STUDIA NAD BEZPIECZEŃSTWEM

Nr 4 ss. 5–15 2019

ISSN 2543–7321

Przyjęto: 20.11.2018
Zaakceptowano: 25.11.2019

Oryginalna praca badawcza

DOI: 10.34858/SNB.1.2019.001

Józef Sadowski
Akademia Pomorska
Słupsk
jozef.sadowski@apsl.edu.pl

ZAGROŻENIA SYSTEMÓW INFRASTRUKTURY KRYTYCZNEJ ATAKAMI TERRORYSTYCZNYMI

THREATS OF TERRORIST ATTACKS TO CRITICAL INFRASTRUCTURE SYSTEMS

***Zarys treści*:** Zgodnie z Ustawą o zarządzaniu kryzysowym infrastruktura krytyczna w Polsce obejmuje 11 systemów, spełniających kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W artykule przedstawiono stosowane formy ataków terrorystycznych na systemy infrastruktury krytycznej. Na podstawie prowadzonych kontroli opisano spotykane błędy w zakresie ochrony systemów IK. W końcowej części artykułu powtórzono za NPOIK, że stosowane systemy ochrony IK powinny mieć zastosowanie do wszystkich typów zagrożeń, a także być przygotowane do możliwie szybkiego przywrócenia funkcji realizowanych przez daną IK.
***Słowa kluczowe*:** infrastruktura krytyczna, systemy infrastruktury krytycznej, stan infrastruktury krytycznej, ataki terrorystyczne.
***Key words*:** critical infrastructure, critical infrastructure systems, critical infrastructure condition, terrorist attacks.

Ochrona infrastruktury krytycznej to pojęcie, które w polskim systemie prawnym pojawiło się wraz z wejściem w życie ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

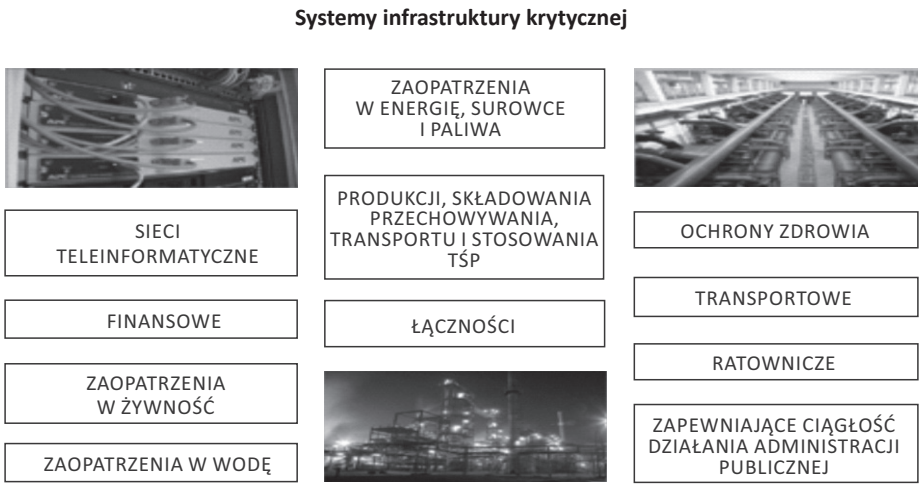
Zgodnie ze znowelizowaną Ustawą o zarządzaniu kryzysowym, infrastruktura krytyczna (IK) są to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[1]. Z Ustawy wynika, że infrastruktura krytyczna to kluczowe elementy gospodarki

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2013, poz. 1166, art. 3, pkt 2).

narodowej i że spełnia ona kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli.

Systemy infrastruktury krytycznej w Polsce

W Rzeczypospolitej Polskiej infrastruktura krytyczna wchodzi w skład 11 systemów (rys. 1), które mają kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.



Rys. 1. Systemy infrastruktury krytycznej
Fig. 1. Critical infrastructure systems
Źródło: Ustawa o zarządzaniu kryzysowym (Dz.U. 2011 Nr 22, poz. 114) oraz: www.rcb.gov.pl.

Infrastruktura krytyczna obejmuje[2]:

1) Systemy zaopatrzenia w energię, surowce energetyczne i paliwa:
   - do produkcji, przesyłania i dystrybucji energii elektrycznej (energetyka – elektrownie i inne obiekty elektroenergetyczne);
   - do produkcji, transportu i dystrybucji paliw gazowych (gazoporty, bazy, składy, gazociągi i magazyny paliw);
   - do produkcji, transportu i dystrybucji ropy naftowej i produktów ropopochodnych (bazy, składy, rurociągi i magazyny paliw);

[2] Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1 – Charakterystyka systemów infrastruktury krytycznej, Rządowe Centrum Bezpieczeństwa, 2013; Sztab Generalny WP, Zarząd Planowania Operacyjnego – P3, Materiały wyjściowe do Koncepcji Przestrzennego Zagospodarowania Kraju na lata 2008–2033, P3/1061/08 z 9 maja 2008 r.; M. Żuber, *Infrastruktura krytyczna państwa, jako obszar potencjalnego oddziaływania terrorystycznego*, Wyższa Szkoła Oficerska Wojsk Lądowych im. generała T. Kościuszki we Wrocławiu.

- do produkcji, transportu i dystrybucji ciepła (zakłady mające bezpośredni związek z produkcją ciepła, sieci transportu, przesyłu i dystrybucji).

2) Systemy łączności, zapewniające przekazywanie informacji, obejmujące infrastrukturę operatorów publicznych świadczących usługi pocztowe, oraz telekomunikację, jak również obiekty Telewizji Publicznej oraz Polskiego Radia.
3) 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.
4) Systemy finansowe to ogół norm prawnych oraz zespół instytucji finansowych, których zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa.
5) Systemy finansowe obejmują: 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.
6) System zaopatrzenia w żywność to dziedzina gospodarki, na którą składają się obiekty bezpośrednio związane z produkcją żywności, a także infrastruktura związana z przechowywaniem i transportem do bezpośrednich odbiorców. 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 i 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.
7) System zaopatrzenia w wodę (woda pitna, ścieki, wody powierzchniowe) to zespół osób i instytucji, powiązane ze sobą przedsiębiorstwa i urządzenia pobierające, gromadzące, uszlachetniające, dostarczające i oczyszczające wodę dla ludności i przemysłu.
8) System ochrony zdrowia (apteki, szpitale, przychodnie, magazyny rezerw państwowych produktów leczniczych i wyrobów medycznych oraz zakłady i przedsiębiorstwa farmaceutyczne), mający za zadanie zapewnić opiekę i świadczenia zdrowotne ludności, a jego sprawne funkcjonowanie (wraz z systemem ratowniczym) jest gwarantem praw obywatela zapisanych w Konstytucji.
9) Systemy transportowe (obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, śródlądowego i morskiego – drogi, kolej, lotniska, porty) – czyli możliwość przemieszczania się ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu.
10) 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. Są to wytypowane obiekty Państwowej Straży Pożarnej oraz infrastruktura jednostek powołanych do ratowania życia i ochrony własności.

11) Systemy 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. Do systemu zalicza się obiekty: urzędów wojewódzkich, jednostek organizacyjnych służb zespolonych, inspekcji i straży, administracji publicznej, organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji lub przez niego nadzorowanych, podległe Ministrowi Spraw Zagranicznych, jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, Agencji Wywiadu, Agencji Bezpieczeństwa Wewnętrznego, Policji, Straży Granicznej, Biura Ochrony Rządu (obecnie Służby Ochrony Państwa), Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, znajdujące się we właściwości Ministra Sprawiedliwości oraz ważne obiekty innych organów centralnych.
12) Produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągi substancji niebezpiecznych).

Do IK zalicza się także 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, oraz instalacje i urządzenia służące ochronie granicy państwowej.

Urządzenia, instalacje, obiekty czy usługi wchodzące w skład infrastruktury krytycznej charakteryzują się następującymi cechami:

- długotrwały okres użytkowania i trudności związane z przystosowaniem urządzeń do nowych oczekiwań użytkowników;
- urządzenia infrastruktury charakteryzują się publicznym charakterem;
- obiekty, instalacje czy urządzenia lub usługi infrastruktury krytycznej koniecznie muszą być dostosowane do warunków miejscowych;
- infrastruktura spełnia funkcje usług podstawowych i wyspecjalizowanych;
- decydującą, bardzo ważną rolę w działaniu infrastruktury odgrywa człowiek, który zapewnia jej prawidłowe funkcjonowanie;
- infrastruktura charakteryzuje się służebnym charakterem, nie istnieje sama dla siebie, świadczy usługi dla sfery przemysłowej lub konsumpcyjnej;
- formy własności infrastruktury mogą być różne. Może ona należeć do państwa, być własnością korporacji lub być własnością komunalną albo osób prywatnych;
- infrastruktura krytyczna może mieć międzynarodowy charakter ze względu na sieć powiązań i zależności, np. sieci energetyczne, telekomunikacyjne i inne;
- mając na uwadze obronność i bezpieczeństwo państwa, elementy składowe infrastruktury krytycznej mają charakter informacji niejawnych i stanowią tajemnicę państwową czy wojskową[3].

[3] A. Wojtczak, *Infrastruktura krytyczna*, [w:] *Elementy ochrony infrastruktury krytycznej w zarządzaniu kryzysowym*, B. Kosowski (red.), Katowice 2014, s. 23.

Formy ataków terrorystycznych na systemy infrastruktury krytycznej

Do znaczących zagrożeń obiektów infrastruktury krytycznej zalicza się ataki terrorystyczne.

Najważniejszym obiektem w pierwszym systemie IK są niewątpliwie elektrownie. Możliwe są następujące formy ataku terrorystycznego na elektrownie:

a) bezpośredni atak na system – celem ataku jest fizyczna infrastruktura systemu; mogą zostać zaatakowane stacje elektroenergetyczne lub kluczowe linie w celu wywołania awarii na dużym obszarze sieci;
b) atak poprzez system elektroenergetyczny – mogą zostać użyte niektóre instalacje w systemie elektroenergetycznym do zaatakowania innych elementów jego infrastruktury, wywołany silny impuls elektromagnetyczny w sieci w celu uszkodzenia komputerów i infrastruktury telekomunikacyjnej;
c) możliwość przeprowadzenia sabotażu wewnątrz elektrowni przez osobę kierującą się korzyściami materialnymi lub ideologią;
d) przejęcie systemu sterowania pracą reaktorów z poziomu sterowni przez uzbrojoną grupę terrorystyczną, która przeprowadziła udany atak i obezwładniła ochronę elektrowni;
e) uderzenie dużego samolotu (samolotu pasażerskiego lub transportowego) w reaktor elektrowni. Jest to szczególnie niebezpieczne dla elektrowni starego typu, których reaktory nie zostały zabezpieczone przed taką ewentualnością.

Niezwykle istotnym problemem bezpieczeństwa obiektów infrastruktury energetycznej jest zagrożenie potencjalnym atakiem elektrowni jądrowych. Obecnie w Europie pracuje około 220 reaktorów. Najbardziej rozbudowane systemy pozyskiwania energii atomowej mają państwa najbardziej zagrożone terroryzmem: Francja, Wielka Brytania, Niemcy i Rosja. Polska nie posiada obecnie elektrowni jądrowej, jednak w jej bliskim sąsiedztwie w promieniu do ok. 300 km od granic pracuje 10 elektrowni tego typu (Litwa – 1, Ukraina – 2, Słowacja – 2, Węgry – 1, Czechy – 2, Niemcy – 1, Szwecja – 1) z 23 blokami energetycznymi, które w przypadku awarii mogą znacząco zagrozić ludności zamieszkującej obszar naszego kraju[4].

Systemy łączności oraz sieci teleinformatyczne to systemy i sieci, których nieprawidłowe funkcjonowanie lub uszkodzenie – niezależne od przyczyn i zakresu – może spowodować istotne zagrożenie dla życia lub zdrowia ludzi, interesów obronności oraz bezpieczeństwa państwa i obywateli albo narazić te interesy na co najmniej znaczną szkodę. Warunkiem zapewnienia bezpieczeństwa tej infrastruktury na poziomie krajowym jest współpraca pomiędzy zarządcami poszczególnych jej części (tzw. partnerstwo publiczno-prywatne). Oddzielny problem stanowi cyberterroryzm polegający na celowym zakłóceniu interaktywnego, zorganizowanego obiegu informacji w cyberprzestrzeni.

[4] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje, struktury, funkcjonowanie*, Warszawa 1999, s. 112–114.

Do obiektów w grupie systemów finansowych zaliczyć można siedziby główne banków i ich placówki terenowe, siedziby giełd finansowych, mennice i wytwórnie papierów wartościowych, systemy płatnicze, centra rozliczeniowe dla kart płatniczych oraz sieci bankomatowe i POS. Atak terrorystyczny może przybrać formę zamachu bombowego, mającego na celu zniszczenie infrastruktury i spowodowanie strat w personelu i klienteli lub formę cyberataku na finansowe systemy informatyczne. Cyberterrorystyczne ataki skierowane na wymienione elementy sektora bankowego mogą skutkować:

- zakłóceniem swobodnego przepływu środków pieniężnych;
- zafałszowaniem danych dotyczących bieżącej sytuacji gospodarczej i finansowej;
- manipulowaniem notowaniami kursowymi bądź giełdowymi;
- odebraniem firmom i osobom prywatnym bieżącego dostępu do zgromadzonych środków;
- zafałszowaniem informacji dotyczących poziomu zadłużenia;
- kradzieżą i legalizacją znacznych sum[5].

Prowadzenie ataków terrorystycznych przeciwko systemowi zaopatrzenia w żywność (sektorowi rolniczemu) określa się mianem agroterroryzmu. Stanowi on rodzaj bioterroryzmu i może być definiowany jako celowe uwolnienie patogenów zwierzęcych lub roślinnych do wywołania strachu, strat ekonomicznych oraz destabilizacji państwa. W systemie zaopatrzenia w żywność do celowych zakłóceń dojść może na różnych poziomach przygotowania żywności. Może to mieć miejsce w fazie:

- produkcji rolnej (uprawa i hodowla);
- transportu i przechowywania surowców;
- produkcji i przechowywania żywności;
- dystrybucji;
- sieci gastronomicznej[6].

Celem działań terrorystycznych może być wywołanie znacznych strat w ludziach, wywołanie stanu paniki bądź spowodowanie strat gospodarczych poprzez zahamowanie eksportu, jako efektu skażenia żywności na którymś z poziomów jej produkcji.

Nie mniej wrażliwym systemem jest system zaopatrzenia w wodę, zwłaszcza dużych aglomeracji miejskich. Tworzą go ujęcia wody pitnej i wodociągi. Atak na ten system polegać może na skażeniu ujęć wody przy pomocy środków biologicznych lub chemicznych. Celem ataku terrorystycznego z użyciem tego rodzaju broni będzie spowodowanie na znacznym obszarze śmierci lub schorzeń mogących przybrać rozmiar epidemii, co spowodować może utratę zaufania do władz oraz destabilizację struktur społecznych i politycznych.

---

[5] J. Syta, *Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego*, [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioła, J. Kisielnicki, K. Rajchel (red.), Wyższa Szkoła Policji, Szczytno 2009, s. 698.

[6] R. Zięba, *Instytucjonalizacja*, *op. cit*., s. 33.

Niezmiernie istotnym systemem infrastruktury krytycznej bezpośrednio wpływającym na poczucie bezpieczeństwa przez obywateli jest system ochrony zdrowia. Zakłócenie funkcjonowania tego systemu spowodować może wzrost niezadowolenia społecznego, wynikającego z poczucia zagrożenia oraz troski o losy ludzi słabych i chorych niezdolnych do samodzielnego zapewnienia sobie bezpieczeństwa.

Infrastruktura krytyczna związana z transportem i komunikacją jest jednym z głównych celów ataków terrorystycznych. Narażone są wszystkie rodzaje transportu i komunikacji: lotnicza, kolejowa, drogowa i morska oraz infrastruktura z nią związana. Obiektem ataku terrorystycznego mogą więc być elementy infrastruktury lotniskowej oraz samoloty zarówno na lotniskach, jak i podczas wykonywania operacji startu i lądowania, a także podczas lotu. Zagrożenie atakiem terrorystycznym na lotnisku jest ciągle zagrożeniem aktualnym. Terroryści, dążąc do zniszczenia infrastruktury portu lotniczego lub samolotów (zarówno na ziemi, jak i w powietrzu), mogą wnosić na teren lotniska oraz do samolotów ładunki wybuchowe. Mogą również dążyć do uprowadzenia samolotu pasażerskiego celem użycia go do ataku z powietrza na ważny, wybrany obiekt (np. budynek administracji rządowej, duży port lotniczy). Mogą też uprowadzić cywilny statek powietrzny, a następnie użyć go do ataku samobójczego na samolot pasażerski, będący na lotnisku lub w powietrzu. Nie wyklucza się także użycia środków rażenia do zniszczenia (uszkodzenia) infrastruktury lotniska lub samolotu na lotnisku podczas wykonywania startu lub lądowania. Innym rodzajem zagrożenia terrorystycznego jest atak wymierzony w systemy kierowania ruchem powietrznym i zarządzania lotniskiem za pomocą sieci komputerowych przez cyberterrorystów.

Celem ataku terrorystycznego na obiekty infrastruktury systemu ratowniczego (centra zarządzania kryzysowego, strażnice Państwowej Straży Pożarnej, obiekty Państwowego Ratownictwa Medycznego, pogotowia techniczne) będzie destabilizacja centrów zarządzania i kierowania akcją ratowniczą, wyeliminowanie ratowników oraz zniszczenie pojazdów i sprzętu ratunkowego lub też uniemożliwienia przeprowadzenia akcji ratunkowej.

System zapewniający ciągłość funkcjonowania administracji publicznej stanowią obiekty administracji państwowej, zwłaszcza te, w których urzędują organy państwa odpowiedzialne za przeciwdziałanie, zwalczanie, rozpoznawanie terroryzmu czy zarządzanie kryzysowe. Stanowią one jeden z głównych celów zamachów terrorystycznych na całym świecie, ze względu na swój strategiczny i symboliczny charakter. Zagrożone mogą być także bazy danych znajdujące się w tych obiektach.

Systemy produkcji, składowania, przechowywania oraz stosowania substancji chemicznych i promieniotwórczych stanowią opłacalne obiekty ataków terrorystycznych. Skutki ataków przy użyciu ładunków wybuchowych lub artyleryjskich środków rażenia mogą powodować rozległe pożary lub uwolnienie do atmosfery znacznych ilości substancji trujących, tzw. toksycznych środków przemysłowych (TŚP), powodujących masowe zatrucia ludzi lub skażenie środowiska.

Stan bezpieczeństwa IK

Często mówimy o bezpieczeństwie infrastruktury krytycznej. To dobry symptom, bo choć odgrywa ona kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, to w wielu przypadkach poziom jej ochrony jest daleki od założeń ustawowych. Niewłaściwa realizacja zadań z zakresu ochrony IK przez wojewodów oraz jednostki samorządu terytorialnego – wójtów (burmistrzów, prezydentów), brak odpowiednich zabezpieczeń, m.in. w obszarach ochrony fizycznej i osobowej, może powodować wystąpienie niebezpiecznych incydentów.

Istotnym zagrożeniem dla bezpieczeństwa infrastruktury krytycznej jest lekceważenie istniejących uregulowań formalnoprawnych.

Różne kontrole, w tym kontrola NIK[7], wykazują w obszarze bezpieczeństwa nadal niekorzystne przypadki.

1) Negatywne przypadki wśród organów władzy rządowej i samorządowej:
   - nie przekazuje się organom gmin informacji o znajdującej się na ich terenach infrastrukturze krytycznej;
   - nie gromadzi się w gminach i nie przetwarzali informacji dotyczących zagrożeń IK;
   - nie opracowuje się i nie wdraża procedur na wypadek wystąpienia takich zagrożeń i rozwiązań w razie zniszczenia lub zakłócenia funkcjonowania IK; o zdarzeniach mogących mieć wpływ na bezpieczeństwo IK starostwa i gminy dowiadują się często ze środków masowego przekazu;
   - nie aktualizuje się powiatowych i gminnych planów zarządzania kryzysowego w zakresie dostosowania ich zapisów do wymogów dotyczących ochrony IK określonych w ustawie o zarządzaniu kryzysowym;
   - często nadal brakuje ścisłej współpracy organów samorządu terytorialnego z operatorami IK w zakresie ochrony IK.
2) Negatywne przypadki wśród operatorów IK:
   - nie stosuje się wystarczających zabezpieczeń w obszarach ochrony fizycznej i osobowej IK; brak odpowiednich zabezpieczeń w tych obszarach ochrony może spowodować wystąpienie niebezpiecznych incydentów na terenach obiektów infrastruktury krytycznej czy też związanych z prawidłową eksploatacją instalacji infrastruktury krytycznej;
   - nie obejmuje się ochroną fizyczną wszystkich obiektów infrastruktury krytycznej powiązanych ze sobą funkcjonalnie i niezbędnych do zapewnienia bezpieczeństwa jej funkcjonowania;
   - część terenów, na których znajdują się obiekty infrastruktury krytycznej, nie jest właściwie zabezpieczona przed dostępem osób nieuprawnionych;
   - wejścia do niektórych obiektów nie spełniają norm bezpieczeństwa i nie zostały objęte systemem kontroli dostępu, bramy wjazdowe nie zostały wyposażone w zapory zabezpieczające przed wtargnięciem, brakuje monitoringu wizyjnego;

[7] www.nik.gov.pl (dostęp: 12.04.2018).

- w dużej liczbie skontrolowanych podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej nie wprowadza się rozwiązań w razie wystąpienia sabotażu lub wyrządzenia szkód przez pracowników na terenie obiektów infrastruktury krytycznej;
- nie wyodrębnia się personelu kluczowego ze względu na przestrzeganie zasad bezpieczeństwa infrastruktury krytycznej;
- nie określa się procedur umożliwiających sprawdzenie wybranego oferenta wykonującego usługi na rzecz operatora infrastruktury krytycznej pod kątem jakości wykonywanych usług oraz zachowania poufności wykonywanych prac;
- nie realizuje się przez skontrolowane podmioty niektórych rekomendacji audytu sieci informatycznych działających na potrzeby obiektów infrastruktury krytycznej;
- zdarzają się przypadki niedbałego traktowanie kwestii ochrony przez operatorów IK – podejmują oni działanie jedynie po to, aby wypełnić wymogi formalne.

Zapewnienie bezpieczeństwa infrastrukturze krytycznej

Ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej. Celem tych działań jest zapobieganie zagrożeniom, ograniczanie i neutralizacja ich skutków oraz szybkie odtworzenie tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Systemy ochrony IK przygotowuje Rządowe Centrum Bezpieczeństwa. Dyrektor RCB, we współpracy z ministrami i kierownikami urzędów centralnych, odpowiedzialnych za poszczególne systemy IK przygotowuje, aktualizowany co dwa lata, Narodowy Program Ochrony Infrastruktury krytycznej (NPOIK).

Program określa:

1) narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej;
2) ministrów i kierowników urzędów centralnych odpowiedzialnych za poszczególne systemy IK;
3) szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów IK[8].

Stosowane systemy ochrony IK, zgodnie z NPOIK, powinny mieć zastosowanie do wszystkich typów zagrożeń, a także być przygotowane do możliwie szybkiego przywrócenia funkcji realizowanych przez daną IK. Ponadto powinna cechować je kompleksowość i elastyczność oraz łatwość zastosowania i zrozumienia przez odpowiedzialnych za ochronę IK.

[8] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2013, poz. 1166, art. 3, pkt 2).

Działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia przez: zmniejszenie prawdopodobieństwa wystąpienia zagrożenia, zmniejszanie podatności, minimalizowanie skutków wystąpienia zagrożenia. Na te działania składają się[9]:

1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK.

[9] Narodowy Program Ochrony Infrastruktury krytycznej – tekst jednolity, s. 30, https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument--Główny-tekst-jednolity.pdf (dostęp: 12.04.2018).

Bibliografia

Materiały wyjściowe do Koncepcji Przestrzennego Zagospodarowania Kraju na lata 2008––2033, Sztab Generalny WP, Zarząd Planowania Operacyjnego – P3, P3/1061/08 z 9 maja 2008 r.

Narodowy Program Ochrony Infrastruktury krytycznej – tekst jednolity, https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-Główny-tekst-jednolity.pdf (dostęp: 12.04.2018).

Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1 – Charakterystyka systemów infrastruktury krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

Syta J., *Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego*, [w:] *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioła, J. Kisielnicki, K. Rajchel (red.), Wyższa Szkoła Policji, Szczytno 2009.

Wojtczak A., *Infrastruktura krytyczna*, [w:] *Elementy ochrony infrastruktury krytycznej w zarządzaniu kryzysowym*, B. Kosowski (red.), Katowice 2014.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje, struktury, funkcjonowanie*, Warszawa 1999.

Żuber M., *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, Wyższa Szkoła Oficerska Wojsk Lądowych im. generała T. Kościuszki we Wrocławiu.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2013, poz. 1166).

www.nik.gov.pl (dostęp:12.04.2018).
www.rcb.gov.pl (dostęp:12.04.2018).

Summary

According to the Act on Crisis Management, critical infrastructure (CI) in Poland includes 11 systems that fulfill a key role in the functioning of the state and the life of its citizens. The article presents applied forms of terrorist attacks on CI systems. On the basis of checks that were carried out, errors in the protection of CI systems are described. In the final part of the article it is repeated after NPOIK that the applied CI protection systems should apply to all types of threats and be prepared for the fastest possible restoration of functions performed by the given CI.