Historia i Polityka
Nr 25(32)/2018, ss. 93–113
www.hip.umk.pl
ISSN 1899-5160, e-ISSN 2391-7652
DOI: http://dx.doi.org/10.12775/HiP.2018.025

Grzegorz PIETREK
Wyższa Szkoła Bankowa, Wydział Finansów i Zarządzania, Gdańsk, Polska

Zagrożenia dla społeczności lokalnej ze strony gminnej infrastruktury krytycznej

Threats to the Local Community Related to the Communal Critical Infrastructure

• **Abstrakt** •

Infrastruktura krytyczna odgrywa kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W rezultacie zagrożeń wynikających ze zjawisk związanych z siłami natury lub będących konsekwencją działań człowieka infrastruktura krytyczna może być zniszczona albo uszkodzona, a jej działanie może ulec zakłóceniu, przez co może być zagrożona równowaga funkcjonowania państwa i społeczeństwa. Dlatego też ochrona infrastruktury krytycznej jest jednym z priorytetów państwa.

Słowa kluczowe: zarządzanie kryzysowe, infrastruktura krytyczna, administracja publiczna.

• **Abstract** •

Critical infrastructure is key to functioning of the state and the life of its citizens. As a result of threats connected with natural disasters or human activity, critical infrastructure can be destroyed or damaged, its functioning disrupted, which can affect the functioning of the state and the society. Therefore protection of critical infrastructure is a top priority for any government.

Keywords: crisis management, critical infrastructure, civil service

Wprowadzenie

Biorąc pod uwagę fakt, że inicjatywa stworzenia systemu ochrony infrastruktury krytycznej powstała po stronie administracji publicznej, to współdziałanie tego typu organów stanowi jeden z podstawowych elementów zarządzania kryzysowego w tym właśnie zakresie. Współdziałanie to ma polegać na wspólnych przedsięwzięciach, których celem jest poprawa warunków bezpieczeństwa, co oznacza tworzenie koncepcji, standardów oraz propagowanie rozwiązań dotyczących ochrony infrastruktury. Omawiana kooperacja administracji publicznej w ramach ochrony tejże infrastruktury ma polegać na nieustannej wymianie informacji, co

przyspieszy i podniesie efektywność tej ochrony oraz pozytywnie wpłynie na proces zarządzania bezpieczeństwem.

W opinii specjalistów pod pojęciem „infrastruktura krytyczna państwa" rozumieć należy obiekty i urządzenia, służby odpowiedzialne za ich obsługę, komputerowe systemy informatyczne istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa oraz efektywnego funkcjonowania. Pojęcie to obejmuje:

– systemy energetyczne, telekomunikacyjne, pocztowe, teleinformatyczne, finansowe i bankowe, zarządzania zasobami wodnymi, dostaw żywności i wody, opieki zdrowotnej, transportowe;
– usługi związane z zapewnieniem bezpieczeństwa powszechnego i porządku publicznego;
– zapewnienie prawidłowego funkcjonowania najważniejszych struktur administracji publicznej w sytuacjach nadzwyczajnych zagrożeń;
– ochronę przemysłu o znaczeniu strategicznym, w tym obronnego.

Jak można wywnioskować, przedsięwzięcia związane z ochroną infrastruktury krytycznej są bardzo istotnym obszarem w zarządzaniu kryzysowym, w aspekcie bezpieczeństwa państwa. Infrastruktura krytyczna obejmuje systemy:

– 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.

Poza elementami narodowej infrastruktury krytycznej w obszarze zainteresowania zarządzania kryzysowego znajduje się także europejska infrastruktura krytyczna. Jest ona rozumiana jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach, o których mowa w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego

zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie (Ustawa z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym, art. 3, pkt 2).

Podstawy prawne

Ustawa o zarządzaniu kryzysowym nie zamyka katalogu obiektów i systemów, które mogą stanowić o bezpieczeństwie państwa i równowadze jego funkcjonowania. Potrzeba ochrony obiektów szczególnie ważnych ze względu na bezpieczeństwo państwa została uwzględniona już w 1967 roku w ustawie z 21 listopada o powszechnym obowiązku obrony Rzeczypospolitej Polskiej ochrony (Ustawa z 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej) oraz w rozporządzeniu z 24 czerwca 2003 roku w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Rozporządzenie z 24 czerwca 2003 roku w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony), które wskazuje na dwie kategorie obiektów. Do pierwszej kategorii, związanej z potencjałem obronnym państwa, zaliczono:

- zakłady produkujące, remontujące, magazynujące uzbrojenie, sprzęt wojskowy i środki bojowe;
- zakłady prowadzące prace badawczo-rozwojowe oraz konstruktorskie w dziedzinie bezpieczeństwa i obronności państwa;
- magazyny rezerw państwowych (np. bazy paliw płynnych, żywności, leków, materiałów sanitarnych);
- obiekty podległe ministrowi obrony narodowej lub przez niego nadzorowane;
- obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, morskiego, wodnego śródlądowego, drogownictwa, kolejnictwa i łączności;
- ośrodki dokumentacji geodezyjnej i kartograficznej;
- zapory wodne;
- urządzenia hydrotechniczne;
- obiekty należące do jednostek organizacyjnych Agencji Wywiadu;
- obiekty Narodowego Banku Polskiego;
- obiekty Banku Gospodarstwa Krajowego;
- obiekty Polskiej Wytwórni Papierów Wartościowych oraz Mennicy Państwowej;

– obiekty telekomunikacyjne służące nadawaniu programów radiowych i telewizji publicznej;
– obiekty i miejsca, w których produkowane, stosowane lub magazynowane są materiały jądrowe czy też źródła i odpady promieniotwórcze (Rozporządzenie z 24 czerwca 2003 roku, § 2 pkt 1–9).

Do drugiej kategorii należą obiekty związane z właściwym funkcjonowaniem administracji publicznej oraz zapewnieniem odpowiedniego poziomu bezpieczeństwa i porządku publicznego:

– obiekty organów i jednostek organizacyjnych podległych ministrowi spraw wewnętrznych i administracji lub przez niego administrowane;
– obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego;
– obiekty Policji, Straży Granicznej, Państwowej Straży Pożarnej;
– obiekty będące we właściwości ministra sprawiedliwości, Służby Więziennej oraz jednostek organizacyjnych, które podlegają ministrowi sprawiedliwości bądź są przez niego nadzorowane;
– zakłady, których działalność ma związek z wydobywaniem kopalin podstawowych;
– obiekty (miejsca), w których produkowane, stosowane lub magazynowane są materiały stwarzające zagrożenie pożarem lub wybuchem;
– obiekty w których prowadzona jest działalność oparta na wykorzystywaniu toksycznych związków chemicznych i ich prekursorów, środków biologicznych i mikrobiologicznych, mikroorganizmów, toksyn i innych substancji powodujących zachorowania u ludzi i (lub) zwierząt;
– elektrownie oraz inne obiekty elektroenergetyczne;
– inne obiekty znajdujące się we właściwości organów administracji rządowej lub też organów jednostek samorządu terytorialnego, formacji, instytucji państwowych, a także prywatnych przedsiębiorców (Rozporządzenie z 24 czerwca 2003 roku, § 2 pkt 10–19).

Ustawa o ochronie osób i mienia z 1997 roku także wymienia wiele obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. W ustawie tej dokonano doprecyzowania kryteriów i podziału wspomnianej infrastruktury na związane z obronnością państwa, ochroną interesu gospodarczego państwa, bezpieczeństwem publicznym oraz innymi ważnymi interesami państwa (Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia).

Infrastruktura krytyczna odgrywa kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W rezultacie zagrożeń wynikających ze zjawisk związanych z siłami natury lub będących konsekwencją działań człowieka infrastruktura krytyczna może być zniszczona albo uszkodzona, a jej działanie może ulec zakłóceniu,

przez co może być zagrożona równowaga funkcjonowania państwa i społeczeństwa. Dlatego też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed państwem. Tak więc przez „ochronę infrastruktury krytycznej" należy rozumieć „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie" (Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym).

Infrastruktura krytyczna to system połączonych ze sobą elementów różnego rodzaju, których funkcjonowanie służy prawidłowemu działaniu organów administracji publicznej. Ochrona infrastruktury krytycznej zaś to wszelkie działania podejmowane w celu utrzymania ciągłości i sprawności pracy jednostek infrastruktury krytycznej. Jednostki te to zaopatrzenie w energię cieplną, zaopatrzenie w wodę i żywność, system ochrony zdrowia, ciągłość działania administracji publicznej, system transportowy i ratowniczy, system finansowy i sieci teleinformatycznych (Małyjurek, Krynojewski, 2010).

Ochrona infrastruktury krytycznej obejmuje znaczny zakres kompetencji i zadań. Kryteria identyfikacji obiektów takiej infrastruktury podzielić można na trzy etapy. Pierwszy etap to wstępna selekcja obiektów, urządzeń, instalacji itp. Drugi etap poświęcony jest sprawdzeniu, jaką rolę w całej infrastrukturze krytycznej pełni dany obiekt i czy jego uszkodzenie wpłynie na działanie administracji publicznej. Etap trzeci sprowadza się do oceny potencjalnych skutków zniszczenia.

Ochronę infrastruktury krytycznej należy pojmować jako proces zapewnienia jej bezpieczeństwa:

- uwzględniający dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie;
- obejmujący znaczną ilość obszarów zadaniowych i kompetencji;
- angażujący wiele zainteresowanych stron;
- obejmujący wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej.

Tak rozumiany proces ochrony infrastruktury krytycznej składa się z następujących etapów:

1) wskazanie zakresu, celów do osiągnięcia w ramach ochrony infrastruktury krytycznej oraz adresatów tych działań;
2) identyfikacja krytycznych zasobów, funkcji oraz określenia sieci powiązań (zależności) z innymi systemami infrastruktury krytycznej, w tym podmiotami i organami;

3) określenie ról i odpowiedzialności uczestniczących w procesie ochrony infrastruktury krytycznej;
4) ocena ryzyka;
5) wskazanie priorytetów działania i dokonanie ich hierarchizacji w zależności od wyników oceny ryzyka;
6) rozwój i wdrażanie systemu ochrony infrastruktury krytycznej, w tym opracowania i akceptacji planów ochrony i odtwarzania infrastruktury;
7) testowanie (przez ćwiczenia) i przegląd (przez audyt i samoocenę) systemu ochrony infrastruktury krytycznej oraz pomiar postępów na drodze do osiągnięcia celu;
8) doskonalenie, rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów i pomiarów (za: Rządowe Centrum Bezpieczeństwa).

Narodowy program ochrony infrastruktury krytycznej

Jednym z zadań Rządowego Centrum Bezpieczeństwa jest tworzenie i aktualizowanie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK). Przy jego przygotowaniu i uaktualnianiu RCB współdziała z ministrami i kierownikami urzędów centralnych właściwych w sprawach bezpieczeństwa narodowego, a także odpowiedzialnymi za systemy w infrastrukturze krytycznej. Program ten określa:

– narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej;
– ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy infrastruktury krytycznej;
– szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa oraz zaspokojenia potrzeb obywateli.

W NPOIK zawarty jest wykaz obiektów wchodzących w skład infrastruktury krytycznej w zależności od danego terenu (najczęściej województwa; Małyjurek, Krynojewski, 2010). Można stwierdzić, że priorytetami dla systemu ochrony infrastruktury krytycznej są:

– zapobieganie różnorakim zdarzeniom, mogącym doprowadzić do zakłócenia funkcjonowania któregoś elementu infrastruktury krytycznej;

– poczynania prowadzące do przygotowania systemu na negatywne oddziaływanie w stosunku do sytuacji kryzysowej;
– odtwarzanie i przywracanie do stanu sprzed wystąpienia sytuacji kryzysowej całego, spójnie działającego, systemu infrastruktury krytycznej (Narodowy Program Ochrony Infrastruktury Krytycznej).

Celem Programu jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny, czyli podniesienie bezpieczeństwa Rzeczypospolitej Polskiej. Cele pośrednie 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.

Identyfikacja obiektów, urządzeń, instalacji lub usług, których zniszczenie lub zakłócenie funkcjonowania mogłoby spowodować sytuację kryzysową, jest kluczowym etapem procesu ochrony infrastruktury krytycznej.

W celu maksymalnej obiektywizacji Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych oraz przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji infrastruktury krytycznej. Kryteria podzielone są na dwie grupy:

1) kryteria systemowe – charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów tej infrastruktury;
2) kryteria przekrojowe – opisujące parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria przekrojowe obejmują:
   – ofiary w ludziach,
   – skutki finansowe,
   – konieczność ewakuacji,

– utratę usługi,
– czas odbudowy,
– efekt międzynarodowy,
– unikatowość.

Wyżej wskazane kryteria określają wartości liczbowe stosowane dla scharakteryzowania cechy, ze względu na którą dana infrastruktura klasyfikowana jest jako krytyczna. W przypadku braku takiej możliwości opisano funkcje realizowane przez badaną infrastrukturę. Identyfikacja infrastruktury krytycznej została podzielona na trzy etapy:

– etap pierwszy – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za infrastrukturę krytyczną w danym systemie, do infrastruktury systemu należy zastosować kryteria systemowe, właściwe dla danego systemu infrastruktury krytycznej;
– etap drugi – w celu sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców;
– etap trzeci – w celu oceny potencjalnych skutków zniszczenia lub zaprzestania funkcjonowania potencjalnej infrastruktury krytycznej.

Do infrastruktury wyłonionej w etapie pierwszym i drugim należy zastosować kryteria przekrojowe, przy czym potencjalna infrastruktura musi spełnić przynajmniej dwa kryteria przekrojowe.

Ochrona infrastruktury krytycznej w unii europejskiej

Określenie tego, co stanowi infrastrukturę krytyczną, w Unii Europejskiej zależy od jej charakteru transgranicznego, czyli ustalenia, czy ewentualny incydent mógłby mieć poważne skutki poza terytorium państwa członkowskiego, na którym usytuowane są urządzenia. Elementem, który też należy brać pod uwagę, jest fakt, że dwustronne programy współpracy, dotyczące ochrony infrastruktury krytycznej, zawierane pomiędzy państwami członkowskimi stanowią sprawdzony i skuteczny środek rozwiązywania problemów w dziedzinie infrastruktury krytycznej znajdujących się na obszarze dwóch państwa członkowskich. Tego typu współpraca stanowi uzupełnienie Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK), do której można zaliczyć zasoby fizyczne, usługi, sprzęt informatyczny, sieci i aktywa infrastruktury, których zakłócenie lub znisz-

czenie miałoby poważny wpływ na zdrowie, bezpieczeństwo, dobrobyt gospodarczy lub społeczny dwóch lub większej liczby państw członkowskich. Europejski Program Ochrony Infrastruktury Krytycznej przyczynia się do wspierania starań państw członkowskich mających na celu zapobieganie atakom terrorystycznym i innym wydarzeniom związanym z bezpieczeństwem. Unia Europejska uznaje, że należy również uwzględniać infrastrukturę krytyczną pochodzącą spoza UE lub istniejącą poza nią, ale współzależną.

Działania z zakresu ochrony infrastruktury krytycznej prowadzone na szczeblu krajowym wpisują się w szerszy kontekst europejski, czego przejawem jest właśnie wdrażany na forum Unii Europejskiej Europejski Program Ochrony Infrastruktury Krytycznej (EPOIK).

Na działania w ramach Europejskiego Programu Ochrony Infrastruktury Krytycznej składają się:

- dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony;
- instrumenty finansujące działania z zakresu ochrony infrastruktury krytycznej – w latach 2007–2013: program *Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa* – CIPS, w latach 2014–2020 instrument „Fundusz Bezpieczeństwa Wewnętrznego" – ISF;
- działania wspomagające państwa członkowskie w implementacji dyrektywy (m.in. system wymiany informacji – CIWIN);
- wymiar zewnętrzny – koncepcja współpracy z państwami trzecimi, na których terytorium zlokalizowana jest infrastruktura, która w przypadku wystąpienia zakłóceń lub zniszczenia może mieć wpływ na infrastrukturę państw członkowskich (konkluzje Rady w sprawie rozwoju zewnętrznego wymiaru Europejskiego Programu Ochrony Infrastruktury Krytycznej);
- możliwa pomoc państwom członkowskim w pracach nad rozwiązaniami krajowymi z zakresu infrastruktury krytycznej.

Najważniejszym elementem EPOIK jest wymieniona powyżej dyrektywa, która określa proces rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej. Jednocześnie zapewnia ona wspólne podejście do oceny potrzeb poprawy ochrony tej infrastruktury.

Dyrektywa w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony określa europejską infrastrukturę krytyczną jako infrastrukturę zlokalizowaną na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałoby istotny wpływ

na co najmniej dwa państwa członkowskie. To, czy wpływ jest istotny, ocenia się w odniesieniu do wcześniej opisanych kryteriów przekrojowych.

Europejska infrastruktura krytyczna wyznaczana jest w dwóch sektorach – sektorze energii i sektorze transportu. W 2013 roku, po dokonaniu przeglądu dyrektywy i EPOIK, Komisja przyjęła Dokument Roboczy Komisji w sprawie nowego podejścia do Europejskiego Programu Ochrony Infrastruktury Krytycznej (SWD(2013)318), uszczegóławiający kierunki prac uczestników programu w kolejnych latach.

Polska aktywnie uczestniczy w przedsięwzięciach realizowanych w ramach EPOIK. Funkcję koordynatora tych działań, jako krajowy punkt kontaktowy, pełni Rządowe Centrum Bezpieczeństwa (*Narodowy Program Ochrony Infrastruktury Krytycznej*).

Sprawozdanie z badań

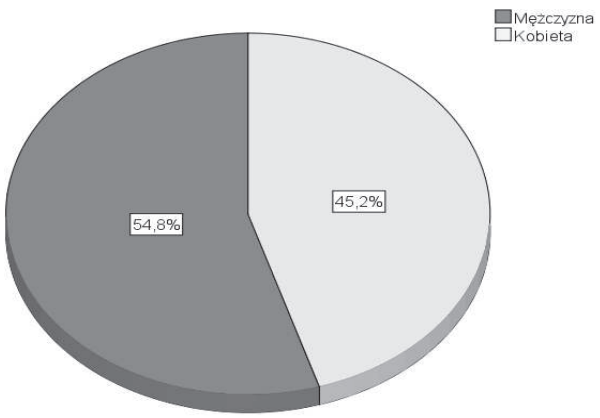
Istotność różnic pomiędzy dwiema wartościami średnimi sprawdzano za pomocą testu t Studenta dla prób niezależnych. Korelacje pomiędzy zmiennymi ilościowymi sprawdzono za pomocą współczynnika korelacji rang Spearmana. Współczynnik ten przyjmuje wartości od +1 (silna korelacja dodatnia, wraz ze wzrostem jednej zmiennej, następuje wzrost drugiej zmiennej), poprzez 0 (brak korelacji) do -1 (silna korelacja ujemna, wzrost wartości jednej zmiennej, powodował spadek wartości drugiej zmiennej). Rzetelność tworzonych skal zmierzono za pomocą współczynnika alfa Cronbacha. W analizach statystycznych przyjęto poziom istotności p = 0,05. Analiz dokonywano za pomocą programu SPSS.

Analiza grupy badawczej

W badaniu ankietowym wzięło udział 225 ankietowanych, z czego blisko 55% respondentów to mężczyźni, a 45% to kobiety (Wyk. 1). Najwięcej ankietowanych było w wieku od 46 do 55 lat (34%), w wieku od 18 do 25 lat – 11% respondentów, w wieku od 26 do 35 lat 22%, w wieku od 36 do 45 lat 27%. Grupę badawczą uzupełniały osoby w wieku powyżej 55 lat (6%; Wyk. 2). Większość osób pracowała w zawodzie powyżej 8 lat (62%), staż pracy do 3 lat miało 8% ankietowanych, od 4 do 6 lat – 15%, od 6 do 8 lat – 15% (Wyk. 3). Zdecydowany odsetek ankietowanych posiadał wykształcenie wyższe (78%), pozostali respondenci posiadali wykształcenie średnie (22%; Wyk. 4). Większość osób pracowała na stano-

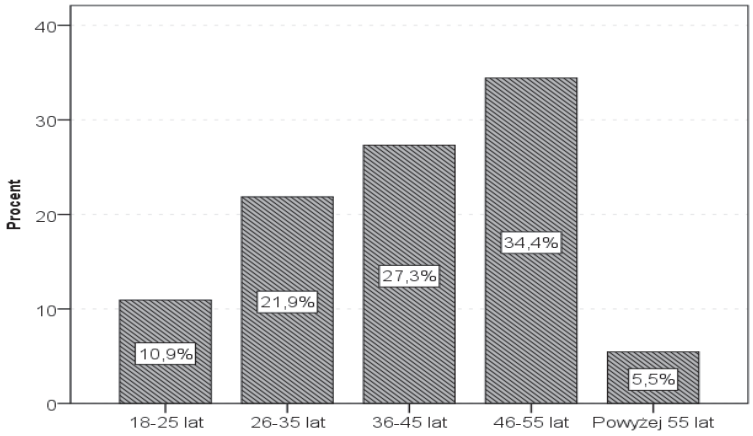
wisku ds. zarządzania kryzysowego (64%), duży odsetek ankietowanych pracował na stanowisku ds. OC, obronnych (25%). Pozostali ankietowani pracowali na stanowisku ds. łączności (5%), byli kierownikami oddziału (3%), dyrektorami (2%) lub pracowali na stanowisku ds. informatyki (2%; Wyk. 5).

Wykres 1. Płeć ankietowanego



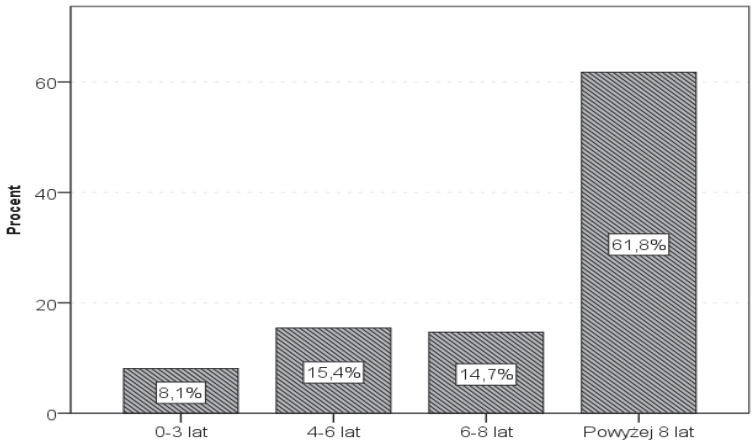
Źródło: opracowanie własne.

Wykres 2. Wiek ankietowanego



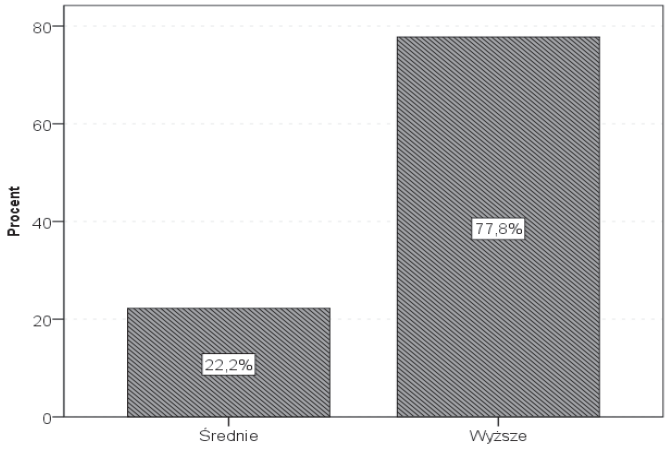
Źródło: opracowanie własne.

Wykres 3. Okres zatrudnienia ankietowanego



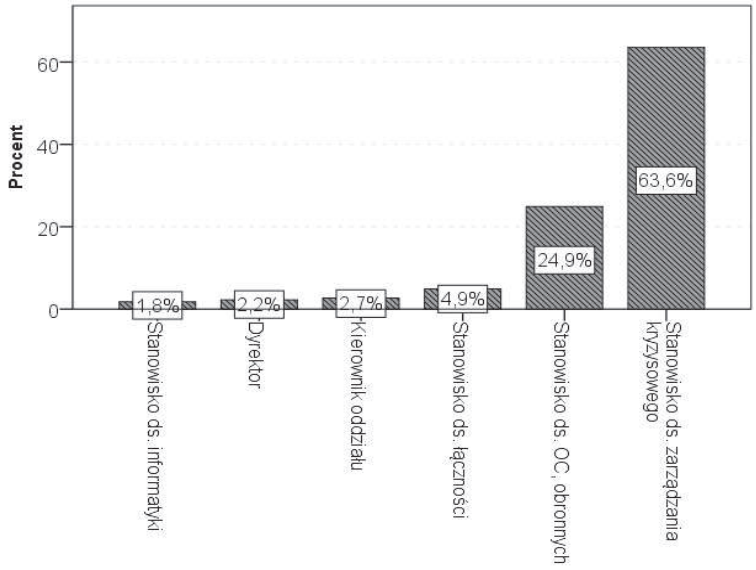
Źródło: opracowanie własne.

Wykres 4. Wykształcenie ankietowanego



Źródło: opracowanie własne.

Wykres 5. Zajmowane stanowisko ankietowanego



Źródło: opracowanie własne.

Poprawność realizacji procedur w zakresie ochrony poszczególnych systemów składających się na infrastrukturę krytyczną

Ankietowani za pomocą 5-punktowej skali musieli ocenić poprawność procedur w zakresie ochrony poszczególnych systemów składających się na infrastrukturę krytyczną, gdzie 1 oznaczało bardzo złą ocenę, 2 – złą, 3 – dostateczną, 4 – dobrą, 5 – bardzo dobrą. Wartości uśredniono i uszeregowano od najwyższych do najniższych, od procedur najwyżej ocenianych do procedur ocenianych najniżej.

Najwyżej oceniono (ponad połowa ankietowanych wystawiała ocenę przynajmniej dobrą): systemy łączności (4,1), ratownicze (3,9), ochrony zdrowia (3,8), zapewniające ciągłość działania administracji publicznej (3,8), sieci teleinformatycznych (3,6), zaopatrzenia w energię i paliwa (3,6).

Najniżej oceniano (co najmniej połowa ankietowanych przyznała ocenę 3 lub niższą): systemy zaopatrzenia w żywność (3,4), w wodę (3,4), systemy transportowe (3,4), finansowe (3,4), systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (3,3).

Średnia przyznawana ocena dla całego analizowanego obszaru wynosiła 3,6, przy odchyleniu standardowym wynoszącym 0,85. Najczęściej przyznawaną oceną było 4 (Tab. 1).

Tabela 1. Miary tendencji centralnej oraz rozproszenia ocen ankietowanych (1 – bardzo źle, 2 – źle, 3 – dostatecznie, 4 – dobrze, 5 – bardzo dobrze)

Procedury:	***M***	***SD***	***Me***	***Mo***
Systemy łączności	4,1	0,71	4	4
Systemy ratownicze	3,9	0,65	4	4
Systemy ochrony zdrowia	3,8	0,69	4	4
Systemy zapewniające ciągłość działania administracji publicznej	3,8	0,77	4	4
Systemy sieci teleinformatycznych	3,6	0,76	4	4
Systemy zaopatrzenia w energię i paliwa	3,6	0,93	4	4
Systemy zaopatrzenia w żywność	3,4	0,82	3	4
Systemy zaopatrzenia w wodę	3,4	0,86	3	4
Systemy transportowe	3,4	0,86	3	4
Systemy finansowe	3,4	0,87	4	4
Systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	3,3	1,00	4	4
Podsumowanie ocen dla całego obszaru	**3,6**	**0,85**	**4**	**4**

M – średnia, *SD* – odchylenie standardowe, *Me* – mediana, *Mo* – dominanta

Źródło: opracowanie własne.

W celu stworzenia jednolitej skali mierzącej poprawność realizacji procedur w zakresie ochrony poszczególnych systemów składających się na infrastrukturę krytyczną zsumowano wszystkie oceny. Tak stworzona skala przyjmowała wartości od 11 do 55 punktów, a współczynnik rzetelności alfa Cronbacha tak stworzonej skali wynosił 0,74.

Średnia liczba punktów uzyskana przez ankietowanych wynosiła 39,6, przy odchyleniu standardowym wynoszącym 4,75 punktów. Co najmniej połowa respondentów uzyskała przynajmniej 41 punktów. Najniższa uzyskana liczba punktów to 25, natomiast najwyższa to 51 punktów (Tab. 2, Wyk. 6).

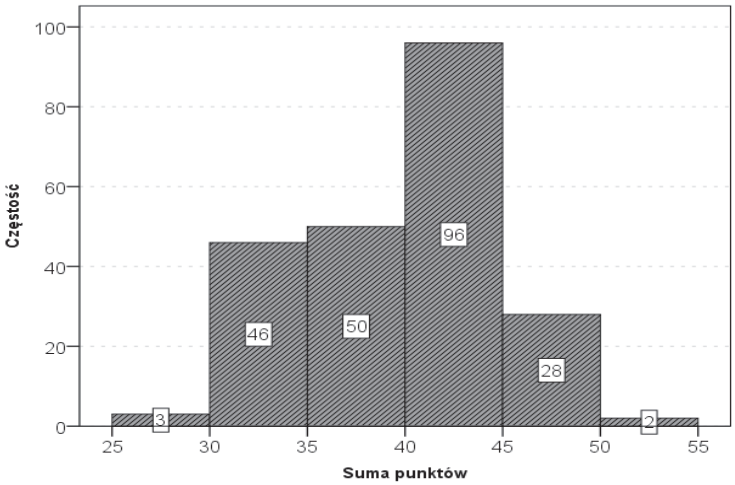
Tabela 2. Miary tendencji centralnej oraz rozproszenia. Suma punktów

	M	*SD*	*Me*	*Mo*	*Min.*	*Maks.*
Suma punktów	39,6	4,75	41,0	44,0	25,0	51,0

M – średnia, *SD* – odchylenie standardowe, *Me* – mediana, *Mo* – dominanta, *Min.* – wartość minimalna, *Maks.* – wartość maksymalna

Źródło: opracowanie własne.

Wykres 6. Suma punktów dla skali mierzącej poprawność realizacji procedur w zakresie ochrony poszczególnych systemów składających się na infrastrukturę krytyczną



Źródło: opracowanie własne.

Poprawność realizacji procedur w zakresie realizacji zadań ochrony infrastruktury krytycznej

Ankietowani za pomocą 5-punktowej skali musieli ocenić poprawność realizacji procedur w zakresie realizacji zadań ochrony infrastruktury krytycznej, gdzie 1 oznaczało bardzo złą ocenę, 2 – złą, 3 – dostateczną, 4 – dobrą, 5 – bardzo dobrą. Wartości uśredniono i uszeregowano od najwyższych do najniższych, od procedur najwyżej ocenianych do procedur ocenianych najniżej.

Najwyżej oceniono (ponad połowa ankietowanych wystawiała ocenę przynajmniej dobrą): gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej (3,8), opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej (3,4).

Najniżej oceniano (co najmniej połowa ankietowanych przyznała ocenę 3 lub niższą): współpracę między administracją publiczną a właścicielami oraz posiada-

czami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony (3,2), odtwarzanie infrastruktury krytycznej (3,2).

Średnia przyznawana ocena dla całego analizowanego obszaru wynosiła 3,4, przy odchyleniu standardowym wynoszącym 0,85. Najczęściej przyznawaną oceną było 4 (Tab. 3).

Tabela 3. Miary tendencji centralnej oraz rozproszenia ocen ankietowanych (1 – bardzo źle, 2 – źle, 3 – dostatecznie, 4 – dobrze, 5 – bardzo dobrze)

Procedury:	***M***	***SD***	***Me***	***Mo***
Gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej	3,8	0,61	4	4
Opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej	3,4	0,91	4	4
Współpraca między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochron	3,2	0,85	3	4
Odtwarzanie infrastruktury krytycznej	3,2	0,88	3	4
Podsumowanie ocen dla całego obszaru	**3,4**	**0,85**	**4**	**4**

M – średnia, *SD* – odchylenie standardowe, *Me* – mediana, *Mo* – dominanta

Źródło: opracowanie własne.

W celu stworzenia jednolitej skali mierzącej poprawność realizacji procedur w zakresie realizacji zadań ochrony infrastruktury krytycznej zsumowano wszystkie oceny. Tak stworzona skala przyjmowała wartości od 4 do 20 punktów, a współczynnik rzetelności alfa Cronbacha wynosił dla niej 0,67.

Średnia liczba punktów uzyskana przez ankietowanych wynosiła 13,7, przy odchyleniu standardowym wynoszącym 2,33 punktów. Co najmniej połowa respondentów uzyskała przynajmniej 13 punktów. Najniższa uzyskana liczba punktów to 7, natomiast najwyższa to 20 punktów (Tab. 4, Wyk. 7).

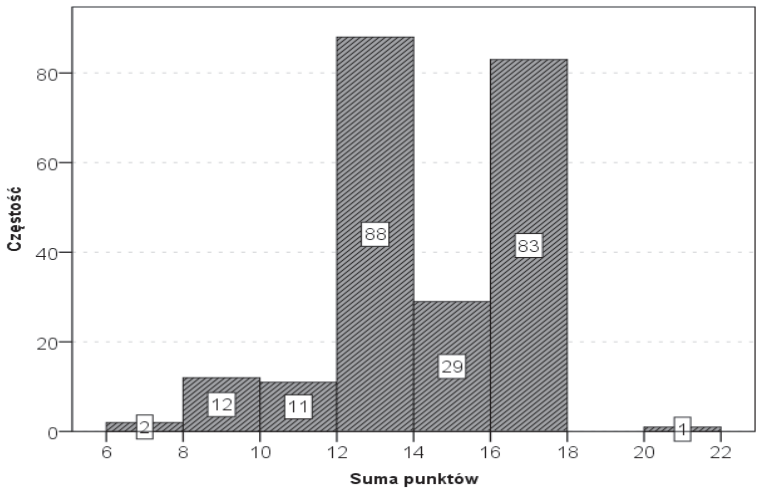
Tabela 4. Miary tendencji centralnej oraz rozproszenia. Suma punktów

	M	***SD***	***Me***	***Mo***	***Min.***	***Maks.***
Suma punktów	13,7	2,33	13,5	16,0	7,0	20,0

M – średnia, *SD* – odchylenie standardowe, *Me* – mediana, *Mo* – dominanta, *Min.* – wartość minimalna, *Maks.* – wartość maksymalna

Źródło: opracowanie własne.

Wykres 7. Suma punktów dla skali mierzącej poprawność realizacji procedur w zakresie realizacji zadań ochrony infrastruktury krytycznej



Źródło: opracowanie własne.

Poprawność realizacji procedur w zakresie tworzenia warunków do poprawy bezpieczeństwa infrastruktury krytycznej wskazanych w Narodowym Programie Ochrony Infrastruktury Krytycznej

Ankietowani za pomocą 5-punktowej skali musieli ocenić poprawność realizacji procedur w zakresie tworzenia warunków do poprawy bezpieczeństwa infrastruktury krytycznej wskazanych w Narodowym Programie Ochrony Infrastruktury Krytycznej, gdzie 1 oznaczało bardzo złą ocenę, 2 – złą, 3 – dostateczną, 4 – dobrą, 5 – bardzo dobrą. Wartości uśredniono i uszeregowano od najwyższych do najniższych, od procedur najwyżej ocenianych do procedur ocenianych najniżej.

Najwyżej oceniono (ponad połowa ankietowanych wystawiała ocenę przynajmniej dobrą): odtwarzanie infrastruktury krytycznej (4,1), przygotowanie na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną (3,9), zapobieganie zakłóceniom funkcjonowania infrastruktury krytycznej (3,5), uszczegółowienie kryteriów pozwalających wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli (3,4).

Najniżej oceniano (co najmniej połowa ankietowanych przyznała ocenę 3 lub niższą): określenie narodowych priorytetów, celów, wymagań i standardów służących zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej (3,4), re-

agowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej (3,2).

Średnia przyznawana ocena dla całego analizowanego obszaru wynosiła 3,6, przy odchyleniu standardowym wynoszącym 0,88. Najczęściej przyznawaną oceną było 4 (Tab. 5).

Tabela 5. Miary tendencji centralnej oraz rozproszenia ocen ankietowanych (1 – bardzo źle, 2 – źle, 3 – dostatecznie, 4 – dobrze, 5 – bardzo dobrze)

Procedury:	***M***	***SD***	***Me***	***Mo***
Przygotowanie na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną	3,9	0,65	4	4
Zapobieganie zakłóceniom funkcjonowania infrastruktury krytycznej	3,5	0,91	4	4
Uszczegółowienie kryteriów pozwalających wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli	3,4	0,82	4	4
Określenie narodowych priorytetów, celów, wymagań i standardów służących zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej	3,4	0,86	3	4
Reagowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej	3,2	0,90	3	4
Podsumowanie ocen dla całego obszaru	**3,6**	**0,88**	**4**	**4**

M – średnia, *SD* – odchylenie standardowe, *Me* – mediana, *Mo* – dominanta

Źródło: opracowanie własne.

W celu stworzenia jednolitej skali mierzącej poprawność realizacji procedur w zakresie tworzenia warunków do poprawy bezpieczeństwa infrastruktury krytycznej wskazanych w Narodowym Programie Ochrony Infrastruktury Krytycznej zsumowano wszystkie oceny. Tak stworzona skala przyjmowała wartości od 6 do 30 punktów, a współczynnik rzetelności alfa Cronbacha tak stworzonej skali wynosił 0,59.

Średnia liczba punktów uzyskana przez ankietowanych wynosiła 21,5, przy odchyleniu standardowym wynoszącym 2,79 punktów. Co najmniej połowa re-

spondentów uzyskała przynajmniej 21 punktów. Najniższa uzyskana liczba punktów to 14, natomiast najwyższa to 29 punktów (Tab. 6, Wyk. 8).

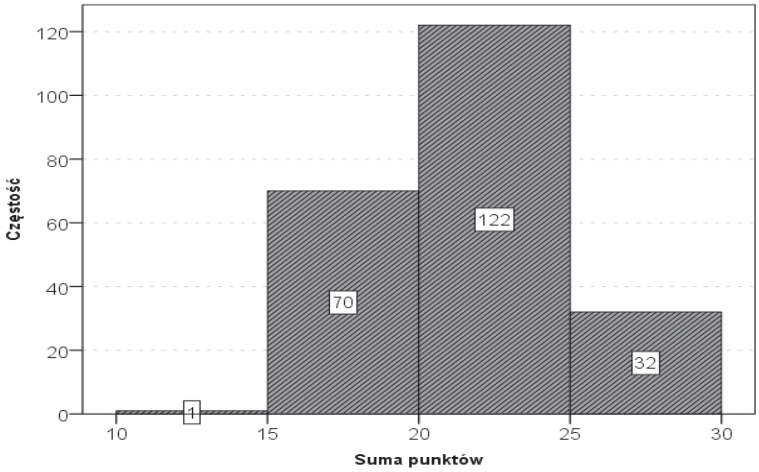
Tabela 6. Miary tendencji centralnej oraz rozproszenia. Suma punktów

	M	*SD*	*Me*	*Mo*	*Min.*	*Maks.*
Suma punktów	21,5	2,79	21,0	19,0	14,0	29,0

M – średnia, *SD* – odchylenie standardowe, *Me* – mediana, *Mo* – dominanta, *Min.* – wartość minimalna, *Maks.* – wartość maksymalna

Źródło: opracowanie własne.

Wykres 8. Suma punktów dla skali mierzącej poprawność realizacji procedur w zakresie tworzenia warunków do poprawy bezpieczeństwa infrastruktury krytycznej wskazanych w Narodowym Programie Ochrony Infrastruktury Krytycznej



Źródło: opracowanie własne.

W tej części badania, na zakończenie kwestionariusza ankiety, postawiono kilka pytań otwartych. Respondenci poproszeni zostali o szczere, merytoryczne odpowiedzi. Opracowując wyniki tej części sondażu, oparto się na tych odpowiedziach, które wnoszą do diagnozowanych obszarów ważne informacje, propozycje, spostrzeżenia i wnioski. Poniżej zaprezentowane zostały najważniejsze treści.

Pytanie otwarte o funkcjonowanie systemu ochrony infrastruktury krytycznej

Respondenci w tym segmencie wypowiadali się dosyć lakonicznie. W zasadzie odpowiedzi reprezentujące poziomy powyżej powiatowego (województwo i wyżej) skłaniały się do opinii pozytywnych. Poziomy powiatowy, a zwłaszcza gminny wskazywały na wiele niedostatków. Nie można jednak przytoczyć zbyt wielu opinii, gdyż niestety ograniczały się one do określeń typu „funkcjonuje źle" czy „nie działa". Z opinii zebranych w ramach badania tego obszaru można wywnioskować, że wątpliwości w zakresie funkcjonalności mogą dotyczyć wykonywania zadań z zakresu odtwarzania infrastruktury krytycznej. Obowiązek zaplanowania działań m.in. w warunkach zakłócenia funkcjonowania infrastruktury krytycznej oraz odtwarzania infrastruktury krytycznej został nałożony na operatorów tejże infrastruktury przez zapis rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej (§ 2 ust. 3 pkt 4). Odtwarzanie infrastruktury krytycznej jest także przypisywane do zadań wojewody, starosty, prezydenta miasta, wójta, burmistrza – w ramach wykonywania zadań z zakresu ochrony infrastruktury krytycznej na podstawie tego samego aktu prawnego (art. 6 ust. 1 pkt 4). Taki niefortunny zapis z zakresu odtwarzania infrastruktury krytycznej może w przyszłości powodować spory kompetencyjne. Tymczasem jej odtwarzanie powinno leżeć w gestii właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej.

Podsumowanie

Biorąc pod uwagę fakt, że najbardziej kompleksowym rozwiązaniem w obszarze ochrony kluczowej infrastruktury państwa (infrastruktury bezpieczeństwa państwa) jest system ochrony infrastruktury krytycznej, ustawą stanowiącą podstawę inicjowanych prac powinna być ustawa o zarządzaniu kryzysowym.

Tak omawiana integracja powinna obejmować podział na infrastrukturę krytyczną ważną ze względu na interes państwa i odpowiednio województwa, powiatu i gminy, z przypisaniem kategoryzacji. Pozwoliłoby to na ujęcie wszystkich obiektów podlegających ochronie w myśl powyższych przepisów w skład infrastruktury krytycznej, która będzie chroniona niezależnie od sytuacji (również w czasie wojny). Infrastruktura krytyczna szczebla krajowego wyłaniana byłaby na podstawie kryteriów przygotowywanych przez Dyrektora Rządowego Centrum Bezpieczeństwa we współpracy z ministrami oraz kierownikami urzędów central-

nych odpowiedzialnymi za systemy infrastruktury krytycznej. Infrastruktura krytyczna na szczeblu wojewódzkim, powiatowym i gminnym wyodrębniana byłaby na podstawie jednolitych kryteriów, jednak z uwzględnieniem specyfiki regionu.

Bibliografia:

Małyjurek, K., Krynojewski, F.R. (2010). *Zarządzanie kryzysowe w administracji publicznej: zarządzanie bezpieczeństwem*. Warszawa: Difin.

Narodowy Program Ochrony Infrastruktury Krytycznej. (2015). Pobrane z: http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf.

Rozporządzenie z 24 czerwca 2003 roku w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz.U. Nr 116, poz. 1090).

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej (Dz.U. Nr 83, poz. 542).

Rządowe Centrum Bezpieczeństwa. (2017). Pobrane z: www.reg.gov.pl.infrastruktura/dokumenty 2016.

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

Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia (Dz.U. z 1997 r., Nr 114, poz. 740 z późn. zm.).

Ustawa z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. z 2010 roku, Nr 240, poz. 1600).