**Maciej Brocki**
orcid.org/
0000-0003-0640-4412

# Narodowy Program Ochrony Infrastruktury Krytycznej 2018 w kształtowaniu bezpieczeństwa Rzeczypospolitej Polskiej

## Wprowadzenie

We współczesnym świecie rozwój poszczególnych państw w dużej mierze zależny jest od ciągłego „tworzenia" bezpieczeństwa, które przez liczne, wielopłaszczyznowe przedsięwzięcia ma zapewnić skuteczną ochronę interesu narodowego. Pojęcie bepieczeństwo, mimo iż ma wiele definicji, a jego problematyka znajduje się w zainteresowaniu wielu nauk, m.in.: społecznych, humanistycznych czy ekonomicznych, można krótko scharakteryzować jako wolność oraz umiejętność ochrony i obrony przed zagrożeniami[1]. Istota bezpieczeństwa została zdefiniowana przez Ryszarda Kuźniara w następujący sposób: „Jest ono pierwotną potrzebą jednostek, grup społecznych, wreszcie państw"[2]. Zapewnienie jego odpowiedniego poziomu jest kluczowym zadaniem każdego demokratycznego państwa. Na przestrzeni ostatnich lat stało się ono priorytetem wszystkich rządów, jak również organizacji międzynarodowych. Za ważny element bezpieczeństwa każdego narodu należy uznać infrastrukturę krytyczną, która została zdefiniowana w Polsce w 2007 r. wraz z wejściem w życie ustawy o zarządzaniu kryzysowym. Należy w tym miejscu podkreślić, że zapewnienie odpowiedniej ochrony infrastruktury krytycznej pozwala swobodnie i bezpiecznie funkcjonować każdemu obywatelowi, umożliwiając niezależny dostęp do wielu dziedzin życia, takich jak m.in.: pomoc lekarska, dostarczenie energii czy możliwość korzystania z innych powszechnych dóbr, typu usługi telekomunikacyjne, transportowe. Wszelkie nieprawidłowości oraz jakiekolwiek uszkodzenia elementów infrastruktury krytycznej mogą nieść poważne zaburzenia dla wielu sektorów państwa, jak i poszczególnych jego obywateli. W niniejszym artykule zostanie przybliżona tematyka infrastruktury krytycznej, obecności tego terminu w polskich przepisach prawa oraz

[1] A. Skrabacz, *Organizacje pozarządowe wobec wyzwań i zagrożeń bezpieczeństwa narodowego Polski w XXI wieku*, Warszawa 2006, s. 7.

[2] R. Kuźniar, *Po pierwsze bezpieczeństwo*, „Rzeczpospolita" z 9.01.1996 r.

przedstawiony będzie *Narodowy Program Ochrony Infrastruktury Krytycznej 2018* (dalej: NPOIK 2018), którego najważniejszym celem jest podniesienie bezpieczeństwa Rzeczypospolitej Polskiej. Program ten adresowany jest szczególnie do administracji rządowej oraz operatorów infrastruktury krytycznej, lecz postanowienia NPOIK 2018 mogą być stosowane również przez samorządy i podmioty prywatne, niebędące operatorami infrastruktury krytycznej.

## Infrastruktura krytyczna w Polsce

Problematyka infrastruktury krytycznej, a co za tym idzie – jej ochrony pojawiła się w Polsce w momencie przygotowań naszego kraju do wstąpienia w struktury NATO w roku 2002. Przystąpienie naszego kraju do Paktu Północnoatlantyckiego wymagało dostosowania procedur oraz norm prawnych w aspekcie ochrony infrastruktury krytycznej[3]. Mimo iż tematyka infrastruktury krytycznej w tym okresie traktowana była już jako jeden z kluczowych elementów, który może mieć wpływ na stabilność bezpieczeństwa narodowego, jak również spokój poszczególnych obywateli, brakowało zdefiniowania tego pojęcia. W wypracowaniu i sprecyzowaniu definicji, jak również określeniu kluczowych sektorów społeczno-gospodarczych, które obejmie infrastruktura krytyczna, pomogły doświadczenia innych państw. Należy tu wymienić USA czy Wielką Brytanię, które dużo wcześniej podjęły prace mające na celu zwiększenie bezpieczeństwa infrastruktury krytycznej lub też, jak Kanada, same doświadczyły zagrożeń związanych z awariami zasilania w roku 2003. Początkowe definicje infrastruktury krytycznej zbieżne były z teminem „samej" infrastruktury i określały ją jako „zespół podstawowych urządzeń i instytucji usługowych niezbędnych do należytego funkcjonowania produkcyjnych działów gospodarki"[4]. Kolejne pojawiające się opracowania poświęcone zagadnieniom infrastruktury krytycznej wprowadzały bardziej rozbudowane oraz bliższe obecnej definicji stwierdzenia, że infrastruktura krytyczna to: „urządzenia, instalacje i usługi, powiązane ze sobą więzami funkcjonalnymi, kluczowe dla bezpieczeństwa państwa i jego obywateli oraz zapewnienia sprawnego funkcjowania organów władzy i administracji publicznej, a także instytucji i przedsiębiorców"[5]. Dopiero po wejściu w życie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym w 2007 r. zostało wprowadzone do polskiego prawa pojęcie infrastruktury krytycznej, które zostało określone jako „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 publicz-

[3] A. Tyburska, *Ochrona infrastruktury krytycznej w Polsce – wyzwania w tworzeniu bezpieczeństwa narodowego*, Warszawa 2013, s. 87.

[4] W. Wojciechowicz, *Ochrona infrastruktury krytycznej państwa*, „Myśl Wojskowa" 2004, nr 1, s. 10.

[5] W. Wójtowicz, *Bezpieczeństwo infrastruktury krytycznej*, Warszawa 2006, s. 65.

nej, a także instytucji i przedsiębiorców”[6]. Warto podkreślić że, powyższa definicja jest obecnie powszechnie przywoływana w podręcznikach akademickich, opracowaniach naukowych czy dokumentach doktrynalnych, jak również przez osoby i środowiska akademickie zajmujące się tą problematyką. Rządowe Centrum Bezpieczeństwa, które jest koordynatorem ochrony infrastruktury krytycznej na szczeblu krajowym, zwięźle definiuje przedmiotowe pojęcie jako rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa. Nie każdy strategiczny obiekt należy do infrastruktury krytycznej[7]. Ponadto w ustawie o zarządzaniu kryzysowym podano, że infrastrukturę krytyczną stanowią systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[8].

System zaopatrzenia w energię, surowce energetyczne i paliwa należy uznać za kluczowy w funkcjonowaniu gospodarki i społeczeństwa, i jest on uznawany za szczególny dla prawidłowej działalności państwa. System ten swym zasięgiem obejmuje elektrownie, stacje elektroenergetyczne, obiekty przesyłu gazu, energetyczne sieci przemysłowe, kopalnie węgla i zakłady wydobywające kopaliny, bazy i magazyny paliw, obiekty przesyłu i przeróbki paliw, a także całość urządzeń, które dostarczają energię do odbiorców. O tym, jak ważny jest system zaopatrzenia w energię, surowce energetyczne i paliwa, świadczyć może stopień uzależnienia poszczególnych jednostek społeczeństwa, jak i całej gospodarki od energii elektrycznej. Każde zakłócenie w dostawie energii elektrycznej byłoby przyczyną problemów w kluczowych dziedzinach życia społeczno-gospodarczego[9].

Systemy łączności odpowiadają za zapewnienie przekazu informacji, obejmują pocztę oraz telekomunikację, w tym łączność telefoniczną (telefonię stacjonarną i mobilną), dostęp do internetu, jak również radiofonię i telewizję. Jako telekomunikację należy postrzegać nadawanie, odbiór, transmisję informacji za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną. Stały dostęp do łączności oraz brak zakłóceń tego systemu jest bardzo ważnym elementem każdego nowoczesnego państwa. Ma on znaczny wpływ na rozwój gospodarki, jak również pozwala bezproblemowo przekazywać informacje między obywatelami czy obywatelami a organami administracji[10].

System sieci teleinformatycznych zgodnie z definicją przedstawioną w ustawie o świadczeniu usług drogą elektroniczną to: „zespół współpracujących ze sobą

[6] Dz.U. z 2007 r. nr 89, poz. 590.

[7] *Infrastruktura krytyczna*, https://rcb.gov.pl/infrastruktura-krytyczna [dostęp: 5.02.2019].

[8] Dz.U. z 2007 r. nr 89, poz. 590.

[9] Szerzej na ten temat: *Narodowy Program Ochrony Infrastruktury Krytycznej 2013* [Warszawa 2013] (dalej cyt.: NPOIK 2013), zał. nr 1. *Charakterystyka systemów infrastruktury krytycznej*, Warszawa 2013, s. 4–26.

[10] Tamże, s. 27.

urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego"[11]. Są to przede wszystkim sieci teleinformacyjne czy też systemy teleinformatyczne przeznaczone do przetwarzania, zbierania różnorodnych danych, wykorzystywane przez administrację publiczną do swoich ustawowych zadań[12].

Systemy finansowe są niezwykle ważne dla właściwego rozwoju i funkcjonowania państwa, wpływają znacząco na ekonomiczny byt kraju. Należy je rozumieć jako ogół norm prawnych oraz zespół instytucji finansowych, odpowiadających za gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa. Systemy finansowe składają się z następujących segmentów: budżetowego, bankowego, ubezpieczeniowego oraz kapitałowego[13].

Systemy zaopatrzenia w żywność są dziedziną gospodarki, która odpowiedzialna jest za wytworzenie środków produkcyjnych, takich jak: pasze, nawozy, usługi dla rolnictwa, czy też produkcję oraz pozyskiwanie surowców żywnościowych. Kontroluje ona również skup surowców żywnościowych, przetwórstwo surowców żywnościowych, obrót towarami, produktami żywnościowymi oraz system bezpieczeństwa żywności. System zaopatrzenia w żywność jest głównym filarem gospodarki narodowej, który z kolei wpływa na bezpieczeństwo ekonomiczne państwa. Kluczowym celem systemu jest zapewnienie wyżywienia narodu[14].

W skład systemów zaopatrzenia w wodę wchodzą systemy, instalacje, urządzenia i obiekty służące pobieraniu, oczyszczaniu, uszlachetnianiu, a przede wszystkim dostarczaniu wody dla potrzeb pojedyńczych obywateli, jak również przemysłu. Zaopatrzenie w wodę oraz odbiór ścieków jest jedną z najważniejszych usług, która ma zapewnić właściwe funkcjonowanie społeczności[15].

Kolejnym ważnym z punktu widzenia potrzeb społeczeństwa systemem infrastruktury krytycznej jest system ochrony zdrowia. Jest to zespół osób i instytucji, który ma za zadanie zapewnić opiekę zdrowotną ludności, a jego sprawne funkcjonowanie wspólnie z systemem ratowniczym jest gwarantem praw obywatela zapisanych w konstytucji. Głównymi elementami ze względu na dostępność systemu są podmioty lecznicze oraz Narodowy Fundusz Zdrowia[16]. W tym miejscu należy wspomnieć o kolejnym systemie, który jest ściśle związany z systemem ochrony zdrowia. Jest to ratownictwo, które postrzegane jest jako ogół środków, przedsięwzięć organizacyjnych podejmowanych w celu ratowania zdrowia i życia, mienia i środowiska. W ramach systemu ratownictwa w Polsce funkcjonują: Krajowy System Ratowniczo-Gaśniczy, Państwowe Ratownictwo Medyczne, System Powiadamiania Ratunkowego, ratownictwo górskie, ratownictwo morskie,

[11] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r. nr 144, poz. 1204 ze zm.

[12] NPOIK 2013, s. 36.

[13] Tamże, s. 37–41.

[14] Tamże, s. 42–57.

[15] Tamże, s. 58–59.

[16] Tamże, s. 60–61.

ratownictwo górnicze, ratownictwo wodne, Krajowy System Wykrywania Skażeń i Alarmowania[17].

Systemy transportowe to sieć wzajemnie powiązanych ze sobą dróg oraz pracujące tam różne rodzaje transportu. Jest to zarówno przemieszczanie ludzi, jak i ładunków przy wykorzystaniu odpowiednich środków transportu. Cały system transportu ma ogromny wpływ na współczesną gospodarkę i społeczeństwo, dlatego jego sprawne funkcjonowanie stanowi jeden z filarów nowoczesnego państwa. Ogólnie transport można podzielić na transport pasażerski, czyli komunikację, i transport towarowy[18].

W skład infrastruktury krytycznej wchodzą również systemy zapewniające ciągłość działania administracji publicznej, do których należy zaliczyć obiekty urzędów administracji, służb, inspekcji, agencji i straży czy też sądy. Administrację publiczną w Polsce tworzy administracja rządowa i samorządowa[19].

Ostatnim elementem, który tworzy infrastrukturę krytyczną, są systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Są to m.in. obiekty jądrowe i źródła promieniowania jonizującego, rurociągi substancji niebezpiecznych, jak również sieci transportu, przesyłu i dystrybucji, składy i magazyny tych substancji[20].

Systemy te zostały szczegółowo scharakteryzowane w załączniku do NPOIK 2013, gdzie ukazano istotę każdego z nich. Podczas analizy tychże systemów oraz wchodzących w ich skład obiektów, urządzeń czy instalacji i usług należy wskazać, że mają one ogromny wpływ na możliwość rozwoju państwa.

Definicja infrastruktury krytycznej, jak również wymienione systemy stanowiące infrastrukturę krytyczną w kolejnych nowelizacjach ustawy o zarządzaniu kryzysowym były korygowane. Świadczy to o złożonym charakterze zagadnienia, a także fakcie, iż jest ona kluczową częścią infrastruktury państwa, która w przypadku zakłóceń jej funkjonowania może powodować zagrożenie dla bezpieczeństwa narodowego RP.

Wraz z wejściem w życie ustawy o zarządzaniu kryzysowym zostało również zdefiniowane pojęcie ochrony infrastruktury krytycznej, zgodnie z którą jest to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia infrastruktury krytycznej na wypadek zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie[21]. Powyższe pojęcie, tak jak w przypadku definicji infrastruktury krytycznej, wraz z kolejnymi nowelizacjami ustawy było modyfikowane szczególnie w kwestii zapewnienia nie tylko funkcjonalności, ale także ciągłości działania

[17] Tamże, s. 67–69.
[18] Tamże, s. 62–66.
[19] Tamże, s. 70–73.
[20] Tamże, s. 74–77.
[21] Dz.U. z 2007 r. nr 89, poz. 590.

elementów kluczowych infrastruktury krytycznej[22]. Wszystkie elementy wymienione w definicji ochrony infrastruktury krytycznej są ze sobą ścisle powiązane i zależne od siebie. Skutki zaniedbań w sferze ochrony infrastruktury krytycznej mogą nieść ogromne straty dla państwa i obywateli, jak również gospodarki. Zgodnie z NPOIK 2013 ochrona infrastruktury krytycznej obejmuje ochronę: fizyczną, techniczną, osobową, teleinformatyczną, prawną oraz plany odbudowy.

Zagadnienia dotyczące ochrony infrastruktury krytycznej zostały również zawarte w innych niż ustawa o zarządzaniu kryzysowym regulacjach prawnych. Jednym z takich aktów prawnych jest ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, która nakazuje współpracę właścicieli i posiadaczy obiektów, instalacji, urządzeń infrastruktury krytycznej z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych. Ustawa ta zobowiązuje operatorów obiektów infrastruktury krytycznej do niezwłocznego przekazania szefowi Agencji Bezpieczeństwa Wewnętrznego informacji na temat zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej. Kolejne uregulowania dotyczące ochrony infrastruktury krytycznej zostały przyjęte w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych. Obydwie te ustawy wprowadziły szereg uzgodnień i form współpracy między operatorami infrastruktury krytycznej a poszczególnymi podmiotami odpowiedzialnymi za cyberbezpieczeństwo czy też działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych.

## Cele, priorytety oraz założenia *Narodowego Programu Ochrony Insfrastruktury Krytycznej 2018*

*Narodowy Program Ochrony Insfrastruktury Krytycznej 2018* (NPOIK 2018) powstał na podstawie art. 5b ust. 1 ustawy o zarządzaniu kryzysowym, gdzie wskazano, że Rada Ministrów ma w drodze uchwały przyjąć powyższy program. Jest to dokument opracowywany na szczeblu centralnym przez Rządowe Centrum Bezpieczeństwa. Został on przygotowany z uwzględnieniem obowiązujących w Polsce przepisów prawnych, jak również dostosowany do przepisów międzynarodowych w związku z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego, Organizacji Bezpieczeństwa i Współpracy w Europie oraz innych organizacjach międzynarodowych[23]. Sposób realizacji obowiązków i współpracy w zakresie NPOIK 2018 przez organy administracji publicznej, służby odpowiedzialne za bezpieczeństwo

[22] A. Tyburska, dz. cyt., s. 98.

[23] *Narodowy Program Ochrony Insfrastruktury Krytycznej 2018* [Warszawa 2018] (dalej cyt.: NPOIK 2018), s. 8.

narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej określa rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie NPOIK 2018[24]. Program określa wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań, integralności infrastruktury krytycznej państwa. Celem tych działań jest zapobieganie zagrożeniom, ryzyku, słabym punktom oraz ograniczenie ich skutków i szybkie odtworzenie infrastruktury na wypadek awarii, ataków czy innych zdarzeń, które mogą zakłócić jej prawidłowe funkcjonowanie[25]. Poddany analizie *Narodowy Program Ochrony Insfrastruktury Krytycznej 2018* został wprowadzony uchwałą nr 121/2018 Rady Ministrów z dnia 7 września 2018 r. zmieniającej uchwałę w sprawie przyjęcia NPOIK. Stanowi on czwartą aktualizację pierwotnego dokumentu, który został przyjęty w 2013 r.

W NPOIK 2018 jako nadrzędny cel zostało wskazane podniesienie bezpieczeństwa Polski. Wyszczególnione zostały również cele pośrednie, bez których niemożliwe będzie zrealizowanie celu nadrzędnego. Są to:

- zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia infrastruktury krytycznej dla sprawnego funkcjonowania państwa oraz sposobów i metod jej ochrony,
- wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach,
- wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony infrastruktury krytycznej,
- budowa partnerstwa między uczestnikami procesu ochrony infrastruktury krytycznej, wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony infrastruktury krytycznej[26].

Obowiązujący program wskazuje również trzy priorytety, które mają mieć kluczowe znaczenie dla osiągnięcia celów wskazanych w NPOIK 2018:

- pogłębienie współpracy między uczestnikami programu w obszarze ochrony infrastruktury krytycznej,
- identyfikacja zależności między systemami infrastruktury krytycznej,
- dokonanie oceny ryzyka zakłócenia funkcjonowania systemu infrastruktury krytycznej[27].

NPOIK 2018 nie przewiduje sankcji w przypadku niedopełnienia obowiązków dla uczestników ochrony infrastruktury krytycznej, gdyż autorzy kwestionują skuteczność podejścia regulacyjnego, które jasno wskazuje odpowiednie sankcje za poszczególne uchybienia. Powyższe założenie ma ułatwić osiągnięcie celów pro-

[24] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. z 2010 r. nr 83, poz. 541.

[25] W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, *Ochrona infrastruktury krytycznej*, Warszawa 2012, s. 41.

[26] NPOIK 2018, s. 8.

[27] Tamże, s. 9.

gramu. Jednocześnie program przewiduje możliwość wprowadzenia szczegółowych uregulowań prawnych w przypadku negatywnej oceny NPOIK 2018[28]. Ryszard Radziejewski podkreśla, że choć program wyczerpuje problematykę infrastruktury krytycznej, to przez zawarte w nim podejście bez stosowania sankcji „nie ma mocy sprawczej"[29]. Dokument wskazał również najważniejsze filary i zasady programu, którymi są:

- współodpowiedzialność – wiodąca zasada przyjęta przy budowie systemu ochrony infrastruktury krytycznej. Rozumiana jest jako wspólne (zbiorowe) dążenie do poprawy bezpieczeństwa infrastruktury krytycznej wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów infrastruktury krytycznej, społeczeństwa, gospodarki i w konsekwencji państwa. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno jej operatorów, jak i odpowiedzialnej za funkcjonowanie państwa administracji,
- współpraca – drugi filar systemu ochrony infrastruktury krytycznej. W kontekście programu oznacza wykonywanie razem przez uczestników ochrony infrastruktury krytycznej określonych, zbieżnych i wzajemnie uzupełniających się zadań dla osiągnięcia wspólnego celu, który wynika z zasady współodpowiedzialności. Współpraca jest niezbędna w przypadku chęci uniknięcia powielania działań i ponoszonych kosztów oraz efektywniejszego wykorzystania posiadanych sił i środków,
- zaufanie – trzeci filar systemu ochrony infrastruktury krytycznej. W programie rozumiane jako przekonanie, że motywacją działania uczestników ochrony infrastruktury krytycznej (dotyczy to w szczególności administracji i operatorów infrastruktury krytycznej) jest dążenie do wspólnego celu – poprawy bezpieczeństwa infrastruktury krytycznej i RP. Osiągnięcie tego celu będzie zatem korzystne dla wszystkich zainteresowanych stron, w tym przede wszystkim społeczeństwa. Zaufanie jest niezbędne do osiągnięcia celów programu[30].

Program kieruje się również zasadami:

- proporcjonalności i działań opartych na ocenie ryzyka – działania nakierowane na podniesienie poziomu ochrony infrastruktury krytycznej powinny być adekwatne do poziomu ryzyka. Dotyczy to zarówno przyjętego modelu ochrony infrastruktury krytycznej, jak i użytych sił i środków. Ocena ryzyka powinna być podstawą określenia standardów ochrony infrastruktury krytycznej i dla ustalenia priorytetów działań,
- uznania różnic między systemami infrastruktury krytycznej – systemy IK cechuje wiele podobieństw, mają jednak pewne unikalne cechy, które w obszarze ochrony infrastruktury krytycznej powinny zostać uwzględnione,

[28] Tamże.

[29] R. Radziejewski, *Ochrona infrastruktury krytycznej, Teoria a parktyka*, Warszawa 2014, s. 66.

[30] NPOIK 2018, s. 9–10.

- wiodącej roli ministra odpowiedzialnego za system infrastruktury krytycznej – inicjatywa zwiększenia poziomu ochrony infrastruktury kluczowej dla funkcjonowania społeczeństwa wyszła ze strony administracji, dlatego powinna ona mieć znaczący udział w działaniach na rzecz poprawy bezpieczeństwa infrastruktury krytycznej. Tę rolę w budowie zaufania i skutecznej współpracy odgrywają ministrowie odpowiedzialni za system infrastruktury krytycznej, niezależnie od obowiązku ochrony infrastruktury krytycznej ciążącego na operatorze infrastruktury krytycznej,
- równości operatorów infrastruktury krytycznej – operatorami infrastruktury krytycznej są zarówno podmioty prywatne, podmioty stanowiące własność państwa, jak i sama administracja. Program nie dokonuje rozróżnień i w jego rozumieniu wszyscy operatorzy są równi i zobowiązani do realizacji tego samego obowiązku – ochrony infrastruktury krytycznej, którą władają,
- komplementarności – w użyciu pozostaje wiele rozwiązań, które skutecznie przyczyniają się do bezpiecznego funkcjonowania infrastruktury krytycznej. Zapisy NPOIK 2018 będą miały charakter uzupełniający w stosunku do istniejących rozwiązań prawno-instytucjonalnych. Nie będą powielały rozwiązań i przyjętych praktyk wynikających z obowiązującego prawa[31].

NPOIK 2018 wskazuje również adresatów programu, którymi w głównej mierze ma być administracja rządowa oraz operatorzy infrastruktury krytycznej[32]. Program ma być aktualizowany nie rzadziej niż co dwa lata, biorąc pod uwagę następujące zmiany otoczenia i uwarunkowania ochrony infrastruktury krytycznej, a przedstawione w nim cele mają zostać zrealizowane w ciągu czterech lat[33]. Program w obecnej formie zawiera dwa załączniki. Pierwszym załącznikiem jest dokument zatytułowany: *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, gdzie zawarte są podstawowe informacje na temat technicznych i organizacyjnych aspektów ochrony infrastruktury krytycznej. Drugim załącznikiem jest dokument zastrzeżony: *Kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej*.

## Podsumowanie

Problematyka infrastruktury krytycznej i jej ochrony ma decydujący wpływ na zapewnienie bezpieczeństwa całego państwa, jak również zapewnienie odpowiedniego standardu życia obywatelom Rzeczypospolitej Polskiej. NPOIK 2018 jest bez wątpienia kluczowym dokumentem z zakresu ochrony infrastruktury krytycznej. W sposób klarowny uporządkował zagadnienia z omawianej dziedziny. W programie została właściwie zidentyfikowana infrastruktura krytyczna, wskazano organy i podmioty biorące udział w jej tworzeniu. Gdy analizuje się NPOIK

[31] Tamże, s. 10.
[32] Tamże, s. 11.
[33] Tamże, s. 12.

2018, należy poruszyć kwestię odpowiedniej współpracy operatorów infrastruktury krytycznej sektora prywatnego z administracją publiczną, gdyż zapisy programu nie przewidziały żadnych sankcji w przypadku niewłaściwego wywiązywania się z obowiązków określonych w ustawie. W podsumowaniu programu, jak również pozostałych rozważań dotyczących infrastruktury krytycznej należy pamiętać o postępującym rozwoju technologicznym i cywilizacyjnym, który wymusza ciągłą kontrolę nad obiektami i urządzeniami infrastruktury krytycznej.

## Bibliografia

**Akty prawne, dokumenty:**

*Narodowy Program Ochrony Infrastruktury Krytycznej 2013* [Warszawa 2013].

*Narodowy Program Ochrony Infrastruktury Krytycznej 2018* [Warszawa 2018].

Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. z 2010 r. nr 83, poz. 541.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r. nr 144, poz. 1204 ze zm.

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

**Monografie:**

Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej*, Warszawa 2012.

Radziejewski R., *Ochrona infrastruktury krytycznej. Teoria a parktyka*, Warszawa 2014.

Skrabacz A., *Organizacje pozarządowe wobec wyzwań i zagrożeń bezpieczeństwa narodowego Polski w XXI wieku*, Warszawa 2006.

Tyburska A., *Ochrona infrastruktury krytycznej w Polsce – wyzwania w tworzeniu bezpieczeństwa narodowego*, Warszawa 2013.

Wójtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, Warszawa 2006.

**Artykuły naukowe:**

Wojciechowicz W., *Ochrona infrastruktury krytycznej państwa*, „Myśl Wojskowa" 2004, nr 1.

**Artykuły prasowe:**

Kuźniar R., *Po pierwsze bezpieczeństwo*, „Rzeczpospolita" z 9.01.1996 r.

**Źródła internetowe:**

*Infrastruktura krytyczna*, https://rcb.gov.pl/infrastruktura-krytyczna.

**Streszczenie:**

Infrastruktura krytyczna, mimo iż jest obecna stosunkowo od niedawna w polskich przepisach prawa, odgrywa kluczową rolę w funkcjonowaniu państwa, jak również w życiu poszczególnych obywateli. Ochrona infrastruktury krytycznej należy do priorytetów stojących przed każdym państwem, również polskim. Podmioty realizujące zadania

z zakresu ochrony infrastruktury krytycznej mają za zadanie nie tylko zapewnienie należytego jej zabezpieczenia, ale dodatkowo są zobowiązane do szybkiego oraz całkowitego usunięcia uszkodzeń lub zakłóceń w przypadku ich wystąpienia. Celem artykułu jest wskazanie roli Narodowego Programu Ochrony Infrastruktury Krytycznej w kształtowaniu bezpieczeństwa Rzeczypospolitej Polskiej, co jest celem nadrzędnym tego programu.

**Słowa kluczowe:** infrastruktura krytyczna, bezpieczeństwo państwa, ochrona infrastruktury krytycznej, zarządzanie kryzysowe.

**National Critical Infrastructure Protection Program in Shaping the Security of the Republic of Poland**

**Abstract:**
Although critical infrastructure has been present relatively recently in Polish law, it plays a key role in the functioning of the state as well as in the life of individual citizens. The protection of critical infrastructure is one of the priorities for each country, including Poland. Entities carrying out the tasks in the field of critical infrastructure protection are not only required to ensure its adequate protection, but additionally are obliged to remove damage or disruptions quickly and completely in the event of their occurrence. The aim of the article is to indicate the role of the National Critical Infrastructure Protection Program in shaping the security of the Republic of Poland, which is the overriding objective of this program.

**Keywords:** critical infrastructure, national security, protection of critical infrastructure, crisis management.