Marlena Derlicka
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Humanistyczny

BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ W POLSCE W XXI WIEKU

SECURITY OF CRITICAL INFRASTRUCTURE IN POLAND IN THE 21ST CENTURY

Streszczenie: Artykuł ma na celu przedstawienie aktualnego stanu prawnego dotyczącego bezpieczeństwa infrastruktury krytycznej w Polsce. Bez wątpienia ta infrastruktura ma wpływ na sprawne funkcjonowanie państwa, grup, jednostek. Dlatego też tak ważne jest, by ciągle o nią dbać. W Polsce przygotowano specjalny dokument, Narodowy Program Ochrony Infrastruktury Krytycznej, który jest nowelizowany. W oparciu o najnowsze opracowanie przedstawiono kluczowe kwestie związane z utrzymywaniem bezpieczeństwa polskiej infrastruktury krytycznej w XXI wieku.
Słowa kluczowe: bezpieczeństwo, infrastruktura krytyczna, współczesna Polska

Summary: The aim of the article is to present the current legal status concerning the security of critical infrastructure in Poland. Undoubtedly, this infrastructure has an impact on the smooth functioning of the state, groups and individuals. That is why it is so important to constantly look after it. A special document has been drawn up in Poland, the National Critical Infrastructure Protection Program and it is currently being amended. Based on the latest study, the key issues related to maintaining the security of Polish critical infrastructure in the 21st century were presented in the article.
Keywords: security, critical infrastructure, contemporary Poland

Wprowadzenie

Bezpieczeństwo jest ważne dla całego narodu i funkcjonowania państwa, ale także dla każdego człowieka z osobna. W XXI wieku rozwój następuje w bardzo szybkim tempie. Globalizacja może przynieść zarówno wiele korzyści, jak i ukazać się w bardzo negatywnym świetle. Niezależnie od tego, czy do końca zdajemy sobie z tego sprawę, czy nie, z każdym dniem coraz bardziej uzależniamy się od

postępu, od szybkiego przekazu informacji, obiegu funduszy zarówno w formie papierowej, jak i wirtualnie, dostaw żywności, lekarstw czy nawet korzystania z szeroko rozumianej infrastruktury drogowej. Wszystkie te aspekty rozwoju (i wiele innych) mają na celu ułatwienie funkcjonowania człowiekowi. Jednakże – chcemy tego czy nie – o wszystko trzeba dbać, by w pełni korzystać z dostępnych nam udogodnień, gdyż w wyniku zaniedbania czy też innych kwestii, może dojść do zatrzymania wypełniania funkcji przez dany wynalazek. Tak jest również z infrastrukturą krytyczną, która z biegiem czasu okazuje się coraz częstszym tematem rozważań ludzi z wielu kręgów zawodowych i naukowych. Również przedstawiciele władz w Polsce pochylili się nad tą kwestią, czego dowodem jest m.in. Narodowy Program Ochrony Infrastruktury Krytycznej.

Infrastruktura krytyczna

W celu określenia istoty i założeń Narodowego Programu Ochrony Infrastruktury Krytycznej warto zdefiniować, czym właściwie jest infrastruktura krytyczna. Zgodnie z definicją zapisaną w Ustawie z 26 kwietnia 2007 r. o zarządzaniu kryzysowym infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[1].

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) – zgodnie z art. 5b ust. 1 Ustawy o zarządzaniu kryzysowym – to dokument, którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. NPOIK określa zasady ochrony infrastruktury krytycznej (IK) oraz współpracy właścicieli IK z administracją publiczną. Jest to dokument nowatorski i wyjątkowy. Jego wyjątkowość polega m.in. na bezsankcyjnym, opartym na zaufaniu i współpracy administracji publicznej z właścicielami i posiadaczami obiektów IK podejściu do ochrony infrastruktury krytycznej. Został także opracowany jednolity wykaz obiektów IK.

[1] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3 ust. 2.

Organem, którego dyrektor przygotowuje[2] program i jego nowelizacje, jest Rządowe Centrum Bezpieczeństwa, będące państwową jednostką budżetową podległą prezesowi Rady Ministrów, działającą od 2 sierpnia 2008 roku na mocy Ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (art. 10) i rozporządzenia prezesa Rady Ministrów z 11 kwietnia 2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa. Dyrektorem RCB od 17 grudnia 2015 roku jest Marek Kubiak[3].

Dyrektor Centrum, przy pomocy zastępców i kierowników komórek organizacyjnych, kieruje pracą RCB i nadzoruje ją[4]. Utworzenie Rządowego Centrum Bezpieczeństwa było znaczącym krokiem w budowaniu efektywnego oraz kompleksowego systemu zarządzania kryzysowego. To właśnie dzięki takiemu systemowi można skuteczniej zapobiegać kryzysom**,** a w razie ich wystąpienia, poprzez profesjonalne działania, minimalizować ich skutki. Ponadto została stworzona struktura ponadresortowa**,** mająca na celu zoptymalizowanie i ujednolicenie postrzegania zagrożeń przez poszczególne resorty, co przekłada się na podwyższenie stopnia zdolności radzenia sobie z trudnymi sytuacjami przez właściwe służby i organy administracji publicznej.

Do podstawowych zadań RCB należy:

- dokonywanie pełnej analizy zagrożeń w oparciu o dane uzyskiwane ze wszystkich możliwych „ośrodków kryzysowych" funkcjonujących w ramach administracji publicznej oraz w oparciu o dane od partnerów międzynarodowych,
- opracowywanie optymalnych rozwiązań pojawiających się sytuacji kryzysowych,
- koordynowanie przepływu informacji o zagrożeniach.

Pozostałe zadania Rządowego Centrum Bezpieczeństwa to:

- ,,tworzenie katalogu zagrożeń,
- monitorowanie zagrożeń,
- uruchamianie procedur zarządzania kryzysowego na poziomie krajowym,

[2] Zob. W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010, s. 97.

[3] RCB, http://rcb.gov.pl/o-rcb/, (10.06.2018).

[4] Zob. Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa, § 2. 1.

- realizacja zadań planistycznych i programowych z zakresu zarządzania kryzysowego
  i ochrony infrastruktury krytycznej,
- nadzór nad spójnością procedur reagowania kryzysowego,
- organizowanie i prowadzenie szkoleń i ćwiczeń z zakresu zarządzania kryzysowego,
- realizacja zadań z zakresu przeciwdziałania, zapobiegania i likwidacji skutków zdarzeń o charakterze terrorystycznym,
- współpraca międzynarodowa, szczególnie z NATO i UE w ramach zarządzania kryzysowego"[5].

Dzięki współpracy ustalono systemy infrastruktury krytycznej. Zatem IK 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.

Cele Narodowego Programu Ochrony Infrastruktury Krytycznej

Celem Narodowego Programu Ochrony Infrastruktury Krytycznej jest stworzenie warunków poprawy bezpieczeństwa IK. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny – podniesienie bezpieczeństwa Polski. Osiągnięcie tego celu wymaga osiągnięcia szeregu celów pośrednich (operacyjnych), którymi są:

[5] RCB, https://rcb.gov.pl/o-rcb/, (10.06.2018).

1. Podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów jej ochrony;
2. Określenie ról i zakresu odpowiedzialności podmiotów publicznych i prywatnych uczestniczących w działaniach na rzecz ochrony IK;
3. Wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń,
   w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach;
4. Wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony IK;
5. Budowa partnerstwa między uczestnikami procesu ochrony IK;
6. Wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony IK;
7. Przygotowanie strategicznego programu podniesienia bezpieczeństwa IK oraz wsparcia wybranych programów badawczych i rozwojowych, edukacyjnych i szkoleniowych ukierunkowanych na podnoszenie odporności infrastruktury[6].

Priorytety

Priorytety NPOIK są następujące:

1. Podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów jej ochrony;
2. Zainicjowanie skutecznej współpracy między uczestnikami programu w obszarze ochrony IK.

Zasady programu

W ochronie kluczowych elementów infrastruktury państwa powszechnie stosuje się podejście regulacyjne – określające szczegółowo obowiązki oraz przewidujące sankcje za ich niedopełnienie. Jego skuteczność okazuje się jednak niezadowalająca. Represyjny charakter takiego podejścia przynosi skutki uboczne,

[6] Narodowy Program Ochrony Infrastruktury Krytycznej, Warszawa 2015, s. 6-7.

gdyż powoduje głęboką niechęć wykonawców do narzuconych zadań i w konsekwencji próby uchylania się od realizacji narzuconych obowiązków bądź wykonywanie ich minimalnym kosztem.

Aby osiągnąć cele programu, przyjęto bezsankcyjne podejście do ochrony infrastruktury krytycznej. Jego podstawą jest założenie, że zwiększenie skuteczności ochrony IK może nastąpić jedynie przez działania jej operatorów wspieranych przez możliwości i potencjał administracji publicznej. Operatorzy IK mają najlepszą wiedzę i narzędzia do ograniczenia zagrożeń dla ich działalności. Są również w stanie dokonać najwłaściwszego wyboru strategii minimalizacji skutków tych zagrożeń. Podejście to nie przewiduje sankcji za niedopełnienie obowiązków określonych w ustawie.

Niezależnie od przyjętego podejścia, w przypadku negatywnej oceny skuteczności programu bądź działań uczestników procesu ochrony IK lub w celu redukcji niektórych rodzajów ryzyka, dopuszcza się możliwość wprowadzenia szczegółowych uregulowań prawnych dotyczących realizacji programu.

Uczestnicy Programu powinni kierować się zasadami. Aby te zasady mogły mieć swoje praktyczne odzwierciedlenie, postanowiono stworzyć ,,konstrukcję" opartą na trzech filarach, tj. współodpowiedzialność, współpraca, zaufanie. System ochrony infrastruktury krytycznej, którego filary są silne i stabilne, może sprawnie funkcjonować. Ale ku temu potrzebne są:

1. Współodpowiedzialność – wiodąca zasada przyjęta przy budowie systemu OIK. Dążenie do poprawy bezpieczeństwa IK wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów IK, społeczeństwa, gospodarki i państwa będące wspólnym działaniem. Wynika to z tego, że ochrona infrastruktury krytycznej leży w interesie nie tylko operatorów, ale także odpowiedzialnej za funkcjonowanie państwa administracji.
2. Współpraca – drugi filar systemu ochrony IK. Współpraca w rozumieniu zapisów NPOIK to wykonywanie przez uczestników ochrony IK określonych, zbieżnych i wzajemnie uzupełniających się zadań dla osiągnięcia wspólnego celu. Wynika to także z pierwszego filaru, tj. z zasady współ-

odpowiedzialności. Współpraca jest wskazana w przypadku chęci uniknięcia kalkowania działań i ponoszonych opłat oraz efektywniejszego wykorzystania posiadanych sił i środków.

3. Zaufanie – w programie pojęcie zaufania rozumiane jest jako przekonanie, że motywacją działania uczestników ochrony IK jest dążenie do uzyskania zbieżnego celu – poprawy bezpieczeństwa IK i RP. Osiągnięcie tego będzie korzystne dla wszystkich zainteresowanych stron, a przede wszystkim społeczeństwa. Zaufanie jest nieodzowne do osiągnięcia celów programu[7].

Jak wspomniano, aby Narodowy Program Ochrony Infrastruktury Krytycznej w Polsce funkcjonował sprawnie, zostały opracowane jego zasady. Są to:

1. Zasada proporcjonalności i działań opartych na ocenie ryzyka – działania nakierowane na podniesienie poziomu ochrony IK powinny być adekwatne do poziomu ryzyka. Dotyczy to nie tylko przyjętego modelu ochrony IK, ale również użytych sił i środków. Ocena ryzyka powinna być podstawą określenia norm ochrony IK i porozumienia w kwestii priorytetów działań.
2. Zasada uznania różnic między systemami IK – systemy IK cechuje wiele podobieństw, posiadają jednak pewne unikatowe cechy, dlatego działania w obszarze ochrony IK powinny uwzględniać charakterystykę poszczególnych systemów.
3. Zasada wiodącej roli ministra odpowiedzialnego za system IK – pomysł zwiększenia poziomu ochrony infrastruktury kluczowej dla funkcjonowania społeczeństwa wyszedł ze strony administracji. Ważną rolę w budowie zaufania i skutecznej kooperacji odgrywają ministrowie odpowiedzialni za system IK, niezależnie od obowiązku ochrony IK ciążącego na operatorze IK.
4. Zasada równości operatorów IK – operatorami IK są podmioty prywatne, podmioty stanowiące własność państwa oraz administracja. Program nie dokonuje rozróżnień, więc wszyscy operatorzy są równi i zobowiązani do wykonania tego samego obowiązku, tj. ochrony IK, którą posiadają.

[7] Ibidem, s. 9.

5. Zasada komplementarności – zapisy NPOIK mają charakter uzupełniający w stosunku do istniejących rozwiązań prawno-instytucjonalnych[8].

Czas

Ochrona infrastruktury krytycznej rozumiana jako proces zakłada sukcesywne dochodzenie do oczekiwanego rezultatu oraz nieustanne dopracowywanie. Nie jest to stan czy też produkt końcowy. Sam program nie jest przez to ograniczony żadną datą końcową. Tym niemniej zakłada się, że zawarte w programie cele powinny zostać osiągnięte w ciągu 6 lat. Ze względu na dbałość o właściwą adaptację wdrożonych rozwiązań postanowiono, że program będzie aktualizowany nie rzadziej niż co 2 lata, z uwzględnieniem zmian otoczenia i uwarunkowań ochrony IK.

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

Kryteria

W celu maksymalnej obiektywizacji identyfikacji IK Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych oraz przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji IK. Określono wartości liczbowe, stosowane dla scharakteryzowania cechy, ze względu na którą dana infrastruktura klasyfikowana jest jako IK. W przypadku braku takiej możliwości opisano funkcje realizowane przez badaną infrastrukturę[9].

Kryteria identyfikacji infrastruktury krytycznej podzielono na dwa rodzaje:

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 IK.

[8] Ibidem, s. 10.
[9] Ibidem, s. 12.

2. Kryteria przekrojowe – opisujące parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria przekrojowe obejmują:
    a) ofiary w ludziach,
    b) skutki finansowe,
    c) konieczność ewakuacji,
    d) utratę usługi,
    e) czas odbudowy,
    f) efekt międzynarodowy,
    g) unikatowość.

Identyfikacja IK, zgodnie z przyjętą metodyką, została podzielona na trzy przedstawione poniżej etapy:

1. Etap pierwszy – pierwsza selekcja obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, odbywa się poprzez zastosowanie do infrastruktury systemu kryterium systemowego, właściwego dla danego systemu IK,
2. Etap drugi – aby sprawdzić, czy obiekt, urządzenie, instalacja lub usługa odgrywa kluczową rolę dla bezpieczeństwa państwa i jego obywateli, a także czy służy zapewnieniu sprawnego działania organów administracji publicznej oraz instytucji i przedsiębiorców, do infrastruktury wyłonionej w etapie pierwszym należy zastosować definicję zawartą w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym,
3. Etap trzeci – oceniając potencjalne skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w etapie pierwszym i drugim należy zastosować kryteria przekrojowe, mając na uwadze, że potencjalna IK musi spełnić co najmniej dwa kryteria przekrojowe.

Zaznaczyć należy, iż zarówno kryteria identyfikacji IK, jak i sam program, będą podlegały aktualizacji. Mechanizm tejże aktualizacji będzie wykorzystany do unormowania kryteriów wraz ze wzrostem wiedzy na temat funkcjonowania systemów IK, tak aby odpowiednio odzwierciedlały potrzeby ochrony IK.

Zakłada się, że wraz z opracowaniem narzędzi, pozwalających w miarodajny sposób ocenić skutki zniszczenia lub zaprzestania funkcjonowania IK, możliwa będzie rezygnacja z kryteriów systemowych. W efekcie kryteria przekrojowe stosowane byłyby do dowolnie wybranej infrastruktury systemu lub do jakiejkolwiek infrastruktury państwa[10].

Aktualnie ciągle trwają konsultacje dotyczące kryteriów identyfikacji infrastruktury krytycznej w Polsce. Cyklicznie odbywają się spotkania, podczas których głos zabierają eksperci z różnych branż. Tak było również na V Krajowym Forum Ochrony Infrastruktury Krytycznej, które odbyło się w RCB 11 grudnia 2017 roku. Otwierając Forum, dyrektor Rządowego Centrum Bezpieczeństwa, Marek Kubiak, podkreślił znaczenie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), a także zwrócił uwagę, że IK należy traktować szerzej – jako ochronę podstawowych usług w ramach ochrony gospodarczych i społecznych fundamentów państwa. Kluczowym elementem tego Forum było przedstawienie nowego podejścia do ochrony infrastruktury krytycznej. Podkreślono więc konieczność zmian w procesie wyłaniania infrastruktury krytycznej, z uwagi na to, że kryteria przekrojowe nie przystają do niektórych systemów IK, część elementów wchodzących w skład systemów IK, które mają wpływ na świadczenie usług, nie zostało uwzględnionych oraz brak jest możliwości zastosowania obecnych kryteriów do obiektów, które są na niższych poziomach administracji. Ta diagnoza przyczyniła się do zaproponowania nowego spojrzenia na IK – z obiektowego do usługowego[11]. Jak zaznacza Maciej Pyznar, szef Wydziału Ochrony Infrastruktury Krytycznej w RCB: ,,Podstawowym celem zmiany podejścia jest dostosowanie się do zmian w środowisku bezpieczeństwa. Po szczycie NATO w Warszawie Polska, podobnie jak pozostałe państwa członkowskie, złożyła zobowiązanie do wzmocnienia odporności, które w znacznej części wpisuje się w obszar infrastruktury krytycznej i szeroko pojętego zarządzania kryzysowego. Z punktu widzenia NATO odporność państwa na zagrożenia jest funkcją m.in. zapewnienia ciągłości świadczenia podstawowych usług. Odradzające się w Europie zagrożenie terrorystyczne to

[10] M. Pyznar, *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, [w:] *Ochrona infrastruktury krytycznej*, A. Tyburska (red.), Szczytno 2010, s. 105.

[11] OCK, http://www.ock.gov.pl/aktualnosci/aktualnosci/V-Krajowe-Forum-Ochrony-Infrastruktury-Krytycznej/idn:35575, (1.07.2018).

kolejna zmiana w środowisku bezpieczeństwa, którą musimy brać pod uwagę”[12]. Spotkania dotyczące ochrony infrastruktury krytycznej są zatem okazją do przedstawienia, co dotychczas zostało wypracowane w zakresie ochrony IK oraz krótkiego nakreślenia przyszłych działań. Wspomniany Maciej Pyznar po V Krajowym Forum Ochrony Infrastruktury Krytycznej stwierdził: ,,Przedstawiając na Forum założenia zmian, spotkaliśmy się z przychylnym przyjęciem. Operatorzy również zauważają niedoskonałości systemu. W opinii uczestników kierunek zmian jest dobry, ale o ostatecznej akceptacji będziemy mogli mówić, gdy opracujemy szczegóły zaproponowanych rozwiązań, które jak wiadomo decydują również o skuteczności”[13].

Zakończenie

Rozważania dotyczące infrastruktury krytycznej w Polsce rozpoczęto, ale nie jest to proces zakończony. Na podstawie dotychczasowych działań mających na celu poprawę ochrony infrastruktury krytycznej oraz przyglądając się istocie i założeniom Narodowego Programu Ochrony Infrastruktury Krytycznej, można wyciągnąć następujące wnioski:

1. NPOIK to dokument, w którym rząd przedstawia wizję ochrony składników infrastruktury Polski kluczowych dla funkcjonowania państwa.
2. Zapis programu wskazuje wymagania, standardy, cele, priorytety, ale także organy i podmioty ochrony infrastruktury krytycznej czy systemy IK.
3. Istota zadań odnoszących się do infrastruktury krytycznej koncentruje się nie tylko wokół zapewnienia jej ochrony przed zagrożeniami, ale również wokół zminimalizowania czasu trwania ewentualnych uszkodzeń i zakłóceń, łatwego ich usunięcia bez dodatkowych strat dla gospodarki i obywateli.
4. Istota i założenia NPOIK powinny być nie tylko teoretyczne, ale mieć odzwierciedlenie w rzeczywistości, zatem opracowano model pogłębiania współpracy, współodpowiedzialności i zaufania uczestników ochrony infrastruktury krytycznej.

[12] ASPOLSKA, http://aspolska.pl/ochrona-infrastruktury-krytycznej-rzad-zmienia-podejscie/ (1.07.2018).
[13] Ibidem.

Wyniki kwerend, spotkań, konferencji czy też innych działań sprzyjających zgłębieniu tematu poprawienia stanu bezpieczeństwa zarówno ludności, jak i infrastruktury krytycznej wskazują na to, że jest to ciągle proces, który wymaga uwagi i czasu. Niemniej jednak warto się temu poświęcić, by nie zatracić już uzyskanych wyników działań.

Bibliografia

Wydawnictwa zwarte

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

Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, Wrocław 2010.

Tyburska A. (red.), *Ochrona infrastruktury krytycznej*, Szczytno 2010.

Tyburska A., Nepalski M., *Ochrona infrastruktury krytycznej*, Szczytno 2008.

Akty prawne

Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej.

Strony internetowe

ASPOLSKA,http://aspolska.pl/ochrona-infrastruktury-krytycznej-rzad-zmienia-podejscie/, (1.07.2018)

OCK,http://www.ock.gov.pl/aktualnosci/aktualnosci/V-Krajowe-Forum-Ochrony-Infrastruktury-Krytycznej/idn:35575, (1.07.2018).

RCB, http://rcb.gov.pl/o-rcb/ (10.06.2018).