Dr inż. Grzegorz Kunikowski, Wydział Zarządzania, Politechnika Warszawska

Ocena ryzyka

w perspektywie przedsiębiorstwa energetycznego

W artykule przedstawiono podstawy prawne obowiązku opracowywania planów ochrony obiektów energetycznych, zaliczonych do infrastruktury krytycznej. Omówiono wybrane podejścia metodyczne oceny ryzyka i przedstawiono ustawodawcze trendy zarządzania kryzysowego związane z odchodzeniem od ochrony infrastruktury krytycznej na rzecz bezpieczeństwa dostaw usług kluczowych. Zwrócono uwagę na potrzeby kompetencji specjalistów zarządzania bezpieczeństwem usług kluczowych.

O rosnącym znaczeniu oceny ryzyka w zarządzaniu świadczą wymagania i praktyka, zarówno w administracji publicznej i spółkach Skarbu Państwa, gdzie dotyczą one m. in. kontroli zarządczej (Dz. Urz. Min. Fin. poz. 56, 2012; Dz.U. 2009 nr 157 poz. 1240, 2009), jak i w sektorze komercyjnym, chociażby w bankowości. Ocena ryzyka ma szczególne znaczenie w zarządzaniu bezpieczeństwem infrastruktury krytycznej. Jest też nieodłącznym elementem w zarządzaniu kryzysowym, gdzie określone wymagania formułuje Unijny Mechanizm Ochrony Ludności.

Jako swoistą ciekawostkę warto przytoczyć, że nałożone na jednostki samorządowe obowiązki planistyczne związane z zarządzaniem kryzysowym obejmują nie tylko przygotowanie takich planów, ale również zagwarantowanie ich spójności. Wiąże się to z licznymi problemami, „występuje powtarzalność danych (analiza obszaru, analiza ryzyka, siły i środki, itp.) w różnych planach, odnoszących się do tego samego terenu (szczebla zarządzania państwem), przy czym jedne z planów to dokumenty jawne, inne natomiast o stosownej klauzuli tajności" (Kosowski, 2013, s. 59). W rezultacie postulowane jest ograniczanie liczby planów do jednego planu zarządzania bezpieczeństwem.

Na przedsiębiorstwa będące operatorami infrastruktury krytycznej, szczególnie istotne są dwa zadania. Mianowicie wyznaczenie pełnomocnika ds. ochrony infrastruktury krytycznej oraz zapewnienie jej bezpieczeństwa, czego elementem są plany ochrony. Plany wymagają szeregu uzgodnień m.in. z organami administracji publicznej i instytucjami odpowiedzialnymi za bezpieczeństwo. Ostatecznie zatwierdzane są przez Rządowe Centrum Bezpieczeństwa.

Podstawy formalne

Odnosząc się do zarządzania ryzykiem należy w szerszym kontekście przywołać Unijny Mechanizm Ochrony Ludności, który kształtuje modelowe podejście do zarządzania kryzysowego. Obiekty infrastruktury krytycznej o szczególnym znaczeniu dla państwa i gospodarki, są identyfikowane i oceniane pod względem koniecznych zabezpieczeń (zadanie Rządowego Centrum Bezpieczeństwa, RCB), również w kontekście międzynarodowym, a w tym transgranicznym. Plany ich ochrony w aspekcie transgranicznym muszą być zatwierdzane przez instytucje koordynacyjne. W Polsce jest to RCB.

Opracowywanie planów zarządzania ryzykiem w wymiarze klęsk żywiołowych na szczeblach krajowym i niższych zalecane jest w Unijnym Mechanizmie Ochrony Ludności. Państwa członkowskie powinny zapewnić skuteczne i spójne podejście do zapobiegania klęskom i katastrofom przez wymianę niepodlegających specjalnej ochronie informacji, mianowicie informacji, których ujawnienie nie byłoby sprzeczne z podstawowym interesem bezpieczeństwa państw członkowskich oraz wymianę najlepszych praktyk w ramach unijnego mechanizmu.

Dla zidentyfikowanych obiektów infrastruktury krytycznej, w sytuacjach kryzysowych o transgranicznym wy-

miarze skutków realizowana jest współpraca międzynarodowa, inicjowana i prowadzona pomiędzy kierownikami urzędów centralnych i odpowiadających im centrami UE i NATO. W odniesieniu do operatorów infrastruktury krytycznej rekomendowane jest zawieranie porozumień o wzajemnej pomocy obowiązujące właścicieli i/lub operatorów. *„Poszczególne sektory mają własne doświadczenia, wiedzę fachową i wymagania w odniesieniu do ochrony infrastruktury krytycznej, dlatego należy opracować i zrealizować wspólnotowe podejście do ochrony infrastruktury krytycznej, z uwzględnieniem specyfiki poszczególnych sektorów i dotychczasowych środków sektorowych, w tym środków już stosowanych na poziomie Wspólnoty, na poziomie krajowym lub regionalnym oraz, w stosownych przypadkach, transgraniczne porozumienia o wzajemnej pomocy obowiązujące właścicieli/operatorów infrastruktury krytycznej. Wspólnotowe podejście wymaga założenia pełnego zaangażowania sektora prywatnego z uwagi na bardzo istotny udział tego sektora w nadzorowaniu ryzyka, zarządzaniu ryzykiem, planowaniu ciągłości działania i w procesie przywracania stanu sprzed katastrofy* (KE, 2008, s. pkt. 8).

Obowiązki operatorów infrastruktury krytycznej w zakresie zabezpieczeń wynikają z zapisów Ustawy o zarządzaniu kryzysowym i Narodowego Programu Ochrony Infrastruktury Krytycznej, który przygotowuje i aktualizuje RCB. Zgodnie z Programem, operatorzy są zobowiązani do:

- przygotowania i wdrażania, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia,
- wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej,
- niezwłoczne przekazywanie Szefowi Agencji Bezpieczeństwa Wewnętrznego, informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej,
- współpracy w tworzeniu i realizacji Programu (RCB, 2018, s. 16).

W planach ochrony zaś konieczne jest dokonywanie oceny ryzyka zakłócenia funkcjonowania systemu IK, wywołanego zniszczeniem lub zakłóceniem funkcjonowania IK (gromadzenie informacji niezbędnych do identyfikacji zagrożeń, określania skutków zakłócenia IK oraz określenia podatności systemu IK (RCB, 2018, s. 19).

Zakres planów ochrony infrastruktury krytycznej, które przygotowują jej operatorzy określa przedmiotowe rozporządzenie (Dz. U. 2010 nr 83 poz. 542, 2010). Elementami planu (oprócz danych ogólnych, danych dotyczących konkretnej infrastruktury oraz ustalonych zasad współpracy z centrami zarządzania kryzysowego i organami administracji publicznej) są charakterystyki:

- zagrożeń oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń,
- zależności infrastruktury krytycznej od pozostałych systemów infrastruktury krytycznej oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej,
- zasobów własnych możliwych do wykorzystania w celu ochrony infrastruktury krytycznej.

Dla zidentyfikowanych i ocenionych zagrożeń określane warianty: działania w sytuacji zagrożenia lub zakłócenia funkcjonowania; zapewniania ciągłości funkcjonowania; odtwarzania.

Wybrane metody oceny ryzyka

Ocena ryzyka jest nieodłącznym elementem planowania w zarządzaniu kryzysowym. Współczesny model zarządzania kryzysowego uwzględnia cztery etapy: zapobieganie, przygotowanie, reagowanie i odbudowę. Warto zwrócić uwagę na odchodzenie od militarnego charakteru zarządzania kryzysowego na rzecz modelu współpracy (Alexander, 2016, s. 8), czy też otwarcia na administrację publiczną (Gołębiewski, 2015, s. 9-10). Powszechnym standardem w zakresie oceny ryzyka jest rodzina standardów ISO 31000, kierowana do publicznych, prywatnych lub spółdzielczych przedsiębiorstw, stowarzyszeń, grup, a nawet osób fizycznych. *ISO 31000 została zaadaptowany przez 41 państw, począwszy od Japonii do Stanów Zjednoczonych, gdzie stanowi standardy zarządzania ryzykiem w sektorze publicznym organizacji* (Drennan, McConnell, & Stark, 2014, s. 11). Pierwowzorem dla ISO 31000 był standard zarządzania ryzykiem AS/NZS 4360 opracowany w Australii i Nowej Zelandii, który upowszechniał się początkowo w Kanadzie i Japonii. W Europie organizacje branżowe np. FERMA (*Federation of European Risk Management Associations*) adoptowały i upowszechniały standardy opracowane w Wielkiej Brytanii. Zestawienie metod i technik podaje norma (ISO/IEC, 2009), a metody oceny i zarządzania ryzykiem w zarządzaniu kryzysowym rozwinięto i opisano w publikacjach naukowych i praktycznych, np. (Kosieradzka & Zawiła-Niedźwiecki, 2016; Skomra, 2015; Zawiła-Niedźwiecki, 2018).

We współczesnym zarządzaniu kryzysowym proces oceny ryzyka został podzielony na pięć podprocesów:

- ustalenie kontekstu procesu - skupiające się na identyfikacji i opisie podmiotu chronionego,
- identyfikacja zagrożeń - polegająca na identyfikacji wszelkich zjawisk oraz zdarzeń, które stanowią potencjalne ryzyko dla badanej organizacji - wynikiem podjętych działań jest wykaz zagrożeń oraz powiązania zachodzące pomiędzy nimi,
- analiza ryzyka - skupiająca się na analizie przyczyn, mechanizmu re-

alizacji zagrożenia i skutków jego wypełnienia - wynikiem podjętych działań są opracowane kryteria skutków i prawdopodobieństwa wystąpienia zagrożenia,
- szacowanie ryzyka - polegające na dokonaniu oceny prawdopodobieństwa i skutku każdego zidentyfikowanego ryzyka - wynikiem podjętych działań jest skwantyfikowane ryzyko oraz opracowana macierz ryzyka,
- postępowanie z ryzykiem - skupiające się na opracowaniu działań wykonywanych w ramach tolerowania, zapobiegania i monitorowania ryzyka - wynikiem działań jest opracowanie planów postępowania z ryzykiem (Kosieradzka & Zawiła-Niedźwiecki, 2016, s. 185).

> Ocena ryzyka jest nieodłącznym elementem planowania w zarządzaniu kryzysowym. Współczesny model zarządzania kryzysowego uwzględnia cztery etapy: zapobieganie, przygotowanie, reagowanie i odbudowę

Do najważniejszych norm z zakresu zarządzania ryzykiem należą (Kosieradzka & Zawiła-Niedźwiecki, 2016, s. 24-26):
- PKN-ISO Guide 73:2012P - przedstawiająca spójne podejście do zarządzania ryzykiem i standaryzująca terminologię z nim związaną,
- PN-ISO 31000:2018-08 (wersja ang., zastępująca PN-ISO 31000:2012) - przedstawiająca ogólne zasady i wytyczne dotyczące poszczególnych faz procesu zarządzania ryzykiem w organizacji,
- BS 31100:2011 - przedstawiający praktyczne wskazówki wdrożenia zasad efektywnego zarządzania ryzykiem,
- PN-ISO/IEC 27005:2010P - przedstawiająca wytyczne dotyczące zarządzania ryzykiem związanego z bezpieczeństwem informacji,
- BSI Threat Catalogues - przedstawiająca typowe zagrożenia w systemach IT,
- ISO/IEC TR 13335 - przedstawiająca listę zagrożeń i stosowane metody w zakresie zarządzania bezpieczeństwem systemów informatycznych.

Przywołany wcześniej Narodowy Program Ochrony Infrastruktury Krytycznej, przyjmuje jako kluczową zasadę *proporcjonalności i działań opartych na ocenie ryzyka. Oznacza ona, że wszelkie działania podejmowane w celu zapewnienia ochrony IK powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania. Dotyczy to zarówno przyjętego modelu ochrony IK, jej rodzajów, a także użytych sił i środków* (RCB, 2015, s. 121). Rekomendowane jest zgodne z normą (PN-ISO 31000:2018-08, 2018, s.) szacowanie ryzyka, na które składa się: identyfikacja zagrożeń, analiza ryzyka i ewaluacja ryzyka. Wskazywana jest teoria zarządzania ciągłością działania organizacji i zwrócenie uwagi na procesy krytyczne w danej organizacji. Te zaś można identyfikować stosując podejście określane analizą wpływu (BIA - *Business Impact Analysis*).

Zidentyfikowane ryzyko, które zostało ocenione, w zależności od uzyskanego rezultatu można tolerować, inaczej akceptować, unikać, minimalizować lub transferować, czyli przenosić na inne podmioty.

Od ochrony obiektów do ochrony usług

Relatywnie nowym podejście w zarządzaniu kryzysowym i bezpieczeństwie infrastruktury krytycznej jest wyodrębnienie usług kluczowych. W ustawie o cyberbezpieczeństwie usługa kluczowa jest definiowana jako usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych (Dz.U. 2018 poz. 1560, 2018, s. Art. 2, pdpk. 16).

Usługi kluczowe przyporządkowywane są danego sektora, podsektora i rodzaju podmiotu. Natomiast progi istotności skutku zakłócającego nie są określane wg perspektywy geograficznego zasięgu, lecz poprzez inne parametry, takie jak: liczbę użytkowników zależnych, zależność innych sektorów, uwzględnienie skutków oddziaływania na ogólnie określaną działalność gospodarczą i społeczną oraz bezpieczeństwo publiczne.

Z usługami kluczowymi łączy się szereg wyzwań. Mianowicie obowiązująca dyrektywa, która dotyczy bezpieczeństwa sieci i systemów teleinformatycznych mówi o tym, że *...państwa członkowskie powinny być odpowiedzialne za określanie, które podmioty spełniają kryteria definicji operatora usług kluczowych (...) przy czym (...) aby zapewnić spójne podejście, definicja operatora usług kluczowych powinna być stosowana w sposób spójny przez wszystkie państwa członkowskie* (KE, 2016). Dyrektywa została transponowana do prawa krajowego w zakresie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560, 2018), a na opracowywanym, w randze rozporządzenia wykazie dostawców usług kluczowych (RM-110-89-18/projekt, 2018, s. Zał. 2) znajdujemy przedsiębiorstwa sektora paliwowo-energetycznego w układzie: elektroenergetyka (wytwarzanie, przesył i dystrybucja); ropa naftowa (rafinacja, produkcja i dystrybucja paliw, przesył i magazynowanie); gaz (dostawcy, przetwórcy, dystrybucja, przesył, magazynowanie, operatorzy systemu LNG).

Wnioski

Dotychczas stosowane metody oceny ryzyka w zakresie obecnych potrzeb sprawdzają się i są wystarczająco skuteczne. Wywodzące się z sektora bankowego z powodzeniem zostały zaadoptowane i są skutecznie stosowane w administracji i sektorze przedsiębiorstw.

Należy zwrócić uwagę i dostrzec znaczenie przechodzenie w zarządzaniu kryzysowym od ochrony obiektów infrastruktury krytycznej do perspektywy usług kluczowych, co wiąże się z kierunkiem przyszłej nowelizacji Ustawy o zarządzaniu kryzysowym. W konsekwencji zaś oznacza wyzwania dla operatorów infrastruktury krytycznej w zakresie oceny skutków zakłóceń ciągłości działania. Wyzwania wynikają stąd, że usługa kluczowa jest zazwyczaj zależna od kilku systemów infrastruktury krytycznej. Powiązania pomiędzy systemami należy skutecznie identyfikować, a następnie oceniać ryzyka i skutki z szerszej perspektywy współzależności, np. dostawców energii i systemów teleinformatycznych. Należy zakładać, że w planowaniu zabezpieczeń wzrośnie znaczenie podejścia sytuacyjnego, analiz scenariuszy i efektu domina (kaskady zdarzeń) i zaawansowanych metod symulacji. Nie ulega też wątpliwości, że konieczne będzie przygotowanie kadry osób zajmujących się bezpieczeństwem, a posiadających techniczne kompetencje, pozwalające na rozumienie funkcjonowania systemów infrastruktury krytycznej z perspektywy ich współzależności.

Literatura

Alexander, D. E. (2016). How to Write an Emergency Plan. Edinburgh, England: Dunedin Academic Press.

Drennan, L. T., McConnell, A., & Stark, A. (2014). Risk and Crisis Management in the Public Sector (2 edition). New York: Routledge.

Dynak Robert. (2013). Przygotowanie struktur kierowania do działania w sytuacjach kryzysowych na szczeblu lokalnym (s. 87-108). Zaprezentowano na Planowanie cywilne w systemie zarządzania kryzysowego, Józefów: Wydawnictwo Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej im. Józefa Tuliszewskiego.

Dz. Urz. Min. Fin. poz. 56. (2012). Komunikat Nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem.

Dz.U. 2009 nr 157 poz. 1240. (2009). Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych.

Dz.U. 2010 nr 83 poz. 542. (2010). Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej.

Dz.U. 2018 poz. 1560. (2018). Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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

Gołębiewski, J. (2015). Zarządzanie kryzysowe na szczeblu samorządowym: teoria i praktyka. Warszawa: Difin.

ISO/IEC. (2009). IEC 31010:2009 Risk management - Risk assessment techniques.

KE. (2008). Dyrektywa Parlamentu Europejskiego i 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. Dziennik Urzędowy Unii Europejskiej L.345/75.

KE. (2013). DECYZJA PARLAMENTU EUROPEJSKIEGO I RADY NR 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności. Dziennik Urzędowy Unii Europejskiej L347/924.

KE. (2016, lipiec 19). 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. Dziennik Urzędowy Unii Europejskiej L.194/1. Pobrano z http://data.europa.eu/eli/dir/2016/1148/oj/pol

Kosieradzka, A., & Zawiła-Niedźwiecki, J. (Red.). (2016). Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym. Kraków ; Legionowo: edu-Libri.

Kosowski, B. (Red.). (2013). Planowanie w systemie zarządzania bezpieczeństwem sfery cywilnej (s. 89-106). Zaprezentowano na Planowanie cywilne w systemie zarządzania kryzysowego, Józefów: Wydawnictwo Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej im. Józefa Tuliszewskiego.

PN-ISO 31000:2018-08. (2018). Risk management - Guidelines.

RCB. (2015). Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1 Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej - dobre praktyki i rekomendacje. Warszawa: Rządowe Centrum Bezpieczeństwa.

RCB. (2018). Narodowy Program Ochrony Infrastruktury Krytycznej. Warszawa: Rządowe Centrum Bezpieczeństwa.

RM-110-89-18/projekt. (2018). Projekt Rozporządzenia Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

Skomra, W. (Red.). (2015). Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP. Warszawa: Szkoła Główna Służby Pożarniczej: BEL Studio.

Zawiła-Niedźwiecki, J. (2018). Od zarządzania ryzykiem operacyjnym do publicznego zarządzania kryzysowego: wyzwania badawcze. Kraków; Legionowo: edu-Libri.

Prezentowane wyniki badań są częścią projektu badawczo-rozwojowego NCBiR pt. Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej Rzeczypospolitej Polskiej oraz w jednostkach organizacyjnych Krajowego Systemu Ratowniczo Gaśniczego, nr umowy DOB - BIO7/11/02/2015 realizowanego przez konsorcjum: Politechnika Warszawska (Wydział Zarządzania), Medcore sp. z o.o.