Witold Mazurek
Uniwersytet Ignatianum w Krakowie
https://orcid.org/0000-0002-9440-7324

Wyzwania i problemy stojące przed systemem ochrony infrastruktury krytycznej w kontekście planowanej rozbudowy sektora energetyki jądrowej w Polsce

Streszczenie

Infrastruktura krytyczna stanowi fundament funkcjonowania współczesnych państw, a jej odporność przesądza o stabilności politycznej, gospodarczej i społecznej. Szczególne miejsce wśród sektorów infrastruktury krytycznej zajmuje energetyka, w tym planowane w Polsce elektrownie jądrowe. Celem artykułu jest identyfikacja kluczowych wyzwań w ochronie infrastruktury krytycznej w Polsce z perspektywy budowy elektrowni jądrowych oraz ocena adekwatności obecnych rozwiązań systemowych. W pierwszej części przedstawiono ewolucję pojęcia infrastruktury krytycznej oraz jej miejsce w krajowych i unijnych regulacjach prawnych. Następnie przeanalizowano główne kategorie zagrożeń – naturalne, technologiczne, terrorystyczne, cybernetyczne i hybrydowe – ze szczególnym uwzględnieniem ich wpływu na sektor energetyczny. W dalszej części omówiono specyfikę bezpieczeństwa obiektów jądrowych oraz zaprezentowano postulaty w zakresie wzmocnienia systemu ochrony, w tym powołania wyspecjalizowanej służby odpowiedzialnej za ochronę infrastruktury krytycznej. Artykuł kończą rekomendacje dotyczące budowy zintegrowanego modelu bezpieczeństwa elektrowni jądrowych w Polsce.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo jądrowe, elektrownia jądrowa, cyberbezpieczeństwo, zagrożenia hybrydowe

New challenges in critical infrastructure protection: the perspective of planned nuclear power plants in Poland

Abstract

Critical infrastructure constitutes the backbone of modern states, and its resilience determines political, economic and social stability. The energy sector, including planned nuclear power plants in Poland, has a special place among critical infrastructure sectors. The aim of the article is to identify key challenges in critical infrastructure protection in Poland from the perspective of the construction of nuclear power plants and to assess the adequacy of the current systemic solutions. The first part presents the evolution of the concept of critical infrastructure and its place in national and EU legal regulations. The paper then analyses the main categories of threats – natural, technological, terrorist, cyber and hybrid – with particular emphasis on their impact on the energy sector. The next part discusses the specific nature of nuclear facilities' security and presents proposals for strengthening the protection system, including the establishment of a specialised service responsible for critical infrastructure protection. The article concludes with recommendations for building an integrated model of nuclear power plants' security in Poland.

Keywords: critical infrastructure, nuclear security, nuclear power plant, cybersecurity, hybrid threats

Wprowadzenie

Infrastruktura krytyczna jest jednym z centralnych pojęć współczesnych studiów nad bezpieczeństwem narodowym. Obejmuje ona systemy, obiekty i usługi, których zakłócenie lub zniszczenie prowadziłoby do poważnych konsekwencji dla funkcjonowania państwa i jakości życia obywateli[1]. W warunkach narastającej złożoności środowiska bezpieczeństwa – na które składają się zmiany klimatyczne, postępująca cyfryzacja, rywalizacja mocarstw i rozwój zagrożeń hybrydowych – ochrona infrastruktury krytycznej staje się jednym z kluczowych zadań państwa.

Szczególne znaczenie ma sektor energetyczny, zapewniający funkcjonowanie wszystkich pozostałych sektorów infrastruktury krytycznej. W tym kontekście elektrownie jądrowe są postrzegane jako obiekty o strategicznej wadze: z jednej strony oferują stabilne i niskoemisyjne źródło energii, z drugiej – koncentrują w sobie ryzyka o potencjalnie katastrofalnych konsekwencjach[2]. Dla Polski, która znajduje się na etapie przygotowań do budowy pierwszych bloków jądrowych, zagadnienie bezpieczeństwa tych obiektów ma wymiar nie tylko techniczny, ale przede wszystkim systemowy i strategiczny.

Celem artykułu jest analiza wyzwań stojących przed systemem ochrony infrastruktury krytycznej w Polsce w perspektywie planowanych elektrowni jądrowych. Postawiono następujące pytania badawcze:

1. Jak kształtowały się pojęcie i regulacje infrastruktury krytycznej w Polsce i UE?
2. Jakie są główne kategorie zagrożeń dla infrastruktury krytycznej, w szczególności dla energetyki jądrowej?
3. Na ile obecny model ochrony infrastruktury krytycznej w Polsce jest adekwatny do wyzwań związanych z budową i eksploatacją elektrowni jądrowych?
4. Jakie zmiany instytucjonalne i organizacyjne są pożądane, aby zwiększyć odporność systemu?

Struktura artykułu obejmuje część teoretyczno-prawną, charakterystykę zagrożeń, analizę specyfiki bezpieczeństwa jądrowego oraz postulaty dotyczące modelu ochrony elektrowni jądrowych w Polsce.

1. Infrastruktura krytyczna – ewolucja pojęcia i ujęcie systemowe

1.1. Definicje i podstawowe cechy

W polskim porządku prawnym pojęcie infrastruktury krytycznej zostało zdefiniowane w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3]. Zgodnie z art. 3 pkt 2, infrastrukturę krytyczną stanowią systemy oraz wchodzące w ich skład obiekty, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej i podmiotów gospodarczych. Kluczowy jest tu akcent na systemowość i funkcjonalne powiązania – infrastruktura krytyczna

nie jest prostą sumą pojedynczych obiektów, lecz złożoną siecią elementów wzajemnie się warunkujących.

W literaturze podkreśla się dualny charakter infrastruktury krytycznej: obejmuje ona zarówno infrastrukturę materialną (hardware), jak sieci energetyczne, wodociągi, gazociągi, obiekty transportowe, jak i infrastrukturę niematerialną (software) – systemy teleinformatyczne, procedury zarządzania, wiedzę ekspercką oraz kulturę organizacyjną[4]. Z tej perspektywy infrastruktura krytyczna pełni funkcję „kręgosłupa" państwa – jej odporność decyduje o zdolności systemu polityczno-gospodarczego do przetrwania w sytuacjach kryzysowych.

Do podstawowych cech infrastruktury krytycznej zalicza się:
– **systemowość** – silne powiązania między sektorami, generujące efekt kaskadowy;
– **strategiczność** – kluczowe znaczenie dla ciągłości funkcjonowania państwa;
– **wrażliwość na zagrożenia** – zarówno naturalne, jak i antropogeniczne;
– **interdyscyplinarność ochrony** – konieczność współdziałania administracji, służb, sektora prywatnego i nauki;
– **dynamiczność** – zmienność katalogu sektorów i priorytetów wraz z rozwojem technologii i zagrożeń[5].

1.2. Infrastruktura krytyczna w regulacjach Unii Europejskiej

Na poziomie Unii Europejskiej pojęcie infrastruktury krytycznej zyskało znaczenie wraz z przyjęciem dyrektywy 2008/114/WE dotyczącej identyfikacji i wyznaczania europejskiej infrastruktury krytycznej[6]. Skoncentrowano się wówczas na sektorach energii i transportu, których zakłócenie mogłoby mieć ponadnarodowe skutki. Kolejnym krokiem była dyrektywa CER z 2022 r., odnosząca się do odporności podmiotów krytycznych, oraz dyrektywa NIS2, która rozszerzyła wymagania w zakresie cyberbezpieczeństwa.

Implementacja tych regulacji doprowadziła do dostosowania polskiego systemu prawnego, m.in. poprzez wprowadzenie pojęcia europejskiej infrastruktury krytycznej oraz aktualizację Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)[7]. Program ten nie tylko identyfikuje sektory IK, ale również definiuje zasady współpracy i podziału odpowiedzialności między państwem a operatorami.

2. Elektrownie jądrowe jako element infrastruktury krytycznej

2.1. Znaczenie dla bezpieczeństwa energetycznego

Elektrownie jądrowe są zaliczane do sektora energetycznego, który ma fundamentalne znaczenie dla funkcjonowania wszystkich pozostałych sektorów infrastruktury krytycznej. Z punktu widzenia bezpieczeństwa energetycznego wyróżnia je kilka cech:

1. **Stabilność dostaw** – w odróżnieniu od części źródeł odnawialnych, energia jądrowa nie jest bezpośrednio zależna od warunków pogodowych.
2. **Niskoemisyjność** – wytwarzanie energii elektrycznej w reaktorach jądrowych wiąże się z bardzo niską emisją CO_2, co czyni je ważnym narzędziem realizacji polityki klimatycznej[8].
3. **Redukcja zależności importowej** – rozwój energetyki jądrowej może ograniczać zależność od importu paliw kopalnych, co ma istotny wymiar geopolityczny.

Jednocześnie elektrownie jądrowe generują specyficzne ryzyka, związane m.in. z potencjalnymi awariami reaktora, skażeniem radiologicznym oraz możliwością wykorzystania materiałów jądrowych do celów przestępczych lub terrorystycznych[9].

2.2. Specyfika bezpieczeństwa jądrowego

Bezpieczeństwo jądrowe opiera się na zasadzie „obrony w głąb" (defence-in-depth), która zakłada tworzenie wielopoziomowych barier technicznych, organizacyjnych i proceduralnych, mających zapobiegać awariom i ograniczać ich skutki[10]. Obejmuje to:

– projektowanie reaktorów o wysokich parametrach bezpieczeństwa;
– redundantne systemy chłodzenia i zasilania;
– wzmocnione konstrukcje budynków reaktora;
– rozwinięte procedury reagowania awaryjnego;
– ścisły nadzór regulacyjny.

Doświadczenia Czarnobyla i Fukushimy pokazały, że kluczowe znaczenie mają nie tylko rozwiązania techniczne, lecz także kultura bezpieczeństwa, jakość regulacji i zdolność państwa do zarządzania kryzysem[11].

3. Kategorie zagrożeń dla infrastruktury krytycznej i elektrowni jądrowych

3.1. Zagrożenia naturalne i technologiczne

Infrastruktura krytyczna jest narażona na szerokie spektrum zagrożeń naturalnych: powodzie, huragany, ekstremalne temperatury, susze czy osuwiska[12]. W przypadku elektrowni jądrowych szczególnie istotne są:

– dostępność wody do chłodzenia,
– ryzyko powodzi i podtopień,
– ekstremalne zjawiska meteorologiczne (silny wiatr, burze, lód)[13].

Zagrożenia technologiczne obejmują awarie urządzeń, wady materiałowe, błędy projektowe oraz niewystarczającą modernizację. Niedoinwestowanie infrastruktury, opóźnienia w wymianie zużytych elementów oraz braki w konserwacji zwiększają podatność systemów na zakłócenia[14].

3.2. Terroryzm i sabotaż

Ze względu na potencjalnie katastrofalne skutki awarii, elektrownie jądrowe stanowią atrakcyjny cel dla terrorystów. Możliwe scenariusze obejmują zarówno ataki zewnętrzne (np. przy użyciu broni palnej, materiałów wybuchowych, bezzałogowych statków powietrznych), jak i działanie wewnętrzne (insider threat)[15].

Sabotaż wewnętrzny jest szczególnie groźny, ponieważ sprawca dysponuje wiedzą o procedurach i słabych punktach systemu[16]. Dlatego tak duży nacisk kładzie się na weryfikację personelu, systemy kontroli dostępu, podział obowiązków oraz rozwijanie kultury bezpieczeństwa jądrowego.

3.3. Cyberzagrożenia

Postępująca cyfryzacja systemów sterowania procesami (SCADA, ICS) przyniosła wzrost efektywności, lecz jednocześnie otworzyła nowy wektor zagrożeń. Przykłady udanych cyberataków na systemy energetyczne, w tym ataki na ukraińskie sieci elektroenergetyczne oraz incydent Colonial Pipeline, pokazują realność ryzyka paraliżu infrastruktury poprzez złośliwe oprogramowanie (w tym ransomware)[17].

W kontekście elektrowni jądrowych kluczowe jest fizyczne i logiczne separowanie systemów sterowania od sieci zewnętrznych, stosowanie dedykowanych rozwiązań bezpieczeństwa (IDS/IPS, monitorowanie integralności danych), ciągły audyt bezpieczeństwa oraz rozwój kompetencji personelu technicznego[18].

3.4. Zagrożenia hybrydowe

Zagrożenia hybrydowe łączą środki militarne i pozamilitarne: cyberataki, sabotaż, operacje informacyjne, szantaż energetyczny, wsparcie grup ekstremistycznych. Celem jest nie tylko fizyczne uszkodzenie infrastruktury, ale także podważenie zaufania społecznego do instytucji państwa, wywołanie chaosu i polaryzacji[19].

Połączenie cyberataku na systemy energetyczne z fizycznym sabotażem i kampanią dezinformacyjną wokół rzekomego zagrożenia radiologicznego mogłoby doprowadzić do masowej paniki, ucieczek ludności i poważnego kryzysu politycznego[20]. W tym sensie elektrownie jądrowe stają się nie tylko obiektem inżynieryjnym, ale także symbolem, wokół którego mogą być prowadzone operacje psychologiczne.

4. Polski system ochrony infrastruktury krytycznej w kontekście energetyki jądrowej

4.1. Ramy instytucjonalno-prawne

Polski system ochrony infrastruktury krytycznej opiera się na współpracy administracji publicznej (w tym Rządowego Centrum Bezpieczeństwa), operatorów poszczególnych sektorów oraz służb odpowiedzialnych za bezpieczeństwo wewnętrzne i obronę narodową[21]. Podstawę prawną stanowią m.in.:

– ustawa o zarządzaniu kryzysowym,
– akty sektorowe (Prawo energetyczne, Prawo atomowe, ustawy o transporcie, łączności),
– Narodowy Program Ochrony Infrastruktury Krytycznej,
– strategie bezpieczeństwa narodowego i cyberbezpieczeństwa.

Dotychczas model ten rozwijano w warunkach braku elektrowni jądrowych. Planowana budowa takich obiektów wymaga jednak wzmocnienia komponentu związanego z bezpieczeństwem jądrowym i radiologicznym, zarówno na poziomie regulacyjnym (rola Państwowej Agencji Atomistyki), jak i operacyjnym[22].

4.2. Ograniczenia obecnego modelu

W literaturze i raportach wskazuje się na kilka słabości obecnego systemu ochrony IK w Polsce[23]:

– rozproszenie kompetencji i brak jednego podmiotu odpowiedzialnego za całościową koordynację ochrony IK;
– zróżnicowany poziom dojrzałości systemów bezpieczeństwa między sektorami i

operatorami;
– ograniczone zasoby kadrowe i finansowe dedykowane ochronie IK;
– niewystarczające uwzględnienie scenariuszy hybrydowych i wielodomenowych.

W przypadku sektora energetyki jądrowej oznacza to ryzyko niedostosowania systemu do specyfiki zagrożeń radiologicznych i jądrowych oraz potencjalnych konsekwencji transgranicznych.

5. Koncepcja wyspecjalizowanej służby ochrony infrastruktury krytycznej

Jedną z propozycji pojawiających się w debacie jest powołanie wyspecjalizowanej służby ochrony infrastruktury krytycznej (SOIK), w ramach której funkcjonowałaby sprofilowana Służba Ochrony Elektrowni Atomowych (SOEA) [24].

Do kluczowych zadań takiej służby należałoby:

– planowanie i realizacja ochrony fizycznej obiektów IK,
– zapewnienie ciągłej ochrony cybernetycznej (we współpracy z CSIRT-ami sektorowymi),
– prowadzenie analiz zagrożeń i ocen ryzyka,
– koordynacja reagowania kryzysowego w obiektach IK,
– współpraca z policją, służbami specjalnymi i siłami zbrojnymi.

Model ten, inspirowany rozwiązaniami funkcjonującymi w wybranych państwach NATO, umożliwiałby kumulację specjalistycznych kompetencji oraz budowę jednolitych standardów bezpieczeństwa w skali krajowej[25].

6. Wnioski i rekomendacje

Analiza pokazuje, że:

1. Infrastruktura krytyczna, w tym sektor energetyki jądrowej, stanowi centralny element bezpieczeństwa narodowego i wymaga podejścia systemowego, uwzględniającego sprzężenia między sektorami.
2. Katalog zagrożeń dla infrastruktury krytycznej uległ znacznemu poszerzeniu – od klasycznych zagrożeń naturalnych i technicznych po cyberataki i złożone działania hybrydowe.

3. Planowana budowa elektrowni jądrowych w Polsce stanowi szansę na wzmocnienie bezpieczeństwa energetycznego, ale równocześnie wymaga głębokiej przebudowy systemu ochrony infrastruktury krytycznej.
4. Obecny model ochrony IK, oparty na rozproszonej odpowiedzialności, powinien zostać uzupełniony o wyspecjalizowane struktury dedykowane ochronie obiektów o szczególnym znaczeniu, zwłaszcza elektrowni jądrowych.
5. Kluczowe znaczenie ma inwestowanie nie tylko w technologie i infrastrukturę fizyczną, lecz także w kulturę bezpieczeństwa, szkolenia personelu, zdolności analityczne oraz współpracę międzynarodową.

Rekomenduje się w szczególności:

– stworzenie wyspecjalizowanej Służby Ochrony Infrastruktury Krytycznej;
– wzmocnienie roli organów odpowiedzialnych za bezpieczeństwo jądrowe i radiologiczne;
– rozwijanie scenariuszy ćwiczeń obejmujących jednoczesne wystąpienie zdarzeń fizycznych, cybernetycznych i informacyjnych;
– systematyczne korzystanie z dobrych praktyk MAEA, UE i NATO w zakresie bezpieczeństwa jądrowego i ochrony IK;
– włączenie zagadnień związanych z odpornością infrastruktury krytycznej do szerszej debaty publicznej nad bezpieczeństwem państwa.

Bibliografia

1. Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, AON, Warszawa 2011.
2. Jędrzejczyk K., *Bezpieczeństwo energetyczne państwa. Ujęcie teoretyczne i praktyczne*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Warszawa 2017.
3. Gryz J., Kitler W., *System reagowania kryzysowego*, Toruń 2007.
4. Cieślarczyk M., *Teoria i praktyka bezpieczeństwa narodowego w ujęciu systemowym*, AON, Warszawa 2011.
5. Mazurek W., *Brudny terroryzm. Zagrożenia terrorystyczne w energetyce jądrowej*, Wydawnictwo WAM, Kraków 2017.
6. Küfeoğlu S., Akgün A.T., *Cyber Resilience in Critical Infrastructure*, CRC Press, Boca Raton 2023.
7. Lannoy A., *Reliability of Nuclear Power Plants*, Wiley-ISTE, London 2022.
8. *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, Warszawa 2023.
9. *Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1 (Rev. 1)*, IAEA, Vienna 2016.
10. *Report Fukushima: Ten Years On*, OECD/NEA, Paris 2021.
11. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z późn. zm.).
12. *Konwencja o wczesnym powiadamianiu o awarii jądrowej*, Wiedeń, 26 września 1986 r., Dz.U. 1988, nr 31, poz. 216.
13. *Konwencja o pomocy w przypadku awarii jądrowej lub zagrożenia radiologicznego*, Wiedeń, 26 września 1986 r.
14. *NIK o bezpieczeństwie obiektów infrastruktury krytycznej*, Najwyższa Izba Kontroli, dostęp: 06.02.2025.
15. *IAEA Safety Standards*, Międzynarodowa Agencja Energii Atomowej, dostęp: 29.09.2025.
16. *Ransomware – jedno z najpoważniejszych zagrożeń w cyberprzestrzeni*, gov.pl, dostęp: 30.09.2025.
17. *Raport Cyberbezpieczeństwo w energetyce*, 2024, dostęp: 29.02.2024.