dr hab. inż. Andrzej WŁODARSKI, prof. SGSP
mł. kpt. mgr inż. Adrian BRALEWSKI
Zakład Ochrony Infrastruktury
Katedra Bezpieczeństwa Wewnętrznego
Wydział Inżynierii Bezpieczeństwa Cywilnego
Szkoła Główna Służby Pożarniczej

Istota i cel ochrony infrastruktury krytycznej

Nature and Purpose of Critical Infrastructure Protection

Streszczenie

W artykule poruszona została problematyka dotycząca wagi infrastruktury krytycznej w realiach współczesnego świata, ze szczególnym akcentem na rolę infrastruktury krytycznej w Polsce. Z biegiem czasu oraz wraz z rozwojem gospodarczym, społeczeństwo staje się coraz bardziej zależne od otaczających go dóbr. Te z kolei stają się podatniejsze na różnego typu ataki i awarie. Problem ten zauważają między innymi władze państwowe i organizacje międzynarodowe. W pierwszej części artykułu skupiono się na ogólnej definicji infrastruktury oraz infrastruktury krytycznej, przywołując różne źródła prawa i omawiając ujęte w nich zagadnienia dotyczące pojmowania infrastruktury krytycznej. Część druga jest analizą systemów, możliwości i szans ochrony infrastruktury krytycznej.

Słowa kluczowe: infrastruktura krytyczna (IK), ochrona infrastruktury krytycznej (OIK), NPOIK

Summary

The article presents the problems concerning the importance of critical infrastructure in the realities of the modern world with special emphasis on the role of critical infrastructure in Poland. With time passing and the economic development, the society becomes increasingly dependent on the surrounding property. And these, in turn, are becoming increasingly vulnerable to various types of attacks and failures. The problem has been noticed, among others, by the national authorities and international organizations. In the first part, the article focuses on the definition of critical infrastructure, mentioning various sources of law and discussing the issues, included in the mentioned sources, related to critical infrastructure. The second part is an analysis of the systems, capabilities and opportunities for critical infrastructure protection.

Keywords: critical infrastructure, critical infrastructure protection

Wstęp

Aktywizacja gospodarki oraz wzrost poziomu życia coraz bardziej wpływają na rozwój i znaczenie infrastruktury we współczesnym świecie. Z infrastrukturą mamy do czynienia na każdym kroku. System zaopatrzenia w energię (np. sieci energetyczne), systemy finansowe (np. banki), systemy transportowe (np. drogi, mosty), to tylko niektóre elementy infrastruktury, wpływające na komfort życia człowieka, stanowiące gwarancję zaspokajania jego zróżnicowanych potrzeb społeczeństwa. Aby każda organizacja (instytucja), każde państwo, rozwijało się w niezakłócony sposób w obszarze infrastruktury, potrzebne są rozwiązania systemowe wynikające m.in. z rodzaju infrastruktury krytycznej oraz jej przeznaczenia.

Pojęcie infrastruktury w przeszłości używane było w odniesieniu do obiektów strategicznych, takich jak drogi, mosty, systemy wodne oraz transportowe, a ich ochrona stanowiła ważną część planów obronnych. Koniec zimnej wojny doprowadził do sytuacji, w której uznano, że celowość ataków na te obiekty jest wątpliwa, a ujmowanie tych obiektów w planach obronnych jest bezcelowe. Brak jednoznacznej definicji infrastruktury krytycznej powodował, że stan taki utrzymywał się do lat 90. XX wieku[1], kiedy to do używanego wcześniej pojęcia infrastruktury dodany został przymiotnik krytyczna. Infrastrukturą krytyczną uznano wówczas obiekty, od których w dużym stopniu zależne było społeczeństwo.

Jako przykład uzależnienia społeczeństw od infrastruktury (rozumianej w kontekście ogólnym, bez podziału na jej rodzaje) przytoczyć należy wydarzenia z 13 lipca 1977 r., jakie miały miejsce w Nowym Jorku. Tego dnia nastąpiła jedna z największych awarii linii energetycznych na świecie (tzw. blackout). Przyczyną awarii było uderzenie pioruna w jedną ze stacji zasilania. Miasto wraz z przedmieściami zostało całkowicie pozbawione energii elektrycznej na ponad 25 godzin. Skutki braku zasilania odczuło ponad 12 milionów osób. W sparaliżowanym mieście wybuchły zamieszki i grabieże, które określane były mianem najgorszych w historii miasta. W następstwie owych zamieszek zrabowano i zniszczono ponad 1600 sklepów, wybuchło ponad tysiąc pożarów w całym mieście. Aresztowano 3776 osób. Grabieże oraz zniszczenia spowodowały straty szacowane na ponad 300 milionów dolarów[2].

Zjawiska wynikające z uszkodzeń i awarii obiektów infrastruktury mają tendencje zbliżone do efektu domina. Jedno w porę niezneutralizowane zagrożenie może spowodować zmaterializowanie się problemów o zupełnie innym charakterze, w zupełnie innym miejscu i czasie. Istnieje przy tym wiele czynników i okoliczności sprzyjających powstawaniu potencjalnych zagrożeń, które w niektórych

[1] W. Wójtowicz: Bezpieczeństwo infrastruktury krytycznej, MON, Warszawa 2011, s. 9.
[2] www.elektroda.pl/rtvforum/topic1716001.html (dostęp 28.01.2014).

przypadkach mogą je potęgować. Wśród tych czynników znajdują się niektóre cechy takiego środowiska, do których J. Marczak zalicza:

- zagęszczenie ludności (budynki, wysokie, środki masowej komunikacji);
- uzależnienie warunków bytowych ludności oraz funkcjonowania transportu i gospodarki od dostaw energii elektrycznej, gazu, wody, paliwa, żywności itd.;
- rozbudowana infrastruktura krytyczna, którą stanowią m.in. budynki będące siedzibą władz, centra łączności, centra finansowe, węzły komunikacyjne, mosty, ujęcia wody, elektrownie, stacje radiowo-telewizyjne itp.;
- istnienie potencjalnych źródeł zagrożeń, takich jak składy TŚP (toksycznych środków przemysłowych), składy i rurociągi paliwa, lasy, drogi kołowe i kolejowe o dużej intensywności ruchu;
- niska świadomość zagrożonej ludności oraz słabe przygotowanie władz, społeczeństwa, infrastruktury do reagowania kryzysowego;
- ograniczona możliwość czy w ogóle brak możliwości wsparcia wojskowego władz i społeczeństwa[3].

Kontrola wspomnianych wyżej czynników, jak również dążenie do podniesienia poziomu bezpieczeństwa obywateli jest kluczowym zadaniem, z jakim muszą zmierzyć się władze i których zapewnienie wynika z najważniejszego dokumentu w Polsce, czyli konstytucji.

„Przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych”[4].

Podkreślenia wymaga fakt, że przez to poszanowanie i ochronę nie należy rozumieć tylko bezpośredniej ochrony przed czynnikami fizycznymi (napady, rozboje, urazy), ale również swoistą próbę utrzymania odpowiednio wysokiego poziomu poczucia bezpieczeństwa, które to z kolei wpływa na psychiczny komfort życia obywateli i znajduje swoje odniesienie w innych formach ich aktywności. Owe poczucie bezpieczeństwa i konieczność ogólnie pojętego bezpieczeństwa ściśle łączy się z ochroną infrastruktury krytycznej. Szczególnie istotna jest ochrona tych obiektów IK, których zniszczenie/uszkodzenie może mieć katastrofalne skutki. Ochrona powyższych obiektów w czasach coraz większego uzależnienia społeczeństw od techniki, nabiera nowego bardziej globalnego i opartego na zdalnym sterowaniu znaczenia.

W ochronie infrastruktury dopatrzeć się można elementów odpowiedzialnych za życie tysięcy ludzi; to sprawnie zarządzana infrastruktura daje możliwość zapew-

[3] J. Marczak (kier. nauk.): Przygotowanie i koordynacja połączonych działań obrony terytorialnej i układu pozamilitarnego w sytuacjach kryzysowych, Koordynacja – część druga. AON, Warszawa 2003, s. 12.

[4] Art. 30 Konstytucji RP.

nienia obywatelom odpowiedniego bytu, jak również wpływa na pozytywne postrzeganie władzy w społeczeństwie. Można śmiało powiedzieć, że infrastruktura (zarówno krytyczna, techniczna, jak i ekonomiczno-społeczna) świadczy o zamożności danego kraju, a nawet o szansach jego przyszłego rozwoju.

Celem artykułu jest wprowadzenie czytelnika w tematykę infrastruktury krytycznej oraz przybliżenie podstawowych pojęć, jakie niesie za sobą definicja ochrony infrastruktury krytycznej. Ponadto artykuł ma stanowić wprowadzenie do dalszych rozważań autorów we wskazanej tematyce.

1. Definicja infrastruktury krytycznej

1.1. Geneza i ogólna definicja słowa „infrastruktura"

Termin INFRASTRUKTURA po raz pierwszy pojawił się w drugiej połowie XX w. (o czym pisze R. Radziejewski)[5] i używany był w odniesieniu do obiektów strategicznych, głównie wojskowych, przeznaczonych do stałego użytku (lotniska, poligony, koszary). Termin ten szybko znalazł jednak swoje zastosowanie w innych dziedzinach nauki i życia, m.in. w ekonomii czy zarządzaniu. Oznaczał obiekty, które miały znaczenie dla ekonomistów i właścicieli firm, czyli mówiąc kolokwialnie, stwarzały szansę czerpania z nich korzyści finansowych.

Współcześnie infrastruktura **„oznacza urządzenia i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki"**[6].

Czy taka definicja infrastruktury zawarta w słowniku PWN jest poprawna i pełna? Gdzie można dopatrzeć się jej braków? Otóż pierwszym problemem jest to, czy definiowanie infrastruktury jedynie jako urządzenia i instytucje usługowe jest poprawne? Pierwsze skojarzenia związane z infrastrukturą wzbudzają w wyobraźni widok monstrualnych mostów, budynków i innych budowli, które stanowią o sile i wiedzy człowieka w świecie. Infrastruktura większości ludziom kojarzy się z jakimiś udogodnieniami: łatwiejszy dojazd (drogi), lepszy dostęp do Internetu (nowe światłowody), łatwiejszy dostęp do lekarzy (szpitale). Czy wpisuje się to w jakikolwiek sposób w definicję urządzenia i instytucji, które łączą się w definicji infrastruktury?

URZĄDZENIA – mechanizm lub zespół mechanizmów służący do wykonania określonych czynności (PWN);

INSTYTUCJA – zakład o charakterze publicznym zajmujący się określonym zakresem spraw (PWN)[7].

[5] Radziejewski R.: Ochrona Infrastruktury Krytycznej. Teoria a praktyka. PWN 2014, s. 28.
[6] Słownik PWN http://sjp.pwn.pl, (dostęp 22.12.2014).
[7] Słownik PWN http://sjp.pwn.pl, (dostęp 22.12.2014).

Przytoczone hasła nie oddają w pełni istoty słowa infrastruktura. Nie można obiektów infrastruktury definiować tylko jako mechanizmy lub zakłady. O ile urządzenia kojarzą się z czymś co posiada w sobie jakiś element ruchomy (mechanizm), o tyle nie jest to warunek, który musi spełnić obiekt infrastruktury. Podobnie sprawa się ma z „zakładem o charakterze publicznym". Jako przykład posłużyć może duża fabryka. Mimo że nie będzie miała charakteru publicznego, czyli nie będzie własnością publiczną, może być nazwana infrastrukturą. Co więcej, infrastrukturą o strategicznym znaczeniu dla lokalnej ludności.

Podejmując problem definicji słowa „infrastruktura", warto byłoby spojrzeć na nie, nie tylko przez czysto fizyczne jej znaczenie, ale przez pryzmat jej użyteczności oraz przydatności dla ludzi. Zdecydowanie większe bowiem znaczenie będzie miała dla społeczności odpowiednia dbałość o drogi niż o w pełni zmechanizowaną maszynę w prywatnym zakładzie. Zatem definicja infrastruktury powinna odnosić się do liczby osób, jakie z niej korzystają, i które są od niej w jakiś sposób uzależnione. Infrastruktura powinna mieć zdecydowany wpływ na komfort życia lub na ochronę komfortu tego życia.

1.2. Infrastruktura krytyczna – co to takiego?

W naukach o bezpieczeństwie i w zarządzaniu kryzysowym słowo infrastruktura występuje bardzo często (czasem wręcz nierozerwalnie) z przymiotnikiem „krytyczna". Termin ten ma za zadanie nadać odpowiednią wagę słowa infrastruktura oraz jego znaczenie dla funkcjonowania określonej jednostki terytorialnej. Co więcej, samo słowo „krytyczna" może bardziej odnosić się do sytuacji, jaka ma szansę (ale nie musi) wystąpić w przypadku uszkodzenia jakiegokolwiek z elementów infrastruktury, mającego duży wpływ na prawidłowe funkcjonowanie różnych dziedzin działalności człowieka i państwa.

Z terminem infrastruktura krytyczna po raz pierwszy spotkano się w 1996 r.[8], kiedy to w USA prezydent Bill Clinton utworzył Komisję (President's Commission on Critical Infrastructure Protection – PCCIP), która miała za zadanie przedstawić wszelkie zagrożenia, jakie mogły mieć wpływ na działanie i użytkowanie infrastruktury krytycznej (zarówno fizyczne, jak i cybernetyczne). Zadaniem komisji stało się opracowanie kompleksowej strategii i polityki krajowej, która w najbardziej efektywny sposób mogłaby chronić obiekty IK. Tym samym komisja wyszła z propozycją zmian ustawowych, które mogłyby wpłynąć na poziom bezpieczeństwa IK[9].

W realiach polskich definicje IK oraz zadania podmiotów odpowiedzialnych za jej funkcjonowanie formułuje Ustawa o zarządzaniu kryzysowym (UZK), której celem było przygotowanie państwa do odpowiedzi na coraz częściej wystę-

[8] Skomra W.: Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy. PRESSCOM, Wrocław 2010, s. 92.

[9] J. Ellis, D. Fisher,T. Longstaff, L. Pesante, R. Pethia: Report to the President's Commission on Critical Infrastructure Protection. Software Engineering Institute, USA 1997.

pujące sytuacje kryzysowe powstające w wyniku wielkich awarii budowlanych, awarii przemysłowych czy klęsk naturalnych. Zgodnie z powyższą ustawą, przez infrastrukturę krytyczną należy rozumieć **„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. Infrastruktura krytyczna obejmuje systemy:**

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych”[10].

Wśród wymienionych systemów można wyróżnić (warunkując najbardziej prosty sposób) systemy zdecydowanie specjalistyczne, ukierunkowane na konkretną gałąź przemysłu (np. system zaopatrzenia w energię i paliwa, łączność i sieci teleinformatyczne), jak i te ogólne i zależne od innych systemów (ratownictwa, zapewnienia ciągłości działania administracji publicznej). O ile w pierwszym rodzaju systemów można wyodrębnić konkretne firmy (np. PGE, TVP), na których spoczywają obowiązki wobec danych systemów (np. dobrą praktyką jest zachowanie standardu ISO/IEC 27002 w przypadku ochrony informacji), o tyle w drugim przypadku odpowiedzialność za systemy wydaje się być rozdrobniona na wiele firm, organizacji lub nawet jednostek, że mowa o całościowym ujęciu problemu jest niebywale trudna i wymaga konkretnych działań na poszczególnych szczeblach władzy.

Definicja IK zaczerpnięta z Ustawy o zarządzaniu kryzysowym pozwala na dość szerokie spojrzenie na jej zakres. Pierwsza część definicji IK określa wszystkie systemy i powiązane z nimi funkcjonalnie obiekty, urządzenia itp., które mają znaczenia dla obywateli, przedsiębiorców i instytucji. Od razu nasuwa się tu problem: Czy to, co jest ważne dla przedsiębiorcy prywatnego, musi być ważne dla ogółu obywateli oraz czy przedsiębiorca jest świadomy swojego obowiązku w stosunku do obywateli polegającego na zapewnieniu działania IK?

[10] Art. 3, ust. 2 Ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Jako przykład posłużyć może program komputerowy do zarządzania flotą samochodów ciężarowych w firmie transportowej. Dla przedsiębiorcy program ten ma ogromne znaczenie. Pozwala monitorować trasy pojazdów, obciążenie kierowców, planować przyszłe wyjazdy i prognozować dochody. Nawet drobne uszkodzenia i przestoje w sprawnym działaniu systemu wpływają na dochód przedsiębiorcy i tym samym stają się one dla niego niedopuszczalne. Sam system i jego otoczenie (komputery, serwery itp.) stanowią dla przedsiębiorcy wewnętrzną IK, od której zależy być albo nie być jego firmy. Jakie jednak ma to znaczenie dla zwykłego Kowalskiego niezwiązanego z prywatną firmą? Odpowiedź brzmi: żadne. Problemy z systemem nie przeniosą się na status majątkowy Kowalskiego, nie wpłyną na jego sytuację w pracy ani nie ułatwią mu wykonywania codziennych czynności. Patrząc z tej perspektywy, zdecydowanie własność przedsiębiorców prywatnych, a tym samym infrastruktura, która daje im dochody i odpowiedzialność za nią powinna spoczywać na barkach przedsiębiorców a nie państwa. Z drugiej jednak strony, znaczna część firm w Polsce już jest albo dopiero przechodzi w ręce prywatne. Mowa tu nie o małych rodzinnych przedsiębiorstwach, ale o dużych firmach o znaczeniu lokalnym, krajowym lub nawet międzynarodowym. Takie firmy charakteryzują się tym, że zatrudniają dużą liczbę osób. Stanowią one o dobrej kondycji zarówno gospodarczej, jak i mentalnej regionu. W rękach bowiem lokalnych dużych przedsiębiorstw leży zatrudnienie znacznej części okolicznych mieszkańców, a co za tym idzie wpływa na poziom bezrobocia i inne bardziej „polityczne" nastroje w regionie. Tak dwojaki sposób patrzenia na problem zmusza do refleksji, gdzie jest granica pomiędzy infrastrukturą (w rozumieniu ogólnym), a infrastrukturą krytyczną? Odpowiedzi na to pytanie można znaleźć m.in. w kryteriach pochodzących z „Zielonej Księgi w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej"[11], które wyodrębnili Popescu i Simion:

- dotkliwość skutków w przypadku zakłóceń i uszkodzeń obiektów infrastruktury,
- skutki transgraniczne uszkodzeń infrastruktury,
- współzależności z innymi sektorami i systemami[12].

Znaczenie obiektu w kontekście wskazanych kryteriów pozwala dokładniej określić elementy decydujące o zakwalifikowania infrastruktury jako „krytyczna".

W tym miejscu warto przytoczyć również definicję opracowaną przez ekspertów Komitetu Ochrony Cywilnej NATO. Infrastruktura krytyczna definiowana jest w tym przypadku jako „obiekty, służby i systemy informacyjne, które są tak żywotne dla państwa, że ich uszkodzenie lub zniszczenie mogłoby mieć niebaga-

[11] Zielona Księga w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej. Bruksela 17.11.2005.

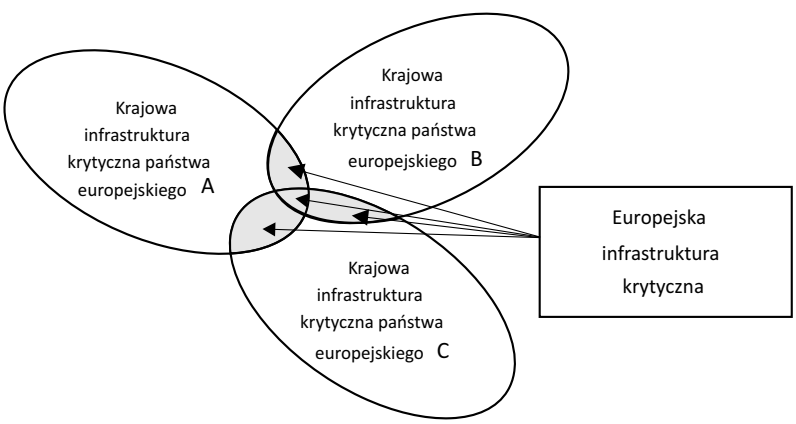
[12] Cristian-Aurelian Popescu, Cristina Petronela Simion: A method for defining critical infrastructures [w:] Energy, Bucharest, 2011.

telny wpływ na bezpieczeństwo państwa, krajową gospodarkę, zdrowie i bezpieczeństwo publiczne oraz prawidłowe funkcjonowanie rządu”[13].

2. Ochrona IK

Z racji określenia (w UZK) infrastruktury krytycznej jako elementów niebywale ważnych dla funkcjonowania państw i obywateli, szczególne znaczenie zaczyna przybierać praktyka ochrony IK. Obowiązek ochrony infrastruktury krytycznej wynika między innymi z członkostwa Polski w Unii Europejskiej oraz w Sojuszu Północnoatlantyckim. Wskutek powiązań systemów o aspekcie transnarodowym, uszkodzenie lub zniszczenie infrastruktury krytycznej w jednym państwie ma wpływ na państwa sąsiednie. Infrastruktura o takim znaczeniu została nazwana Europejską Infrastrukturą Krytyczną (EIK).

„Europejska infrastruktura krytyczna” lub „EIK” oznacza infrastrukturę krytyczną 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 kryteriów przekrojowych. Obejmuje to skutki wynikające z międzysektorowych współzależności z innymi rodzajami infrastruktury (…)”[14]



Rys. 1. Europejska infrastruktura krytyczna

Nie bez znaczenia zatem pozostają uregulowania prawne wynikające z członkostwa Polski w Unii Europejskiej w tej kwestii. W ramach UE ustanowiono dyrektywę w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. Ustanowiła ona kryteria przekrojowe i sektorowe do wytypowania takiej infrastruktury.

[13] Defincja Grupy Ekspertów NATO.
[14] Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.

Kryteria przekrojowe obejmują:
- kryterium ofiar w ludziach;
- kryterium skutków ekonomicznych;
- kryterium skutków społecznych.

Progi tych kryteriów ustalane są przez państwa członkowskie, na które został również nałożony obowiązek corocznego informowania Komisji Europejskiej o liczbie infrastruktur w poszczególnych sektorach.

Kryteria sektorowe określają natomiast charakterystyczne cechy infrastruktury krytycznej państw członkowskich. Obejmują progi liczbowe parametrów charakterystycznych oraz funkcje infrastruktury krytycznej. Kryteria te są niejawne i fakultatywne dla państw UE.

Mówiąc o ochronie infrastruktury krytycznej, po raz kolejny należy odnieść się do Ustawy o zarządzaniu kryzysowym, zgodnie z którą 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”**[15].

Ustawa o zarządzaniu kryzysowym, jak wspomniano wcześniej, była powołana do życia w 2007 r. Jednakże już w 1997 r. po raz pierwszy w prawie polskim wspomniano o konieczności ochrony obiektów kluczowych dla Polski. Ujęto to w Ustawie o ochronie osób i mienia w sposób następujący: **„Obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa podlegają obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne (…)”**[16].

Bardzo ważnym aktem prawnym w Polsce dotyczącym zagadnień ochrony IK jest Ustawa o powszechnym obowiązku obrony Rzeczpospolitej, zgodnie z którą zapewnienie bezpieczeństwa państwa związane jest z określeniem obiektów szczególnie ważnych dla bezpieczeństwa i obronności, ich kategorii oraz zadań w zakresie ich ochrony[17]. Dodatkowo, w 2003 r. wprowadzono rozporządzenie Rady Ministrów regulujące zasady ochrony obiektów szczególnie istotnych dla bezpieczeństwa i obronności państwa[18]. Dokumenty te nie odnoszą się bezpośrednio do IK, część obiektów zakwalifikowanym do IK może jednak podlegać zawartym w tych dokumentach unormowaniom.

[15] Art. 3, ust. 3 Ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
[16] Art. 5, ust. 1 Ustawy z 22 sierpnia 1997 r. o ochronie osób i mienia.
[17] Art 6, ust. 5, Ustawy o powszechnym obowiązku obrony Rzeczpospolitej Polskiej, DzU z 2006 r. nr 104, poz. 708 i 711.
[18] Rozporządzenie Rady Ministrów z 24 czerwca 2003 r. W sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, DzU z 2003 r. nr 116, poz. 1090.

Ochrona infrastruktury krytycznej znalazła również swoje miejsce w Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej 2014, w której zagadnienie to ujęto następująco: **„Niezwykle istotne jest zapewnienie warunków ochrony infrastruktury krytycznej. Infrastruktura ta obejmuje kluczowe systemy i elementy zapewniające bezpieczeństwo państwa i jego obywateli oraz sprawne funkcjonowanie organów administracji publicznej, instytucji i przedsiębiorców. Ochrona infrastruktury krytycznej jest obowiązkiem operatorów i właścicieli, którzy są wspierani przez potencjał administracji publicznej. W Polsce wdrażane jest nowatorskie podejście w tym zakresie, bazujące na zasadach współodpowiedzialności zainteresowanych stron, rozbudowanej współpracy i wzajemnego zaufania. Działania państwa polegają na ewentualnym uruchomieniu sytemu zarządzania kryzysowego na wypadek zakłócenia funkcjonowania infrastruktury krytycznej, a także na podnoszeniu świadomości, wiedzy i kompetencji oraz propagowaniu współpracy w tym obszarze"**[19].

Wszystkie przytoczone wyżej dokumenty regulują kwestię obowiązku ochrony infrastruktury krytycznej i to, na kim on spoczywa. W znacznej mierze obowiązek ten jest skierowany na „operatorów i właścicieli". Pozostaje zatem pytanie, czy to podejście jest słuszne?

Nawet pobieżna analiza nazw wszystkich systemów IK wskazuje, że mają one kluczowe znaczenie dla bezpieczeństwa państwa i obywateli. Logicznym zatem w takim przypadku jest, żeby państwo w większym stopniu niż prywatni właściciele decydowało o infrastrukturze krytycznej. Nawet więcej, obywatele mają prawo wymagać od władz, aby w należyty sposób dbały o ich bezpieczeństwo.

Właścicielom obiektów infrastruktury zdecydowanie bardziej niż na działaniach prewencyjnych będzie zależało na działaniach mogących przynieść jakieś konkretne zyski. Działania prewencyjne mają to do siebie, że zwykle nie widać efektów jakie przynoszą. Ponadto działania te mają na celu ochronę przed zdarzeniami potencjalnymi, czyli takimi, które tak naprawdę mogą nie wystąpić. Dlatego też prywatni inwestorzy, będą szukali możliwości szybkiego cięcia kosztów, i zrobią to zazwyczaj z puli przeznaczonej na działania zapobiegawcze i prewencyjne. Czy na ryzyko takiego zachowania mogą sobie pozwolić władze i oddać odpowiedzialność za IK tylko właścicielom? Pytanie jest trudne, ale na mocy obowiązującego prawa tak robią.

Patrząc jednak z drugiej strony, to właśnie właściciele i zarządcy obiektów IK z racji tego, że mają bezpośredni kontakt z tymi obiektami są najbardziej świadomi zagrożeń, na jakie mogą być one narażone. To także oni w najbardziej realny sposób będą wiedzieli, jakie środki ochrony zastosować, aby zapewnić, bądź co bądź swoim interesom, odpowiedni bufor bezpieczeństwa. Występuje tu jednak obawa, czy osoba będąca właścicielem będzie sobie w stanie sama poradzić w przypadku zmasowanego ataku na będącą w jej posiadaniu IK? Co więcej, jeśli jeden organ skupia w sobie kilka systemów IK? Czy dalej musi sam dbać o wszystko?

[19] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warszawa 2014, s. 35.

Rozważmy przykład. Fikcyjna rafineria będąca prywatną firmą zaopatrującą w paliwa znaczną część kraju (również fikcyjnego). W firmie pracuje wiele osób, gdzie większość stanowi ludność lokalna, z sąsiednich miast. Na skutek ataku hakerów dochodzi do częściowego zatrzymania dostaw paliw do rafinerii. Jednoczesny masowy atak terrorystyczny na obiekty rafinerii oraz rurociągi transportujące surowce z i do zakładu wyłączają ją z prawidłowego funkcjonowania na długie miesiące. Zakład staje przed groźbą upadłości. W wyniku ataku automatycznie uszkodzone zostają systemy IK, takie jak: zaopatrzenia w energię i paliwa; produkcji, składowania, przechowywania i stosowania substancji chemicznych, w tym rurociągi substancji niebezpiecznych. To jednak nie wszystko. Zakład słynął z bardzo dobrej polityki prospołecznej; wszystkim swoim pracownikom i ich rodzinom zapewniał bezpłatną opiekę medyczną oferowaną na terenie zakładu (system ochrony zdrowia). Idąc dalej tym tokiem rozumowania: na terenie zakładu funkcjonowała Zakładowa Straż Pożarna, która swoim działaniem chroniła nie tylko zakład, ale również wspomagała w działaniach Państwową Straż Pożarną (system ratowniczy). Czy wówczas, gdy w jednym zakładzie skupia się zależność wielu systemów IK można je pozostawić same sobie z ochrona tego co decyduje o naszym wspólnym dobru?

Przytoczony przykład pokazuje bardzo ważną cechę wszystkich systemów, mianowicie taką, że są one ze sobą ściśle powiązane. Działania w jednym systemie na pewno nie pozostaną bez oddźwięku w innych systemach. Taki proces, który w sposób nieunikniony wywołuje kolejne zdarzenia, nazywany jest „efektem domina”[20] (Skomra). Ochrona IK powinna zatem przybierać równie uniwersalne znaczenie, a stosowanie środków ochrony docelowo powinno zostać zoptymalizowane dla wszystkich systemów.

Szczególny przypadek występuje, gdy awarie i uszkodzenia IK mają znaczenie nie tylko krajowe, ale transgraniczne. Może bowiem dochodzić do sytuacji, gdy elementy IK przenikają się między granicami (ma to miejsce np. w przypadku dostaw energii elektrycznej lub telefonii). Wówczas logiczne jest, że ochrona infrastruktury krytycznej przybiera wymiar międzynarodowy i jest wsparta międzynarodową współpracą.

Mówiąc o ochronie IK, nie można pominąć jeszcze jednego ważnego dokumentu, mianowicie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), którego „celem jest stworzenie warunków poprawy bezpieczeństwa IK. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny – podniesienie bezpieczeństwa Polski. Decydujące znaczenie dla osiągnięcia tego celu mają:

- podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów jej ochrony,

[20] Skomra W.: Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy, Wyd. PRESSCOM Sp. z o.o, Wrocław 2010, s. 92.

- zainicjowanie skutecznej współpracy między uczestnikami Programu w obszarze ochrony IK"[21].

Z priorytetów programu wynika, że uświadomienie społeczeństwa w dziedzinie znaczenia i ochrony IK stanowi cel nadrzędny. W dobie coraz częstszych ataków terrorystycznych, punkty o kluczowym znaczeniu dla państwa są szczególnie a nie podatne. Co za tym idzie uświadomienie operatorów i użytkowników IK oraz wyczulenie ich na niepożądane działania osób trzecich leży jak najbardziej w dziedzinie bezpieczeństwa RP.

Na poziomie rządowym oraz wojewódzkim tworzy się ponadto plany ochrony infrastruktury krytycznej[22], które zawierają:

- wykaz obiektów i systemów IK;
- charakterystykę zagrożeń dla IK oraz ocenę ryzyka ich wystąpienia;
- charakterystykę zasobów możliwych do wykorzystania w celu ochrony infrastruktury krytycznej;
- warianty działania w sytuacji zagrożeń lub zakłócania funkcjonowania infrastruktury krytycznej
- warianty odtwarzania IK;
- zasady współpracy administracji publicznej z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń IK w zakresie jej ochrony, w tym zasady przekazywania informacji;
- wskazanie terminów i tryby aktualizacji planu[23].

Zapewnienie ciągłości i sprawnego funkcjonowania infrastruktury krytycznej spoczywa na administracji rządowej i samorządowej[24]. Właściciele oraz posiadacze obiektów, urządzeń i instalacji infrastruktury krytycznej są zobowiązani do ich ochrony. Ochrona ta w szczególności polega na przygotowywaniu i wdrażaniu stosownie do przewidywanych zagrożeń na podstawie analiz i prognoz, planów ochrony infrastruktury krytycznej na wypadek zaistnienia zagrożenia oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia. Właściciele oraz posiadacze obiektów IK mają również obowiązek wyznaczenia osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami odpowiedzialnymi za ochronę infrastruktury krytycznej (służby, straże, centra zarządzania kryzysowego itp.)[25].

---

[21] Narodowy Program Ochrony Infrastruktury Krytycznej, 2013.

[22] Wytyczne co do planów ochrony IK zawarto w Rozporządzeniu Rady Ministrów z 30 kwietnia, 2010 r. w sprawie planów ochrony infrastruktury krytycznej. DzU z 2010 r. nr 83, poz. 542.

[23] K. Sienkiewicz-Małyjurek, F.R. Krynojnewski: Zarzadzanie kryzysowe w administracji publicznej, s. 35.

[24] Art. 23 Ustawy o zarządzaniu kryzysowym z 2007 DzU z 2011 r. nr 22, poz. 114.

[25] Problematykę współpracy i obowiązków organów administracji publicznej i służb odpowiedzialnych za bezpieczeństwo państwa z właścicielami elementów i całych systemów IK oraz innymi służbami publicznymi i organami reguluje Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, DzU z 2010 r. nr 83, poz. 541.

Do zadań z zakresu ochrony infrastruktury krytycznej należą w szczególności:

- gromadzenie oraz wymiana informacji o zagrożeniach dla IK,
- opracowanie i wdrażanie procedur na wypadek wystąpienia zagrożeń IK,
- odtwarzanie infrastruktury krytycznej,
- współpraca między administracją publiczną a właścicielami, operatorami oraz posiadaczami IK w zakresie jej ochrony.

Natomiast do metod ochrony infrastruktury krytycznej (rys. 1.) zaliczamy przedsięwzięcia takie, jak:

- ochrona fizyczna,
- ochrona techniczna,
- ochrona osobowa,
- ochrona teleinformatyczna,
- ochrona prawna,
- wsparcie etapu odbudowy[26].

Rys. 2. Ochrona infrastruktury krytycznej

Źródło: Prezentacja RCB na temat infrastruktury krytycznej

Zastosowanie konkretnych rodzajów ochrony powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK, przy czym:

1) ochrona fizyczna – jest to zespół przedsięwzięć minimalizujących ryzyko zakłócenia funkcjonowania IK przez osoby, które znalazły się na terenie IK w sposób nieautoryzowany; ochrona fizyczna obejmuje ochronę osób, rozumianą jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej, ochronę mienia, czyli działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do

[26] Infrastruktura krytyczna, RCB.

wstępu osób nieuprawnionych na teren chroniony, a także techniczne środki ochrony, czyli wykorzystanie w ochronie obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych itp. środków,

2) ochrona techniczna – to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z technicznymi aspektami budowy i eksploatacji obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej; ochrona techniczna IK obejmuje: kwestie związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi przepisami i normami np. budowlanymi, przeciwpożarowymi itp., działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług, działania techniczne mające na celu zapewnienie ciągłości funkcjonowania IK,
3) ochrona osobowa – zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które przez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu; ochronę tę należy zatem powiązać z pracownikami oraz innymi osobami czasowo przebywającymi w obrębie IK (usługodawcy, dostawcy, goście),
4) ochrona teleinformatyczna – stanowi zespół przedsięwzięć, procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych; oznacza to również ochronę przed cyberatakami, cyberprzestępstwami i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom,
5) ochrona prawna – zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością osób fizycznych lub przedsiębiorców (prywatnych krajowych lub zagranicznych), których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK; oznacza to zastosowanie narzędzi prawnych niedopuszczających, przez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów, do np. wrogiego przejęcia, fuzji czy też sprzedaży niektórych elementów infrastruktury, której efektem mogą być zakłócenia w jej funkcjonowaniu,
6) plany odtwarzania, rozumiane jako odtwarzanie funkcji realizowanych przez IK.

W ochronie IK istotne znaczenie ma również współpraca sektora publicznego z sektorem prywatnym oraz współpraca wewnątrz tych sektorów. Jej głównym elementem jest wypracowanie na drodze konsensusu przejrzystych zasad i procedur między organami i służbami państwa a właścicielami oraz posiadaczami samoistnych i zależnych IK. Wynika to z faktu, iż znaczna część infrastruktury, mającej kluczowe znaczenie dla bezpieczeństwa państwa, znajduje się w posiadaniu sektora prywatnego[27].

[27] www.rcb.gov.

Istotny wpływ na bezpieczeństwo i ochronę IK w Polsce mają również stopnie alarmowe ustanowione na mocy Ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, (zm. ustawą z 17 lipca 2009 r.) oraz zarządzenia Prezesa Rady Ministrów. W ramach stopni alarmowych realizowane są zadania w celu ochrony przed atakiem i przeciwdziałania zagrożeniu atakiem terrorystycznym lub sabotażowym[28]. Istnieją cztery stopnie alarmowe: ALFA, BRAVO, CHARLIE oraz najwyższy stopień DELTA. Każdy z nich wprowadza szereg zadań do realizacji przez podmioty wykonawcze na rzecz ochrony infrastruktury oraz ludności[29].

Do zadań realizowanych na rzecz ochrony zagrożonej infrastruktury (nie tyko krytycznej) przy wprowadzeniu pierwszego stopnia alarmowego (ALFA) należą:
- informowanie i dostępność personelu,
- kontrola pojazdów i osób na terenie obiektów,
- sprawdzenie obiektów i pomieszczeń,
- sprawdzenie środków łączności i systemu alarmowego,
- przegląd procedur i zadań.

Do zadań realizowanych na rzecz ochrony zagrożonej infrastruktury przy wprowadzeniu drugiego stopnia alarmowego (BRAVO) należą wszystkie przedsięwzięcia pierwszego stopnia, oraz:
- ostrzeżenie personelu,
- odsunięcie pojazdów od obiektów i kontrola parkowania,
- wzmocnienie ochrony obiektów,
- kontrola osób, bagażu i przesyłek pocztowych do urzędów,
- ochrona środków transportu służbowego,
- przegląd zapasów i sprzętu.

Do zadań realizowanych na rzecz ochrony zagrożonej infrastruktury przy wprowadzeniu trzeciego stopnia alarmowego (CHARLIE) należą wszystkie przedsięwzięcia pierwszego i drugiego stopnia, oraz:
- dyżury dla osób funkcyjnych;
- ścisła kontrola osób i pojazdów, ograniczenie ogólnego dostępu;
- wzmocnienie służby ochronnej, uzbrojenie uprawnionych osób ochrony;
- dodatkowe procedury ochrony i osłony kontrwywiadowczej;
- dodatkowe procedury ochrony w placówkach dyplomatycznych.

Do zadań realizowanych na rzecz ochrony zagrożonej infrastruktury przy wprowadzeniu czwartego stopnia alarmowego (DELTA) należą wszystkie przedsięwzięcia pierwszego, drugiego i trzeciego stopnia, oraz:
- zapewnienie ciągłości pracy sztabów kryzysowych;
- zidentyfikowanie wszystkich pojazdów na terenie obiektu;
- wprowadzenie pełnej kontroli dostępu do obiektu;
- prowadzenie częstych kontroli na zewnątrz obiektu i na parkingach;
- ograniczenie liczby podróży służbowych i wizyt.

[28] Art. 23 Ustawy o zarządzaniu kryzysowym z 2007 r., DzU z 2011 r. nr 22, poz. 114.
[29] Infrastruktura krytyczna, RCB.

Dzięki podwyższaniu gotowości podmiotów odpowiedzialnych za ochronę infrastruktury oraz jej posiadaczy, każdy stopień alarmowy, w zależności od powagi sytuacji, umożliwia użycie całej gamy instrumentów zmniejszających ryzyko uszkodzenia, zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej.

W świetle końcowych rozważań o IK i jej ochronie, warto zastanowić się nad jeszcze jedną kwestią. Czy w realiach polskich istnieje instytucja, która miałaby prawo i obowiązek kontroli i nakładania kar za złe praktyki w odniesieniu do infrastruktury krytycznej? Jakie bowiem znaczenie mają dokumenty mówiące o ochronie infrastruktury krytycznej, jeśli nie będzie organu trzymającego nad nią pieczy. Należałoby zadać sobie pytanie, czy taką kontrolę powinno sprawować RCB (przygotowujące NPOIK) czy może ABW (odpowiedzialne m.in. za ataki terrorystyczne) albo NIK (naczelny i niezależny organ kontroli państwowej z misją strażnika grosza publicznego[30]), sprawując kontrolę nad prawidłowo zainwestowanymi środkami w kontekście IK? A może całkiem inna organizacja? Pytanie to należy pozostawić do dyskusji.

Podsumowanie

Tematy dotyczące IK są ciągle tym elementem nauki, o którym warto dyskutować, i który należy rozwijać. Stanowi to jednak bardzo dobre źródło możliwości i szans na nowe podejście do problemu i ujęcie go w możliwie najciekawszy sposób.

IK, ze względu na swoje znaczenie oraz obecność i wpływ na wszystkie dziedziny życia, stanowi o bezpieczeństwie każdego kraju. Co więcej, IK często jest tym fragmentem decydującym o funkcjonowaniu państwa, który na pierwszy rzut jest narażony na działania mające na celu jego destabilizację. Działania terrorystyczne, wojenne czy wewnętrzne akty sabotażu są tymi zdarzeniami, które jako pierwszy obszar oddziaływania wybierają infrastrukturę krytyczną. Co więcej ataki na IK chyba w największej mierze będą w stanie wpłynąć na destabilizację porządku w państwie oraz bezpieczeństwa w regionie. Niepodważalna jest zatem rola IK. W Polsce i Europie problem ten jest coraz bardziej dostrzegalny i rozwijany. Można powiedzieć, że w polskich realiach impulsem do podjęcia rozważań o infrastrukturze krytycznej stała się UZK (Lidwa). To właśnie UZK stała się podstawą do stworzenia NPOIK, a co za tym idzie nakreślenia ścieżek postępowania ze zdarzeniami zagrażającymi infrastrukturze.

Ochrona IK niesie za sobą pewne, i to niemałe, koszty. A wszędzie tam, gdzie w grę wchodzą pieniądze, konieczna staje się dokładna analiza problemu. Im więcej przeanalizowanych i poddanych dyskusji pomysłów i propozycji dotyczących OIK, tym większa szansa na znalezienie rozwiązania zbalansowanego między przeznaczonymi środkami, a zachowaniem odpowiedniego poziomu bezpieczeństwa.

[30] http://www.nik.gov.pl/o-nik/, dn. 28.01.2015 r.

Literatura

Akty prawne

[1] Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.
[2] Ustawa z 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, DzU 1967, nr. 44, poz. 220.
[3] Ustawa z 22 sierpnia 1997 r. o ochronie osób i mienia, DzU 2007, nr. 114, poz. 740.
[4] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, DzU 2007, nr 89, poz. 590.
[5] Rozporządzeniu Rady Ministrów z 30 kwietnia, 2010 r w sprawie planów ochrony infrastruktury krytycznej. DzU z 2010 r. nr 83, poz. 542.
[6] Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, DzU z 2010 r. nr 83, poz. 541.

Publikacje i artykuły naukowe

[7] Lidwa W., Krzeszowski W., Więcek W., Kamiński P.: Ochrona Infrastruktury krytycznej. Wydawnictwo AON, Warszawa 2012.
[8] Marczak J.: Przygotowanie i koordynacja połączonych działań obrony terytorialnej i układu pozamilitarnego w sytuacjach kryzysowych „Koordynacja" – część druga. AON, Warszawa 2003.
[9] Radziejewski R.: Ochrona Infrastruktury. Krytycznej Teoria a praktyka. PWN, 2014.
[10] Sienkiewicz-Małyjurek K.F., Krynojnewski R.: Zarządzanie kryzysowe w administracji publicznej. Difin, Warszawa 2010.
[11] Skomra W.: Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy. PRESSCOM, Wrocław 2010.
[12] Tyburska A.: Ochrona infrastruktury krytycznej. Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2012.
[13] Wójtowicz W.: Bezpieczeństwo infrastruktury krytycznej. MON, Warszawa 2011.
[14] Cristian-Aurelian Popescu, Cristina Petronela Simion: A method for defining critical infrastructures [w:] Energy, Bucharest, 2011.

Dokumenty

[15] Ellis J., Fisher D., Longstaff T., Pesante L., Pethia R.: Report to the President's Commission on Critical Infrastructure Protection, Software Engineering Institute, USA 1997.
[16] Zielona Księga w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej, Bruksela 17.11.2005.
[17] Narodowy Program Ochrony Infrastruktury Krytycznej, 2013.
[18] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

Strony internetowe

[18] http://sjp.pwn.pl (dostęp 22.12.2014).
[19] www.elektroda.pl/rtvforum/topic1716001.html (dostęp 28.01.2014).