CZASOPISMO INŻYNIERII LĄDOWEJ, ŚRODOWISKA I ARCHITEKTURY
JOURNAL OF CIVIL ENGINEERING, ENVIRONMENT AND ARCHITECTURE
JCEEA, t. XXXIII, z. 63 (2/I/16), kwiecień-czerwiec 2016, s. 291-298

Janusz RAK[1]

ZASADY OKREŚLANIA PRZYNALEŻNOŚCI DO INFRASTRUKTURY KRYTYCZNEJ

Bezpieczeństwo i ochrona systemu są ściśle związane z różnego rodzaju zagrożeniami, które w sposób dynamiczny ewoluują. To z kolei powoduje konieczność antycypacji i kreowania nowych metod przeciwdziałania tego rodzaju zagrożeniom. W pracy poddano analizie metodologię określania przynależności do infrastruktury krytycznej. Wykaz sektorów określa ustawa o zarządzaniu kryzysowym. Krótko omówiono dwie awarie infrastruktury krytycznej. Podano kryteria kwalifikacji do infrastruktury krytycznej. Zaproponowano nowe sposoby finansowania ryzyka katastroficznego. Odniesiono się do elementów ochrony infrastruktury krytycznej. Na przykładzie systemu zbiorowego zaopatrzenia w wodę szczegółowo przedstawiono kryteria identyfikacyjne. Podsumowaniem rozważań naukowych jest określenie strategii zrównoważonego systemu wodociągowego.

Słowa kluczowe: infrastruktura krytyczna, system wodociągowy, zagrożenia, ochrona

1. Wstęp

Panuje pogląd, że etymologia słowa infrastruktura wywodzi się z łacińskiego terminu „infra structura", co oznacza „podstawę określonego układu lub konstrukcji"[3]. Infrastrukturę charakteryzuje: niezbędność – coś, bez czego nie można się obejść, coś nieodzownego, niezbędnego; podstawa – coś na czym to stoi, wspiera się, fundament czegoś. Paradoksalnie można stwierdzić, że istotą ochrony infrastruktury jest ona sama, a nie zachodzące dzięki niej procesy. Wykaz sektorów infrastruktury krytycznej przedstawia się następująco: energetyka (energia elektryczna, ropa i gaz ziemny), technologie informacyjno – komunikacyjne, zaopatrzenia w żywność i wodę, służba zdrowia, finanse, transport i przemysł chemiczny [9].

W odniesieniu do zbiorowego zaopatrzenia w wodę przez wodociąg infrastruktura krytyczna to systemy, oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty budowlane, urządzenia, sieci instalacyjne kluczowe dla

[1] Janusz R. Rak, Politechnika Rzeszowska, al. Powstańców Warszawy 6, 35-959 Rzeszów, tel. 17/865-14-49, rakjan@prz.edu.pl

bezpieczeństwa zaopatrzenia w wodę aglomeracji miejskiej i jej mieszkańców [7].

Wg Ustawy o zarządzaniu kryzysowym z 26 kwietnia 2007 roku infrastruktura krytyczna obejmuje następujące systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatyczne, finansowe, zaopatrzenie w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewnienia ciągłości działania administracji publicznej oraz produkcji, składowania i przechowywania oraz stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi [9].

W Unii Europejskiej obowiązuje Dyrektywa Rady z 2008 roku, która definiuje infrastrukturę krytyczną jako „składnik, system lub część infrastruktury zlokalizowanej na terytorium państw członkowskich, 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 dane państwo członkowskie w wyniku utracenia tych funkcji" [2].

2. Sposoby finansowania ryzyka katastroficznego

Istnieją dwa podstawowe sposoby finansowania ryzyka związanego ze zdarzeniami niepożądanymi [10].

Prospektywne finansowanie ryzyka zachodzi wówczas, gdy przed wystąpieniem negatywnych skutków ryzyka przedsiębiorstwo przygotowuje środki na ich sfinansowanie. Stosuje się mechanizm gromadzenia rezerw.

Retrospektywne finansowanie ryzyka występuje wówczas, gdy środki finansowe przeznaczone na pokrycie niekorzystnych skutków ryzyka przedsiębiorstwo pozyskuje dopiero wtedy, kiedy ryzyko się zmaterializuje. Środki mogą przykładowo pochodzić z wcześniej określonego źródła (np. odszkodowanie od ubezpieczyciela).Tradycyjne instrumenty finansowania ryzyka dzieli się na:

- instrumenty retencji ryzyka, które wymagają tworzenia rezerw finansowych na pokrycie negatywnych skutków ryzyka;
- instrumenty transferu ryzyka, które polegają na finansowaniu niepożądanych skutków przez podmiot trzeci.

Współczesne metody zarządzania ryzykiem w przedsiębiorstwach wykonywały instrumenty alternatywnego finansowania ryzyka, które wywodzą się z rynku reasekuracji. Instrumenty alternatywne opierają się na równoczesnym stosowaniu retencji i transferu ryzyka. Efektywność finansowania niepożądanych skutków ryzyka zakłada, że transfer ryzyka uruchamia się po wykorzystaniu rezerw utworzonych w ramach retencji ryzyka [10].

3. Spektakularne awarie infrastruktury krytycznej

W sierpniu 2003 roku na pograniczu USA i Kanady na skutek przeciążeń w systemie elektroenergetycznym nastąpiło wyłączenie około 100 elektrowni. Ponad 60 mln ludzi przez 20 godzin zostało pozbawionych dostawy energii elektrycznej. Blackout objął największe aglomeracje tego regionu: Nowy Jork, Toronto, Detroit czy Ottawę, powodując zawieszenia na lotniskach tych miast loty samolotów, stanął transport kolejowy, stanęło metro, wystąpiły ograniczenia w dostawie wody, a brak sygnalizacji świetlnej spowodował chaos w ruchu ulicznym. Z kolei w Polsce w nocy z 7 na 8 kwietnia w oddalonym o 100 kilometrów od Szczecina Krojniku pod wpływem ciężaru mokrego śniegu zawalił się słup energetyczny. Spowodowało to efekt domina w postaci zniszczenia kolejnych słupów. O godzinie 3^{30} pogrążyła się w ciemności lewobrzeżna część Szczecina. Poranek został już kilkaset tysięcy ludzi bez prądu. Z nielicznych otwartych sklepów, które nie posiadały kas fiskalnych masowo wykupywano pieczywo i wodę mineralną. W dużej części mieszkań nie było wody i pojawiły się problemy z odprowadzaniem ścieków (Szczecin posiada liczną i rozbudowaną sieć przepompowni kanalizacyjnych), przestały działać też sieci telefonii komórkowej. W celach prewencyjnych na ulicach miasta pojawiły się wspólne patrole policji i żandarmerii wojskowej.

Jakkolwiek najbardziej spektakularne awarie infrastruktury krytycznej dotyczyły systemów zaopatrzenia w energię elektryczną, to jednak efekt domina obejmował także inne systemy zaliczane do tej grupy [7].

4. Elementy ochrony infrastruktury krytycznej

Cechą ochrony infrastruktury krytycznej powinno być zapewnienie jej ciągłości działania, szczególnie w stanach zagrożenia jej bezpieczeństwa. Jest wszechobecna oraz niezbędna, co uświadamiamy sobie dopiero, gdy zabraknie prądu, wody albo gdy nie można uzyskać dostępu w połączeniach np. telefonii komórkowej. Rodzaje ochrony [4]:

- ochrona fizyczna – ma za zadanie minimalizować ryzyko zakłócenia funkcjonowania infrastruktury przez osoby, które znalazły się na jej terenie w sposób nieuprawniony. Ma na celu zapewnienie bezpieczeństwa dla uprawnionych pracowników, ochronę mienia poprzez zapobieganie wykroczeniom lub przestępstwom;
- ochrona techniczna – ma za zadanie minimalizować ryzyka zakłócenia eksploatacji obiektów, urządzeń i instalacji. Działania techniczne mają zapewnić ciągłość funkcjonowania infrastruktury krytycznej w zgodności z obowiązującymi przepisami i normami;
- ochrona teleinformatyczna – ma za zadanie minimalizować ryzyko zakłócenia związanego z wykorzystaniem do użytkowania infrastruktury systemów i sieci

teleinformatycznych. Ochrona obejmuje również przedsięwzięcie przed cyberatakami, cyberprzestępcami, a także cyberterroryzmem. Procedury z nią związane obejmują także przeciwdziałania tego rodzaju zdarzeniom niepożądanym. Działania ochronne ze swej natury mają charakter prewencyjny i dotyczą zagrożeń, które można antycypować. Ochrona infrastruktury krytycznej jest warunkiem koniecznym ale nie wystraczającym zapewnieni jej bezpieczeństwa.

5. Kryteria kwalifikacji do infrastruktury krytycznej

Rządowe Centrum Bezpieczeństwa nie ujawnia szczegółów identyfikacji przynależności do infrastruktury krytycznej. Podawane są tylko ogólne procedury w tym zakresie, które podzielone są na dwie grupy [5,6]:

- kryteria systemowe – w sposób ilościowy określają parametry obiektu, urządzenia, instalacji lub usługi, których spełnienie może skutkować zaliczeniem do infrastruktury krytycznej. Kryteria te są odrębne dla każdego z systemów zaliczanych do infrastruktury krytycznej;
- kryteria przekrojowe – dotyczą parametrów odnoszących się do skutków zniszczenia lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji bądź usługi. Kryteria te obejmują: ofiary w ludziach, skutki finansowe, konieczność ewakuacji, utratę usługi, czas odbudowy, efekt międzynarodowy oraz unikatowość.

Końcowa identyfikacja przynależności do infrastruktury krytycznej odbywa się w trzech etapach [4]:

- pierwsza selekcja polega na zastosowaniu kryteriów systemowych właściwych dla danego systemu infrastruktury krytycznej w odniesieniu do obiektów, urządzeń, instalacji lub usług;
- drugi etap, to sprawdzenie czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa (regionu), aglomeracji miejskiej i obywateli oraz czy zapewnia sprawne funkcjonowanie organów administracji publicznej i podmiotów gospodarczych;
- trzeci etap ma na celu ocenę potencjalnych skutków zaprzestania funkcjonowania infrastruktury krytycznej lub jej zniszczenia. Wyłonione w pierwszych dwóch etapach elementy infrastruktury krytycznej aby być rozpatrywane w trzecim etapie muszą spełniać co najmniej dwa kryteria przekrojowe.

Można pokusić się o określenie własnych przemyśleń związanych z wystąpieniem określonych zagrożeń:

- w odniesieniu do ludności:
  - liczba zajść śmiertelnych;
  - liczba osób hospitalizowanych;
  - liczba osób objętych powodzią;
  - liczba osób objętych suszą;
  - liczba osób ewakuowanych;

  - liczba osób, która utraciła podstawowe usługi;
- w odniesieniu do gospodarki:
  - koszty strat wystąpienia danego scenariusza zdarzeń;
  - zakłócenia na poziomie regionalnym, krajowym lub globalnym;
- w odniesieniu do środowiska:
  - długotrwałe zakłócenia;
  - nieodwracalne zmiany;
- w odniesieniu do stabilności państwa:
  - trudności w wypełnianiu konstytucyjnych obowiązków państwa.

Wymienione zagrożenia należy rozpatrywać w aspekcie scenariuszy bezpośrednich, uwzględniających efekt domina oraz rozłożonych w perspektywie długoterminowej [8].

System zarządzania bezpieczeństwem to organizacje i działanie przyjęte przez zarządcę infrastruktury wodociągowej dla zapewnienia bezpieczeństwa.

Wspólne wymagania bezpieczeństwa (CST), to minimalne poziomy bezpieczeństwa, które powinny być osiągane przez SZZW wyrażone w kryteriach akceptacji ryzyka.

Wspólne metody oceny bezpieczeństwa (CSM), to metody oceny bezpieczeństwa ustalone, opisujące sposoby oceny poziomu bezpieczeństwa i spełniania wymagań bezpieczeństwa.

Wspólne wskaźniki bezpieczeństwa (CSI), to estymatory statystyczne odnoszące się do zdarzeń niepożądanych, ich skutków i bezpieczeństwa infrastruktury technicznej, a także zarządzania bezpieczeństwem.

Bezpieczeństwo czynne (aktywne) związane jest z cechami systemu, dzięki którym zmniejsza się ryzyko wystąpienia zdarzenia niepożądanego. Bezpieczeństwo bierne (pasywne) to pojęcie gdy już do zdarzenia niepożądanego dojdzie. To zespół cech, których celem jest maksymalne zmniejszenie skutków zaistniałego zdarzenia niepożądanego.

6. Strategia zrównoważonego wodociągu

Kreowanie polityki zaopatrzenia w wodę wymaga opracowania strategii. Autorska koncepcja składa się z 9 etapów:

A. Identyfikacja

W pierwszym kroku należy zidentyfikować zjawiska, procesy i zasoby istotne dla funkcjonowania SZZW [7]. Identyfikacja polega na stopniowej dekompozycji związanej z obiektami rozważań, określenie domen rozważań, a kończy szczegółową identyfikacją. Dane statystyki historyczne o wybranych zjawiskach mogą posłużyć do przeprowadzenia analizy trendu. W ten sposób uzyska się bazę do opracowania stanów aktualnych i określenia przyczyn stanów zawodnościowych i związanych z utratą bezpieczeństwa odbiorców wody. Ostatnim kro-

kiem tego etapu jest zastosowanie hierarchiczne zjawisk, zasobów i procesów, z podziałem na konstruktywne i destruktywne [1].

B. Prognoza

Przeprowadzenie prognoz procesów o istotnym wpływie na efektywność w sferze eksploatacji i inwestycji związanych z funkcjonowaniem SZZW.

C. Diagnoza strategiczna

Ma na celu osiągnięcie sukcesu długofalowego w samym SZZW z uwzględnieniem procesów zachodzących w jego otoczeniu a związanych z działaniami sił konkurencyjnych.

D. Opracowanie scenariuszy

Mają na celu określenie skutków w myśl zasady „co będzie, jeżeli …?". Tutaj należy wykorzystać dane z prognozy procesów.

E. Ocena efektywności i ryzyka

Dotyczy konkretnych i destrukcyjnych skutków dal wytypowanych scenariuszy.

F. Wybór wariantów

Dla strategii zrównoważonego rozwoju SZZW wybór wariantów inwestycyjnych i możliwości ich finansowania.

G. Założenia techniczne, organizacyjne i finansowe

Dla wybranych wariantów.

H. Projekty działań

Dotyczą działań operacyjnych wraz ze szczegółową analizą kosztów, korzyści i ryzyka, wraz z analizą krótko i długo terminową efektów ekonomicznych

I.Wybór końcowy

Prezentacja wariantów strategii przed gremium decyzyjnym wraz z wyborem i akceptacją projektu strategii w postaci raportu końcowego.

7. Podsumowanie

- Badania konsumenckie postrzegania natury ryzyka w dalszym ciągu nie rozstrzygają czy obowiązuje model multiplikatywny (czynniki pomnożone) czy model addytywny (czynniki dodawane), czy konsekwencje (straty) i prawdopodobieństwo (częstość) ich wystąpienia są ze sobą powiązane, czy są to komponenty niezależne od siebie. Wątpliwe jest także, który komponent jest ważniejszy dla konsumenta, czy oba są tak samo ważne?
- Bezpieczeństwo i ochrona systemu są ściśle związane z różnego rodzaju zagrożeniami, które w sposób dynamiczny ewoluują. To z kolei powoduje konieczność antycypacji i kreowania nowych metod przeciwdziałania tego rodzaju zagrożeniom. Analizując zagrożenia należy rozpatrywać alternatywne sposoby ochrony, a scenariusze powinny obejmować także zagrożenia terrorystyczne, a nawet militarne, Przynależność do infrastruktury krytycznej powin-

na wiązać się z pewnego rodzaju „przywilejami". Mogło by to polegać na szybkich ścieżkach otrzymywania odszkodowań za straty poniesione w sytuacjach awaryjnych, czy możliwości tworzenia zachęt do utrzymywania zwiększonych własnych zasobów finansowych służących do odtwarzania infrastruktury krytycznej albo uzyskania wsparcia ekip remontowych z innych sektorów gospodarki, a nawet wojska.

- Metody dedukcyjne analizy ryzyka polegają na założeniu określenia zdarzenia końcowego, a szukane są zdarzenia mogące doprowadzić do zdarzenia końcowego. Metody indukcyjne analizy ryzyka polegają na założeniu danego rodzaju awarii, a analizuje się i identyfikuje zdarzenia, które mogą być spowodowane tą awarią.
- Ryzyko może dotyczyć zdarzeń utraty zdrowia lub życia ludzi, w stratach finansowych związanych z brakiem produkcji wody, stratach związanych z brakiem możliwości użytkowania wody, w stratach w obszarze zasobów wody.

Literatura

[1] Damodaran A.; Ryzyko strategiczne. Podstawy zarządzania ryzykiem, Wyd. Akademickie i Profesjonalne, Warszawa 2009.
[2] Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 roku w sprawie rozpoznania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dz.U.UE.L.08.345.75.
[3] Kopaliński W.; Słownik wyrazów obcych i zwrotów obcojęzycznych, Wyd. Wiedza Powszechna, Warszawa 1983.
[4] Narodowy Program Ochrony Infrastruktury Krytycznej, Wydawnictwo Rządowego Centrum Bezpieczeństwa, Warszawa 2013.
[5] Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1, Charakterystyka systemów infrastruktury krytycznej, Wydawnictwo Rządowego Centrum Bezpieczeństwa, Warszawa 2013.
[6] Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 2, Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Wydawnictwo Rządowego Centrum Bezpieczeństwa, Warszawa 2013.
[7] Rak R.J.; Problematyka ryzyka w wodociągach, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2014.
[8] Ustawa z dnia 18 kwietnia 2002 roku o stanie klęski żywiołowej. Dz.U. z 2002 r. nr 62, poz. 558 ze zm.
[9] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym. Dz.U. z 2007 r., nr 89, poz. 590 ze zm.
[10] Wieczorek-Kosmala M.; Nietradycyjne instrumenty finansowania ryzyka w przedsiębiorstwie. Ekonomia, finanse. Współczesne wyzwania i kierunki rozwoju, Wyd. Uniwersytetu Ekonomicznego w Katowicach, Katowice 2010.

RULES FOR DETERMINING THE BELONGING TO CRITICAL INFRASTRUCTURE

S u m m a r y

Safety and security systems are closely related to various types of threats that are evolving in a dynamic way. This in turn makes it necessary to anticipate and create new methods to counter such threats. In the article the methodology for determining the belonging to the critical infrastructure was analyzed. The list of sectors is determined by the regulation of crisis management. Two failures of critical infrastructure were briefly discussed. Qualification criteria for critical infrastructure were given. New ways of financing catastrophe risk were proposed. Reference was made to the elements of critical infrastructure protection. On the example of the collective water supply system, identification criteria was presented in detail. A summary of the scientific consideration is to identify strategies for sustainable water supply system.

Keywords: critical infrastructure of the water supply system, threats, protection

Przesłano do redakcji: 10.03.2016 r.
Przyjęto do druku: 1.06.2016 r.

DOI: 10.7862/rb.2016.130