KOMPLEKSOWE PODEJŚCIE DO WYŁANIANIA I OCHRONY INFRASTRUKTURY KRYTYCZNEJ

dr inż. Witold Skomra

Doradca
Rządowe Centrum Bezpieczeństwa

Technologie cyfrowe z jednej strony poprawiają jakość usług świadczonych na rzecz obywateli, ale równocześnie są źródłem nowych zagrożeń. W efekcie, poza dotychczasowymi rodzajami zarządzania bezpieczeństwem (bezpieczeństwem fizycznym czy technicznym) pojawiają się jego nowe formy, będące odpowiedzią na nowe zagrożenia (bezpieczeństwo cybernetyczne, bezpieczeństwo danych osobowych itp.). Te zróżnicowane działania, aby mogły osiągnąć zamierzony efekt, powinny być traktowane jako elementy większej całości. Ta większa całość to kompleksowe zarządzanie bezpieczeństwem obejmujące nie tylko działania na rzecz własnej jednostki, ale uwzględniające zarówno oddziaływanie podmiotów zewnętrznych, jak i ewentualne skutki społeczne, jakie może spowodować dysfunkcja usług, które podmiot dostarcza. Podejście usługowe jako metoda pozwalająca na hierarchizację procesów realizowanych w ramach administracji publicznej to zupełnie nowe zagadnienie wymagające zarówno zmian mentalnych wśród kadry zarządzającej, jak i dostosowania struktur formalnych do wymagań związanych z koniecznością wdrożenia nowych form zarządzania bezpieczeństwem.

WPROWADZENIE

Współczesne życie społeczne jest determinowane przez technologie cyfrowe oraz systemy teleinformatyczne. Proces cyfrowej transformacji dotyczy zarówno obszaru biznesu, jak i działań administracji publicznej. Towarzyszą mu nowe zagrożenia i powiązane z nimi ryzyka. Powstają przy tym wzajemne współzależności, w efekcie czego kto inny może być właścicielem infrastruktury (i ryzyk z nią związanych), a kto inny właścicielem skutków wynikających z dysfunkcji tej infrastruktury (ryzyko związane ze skutkami społecznymi). Nawet jeśli potrafimy precyzyjnie określić, czy infrastruktura jest w posiadaniu administracji czy podmiotu prywatnego, to wcale nie musi oznaczać, że potrafimy określić, kto jest odpowiedzialny za wtórne skutki awarii tej infrastruktury. To, że administracja publiczna nie może się obyć bez energii elektrycznej dostarczanej przez podmioty gospodarcze, jest dla wszystkich oczywistością. Natomiast nie jest już tak oczywiste, że administracja, poprzez rejestry państwowe czy dostarczanie programów do rozliczania podatków, oddziałuje na procesy realizowane przez świat biznesu. W tym drugim przypadku można wręcz stwierdzić, że działalność administracji jest źródłem ryzyka operacyjnego dla podmiotu gospodarczego. Już ten pobieżny przegląd zjawisk, z jakimi mamy do czynienia, wskazuje, że wyłanianie i kompleksowa ochrona infrastruktury krytycznej (w skrócie IK) muszą być stale dostosowywane do rzeczywistości technicznej, gospodarczej i społecznej.

Formalne podstawy ochrony IK

Podstawową regulacją prawną w tym zakresie jest ustawa o zarządzaniu kryzysowym[1] (w skrócie uzk), która reguluje tryb wyłaniania obiektów IK, zasady i obowiązki w zakresie ich ochrony, a także zasady współpracy administracji i podmiotów gospodarczych na rzecz tej ochrony. Należy jednak zwrócić uwagę, że ustawodawca za ochronę IK uznał również zapewnienie jej funkcjonalności oraz ciągłości działania, a nie tylko zapewnienie funkcjonowania i szybkiego odtworzenia. Obecne brzmienie terminu ochrony IK jest efektem implementacji dyrektywy Rady w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[2]. Zgodnie z art. 2 dyrektywy ochrona zdefiniowana została jako wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności IK w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków. Tę definicję zaimplementowano poprzez uzk. W efekcie ustawa określa, że IK ma być chroniona przed wszelkimi zagrożeniami, zarówno spowodowanymi działalnością ludzką (np. atakiem terrorystycznym), jak i przed zagrożeniami naturalnymi czy będącymi skutkiem awarii technicznej[3].

Zgodnie z filozofią uzk dyrektor RCB został zobowiązany do przygotowania w porozumieniu z właściwymi ministrami oraz kierownikami urzędów centralnych wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład IK. Po jego sporządzeniu dyrektor RCB sporządza wyciągi z wykazu dla ministrów i kierowników urzędów centralnych odpowiedzialnych za poszczególne systemy IK oraz wojewodów, na których terenach znajduje się dana infrastruktura. Ponadto dyrektora RCB zobowiązano do poinformowania właścicieli i posiadaczy IK o ujęciu ich obiektów w omawianym wykazie. Ustawodawca upoważnił wojewodę do poinformowania odpowiednich organów administracji publicznej o infrastrukturze znajdującej się na terenie danego województwa, co powoduje, że informacja o IK przekazywana jest jedynie niezbędnym podmiotom. Jednak w celu właściwej realizacji zadań z zakresu IK może zaistnieć potrzeba, by poszczególni wojewodowie, jak i inne organy administracji publicznej mogły się dowiedzieć o ujętej w wykazie infrastrukturze, która może mieć wpływ na realizację ich zadań. W tym celu uzk pozwala organom właściwym w sprawach zarządzania kryzysowego oraz dyrektorowi RCB żądać udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji ustawowych zadań[4].

Zazwyczaj ochrona infrastruktury kojarzona jest z ochroną fizyczną. Warto zatem wspomnieć, że zagadnienie to zostało już rozwiązane postanowieniami ustawy o ochronie osób i mienia[5] (UoOOiM). Zgodnie z nią obowiązek stosowania odpowiednich form ochrony obejmuje obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa. Ustawa wprost wskazuje, że jej postanowienia są rozciągnięte na obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej. Jednak zakres jej oddziaływania jest znacznie szerszy i dotyczy obiektów, które nie są uznawane za IK.

Organem nadzorującym wykonanie obowiązków wynikających z UoOOiM jest komendant wojewódzki Policji, który zatwierdza plany ochrony obiektu oraz sprawuje nadzór nad funkcjonowaniem wewnętrznych służb ochrony (w zakresie zagrożeń o charakterze terrorystycznym plany uzgadnia właściwy terytorialnie dyrektor delegatury Agencji Bezpieczeństwa Wewnętrznego). Nadzór nad firmami zajmującymi się ochroną fizyczną (specjalistycznymi uzbrojonymi formacjami ochronnymi, w skrócie SUFO) sprawuje Komendant Główny Policji, ale realizuje to zadanie poprzez komendanta wojewódzkiego.

Do wyłonienia obiektów i obszarów istotnych dla społeczności lokalnych oraz w celu zapewnienia właściwego poziomu ich ochrony, konieczna jest **współpraca następujących organów**:

- **wójta, burmistrza lub prezydenta miasta** (ustalenie stopnia ważności obiektu dla społeczności lokalnej, szczególnie dla funkcjonowania aglomeracji miejskich);
- **szefa ABW** (określenie poziomu wrażliwości obiektu na ewentualny atak terrorystyczny);
- **wojewody** (decyzje administracyjne związane z wykazem obiektów podlegających ochronie);
- **komendanta wojewódzkiego Policji** (zatwierdzanie planu ochrony obiektu, nadzór nad funkcjonowaniem służb ochrony).

Niekiedy utrzymywanie pełnej ochrony fizycznej obiektu jest ekonomicznie nieuzasadnione. W takim przypadku w planach ochrony obiektów można zawrzeć różne formy ochrony stosowane w zależności od stopnia zagrożenia.

Jednak ochrona fizyczna to tylko jeden z elementów kompleksowej ochrony IK. Działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia IK przez:

- zmniejszenie prawdopodobieństwa wystąpienia zagrożenia,
- zmniejszanie podatności,
- minimalizowanie skutków wystąpienia zagrożenia.

Na te działania składają się:

- **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;
- **zapewnienie bezpieczeństwa technicznego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
- **zapewnienie bezpieczeństwa osobowego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
- **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;
- **zapewnienie bezpieczeństwa prawnego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
- **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[6].

Zgodnie z uzk ochrona IK spoczywa przede wszystkim na właścicielach oraz posiadaczach samoistnych i zależnych obiektów, instalacji lub urządzeń IK. W celu zapewnienia ochrony IK Rada Ministrów wydała rozporządzenie, które określa sposób tworzenia i aktualizacji planów ochrony IK oraz zapewnia warunki i tryb uznania spełnienia obowiązku posiadania planu ochrony. Warunkiem niezbędnym jest, by posiadany już plan spełniał wymagania określone w rozporządzeniu RM w sprawie planów ochrony IK[7].

Właściciel lub posiadacz IK, poza elementami wymaganymi w myśl rozporządzenia, może zawrzeć w planie dodatkowe informacje, które są związane z jej specyficznym charakterem. W celu skorelowania planów ochrony z przygotowywanymi planami zarządzania kryzysowego oraz innymi przepisami z zakresu zarządzania kryzysowego plany wymagają uzgodnienia z następującymi organami:

1) w zakresie ich dotyczącym z właściwymi terytorialnie:
   a) wojewodą,
   b) komendantem wojewódzkim PSP,
   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 IK[8].

Plany, zarówno już posiadane, jak i opracowane na nowo, zatwierdzane są przez dyrektora RCB. Mając na uwadze, że nie wszyscy właściciele oraz posiadacze IK mogą posiadać odpowiednie poświadczenia i warunki przetwarzania informacji niejawnych, do planów stosować można przepisy o ochronie informacji niejawnych albo o ochronie tajemnicy przedsiębiorstwa. Plany podlegają aktualizacji w zależności od potrzeb, ale nie rzadziej niż raz na dwa lata.

Odpowiedzialność za ochronę IK

Jak już zostało wyżej wspomniane, ciężar ochrony IK spoczywa na jej operatorach. Zasadę, że to operator odpowiada za ochronę obiektów IK, podkreślają dokumenty planistyczne. W ustawie zrezygnowano z przygotowywania krajowego planu ochrony IK oraz planów wojewódzkich (pojęcie takich planów istniało w pierwotnej wersji uzk z 2007 r.). Obowiązek sporządzania planów ochrony IK spoczywa tylko na operatorach. Jednak biorąc pod uwagę znaczenie IK dla funkcjonowania państwa, ustawodawca zadania z zakresu ochrony tejże infrastruktury przypisał również podmiotom administracji publicznej. Nie można sobie wyobrazić, by władze publiczne, mając na uwadze potencjalne skutki awarii IK dla ludzi, ich mienia, gospodarki narodowej czy środowiska, odmówiły pomocy poszkodowanym, pozostawiając ten problem wyłącznie operatorowi IK. I bez znaczenia jest tu fakt, czy IK jest w zarządzie administracji publicznej, czy pozostaje całkowicie we władaniu podmiotów gospodarczych. Właśnie ze względu na spodziewane skutki awarii IK zadania z zakresu jej ochrony realizowane są na wszystkich szczeblach administracji, począwszy od administracji rządowej, a skończywszy na administracji samorządowej. Między innymi elementy związane z operacyjnymi działaniami w obszarze ochrony IK stały się załącznikami funkcjonalnymi do planów zarządzania kryzysowego[9].

W ramach działań podejmowanych przez administrację państwową szczególna rola przypada Szefowi ABW. Ustawodawca przypisał mu wiodącą rolę w sytuacji zagrożeń terrorystycznych dla IK. Ponieważ administracja publiczna, poza nielicznymi wyjątkami, nie ma możliwości prowadzenia kontroli w podmiotach gospodarczych, proces zatwierdzania planu jest podstawową formą działań mających na celu zmniejszenie poziomu ryzyka w obiektach IK. Dopiero po wprowadzeniu 2. lub wyższego stopnia alarmowego administracja aktywnie włącza się do działań mających chronić obiekty IK. Między innymi Szef ABW, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, może wydać Policji zalecenie szczególnego zabezpieczenia poszczególnych obiektów uwzględniające rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym[10].

Dwoistość postrzegania IK

W tym miejscu warto zwrócić uwagę na pewien paradoks związany z istnieniem IK. Dla jej właściciela (operatora) infrastruktura powinna przede wszystkim służyć osiąganiu zysku. W razie awarii straty powinny być pokryte ze środków własnych (w ramach bezpieczeństwa finansowego prowadzonej działalności) albo wyrównane poprzez ubezpieczenie (przeniesienie ryzyka na podmiot zewnętrzny). Decyzję o odbudowie powinna poprzedzić analiza kosztów (być może infrastruktury nie opłaca się odbudowywać, a przynajmniej nie w dotychczasowej for-

Rysunek 1. Podział skutków zdarzenia ze względu na podmiot odpowiedzialny. *Źródło: opracowanie własne.*

mie). Z punktu widzenia odbiorcy usługi, infrastruktura, a precyzyjniej usługa świadczona przez infrastrukturę, powinna zostać odtworzona w jak najkrótszym czasie, bez względu na koszty. Stąd wynika dwoistość postrzegania ochrony IK. Jednocześnie należy chronić obiekt IK oraz społeczność, którą mogą dotknąć skutki dysfunkcji IK. Za ochronę przed społecznymi skutkami awarii IK odpowiada już administracja publiczna. Zakres tych skutków można wywnioskować z definicji zawartych w ustawie o zarządzaniu kryzysowym. Zgodnie z ustawą, ilekroć mowa o sytuacji kryzysowej, należy przez to rozumieć: „sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej". W odniesieniu do obiektów IK ustawa posługuje się dodatkowo takimi pojęciami, jak: „kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców" (uzk, art. 3).
Biorąc powyższe pod uwagę, można dokonać podziału skutków zdarzeń ze względu na właściciela ryzyka (rys. 1).
Uogólniając powyższe spostrzeżenie, omawiany rysunek można zinterpretować następująco.

Dla właściciela (operatora IK) infrastruktura przez niego zarządzana powinna służyć przede wszystkim osiąganiu celów biznesowych (zysku). Jednocześnie ta sama infrastruktura powinna, poza celami biznesowymi, uwzględniać aspekt społeczny, jeśli prowadzona działalność lub jej czasowe zaprzestanie mogą wywołać skutki dla ludzi, ich mienia lub środowiska. Próby zdefiniowania, czym jest taka infrastruktura biznesowo-społeczna, podejmowane są w ramach badań naukowych nad logistyką społeczną. W ramach nich stwierdzono, że istnieją pewne usługi, np. związane z ratowaniem zagrożonego życia i zapewnieniem bezpieczeństwa (publicznego oraz w przestrzeni publicznej), które nie są realizowane z potrzeby zysku. Jednak grupę podmiotów kierujących się takimi celami ograniczono do organizacji non profit [Szołtysek, 2014, s. 5]. Inaczej podeszli do tego zagadnienia twórcy podziału logistyki na wojskową, cywilną i kryzysową. Według tej koncepcji głównym celem działania logistyki cywilnej jest maksymalizacja zysku przedsiębiorstwa, zaś logistyki kryzysowej – zaspokojenie elementarnych potrzeb logistycznych ludności. W tym drugim przypadku rachunek ekonomiczny ma znaczenie trzeciorzędne [Nowak, Nowak, 2009]. Oba te podejścia nie oddają w pełni, czym jest IK, i to zagadnienie wymaga dalszych badań.

Niezależnie jednak od prób zdefiniowania, czym jest IK jednocześnie z biznesowego i społecznego punktu widzenia, należy stwierdzić, że usługi (oraz związane z nimi procesy, podprocesy i procedury) dostarczane przez tę infrastrukturę można podzielić na takie, które służą wyłącznie celom biznesowym, i takie, których dysfunkcja wywoła społeczne skutki na tyle dolegliwe, że zarządzać nimi będzie musiało państwo. To stwierdzenie pozwala zadać pytanie, czy obecnie stosowany sposób wyłaniania obiektów IK uwzględnia aspekt społeczny. Aby udzielić odpowiedzi, konieczne jest spojrzenie na IK poprzez usługi, jakich ta infrastruktura dostarcza. Aby zrozumieć ideę podejścia usługowego, należy zauważyć, że operator IK nie jest właścicielem wszystkich ryzyk (a więc i skutków zdarzeń niekorzystnych) związanych z prowadzoną działalnością. W skali makroekonomicznej działania podmiotów gospodarczych mają wymiar społeczny i w tym przypadku właścicielem ryzyka staje się państwo. Dotyczy to nie tylko awarii i ich skutków, ale również zagadnień związanych z wyczerpywaniem się zasobów, zmianami w środowisku naturalnym czy zagospodarowaniem przestrzennym.

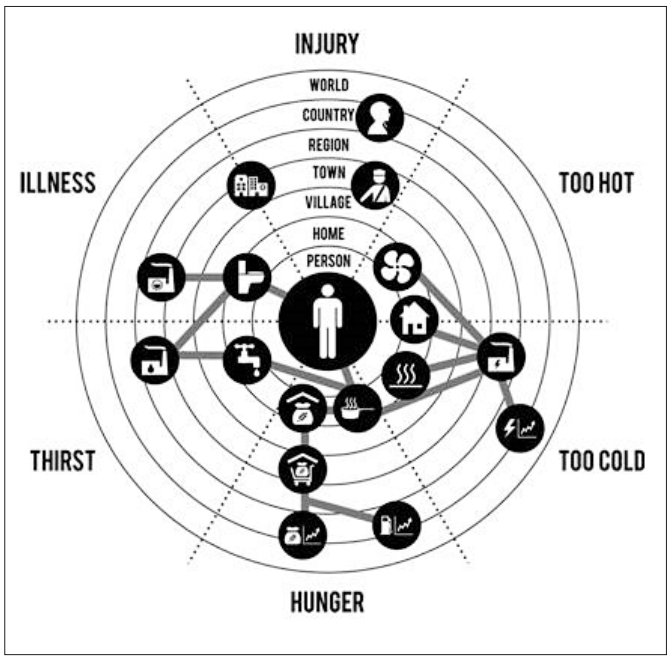
Społeczne skutki dysfunkcji IK

Wracając jednak na grunt sytuacji kryzysowych, trzeba podkreślić, że to oddziaływanie ma charakter bardziej dynamiczny i kompleksowy. Przykładowo – brak prądu w skali mikroekonomicznej oznacza dla elektrowni brak zysków i ewentualnie konieczność wypłaty odszkodowań. W skali makroekonomicznej brak prądu może oznaczać dla odbiorcy brak dostępu do pieniądza (nie działają bankomaty), brak możliwości przemieszczania się (niemożność zatankowania pojazdu) czy trudności z zakupem żywności (znaczna część produktów spożywczych wymaga chłodni). Te rodzaje ryzyk nie wchodzą w zakres odpowiedzialności elektrowni. Narzędziem do regulacji odpowiedzialności i podejmowania działań są w takiej sytuacji rozwiązania ustawowe. Podstawy teoretyczne pozwalające na zastosowanie podejścia usługowego w administracji publicznej istnieją od dawna, jednak dopiero cyfryzacja administracji oparta na realizowanych procesach przyśpieszyła te zmiany. Przykładowo, zorientowanie na procesy w administracji publicznej i usługi, jakie ona zapewnia, jest jedną z czterech podstawowych zasad, na których opiera się informatyzacja zintegrowana wdrażana w ramach e-administracji.
W efekcie w administracji publicznej można obserwować ten sam trend, który nastąpił w działalności biznesowej, gdzie podejście procesowe zaczyna dominować nad podejściem systemowym [Zawiła-Niedźwiedzki, Gołąb, 2010, s. 214]. Należy przyjąć, że ten kierunek działań zapewne będzie się pogłębiać, biorąc pod uwagę postanowienia dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[11] (tzw. dyrektywa NIS). Dyrektywa nakłada obowiązek wyłonienia przez państwa członkowskie tzw. usług kluczowych, tj. takich, które służą utrzymaniu „krytycznej działalności społecznej i gospodarczej". Formalnie dyrektywa odnosi się wyłącznie do bezpieczeństwa sieci i systemów teleinformatycznych w niektórych sektorach (energetyka, transport, bankowość i instytucje kredytowe, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa). Jednak celem szerszego zastosowania podejścia usługowego w dziedzinie ochrony IK, w RCB trwają prace koncepcyjne nad nową procedurą wyłaniania IK w oparciu o wcześniej zdefiniowaną listę usług kluczowych. Pierwszym krokiem na tej drodze jest ustalenie listy kryteriów, które uznajemy za krytyczne. Pomocna w tym przypadku może być metodyka „6 ways to die". Zgodnie z tym podejściem rolą administracji publicznej jest eliminacja sześciu czynników, które mogą spowodować śmierć człowieka. Tymi czynnikami są:

- głód,
- pragnienie,

- zranienia,
- choroby,
- zbyt wysoka temperatura,
- zbyt niska temperatura.

Jeśli dodamy do tych czynników niezbędne usługi z nimi związane i kolejne poziomy administracji, powstaje graf obrazujący wzajemne zależności:



Rysunek 2. Mapa infrastruktury krytycznej i jej poziomów.
Źródło: Źródło: Bennett, Gupta, 2010; za: Pyznar, Abgarowicz, 2014, s. 16.

Jak widać na rysunku, każdemu czynnikowi mogącemu spowodować śmierć osoby, można przypisać procesy i systemy oraz szczebel administracji odpowiedzialny za ich sprawne działanie (co nie oznacza, że administracja musi być operatorem danego systemu). Przykładowo – w ramach systemu „zaopatrzenie w wodę" można wyodrębnić procesy:

- ujmowanie i uzdatnianie wody przeznaczonej do spożycia przez ludzi;
- dostarczanie wody przeznaczonej do spożycia przez ludzi;
- odbiór i oczyszczanie ścieków.

Każdemu z nich można przypisać prawdopodobieństwo awarii i ocenić spodziewane skutki, wyliczając poziom ryzyka. Skutki można sparametryzować i przypisać do poszczególnych poziomów administracji, uzyskując w ten sposób podział na krytyczną infrastrukturę lokalną, regionalną i centralną (krajową). Przykładowo – lokalna IK może oznaczać brak usługi dla 100 tys. osób i więcej, regionalna powyżej 300 tys., zaś krajowa powyżej 500 tys. Przy okazji każdemu poziomowi można przypisać odpowiedni poziom ochrony, tak by niezbędne nakłady finansowe były adekwatne do poziomu ryzyka.

Proces wyłaniania obiektów IK przy takim podejściu składałby się z dwóch etapów:

- zidentyfikowanie usług krytycznych świadczonych przez dany obiekt;
- określenie skutków dysfunkcji danej usługi i porównanie z kryteriami przekrojowymi definiującymi IK lokalne, regionalne i krajowe.

Na koniec można wskazać niezbędny poziom zabezpieczeń adekwatny do klasy IK (lokalna, regionalna lub krajowa) i poziomu ryzyka.

Pierwszym etapem wdrożenia kompleksowej ochrony IK w rozumieniu usługowym jest uświadomienie decydentom skali złożoności problematyki związanej z całościowym ujęciem bezpieczeństwa. To z kolei wymaga ścisłej współpracy między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń IK. W celu stworzenia przejrzystego i prostego sposobu kontaktu administracji z właścicielami i posiadaczami IK zostali oni zobowiązani do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK[12]. Ta zasada nieco inaczej jest realizowana w odniesieniu do podmiotów działających w sektorach energii elektrycznej, ropy naftowej i paliw gazowych.

Zgodnie z ustawą o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych zarząd spółki, w porozumieniu z ministrem właściwym do spraw Skarbu Państwa[13] oraz dyrektorem RCB, powołuje i odwołuje pełnomocnika do spraw ochrony infrastruktury krytycznej[14]. Pełnomocnik do spraw ochrony infrastruktury krytycznej jest pracownikiem spółki monitorującym jej działalność w zakresie działań, co do których minister Skarbu Państwa ma prawo zgłoszenia sprzeciwu. Ponadto pełnomocnik może być odpowiedzialny za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej i ma wiele dodatkowych zadań ustawowych. W efekcie powstały dwa różne systemy organizacyjne ochrony obiektów IK ze strony jej właściciela lub posiadacza. Pierwszy, wynikający z uzk, zakłada, że administracja rządowa nie ingeruje w strukturę organizacyjną podmiotu i zakres zadań osoby odpowiedzialnej za bezpieczeństwo IK. Drugi, wynikający z ustawy o szczególnych uprawnieniach (…), opiera się na ingerencji w strukturę podmiotu zarządzającego IK i ściśle zdefiniowanych ustawowo zadaniach pełnomocnika do spraw ochrony IK. Przy okazji pojawiły się dwa różne określenia osoby zajmującej się taką ochroną. Raz jest to „osoba odpowiedzialna za kontakty", w drugim przypadku „pełnomocnik do spraw ochrony IK". Wydaje się, że w dłuższej perspektywie taka dwoistość w podejściu do ochrony IK powinna zostać zlikwidowana na rzecz tego drugiego rozwiązania.

Niezależnie od tego, która ustawa reguluje zasady organizacyjne, z całą stanowczością należy podkreślić, że jedynie dobra współpraca pomiędzy osobą odpowiedzialną za utrzymywanie kontaktów (ewentualnie pełnomocnika) a właściwymi podmiotami, w zakresie których leżą zadania z zakresu ochrony IK, daje gwarancję, iż opisany w niniejszym artykule mechanizm jej ochrony przyniesie spodziewane rezultaty.

PODSUMOWANIE

Całościowe podejście do ochrony IK wymaga kompleksowego zarządzania ryzykiem w rozumieniu oddziaływania na przyczynę (źródło zagrożenia), środowisko, w którym ryzyko może się rozprzestrzeniać (redukowanie podatności), oraz skutki (zarówno w aspekcie technicznym, finansowym, jak i społecznym). Jednocześnie wszystkie formy ochrony muszą być traktowane jako równie istotne. Zatem zarówno ochrona fizyczna, jak i ochrona teleinformatyczna (jak i wszystkie pozostałe) muszą być traktowane równorzędnie, jako element zarządzania bezpieczeństwem.

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209, z późn. zm.).

[2] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345/75).

[3] W kwestii ochrony IK na świecie widoczne są dwa trendy. Pierwszy, w którym ochrona IK nakierowana jest głównie na zagrożenia przed atakami terrorystycznymi, i drugi, w którym ochrona ma na celu przeciwdziałanie wszelkim zagrożeniom. Należy zauważyć, że powoli zmienia się podejście państw w tej kwestii i działania ochrony kierowane są na przeciwdziałanie wszelkim zagrożeniom. Całościowe podejście obejmuje jednocześnie zagrożenia dla IK i zagrożenia powodowane przez dysfunkcję IK. Przykładem kraju, gdzie obowiązuje takie podejście, są Stany Zjednoczone Ameryki.

[4] Tamże, art. 20a.

[5] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2016 r. poz. 1432, z późn. zm.).

[6] NPOIK, RCB 2015, s. 31–32.

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

[8] Tamże, § 4 ust. 1.

[9] Art. 12 ust. 2 pkt 4, art. 14 ust. 2 pkt 7, art. 15, art. 17 ust. 2 pkt 6, art. 19 ust. 2 pkt 6 uzk.

[10] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904, z późn. zm.).

[11] Dyrektywa Parlamentu i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1).

[12] Art. 6 ust. 5a ustawy o zarządzaniu kryzysowym.

[13] W odniesieniu do operatora systemu przesyłowego elektroenergetycznego i operatora systemu przesyłowego gazowego rolę ministra właściwego do spraw Skarbu Państwa realizuje Pełnomocnik rządu do spraw Strategicznej Infrastruktury Energetycznej. Zob. szerzej: rozporządzenie Rady Ministrów z dnia 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej (Dz. U. poz. 2116).

[14] Zob. szerzej: ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2016 r. poz. 2012).

Bibliografia

Bennett M., Gupta V., *Dealing in Security understanding vital services and how they keep you safe*, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 7.11.2017 r.].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19.7.2016 r.).

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345/75 z 8.12.2008 r.).

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) z dnia 2 listopada 2015 r. przyjęty uchwałą Rady Ministrów nr 210/2015 z uwzględnieniem uchwały nr 61/2016 Rady Ministrów z dnia 1 czerwca 2016 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf [dostęp: 7.11.2017 r.].

Nowak W., Nowak E., *Podstawy logistyki w sytuacjach kryzysowych z elementami zarządzania logistycznego*, SWSPiZ, Łódź–Warszawa 2009.

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

Pyznar M., Abgarowicz G., *Rola infrastruktury krytycznej w funkcjonowaniu państwa*, w: *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, red J. Świątkowska, Instytut Kościuszki, Kraków 2014.

Skomra W., *Ochrona Infrastruktury Krytycznej w systemie zarządzania kryzysowego*, w: *Ochrona infrastruktury krytycznej*, red. A. Tyburska, Wydawnictwo WSPol, Szczytno 2010.

Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik*, Wydawnictwo Presscom, Wrocław 2016.

Szołtysek J., *Przesłanki i założenia koncepcji logistyki społecznej*, „Gospodarka Materiałowa i Logistyka" 2014, nr 2.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Public Law 107–56, OCT. 26, 2001.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904, z późn. zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209, z późn. zm.).

Zapłata S., Kaźmierczak M., *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Oficyna Wolter Kluwer Business, Warszawa 2011.

Zawiła-Niedźwiecki J., Gołąb P., *Zapewnienie ciągłości działania jako ograniczenie ryzyka operacyjnego*, w: *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

Summary

Comprehensive approach for the selection and protection of critical infrastructure

Digital technologies on the one hand improve the quality of services supplied for citizens, but at the same time they are the source of new threats. As a result, apart from current types of security management (physical or technical security) there appear its new forms, being a reply to new threats (cybernetic security, personal data security etc). These diversified actions, to achieve the intentional effect, should be treated as elements of the greater whole. This greater whole means the comprehensive security management including not only actions in favour of the own unit, but also the ones taking into account both the influence of outside entities and possible social effects deriving from a dysfunction of services provided by the entity. A service approach, as a method allowing for the hierarchization of processes carried out as part of the civil service, is a brand new issue requiring both mental changes amongst the managing staff as well as the adaptation of formal structures to requirements connected with the necessity to implement new forms of the security management.

Tłumaczenie: Renata Cedro