

WITOLD MAZUREK

**WYZWANIA W OCHRONIE
INFRASTRUKTURY KRYTYCZNEJ
PERSPEKTYWA ELEKTROWNI ATOMOWYCH
W POLSCE**

WYDAWNICTWO NAUKOWE
UNIwersytetu Ignatianum w Krakowie

KRAKÓW 2026

SPIS TREŚCI

WSTĘP	9
1. WPROWADZENIE DO PROBLEMATYKI OCHRONY I BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ ZE SZCZEGÓLNYM UWZGLĘDNIENIEM STRATEGICZNEGO ZNACZENIA ELEKTROWNI ATOMOWYCH	13
1.1. Pojęcie i charakterystyka infrastruktury krytycznej (IK)	14
1.2. Sektory IK w Polsce	16
1.3. Zagrożenia dla infrastruktury krytycznej	16
1.4. Elektrownie atomowe jako element Infrastruktury Krytycznej	18
1.5. Specyfika bezpieczeństwa elektrowni atomowych	19
1.6. Energetyka jądrowa w Polsce – kontekst rozwoju	21
1.7. Współpraca i regulacje prawne w ochronie infrastruktury krytycznej	22
1.8. Odporność infrastruktury krytycznej na zagrożenia asymetryczne i terroryzm	22
1.9. Energetyka jądrowa w Unii Europejskiej – kontekst międzynarodowy	23
2. WYZWANIA DLA OCHRONY INFRASTRUKTURY KRYTYCZNEJ	25
2.1. Ewolucja zagrożeń i wyzwań dla ochrony IK	25
2.2. Analiza obecnego systemu ochrony IK w Polsce w kontekście elektrowni atomowych	26
2.3. Wymagania specyficzne w zakresie ochrony elektrowni atomowych	27
2.4. Propozycje wdrożenia wyspecjalizowanych rozwiązań ochrony	29
2.4.1. Bezpieczeństwo fizyczne	29
2.4.2. Cyberbezpieczeństwo	29
2.5. Analiza ogólnych zagrożeń i ryzyk dla infrastruktury krytycznej w Polsce	31
2.5.1. Typologia zagrożeń (naturalne, technologiczne, terrorystyczne, cybernetyczne, hybrydowe) w kontekście różnych sektorów IK	32

2.5.1.1. Zagrożenia naturalne	32
2.5.1.2. Zagrożenia technologiczne (awaryjne)	33
2.5.1.3. Błąd ludzki i zaniedbania	34
2.5.1.4. Zagrożenia terrorystyczne	35
2.5.1.5. Zagrożenia cybernetyczne	37
2.5.1.6. Zagrożenia hybrydowe	40
2.6. Uzasadnienie potrzeby utworzenia Służby Ochrony Infrastruktury Krytycznej w Polsce, w tym sprofilowanej Służby Ochrony Elektrowni Atomowych (SOEA)	44
2.6.1. Uwarunkowania systemowe	44
2.6.2. Argumenty za powołaniem Służby	46
2.6.3. Zintegrowane podejście do ochrony	50
2.6.4. Wzmocnienie cyberbezpieczeństwa	50
2.6.5. Struktura i zadania Służby	51
2.6.6. Integracja wyspecjalizowanych rozwiązań i dedy- kowanej Służby w kompleksowy system ochrony	53
2.6.7. Monitorowanie i ocena efektywności	54
2.6.8. Podsumowanie i wnioski	54
3. TEORETYCZNE I PRAWNE ASPEKTY INFRASTRUKTURY KRY- TYCZNEJ	57
3.1. Infrastruktura krytyczna: ewolucja pojęcia i prawne ramy definicyjne	59
3.2. Klasyfikacje infrastruktury krytycznej: sektory i wzajem- ne zależności	62
3.3. Elektrownie atomowe: filary energetyczne	65
4. ZNACZENIE INFRASTRUKTURY KRYTYCZNEJ DLA PAŃSTWA I SPOŁECZEŃSTWA. STRATEGICZNY WPŁYW ELEKTROWNI ATOMOWYCH NA BEZPIECZEŃSTWO ENERGETYCZNE	69
4.1. Infrastruktura krytyczna jako filar stabilności państwa i rozwoju społecznego	69
4.2. Strategiczny wpływ elektrowni atomowych na bezpie- czeństwo energetyczne państwa	70
4.3. Wzajemne zależności sektorów infrastruktury krytycz- nej i wyzwania odporności systemowej	72
4.4. Ekonomiczne i społeczne implikacje zakłóceń w infra- strukturze krytycznej	74
4.5. Adaptacja infrastruktury krytycznej do zmian klimatycz- nych i wpływ na odporność elektrowni atomowych	75
4.6. Rola współpracy międzynarodowej w ochronie infra- struktury krytycznej i bezpieczeństwa jądrowego	76
4.7. Innowacyjne technologie i przyszłe trendy w ochronie infrastruktury krytycznej	78

5. PODSTAWY PRAWNE OCHRONY INFRASTRUKTURY KRYTYCZNEJ W POLSCE I MIĘDZYNARODOWE REGULACJE DOTYCZĄCE BEZPIECZEŃSTWA JĄDROWEGO	81
5.1. Krajowe podstawy prawne ochrony infrastruktury krytycznej w Polsce	81
5.2. Międzynarodowe regulacje dotyczące bezpieczeństwa jądrowego	86
5.3. Wnioski i postulaty dla polskiego systemu prawnego w perspektywie przyszłości	89
6. MIĘDZYNARODOWE STANDARDY I DOBRE PRAKTYKI W ZAKRESIE OCHRONY INFRASTRUKTURY KRYTYCZNEJ I BEZPIECZEŃSTWA JĄDROWEGO	93
6.1. Rola organizacji międzynarodowych w kształtowaniu standardów bezpieczeństwa	93
6.2. Międzynarodowe konwencje i traktaty dotyczące bezpieczeństwa jądrowego	97
6.3. Zarządzanie starzeniem się obiektów jądrowych	98
6.4. Postulaty dla Polski w kontekście międzynarodowych standardów	99
7. CHARAKTERYSTYKA SPECYFICZNYCH ZAGROŻEŃ DLA WYBRANYCH SEKTORÓW INFRASTRUKTURY KRYTYCZNEJ	101
7.1. Sektor energetyczny (poza energetyką jądrową)	102
7.2. Sektor transportu	104
7.3. Sektor teleinformatyczny (ICT)	107
7.4. Sektor wodny i kanalizacyjny	110
7.5. Sektor zdrowia	112
8. OCENA OGÓLNEJ PODATNOŚCI INFRASTRUKTURY KRYTYCZNEJ NA ZAGROŻENIA	117
8.1. Charakterystyka podatności infrastruktury krytycznej na zagrożenia	118
8.2. Rodzaje zagrożeń dla infrastruktury krytycznej	119
8.3. Metody oceny podatności elektrowni atomowych na zagrożenia i zarządzanie ryzykiem	121
8.4. Zalecenia i postulaty w zakresie zmniejszania podatności na zagrożenia	124
9. WYBRANE STUDIA PRZYPADKÓW INCYDENTÓW ZWIĄZANYCH Z INFRASTRUKTURĄ KRYTYCZNĄ (INNE NIŻ INCYDENTY JĄDROWE)	127
9.1. Incydenty cybernetyczne – nowa domena zagrożeń	127
9.2. Awarie techniczne i błędy ludzkie – czynnik ludzki i sprzętowy	128
9.2. Incydenty naturalne i środowiskowe – siła przyrody	129

10. WIELOPOZIOMOWY SYSTEM OCHRONY FIZYCZNEJ ELEKTROWNIAW ATOMOWYCH W POLSCE: ZABEZPIECZENIA PERYMETRYCZNE, SYSTEMY KONTROLI DOSTĘPU, MONITORING, OCHRONA WEWNĘTRZNA	133
10.1. Zabezpieczenia perymetryczne: pierwsza linia obrony	133
10.2. Systemy kontroli dostępu: zarządzanie przepływem ludzi i materiałów	136
10.3. Monitoring	137
10.4. Ochrona wewnętrzna i siły reakcji: ostatnia linia obrony	139
10.5. Postulaty nowych rozwiązań i przyszłe wyzwania	143
10.6. Wnioski	144
11. TECHNICZNE I PROCEDURALNE ASPEKTY BEZPIECZEŃSTWA JĄDROWEGO I OCHRONY FIZYCZNEJ OBIEKTÓW JĄDROWYCH	147
11.1. Bezpieczeństwo jądrowe: wielobarierowe podejście inżynierskie i organizacyjne	147
11.2. Proceduralne aspekty bezpieczeństwa jądrowego: ludzki wymiar obrony	149
11.3. Ochrona fizyczna obiektów jądrowych: prewencja, detekcja, reakcja	151
11.4. Integracja bezpieczeństwa jądrowego i ochrony fizycznej: holistyczne podejście do ryzyka	154
12. POTENCJALNE WYZWANIA W SYSTEMIE OCHRONY ELEKTROWNIAW ATOMOWYCH W POLSCE	157
12.1. Ewolucja zagrożeń asymetrycznych i ich wpływ na ochronę fizyczną	157
12.2. Wyzwania w cyberbezpieczeństwie i ochronie systemów sterowania	159
12.3. Aspekty ludzkie i szkoleniowe	160
12.4. Wnioski	161
ZAKOŃCZENIE	163
BIBLIOGRAFIA	167
INDEKS OSÓB	175
SUMMARY	177

WSTĘP

Infrastruktura krytyczna stanowi fundament współczesnego państwa i społeczeństwa, zaś jej prawidłowe funkcjonowanie warunkuje stabilność systemu politycznego, gospodarczego i społecznego. W dobie rosnącej złożoności procesów globalnych, przyspieszającej cyfryzacji oraz nasilających się zagrożeń zarówno naturalnych, jak i antropogenicznych, kwestia ochrony i bezpieczeństwa infrastruktury krytycznej staje się jednym z kluczowych zagadnień badań nad bezpieczeństwem narodowym. W szczególnym stopniu dotyczy to sektora energetycznego, którego funkcjonowanie zapewnia nie tylko ciągłość dostaw energii elektrycznej, ale także umożliwia prawidłowe działanie pozostałych sektorów infrastruktury. W tym kontekście elektrownie jądrowe jawią się jako obiekty o wyjątkowym znaczeniu strategicznym, z jednej strony gwarantujące stabilne, niskoemisyjne źródło energii, z drugiej zaś generujące specyficzne zagrożenia związane z potencjalnymi awariami, terroryzmem, sabotażem czy cyberatakami.

Rozwój koncepcji ochrony infrastruktury krytycznej w Polsce i na świecie jest rezultatem procesów zachodzących od końca XX wieku. Zmieniający się układ sił międzynarodowych, powstawanie nowych zagrożeń asymetrycznych, a także przyjęcie złożonego modelu współzależności gospodarczych sprawiły, że infrastruktura krytyczna przestała być postrzegana wyłącznie w wymiarze technicznym, a zaczęła być rozumiana jako całościowy system naczyń połączonych. Awarie lub zakłócenia w jednym sektorze mogą prowadzić do efektów kaskadowych, dotyczących całe społeczeństwo. Współczesne państwa, szczególnie w ramach Unii Europejskiej i NATO, coraz większy nacisk kładą na konstruowanie odporności systemowej, czyli zdolności do szybkiego reagowania na kryzysy oraz do odbudowywania i funkcjonowania w krótkim czasie.

W XXI wieku problematyka ochrony infrastruktury krytycznej nabrała jeszcze większego znaczenia w wyniku wzrostu liczby incydentów o charakterze globalnym. Zmiany klimatyczne skutkują coraz częstszym występowaniem gwałtownych zjawisk naturalnych: powodzi, huraganów czy fal upałów, które destabilizują systemy energetyczne, transportowe i wodne. Terroryzm międzynarodowy, szczególnie po wydarzeniach z 11 września 2001 roku, wymusił nowe podejście do ochrony fizycznej kluczowych obiektów gwarantujących funkcjonowania społeczeństwa i państwa. Z kolei cyberprzestrzeń stała się nowym polem walki, w którym zagrożenia mogą mieć również poważne skutki

jak tradycyjne ataki militarne. Przykłady z ostatnich lat, takie jak cyberataki na ukraińską sieć energetyczną czy atak *ransomware* na amerykański system rurociągów Colonial Pipeline, dowodzą, że infrastruktura krytyczna jest szczególnie narażona na tego typu incydenty, stanowiąc cele ataków nie tylko w czasie pokoju, ale również podczas wojny.

W tym kontekście szczególnie miejsce zajmuje energetyka jądrowa. Elektrownie atomowe postrzegane są jako strategiczne narzędzie zapewnienia bezpieczeństwa energetycznego państwa oraz realizacji celów polityki klimatycznej, ponieważ wytwarzają energię elektryczną bez emisji dwutlenku węgla i mogą stabilizować system elektroenergetyczny w dobie rozwoju źródeł odnawialnych. Jednocześnie są to obiekty wymagające wyjątkowych mechanizmów ochrony zarówno w wymiarze technicznym, jak i organizacyjnym. Zagrożenia związane z potencjalnymi awariami, atakami terrorystycznymi czy cybernetycznymi mają charakter transnarodowy i mogą wpływać nie tylko na bezpieczeństwo danego państwa, lecz także na cały region. W przypadku Polski, która przygotowuje się do budowy pierwszej elektrowni jądrowej, problematyka ta ma szczególne znaczenie i wymaga dogłębnej analizy.

Niniejsza praca koncentruje się na zagadnieniach związanych z ochroną i bezpieczeństwem infrastruktury krytycznej w Polsce, ze szczególnym uwzględnieniem strategicznej roli elektrowni atomowych. Jej celem jest identyfikacja kluczowych wyzwań, analiza podatności oraz wskazanie rekomendacji dotyczących budowy zintegrowanego systemu ochrony, odpowiadającego współczesnym realiom zagrożeń.

Zakres badawczy książki obejmuje analizę teoretycznych i prawnych podstaw ochrony infrastruktury krytycznej, identyfikację zagrożeń i ryzyk, a także studium przypadków wybranych sektorów. Szczególną uwagę poświęcono sektorowi energetycznemu, ponieważ to właśnie on w największym stopniu decyduje o stabilności systemu bezpieczeństwa narodowego. Metodologia badań opiera się na analizie literatury naukowej, aktów prawnych, dokumentów strategicznych oraz raportów organizacji międzynarodowych. Wykorzystano również analizę porównawczą doświadczeń innych państw w zakresie ochrony infrastruktury jądrowej, aby wskazać dobre praktyki, które mogą być zastosowane w Polsce.

Struktura pracy została podporządkowana logice badań, przechodząc od podstaw teoretycznych i prawnych, przez analizę zagrożeń, aż po studium sektorowe. Takie ujęcie pozwala na holistyczne spojrzenie na problematykę ochrony infrastruktury krytycznej, a jednocześnie umożliwia szczegółowe omówienie najważniejszych zagadnień związanych z bezpieczeństwem elektrowni jądrowych. Praca kończy się wnioskami i rekomendacjami, których celem jest wskazanie kierunków działań niezbędnych dla zwiększenia odporności polskiego systemu ochrony infrastruktury krytycznej w perspektywie nadchodzących dekad.

Wstęp ten stanowi nie tylko wprowadzenie do analizy, ale także podkreśla wagę podjętego problemu badawczego. Ochrona infrastruktury krytycznej, a zwłaszcza energetyki jądrowej, to jedno z najważniejszych wyzwań współczesnych państw. Polska, będąc na etapie przygotowań do uruchomienia własnego programu jądrowego, stoi przed historyczną szansą i jednocześnie obowiązkiem stworzenia systemu ochrony, który sprosta zarówno wyzwaniom współczesności, jak i przyszłości.

Mam nadzieję, że książka choć w niewielkim stopniu wyznaczy kierunki doskonalenia dotychczasowych rozwiązań, szczególnie w kontekście budowanych w Polsce elektrowni atomowych. W moim przekonaniu może ona stanowić opracowanie przydatne zarówno dla nauczycieli akademickich, jak również studentów kierunków Bezpieczeństwo wewnętrzne, Bezpieczeństwo narodowe czy Inżynieria bezpieczeństwa. Jest ona przeznaczona dla badaczy systemów ochrony infrastruktury krytycznej oraz dla praktyków realizujących zadania na rzecz ochrony tej istotnej infrastruktury państwa.