INSTYTUT POLITYKI ENERGETYCZNEJ IM. IGNACEGO ŁUKASIEWICZA

ANALIZA NR 5/2022

PLAN OCHRONY DLA INFRASTRUKTURY ENERGETYCZNEJ W ASPEKCIE ROZWOJU MORSKIEJ ENERGETYKI WIATROWEJ NA OBSZARACH MORSKICH RP

Tomasz CHYŁA[1]

[1] kmdr ppor. mgr inż. Tomasz CHYŁA, starszy wykładowca na Wydziale Dowodzenia i Operacji Morskich w Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni, ekspert Instytutu Polityki Energetycznej im. Ignacego Łukasiewicza w Rzeszowie.

MOŻLIWE ZAGROŻENIA DLA MORSKICH FARM WIATROWYCH

Mając na uwadze wydarzenia, które miały miejsce we wrześniu br. na Morzu Bałtyckim (w niewielkiej odległości od polskiej wyłącznej strefy ekonomicznej), tj. potwierdzony fakt sabotażu gazociągów Nord Stream oraz ostatnie wyliczenia PSEW zawarte w raporcie „Potencjał Morskiej Energetyki Wiatrowej w Polsce" mówiące o tym, że poprzez wykorzystanie całkowitego, szacowanego potencjału polskiej części Bałtyku, do 2040 r. morska energetyka wiatrowa mogłaby zaspokajać nawet 57% całkowitego zapotrzebowania na energię elektryczną w Polsce, można z powodzeniem uznać, że bezpieczeństwo energetyczne naszego kraju w dużym stopniu oparte będzie o instalacje OZE na morzu, które będą podatne na różne zagrożenia, oraz póki co niemal całkowicie niezabezpieczone. W celu sprostania rosnącym wyzwaniom i zagrożeniom, w trudnej do monitorowania i sprawowania skutecznej ochrony domenie morskiej (zarówno toń wodna jak i jej dolna półsfera), należy uświadomić sobie skalę możliwych zagrożeń i przygotować adekwatną strategię reakcji. Brak oficjalnego zdefiniowania „wind - offshoru" na polskich obszarach morskich, nie jest przyczynkiem do tego, aby zaniechać przygotowanie kontrreakcji na możliwe ryzyka w trakcie ponad 30 letniej eksploatacji (faza budowy, eksploatacji i likwidacji). Ochrona tej infrastruktury, w związku z jej strategicznym znaczeniem dla polskiej energetyki, a co za tym idzie polskiej gospodarki i jej konkurencyjności, powinna być rozpatrywana przez pryzmat polskiej legislacji oraz wytycznych Rządowego Centrum Bezpieczeństwa.

ZARZĄDZANIE KRYZYSOWE A WIND-OFFSHORE

W Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (ZK) ochrona infrastruktury krytycznej definiowana jest jako wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Zgodnie z zapisem Art. 5. 1. tejże ustawy tworzy się Krajowy Plan Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego, zwane dalej „planami zarządzania kryzysowego" w skład, którego wchodzą min.: załączniki funkcjonalne planu głównego określające procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym związane z ochroną infrastruktury krytycznej.

Z kolei Art. 5b. 1. Wskazuje na przyjęcie (w drodze uchwały Rady Ministrów), Narodowego Programu Ochrony Infrastruktury Krytycznej, którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w szczególności w zakresie:

1) zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej,
2) przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
3) reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
4) odtwarzania infrastruktury krytycznej.

Art. 6. 1. Konkretyzuje zadania z zakresu ochrony infrastruktury krytycznej, które obejmują:

1) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej,

2) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej,
3) odtwarzanie infrastruktury krytycznej,
4) współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

Ponadto właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia.

PLAN OCHRONY - WYMAGANIA

Aktem wykonawczym przytoczonej ustawy to Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej. W jego zapisach sprecyzowano sposób tworzenia, aktualizacji oraz strukturę planów ochrony infrastruktury krytycznej opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, zwanych dalej „operatorami infrastruktury krytycznej", oraz warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

W rozporządzeniu określono min. elementy, które powinny znaleźć się w planie, i są to w kolejności:

1) Dane ogólne obejmujące między innymi: nazwę i lokalizację infrastruktury krytycznej, jej operatora i podmiot zarządzający przedsiębiorstwem w imieniu operatora, dane osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej oraz osoby sporządzającej plan.
2) Dane infrastruktury krytycznej obejmujące między innymi: charakterystykę i podstawowe parametry techniczne, plan (mapę) z naniesieniem lokalizacji obiektów, instalacji lub systemu oraz funkcjonalne połączenia z innymi obiektami, instalacjami, urządzeniami lub usługami.
3) Charakterystyka między innymi: zagrożeń dla infrastruktury krytycznej 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 oraz zasobów właściwych terytorialnie organów, możliwych do wykorzystania w celu ochrony infrastruktury krytycznej.
4) Zasadnicze warianty między innymi: działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, zapewnienia ciągłości funkcjonowania infrastruktury krytycznej oraz odtwarzania tejże.
5) zasady współpracy z właściwymi miejscowo: centrami zarządzania kryzysowego, oraz organami administracji publicznej.

Zgodnie z Ustawą o ZK Dyrektor Rządowego Centrum Bezpieczeństwa: sporządza na podstawie szczegółowych kryteriów, o których mowa w ust. 2 pkt 3, we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. W wykazie wyróżnia się także europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską. Wykaz ma charakter niejawny. Ustawowy obowiązek ma odzwierciedlenie w Załączniku nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej (tekst z 2020 roku, klauzula „ZASTRZEŻONY" – „Załącznik nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej – Kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej – tekst jednolity". Operator infrastruktury krytycznej sporządza plan w terminie 9 miesięcy od daty otrzymania od dyrektora Rządowego Centrum Bezpieczeństwa informacji o umieszczeniu inwestycji w wykazie powyższych obiektów.

Plan wg. rozporządzenia uzgadniany jest z (w zakresie ich dotyczącym z właściwymi terytorialnie):

1) wojewodą,
2) komendantem wojewódzkim Państwowej Straży Pożarnej,
3) komendantem wojewódzkim Policji,
4) dyrektorem regionalnego zarządu gospodarki wodnej,
5) wojewódzkim inspektorem nadzoru budowlanego,
6) wojewódzkim lekarzem weterynarii,
7) państwowym wojewódzkim inspektorem sanitarnym,
8) dyrektorem urzędu morskiego,
9) oraz z Ministrem Klimatu i Środowiska.

Uzgodnienie następuje przez podpisanie arkusza uzgodnień z powyższymi w terminie 14 dni od daty otrzymania przez niego planu (prócz Ministra KiS, który podpisuje arkusz w terminie 45 dni od daty przedłożenia planu).Operatorowi IK może zostać odmówione uzgodnienie planu zarówno w całości jak i w części, może to nastąpić w przypadku: przedstawienia rozwiązań niegwarantujących bezpieczeństwa infrastruktury krytycznej czy też braku spójności z Narodowym Programem Ochrony Infrastruktury Krytycznej Dyrektor Centrum, po rozpatrzeniu ewentualnych rozbieżności (operator infrastruktury krytycznej przedkłada plan wraz z protokołem rozbieżności do zatwierdzenia dyrektorowi Centrum w terminie 14 dni od daty zakończenia uzgodnień ze wszystkimi podmiotami), zatwierdza plan w terminie 90 dni od daty przedłożenia. Należy również zauważyć, iż plany należy aktualizować w zależności od potrzeb jednak nie rzadziej niż raz na dwa lata.

ZARZĄDZANIE RYZYKIEM

Kolejnym kluczowym aspektem (choćby w aspekcie cyberataków na sektor energetyczny Ukrainy czy operatora elektrowni wiatrowych w Niemczech), jest zapewnienie bezpieczeństwa teleinformatycznego. Art. 6.1.5 b Ustawy o ZK, dotyczy operatorów IK (właścicieli, posiadaczom samoistnym i zależnym), będących jednocześnie operatorami usług kluczowych (Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa określa z operatorów

usług kluczowych, jako firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Takimi operatorami są między innymi przedstawiciele sektora energetycznego). Artykuł ten nakazuje uwzględnienie w planach ochrony infrastruktury krytycznej dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych.

Najbardziej kluczowe dla operatorów w najbliższej perspektywie jest świadome wybranie doświadczonego podmiotu do realizacji tego kluczowego zadania, wypracowanie procedur, zdefiniowanie zestawu możliwych zagrożeń dla infrastruktury krytycznej oraz oceny ryzyka ich wystąpienia wraz z przewidywanymi scenariuszami rozwoju zdarzeń oraz implementacja adekwatnego zabezpieczenie technicznego obiektów.

Wskazówki, jak należycie realizować ochronę IK znaleźć można w opublikowanym przez Rządowe Centrum Bezpieczeństwa w 2020 roku „Narodowym Programie Ochrony Infrastruktury Krytycznej. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje".

Dokument ten zawiera podstawowe informacje na temat technicznych i organizacyjnych aspektów ochrony infrastruktury krytycznej. Może on zostać użyty jako zestaw konkretnych wskazówek dotyczących budowy i funkcjonowania systemu ochrony IK. Dodatkowo w dokumencie tym można znaleźć ocenę skuteczności poszczególnych metod zapewnienia bezpieczeństwa, jak również propozycję strategii implementacji, która zapewni, że będzie ona najbardziej efektywna.

Kluczowym jest traktowanie kwestii ochrony infrastruktury krytycznej jako zagadnienia interdyscyplinarnego. Bez względu na to, jakie rodzaje ochrony zostaną wybrane i wprowadzone w życie w organizacji, cztery elementy mają znaczenie we wdrożeniu wszystkich ich rodzajów:

1) prowadzenie działań edukacyjnych,
2) właściwa struktura organizacyjna pionu zarządzania bezpieczeństwem,
3) wybór strategii wdrożenia,
4) weryfikacja przyjętych rozwiązań i ich aktualizacja.

Jedną z prymarnych zasad zawartych w powyższym dokumencie jest zasada 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. Z punktu widzenia Programu jest to element kluczowy, determinujący i uzasadniający działania podejmowane w celu obniżenia ryzyka zakłócenia funkcjonowania IK.

Ocena ryzyka powinna być podstawą określenia standardów ochrony IK i ustalenia priorytetów działań. Przed rozpoczęciem jakichkolwiek analiz związanych z ryzykiem (wpływem niepewności na cel) należy wziąć pod uwagę dwa zagadnienia. Po pierwsze należy pamiętać, że szacowanie ryzyka jest pojęciem kompleksowym. Zgodnie z normą PN-ISO 31000 na szacowanie ryzyka składają się:

1) identyfikacja zagrożeń,
2) analiza ryzyka,
3) ewaluacja ryzyka.

Rekomendowanym sposobem przeprowadzania identyfikacji zagrożeń, analizy i szacowania ryzyka jest realizacja następujących kroków:

1) identyfikacja procesów zachodzących w organizacji,
2) określenie skutków – identyfikacja procesów krytycznych,
3) wskazanie zasobów,
4) identyfikacja zagrożeń i podatności,
5) przeanalizowanie ryzyka,
6) ewaluacja ryzyka.

WNIOSKI

Reasumując, kwestie zapewnienia bezpieczeństwa w dobie rosnącego znaczenia energii elektrycznej i zwiększonej aktywności podmiotów związanych z Federacją Rosyjską, mającej na celu swoimi działaniami destabilizowanie stabilnych dostaw strumieni energii i zarządzanie strachem, w powiązaniu ze znacznym oddaleniem Morskich Farm Wiatrowych od portów, z których mogą operować zdolne i prawnie uprawnione do interwencji służby, są niezwykle istotne. Planowana od 2025 roku produkcja prądu „z morza", powinna być poprzedzona staranną analizą zagrożeń i zabezpieczeń dla tej kluczowej dla bezpieczeństwa energetycznego kraju i dla dekarbonizacji polskiej energetyki, gałęzi wytwórczej. Analizy powinny być realizowane w perspektywie kilkudziesięciu najbliższych lat, a procedury konfrontowane z mnogością zagrożeń występujących na morzu. Szacowanie ryzyka powinno odbywać się przy udziale specjalistów z domeny fizycznej i cybernetycznej obrony obiektów, jak również z ekspertami bezpośrednio znającymi specyfikę działań na morzu,