Józef SADOWSKI

OCHRONA INFRASTRUKTURY KRYTYCZNEJ. UREGULOWANIA PRAWNE

Infrastruktura krytyczna, to zgodnie z polskim prawodawstwem 11 systemów, które mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli, muszą więc podlegać specjalnej ochronie. Dwa z tych systemów (zaopatrzenia w energię, surowce energetyczne i paliwa oraz transportowe) wchodzą w skład Europejskiej Infrastruktury Krytycznej a ich szczególna ochrona wynika z członkostwa Polski w Unii Europejskiej oraz w Sojuszu Północnoatlantyckim. W artykule scharakteryzowano te systemy, oraz podstawy prawne normujące bezpieczeństwo infrastruktury krytycznej w Polsce. Opisano także ustanowione 4 stopnie alarmowe oraz ich wpływ na bezpieczeństwo i ochronę IK. Przedstawiono cel tworzenia i zakres treści Narodowego Programu Ochrony Infrastruktury Krytycznej oraz Planu ochrony infrastruktury krytycznej.

WSTĘP

Termin infrastruktura krytyczna (IK) odnosi się przede wszystkim do zasobów krajowych mających podstawowe znaczenie dla funkcjonowania państwa i jego obywateli. Pojęcie to oznacza obiekty fizyczne, systemy zaopatrzenia, technologie i sieci informatyczne, które w wyniku zniszczenia, zakłócenia lub uszkodzenia stają się niedostępne przez dłuższy okres, a tym samym mogą znacząco uderzać w społeczne lub ekonomiczne warunki społeczeństwa, lub wpływać na możliwości zapewnienia obrony i bezpieczeństwa narodowego. Infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (a w tych systemach obiekty, urządzenia bądź instalacje) niezbędne do funkcjonowania gospodarki i państwa. Pełni ona kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka, infrastruktura krytyczna może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu, przez co zagrożone może być życie i mienie obywateli. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa.

1. INFRASTRUKTURA KRYTYCZNA W POLSCE

Zgodnie ze znowelizowaną Ustawą o zarządzaniu kryzysowym, IK są 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" [7, art.3, pkt. 2] .

W Rzeczypospolitej Polskiej infrastruktura krytyczna wchodzi w skład 11 systemów, które mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

IC obejmuje [3] :

a) systemy zaopatrzenia w energię, surowce energetyczne i paliwa:
   - do produkcji, przesyłania i dystrybucji energii elektrycznej (energetyka),
   - do produkcji, transportu i dystrybucji paliw gazowych,
   - do produkcji, transportu i dystrybucji ropy naftowej i produktów ropopochodnych,
   - do produkcji, transportu i dystrybucji ciepła;
b) systemy łączności, zapewniające przekazywanie informacji, obejmujące pocztę oraz telekomunikację, jak również radiofonię i telewizję;
c) sieci teleinformatyczne, zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego, dla danego rodzaju sieci, urządzenia końcowego;
d) systemy finansowe, to ogół norm prawnych oraz zespół instytucji finansowych, których zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa;
e) system zaopatrzenia w żywność, to dziedzina gospodarki, na którą składa się wytworzenie środków produkcyjnych (np.: nawozy, pasze) i usług dla rolnictwa, produkcja i pozyskiwanie surowców żywnościowych (w rolnictwie, rybactwie, leśnictwie, łowiectwie), skup surowców żywnościowych, ich przechowywanie i transport, przetwórstwo surowców żywnościowych, obrót towarowy produktami żywnościowymi (magazynowanie i przechowywanie żywności, handel hurtowy i detaliczny, eksport i import) oraz system bezpieczeństwa żywności obejmujący wszystkie składowe łańcucha zaopatrzenia w żywność;
f) system zaopatrzenia w wodę (woda pitna, ścieki, wody powierzchniowe) to powiązane ze sobą przedsiębiorstwa i urządzenia pobierające, uszlachetniające, dostarczające i oczyszczające wodę dla ludności i przemysłu;
g) system ochrony zdrowia (apteki, szpitale, przychodnie) to zespół osób i instytucji mający za zadanie zapewnić opiekę zdrowotną ludności, a jego sprawne funkcjonowanie (wraz z systemem ratowniczym) jest gwarantem praw obywatela zapisanych w Konstytucji;
h) transportowe (drogi, kolej, lotniska, porty) – czyli możliwość przemieszczania się ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu;
i) systemy ratownicze – ogół środków i przedsięwzięć organizacyjnych podejmowanych w celu ratowania zdrowia i życia, mienia i środowiska, znajdującym się w niebezpieczeństwie oraz przewidywania, rozpoznawania i likwidacji skutków zdarzeń;
j) zapewniające ciągłość działania administracji publicznej, czyli realizację prawa władczego wykonywania zadań przypisywanych przez porządek prawny państwu i jego organom lub innym podmiotom wykonującym funkcje władcze;

k) k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągi substancji niebezpiecznych).

Graficzne zobrazowanie IK przedstawia rys. 1 oraz tabela 1.

Z przytoczonej oficjalnej definicji wynika, że infrastruktura krytyczna odgrywa szczególną rolę w zapewnieniu ciągłości funkcjonowania państwa, jego organów, instytucji, służb oraz wymiany informacji między nimi. Sprawność infrastruktury krytycznej zapewnia określony poziom i ciągłość dystrybucji tych usług, za które odpowiada państwo. Jej właściwe funkcjonowanie pozwala także na efektywne wykorzystywanie posiadanych zasobów w razie nadzwyczajnych wydarzeń, zakłócających normalne funkcjonowanie państwa i jego gospodarki.

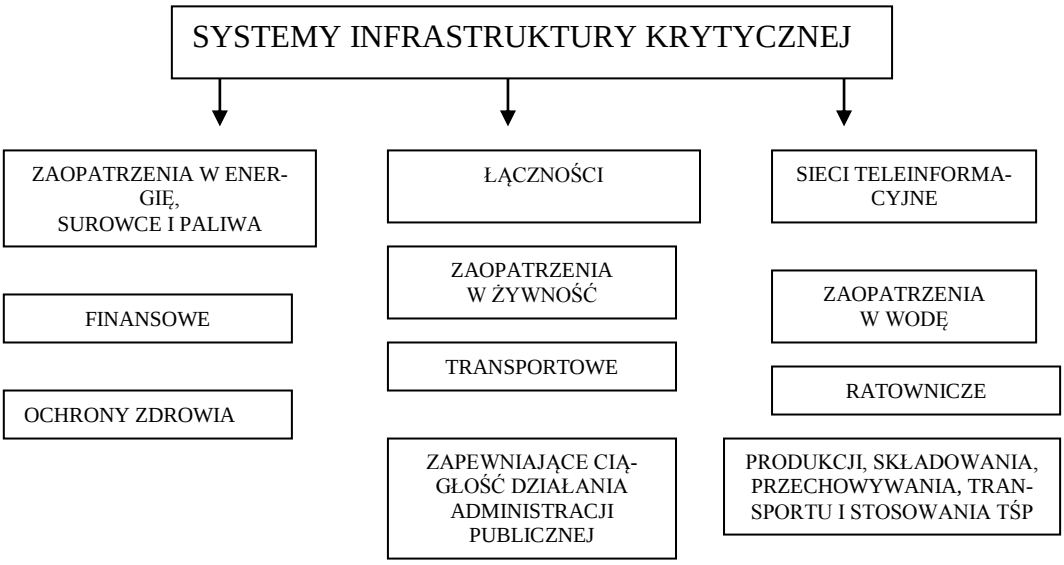
Sprawność dużej części zasobów uznawanych za infrastrukturę krytyczną, warunkuje także postęp technologiczny i rozwój gospodarczy. Tak jest m.in. w przypadku systemów dostaw paliw płynnych dla sektora transportowego oraz energii elektrycznej dla zakładów produkcyjnych. Długotrwałe utrudnienia w tym obszarze zawsze mają poważne skutki gospodarcze, co przekłada się bezpośrednio na możliwości państwa i jego obywateli. Przejawia się to m.in. zmniejszeniem potencjału obronnego, przeszkodami w realizacji przez państwo zadań istotnych społecznie czy mniejszymi wpływami do budżetu. Taka sytuacja będzie więc miała także bezpośrednie przełożenie na komfort życia obywateli i zaburzenie życia społecznego. Trudno wyobrazić sobie funkcjonowanie kilkusettysięcznej aglomeracji miejskiej, pozbawionej dłużej niż kilka godzin np. dostaw energii elektrycznej, czy wody pitnej. A z takimi przypadkami spotykamy się już w naszym kraju po ostatnich wichurach (np. orkan Grzegorz). Przedłużanie się tego stanu doprowadziłoby niewątpliwie do anarchizacji zachowań społecznych, gdyby właściwe służby nie przywróciły sprawności uszkodzonych systemów i porządku publicznego.

Infrastruktura krytyczna ma kluczowe znaczenie dla istnienia państwa, a w jego ramach – zorganizowanego społeczeństwa. Jeśli następuje zakłócenie w jej funkcjonowaniu, państwo i jego instytucje mogą utracić w całości lub części zdolność do wykonywania swoich podstawowych funkcji administracyjnych i usługowych, jak również do sprawowania rzeczywistej kontroli nad całym swoim terytorium. Utrata IK uniemożliwia rozwój gospodarczy i społeczny, a w pewnych przypadkach może nawet doprowadzić do rozkładu życia społecznego. Choć jest to wizja skrajna, taka sytuacja jest jednym z głównych powodów pojawiania się podmiotów określanych jako „państwa w stanie rozkładu" czy obszarów poza jakąkolwiek kontrolą organów państwowych. Przykładem może być sytuacja w państwach Bliskiego Wschodu i płn. Afryki, gdzie w wyniku zniszczeń spowodowanych działaniami zbrojnymi, jeszcze przez kilka kolejnych lat w wielu miastach nadal nie przywrócono regularnych dostaw energii elektrycznej i wody. Miało to określony wpływ na nastroje lokalnej ludności, jak również na ogólny brak bezpieczeństwa w tych miastach.

Przenosząc te rozważania na polski grunt, można stwierdzić, że na razie nie mamy powodów do niepokojów tego rodzaju. Nie oznacza to jednak, że IK w Polsce jest wolna od zagrożeń, a społeczeństwo od skutków jej celowego uszkodzenia lub awarii. Stosownie do skali i źródeł zagrożeń, infrastruktura ta powinna być rozwijana i chroniona przy użyciu odpowiednich instrumentów. Podobnie jak w innych państwach, także w Polsce, nowoczesna i sprawna infrastruktura krytyczna, niezależnie od pojawiających się zagrożeń, jest czynnikiem decydującym o skuteczności funkcjonowania państwa. W sytuacjach nadzwyczajnych przesądza także de facto o jego przetrwaniu [4, s.30].

Elementy systemów infrastruktury krytycznej stanowią zbiór informacji niejawnych i to powoduje, że do decydowania o ich składzie i funkcjonowaniu ma wyspecjalizowana grupa osób, posiadająca certyfikat potwierdzający dostęp do informacji o charakterze niejawnym.

Podstawowym kryterium kwalifikowania określonych obiektów jako infrastruktury krytycznej jest ich podstawowy wpływ na bezpieczeństwo państwa i obywateli. Szczegółowe kryteria przygotowywane są przez Rządowe Centrum Bezpieczeństwa (RCB) we współpracy z właściwymi ministrami i organami centralnymi odpowiedzialnymi za tę część infrastruktury, którą potencjalnie można zaliczyć do krytycznej. Wejście w życie ustawy o zarządzaniu kryzysowym stworzyło podstawowe mechanizmy zorganizowanej



Rys. 1. *Skład systemów infrastruktury krytycznej [7]*

ochrony infrastruktury krytycznej i zdefiniowało systemy wchodzące w jej skład. Niemniej ochrona obiektów budowlanych, urządzeń, instalacji czy usług, które ustawa uznaje za IK, nie rozpoczęła się wraz z jej uchwaleniem. Była prowadzona już wcześniej, choć w sposób nie w pełni skoordynowany. Odpowiednie przepisy znajdują się od dawna w aktach prawnych rożnej rangi (ustawy, rozporządzenia) zarówno z obszaru szeroko pojętej obronności, instytucjonalnej ochrony osób i mienia, jak i rożnych

Tab. 1. *Przykładowa klasyfikacja kategorii obiektów infrastruktury krytycznej [2]*

System	Rodzaje obiektów
Zaopatrzenie w energię i paliwa	Elektrownie i inne obiekty elektroenergetyczne, bazy, składy i magazyny paliw, zakłady mające bezpośredni związek z wydobywaniem kopalin i ich pochodnych, sieci transportu, przesyłu i dystrybucji energii i paliw.
Łączność i sieci teleinformatyczne	Infrastruktura operatorów publicznych świadczących usługi pocztowe, sieci telekomunikacyjne i teleinformatyczne oraz związane z nimi obiekty, a także systemy teleinformatyczne służące do przetwarzania danych i związane z nimi obiekty. Obiekty Telewizji Publicznej oraz Polskiego Radia.
Finansowy	Obiekty NBP oraz BOK, PWPW S.A., Mennicy Państwowej S.A. oraz obiekty i systemy istotne dla zapewnienia stabilności systemu finansowego, systemy płatności, systemy rozliczeń i rachunku papierów wartościowych wraz z obsługującą infrastrukturą oraz rynki regulowane.
Zaopatrzenia w żywność i wodę	Obiekty bezpośrednio związane z produkcją żywności i gromadzeniem wody, a także infrastruktura związana z przechowywaniem i transportem do bezpośrednich odbiorców.
Ochrona zdrowia	Obiekty i systemy istotne ze względu na zapewnienie opieki i świadczeń zdrowotnych obywatelom (szpitale, placówki zdrowia), magazyny rezerw państwowych produktów leczniczych i wyrobów medycznych oraz zakłady i przedsiębiorstwa farmaceutyczne.
Transportowy i komunikacyjny	Obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, śródlądowego i morskiego.
Ratowniczy	Wytypowane obiekty Państwowej Straży Pożarnej oraz infrastruktura jednostek powołanych do ratowania życia i ochrony własności.
Zapewniający ciągłość funkcjonowania państwa	Obiekty urzędów wojewódzkich, obiekty jednostek organizacyjnych służb zespolonych, inspekcji i straży.
Administracji publicznej	Obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji lub przez niego nadzorowanych, obiekty podległe Ministrowi Spraw Zagranicznych, obiekty jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, obiekty Agencji Wywiadu, Agencji Bezpieczeństwa Wewnętrznego, Policji, Straży Granicznej, Biura Ochrony Rządu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, obiekty znajdujące się we właściwości Ministra Sprawiedliwości oraz ważne obiekty innych organów centralnych.
Produkcyjny sektora bezpieczeństwa	Zakłady produkujące, remontujące lub magazynujące uzbrojenie i sprzęt wojskowy oraz środki bojowe, a także zakłady, w których są prowadzone prace badawczo-rozwojowe lub konstruktorskie w zakresie produkcji na potrzeby bezpieczeństwa i obronności państwa.
Ochronne	Instalacje i urządzenia służące ochronie granicy państwowej, posterunki monitoringu.

segmentów funkcjonowania gospodarki. Przepisy te nie wykreowały kompleksowych rozwiązań systemowych, jak również nie nakładały na podmioty zarządzające elementami IK obowiązku przygotowania dokumentacji planistycznej i operacyjnej dotyczącej jej ochrony. Nie narzucały także obowiązku skoordynowania na poziomie państwa działań prowadzonych na rzecz ochrony tych obiektów z analogicznymi działaniami innych podmiotów, które dysponowałyby infrastrukturą powiązaną strukturalnie, czy w inny sposób naturalnie sprzężoną z ich własną. Całościowe spojrzenie na infrastrukturę krytyczną zapewniły dopiero postanowienia ustawy o zarządzaniu kryzysowym [5, s 184].

Infrastruktura krytyczna pełni zasadniczą rolę w funkcjonowaniu państwa i jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka, tzn. w sytuacjach kryzysowych (sytuacjach wpływających negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołujących znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków - w/w Ustawa art. 3. pkt 1), infrastruktura krytyczna może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu. Wydarzenia takie negatywnie wpływają na gospodarkę kraju i życie jego obywateli. Istota zadań związanych z infrastrukturą krytyczną sprowadza się więc nie tylko do zapewnienia jej ochrony przed zagrożeniami, ale również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed państwem polskim.

2. EUROPEJSKA INFRASTRUKTURA KRYTYCZNA

Obowiązek ochrony infrastruktury krytycznej wynika również z członkostwa Polski w Unii Europejskiej (kompatybilność z Europejską Infrastrukturą Krytyczną) oraz w Sojuszu Północnoatlantyckim (np. wypełnianie obowiązków państwa-gospodarza – HNS). W skutek powiązań systemów w aspekcie transnarodowym, uszkodzenie lub zniszczenie infrastruktury krytycznej w jednym państwie ma wpływ na państwa sąsiednie. W ramach UE ustanowiono dyrektywę w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. Przełożenie tych zobowiązań znajduje się w znowelizowanej ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym .

Europejska infrastruktura krytyczna, to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty 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 pkt 2 lit. a i h, 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 lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie” (art.3. pkt. 2a).

Dyrektor RCB „sporządza na podstawie szczegółowych kryteriów, o których mowa w art. 5b. ust. 2 pkt 3, we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. W wykazie wyróżnia się także europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską. Wykaz ma charakter niejawny” (art. 5b ust. 7 pkt 1).

„Dyrektor Rządowego Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy, o których mowa w art. 3 pkt 2a, na bieżąco rozpoznaje potencjalną europejską infrastrukturę krytyczną, badając, czy infrastruktura krytyczna spełnia kolejno następujące wymogi (art.6a):

1. kryteria sektorowe — przybliżone progi liczbowe ustalone przez Komisję Europejską i państwa członkowskie Unii Europejskiej, charakteryzujące parametry, wchodzących w skład systemów infrastruktury krytycznej obiektów, urządzeń oraz instalacji lub funkcje realizowane przez te obiekty, urządzenia oraz instalacje, warunkujące identyfikację infrastruktury krytycznej;
2. stanowi składnik, system lub część infrastruktury, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności, oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na Rzeczpospolitą Polską w wyniku utraty tych funkcji;
3. jej zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie Unii Europejskiej;
4. kryteria przekrojowe — w zakresie przybliżonych progów ustalonych przez Komisję Europejską i państwa członkowskie Unii Europejskiej - obejmujące:
   a. kryterium ofiar w ludziach - oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych,
   b. kryterium skutków ekonomicznych - oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia jakości towarów lub usług, w tym potencjalnych skutków ekologicznych,
   c. kryterium skutków społecznych - oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych osób i zakłócenia codziennego życia, w tym utraty podstawowych usług.

2. Infrastruktura krytyczna jest uznawana za potencjalną europejską infrastrukturę krytyczną po spełnieniu łącznie kolejnych wymogów, o których mowa w ust. 1 pkt 1–3 oraz co najmniej jednego z wymogów, o których mowa w ust. 1 pkt 4".

„1. O potencjalnej europejskiej infrastrukturze krytycznej dyrektor Rządowego Centrum Bezpieczeństwa informuje właściwe organy państw członkowskich Unii Europejskiej, na które ta infrastruktura może mieć istotny wpływ. Dyrektor Rządowego Centrum Bezpieczeństwa podaje nazwę i lokalizację potencjalnej europejskiej infrastruktury krytycznej i przyczyny jej wyznaczenia.

2. W celu wyznaczenia europejskiej infrastruktury krytycznej oraz dokładnych progów kryteriów, o których mowa w art. 6a ust. 1 pkt 1 i 4, dyrektor Rządowego Centrum Bezpieczeństwa prowadzi rozmowy z właściwymi organami państw członkowskich Unii Europejskiej:

1) na które potencjalna europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej może mieć istotny wpływ;

2) na terytorium których jest zlokalizowana potencjalna europejska infrastruktura krytyczna mogąca mieć istotny wpływ na Rzeczpospolitą Polską.

3. Dyrektor Rządowego Centrum Bezpieczeństwa w rozmowach, o których mowa w ust. 2, przedstawia stanowisko uzgodnione z ministrami i kierownikami urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2a, których przedstawiciele mogą brać udział w rozmowach.

4. W przypadku gdy infrastruktura zlokalizowana na terytorium innego państwa członkowskiego Unii Europejskiej, która nie została rozpoznana jako europejska infrastruktura krytyczna, może mieć istotny wpływ na Rzeczpospolitą Polską, dyrektor Rządowego Centrum Bezpieczeństwa informuje Komisję Europejską o zamiarze przeprowadzenia rozmów na ten temat.

5. Na podstawie ustaleń będących wynikiem rozmów, o których mowa w ust. 2, Rada Ministrów wyznacza, w drodze uchwały, z zakresu potencjalnej europejskiej infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej, europejską infrastrukturę krytyczną.

6. Właściwym organom państw członkowskich Unii Europejskiej, na które ma wpływ europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej, dyrektor Rządowego Centrum Bezpieczeństwa przekazuje dane identyfikujące europejską infrastrukturę krytyczną, w tym jej nazwę i lokalizację.

7. Dane, o których mowa w ust. 1 i 6, oraz uchwała, o której mowa w ust. 5, mają charakter niejawny" (art. 6b).

„Dyrektor Rządowego Centrum Bezpieczeństwa przekazuje Komisji Europejskiej:

1) co roku informacje o liczbie infrastruktur krytycznych:

a) w odniesieniu do których prowadzono z właściwymi organami państw członkowskich Unii Europejskiej rozmowy na temat progów kryteriów przekrojowych, umożliwiających wyznaczenie europejskiej infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej,

b) zlokalizowanych na terytorium Rzeczypospolitej Polskiej wchodzących w skład europejskiej infrastruktury krytycznej w poszczególnych systemach, o których mowa w art. 3 pkt 2a, oraz o liczbie państw członkowskich Unii Europejskiej, na które ma ona wpływ;

2) co 2 lata sprawozdanie zawierające ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów stwierdzonych w każdym z systemów, w których została wyznaczona europejska infrastruktura krytyczna zlokalizowana na terytorium Rzeczypospolitej Polskiej.

2. Informacje, o których mowa w ust. 1, mają charakter niejawny" (art. 6c).

3. SPOSOBY OCHRONY INFRASTRUKTURY KRYTYCZNEJ

Ochrona infrastruktury krytycznej określana jest jako "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..." (art.3. pkt.3). Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed państwem polskim.

Zapewnienie ciągłości i sprawnego funkcjonowania infrastruktury krytycznej spoczywa na administracji rządowej i samorządowej oraz na właścicielach i posiadaczach obiektów, urządzeń i instalacji infrastruktury krytycznej. Do ich zadań należy: gromadzenie oraz wymiana informacji o zagrożeniach dla IK, opracowanie i wdrażanie procedur na wypadek wystąpienia zagrożeń, odtwarzanie infrastruktury krytycznej oraz współpraca między administracją publiczną a właścicielami, operatorami i posiadaczami IK w zakresie jej ochrony.

Dawniej elementy tworzące obecną IK funkcjonowały jako niezależne lub jedynie w niewielkim stopniu zależne systemy. Obecnie, poszczególne obiekty i systemy są coraz bardziej współzależne nie tylko w wymiarze jednego państwa, ale i w skali regionalnej, europejskiej, a nawet światowej. Postęp, poza oczywistymi korzyściami, spowodował nowe rodzaje niebezpieczeństw, wcześniej nie znane. W efekcie, istniejąca sieć powiązań powoduje, że uszkodzenie lub utrata części infrastruktury krytycznej w jednym systemie spowoduje straty i uszkodzenia w innych. Zależność sprawnego funkcjonowania państwa i bezpieczeństwa obywateli od kluczowych systemów i usług, a tym samym konieczność ochrony infrastruktury, wchodzącej w skład tych systemów, nie może opierać się wyłącznie na ochronie fizycznej obiektu.

Zgodnie z przyjętą przez RCB filozofią, ochronę infrastruktury krytycznej (OIK) należy rozumieć łącznie jako ochronę fizyczną, techniczną, osobową, teleinformatyczną, prawną, oraz plany jej odtwarzania.

Ochrona fizyczna obejmuje: ochronę osób, rozumianą jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej oraz ochronę mienia, czyli działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także zabezpieczenie wstępu osób nieuprawnionych na teren chroniony. Realizowana jest przez pracowników ochrony, którzy „fizycznie" bronią dostępu do obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej.

Ochrona techniczna to zespół przedsięwzięć związanych z budową i eksploatacją obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, w tym również techniczne środki ochrony, mające na celu minimalizację ryzyka zakłócenia w funkcjonowaniu IK.

Ochrona osobowa jest zespołem przedsięwzięć i procedur mających na celu minimalizację ryzyka będącego ewentualnym skutkiem działań pracowników oraz usługodawców, którzy poprzez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu.

Ochrona teleinformatyczna to zespół przedsięwzięć i ich procedur mających na celu minimalizację zakłóceń w funkcjonowaniu IK związanych z wykorzystaniem do użytkowania tego typu infrastruktury systemów i sieci teleinformatycznych. Oznacza to ochronę przed atakami hakerskimi i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom.

Ochrona prawna infrastruktury krytycznej to zespół przedsięwzięć, mających na celu minimalizację ryzyka związanego z działalnością innych podmiotów gospodarczych, państwowych lub prywatnych, których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK (np. wrogie przejęcia, fuzje czy też sprzedaż niektórych elementów infrastruktury, której efektem mogą być zakłócenia w jej funkcjonowaniu).

W ochronie infrastruktury krytycznej znaczący udział ma Agencja Bezpieczeństwa Wewnętrznego. Zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym są realizowane we współpracy z organami administracji rządowej właściwymi w tych sprawach, w szczególności z Szefem Agencji Bezpieczeństwa Wewnętrznego. Ponadto na organa administracji publicznej oraz posiadaczy infrastruktury krytycznej został nałożony obowiązek niezwłocznego przekazywania Szefowi Agencji Bezpieczeństwa Wewnętrznego, będących w ich posiadaniu, informacji dotyczące zagrożeń o charakterze terrorystycznym dla systemów IK. Szef ABW może również udzielać zaleceń organom i podmiotom zagrożonym działaniami o charakterze terrorystycznym oraz przekazywać im niezbędne informacje służące przeciwdziałaniu zagrożeniom (art.12a).

Nałożono na wojewodę obowiązek, jako organu właściwego w sprawach zarządzania kryzysowego na terenie województwa, współdziałania z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania i zapobiegania zagrożeniom o charakterze terrorystycznym (art. 14).

Istotny wpływ na bezpieczeństwo i ochronę IK w Polsce mają również ustanowione stopnie alarmowe. W ramach stopni alarmowych realizowane są zadania w celu ochrony przed atakiem i przeciwdziałania zagrożeniu atakiem terrorystycznym lub sabotażowym. Stopnie alarmowe mogą zostać wprowadzone w drodze zarządzenia przez Prezesa Rady Ministrów oraz kierowników urzędów centralnych na poziomie centralnym, a na poziomie wojewódzkim przez wojewodę (art. 23). Istnieją 4 stopnie alarmowe: ALFA, BRAVO, CHARLIE oraz DELTA. Każdy z nich wprowadza szereg zadań do realizacji przez podmioty wykonawcze na rzecz ochrony infrastruktury oraz ludności [1].

Do zadań realizowanych przy wprowadzeniu pierwszego stopnia alarmowego (ALFA) należą:

1. Na rzecz ochrony zagrożonej infrastruktury:
   - 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.
2. Na rzecz ochrony ludności:
   - kontrola miejsc skupisk ludzi i obiektów użyteczności publicznej,
   - informowanie służb o zauważonych nietypowych oznakach zachowania lub działalności.

Do zadań realizowanych przy wprowadzeniu drugiego stopnia alarmowego (BRAVO) należą wszystkie przedsięwzięcia pierwszego stopnia, oraz:

1. Na rzecz ochrony zagrożonej infrastruktury:
   - 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.
2. Na rzecz ochrony ludności:
   - kontrola pojazdów, ludzi i obiektów w rejonach zagrożonych,
   - akcja informacyjno-instruktażowa dla społeczeństwa.

Do zadań realizowanych przy wprowadzeniu trzeciego stopnia alarmowego (CHARLIE) należą wszystkie przedsięwzięcia pierwszego i drugiego stopnia, oraz:

1. Na rzecz ochrony zagrożonej infrastruktury:
   - 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.
2. Na rzecz ochrony ludności:
   - wzmocnienie ochrony imprez masowych (odwołanie imprez),
   - przegląd bazy i środków medycznych,
   - zaktualizowanie danych o zaopatrzeniu w wodę i miejscach tymczasowego pobytu ludności.

Do zadań realizowanych przy wprowadzeniu czwartego stopnia alarmowego (DELTA) należą wszystkie przedsięwzięcia pierwszego, drugiego i trzeciego stopnia, oraz:

1. Na rzecz ochrony zagrożonej infrastruktury:
   - 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.
2. Na rzecz ochrony ludności:
   - wprowadzenie ograniczeń komunikacyjnych w rejonach zagrożonych,
   - wprowadzenie zakazu organizacji imprez masowych,
   - przygotowanie zaplecza logistycznego i medyczno-sanitarnego.

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 celu stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej w zakresie: zapobiegania zakłóceniom funkcjonowania infrastruktury krytyczne, przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną, reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej, oraz odtwarzania infrastruktury krytycznej, Rada Ministrów przyjmuje, w drodze uchwały, Narodowy Program Ochrony Infrastruktury Krytycznej [7, art. 5b].

Za przygotowanie Programu odpowiedzialne jest Rządowe Centrum Bezpieczeństwa współpracując z ministrami i kierownikami urzędów centralnych właściwych w sprawach bezpieczeństwa narodowego, a także odpowiedzialnymi za systemy zaliczone do IK.

Celem Programu jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w szczególności w zakresie:
- zapobiegania zakłóceniom funkcjonowania infrastruktury krytyczne,
- przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
- reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- odtwarzania infrastruktury krytycznej.

Program 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 wymienione powyżej,
- szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

W Programie zakłada się współpracę, współodpowiedzialność i wzajemne zaufanie przedsiębiorców – właścicieli IK oraz administracji publicznej.

Dyrektor Rządowego Centrum Bezpieczeństwa w uzgodnieniu z właściwymi ministrami i kierownikami centralnych urzędów państwowych sporządza jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podaniem przynależności do systemu. Wykaz ma charakter niejawny.

Przyjęto następujące kryteria identyfikacji IK:
- 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;
- 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.

W sporządzanym wykazie wyróżnia się Europejską Infrastrukturę Krytyczną, która jest zlokalizowana na terenie Polski oraz EIK położoną na terytorium innych państw Unii Europejskiej, która ma wpływ na funkcjonowanie naszego kraju. Opracowane wykazy mają charakter niejawny i wyciągi z nich we właściwościach w zakresie odpowiedzialności za systemy przekazuje się właściwym ministrom i kierownikom urzędów centralnych. Obiekty, instalacje, urządzenia i usługi znajdujące się na terenie danego województwa, o ile zostały zakwalifikowane jako części składowe infrastruktury krytycznej, zostają w postaci niejawnej podane do wiadomości właściwego wojewody. Właściwi wojewodowie, jeżeli istnieje potrzeba wynikająca z wojewódzkiego planu zarządzania kryzysowego, są upoważnieni do przekazywania niezbędnej informacji o infrastrukturze krytycznej na terenie województwa właściwemu organowi administracji publicznej działającemu na tym terenie, z zachowaniem przepisów o ochronie informacji niejawnych.

Informację o zakwalifikowaniu obiektu w skład infrastruktury krytycznej otrzymują również ich właściciele, bowiem oni zgodnie z ustawowym obowiązkiem są odpowiedzialni za ochronę funkcjonujących obiektów, instalacji, urządzeń i usług. Właściciele przygotowują plany ochrony wyznaczonych obiektów, mają obowiązek utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i potrzymanie funkcjonowania infrastruktury w przypadku awarii do czasu jej ponownego odtworzenia. Właściciel w terminie do 30 dni od otrzymania informacji o zakwalifikowaniu jego urządzeń, usług, systemów w skład infrastruktury krytycznej ma obowiązek wyznaczyć osobę odpowiedzialną do utrzymania kontaktów w zakresie ochrony obiektów wchodzących w jej skład. Opracowany program ochrony wymaga aktualizacji swoich treści nie rzadziej niż raz na dwa lata.

Rada Ministrów określa, w drodze rozporządzenia, sposób realizacji określonych w ustawie obowiązków i współpracy w zakresie programu przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej oraz innymi organami i służbami publicznymi, biorąc pod uwagę konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa infrastruktury krytycznej.

Ustawodawca zobowiązuje także osoby odpowiedzialne za IK do planowania jej ochrony: „Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia" (art.6.1, pkt.5). Zasady tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej określono rozporządzeniem Rady Ministrów.

Plan ochrony infrastruktury krytycznej [6] zawiera:
1. dane ogólne:
   a) obejmujące nazwę i lokalizację infrastruktury krytycznej,
   b) pozwalające zidentyfikować operatora infrastruktury krytycznej: nazwa, adres i siedziba, numery REGON, NIP i KRS,
   c) pozwalające zidentyfikować zarządzającego przedsiębiorstwem w imieniu operatora infrastruktury krytycznej: nazwa, adres i siedziba, numery REGON, NIP i KRS,
   d) obejmujące w zakresie niezbędnym do realizacji zadań wynikających z ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zwanej dalej "ustawą" - dane służbowe osoby, o której mowa w art. 6 ust. 5a ustawy, odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej,
   e) obejmujące imię i nazwisko osoby sporządzającej plan;
2. dane infrastruktury krytycznej obejmujące:
   a) charakterystykę i podstawowe parametry techniczne,
   b) plan (mapę) z naniesieniem lokalizacji obiektów, instalacji lub systemu,

c) funkcjonalne połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami;
3. charakterystyka:
   a) zagrożeń dla infrastruktury krytycznej oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń,
   b) zależności infrastruktury krytycznej od pozostałych systemów infrastruktury krytycznej oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej,
   c) zasobów własnych możliwych do wykorzystania w celu ochrony infrastruktury krytycznej,
   d) zasobów właściwych terytorialnie organów, możliwych do wykorzystania w celu ochrony infrastruktury krytycznej;
4. zasadnicze warianty:
   a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
   b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej,
   c) odtwarzania infrastruktury krytycznej;
5. zasady współpracy z właściwymi miejscowo:
   a) centrami zarządzania kryzysowego,
   b) organami administracji publicznej.

Plan wymaga uzgodnienia:
1. w zakresie ich dotyczącym z właściwymi terytorialnie:
   a) wojewodą,
   b) komendantem wojewódzkim Państwowej Straży Pożarnej,
   c) komendantem wojewódzkim Policji,
   d) dyrektorem regionalnego zarządu gospodarki wodnej,
   e) wojewódzkim inspektorem nadzoru budowlanego,
   f) wojewódzkim lekarzem weterynarii,
   g) państwowym wojewódzkim inspektorem sanitarnym,
   h) dyrektorem urzędu morskiego;
2. z ministrem lub kierownikiem urzędu centralnego, we właściwości którego znajduje się system, do którego została zaliczona dana infrastruktura krytyczna.

Aktualizacja planów odbywa się w zależności od potrzeb, nie rzadziej jednak niż raz na dwa lata. Plan podpisuje operator infrastruktury krytycznej.

Plany ochrony muszą być opracowywane przez operatora infrastruktury krytycznej w terminie do 9 miesięcy od otrzymania informacji o ujęciu w wykazie obiektu, instalacji, urządzenia czy usługi jako systemu infrastruktury krytycznej. Wojewoda musi dokonać uzgodnień w terminie 14 dni od daty przedłożenia planu, a uzgodnienie planu z właściwym ministrem czy dyrektorem urzędu centralnego następuje w terminie do 45 dni. Z chwilą dokonania powyższych uzgodnień operator infrastruktury krytycznej przedkłada plan wraz z arkuszami uzgodnień dla dyrektora Rządowego Centrum Bezpieczeństwa w terminie do 14 dni od daty ostatniego uzgodnienia. Dyrektor Centrum ma obowiązek w terminie 90 dni od daty przedłożenia zatwierdzić plan ochrony.

Opracowanie planu ochrony infrastruktury krytycznej odbywa się z zachowaniem wymogów ochrony informacji niejawnych.

BIBLIOGRAFIA

1. Infrastruktura krytyczna. RCB - załącznik 5.
2. 2. Materiały wyjściowe do Koncepcji Przestrzennego Zagospodarowania Kraju na lata 2008-2033, P3/1061/08 z 9 maja 2008 r., Sztab Generalny WP, Zarząd Planowania Operacyjnego – P3.
3. Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1 – Charakterystyka systemów infrastruktury krytycznej, Rządowe Centrum Bezpieczeństwa, 2013.
4. Sadowski J., Podstawy prawne ochrony infrastruktury krytycznej a zarządzanie kryzysowe, w: Kosowski B. (red), Elementy ochrony infrastruktury krytycznej w zarządzaniu kryzysowym, Katowice 2014.
5. Stec K., Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce, w: Bezpieczeństwo Narodowe nr 19, III – 2011.
6. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. z 2010 r. Nr 83, poz. 542).
7. 7. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. z 2013 r. poz. 1166 (Dz. U. 2017.0.209).

The critical infrastructure protection. Legislation

The content outline: in accordance with law, the Polish critical infrastructure constitutes 11 sectors, vital for national security and public safety persistence. Two of the sectors (energy sector and transportation systems sector), are elements of the European Critical Infrastructure, and due to Poland's EU and NATO membership, are subject to particular protection. The paper describes general principles of Polish critical infrastructure safety law acts and critical infrastructure sectors. Later in this paper, 4 alert states (THREATCON), and their impact on the critical infrastructure safety and protection were presented. The purpose and the program content of the National Critical Infrastructure Protection Programme and the National Infrastructure Protection Plan were described.

Autor:
dr hab. Józef Sadowski prof. nadzw. AP – Akademia Pomorska w Słupsku, Wydział Nauk o Zarządzaniu i Bezpieczeństwie, Katedra Zarządzania, adres e-mail: Jozef.sadowski@apsl.edu.pl

JEL: L99 **DOI**: 10.24136/atest.2018.260
Data zgłoszenia: 2018.05.29 **Data akceptacji**: 2018.06.15