podstawie wymogów regulacyjnych formułowanych przez instytucje UE.

Syntezy podejścia regulacyjnego dokonano w Narodowym Programie Ochrony Infrastruktury Krytycznej, gdzie zapisano, że jest to podejście, gdzie określa się szczegółowo obowiązki oraz sankcje za ich niedopełnienie[31]. Do dalszego procedowania przyjęto wariant podejścia regulacyjnego, w wyniku którego w 2016 roku przyjęto cytowaną wcześniej Dyrektywę, w której zobowiązano państwa członkowskie do implementacji jej postanowień, zwłaszcza zdefiniowania skutecznych, proporcjonalnych i odstraszających sankcji oraz poinformowania KE o takich przepisach i środkach do 9 maja 2018 r.[32] Zatem zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa kara za nierespektowanie przepisów ustawy przez operatora usługi kluczowej lub dostawcę usługi cyfrowej wynosi, w zależności od niedotrzymanego obowiązku, od 1 do 200 tys. zł.

Ponadto przewidziano, że podmiot, który uporczywie uchyla się od stosowania przepisów ustawy i powoduje:

---

28 *Network and Information Security.*

29 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U. UE, L194/1.

30 Komunikat 48 (2013), Wniosek w sprawie Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, Komisja Europejska, Bruksela 2013, pkt 2.

31 Narodowy Program…, op. cit., RCB, Warszawa 2013, s. 7.

32 Dz.U. UE, L194/1, art. 21.

- „bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
- zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych"[33]

może podlegać karze do 1 000 000 zł, na podstawie decyzji organu właściwego ds. cyberbezpieczeństwa. Organ ten ma również prawo do ukarania kierownika operatora usługi kluczowej, jeżeli ten nie dochował należytej staranności przy spełnianiu ustawowych obowiązków, karą w wysokości nieprzekraczającej 200% miesięcznego uposażenia. Jak można przeczytać w załączniku do komunikatu Komisji do Parlamentu Europejskiego i Rady w dyrektywie przyjęto **podejście regulacyjne oparte na analizie ryzyka**[34]. Z art. 17 dyrektywy wynika bowiem, że organy państw członkowskich UE zostały zobowiązane do wykonywania kontroli nadzorczej w ujęciu *ex post*[35].

W celu ustalenia preferowanego podejścia dokonano analizy pozostałych regulujących to zagadnienie aktów prawnych w Polsce. W art. 48 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia stwierdza się, że podmioty niewywiązujące się z obowiązku ochrony takich obiektów mogą podlegać **karze grzywny lub karze ograniczenia albo pozbawienia wolności do 2 lat**[36]. W tym sensie **wątpliwości może budzić** opisane w Narodowym Programie Ochrony Infrastruktury Krytycznej (NPOIK) **bezsankcyjne podejście do zapewniania bezpieczeństwa systemów infrastruktury krytycznej** przez jej operatorów. O ile bowiem **w ustawie o zarządzaniu kryzysowym rzeczywiście nie opisano sankcji** wynikających z nieprzestrzegania przepisów ustawy, o tyle **zaliczenie tych systemów do obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie w praktyce daje podstawę prawną do wyciągania takich konsekwencji**.

Zarówno w ustawie o powszechnym obowiązku obrony RP, jak i rozporządzeniu Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, a także ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych nie określa się sankcji przewidzianych za niewywiązanie się z przepisów dotyczących ochrony wymienionych w niej obiektów.

---

[33] Dz.U. z 2018 r. poz. 1560, art. 73, ust. 5.

[34] Załącznik do komunikatu komisji do Parlamentu Europejskiego i Rady: *Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* COM(2017) 476, s. 40.

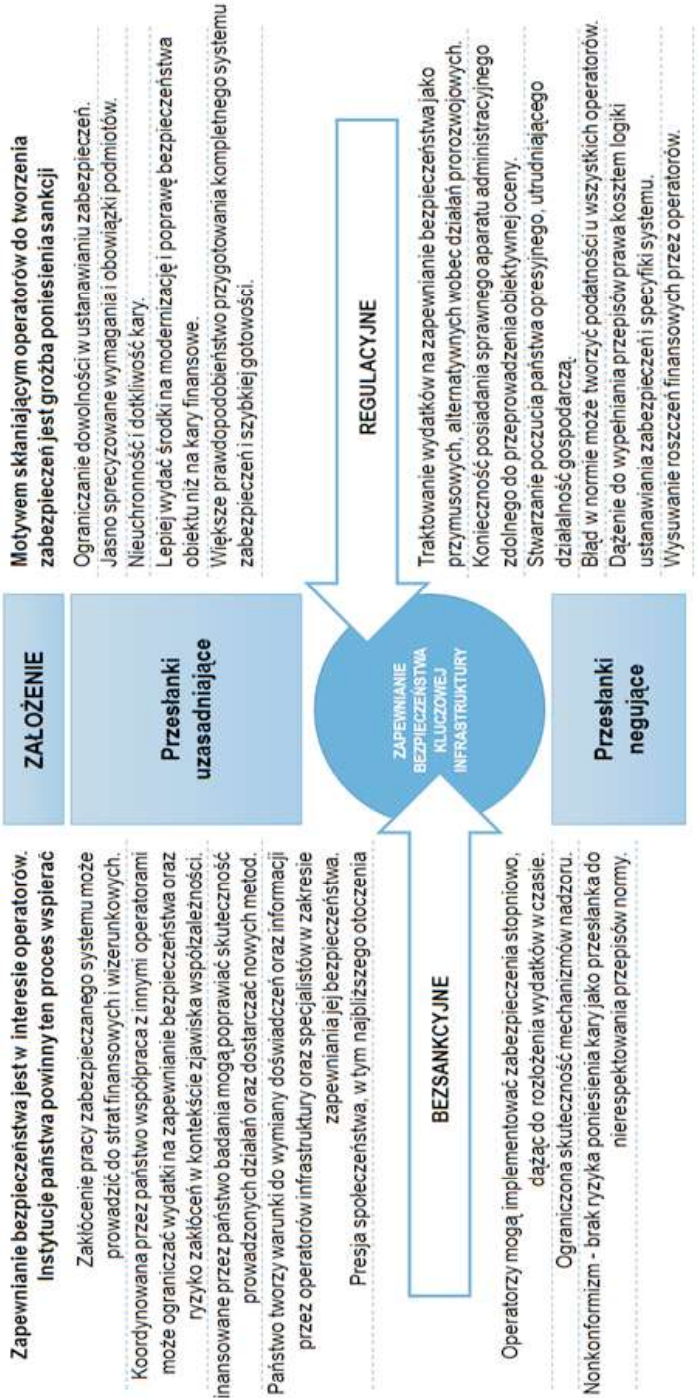
[35] Dz.U. UE, L194/1, art. 17.

[36] Dz.U. 2018 poz. 2142, art. 48.

Na podstawie dokonanej analizy można zastanawiać się, jakie przesłanki uzasadniają wybór lub odrzucenie danego podejścia. Na rysunku 9 przedstawiono argumenty dotyczące zarówno podejścia regulacyjnego, jak i bezsankcyjnego.

Przyjęto, że podstawowym motywem skłaniającym do wyboru podejścia **bezsankcyjnego** jest wspólne rozpatrywanie przez wszystkie zainteresowane strony zakłócenia pracy infrastruktury jako zjawiska negatywnego, które przynosi straty. W interesie wszystkich stron jest zatem przeciwdziałanie takim zjawiskom. Biorąc pod uwagę złożoność, rozległość i współzależność analizowanych w artykule systemów (rys. 8), przyjęto, że w takim podejściu należy silnie akcentować walor współpracy, organizowanej i koordynowanej przez państwo. Jego instytucje mogą ponadto wspierać operatorów z sektora prywatnego poprzez inwestycje w prace badawczo-rozwojowe, dostarczające nowych metod rozwiązywania problemów zapewniania bezpieczeństwa. Organizowana przez państwo współpraca może zatem prowadzić do ograniczania nakładów na ustanawianie systemów bezpieczeństwa. Do wad takiego podejścia zaliczono z kolei ryzyko wydłużenia czasu gotowości ustanawianych zabezpieczeń oraz ograniczenie skuteczności mechanizmów kontrolnych. Brak motywacji negatywnej może ponadto wzmagać zjawisko nonkonformizmu, silnie warunkowane w Polsce czynnikami kulturowymi.

Skuteczność motywacji negatywnej stanowi podstawowe założenie podejścia **regulacyjnego**. Jako zasadniczą przesłankę w jego stosowaniu można uznać przewidywalność zachowania operatora i standaryzację ustanawianych zabezpieczeń. Podejście to opiera się na jasno zdefiniowanych obowiązkach oraz konsekwencjach, jakie niesie ich niewypełnianie. Te przesłanki silnie determinują kompletność zakładaną w dokumencie normatywnym, a więc planowaną gotowość wdrożenia systemu. Standaryzację można jednocześnie traktować jako wadę w przypadku, gdy będące jej podstawą założenia są niepoprawne. Może to bowiem prowadzić do jednoczesnego powstania podatności u dużej liczby operatorów. Stosowanie narzędzi motywacji negatywnej może prowadzić do utożsamiania wydatków na bezpieczeństwo z kosztem alternatywnym działań prorozwojowych, a państwa jako instytucji opresyjnej, hamującej swobodę prowadzenia działalności gospodarczej. W związku z narzucanymi obowiązkami, operatorzy mogą występować z mniej lub bardziej uzasadnionymi roszczeniami wobec państwa lub przenosić koszty ustanawiania zabezpieczeń na konsumentów.



Rys. 9. Przesłanki uzasadniające i negujące zastosowanie analizowanych rodzajów podejścia
Źródło: opracowanie własne

3. Wnioski

Ochrona kluczowych obiektów to jedno z podstawowych zadań systemów bezpieczeństwa narodowego współczesnych państw. Z perspektywy zarządzania kryzysowego takim zadaniem jest ochrona systemów infrastruktury krytycznej. Problem ten może być jednak postrzegany z punktu widzenia różnych dyscyplin naukowych. Aktualny wydaje się być zatem zasygnalizowany w literaturze problem uporządkowania badanych zagadnień na styku: ogólnej teorii ryzyka, zarządzania ryzykiem operacyjnym, logistki społecznej oraz publicznego zarządzania kryzysowego[37].

Na podstawie przedstawionych przesłanek trudno jednoznacznie stwierdzić, które z analizowanych podejść może istotnie poprawić skuteczność działań związanych z zapewnianiem bezpieczeństwa kluczowej infrastruktury. Zarówno przy formułowaniu Narodowego Programu Infrastruktury Krytycznej, jak i prezentowanej w artykule dyrektywy NIS zwracano uwagę na nieskuteczność przeciwstawnego podejścia.

Na podstawie przeprowadzonej analizy aktów prawnych nie można zresztą jednoznacznie orzec, czy zaliczenie infrastruktury krytycznej do obiektów podlegających obowiązkowej ochronie daje podstawy do postrzegania ochrony infrastruktury krytycznej jako podejścia bezsankcyjnego. Rozstrzygająca w tym przypadku wydaje się być praktyka stosowania prawa, której oceny będzie można dokonać dopiero po pewnym czasie.

Należy zauważyć, że w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego RP2022 „zidentyfikowano słabość metody nakładania na operatorów infrastruktury krytycznej obowiązków w drodze ustaw bądź rozporządzeń, ze względu na brak możliwości prowadzenia audytu i kontroli ich realizacji"[38]. W konsekwencji przyjęto, że większą uwagę należy zwrócić na podnoszenie świadomości operatorów infrastruktury krytycznej oraz traktować współodpowiedzialność jako najważniejszą zasadę tworzonego NPOIK.

Warto również podkreślić, że zastosowane przy ustanawianiu zabezpieczeń przez operatorów usług kluczowych i dostawców usług cyfrowych podejście regulacyjne nie zostało poparte wnioskami z funkcjonowania NPOIK, ale wprost – implementacji wytycznych dyrektywy NIS. Nie powinno zatem stanowić przesłanki rozstrzygającej do oceny drugiego podejścia.

---

[37] J. Zawiła-Niedźwiecki, *Od zarządzania ryzykiem operacyjnym do publicznego zarządzania kryzysowego. Wyzwania badawcze*, edu-Libri, Kraków-Legionowo 2018, s. 15-20.

[38] Załącznik do uchwały Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia *Strategii rozwoju Systemu Bezpieczeństwa Narodowego RP 2022*, MP z 2013 r., poz. 377.

BIBLIOGRAFIA

[1] Brzozowska K., *Finansowanie inwestycji infrastrukturalnych przez kapitał prywatny na zasadzie project finance*, CeDeWu, Warszawa 2009.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U. UE, L194/1.

[3] Frischmann B., *Infrastructure. The Social Value of Shared Resources*, Oxford University Press, New York 2012.

[4] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-obiektow-infrastruktury-krytycznej.html

[5] Komunikat 48 (2013), Wniosek w sprawie Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, Komisja Europejska, Bruksela 2013.

[6] *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013.

[7] *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2015.

[8] *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2018.

[9] *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, RCB, Warszawa 2018.

[10] *Nowy słownik języka polskiego*, PWN, Warszawa 2002.

[11] Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Ossolineum, Wrocław, Warszawa, Kraków, Gdańsk 1978.

[12] Radziejewski R., *Ochrona infrastruktury krytycznej. Teoria a praktyka*, PWN, Warszawa 2014.

[13] Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. z 2018 r. poz. 1780.

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

[15] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz.U. z 2018 r. poz. 1806.

[16] Rozporządzenie Rady Ministrów z dnia 16 grudnia 2016 r. zmieniające rozporządzenie w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2017 r. poz. 42.

[17] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz.U. z 2018 r. poz. 2080.

[18] Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. z 2003 r. nr 116, poz. 1090.

[19] Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym, Dz.U. z 2004 r. nr 98, poz. 978.

[20] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz.U. z 2010 r. nr 83, poz. 542.

[21] Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, Dz.U. z 2018 r. poz. 2180.

[22] Szwarc K., *Współzależność jako wyzwanie w aspekcie ochrony infrastruktury krytycznej*, [w:] Z. Czachór, A. Chabasińska (red. nauk.), *Bezpieczeństwo narodowe Polski. Zagrożenia i determinanty zmian*, Difin, Warszawa 2016.

[23] Szwarc K., Zaskórski P., *Modelowanie procesów zapewniania bezpieczeństwa i ciągłości działania organizacji administracji publicznej*, „Studia Bezpieczeństwa Narodowego" nr 12, WAT, Warszawa 2017.

[24] Szwarc K., Zaskórski P., *Zapewnianie bezpieczeństwa informacyjnego w systemach zarządzania kryzysowego,* [w:] B. Jagusiak, K. Karski (red. nauk.), *Praktyczne uwarunkowania bezpieczeństwa europejskiego,* WAT, Warszawa 2017.

[25] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. z 2018 r. poz. 452.

[26] Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu, Dz.U. 2001 nr 27, poz. 298 z późn. zm.

[27] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia Dz.U. 2018 poz. 2142.

[28] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2018 r. poz. 1401.

[29] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r. poz. 1560.

[30] Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, Dz.U. z 2018 r. poz. 138 z późn. zm.

[31] *Webster's New English Dictionary and Thesaurus for Home*, REA, Warszawa 2005.

[32] Załącznik do komunikatu komisji do Parlamentu Europejskiego i Rady: *Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii COM* (2017) 476.

[33] Załącznik do uchwały Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia *Strategii rozwoju Systemu Bezpieczeństwa Narodowego RP2022*, MP z 2013 r., poz. 377.

[34] Zaskórski P., Szwarc K., Tomaszewski Ł., *Bezpieczeństwo informacyjne determinantą ciągłości działania,* [w:] P. Sienkiewicz, H. Świeboda (red.), *Metodologia badań bezpieczeństwa narodowego. Tom 7,* AON, Warszawa 2014.

[35] Zawiła-Niedźwiecki J., *Od zarządzania ryzykiem operacyjnym do publicznego zarządzania kryzysowego. Wyzwania badawcze*, edu-Libri, Kraków–Legionowo 2018.

NATIONAL KEY INFRASTRUCTURE PROTECTION – SANCTION-FREE OR REGULATORY APPROACH?

Summary. The article characterizes and analyses the national key infrastructure. It presents the recommendations and requirements for national key infrastructure protection. According to the national legislation, both regulatory and sanction-free approach were stressed. Based on comparative analysis of both approaches advantages and disadvantages were presented.

Keywords: national key infrastructure, regulatory approach, sanction-free approach, key infrastructure protection.