e-ISSN 2353-9062
ISSN 0867-4752

PAŃSTWOWA AGENCJA ATOMISTYKI

BIULETYN

BEZPIECZEŃSTWO JĄDROWE I OCHRONA RADIOLOGICZNA



3 (141) 2026

Biuletyn „Bezpieczeństwo Jądrowe i Ochrona Radiologiczna" znajduje się w wykazie czasopism naukowych Ministerstwa Edukacji i Nauki. Kwartalnik wydawany przez PAA otrzymał 40 pkt. w następujących dyscyplinach naukowych:

- nauki o bezpieczeństwie,
- nauki fizyczne,
- nauki chemiczne,
- nauki prawne,
- nauki medyczne
- inżyniernia bezpieczeństwa
- biologia medyczna.

WYDAWCA

Państwowa Agencja Atomistyki
UL. Nowy Świat 6/12, 00-400 Warszawa

REDAKCJA

Maciej JURKOWSKI – redaktor naczelny
Elżbieta ZALEWSKA – redaktor prowadzący
Marek WOŹNIAK – redaktor techniczny
Jarosław CHILMON – członek redakcji

UL. Nowy Świat 6/12, 00-400 Warszawa
TEL. 22 628 94 39
FAX 22 621 37 86
E-MAIL biuletyn@paa.gov.pl
WWW. gov.pl/web/paa

RADA PROGRAMOWA

prof. dr hab. **Janusz JANECZEK** – przewodniczący Rady
prof. dr hab. inż. **Andrzej CHMIELEWSKI** – członek Rady
prof. dr hab. n. med. **Marek K. JANIAK** – członek Rady
prof. dr hab. n. med. **Eugeniusz DZIUK** – członek Rady
prof. dr hab. n. med. **Leszek KRÓLICKI** – członek Rady
dr hab. **Agnieszka KORGUL** – członek Rady
dr **Tomasz NOWACKI** – członek Rady

e-ISSN 2353-9062
ISSN 0867-4752

DRUK

PHU OLEJNIK Piotr Olejnik, 01-318 Warszawa, ul. E. Szwankowskiego 2/3
Zdjęcie na okładce: siedziba Państwowej Agencji Atomistyki (fot. PAA).

BEZPIECZEŃSTWO JĄDROWE I OCHRONA RADIOLOGICZNA

BIULETYN INFORMACYJNY PAŃSTWOWEJ AGENCJI ATOMISTYKI

Nr 3 (141) 2026
Warszawa

Spis treści

7 Redakcja Biuletynu BJiOR PAA
Zmarł Andrzej Cholerzyński

9 Artur J. Tyński
Prezes PAA jako naczelny organ dozoru jądrowego

20 Andrzej G. Chmielewski, Antoni Rożeń
Bierne (pasywne) systemy bezpieczeństwa reaktorów jądrowych

33 Karolina Jezierska, Paulina Rotter, Magdalena Sroczyk-Jaszczyńska
Ochrona radiologiczna pacjenta w stomatologii wsparta przepisami prawa w Polsce

43 Agnieszka Szumska
Model LNT a ochrona radiologiczna w zakresie niskich dawek: stan wiedzy i propozycje zmian regulacyjnych w USA

49 Artur Chlebicki
Computer security of nuclear power plant instrumentation and control systems. IAEA guidance versus the Polish legal framework on the eve of the first unit's construction

Szanowni Państwo



Bieżący numer otwiera wspomnienie o wieloletnim dyrektorze Zakładu Unieszkodliwiania Odpadów Promieniotwórczych, Panu **Andrzeju Cholerzyńskim**, zmarłym w końcu lipca 2026 roku. W latach 2012–2016 był on Sekretarzem Rady Bezpieczeństwa Jądrowego i Ochrony Radiologicznej – utworzonego w lipcu 2012 roku organu doradczego i opiniotwórczego Prezesa Państwowej Agencji Atomistyki. Był także przez wiele lat członkiem komisji egzaminacyjnej Prezesa PAA prowadzącej egzaminy państwowe na uprawnienia **inspektora dozoru jądrowego**.

Wspomnienie to poprzedzają ważne bieżące informacje: o podpisaniu przez Prezesa PAA i Wojewodę warmińsko-mazurskiego listu intencyjnego dotyczącego zainstalowania na terenie tego województwa 9 nowych stacji wczesnego wykrywania skażeń promieniotwórczych, oraz o udziale Prezesa PAA w spotkaniu Forum Współpracy Dozorowej (RCF) w Wiedniu.

W pierwszym z opublikowanych artykułów **Artur Tyński** poddaje wnikliwej analizie konstrukcję prawną polegającą na połączeniu w jednym organie, jakim jest Prezes Państwowej Agencji Atomistyki, który jest naczelnym organem dozoru jądrowego, dwóch atrybutów: **centralności** w systemie administracji rządowej w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej oraz **naczelności** w pionie dozoru jądrowego. Autor porządkuje siatkę pojęciową, rozróżniając kontrolę, nadzór i dozór oraz eksponując prewencyjny i prospektywny charakter dozoru jądrowego, ukierunkowanego na ochronę bezpieczeństwa jądrowego, a nie wyłącznie na legalność.

W drugim artykule **Andrzej Chmielewski** i **Antoni Rożeń** przedstawili istotne aspekty stosowania biernych elementów i systemów bezpieczeństwa w nowych projektach reaktorów jądrowych, oraz wyzwania stojące przed organami regulacyjnymi w ocenie niezawodności takich systemów i bezpieczeństwa obiektów jądrowych w nie wyposażonych, w procesach wydawania zezwoleń na budowę i eksploatację takich obiektów. W artykule omówiono podstawowe siły i gradienty wykorzystywane w systemach pasywnych budowanych obecnie reaktorów trzeciej generacji (jak AP1000) i projektowanych reaktorów czwartej generacji. Omówiono kategorie systemów pasywnych według klasyfikacji MAEA, metodologie oceny ich niezawodności, stanowiska do prób modelowych oraz przykłady zastosowanych rozwiązań technicznych w obiektach energetyki jądrowej.

Trzeci artykuł dotyczy ochrony radiologicznej pacjenta. **Karolina Jezierska**, **Paulina Rotter** i **Magdalena Sroczyk-Jaszczyńska** przedstawiły w nim zasady ochrony radiologicznej pacjenta w stomatologii z uwzględnieniem aktualnych wymagań prawnych, zaleceń międzynarodowych oraz wytycznych towarzystw naukowych. W artykule omówiono ewolucję zasady ALARA w kierunku podejścia bardziej zorientowanego na wartość diagnostyczną badania (koncepcja ALADA), oraz uwzględniania dodatkowo konkretnych wskazań klinicznych i indywidualnych cech pacjenta (koncepcja ALADAIP). Podkreślono znaczenie uzasadnienia ekspozycji i świadomego wyboru metody obrazowania z punktu widzenia racjonalnej optymalizacji dawki, a także konieczność właściwego doboru, eksploatacji i kontroli jakości aparatury wykorzystywanej w diagnostyce radiologicznej w stomatologii. Zwrócono uwagę na potrzebę ujednolicenia praktyk nadzorczych oraz doprecyzowanie wytycznych wykonawczych, by stosowanie przepisów było przewidywalne i spójne na terenie całego kraju.

Czwarty z artykułów opublikowanych w bieżącym numerze poświęcony jest dyskusji zasadności przyjęcia modelu liniowego bezprogowego LNT (*Linear No-Threshold)* do oceny i zarządzania ryzykiem skutków stochastycznych narażenia na promieniowanie jonizujące przy małych dawkach. **Agnieszka Szumska** wskazuje w nim, że system ochrony radiologicznej opiera się przede wszystkim na zasadach uzasadnienia, optymalizacji i ograniczania narażenia. Istniejąca obecnie rozbudowana wiedza o złożoności odpowiedzi komórkowej na promieniowanie potwierdza występowanie przy niskich dawkach istotnych niepewności, w szczególności w zakresie stochastycznych efektów dziedzicznych, co sprawia, że hipotezę LNT należy traktować jako użyteczny, ale ostrożny i zachowawczy element ochrony radiologicznej. Skutkuje to inicjatywami jej rewizji, między innymi takimi jak ta, podjęta w 2026 roku przez

US NRC, by lepiej oceniać ryzyko i proporcjonalnie dopasowywać rygory do rzeczywistego zagrożenia (podejście „*risk informed*"), opisana w tym artykule.

Numer zamyka artykuł w angielskiej wersji językowej na temat cyberbezpieczeństwa systemów kontrolno-pomiarowych elektrowni jądrowej. **Artur Chlebicki** wskazuje w nim na luki i niespójności w istniejących polskich ramach prawnych w świetle wymagań i wytycznych *IAEA Nuclear Security Series* (dokumentów z serii bezpieczeństwa i ochrony fizycznej Międzynarodowej Agencji Energii Atomowej) oraz wymagań Międzynarodowej Komisji Elektrotechnicznej (IEC), dotyczących projektowego zapewnienia cyberbezpieczeństwa układów sterowania i zabezpieczeń elektrowni jądrowej już na etapie przystępowania do jej budowy.

Tradycyjne już życzenie Państwu owocnej lektury bieżącego numeru jest tym razem dla mnie także okazją do poinformowania, że dobiega końca moja współpraca z Biuletynem w obecnej formie, jako od blisko dekady jego redaktora naczelnego, a także od 2009 roku, kiedy powołano mnie na stanowisko Wiceprezesa PAA i Głównego Inspektora Dozoru Jądrowego, aż do bieżącego numeru – jako osoby sprawującej z ramienia Prezesa PAA pieczę nad tematyką i jakością merytoryczną publikowanych artykułów. Była to dla mnie wspaniała życiowa i zawodowa przygoda, którą zapoczątkowało współautorstwo artykułu o roli i zadaniach dozoru jądrowego, opublikowanego w pierwszym numerze Biuletynu w 1989 roku.

Byłem potem autorem szeregu artykułów, a od 2009 roku, redagując słowo wstępne w ponad 60 wydaniach Biuletynu, jakie ukazały się od tamtego czasu do bieżącego numeru włącznie, miałem przyjemność przybliżać Państwu w zwięzłej formie zawarte w nich treści, licząc na zainteresowanie opisywanymi tematami, co, mam nadzieję, choć w części przyniosło oczekiwany skutek, za co wszystkim P.T. Czytelnikom bardzo serdecznie dziękuję. Czytać nasz Biuletyn naprawdę warto, a czasem nawet sięgać do starszych numerów, bo wiele z zawartych w nich informacji wcale nie traci na aktualności. Dziękuję także za życzliwe wsparcie i współpracę wszystkim, którzy przyczyniali się przez te lata do utrzymania ciągłości wydawania naszego kwartalnika: Prezesowi i członkom kierownictwa PAA oraz Rady Programowej Biuletynu i ich poprzednikom, autorom zgłaszanych nam tekstów do publikacji, korektorom, recenzentom i oczywiście moim najbliższym współpracownikom w Redakcji, a szczególnie – Redaktor Prowadzącej i Redaktorowi Technicznemu – serdeczne dzięki! A nowemu Redaktorowi Naczelnemu życzę sukcesów i co najmniej takiej satysfakcji, jaka była moim udziałem. Powodzenia!

Redaktor Naczelny
Maciej Jurkowski

Będą nowe stacje monitoringu radiacyjnego na Warmii i Mazurach

Prezes Państwowej Agencji Atomistyki Andrzej Głowacki i wojewoda warmińsko-mazurski Radosław Król podpisali 10 sierpnia 2026 r.w Olsztynie list intencyjny dotyczący rozwoju monitoringu radiacyjnego w regionie.

W najbliższych latach na terenie województwa ma zostać zainstalowanych **9 nowych stacji wczesnego wykrywania skażeń promieniotwórczych**. Ich rozmieszczenie ma wzmocnić system ciągłego monitorowania poziomu promieniowania i umożliwić szybsze wykrywanie potencjalnych skażeń.

Obecnie w województwie działają dwie takie stacje – w **Olsztynie i Gołdapi**. PAA i władze województwa będą współpracować przy wyborze lokalizacji kolejnych urządzeń. Ich rozmieszczenie musi uwzględniać m.in. ukształtowanie i zagospodarowanie terenu, stopień urbanizacji oraz odległość od istniejących stacji.

List intencyjny jest elementem prowadzonego przez PAA rozwoju ogólnopolskiej sieci monitoringu radiacyjnego.



Fot. 1. Podpisanie listu intencyjnego (fot. Agnieszka Modrzejewska).

Prezes PAA o postępach w polskim programie jądrowym podczas Forum Współpracy Dozorowej w Wiedniu

Delegacja Państwowej Agencji Atomistyki (PAA), na czele z prezesem Andrzejem Głowackim, wzięła udział w spotkaniu Forum Współpracy Dozorowej (ang. RCF – *Regulatory Cooperation Forum*) w Wiedniu.

Forum Współpracy Dozorowej zostało powołane z inicjatywy Międzynarodowej Agencji Energii Atomowej (MAEA). Jego celem jest wspieranie organów dozoru jądrowego państw, które planują rozwój energetyki jądrowej, poprzez wymianę doświadczeń z krajami posiadającymi bardziej zaawansowane programy jądrowe.

Udział Polski w pracach RCF pozwala krajowemu dozorowi jądrowemu na rozwijanie i wzmacnianie kompetencji niezbędnych do realizacji zadań wynikających z Programu Polskiej Energetyki Jądrowej. W ramach Forum organizowane są m.in. zagraniczne staże szkoleniowe, wizyty studyjne, warsztaty techniczne oraz spotkania eksperckie.

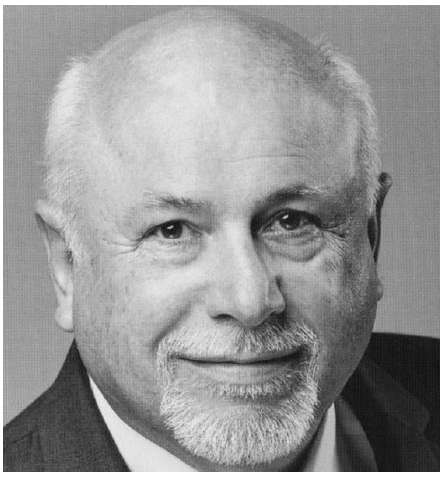
Podczas spotkania Andrzej Głowacki, reprezentujący Polskę, przedstawił proces prowadzonej przez polski dozór jądrowy oceny wniosku spółki Polskie Elektrownie Jądrowe (PEJ) o wydanie zezwolenia na budowę pierwszej w Polsce elektrowni jądrowej.

Prezes PAA poinformował również o prowadzonym dialogu przedlicencyjnym z interesariuszami zainteresowanymi realizacją w Polsce projektów małych reaktorów modułowych (SMR).

Spotkanie RCF jest okazją do wymiany doświadczeń i dobrych praktyk pomiędzy organami dozoru jądrowego oraz do dyskusji nad wyzwaniami związanymi z rozwojem energetyki jądrowej.

Elżbieta Zalewska
Redakcja biulrtynu BJOR

Zmarł Andrzej Cholerzyński



Ze smutkiem przyjęliśmy informację o śmierci emerytowanego wieloletniego i zasłużonego dyrektora Zakładu Unieszkodliwiania Odpadów Promieniotwórczych zarządzającego Krajowym Składowiskiem Odpadów Promieniotwórczych w Różanie, sekretarza Rady do spraw Bezpieczeństwa Jądrowego i Ochrony Radiologicznej pierwszej kadencji, wieloletniego członka komisji egzaminacyjnej Prezesa PAA na uprawnienia inspektora dozoru jądrowego – Andrzeja Cholerzyńskiego, który zmarł 20 lipca 2026 roku w wieku 77 lat.

Andrzej Cholerzyński był absolwentem Wydziału Chemii Politechniki Warszawskiej, gdzie w 1975 roku uzyskał tytuł magistra inżyniera. W marcu tego samego roku rozpoczął pracę zawodową w Instytucie Badań Jądrowych (IBJ) w Świerku w Zakładzie Unieszkodliwiania Substancji Promieniotwórczych (ZUSP). Tak rozpoczęła się jego zawodowa przygoda z odpadami promieniotwórczymi, z którymi przepracował ponad 45 lat, kolejno na wszystkich istotnych stanowiskach związanych z technologiami ich unieszkodliwiania, aż do stanowisk kierowniczych – wicedyrektora Zakładu Unieszkodliwiania Odpadów Promieniotwórczych (ZUOP) i kierownika Centralnego Składowiska Odpadów Promieniotwórczych (CSOP), a następnie dyrektora ZUOP.

Pierwszym zadaniem, jakie otrzymał po rozpoczęciu pracy w ZUSP od kierownika swojej pracowni Włodzimierza Tomczaka, było wdrożenie stosowanej w Belgii technologii oczyszczania niskoaktywnych ścieków promieniotwórczych z zastosowaniem sorbentów nieorganicznych. ZUSP był wtedy zakładem naukowym IBJ, posiadał laboratorium chemiczne, można więc było najpierw przeprowadzić badania laboratoryjne, a dopiero potem próby na instalacjach technologicznych. Pierwsze oczyszczanie odpadów z zastosowaniem nowej technologii dało lepsze wyniki niż oczyszczanie metodami stosowanymi wcześniej.

Pierwszych kilka lat pracy wypełniały mu rutynowe szkolenia i praktyki niezbędne do zdobycia uprawnień wymaganych do prac z odpadami promieniotwórczymi. On jednak szczególnie cenił sobie możliwość udziału w obsłudze instalacji technologicznych. Od początku starał się opanować obsługę wszystkich instalacji w ZUSP. Uczestniczył w tzw. dyżurach technologicznych zapewniających ciągłość obsługi procesów technologicznych w systemie pracy na trzy zmiany, twierdząc, że to najlepszy sposób zdobywania wiedzy i doświadczenia. Twierdził, że wiele można nauczyć się nie tylko od kierowników działów czy sekcji ZUSP, ale także od zwykłych pracowników posiadających duże doświadczenie. Kierownictwo ZUSP, które nastawione było na opanowywanie i rozwijanie nowych technologii, dbało o zapewnienie mu udziału w szkoleniach, kursach i konferencjach organizowanych przez MAEA w Wiedniu, umożliwiło także skorzystanie z rocznego stypendium w BNL[1] w USA. W latach 80. ub. wieku, kiedy ruszała budowa elektrowni jądrowej w Żarnowcu, uczestniczył w projektach związanych z postępowaniem z odpadami i wypalonym paliwem jądrowym w tym obiekcie, odbył wszystkie wymagane szkolenia, także z zakresu ochrony fizycznej, w tym szkolenie w USA. Bardzo cenił sobie nawiązanie współpracy z Politechniką Warszawską oraz Instytutem Chemii i Techniki Jądrowej, której owocem było współautorstwo kilku patentów – jeden z nich dotyczył wdrożenia technologii asfaltowania w zestalaniu ciekłych odpadów promieniotwórczych.

Lata 90. i pierwsza dekada XXI w. to czas ratyfikacji i wejścia w życie Konwencji Wspólnej Bezpieczeństwa Postępowania z Odpadami Promieniotwórczymi i Wypalonym Paliwem Jądrowym, skutkujący koniecznością uczestniczenia w procesach przeglądowych Konwencji Wspólnej, opracowywaniu raportów na organizowane w cyklu

[1] *Brookhaven National Laboratory*. laboratorium narodowe podlegające Departamentowi Energii rządu Stanów Zjednoczonych Ameryki

trzyletnim Spotkania Przeglądowe i wykazywaniu na tych spotkaniach postępów w doskonaleniu bezpieczeństwa postępowania z odpadami w swoim kraju. To także konieczność opracowania nowej ustawy Prawo atomowe, spójnej między innymi z wymaganiami tej konwencji, i dokonania stosownych zmian organizacyjnych. To także czas, kiedy dla państw aspirujących do członkostwa w Unii Europejskiej otworzyły się możliwości wykorzystania środków unijnych na dostosowanie ram prawnych i organizacyjnych do wymagań Unii Europejskiej. Andrzej Cholerzyński był mocno zaangażowany we wszystkich tych obszarach. Dostarczał Prezesowi PAA dane do krajowych raportów przeglądowych i opracowywał odpowiedzi na pytania państw-stron konwencji dotyczące tych raportów, wchodził w skład polskich delegacji i czynnie uczestniczył w kolejnych spotkaniach przeglądowych w MAEA w Wiedniu. Zadbał, by zapisy nowego Prawa atomowego dały podstawę do zmiany statusu Zakładu, który w roku 2002 wyodrębnił się z Instytutu Energii Atomowej, stając się samodzielnym przedsiębiorstwem użyteczności publicznej o nazwie ZUOP, z odrębnym statutem i budżetem, z zabezpieczoną ustawowo (gwarantowaną przez państwo) zdolnością ciągłego przyjmowania powstających na terenie kraju odpadów promieniotwórczych i wypalonego paliwa jądrowego. Potrafił także zapewnić współfinansowanie z unijnego programu PHARE, z programu pomocy technicznej MAEA i z budżetu państwa dwóch koordynowanych przez siebie projektów, wymagających znacznych nakładów i udziału wielu partnerów krajowych i zagranicznych: budowy linii technologicznej oczyszczania ścieków metodą wyparną oraz budowy komory gorącej do kapsułowania wypalonego paliwa z reaktorów. Doprowadził do uruchomienia i funkcjonowania w ZUOP obu tych instalacji, wykorzystujących najnowocześniejsze dostępne technologie, takie jak doczyszczanie skroplin powyparnych metodą odwróconej osmozy przy pomocy instalacji zaprojektowanej i wdrożonej przez IChiTJ, czy zdalne szczelne zamykanie kaset z wypalonym paliwem wypełnianych helem automatem spawalniczym wewnątrz komory gorącej. Wspólnie z Włodzimierzem Tomczakiem doprowadził także, dzięki nawiązanym kontaktom z BNFL[2], do opracowania przez angielskich ekspertów tzw. Safety Case (raportu bezpieczeństwa) dla przyszłego zamknięcia składowiska odpadów promieniotwórczych w Różanie. Odegrał także wiodącą rolę w realizacji w Polsce finansowanego ze środków amerykańskich programu GTRI (Inicjatywa Redukcji Zagrożeń Globalnych), którego celem był zwrot wysokowzbogaconego paliwa jądrowego do kraju producenta, a także zapewnienie i utrzymywanie należytych zabezpieczeń fizycznych użytkowanych w Polsce źródeł wysokoaktywnych.

Jako uznany w kraju i za granicą ekspert w dziedzinie technologii postępowania z odpadami promieniotwórczymi i wypalonym paliwem jądrowym został powołany w lipcu 2012 roku na okres 4 lat do nowo utworzonej wówczas Rady ds. Bezpieczeństwa Jądrowego i Ochrony Radiologicznej przy Prezesie PAA, w której pełnił obowiązki Sekretarza Rady. Od kwietnia 2013 był także przez blisko 10 lat członkiem komisji egzaminacyjnej Prezesa PAA na uprawnienia inspektora dozoru jądrowego II stopnia.

Był specjalistą o ogromnym doświadczeniu i wiedzy praktycznej w zakresie technologii i inżynierii postępowania z odpadami i wypalonym paliwem, znakomitym organizatorem i koordynatorem inżynieryjnych projektów wykorzystujących najnowocześniejsze rozwiązania na poziomie światowym, angażujących wielu partnerów krajowych i zagranicznych, które potrafił doprowadzić z pełnym sukcesem do końca.

Był człowiekiem otwartym i pełnym humoru, łatwo nawiązującym kontakty, konkretnym i solidnym we współpracy z kontrahentami przy realizacji wspólnych projektów, pomysłowym i skutecznym w podejmowanych działaniach, w których dobro zakładu, w którym pracował, a potem nim kierował, zawsze było priorytetem. Niewątpliwie pozostanie wzorem dla swoich młodszych następców.

Cześć Jego pamięci! *Requiescat in pace!*

Koleżanki i koledzy z Komisji Egzaminacyjnej,
Kierownictwo i pracownicy Państwowej Agencji Atomistyki,
Redakcja Biuletynu BJOR PAA

2 BNFL – *British Nuclear Fuel Limited*.

Prezes PAA jako naczelny organ dozoru jądrowego

PAA President as the supreme nuclear regulatory authority

Artur J. Tyński
Wydział Inżynierii Środowiska i Energetyki, Politechnika Śląska w Gliwicach

Streszczenie: Artykuł podejmuje problematykę pozycji ustrojowej Prezesa Państwowej Agencji Atomistyki (dalej: Prezesa PAA) jako naczelnego organu dozoru jądrowego. Autor analizuje konstrukcję prawną polegającą na połączeniu w jednym organie dwóch atrybutów: centralności w systemie administracji rządowej w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej oraz naczelności w pionie dozoru jądrowego. Celem opracowania jest usystematyzowanie wiedzy o istocie naczelności Prezesa PAA, jej relacji z atrybutem centralności oraz jej praktycznym wymiarze, w szczególności w odniesieniu do inspektorów dozoru jądrowego. W pierwszej części autor porządkuje siatkę pojęciową, rozróżniając kontrolę, nadzór i dozór oraz eksponując prewencyjny i prospektywny charakter dozoru jądrowego, ukierunkowanego na ochronę bezpieczeństwa jądrowego, a nie wyłącznie legalności. Następnie omawia status ustrojowy organu, procedurę jego powoływania i odwoływania oraz model nadzoru resortowego. Praktyczną konkretyzację naczelności autor odnajduje w relacji organu wyższego stopnia wobec inspektorów dozoru jądrowego. Weryfikując pozytywnie hipotezę badawczą, autor uznaje przyjęty model za adekwatny do skutecznej realizacji dozoru jądrowego, wskazuje jednak na jego mankamenty.

Słowa kluczowe: Prezes Państwowej Agencji Atomistyki, dozór jądrowy, naczelny organ, bezpieczeństwo jądrowe i ochrona radiologiczna, inspektorzy dozoru jądrowego, niezależność organu regulacyjnego.

Summary: *This article examines the constitutional status of the President of the National Atomic Energy Agency (the President of the PAA) as the supreme nuclear regulatory authority. The author analyses the legal structure which combines two attributes within a single body: centrality within the system of government administration in matters of nuclear safety and radiation protection, and supremacy within the nuclear regulatory hierarchy. The aim of this study is to systematise knowledge regarding the nature of the PAA President's supreme authority, its relationship with the attribute of centrality, and its practical dimension, particularly in relation to nuclear regulatory inspectors. In the first part, the author organises the conceptual framework, distinguishing between control, supervision and oversight, and highlighting the preventive and forward-looking nature of nuclear oversight, which is geared towards safeguarding nuclear safety rather than merely ensuring legality. He then discusses the constitutional status of the authority, the procedure for its appointment and dismissal, and the model of ministerial oversight. The author identifies the practical manifestation of the principle of hierarchy in the relationship between the higher-level authority and nuclear oversight inspectors. Having confirmed the research hypothesis, the author considers the adopted model to be adequate for the effective implementation of nuclear oversight, whilst also pointing out its shortcomings.*

Keywords*: President of the National Atomic Energy Agency, nuclear regulatory oversight, supreme authority, nuclear safety and radiological protection, nuclear regulatory inspectors, independence of the regulatory body.*

Wprowadzenie

Współczesne położenie Polski w obszarze polityki energetycznej i klimatycznej charakteryzuje się głębokim procesem przekształceń, którego ostatecznym horyzontem jest osiągnięcie neutralności klimatycznej. Polityka klimatyczno-energetyczna Unii Europejskiej, wyrażona w ramach Europejskiego Zielonego Ładu oraz pakietu legislacyjnego „Gotowi na 55", zakłada redukcję emisji gazów cieplarnianych o co najmniej 55% do 2030 roku w stosunku do poziomu z 1990 r. oraz osiągnięcie neutralności klimatycznej do 2050 roku.[1] Realizacja tych celów wymaga gruntownej przebudowy krajowych miksów energetycznych, w tym w szczególności struktury wytwarzania energii elektrycznej w Polsce, która tradycyjnie opierała się na wysokoemisyjnych paliwach kopalnych. W ramach toczącej się transformacji energetycznej rosnącą rolę zaczynają odgrywać odnawialne źródła energii[2], spośród których największe znaczenie dla krajowego sektora wytwórczego mają instalacje fotowoltaiczne oraz energetyka wiatrowa[3].

Niesterowalny profil pracy odnawialnych źródeł energii wymusza jednak istnienie w systemie elektroenergetycznym jednostek wytwórczych pracujących w podstawie obciążenia, zdolnych do dostarczania energii elektrycznej w sposób stabilny i przewidywalny. Przejściową rolę w tym zakresie powierzono elektrowniom gazowym[4], natomiast docelowym filarem nowej struktury wytwórczej w Polsce mają być elektrownie jądrowe[5]. Energetyka jądrowa, charakteryzując się stabilnością wytwarzania oraz zerowym poziomem bezpośredniej emisji dwutlenku węgla, stanowi rozwiązanie szczególnie korzystne z perspektywy łączenia celów polityki klimatycznej z wymogiem zachowania bezpieczeństwa energetycznego państwa[6]. Bezpieczeństwo energetyczne na gruncie normatywnym oznacza zdolność do zaspokojenia bieżącego oraz perspektywicznego zapotrzebowania na energię elektryczną w sposób uwzględniający wymogi środowiskowe i ekonomiczne (art. 3 pkt 16 p.e.[7]).

Realizacja założeń Programu polskiej energetyki jądrowej[8] oraz Polityki energetycznej Polski do 2040 r.[9] uruchomiła pierwszy proces inwestycyjny dotyczący wielkoskalowej elektrowni jądrowej, prowadzony na podstawie ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (dalej: ustawa inwestycyjna)[10]. Proces ten, obejmujący szereg etapów (budowlany, eksploatacyjny oraz zaplanowanie etapu likwidacyjnego), angażuje liczne organy oraz instytucje administracji państwowej. Centralną pozycję wśród nich zajmuje Prezes Państwowej Agencji Atomistyki (dalej: Prezes PAA), będący jednoosobowym, centralnym organem administracji rządowej właściwym w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej. Jednocześnie Prezes PAA jest naczelnym organem dozoru jądrowego[11].

Kumulacja w jednym organie dwóch atrybutów ustrojowych, tj. centralności w systemie administracji rządowej w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej oraz naczelności w pionie dozoru jądrowego, stanowi konstrukcję prawną o znacznym potencjale interpretacyjnym, która jak dotąd nie była przedmiotem pogłębionych analiz w polskiej doktrynie prawa administracyjnego. Rozważania nad pozycją ustrojową Prezesa PAA pojawiały się w polskiej literaturze prawniczej rzadko, najczęściej w kontekście analiz niezależności regulatorów sektorowych[12] i usytuowania w strukturze administracji rządowej[13].

1 Komisja Europejska, Europejski Zielony Ład, COM(2019) 640, Bruksela 2019, https://eur-lex.europa.eu/resource.html?uri=cellar:b828d165-1c22-11ea-8c1f-01aa75ed71a1.0016.02 /DOC_1&format=PDF, [dostęp: 10.09.2025], s. 5; Por. Z. Ziemacki, Europejski Zielony Ład i odbudowa gospodarki – szanse i wyzwania, [w:] Sprawy Międzynarodowe 3/2021, Warszawa 2021, s. 91.

2 Ustawa z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz. U. z 2026 r. poz. 68; dalej: Ustawa OZE), art. 2 ust. 9-12.

3 Wzrost z 0 MW zainstalowanych w odnawialnych źródłach energii w 2007 r. do 34 253 MW w 2024 r. Zob. Polskie Sieci Elektroenergetyczne, Raport 2024 KSE: Zestawienie danych ilościowych dotyczących funkcjonowania KSE w 2024 roku, https://www.pse.pl/dane-systemowe/funkcjonowanie-kse/raporty-roczne-z-funkcjonowania-kse-za-rok/ raporty-za-rok-2024, [dostęp: 01.10.2025].

4 S. Michalik, D. Zieliński, Transformacja energetyczna w Polsce w świetle strategicznych dokumentów rządowych, Warszawa 2024, s. 17–18.

5 Załącznik do uchwały nr 141 Rady Ministrów z dnia 2 października 2020 r. w sprawie aktualizacji programu wieloletniego pod nazwą „Program polskiej energetyki jądrowej" (dalej: PPEJ), s. 8–9.

6 A. Strupczewski, Energetyka jądrowa koniecznym elementem elektroenergetyki polskiej, [w:] Academia – Magazyn Polskiej Akademii Nauk 1(65)/2021, Warszawa 2021, s. 89–90.

7 Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. z 2026 poz. 46, 516, 607).

8 Program polskiej energetyki jądrowej przyjęty uchwałą Rady Ministrów nr 141 z dnia 2 października 2020 r. w sprawie aktualizacji programu wieloletniego pod nazwą „Program polskiej energetyki jądrowej" (M.P. z 2020 r. poz. 946).

9 Polityka Energetyczna Polski do 2040 r. przyjęta uchwałą Rady Ministrów nr 22/2021 z dnia 2 lutego 2021 r. ogłoszona Obwieszczeniem Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r. (M.P. z 2021 r. poz. 264).

10 Dz.U. z 2025 r. poz. 1156.

11 Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe (Dz.U. z 2026 r. poz. 1, dalej: Prawo atomowe), art. 109 ust. 1.

12 Zob. T. R. Nowacki, Niezależność organów dozoru jądrowego na tle prawa międzynarodowego, europejskiego i konstytucyjnego, Wrocław 2015, s. 192-204; tegoż, Ograniczenie autonomii Prezesa Państwowej Agencji Atomistyki, [w:] Przegląd Sejmowy 4(147)/2018, Warszawa 2018, s. 53–73; tegoż, *Prawne gwarancje niezależności dozoru jądrowego w Polsce* (w:) I. Ramus (red.), *Obrót powszechny i gospodarczy. Problemy publicznoprawne i ekonomiczne*, Kielce 2014, s. 285–318; tegoż *Niezależność organów dozoru jądrowego. Próba rekonstrukcji zakresu pojęciowego* (w:) K. Jeleń, Z. Rau (red.), *Energetyka jądrowa w Polsce*, Warszawa 2012, s. 580–622.

13 Tegoż, Organy dozoru jądrowego w strukturze administracji rządowej w Polsce, [w:] Zeszyty Prawnicze Biura Analiz Sejmowych 1(69)/2021, Warszawa 2021, s. 9–38

Realizacja Programu polskiej energetyki jądrowej oraz uruchomienie procesu inwestycyjnego dotyczącego wielkoskalowej elektrowni jądrowej sprawiają, że pozycja ustrojowa Prezesa PAA nabiera znaczenia praktycznego[14]. Konsekwencją tego stanu rzeczy powinno być pogłębione zainteresowanie doktryny problematyką ustroju, zakresu działania, zadań, kompetencji oraz relacji organizacyjnych wiążących Prezesa PAA z innymi podmiotami uczestniczącymi w realizacji dozoru jądrowego. Niniejsze opracowanie wpisuje się w ten nurt rozważań, koncentrując się na atrybucie naczelności jako szczególnej cechy ustrojowej, odróżniającej Prezesa PAA od większości innych centralnych organów administracji rządowej.

Celem opracowania jest usystematyzowanie wiedzy na temat istoty naczelności Prezesa PAA, jej relacji z atrybutem centralności organu w systemie administracji rządowej oraz jej praktycznego wymiaru w pionie dozoru jądrowego, w szczególności w odniesieniu do inspektorów dozoru jądrowego. Przyjętą hipotezą badawczą jest twierdzenie, w myśl którego model ustrojowy łączący w jednym organie atrybut centralności w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej z atrybutem naczelności w pionie dozoru jądrowego stanowi adekwatną konstrukcję prawną do skutecznej realizacji dozoru jądrowego, choć nie pozostaje wolny od mankamentów dotyczących gwarancji niezależności regulatora oraz spójności pojęciowej. W toku rozważań zastosowano metodę dogmatyczno-prawną, uzupełnioną o elementy wykładni systemowej oraz odwołania do doktryny prawa administracyjnego i publicznego prawa gospodarczego.

Dozór, nadzór, kontrola – ujęcie systemowe w prawie administracyjnym

Opis pozycji ustrojowej Prezesa PAA wymaga uprzedniego doprecyzowania siatki pojęciowej. Pojęcia „kontroli" i „nadzoru" („dozoru") są w polskim porządku prawnym używane czasami synonimicznie, czasami zaś jako terminy o odrębnych desygnatach. Brak precyzji w tym zakresie skutkuje trudnościami interpretacyjnymi w określaniu faktycznego zakresu uprawnień organów administracji, co w przypadku organów odpowiedzialnych za bezpieczeństwo jądrowe i ochronę radiologiczną nabiera szczególnej doniosłości praktycznej.

W doktrynie prawa administracyjnego przyjmuje się, że kontrola jest działaniem o charakterze diagnostycznym, polegającym na ustaleniu stanu faktycznego, porównaniu go z prawnie określonym wzorcem oraz wyciągnięciu wniosków z tego porównania[15]. Modelowy schemat czynności kontrolnych obejmuje powzięcie zamiaru przeprowadzenia kontroli i ocenę jej zasadności, zawiadomienie podmiotu kontrolowanego, przygotowanie niezbędnej dokumentacji, wszczęcie kontroli, przeprowadzenie właściwych czynności kontrolnych oraz spisanie protokołu pokontrolnego[16]. Charakterystyczną cechą kontroli *stricte* rozumianej jest brak władczego wpływu organu kontrolującego na podmiot kontrolowany. Wnioski formułowane w toku kontroli mogą stanowić podstawę do podjęcia ewentualnych działań korygujących, lecz same w sobie nie kreują nowych obowiązków po stronie podmiotu kontrolowanego[17].

W przeciwieństwie do kontroli nadzór jest kategorią pojęciową szerszą, obejmującą zarówno czynności o charakterze kontrolnym, jak i władczy element ingerencji w sferę praw i obowiązków podmiotu nadzorowanego[18]. Istotą nadzoru pozostaje możliwość skutecznego kształtowania działalności podmiotu nadzorowanego za pomocą środków prawnych, określanych mianem środków nadzorczych, w celu doprowadzenia stanu rzeczywistego do zgodności ze stanem postulowanym przez prawo[19]. Nadzór należy także odróżnić od kierownictwa. Nie obejmuje on bieżącego zarządzania działalnością podmiotu, lecz koncentruje się na weryfikacji jej legalności oraz w określonych przypadkach innych kryteriów[20]. Doktryna prawa administracyjnego wskazuje, że obok legalności kryteriami nadzoru mogą być również celowość, rzetelność, słuszność, bezpieczeństwo lub gospodarność[21]. W kontekście nadzoru realizowanego przez Prezesa PAA następuje zbieg występowania kryterium legalności oraz bezpieczeństwa.

14 Dotychczas Prezes PAA nadzorował działalność z wykorzystaniem mniejszych i nielicznych obiektów jądrowych, jak reaktory badawcze (w tym zestawy krytyczne) i przechowalniki wypalonego paliwa jądrowego oraz jedynego w Polsce składowiska odpadów promieniotwórczych (niebędącego obiektem jądrowym). Największa część działalności Prezesa PAA dotyczy jednak wykorzystywania źródeł promieniotwórczych. W 2024 r. Prezes PAA wydał 1714 decyzji administracyjnych w zakresie reglamentacji działalności związanej z narażeniem na promieniowanie jonizujące oraz 20 decyzji w zakresie bezpieczeństwa jądrowego – zob. Prezes PAA, Raport Roczny 2024. Działalność Prezesa Państwowej Agencji Atomistyki oraz ocena stanu bezpieczeństwa jądrowego i ochrony radiologicznej w Polsce w 2024 r., Warszawa 2025, s. 10. Na tym tle energetyka jądrowa odróżnia się za sprawą skomplikowanej i czasochłonnej procedury, skali inwestycji oraz kosztochłonności przedsięwzięcia. W 2025 r. Prezes PAA wydał 1448 decyzji administracyjnych w zakresie reglamentacji działalności związanej z narażeniem na promieniowanie jonizujące oraz 27 decyzji w zakresie bezpieczeństwa jądrowego, wśród nich 5 decyzji dotyczących autoryzacji laboratoriów i organizacji eksperckich do udziału w kontroli w elektrowniach jądrowych. – zob. Prezes PAA, Raport Roczny 2025, […], Warszawa 2026, s. 12–13.

15 A. Powałowski, Leksykon prawa gospodarczego publicznego, Warszawa 2019, s. 66.

16 A. Powałowski, Leksykon prawa gospodarczego publicznego, s. 67.

17 Z. Snażyk, A. Szafrański, Publiczne prawo gospodarcze, Warszawa 2021, s. 150.

18 J. Zimmermann, Prawo administracyjne, Warszawa 2022, s. 227; Por. B. Dolnicki, Nadzór nad samorządem terytorialnym, Katowice 1993, s. 59.

19 Z. Snażyk, A. Szafrański, Publiczne prawo gospodarcze, s. 150–151.

20 J. Szreniewski, Prawo administracyjne. Część ogólna, Lublin 1993, s. 194; Por. R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Konstytucyjne podstawy funkcjonowania administracji publicznej. System Prawa Administracyjnego. Tom 2, Warszawa 2012, s. 242–243.

21 J. Zimmermann, Prawo administracyjne, s. 227.

W ramach systemu nadzoru wyodrębnić można nadzór prewencyjny oraz nadzór weryfikacyjny[22]. Nadzór prewencyjny wyprzedza działalność podmiotu nadzorowanego i obejmuje przede wszystkim etap reglamentacji, w którym organ weryfikuje zdolność wnioskodawcy do spełnienia wymogów warunkujących prowadzenie działalności[23]. Składa się on z trzech następujących po sobie etapów: kontroli ogólnej, kontroli indywidualnej oraz etapu decyzyjnego. Etap kontroli ogólnej, podejmowany z urzędu i mający charakter ciągły oraz horyzontalny, służy ochronie publicznych dóbr istotnych z punktu widzenia regulacji danego sektora gospodarki[24]. W przypadku dozoru jądrowego do takich dóbr należą bezpieczeństwo jądrowe, ochrona radiologiczna, ochrona fizyczna obiektów i materiałów jądrowych oraz zabezpieczenie materiałów jądrowych, a przykładem kontroli ogólnej jest ocena sytuacji radiacyjnej kraju realizowana w trybie art. 72–75 Prawa atomowego. Etap kontroli indywidualnej następuje po wpływie wniosku o zezwolenie na prowadzenie działalności w zakresie pokojowego wykorzystania energii jądrowej i obejmuje weryfikację spełniania przez wnioskodawcę kryteriów pozytywnych i negatywnych warunkujących wydanie zezwolenia[25]. Etap decyzyjny, stanowiący zwieńczenie nadzoru prewencyjnego, polega na podjęciu rozstrzygnięcia administracyjnego.

Nadzór weryfikacyjny, określany niekiedy jako nadzór bieżący, polega na badaniu zgodności faktycznej działalności podmiotu nadzorowanego z obowiązującymi przepisami prawa oraz z warunkami określonymi w wydanym wcześniej rozstrzygnięciu administracyjnym (np. zezwoleniu)[26]. W przypadku stwierdzenia nieprawidłowości w działalności podmiotu nadzorowanego organ nadzorczy może zastosować środki nadzorcze obejmujące zmianę lub uchylenie wcześniejszej decyzji administracyjnej, nakaz usunięcia nieprawidłowości w określonym terminie, nałożenie kary administracyjnej lub wszczęcie postępowania egzekucyjnego[27].

Pojęcie dozoru jądrowego, choć obecne w nazwie klasyfikacji organów (art. 63 ust. 2 pkt 1, art. 64 ust. 1 pkt 1 Prawa atomowego), nie zostało zdefiniowane ani w Prawie atomowym, ani w innym akcie prawnym. Również doktryna prawa administracyjnego nie wypracowała jak dotąd ustabilizowanej koncepcji tego pojęcia. W związku z tym pomocne jest nawiązanie do definicji legalnej zawartej w nieobowiązującym już art. 51 ustawy z dnia 10 kwietnia 1986 r. – Prawo atomowe[28], zgodnie z którym dozór jądrowy polega na nadzorze i kontroli każdej działalności w zakresie wykorzystania energii jądrowej na potrzeby społeczno-gospodarcze, które powodują lub mogą powodować narażenie ludzi i środowiska na promieniowanie jonizujące. W ślad za argumentacją obecną w uzasadnieniu do projektu ustawy Prawo atomowe z 1986 r. T.R. Nowacki proponuje, aby dozór jądrowy rozumieć nie jako odrębną instytucję organizacyjną, lecz jako zespół czynności[29]. Pomocna w doprecyzowaniu istoty dozoru jądrowego jest analogia z bliskoznacznym pojęciem dozoru technicznego, zdefiniowanym w art. 2 ust. 1 ustawy z dnia 21 grudnia 2000 r. o dozorze technicznym[30]. Zgodnie z tym przepisem dozorem technicznym są działania zmierzające do zapewnienia bezpiecznego funkcjonowania urządzeń technicznych i urządzeń do odzyskiwania par paliwa oraz do zapewnienia bezpieczeństwa publicznego w obszarach związanych z eksploatacją tych urządzeń. W definicji tej eksponowany jest cel czynności dozorowych, którym jest stan bezpieczeństwa technicznego.

Zauważalna w obu pojęciach analogia aksjologiczna pozwala sformułować ogólną charakterystykę dozoru jądrowego jako zespołu czynności zmierzających do zapewnienia bezpieczeństwa jądrowego, ochrony radiologicznej, ochrony fizycznej i zabezpieczenia materiałów jądrowych. Bezpieczeństwo jądrowe definiowane jest jako stan polegający na osiągnięciu odpowiednich warunków do eksploatacji obiektów jądrowych, zapobieganiu awariom oraz łagodzeniu ich skutków, w celu ochrony pracowników oraz społeczności przed zagrożeniami wynikającymi z promieniowania jonizującego (art. 3 pkt 2 Prawa atomowego). W kontekście prawa energii jądrowej bezpieczeństwo jądrowe stanowi wartość priorytetową, której zapewnieniu powinny służyć wszystkie dostępne środki, co znajduje wyraz w fundamentalnej zasadzie prymatu bezpieczeństwa (zasada *safety first*)[31]. Ochrona radiologiczna oznacza wszelkie działania służące zapobieganiu narażeniu ludzi i skażeniu środowiska przez promieniowanie jonizujące. W przypadku gdy niemożliwe jest zapobieżenie takim sytuacjom, to w ramach ochrony radiologicznej identyfikuje się działania służące ograniczeniu skutków promie-

22 B. Dolnicki, Nadzór nad samorządem terytorialnym, s. 67; M. Goss, Nadzór i regulacja sektora ropy i gazu, Warszawa 2016, s. 117.
23 J. Piecha, Sprzeciw w prawie administracyjnym, Warszawa 2016, s. 381; Prawo atomowe, art. 4–5, art. 37a.
24 M. Goss, Nadzór i regulacja sektora ropy i gazu, s. 117; Por. T. Kocowski, Reglamentacja działalności gospodarczej w polskim prawie administracyjnym, Warszawa 2009, s. 344 i n.
25 M. Banasik, Administracyjnoprawne formy działań regulacyjnych niezależnych organów administracji publicznej, Warszawa 2019, s. 183; Zob. M. Goss, Nadzór i regulacja sektora ropy i gazu, s. 119–120.
26 A. Barczak-Oplustil, T. Sroka (red.), Odpowiedzialność publicznoprawna. System Prawa Medycznego. Tom 6, Warszawa 2023, s. 1317.
27 R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Publiczne prawo gospodarcze. System Prawa Administracyjnego. Tom 8A, Warszawa 2018, s. 397–399; Prawo atomowe, art. 12f, art. 35a, art. 37b-37d, art. 38-38b.
28 Dz.U. z 1986 r. nr 12 poz. 70 ze zm.
29 T. R. Nowacki, Niezależność organów dozoru jądrowego..., s. 224–226.
30 Ustawa z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz.U. z 2024 r. poz. 1194, dalej: ustawa o dozorze technicznym), art. 2 ust. 1.
31 Konwencja Bezpieczeństwa Jądrowego, sporządzona w Wiedniu dnia 20 września 1994 r. (Dz.U. z 1997 r. Nr 42, poz. 262), art. 10; Dyrektywa Rady 2009/7/Euratom z 25.06.2009 r. ustanawiająca wspólnotowe ramy bezpieczeństwa obiektów jądrowych, art. 3 ust. 2.

niowania jonizującego do poziomu tak niskiego, jak jest to rozsądnie osiągalne, z uwzględnieniem czynników ekonomicznych, społecznych i zdrowotnych (art. 3 pkt 20 Prawa atomowego). Ochrona fizyczna oznacza całokształt przedsięwzięć organizacyjnych i technicznych, mających na celu skuteczne zabezpieczenie materiałów jądrowych i obiektów jądrowych przed aktami terroru, dywersji, sabotażu i kradzieży (art. 3 pkt 19 Prawa atomowego).

Z powyższych rozważań wynika istotna funkcjonalna różnica pomiędzy nadzorem i kontrolą a dozorem. Nadzór i kontrola, choć zakorzenione w prawie i ukierunkowane na realizację celów publicznoprawnych, koncentrują się przede wszystkim na ochronie legalności, rozumianej jako zgodność działania podmiotu z normami kompetencyjnymi, proceduralnymi i materialnoprawnymi. Dozór jądrowy, choć również realizowany na podstawie i w granicach prawa, ma odmienny punkt ciężkości, ponieważ służy w pierwszej kolejności zabezpieczeniu określonego dobra materialnego, jakim jest bezpieczeństwo jądrowe. Różnica ta nie polega na całkowitym rozdzieleniu funkcji ochrony legalności i ochrony bezpieczeństwa, lecz na odmiennym rozłożeniu akcentów. Dozór jądrowy nie ogranicza się do badania formalnej poprawności zachowań podmiotu dozorowanego, lecz zmierza do zapobiegania powstaniu zagrożeń oraz utrzymania takiego stanu organizacyjnego i technicznego, który minimalizuje ryzyko wystąpienia zdarzeń mogących naruszyć bezpieczeństwo jądrowe i ochronę radiologiczną. Prewencyjny i prospektywny charakter dozoru jądrowego oraz ukierunkowanie na ochronę określonego dobra, a nie wyłącznie na badanie legalności sytuują go w szerszej kategorii nadzoru, który jest typowy m.in. dla dozoru technicznego, czy nadzorów: budowlanego, górniczego, sanitarnego, weterynaryjnego itp., nastawionych na ochronę dobra jakim jest zdrowie i życie, a także sektorów gospodarki takich, jak lotnictwo cywilne, czy obrót produktami leczniczymi.

Status ustrojowy Prezesa PAA

Pozycja ustrojowa Prezesa PAA wynika ze splotu dwóch atrybutów, które ustawodawca przypisał temu organowi w odrębnych przepisach Prawa atomowego. Pierwszym jest centralność. Jej formalnym wyrazem jest art. 109 ust. 1 Prawa atomowego, zgodnie z którym Prezes PAA jest centralnym organem administracji rządowej właściwym w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej. Drugim jest naczelność wynikająca z art. 64 ust. 1 pkt 1 Prawa atomowego, w myśl którego Prezes PAA jest naczelnym organem dozoru jądrowego. Łączne wystąpienie tych atrybutów w jednym organie tworzy konstrukcję prawną o doniosłych konsekwencjach systemowych, której prawidłowe odczytanie wymaga uprzedniego rozważenia natury każdego z nich osobno.

Centralność Prezesa PAA wpisuje się w typologię centralnych organów administracji rządowej. Prezes PAA nie jest organem konstytucyjnym. Konstytucja RP[32] nie wymienia go ani nie określa jego struktury czy pozycji w systemie administracji rządowej. Legitymacja oraz zakres działania organu mają zatem wyłącznie charakter ustawowy[33] i mieszczą się w granicach zasady legalizmu wyrażonej w art. 7 Konstytucji RP. Cechą charakterystyczną tej grupy organów pozostaje szczególna właściwość rzeczowa oraz – w zakresie wskazanym w ustawach – obowiązek wykonywania kierunków działania ustalanych przez Radę Ministrów[34].

W doktrynalnym podziale administracji gospodarczej na administrację bezpośrednią i pośrednią[35] Prezesa PAA należy zaliczyć do administracji bezpośredniej. Administrację bezpośrednią tworzą Rada Ministrów, ministrowie resortów gospodarczych oraz inne centralne organy administracji rządowej, w obrębie których wyodrębnia się dodatkowo grupę niezależnych centralnych organów administracji rządowej realizujących funkcję regulacyjną w sektorach historycznie powiązanych z państwem[36]. Administracja pośrednia obejmuje natomiast jednostki organizacyjne o różnym stopniu prawnej samodzielności, w tym jednostki działające w formach prawa prywatnego, jednostki samorządu terytorialnego oraz samorządy gospodarcze i zawodowe. Prezes PAA, wyposażony w instrumenty kontroli oraz nadzoru oddziałujące na podmioty prowadzące działalność związaną z ryzykiem narażenia na promieniowanie jonizujące, spełnia zatem wszystkie kryteria kwalifikacji do administracji gospodarczej bezpośredniej.

Cechą podstawową organów centralnych jest ogólnokrajowy zakres terytorialny działalności. Polski porządek prawny przewiduje zarówno monokratyczną (model przeważający), jak i kolegialną postać tych organów. Prezes PAA pozostaje organem monokratycznym, wykonującym swoje zadania przy pomocy Państwowej Agencji Atomistyki (dalej: PAA), będącej centralnym urzędem administracji rządowej powołanym do obsługi organizacyjno-administracyjnej organu. PAA zapewnia Prezesowi PAA zaplecze organizacyjne, w tym osobowe, finansowe i techniczne, dzięki czemu organ może prowadzić czynności analityczne, kontrolne oraz operacyjne. PAA jako urząd nie posiada samodzielnej legitymacji kompetencyj-

32 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm., dalej: Konstytucja RP).
33 Tutaj w szczególności: Prawo atomowe oraz ustawa inwestycyjna.
34 M. Swora, Niezależne organy administracji, Warszawa 2012, s. 153–154.
35 H. Gronkiewicz-Waltz, M. Wierzbowski, D. Szafrański, Prawo gospodarcze. Aspekty publicznoprawne, Warszawa 2025, s. 97.
36 K. Strzyczkowski, Prawo gospodarcze publiczne, Warszawa 2011, s. 129; Zob. także H. Gronkiewicz-Waltz, M. Wierzbowski, D. Szafrański, Prawo gospodarcze. Aspekty publicznoprawne, s. 97.

nej. Jej działania mają charakter służebny względem władczych uprawnień organu, którym jest Prezes PAA.

Procedura powoływania Prezesa PAA została unormowana w art. 109 ust. 2 Prawa atomowego. Prezes PAA jest powoływany przez Prezesa Rady Ministrów spośród kandydatów wyłonionych w drodze otwartego i konkurencyjnego naboru, na pięcioletnią kadencję, z możliwością jednokrotnego, ponownego wyboru. Inicjatywa rozpoczęcia naboru należy do ministra właściwego do spraw klimatu (dalej: Minister), który powołuje co najmniej trzyosobowy zespół odpowiedzialny za przeprowadzenie naboru. Zespół typuje nie więcej niż trzech kandydatów, których kandydatury Minister przedkłada Prezesowi Rady Ministrów. Wybór dokonywany jest spośród osób wyłonionych w toku naboru, co oznacza, że formalne uprawnienie powołania pozostaje w gestii Prezesa Rady Ministrów, lecz jest ograniczone listą kandydatów uprzednio zarekomendowanych przez Ministra. Pięcioletnia kadencja, połączona z możliwością jednokrotnego, ponownego wyboru, stanowi istotną część instrumentarium gwarancji niezależności organu[37].

Odwołanie Prezesa PAA przed upływem kadencji jest dopuszczalne wyłącznie w sześciu enumeratywnie wymienionych w art. 109 ust. 2b Prawa atomowego przypadkach. Należą do nich rażące naruszenie prawa przez osobę sprawującą urząd, skazanie prawomocnym wyrokiem za umyślne przestępstwo lub przestępstwo skarbowe, orzeczenie zakazu zajmowania kierowniczych stanowisk lub pełnienia funkcji związanych ze szczególną odpowiedzialnością w organach państwa, choroba trwale uniemożliwiająca wykonywanie zadań, rezygnacja ze sprawowania funkcji do końca kadencji oraz odmowa zaakceptowania przez Prezesa Rady Ministrów sprawozdania rocznego z działalności organu wraz z oceną stanu bezpieczeństwa jądrowego i ochrony radiologicznej kraju. Sprawozdanie roczne, którego treść została unormowana w art. 110 Prawa atomowego, obejmuje szczegółowe informacje o działalności organu, w tym o stanie bezpieczeństwa jądrowego, ochrony radiologicznej, nadzorze nad obiektami jądrowymi, ochronie materiałów jądrowych oraz ocenie sytuacji radiacyjnej państwa.

Szczególną wątpliwość wzbudza ostatnia z wymienionych przesłanek odwołania. Ustawodawca nie określił bowiem metodologii ani kryteriów merytorycznych, na podstawie których Prezes Rady Ministrów dokonuje oceny sprawozdania. Brak ustawowej definicji przesłanek do odmowy zaakceptowania sprawozdania prowadzi do daleko idącego luzu decyzyjnego, którego logiczną konsekwencją jest możliwość arbitralnego zastosowania tej przesłanki w celu odwołania urzędującego Prezesa PAA. W doktrynie zwracano uwagę, że konstrukcja ta stwarza pole do potencjalnej politycznej ingerencji w działalność organu, którego niezależność stanowi, w świetle prawa międzynarodowego niezbędny warunek skutecznej realizacji jego zadań[38]. Zastrzeżenia te są tak ważne, gdyż cała architektura ustrojowa Prezesa PAA została zaprojektowana z myślą o zapewnieniu mu daleko idącej niezależności, a otwarta przesłanka odwołania istotnie te gwarancje osłabia.

Prezes PAA nie podlega żadnemu ministrowi na zasadach kierownictwa. Nie oznacza to wszakże, że organ ten pozostaje poza wszelkim nadzorem ze strony władzy wykonawczej. Nadzór ten sprawuje Minister właściwy do spraw klimatu[39], przy czym jego treść jest stosunkowo ograniczona. Nadzór Ministra przejawia się przede wszystkim w nadawaniu statutu PAA, w udziale w procedurze powoływania Prezesa PAA przez Prezesa Rady Ministrów (który na mocy ustawy ma możliwość określenia szczegółowego zakresu działania w drodze rozporządzenia), w powoływaniu i odwoływaniu, na wniosek Prezesa PAA, wiceprezesów Agencji oraz w wyznaczaniu wiceprezesa pełniącego obowiązki w okresie *sede vacante*. Ponadto Minister opracowuje, na podstawie wniosków z analiz krajowego sprawozdania z przeglądu obiektów jądrowych, krajowy plan działań w zakresie podniesienia poziomu bezpieczeństwa jądrowego (art. 35a ust. 17-19 Prawa atomowego), zobowiązujący Prezesa PAA do podjęcia określonych działań służących zapewnieniu bezpieczeństwa jądrowego[40].

W doktrynie reprezentowane jest stanowisko, w myśl którego aktualny model nadzoru resortowego nad Prezesem PAA wymaga reformy polegającej na przeniesieniu tego nadzoru z poziomu Ministra na poziom Prezesa Rady Ministrów. Argumenty na rzecz takiego rozwiązania mają charakter zarówno historyczny (w okresie przed 1999 roku Prezes PAA pozostawał w bezpośredniej zależności od Prezesa Rady Ministrów), jak i systemowy. Przywrócenie nadzoru Prezesa Rady Ministrów zwiększyłoby ustrojową rangę regulatora, zminimalizowałoby ryzyko subordynacji wobec interesów resortowych oraz znalazłoby uzasadnienie w międzynarodowych przepisach, standardach i praktyce kładących nacisk na niezależność organów regulacyjnych w zakresie bezpieczeństwa jądrowego[41].

Drugim atrybutem ustrojowym Prezesa PAA, jak wskazano powyżej, jest naczelność. Atrybut ten wymaga

37 IAEA, Safety Standards Series No. SF-1: Fundamental Safety Principles, Wiedeń 2006, s. 7–8.

38 T. R. Nowacki, Ograniczenie autonomii Prezesa Państwowej Agencji Atomistyki..., s. 65; T. R. Nowacki, Niezależność organów dozoru jądrowego..., s. 258–260.

39 W latach 1982–1986 Państwowa Agencja Atomistyki podlegała Prezesowi Rady Ministrów; w latach 1986-1999 Prezes PAA pozostawał w analogicznej zależności; od 1999 r. nadzór sprawują kolejno minister właściwy do spraw gospodarki, minister właściwy do spraw środowiska (2001–2020), a obecnie minister właściwy do spraw klimatu. Zob. T. R. Nowacki, Niezależność organów dozoru jądrowego..., s. 204–207.

40 Działania są realizowane za sprawą aparatu Prezesa PAA.

41 T. R. Nowacki, Organy dozoru jądrowego w strukturze administracji rządowej w Polsce..., s. 9–38.

osobnego rozważenia, gdyż jego współczesne znaczenie odbiega od historycznie utrwalonego pojęcia organów naczelnych administracji państwowej. Pod rządami konstytucji z 1952 roku[42] organy naczelne stanowiły wyodrębnioną kategorię ustrojową obejmującą Radę Ministrów oraz ministerstwa. W tekście obecnej konstytucji zrezygnowano z tej kategorii, zastępując ją pojęciem centralnych organów państwowych. Pomimo tej zmiany w niektórych ustawach zwykłych zachowało się pojęcie organów naczelnych, w tym w Prawie atomowym, którego art. 64 ust. 1 pkt 1 określa Prezesa PAA jako naczelny organ dozoru jądrowego.

Współcześnie pojęcie organu naczelnego należy odczytywać w świetle art. 18 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[43]. Przepis ten przewiduje trojaką kwalifikację organów naczelnych. W stosunku do organów administracji rządowej, organów jednostek samorządu terytorialnego (z wyłączeniem samorządowych kolegiów odwoławczych) oraz organów państwowych i samorządowych jednostek organizacyjnych naczelnymi organami są Prezes Rady Ministrów lub właściwi ministrowie. Wobec innych organów państwowych niż wymienione wyżej organami naczelnymi są organy o ogólnokrajowym zasięgu działania. Analogicznie, w stosunku do organów organizacji społecznych są to naczelne organy tych organizacji, a w sytuacji ich braku Prezes Rady Ministrów lub właściwy minister sprawujący nadzór nad ich działalnością.

W przypadku Prezesa PAA naczelność nie oznacza zatem członkostwa w Radzie Ministrów, lecz dzięki wynikającemu z ustawy ogólnokrajowemu zasięgowi działania przesądza o jego węzłowej roli w pionie dozoru jądrowego. Atrybut ten ma charakter funkcjonalny. Jest to rola koordynacyjna oraz rozstrzygająca, która w praktyce eliminuje istnienie organu wyższego stopnia w znaczeniu administracyjnym wobec Prezesa PAA. Środkami weryfikacji decyzji Prezesa PAA pozostają wyłącznie wniosek o ponowne rozpatrzenie sprawy do tego samego organu (art. 127 § 3 k.p.a.) oraz skarga do sądu administracyjnego. Z drugiej strony Prezes PAA pozostaje organem wyższego stopnia względem inspektorów dozoru jądrowego, co zapewnia jednolitość praktyki dozorowej oraz spójność metodyczną realizowanych przez nich czynności. Do istoty pojęcia organu naczelnego należy również jego usytuowanie na czele określonej struktury organizacyjnej w ramach administracji rządowej[44].

Konstrukcja ustrojowa, w której Prezes PAA łączy atrybut centralności z atrybutem naczelności, znajduje swoje uzasadnienie w międzynarodowych zaleceniach z zakresu bezpieczeństwa jądrowego. Punktem odniesienia są tu zalecenia (*safety standards*) Międzynarodowej Agencji Energii Atomowej (MAEA), stanowiące najistotniejszy element międzynarodowego *soft law* w dziedzinie bezpieczeństwa jądrowego i ochrony radiologicznej. Choć formalnie nie mają one charakteru wiążącego, w praktyce pełnią funkcję powszechnie uznawanego wzorca, do którego państwa dostosowują swoje rozwiązania krajowe i na podstawie którego prowadzone są międzynarodowe przeglądy ram regulacyjnych[45]. To właśnie w tych dokumentach zaleca się utworzenie organu regulacyjnego cechującego się odpowiednim autorytetem, zasobami oraz kompetencjami, którego niezależność w decyzjach dotyczących bezpieczeństwa jądrowego i ochrony radiologicznej nie podlegałaby niedozwolonej presji ze strony interesariuszy[46]. Polski model ustrojowy, łączący kompetencje horyzontalne (koordynacyjne) z kompetencjami wertykalnymi (kierowniczymi w pionie dozoru jądrowego), realizuje to zalecenie poprzez koncentrację władzy regulacyjnej w jednym, monokratycznym organie centralnym.

Inspektorzy dozoru jądrowego jako konkretyzacja naczelności Prezesa PAA

Atrybut naczelności Prezesa PAA znajduje swoją praktyczną konkretyzację w relacji organ wyższego stopnia – organ niższego stopnia, łączącej Prezesa PAA z inspektorami dozoru jądrowego (dalej: inspektorzy). Inspektorzy są organami dozoru jądrowego wspólnie z Prezesem PAA tworzącymi strukturę dozoru jądrowego w Polsce (art. 64 ust. 1 Prawa atomowego)[47]. Podstawowym zadaniem inspektorów jest podejmowanie czynności kontrolnych oraz nadzorczych w celu poprawy stanu bezpieczeństwa jądrowego lub ochrony radiologicznej w kontrolowanych jednostkach organizacyjnych wykonujących działalność z narażeniem na promieniowanie jonizujące. Czynności kontrolne inspektorów obejmują kontrole prowadzone w obiektach jądrowych oraz w jednostkach organizacyjnych posiadających materiały jądrowe, źródła promieniowania jonizującego, odpady promieniotwórcze i wypalone paliwo jądrowe (art. 64 ust. 4 pkt 1-2 Prawa atomowego). Czynnościami nadzorczymi realizowanymi przez inspek-

42 Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 r (Dz.U. z 1952 r. nr 33 poz. 232).
43 Dz.U. z 2025 r. poz. 1691.
44 P. M. Przybysz, art. 18, [w:] Kodeks postępowania administracyjnego. Komentarz aktualizowany, LEX/el. 2025.
45 Zob. T. R. Nowacki, *Możliwość uznania standardów bezpieczeństwa MAEA za źródło prawa w świetle Konstytucji Rzeczypospolitej Polskiej* (w:) P. Kapusta et. al. (red.), *Księga pamiątkowa w czterdziestolecie pracy naukowej prof. B. Banaszaka*, Legnica 2017, s. 639–659.
46 Zob. *Fundamental Safety Principles*, IAEA Safety Standards Series No. SF-1 (Safety Fundamentals) IAEA, Wiedeń 2006 (3.3, 3.10, 3.11); *Governmental, Legal and Regulatory Framework for Safety*, IAEA Safety Standards Series No. GSR Part 1 (Rev. 1) (General Safety Requirements), IAEA, Wiedeń 2016 (2.7, 2.8d, 2.9-11, 2.18, 4.6, 4.9, 4.20-21).
47 Więcej na ten temat:. T. Białkowski, Infrastruktura dozoru jądrowego w Polsce, [w:] Biuletyn Informacyjny Państwowej Agencji Atomistyki 2(92)/2013, (red.) T. Białkowski, Warszawa 2013, s. 3.

torów jest natomiast wydawanie decyzji dozorowych, których adresatami pozostają podmioty prowadzące działalność z narażeniem na promieniowanie jonizujące.

Ustawa Prawo atomowe wyodrębnia trzy kategorie inspektorów dozoru jądrowego, różniące się zakresem przysługujących im uprawnień. Inspektorzy I stopnia, na podstawie art. 64 ust. 1 pkt 3 lit. a Prawa atomowego, posiadają uprawnienie do przeprowadzania czynności nadzorczych w jednostkach organizacyjnych prowadzących działalność objętą ochroną radiologiczną. Wyłączeniu z ich kompetencji podlegają jednostki zajmujące się wytwarzaniem, przetwarzaniem, przechowywaniem, transportowaniem lub stosowaniem materiałów jądrowych, materiałów promieniotwórczych lub źródeł promieniotwórczych, a także jednostki wykonujące działalność w zakresie budowy, rozruchu, eksploatacji lub likwidacji obiektów jądrowych oraz składowisk odpadów promieniotwórczych. W konsekwencji inspektorzy I stopnia są właściwi dla podmiotów prowadzących typową działalność związaną z narażeniem na promieniowanie jonizujące w sektorach medycyny, przemysłu, badań naukowych oraz pochodnych im obszarów.

Inspektorzy II stopnia, na podstawie art. 64 ust. 1 pkt 3 lit. b prawa atomowego, dysponują uprawnieniami do przeprowadzania czynności nadzorczych we wszystkich jednostkach organizacyjnych prowadzących działalność związaną z ryzykiem narażenia na promieniowanie jonizujące. Oznacza to, że obejmują oni swoją właściwością podmioty objęte zakresem działania inspektorów I stopnia, a dodatkowo również jednostki prowadzące działalność w zakresie obiektów jądrowych oraz składowisk odpadów promieniotwórczych. Wyłączeniu z kompetencji inspektorów II stopnia podlega jedynie kontrola technologii jądrowych (w rozumieniu art. 40 pkt 4 Prawa atomowego) oraz zabezpieczeń materiałów jądrowych, która stanowi wyłączną właściwość inspektorów dozoru jądrowego do spraw zabezpieczeń (art. 64 ust. 1a Prawa atomowego).

Inspektorzy do spraw zabezpieczeń, których normatywną podstawę działania stanowi art. 64 ust. 1 pkt 3 lit. c Prawa atomowego, są uprawnieni wyłącznie do wykonywania czynności w zakresie kontroli technologii jądrowych i zabezpieczeń materiałów jądrowych. Przedmiotowy zakres ich kompetencji jest zatem wąski, lecz dotyczy obszaru o szczególnym znaczeniu dla międzynarodowego reżimu nieproliferacji broni jądrowej, w którym Polska pozostaje stroną stosownych zobowiązań, w tym traktatowych. Wyodrębnienie tej kategorii inspektorów stanowi przejaw dostosowania krajowej struktury organów dozoru do wymogów wynikających z systemu zabezpieczeń materiałów jądrowych MAEA oraz z odpowiednich rozporządzeń Komisji Europejskiej[48].

Status inspektora dozoru jądrowego wymaga spełnienia kwalifikacyjnych wymogów określonych w art. 65 Prawa atomowego oraz w rozporządzeniu Rady Ministrów z dnia 11 sierpnia 2021 r. w sprawie inspektorów dozoru jądrowego[49]. Inspektorem może zostać osoba posiadająca wykształcenie wyższe w zakresie fizyki, chemii, kierunków technicznych lub innych w specjalnościach przydatnych w dozorze jądrowym, niekarana za przestępstwa umyślne, dysponująca orzeczeniem lekarskim o braku przeciwwskazań do pracy w warunkach narażenia, która odbyła wymaganą prawem praktykę i zdała egzamin kwalifikacyjny.

Wymóg odbycia praktyki został zróżnicowany w zależności od kategorii inspektora. Kandydat na inspektora I stopnia musi odbyć co najmniej dziewięciomiesięczne praktyki, w tym przez co najmniej trzy miesiące w organizacjach prowadzących działalność związaną z narażeniem na promieniowanie jonizujące (§ 2 ust. 1 rozporządzenia inspektorskiego). Kandydat na inspektora II stopnia musi odbyć co najmniej piętnastomiesięczne praktyki, w tym co najmniej trzy miesiące w organizacjach polskich lub zagranicznych prowadzących działalność w zakresie budowy, rozruchu, eksploatacji, zamknięcia lub likwidacji obiektów jądrowych lub składowisk odpadów promieniotwórczych albo w zagranicznych urzędach dozoru jądrowego, a także co najmniej trzy miesiące w organizacjach prowadzących pozostałe rodzaje działalności reglamentowanej (§ 2 ust. 3 rozporządzenia inspektorskiego). Kandydat na inspektora do spraw zabezpieczeń musi natomiast odbyć co najmniej sześciomiesięczne praktyki, w tym co najmniej dwa miesiące w organizacjach polskich lub zagranicznych podlegających wymogom zabezpieczenia materiałów jądrowych lub w zagranicznych urzędach dozoru jądrowego, MAEA lub KE (§ 2 ust. 4 rozporządzenia inspektorskiego).

Pozostałą część praktyki kandydaci odbywają w PAA. Część praktyki realizowana poza PAA odbywa się na podstawie umów zawieranych przez Prezesa PAA z odpowiednimi organizacjami (§ 3 rozporządzenia inspektorskiego). Przebieg praktyki jest dokumentowany w dzienniku praktyki, na podstawie którego Prezes PAA stwierdza prawidłowe jej odbycie (§ 4 rozporządzenia inspektorskiego). W określonych w art. 65 ust. 4 Prawa atomowego przypadkach Prezes PAA może zwolnić kandydata – w całości lub w części – z obowiązku odbycia praktyki, w szczególności gdy przez ostatnie dwa lata pełnił on funkcję inspektora ochrony radiologicznej lub przez ostatnie pięć lat był zatrudniony w warunkach narażenia w organizacji wykonującej działalność reglamentowaną. Po odbyciu praktyki kandydat przystępuje do egzaminu kwalifikacyjnego, składającego się z części pisemnej oraz ustnej. Pozytywny wynik egzaminu jest potwierdzany

[48] Dalej: KE.

[49] Rozporządzenie Rady Ministrów z dnia 11 sierpnia 2021 r. w sprawie inspektorów dozoru jądrowego (Dz.U. z 2021 r. poz. 1577, dalej: rozporządzenie inspektorskie).

zaświadczeniem wydawanym przez przewodniczącego komisji egzaminacyjnej.

Powyższy zarys regulacji uprawnień, kwalifikacji oraz procedury obsadzania stanowiska inspektora dozoru jądrowego pozwala na sformułowanie centralnej tezy dotyczącej naczelności Prezesa PAA. Naczelność ta materializuje się w zespole kompetencji kierowniczych oraz nadzorczych Prezesa PAA wobec inspektorów. Po pierwsze, Prezes PAA jest organem wyłącznie uprawnionym do powoływania oraz odwoływania inspektorów (art. 64 ust. 3 Prawa atomowego). Po drugie, Prezes PAA uzgadnia program szkolenia kandydatów na inspektorów (art. 65 ust. 10 Prawa atomowego). Po trzecie, Prezes PAA dysponuje kompetencją do zwalniania kandydatów z obowiązku odbycia praktyki w określonych prawem przypadkach. Po czwarte, Prezes PAA stwierdza prawidłowość odbycia praktyki na podstawie dziennika praktyki. Po piąte, Prezes PAA zawiera umowy z organizacjami zewnętrznymi, w których odbywa się część praktyki kandydatów. Po szóste – i najistotniejsze – Prezes PAA pozostaje organem wyższego stopnia w rozumieniu art. 17 oraz art. 127 § 2 k.p.a. względem inspektorów, co przesądza o jego pozycji w zakresie rozpatrywania środków zaskarżenia od decyzji wydawanych przez inspektorów. Ostateczny nadzór Prezesa PAA nad działaniami inspektorów stanowi zatem konsekwencję jego naczelności, która w tym kontekście nabiera wymiaru praktycznego, daleko wykraczającego poza formalną deklarację ustawową.

Konsekwentny charakter konstrukcji ustrojowej, w której Prezes PAA odgrywa rolę organu wyższego stopnia względem inspektorów, znalazł swoje wzmocnienie w nowelizacji Prawa atomowego z 2014 r. Ustawą z dnia 4 kwietnia 2014 r. o zmianie ustawy – Prawo atomowe oraz niektórych innych ustaw[50] zlikwidowano funkcję Głównego Inspektora Dozoru Jądrowego, który dotychczas odgrywał rolę ogniwa pośredniego pomiędzy Prezesem PAA, a inspektorami dozoru jądrowego. W jego miejsce wprowadzono bezpośrednią relację Prezes PAA – inspektorzy, w której kompetencje uprzednio przypisane Głównemu Inspektorowi zostały przeniesione na Prezesa PAA[51]. Zmiana ta stanowiła konsekwentny krok w kierunku uproszczenia struktury organów dozoru jądrowego oraz wzmocnienia bezpośredniej naczelności Prezesa PAA. W literaturze przedmiotu zwraca się uwagę, że historyczna ewolucja organów dozoru jądrowego w Polsce konsekwentnie zmierzała do koncentracji władzy nadzorczej w jednym organie centralnym, co znajduje uzasadnienie w przepisach prawa międzynarodowego, jak i w doświadczeniach innych państw[52].

Inspektorów dozoru jądrowego nie należy mylić z inspektorami ochrony radiologicznej, których status prawny został unormowany w art. 7 ust. 3 Prawa atomowego. Pomimo zbieżnej nazwy są to dwie odmienne kategorie podmiotów, różniące się przede wszystkim usytuowaniem w krajowym systemie bezpieczeństwa jądrowego i ochrony radiologicznej. Inspektor dozoru jądrowego jest państwowym organem dozoru jądrowego, sprawującym zewnętrzny nadzór nad jednostką organizacyjną prowadzącą działalność reglamentowaną. Inspektor ochrony radiologicznej natomiast jest osobą sprawującą wewnętrzny nadzór nad przestrzeganiem wymagań ochrony radiologicznej w jednostce organizacyjnej wykonującej działalność reglamentowaną w zakresie sektora energii jądrowej[53]. Inspektor ochrony radiologicznej jest zatem pracownikiem jednostki organizacyjnej, nie zaś organem administracji państwowej.

Wymogi kwalifikacyjne dla inspektora ochrony radiologicznej są zdecydowanie mniej rygorystyczne niż w przypadku inspektora dozoru jądrowego. Inspektorem ochrony radiologicznej może zostać osoba mająca pełną zdolność do czynności prawnych, posiadająca co najmniej wykształcenie średnie lub średnie branżowe, dysponująca orzeczeniem lekarskim o braku przeciwwskazań do pracy w warunkach narażenia, która odbyła odpowiednie szkolenie, zdała egzamin nie wcześniej niż dwa lata przed dniem złożenia wniosku oraz posiada odpowiedni do typu nadanych uprawnień staż pracy (art. 7 ust. 6 Prawa atomowego). Organem właściwym do nadania uprawnień inspektora ochrony radiologicznej również pozostaje Prezes PAA, a formą prawną tej czynności jest decyzja administracyjna. Tę szczególną konstrukcję – powierzenie Prezesowi PAA kompetencji do nadawania uprawnień podmiotom usytuowanym wewnętrznie w jednostkach organizacyjnych, a więc poza strukturą administracji państwowej – należy odczytać jako kolejne wzmocnienie jego pozycji jako naczelnego organu, oddziałującego nie tylko na zewnętrzną strukturę dozoru, lecz również na wewnętrzny system kontroli realizowanej w samych podmiotach prowadzących działalność reglamentowaną.

Podsumowanie

Przeprowadzona analiza pozycji ustrojowej Prezesa PAA w kontekście jego naczelności pozwala na pozytywną weryfikację hipotezy postawionej we wprowadzeniu, choć konieczne jest opatrzenie tego wniosku istotnymi zastrzeżeniami systemowymi. Model ustrojowy łączący w jednym

50 Dz.U. z 2014 r. poz. 587.

51 Więcej na ten temat: M. Gąszczyk, Nowelizacja prawa atomowego. Likwidacja funkcji Głównego Inspektora Dozoru Jądrowego, [w:] Bezpieczeństwo Jądrowe i Ochrona Radiologiczna 2/2014, (red.) M. Woźniak, Warszawa 2014, s. 7–9.

52 T. R. Nowacki, Niezależność organów dozoru jądrowego..., s. 204; Zob. także T. R. Nowacki, Ewolucja prawnego statusu organów nadzorujących bezpieczeństwo wykorzystania energii jądrowej w Polsce, [w:] Zeszyty Prawnicze 18(3)/2018, (red.) J. Zabłocki, Warszawa 2018, s. 142.

53 Więcej: w Ł. Młynarkiewicz, Prawne i organizacyjne aspekty nadzoru wewnętrznego inspektora ochrony radiologicznej, [w:] Bezpieczeństwo Jądrowe i Ochrona Radiologiczna 4/2025, (red.) M. Jurkowski, Warszawa 2025, s. 24.

organie atrybut centralności w sprawach bezpieczeństwa jądrowego i ochrony radiologicznej z atrybutem naczelności w pionie dozoru jądrowego stanowi adekwatną konstrukcję prawną do skutecznej realizacji dozoru jądrowego. O adekwatności tej przesądzają spójność wertykalna systemu dozoru, jednolitość praktyki dozorowej, koncentracja kompetencji władczych w jednym organie monokratycznym oraz zgodność konstrukcji z międzynarodowymi regulacjami. Sprzężenie kompetencji horyzontalnych, charakterystycznych dla centralnego organu administracji rządowej, z kompetencjami wertykalnymi, charakterystycznymi dla organu naczelnego w rozumieniu art. 18 k.p.a., tworzy konstrukcję, w której Prezes PAA zajmuje pozycję na szczycie pionu dozoru jądrowego oraz jest krajowym punktem styku dla wszystkich spraw związanych z bezpieczeństwem jądrowym, ochroną radiologiczną oraz ochroną fizyczną.

Pomimo pozytywnej oceny ogólnego modelu, analiza ujawniła mankamenty związane z możliwością wystąpienia ryzyka upolitycznienia organu, wynikające z konstrukcji odwołania uregulowanej w art. 109 ust. 2b Prawa atomowego. Otwarta przesłanka odwołania, polegająca na odmowie zaakceptowania przez Prezesa Rady Ministrów rocznego sprawozdania z działalności organu, pozbawiona ustawowo zdefiniowanych kryteriów merytorycznych, stwarza pole do potencjalnej politycznej ingerencji, niezgodnej z międzynarodowymi standardami niezależności organów regulacyjnych. Postulat *de lege ferenda* powinien zatem zmierzać do doprecyzowania przesłanek odmowy zaakceptowania sprawozdania. Niezależnie od tej konkretnej przesłanki należy się zgodzić z poglądami wyrażonymi w doktrynie na temat przeniesienia nadzoru nad Prezesem PAA z poziomu ministra bezpośrednio na poziom Prezesa Rady Ministrów, co wzmocniłoby ustrojową rangę organu oraz zminimalizowałoby ryzyko subordynacji organu wobec interesów resortowych.

Notka o autorze

Artur J. Tyński – doktorant w Szkole Doktorskiej Uniwersytetu Śląskiego w Katowicach w obszarze nauk prawnych. Asystent badawczy w Katedrze Maszyn i Urządzeń Energetycznych na Wydziale Inżynierii Środowiska i Energetyki Politechniki Śląskiej w Gliwicach. Absolwent Kolegium Indywidualnych Studiów Międzyobszarowych UŚ (prawo, filozofia). Alumn International School of Nuclear Law odbywającej się na Universite de Montpellier;
email: tynski.artur@gmail.com.

Literatura

1. Banasik M., *Administracyjnoprawne formy działań regulacyjnych niezależnych organów administracji publicznej*, Warszawa 2019.
2. Barczak-Oplustil A., Sroka T. (red.), *Odpowiedzialność publicznoprawna*. System Prawa Medycznego. Tom 6, Warszawa 2023.
3. Białkowski T., *Infrastruktura dozoru jądrowego w Polsce*, [w:] Biuletyn Informacyjny Państwowej Agencji Atomistyki 2(92)/2013, (red.) T. Białkowski, Warszawa 2013.
4. Dolnicki B., *Nadzór nad samorządem terytorialnym*, Katowice 1993.
5. Gąszczyk M., *Nowelizacja prawa atomowego. Likwidacja funkcji Głównego Inspektora Dozoru Jądrowego*, [w:] Bezpieczeństwo Jądrowe i Ochrona Radiologiczna 2/2014, (red.) M. Woźniak, Warszawa 2014.
6. Goss M., *Nadzór i regulacja sektora ropy i gazu*, Warszawa 2016.
7. Gronkiewicz-Waltz H., Wierzbowski M., Szafrański A., *Prawo gospodarcze. Aspekty publicznoprawne*, Warszawa 2025.
8. Hauser R., Niewiadomski Z., Wróbel A. (red.), *Publiczne prawo gospodarcze.* System Prawa Administracyjnego. Tom 8A, Warszawa 2018.
9. Hauser R., Niewiadomski Z., Wróbel A.(red.), *Konstytucyjne podstawy funkcjonowania administracji publicznej.* System Prawa Administracyjnego. Tom 2, Warszawa 2012.
10. Kocowski T., *Reglamentacja działalności gospodarczej w polskim prawie administracyjnym*, Warszawa 2009.
11. Michalik S., Zieliński D., *Transformacja energetyczna w Polsce w świetle strategicznych dokumentów rządowych*, Warszawa 2024.
12. Młynarkiewicz Ł., *Prawne i organizacyjne aspekty nadzoru wewnętrznego inspektora ochrony radiologicznej*, [w:] Bezpieczeństwo Jądrowe i Ochrona Radiologiczna 4/2025, (red.) M. Jurkowski, Warszawa 2025.
13. Nowacki T. R., *Organy dozoru jądrowego w strukturze administracji rządowej w Polsce*, [w:] Zeszyty Prawnicze Biura Analiz Sejmowych 1(69)/2021, Warszawa 2021.
14. Nowacki T. R., *Ewolucja prawnego statusu organów nadzorujących bezpieczeństwo wykorzystania energii jądrowej w Polsce*, [w:] Zeszyty Prawnicze 18(3)/2018, (red.) J. Zabłocki, Warszawa 2018.
15. Nowacki T. R., *Ograniczenie autonomii Prezesa Państwowej Agencji Atomistyki*, [w:] Przegląd Sejmowy 4(147)/2018, Warszawa 2018.
16. Nowacki T. R., *Możliwość uznania standardów bezpieczeństwa MAEA za źródło prawa w świetle Konstytucji Rzeczypospolitej Polskiej* (w:) P. Kapusta et. al. (red.), Księga pamiątkowa w czterdziestolecie pracy naukowej prof. B. Banaszaka, Legnica 2017.
17. Nowacki T. R., *Niezależność organów dozoru jądrowego na tle prawa międzynarodowego, europejskiego i konstytucyjnego*, Wrocław 2015.
18. Nowacki T. R., *Prawne gwarancje niezależności dozoru jądrowego w Polsce* (w:) I. Ramus (red.), Obrót powszechny i gospodarczy. Problemy publicznoprawne i ekonomiczne, Kielce 2014.
19. Nowacki T. R., *Niezależność organów dozoru jądrowego. Próba rekonstrukcji zakresu pojęciowego* (w:) K. Jeleń, Z. Rau (red.), Energetyka jądrowa w Polsce, Warszawa 2012.
20. Powałowski A., *Leksykon prawa gospodarczego publicznego*, Warszawa 2019.
21. Piecha J., *Sprzeciw w prawie administracyjnym*, Warszawa 2016.
22. Przybysz P. M., Art. 18, [w:] *Kodeks postępowania administracyjnego.* Komentarz aktualizowany, LEX/el. 2025.
23. Snażyk Z., Szafrański A., *Publiczne prawo gospodarcze*, Warszawa 2021.
24. Strupczewski A., *Energetyka jądrowa koniecznym elementem elektroenergetyki polskiej*, [w:] Academia – Magazyn Polskiej Akademii Nauk 1(65)/2021, Warszawa 2021.
25. Strzyczkowski K., *Prawo gospodarcze publiczne*, Warszawa 2011.
26. Szreniewski J., *Prawo administracyjne. Część ogólna*, Lublin 1993.
27. Swora M., *Niezależne organy administracji*, Warszawa 2012.
28. Ziemacki Z., *Europejski Zielony Ład i odbudowa gospodarki – szanse i wyzwania*, [w:] Sprawy Międzynarodowe 3/2021, Warszawa 2021.
29. Zimmermann J., *Prawo administracyjne*, Warszawa 2022.

Legislacja

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm., dalej: Konstytucja RP).
2. Konwencja Bezpieczeństwa Jądrowego, sporządzona w Wiedniu dnia 20 września 1994 r. (Dz.U. z 1997 r. Nr 42, poz. 262).
3. Dyrektywa Rady 2009/7/Euratom z 25.06.2009 r. ustanawiająca wspólnotowe ramy bezpieczeństwa obiektów jądrowych.

4. Ustawa z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz. U. z 2026 r. poz. 68; dalej: Ustawa OZE).
5. Ustawa z dnia 4 kwietnia 2014 r. o zmianie ustawy – Prawo atomowe oraz niektórych innych ustaw (Dz.U. z 2014 r. poz. 587).
6. Ustawa z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz.U. z 2025 r. poz. 1156).
7. Ustawa z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz.U. z 2024 r. poz. 1194, dalej: ustawa o dozorze technicznym)
8. Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe (Dz.U. z 2026 r. poz. 1).
9. Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz.U. z 2026 poz. 46, 516, 607).
10. Ustawa z dnia 10 kwietnia 1986 r. – Prawo atomowe (Dz.U. z 1986 r. nr 12 poz. 70 ze zm).
11. Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2025 r. poz. 1691).
12. Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dniu 22 lipca 1952 r (Dz.U. z 1952 r. nr 33 poz. 232).
13. Rozporządzenie Rady Ministrów z dnia 11 sierpnia 2021 r. w sprawie inspektorów dozoru jądrowego (Dz.U. z 2021 r. poz. 1577, dalej: rozporządzenie inspektorskie).
14. Polityka Energetyczna Polski do 2040 r. przyjęta uchwałą Rady Ministrów nr 22/2021 z dnia 2 lutego 2021 r. ogłoszona Obwieszczeniem Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r. (M.P. z 2021 r. poz. 264).
15. Program polskiej energetyki jądrowej przyjęty uchwałą Rady Ministrów nr 141 z dnia 2 października 2020 r. w sprawie aktualizacji programu wieloletniego pod nazwą „Program polskiej energetyki jądrowej" (M.P. z 2020 r. poz. 946).
16. Komisja Europejska, Europejski Zielony Ład, COM(2019) 640, Bruksela 2019, https://eur-lex.europa.eu/resource.html?uri=cellar:b828d165-1c22-11ea-8c1f-01aa75ed71a1.0016.02/DOC_1&format=PDF, [dostęp: 10.09.2025]
17. IAEA Safety Standards Series No. GSR Part 1 (Rev. 1), Wiedeń 2016.
18. IAEA, Safety Standards Series No. SF-1: Fundamental Safety Principles, Wiedeń 2006.

Inne źródła

1. Polskie Sieci Elektroenergetyczne, Raport 2024 KSE: Zestawienie danych ilościowych dotyczących funkcjonowania KSE w 2024 roku, https://www.pse.pl/dane-systemowe/funkcjonowanie-kse/raporty-roczne-z-funkcjonowania-kse-za-rok/raporty-za-rok-2024, [dostęp: 01.10.2025].
2. Prezes PAA, Raport Roczny 2024. Działalność Prezesa Państwowej Agencji Atomistyki oraz ocena stanu bezpieczeństwa jądrowego i ochrony radiologicznej w Polsce w 2024 r. Warszawa 2025.
3. Prezes PAA, Raport Roczny 2025. Działalność Prezesa Państwowej Agencji Atomistyki oraz ocena stanu bezpieczeństwa jądrowego i ochrony radiologicznej w Polsce w 2025 r. Warszawa 2026.

Bierne (pasywne) systemy bezpieczeństwa reaktorów jądrowych

Passive nuclear reactor safety systems

Andrzej G. Chmielewski[1], Antoni Rożeń[2]
[1] *Instytut Chemii i Techniki Jądrowej, Warszawa*
[2] *Politechnika Warszawska, Wydział Inżynierii Chemicznej i Procesowej*

Streszczenie: Nowe projekty reaktorów coraz częściej wykorzystują bierne[1] (inaczej pasywne) elementy bezpieczeństwa w różnych celach, na przykład do chłodzenia rdzenia podczas przejściowych stanów pracy, awarii projektowych, a nawet ciężkich awarii. Również mogą być wykorzystane do chłodzenia obudowy bezpieczeństwa, przyjmując, że systemy pasywne są wysoce niezawodne i zmniejszają koszty związane z instalacją oraz konserwacją systemów wymagających stosowania wielu urządzeń, a także redundantnych źródeł zasilania. Jednym z ważnych zagadnień jest ocena niezawodności biernych systemów bezpieczeństwa. W odróżnieniu od systemów aktywnych, w których przepływ jest wymuszany przez urządzenia mechaniczne, ruch czynnika roboczego w systemach pasywnych wynika z istnienia gradientów wielkości fizycznych, takich jak temperatura, gęstość, ciśnienie oraz skład mieszaniny. Na całym świecie organy regulujące bezpieczeństwo jądrowe (organy dozoru bezpieczeństwa jądrowego) stoją przed istotnymi wyzwaniami w licencjonowaniu nowych biernych systemów bezpieczeństwa i nowych rozwiązań innowacyjnych projektów reaktorów.

Słowa kluczowe: Reaktory jądrowe, bierne systemy bezpieczeństwa, pasywne elementy, ocena niezawodności.

Abstract: *New reactor designs increasingly use passive safety systems for various purposes, for example, to cool down the core during transient operating conditions, design-basis accidents, and even severe accidents. They are also used to cool down the containment, assuming that passive systems are highly reliable and reduce costs associated with installing and maintaining systems that require multiple devices, as well as redundant power sources. Unlike active systems, in which the flow is forced by mechanical devices, the movement of the working medium in passive systems results from the existence of gradients of physical quantities, such as temperature, density, pressure, and mixture composition. One important issue is the assessment of the reliability of passive safety systems. Nuclear safety regulators worldwide face significant challenges in licensing new passive safety systems and new innovative design solutions for reactors.*

Keywords: *Nuclear reactors, passive safety systems, passive components, reliability assessment.*

1. Wstęp

Projekt elektrowni jądrowej musi uwzględniać specyficzne cechy lokalizacji, aspekty eksploatacyjne oraz przyszłe plany likwidacji, tak aby osiągnąć najwyższy poziom bezpieczeństwa. Obowiązkowa jest kompleksowa i dokładna ocena bezpieczeństwa, mająca na celu zapewnienie właściwej ochrony pracowników, społeczeństwa i środowiska. Celem projektu jest zapewnienie bezpiecznej i skutecznej pracy elektrowni jądrowej, minimalizując prawdopodobieństwo awarii i zapewniając, że ich skutki mogą być bezwzględnie ograniczone.

Głównym sposobem osiągnięcia tego celu jest podejście „obrony w głąb"(ang. *defence in depth*), polegające na wdrożeniu kolejnych i niezależnych poziomów ochrony. W odniesieniu do projektowania przepisy bezpieczeństwa wynikające z podejścia „obrony w głąb" obejmują: odpowiedni projekt uwzględniający charakterystykę lokalizacji i stosowanie wielu fizycznych barier uniemożliwiających uwolnienie substancji zawierających izotopy promienio-

[1] „element bierny" to określenie obowiązujące, przyjęte w polskich przepisach (zob. Dz.U. 2012 poz. 1048) w języku polskim są to synonimy.

twórcze. Niezbędne jest stosowanie rygorystycznych wymagań bezpieczeństwa i sprawdzonych praktyk inżynierskich w celu zapewnienia odpowiednich marginesów bezpieczeństwa oraz wysokiej niezawodności cech projektowych, które zachowują integralność tych barier.

Bierne systemy bezpieczeństwa, tzn. te, które wykorzystują siły występujące w naturze, takie jak grawitacja, różnice ciśnienia czy konwekcja naturalna, były już w części stosowane w elektrowniach jądrowych od wielu dziesięcioleci w celu realizacji funkcji bezpieczeństwa bez konieczności użycia aktywnego źródła energii. Tradycyjnie jednak stosowanie takich cech biernych, na przykład do zatrzymania pracy reaktora, było ograniczone, a systemy bezpieczeństwa w dużej mierze opierały się na aktywnych urządzeniach napędowych, np. silnikach elektrycznych.

Ostatnio jednak nowe projekty reaktorów coraz częściej wykorzystują bierne elementy bezpieczeństwa w różnych celach, na przykład do chłodzenia rdzenia podczas przejściowych stanów pracy, przewidywanych stanów eksploatacyjnych i awarii projektowych, a nawet ciężkich awarii. Wykorzystują je również do chłodzenia obudowy bezpieczeństwa, przyjmując, że systemy pasywne są wysoce niezawodne i zmniejszają koszty związane z instalacją oraz konserwacją systemów wymagających stosowania wielu urządzeń, w tym kosztownych pomp, silników i innych systemów, a także redundantnych źródeł zasilania. Jednak słabe gradienty napędowe wielu takich biernych elementów bezpieczeństwa, oparte na przykład na konwekcji naturalnej i małych różnicach ciśnienia, stanowią znaczące wyzwania dla projektowania i demonstracji bezpieczeństwa systemów biernych w szerokim zakresie warunków awarii, a także dodatkowych zdarzeń, które mogą być wywołane przez zagrożenia wewnętrzne lub zewnętrzne [1].

2. Nowe wyzwania dla regulatora bezpieczeństwa jądrowego

Naczelnym organem regulującym zasady bezpieczeństwa jądrowego i kontrolującym ich przestrzeganie w Polsce (naczelnym organem dozoru jądrowego, określanym dalej w skrócie jako regulator) jest Prezes Państwowej Agencji Atomistyki (PAA). PAA jest odpowiedzialna za nadzór i kontrolę zapewnienia bezpiecznego i zgodnego z przepisami wykorzystania tego źródła wytwarzania energii cieplnej i elektrycznej przez posiadacza zezwolenia na jego budowę i eksploatację. Regulatorzy bezpieczeństwa jądrowego na całym świecie stoją również przed istotnymi wyzwaniami w ocenie bezpieczeństwa nowych biernych systemów i nowych rozwiązań innowacyjnych projektów reaktorów. Aby wykazać niezawodność systemów biernych lub ich cech zapewnienia bezpieczeństwa eksploatacji reaktora, a także uwzględnić niezależność różnych poziomów „obrony w głąb”, zasadnicze znaczenie mają wymagania dotyczące projektowania, metod i narzędzi obliczeniowych do analiz zjawisk fizycznych, a również testów eksperymentalnych do weryfikacji.

Bezpieczeństwo jądrowe bloku musi być wykazane na wszystkich etapach całego jego okresu eksploatacji, a w szczególności w okresie przed załadunkiem paliwa jądrowego i rozpoczęciem jego eksploatacji. Należy przeprowadzić kompleksową ocenę bezpieczeństwa, obejmującą deterministyczne i probabilistyczne analizy bezpieczeństwa dla wypadków wewnętrznych i zdarzeń zewnętrznych, aby zapewnić warunki, w których wszystkie wymagania bezpieczeństwa, ustalone w projekcie, są spełnione i zgodne z odpowiednimi krajowymi oraz międzynarodowymi normami i przepisami prawa, a także warunkami zezwolenia.

Ze względu na fakt, że systemy bierne (ang. *Passive Safety Systems*) opierają się na siłach natury, można zmniejszyć liczbę aktywnych komponentów i (lub) systemów wspomagających. W związku z tym ilość źródeł awarii może zostać również zmniejszona. Jednak stosowanie takich systemów rodzi nowe pytania, na przykład dotyczące testowalności, określania niezawodności, specyfikacji wymaganych warunków brzegowych, zastosowania kodów cieplno-przepływowych oraz stosowalności koncepcji pojedynczej awarii. Dodatkowo bierny system bezpieczeństwa może zmienić rozumienie niektórych koncepcji „obrony w głąb”.

Dlatego istotne jest, aby regulatorzy dzielili się swoją wiedzą i omawiali, jak można przeprowadzić przegląd i ocenę systemów biernych w sposób dokładny. Jest to szczególnie ważne ze względu na to, że istniejące przepisy często były opracowywane dla elektrowni jądrowych (EJ) z zastosowanymi głównie aktywnymi systemami bezpieczeństwa.

Niektóre kraje przyjęły formalną definicję systemów pasywnych w swoim ramach regulacyjnych, podczas gdy inne kraje takiej definicji nie posiadają [2]. Definicje pasywnych systemów bezpieczeństwa (dla tych krajów, które posiadają taką formalną definicję) w pewnym stopniu różnią się w zależności od kraju (np. niektóre kraje zakładają istnienie ruchomych części jako cechę wyłącznie systemów aktywnych, podczas gdy inne kraje uważają, że ruchome części mogą należeć zarówno do systemów aktywnych, jak i pasywnych). Niemniej jednak ogólne rozumienie, czym jest system pasywny, jest podobne wśród wielu krajów. Ramowe przepisy regulacyjne w wielu krajach przedkładają stosowanie systemów pasywnych nad aktywnymi i kraje te wprowadziły wyraźne wymagania dotyczące ich stosowania. Inne kraje zachęcają do stosowania systemów pasywnych.

Jednakże nie istnieją różnice w traktowaniu regulacyjnym systemów niezależnie od tego, czy są one uznawane za pasywne, czy aktywne w krajach odpowiadających w następujących obszarach:

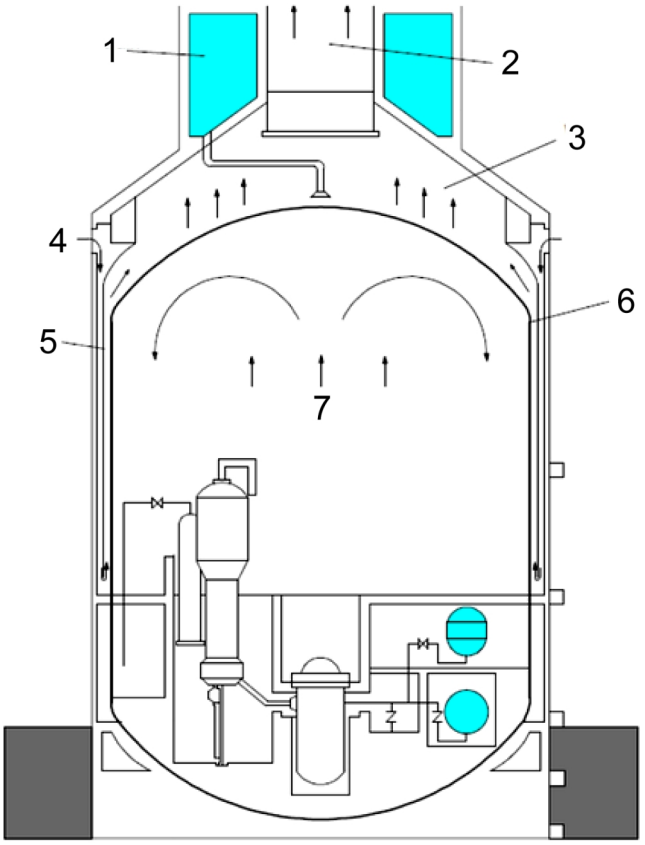
- dostarczanie opisów systemu w raporcie analizy bezpieczeństwa;
- zabezpieczenia przed naruszeniami ustawień eksploatacyjnych;

- ustalanie ograniczeń i warunków eksploatacyjnych;
- klasyfikacja bezpieczeństwa;
- ochrona przed zdarzeniami zewnętrznymi;
- identyfikacja i uwzględnianie awarii funkcjonalnych;
- uzasadnienie parametrów systemu;
- przyrządy i sterowanie;
- demonstracja maksymalnej liczby uruchomień pasywnego systemu bezpieczeństwa (w tym fałszywych uruchomień) oraz wzięcie pod uwagę okresu eksploatacji urządzeń i środowiska, w którym pracują;
- uwzględnienie fałszywych uruchomień i unieruchamiania systemu;
- testowanie podczas rozruchu;
- testowanie podczas eksploatacji.

Mimo to, że nie ma różnic w ramach regulacyjnych dotyczących zasad bezpieczeństwa jądrowego, które należy wykazać dla systemów aktywnych i biernych (pasywnych), warto zauważyć, że wykazanie wydajności systemów biernych (pasywnych) koncentruje się bardziej na uzasadnieniu eksperymentalnym. Jeśli istnieje możliwość wystąpienia negatywnych skutków w wyniku równoczesnego działania kilku biernych (pasywnych) systemów bezpieczeństwa jądrowego (lub ich ciągów), skutki te powinny zostać przeanalizowane i w razie potrzeby zweryfikowane eksperymentalnie [3].

3. Podstawowe siły i gradienty wykorzystywane w biernych (pasywnych) systemach bezpieczeństwa reaktorów jądrowych

Na rysunku 1 przedstawiono schematycznie niektóre elementy biernych (pasywnych) systemów bezpieczeństwa dla reaktora AP1000, jest to reaktor PWR zaprojektowany przez Westinghouse Electric Corporation. Stosuje on bierne (pasywne) systemy bezpieczeństwa, które opierają się na wykorzystaniu grawitacji, sprężonego gazu, zjawisk naturalnej cyrkulacji i parowania w celu zapewnienia długoterminowego chłodzenia rdzenia i obudowy bezpieczeńsywa w przypadku awarii. Do pasywnych systemów bezpieczeństwa w AP1000 należą: pasywne systemy usuwania ciepła powyłączeniowego (PRHRs – ang. *Passive Residual Heat Removal systems*); zbiornik uzupełniający zalanie rdzenia (CMT); system cyrkulacji wody ze zbiornika awaryjnego (CSR – ang. *Containment Sump Recirculation*); pasywny system chłodzenia obudowy (PCCS – ang. *Passive Containment Cooling System*). Komercyjna eksploatacja reaktora AP1000 w chińskiej elektrowni jądrowej Sanmen pokazuje praktyczną możliwość budowy reaktorów z zaawansowanymi, działającymi pasywnymi systemami bezpieczeństwa. Jednak jako pierwszy obiekt tego rodzaju (FOAK – ang. *first-of-a-kind*), wymagał on



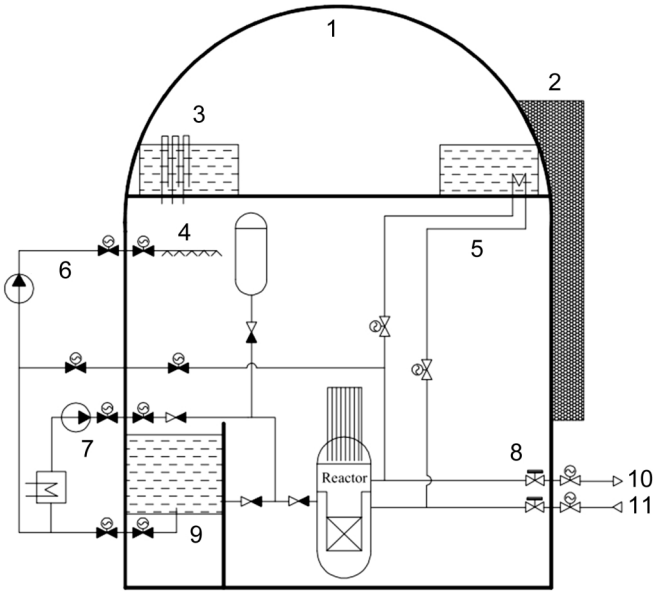
Rys. 1. Schemat niektórych elementów biernych (pasywnych) systemów bezpieczeństwa dla reaktora AP1000 [5]. 1 – zbiornik wody systemu PCCS opróżnianego grawitacyjnie, 2 – odprowadzanie powietrza na drodze konwekcji naturalnej, 3 – parowanie filmu wodnego, 4 – dopływ powietrza chłodzącego z zewnątrz, 5 – przegroda powietrzna, 6 – stalowa obudowa bezpieczeństwa, 7 – kondensacja wewnętrzna i naturalna cyrkulacja.

Fig. 1. *1-PCCS gravity drain water tank, 2 – Natural convection air discharge, 3 – Water film evaporation, 4 – Outside cooling air uptake, 5 – Air baffle, 6 – Steel containment vessel, 7 – Internal condensation and natural circulation.*

solidnej, różnorodnej i niezależnej oceny bezpieczeństwa komponentów i systemów elektrowni [4, 5].

Podobne systemy pasywnego bezpieczeństwa są prezentowane również dla Gen IV. Przykładem jest system proponowany dla zaawansowanego reaktora chłodzonego wodą przy nadkrytycznym ciśnieniu (VVER-SKD[2] lub SCWR – ang. *Super Critical Water Reactor*). Praca reaktora w warunkach nadkrytycznych (P = 25 MPa, t = 540°C) może zapewnić wzrost efektywności elektrowni jądrowej do 44–45% w porównaniu do uzyskiwanej dla klasycznych PWR wynoszącej 33–34%, przy jednoczesnym obniżeniu kosztów kapitałowych i eksploatacyjnych. Celem opracowania VVER-SKD jest zapewnienie bezpieczeństwa instalacji w warunkach normalnych, przejściowych i awaryjnych (rys. 2). Na obecnym etapie rozwiązanie takiego problemu nie może być osiągnięte bez pewnego minimum działań eksperymentalnych, które stanowiłyby podstawę do dalszych obliczeń i prac projektowych [6].

[2] VVER-SKD (ros. ВВЭР-СКД – Водо-водяной энергетический реактор с суперкритическими параметрами) to projekt rosyjskiego reaktora wodnego ciśnieniowego IV generacji, chłodzonego wodą o parametrach nadkrytycznych. Charakteryzuje wyższą sprawnością (powyżej 40–45%) w porównaniu do tradycyjnych VVER, dzięki pracy w wyższym ciśnieniu i temperaturze.



Rys. 2. Pasywny system bezpieczeństwa, chłodzenie reaktora i obudowy reaktora I [5]. 1 – obudowa bezpieczeństwa; 2 – usuwanie ciepła z obudowy bezpieczeństwa (CECS – *Containment Emergency Cooling System*); 3 – zapobieganie wzrostowi ciśnienia w obudowie bezpieczeństwa (PPDS – *Passive Presure Decrease System*, system natryskowy); 4 – natrysk; 5 – pasywny system usuwania ciepła resztkowego z rdzenia (PHRS – *Passive Heat Removal System*); 6 – pompa natryskowa; 7 i 9 – system awaryjnego chłodzenia rdzenia i uzupełniania chłodziwa reaktora (akumulatory i zbiorniki PCFS – *Passive Cooling Feedwater System*, pompy ECCS – *Emergency Core Cooling System*); 8 – główne zawory izolacyjne pary (MSI – *Main Steam Isolation Valves*); 10 – rura do turbiny; 11 – rura z pompy wody świeżej (FWP – *Fresh Water Pump*).

Fig. 2. *VVER-SCP (SCP – Supercritical Parameters.) safety systems [5]. 1 – Containment; 2 – Heat removal from the containment (CECS); 3 – prevention of pressure increase in the containment (PPDS, spray system); 4 – Spray; 5 – Passive Residual Heat Removal System from the core (PHRS); 6 – Spray pump; 7 & 9 – Emergency core cooling system and reactor makeup (PCFS accumulators and tanks, ECCS pumps); 8 – Main Steam Isolation Valves (MSIVs); 10 – Pipe to Turbine; 11 – Pipe from Fresh Water Pump (FWP).*

3.1. Siły napędowe procesów i gradienty

Działanie pasywnych systemów bezpieczeństwa reaktorów jądrowych opiera się na zjawiskach transportu pędu, ciepła i masy zachodzących pod wpływem naturalnych sił napędowych. W odróżnieniu od systemów aktywnych, w których przepływ jest wymuszany przez urządzenia mechaniczne, ruch czynnika roboczego w systemach pasywnych wynika z istnienia gradientów wielkości fizycznych, takich jak temperatura, gęstość, ciśnienie oraz skład mieszaniny. Opis tych procesów bazuje na klasycznych prawach transportu [7].

W ujęciu ogólnym transport pędu, ciepła i masy opisują równania zachowania w postaci różniczkowej. Równanie pędu można zapisać jako:

$$\frac{\vec{u}}{t} \quad \vec{u} \quad \vec{u} \qquad p \qquad \vec{u} \quad (\vec{u})^T \qquad \vec{g}$$

gdzie oznacza gęstość, $\vec{u}$ prędkość, lepkość dynamiczną, a $\vec{g}$ przyspieszenie ziemskie. Równanie bilansu energii, zapisane w postaci entalpii właściwej h, przyjmuje postać:

$$\frac{h}{t} \quad \vec{u} \quad h \qquad k_T \quad T \quad S_h$$

gdzie k_T jest przewodnością cieplną, a S_h obejmuje źródła energii, w tym ciepło powyłączeniowe oraz efekty przemian fazowych. Transport składnika mieszaniny opisuje równanie:

$$\frac{C_i}{t} \quad \vec{u} \quad C_i \qquad D_i \quad C_i \qquad R_i \quad S_i$$

gdzie C_i oznacza stężenie i-tego składnika, D_i współczynnik dyfuzji, a człony R_i i S_i to odpowiednio lokalne szybkości powstawania lub zaniku składnika w wyniku reakcji chemicznych i międzyfazowego transportu masy, związanego np. z parowaniem lub kondensacją.

Równania te są ze sobą sprzężone. Rozkład temperatury wpływa na gęstość i właściwości fizyczne płynu, co modyfikuje pole prędkości, a tym samym transport masy i energii. Z kolei procesy dyfuzji i przemiany fazowe zmieniają lokalny skład mieszaniny i warunki wymiany ciepła. W konsekwencji analiza działania pasywnych systemów bezpieczeństwa wymaga jednoczesnego uwzględnienia transportu pędu, ciepła i masy.

Jednym z podstawowych mechanizmów napędowych jest gradient temperatury. Zależność gęstości od temperatury można przybliżyć relacją:

$$_0 1 \quad (T \quad T_0)$$

gdzie jest współczynnikiem rozszerzalności cieplnej. Powstające różnice gęstości prowadzą do działania siły wyporu:

$$\vec{F}_b \quad \vec{g}(\quad _0)V$$

W układach przepływowych odpowiada to różnicy ciśnień:

$$p \quad g(\quad _0)(z \quad z_0)$$

która napędza cyrkulację naturalną. Zjawisko to występuje zarówno w cieczach, jak i w gazach. W obudowie bezpieczeństwa prowadzi do powstawania cyrkulacji powietrza i pary wodnej, odpowiedzialnej za transport ciepła i masy.

Przepływ ustala się w wyniku równowagi między siłami napędowymi a oporami. Straty ciśnienia można zapisać jako:

$$p_{strat} \quad \frac{L}{d_h} \frac{\overline{u}^2}{2} \quad _j \quad ^j \frac{\overline{u}^2}{2}$$

gdzie oznacza współczynnik strat liniowych, $_j$ współczynniki strat miejscowych, a L i d_h to odpowiednio długość i średnica zastępcza przewodu [8]. Warunek istnienia przepływu ma postać:

$$p \quad p_{strat}$$

Istotnym mechanizmem odbioru ciepła jest kondensacja pary wodnej. Gęstość strumienia ciepła można zapisać jako:

$$q_{kond} \quad {}_{kond} \; T_{sat} \quad T_w$$

a współczynnik wymiany ciepła dla skraplania błonowego można oszacować zależnością:

$${}_{kond} \quad \frac{g \; {}_L \; {}_L \quad {}_V \; k_T^3 \; h}{{}_L \; T_{sat} \quad T_w \; L_w}^{0,25}$$

Gdzie h to ciepło kondensacji, ${}_L$ i ${}_V$ oznaczają odpowiednio gęstość cieczy i pary, T_{sat} i T_w to temperatura pary nasyconej i ścianki, a L_w jest charakterystyczną skalą długości strefy kondensacji [6]. Obecność gazów niekondensujących wprowadza dodatkowy opór dyfuzyjny $1/k_m$, który wpływa na gęstość strumienia masy kondensującego i-tego składnika:

$$m_i \quad k_{m,i} \; C_i \quad C_{sat,i}$$

co ogranicza intensywność wymiany ciepła.

W wielu nowoczesnych konstrukcjach stosuje się pasywne chłodzenie zewnętrznej powierzchni obudowy bezpieczeństwa poprzez spływ cienkiej warstwy wody pod wpływem grawitacji. Odbiór ciepła odbywa się poprzez sprzężenie przewodzenia, konwekcji i parowania:

$$q_{eff} \quad {}_{eff} \; T_w \quad T_e$$

gdzie ${}_{eff}$ uwzględnia wszystkie mechanizmy wymiany ciepła [9], a T_e to temperatura otoczenia. Para wodna powstająca w wyniku parowania jest następnie transportowana przez konwekcję naturalną.

Przy wysokich temperaturach istotny udział w bilansie cieplnym ma również promieniowanie:

$$q_{eff} \quad T_w^4 \quad T_e^4$$

gdzie to emisyjność powierzchni emitującej promieniowania, to stała Stefana–Boltzmanna. Promieniowanie cieplne wpływa na rozkład temperatury i pośrednio na siły wyporu [10].

Należy również pamiętać, że właściwości fizyczne czynnika roboczego, takie jak lepkość, przewodność cieplna i ciepło właściwe, zależą od temperatury i składu [11], co nadaje układowi równań bilansowych opisujących procesy transportu charakter silnie nieliniowy.

Przedstawione zależności pokazują, że siły napędowe w pasywnych systemach bezpieczeństwa wynikają z gradientów temperatury, gęstości, ciśnienia i składu, natomiast ich skuteczność jest determinowana przez równowagę między tymi siłami a oporami przepływu oraz intensywnością procesów wymiany ciepła. Charakterystyczną cechą tych układów jest niewielka wartość sił napędowych, co powoduje dużą wrażliwość ich pracy na zmiany warunków termicznych i hydraulicznych. W konsekwencji opis pracy pasywnych systemów bezpieczeństwa wymaga uwzględnienia sprzężonych procesów transportowych zachodzących w warunkach nieliniowych, w których niewielkie zmiany parametrów mogą prowadzić do utraty stabilności przepływu oraz istotnych zmian charakteru przepływu i intensywności wymiany ciepła.

W takich warunkach klasyczne termohydrauliczne kody systemowe, takie jak TRACE, CATHARE, ATHLET czy nadal szeroko stosowany RELAP5, pozwalają na analizę globalnego zachowania układu, w tym przebiegu ciśnienia, temperatury, przepływu i bilansu energii podczas stanów przejściowych i awaryjnych. Ze względu na stosowane w nich modele oparte głównie na elementach jedno- i zerowymiarowych oraz uśrednionym opisie przepływu, ich możliwości szczegółowego odwzorowania lokalnych zjawisk wielowymiarowych są jednak ograniczone. Fakt ten ma znaczenie w przypadku pasywnych systemów bezpieczeństwa, w których wielowymiarowa konwekcja naturalna, mieszanie i stratyfikacja termiczna lub stężeniowa, lokalna kondensacja pary w obecności gazów niekondensujących oraz niestabilności przepływu mogą wpływać na działanie całego układu. Z tego względu coraz częściej stosuje się metody numerycznej mechaniki płynów (CFD – ang. *Computational Fluid Dynamics*), które umożliwiają szczegółową analizę pól przepływu, temperatury i stężenia oraz ocenę sprzężonych procesów transportowych i ich wpływu na stabilność, a także skuteczność działania pasywnych systemów bezpieczeństwa. Współczesne opracowania wskazują, że podejście CFD stanowi istotne uzupełnienie analiz systemowych, szczególnie w odniesieniu do zjawisk wielowymiarowych oraz sprzężonych procesów transportu pędu, ciepła i masy, a jego rola rośnie wraz z rozwojem metod wieloskalowych, łączących modele systemowe z modelami CFD [12, 13].

3.2. Systemy pasywne kategorii A, B, C i D

IAEA-TECDOC-626 „Safety-Related Terms for Advanced Nuclear Plants" to wydany przez International Atomic Energy Agency raport techniczny uporządkował i zdefiniował kluczowe pojęcia z zakresu bezpieczeństwa jądrowego, ze szczególnym uwzględnieniem projektów reaktorów nowej generacji [14].

Kategoria A

W tej kategorii systemy bierne nie mają ruchomych komponentów mechanicznych ani części i żadnych przemieszczających się czynnych płynów. Ponadto te systemy nie zależą od żadnych zewnętrznych źródeł energii ani od żadnego zewnętrznego sygnału do aktywacji [15]. Przykładami tej kategorii biernych cech bezpieczeństwa są bariery fizyczne przeciwko uwalnianiu produktów rozszczepienia, takie jak powłoki paliwowe oraz elementy i systemy granicy ciśnienia; systemy chłodzenia rdzenia wykorzystujące transfer ciepła przez promieniowanie, konwekcję i przewodzenie od paliwa jądrowego do zewnętrznych części konstrukcyjnych itd.

Kategorie B i C

Systemy pasywne kategorii B i C, powszechnie stosowane w bezpieczeństwie jądrowym (definicje MAEA), różnią się

wykorzystaniem ruchomych części. Systemy kategorii B obejmują ruchome płyny robocze bez ruchomych części mechanicznych (np. chłodzenie w obiegu naturalnym). Systemy kategorii C zawierają ruchome części mechaniczne (np. zawory zwrotne, akumulatory), ale nie mają zewnętrznego zasilania ani inteligentnego systemu sterowania.

Systemy pasywne kategorii B

Definicja: Brak inteligencji/mocy wejściowej, brak ruchomych części mechanicznych, ale opierają się na ruchomych cieczach roboczych ze względu na warunki termohydrauliczne (np. naturalna konwekcja).

Charakterystyka: Działanie opiera się na prawach natury (grawitacja, konwekcja).

Przykłady:

- Wymienniki ciepła z naturalnym obiegiem: Odprowadzanie ciepła rozpadu z rdzenia.
- Pasywne chłodzenie obudowy: Systemy wykorzystujące parowanie/naturalną cyrkulację powietrza.
- Linia wyrównawcza: Podłączenie gorącej odnogi obiegu chłodzenia (*hot leg*) do stabilizatora ciśnienia.

Systemy pasywne kategorii C

Definicja: Brak inteligencji – sterowania/zasilania elektrycznego, ale zawierają ruchome części mechaniczne.

Charakterystyka: Komponenty poruszają się pod wpływem ciśnienia systemowego lub grawitacji, bez ingerencji operatora ani ingerencji elektrycznej.

Przykłady:

- Zawory zwrotne: Otwierane w celu umożliwienia przepływu bez zasilania zewnętrznego.
- Akumulatory/zbiorniki wody uzupełniającej rdzeń (CMT – ang. *Core Make-up Tank*): Wykorzystujące zmagazynowane ciśnienie azotu lub grawitację do wtryskiwania wody.
- Zawory bezpieczeństwa: Otwierane pod wysokim ciśnieniem.

Systemy kategorii B są na ogół uważane za bardziej niezawodne ze względu na mniejszą liczbę typów możliwych awarii, podczas gdy w systemach kategorii C konieczna jest ocena niezawodności komponentów mechanicznych (np. awaria zaworu przy otwieraniu).

Kategoria D

Ta kategoria systemów pasywnych charakteryzuje się pasywnym wykonaniem i aktywnym inicjowaniem ich działania. Oznacza to, że do uruchomienia procesu wymagana jest zewnętrzna inteligencja. Działanie, realizowane po inicjacji procesu, odbywa się środkami pasywnymi. Ta kategoria wyznacza granicę między systemami aktywnymi a pasywnymi. Niektóre przykłady tej kategorii pasywnych funkcji bezpieczeństwa to systemy awaryjnego chłodzenia rdzenia (ECCS – ang. *Emergency Core Cooling System*), które są aktywowane przez elektropneumatyczne zawory i działają na zasadzie przepływu wody napędzanego grawitacją, oraz systemy awaryjnego wyłączenia oparte na prętach kontrolnych napędzanych grawitacją lub ciśnieniem statycznym, które są uruchamiane przez logikę awaryjnego wyłączenia typu *fail–safe*.

3.3. Podstawowe systemy pasywnego zapewnienia bezpieczeństwa eksploatacji reaktora jądrowego

Zaawansowane koncepcje reaktorów w dużym stopniu wykorzystują pasywne zabezpieczenia w połączeniu z aktywnymi systemami bezpieczeństwa lub systemami eksploatacyjnymi. Zgodnie z definicjami Międzynarodowej Agencji Energii Atomowej [14] system pasywny nie wymaga zewnętrznego zasilania, zwłaszcza energii, aby działać. Dlatego też oczekuje się, że systemy pasywne będą łączyć w sobie między innymi zalety prostoty, zmniejszenia potrzeby interakcji z człowiekiem oraz redukcji lub wyeliminowania zewnętrznego zasilania elektrycznego lub sygnałów.

W pracach nad oceną tych systemów należy wziąć pod uwagę takie aspekty ich działania, jak brak danych na temat niektórych zjawisk, brak doświadczenia eksploatacyjnego w szerokim zakresie warunków oraz siły napędowe procesów wymiany pędu, masy oraz ciepła, które w większości przypadków są mniejsze niż w przypadku aktywnych systemów bezpieczeństwa. Istnieją znaczne niepewności związane z czynnikami, które zależą od wielkości tych sił i sił przeciwstawnych (np. wartości współczynników przenikania ciepła i strat ciśnienia). Ponadto, wielkość takich naturalnych sił napędowych zależy od specyficznych warunków i konfiguracji instalacji, które mogą występować w momencie, gdy system jest zobowiązany do realizacji funkcji bezpieczeństwa. Wszystkie te niepewności wpływają na wydajność cieplno-hydrauliczną (T-H) systemów pasywnych. Uwaga ta odnosi się w szczególności do pasywnych systemów kategorii B lub C, tj. wykorzystujących ruchomy czynnik roboczy, zgodnie z klasyfikacją MAEA [14], a w szczególności do pasywnych systemów wykorzystujących cyrkulację naturalną.

Ocena niezawodności pasywnych systemów bezpieczeństwa jest jednym z ważnych zagadnień, ponieważ bezpieczeństwo zaawansowanych reaktorów jądrowych opiera się na kilku pasywnych cechach. W tym kontekście w przeszłości opracowano kilka metodologii, takich jak ocena niezawodności pasywnych systemów bezpieczeństwa (REPAS – ang. *Reliability Evaluation of Passive Safety Systems),* metody niezawodności dla pasywnych funkcji bezpieczeństwa (RMPS – ang. *Reliability Methods for Passive Systems*) oraz analiza niezawodności systemów pasywnych (APSRA – ang. *Assessment of Passive System Reliability*). Systemy bezpieczeństwa biernego uważa się za bardziej niezawodne niż systemy bezpieczeństwa czynnego ze względu na wyeliminowanie potrzeby interwencji człowieka, unikanie zewnętrznego zasilania elektrycznego itp. Jednak włączenie tych systemów w reaktorach jądrowych

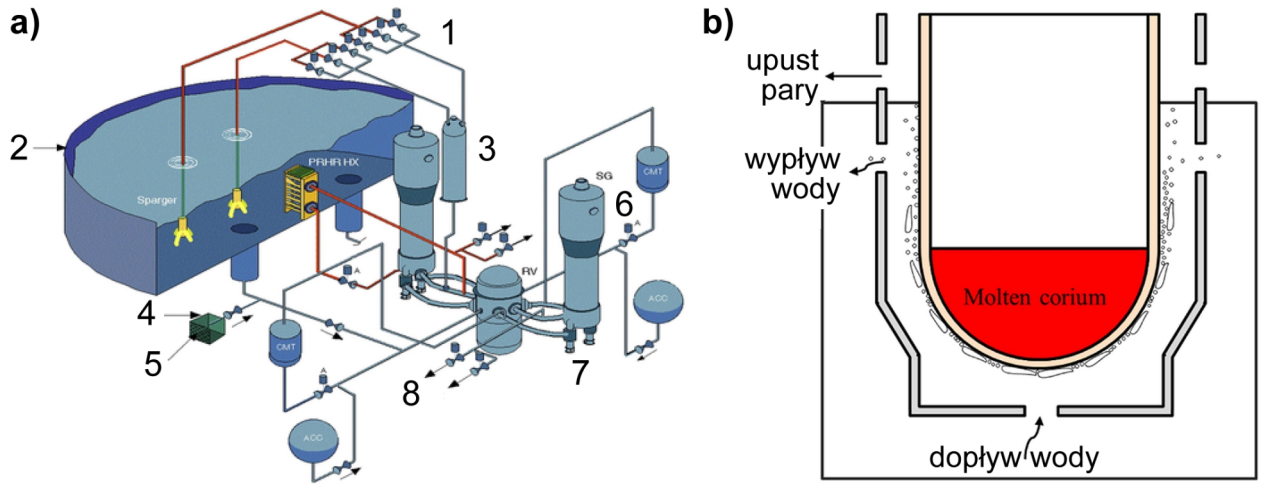
musi być odpowiednio przetestowane z powodu kilku kwestii technicznych, na przykład: brak doświadczenia operacyjnego bloków wyposażonych w systemy bezpieczeństwa pasywnego; niedobór odpowiednich danych eksperymentalnych ze złożonych obiektów testowych lub z testów efektów oddzielnych wynikających z badań poszczególnych składowych systemu prowadzonych w celu poznania charakterystyk efektywności działania tych pasywnych systemów, nie tylko podczas normalnej pracy, ale również podczas awarii i stanów przejściowych; brak uznanych definicji rodzaju awarii dla tych systemów; trudności w modelowaniu niektórych fizycznych zjawisk będących podstawą działania tych systemów.

Ocena niezawodności systemu pasywnego jest trudnym zadaniem. Wymaga jasnego zrozumienia fizyki zjawisk i możliwego mechanizmu awarii systemu pasywnego, co projektant musi zrobić przed przewidywaniem jego niezawodności. Obecnie wydajność systemów pasywnych i ich awarie przewiduje się za pomocą tak zwanych „kodów najlepszego oszacowania". Jednak zastosowanie „kodów najlepszych szacunków" do oceny wydajności i awarii systemów pasywnych nie jest dobrze ugruntowane ze względu na brak wystarczających danych z obiektu/eksperymentalnych. Wprowadza to duże niepewności i błędy, gdy takie kody są stosowane do oceny wydajności systemu pasywnego. Wydajność systemów pasywnych jest w dużym stopniu zależna od odchyleń parametrów procesów od ich wartości nominalnych. Podczas ekstremalnych zdarzeń zmiany tych wartości parametrów procesów mogą zwiększać lub zmniejszać prawdopodobieństwo wystąpienia zdarzenia oraz wskaźnik awarii komponentów. Ponadto komponenty systemów pasywnych mogą ulegać awarii w dowolnych pośrednich pozycjach działania zamiast klasycznego założenia awarii w stanach binarnych. Obecne metodyki nie uwzględniają tych dynamicznych cech awarii komponentów systemów pasywnych [16], [17]. Systemy pasywne bazują na prawach fizyki, takich jak grawitacja czy różnica gęstości (konwekcja). W praktyce inżynieryjnej rzadko są one jednak w stu procentach odizolowane od urządzeń aktywnych. Projektanci mogą uznać system za w pełni autonomiczny i nie zauważyć, że awaria małego komponentu aktywnego blokuje całą gałąź bezpieczeństwa. Wiele systemów pasywnych wymaga początkowego impulsu, na przykład otwarcia zaworu sterowanego sygnałem elektrycznym lub hydraulicznym. Nowoczesne probabilistyczne analizy bezpieczeństwa (tzw. PSA – *Probabilistic Safety Assessment*) muszą uwzględniać te powiązania, tak, aby poprawnie ocenić realną odporność reaktora na tego typu zjawiska.

4. Przykłady rozwiązań technicznych

AP1000 to reaktor PWR zaprojektowany przez Westinghouse Electric Corporation. Wykorzystuje on pasywne systemy bezpieczeństwa, które opierają się na grawitacji, sprężonym gazie, naturalnej cyrkulacji i parowaniu, mają za zadanie zapewnić długoterminowe chłodzenie w przypadku awarii. Systemy pasywne zapewniają bezpieczeństwo elektrowni i chronią inwestycje kapitałowe. Utrzymują i zapewniają chłodzenie rdzenia oraz integralność osłony w sposób nieograniczony czasowo, bez wymagań dotyczących obsługi operatora ani zasilania prądem elektrycznym. Systemy pasywne spełniają kryteria zapobiegania pojedynczej awarii (ang. *single failure accident*), a probabilistyczne oceny ryzyka (PRA – ang. *Probabilistic Risk Assessment,* PSA – *Probabilistic Safety Assessment*) stosowane są do weryfikacji ich niezawodności. Pasywne systemy bezpieczeństwa są znacznie prostsze od typowych systemów bezpieczeństwa PWR. Pasywny system chłodzenia rdzenia (PXS), pokazany na rysunku 3a, chroni obiekt przed wyciekami i pęknięciami obiegu chłodzenia reaktora RCS (ang. *Reactor Cooling System*) o różnych rozmiarach oraz lokalizacjach [18]. Pasywny system chłodzenia rdzenia obejmuje pasywny układ odprowadzania ciepła powyłączeniowego RHRS (ang. *Residual Heat Removal System*) oraz system wtrysku bezpieczeństwa i zrzutu ciśnienia, aby zapewnić awaryjne chłodzenie rdzenia i usuwanie ciepła resztkowego w różnych możliwych wypadkach. Wytwornica pary (SG – ang. *Steam Generator*) to wymiennik ciepła, w którym gorąca woda z obiegu pierwotnego (ogrzewana przez rdzeń reaktora) przekazuje ciepło do obiegu wtórnego, zamieniając wodę w parę wodną, która następnie napędza turbinę generatora prądu. Wtrysk wody zawierającej kwas borowy napędzany jest grawitacją. Wymiennik ciepła pasywnego RHRS (ang. *Residual Heat Removal System*) wykorzystuje IRWST (ang. *In-containment Refueling Water Storage Tank*) jako zasobnik chłodziwa zdolnego zapewnić niezbędne chłodzenie w przypadku braku możliwości usuwania ciepła na zewnątrz. W przypadku stopienia rdzenia strategia zatrzymania wytworzonych produktów wewnątrz reaktora opiera się na stosowaniu zewnętrznej obudowy bezpieczeństwa (ang. *Containment*) reaktora (rys. 3b). Osłona ochronna zbiornika reaktora tworzy przestrzeń pierścieniową pomiędzy nią a zbiornikiem reaktora, umożliwiając wodzie chłodzącej bezpośredni kontakt z powierzchnią zbiornika. Przewidziano ujście pary powstającej w tej przestrzeni do obszaru obudowy. Para ta skrapla się na powierzchni obudowy bezpieczeństwa, a skropliny są zawracane z powrotem do obszaru konstrukcji zapewniającej usadowienia reaktora.

PXS zapewnia usuwanie resztkowego ciepła z rdzenia, wtrysk wody oraz dekompresję. Analizy bezpieczeństwa (przy użyciu kodów zatwierdzonych przez amerykańską Komisję dozoru jądrowego US-NRC (*United States Nuclear Regulatory Commission*) wykazują skuteczność PXS w ochronie rdzenia po różnych zdarzeniach przerwania obiegu chłodzenia reaktora RCS (ang. *Reactor Cooling System*). Nawet w przypadku pęknięć tak poważnych jak 20,0 cm (8 cali) nie dochodzi do odsłonięcia



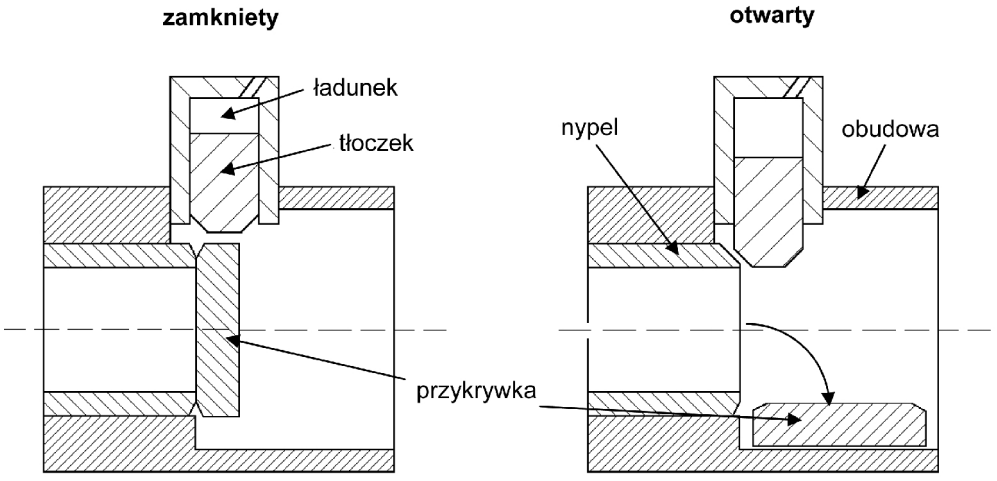
Rys. 3. **(a)** Pasywny system chłodzenia rdzenia PXS (*Passive Core Cooling System*). 1 – zawory odprężania ciśnienia; 2 – zbiornik IRWST (*In-containment Refueling Water Storage Tank)* stanowi część pasywnego układu usuwania ciepła powyłączeniowego; 3 – stabilizator ciśnienia; 4 – studnia spływowa; 5 – osłona; 6 – wytwornica pary (SG); 7 – główne pompy cyrkulacyjne (MCP); 8 – węzeł cyrkulacyjny. **(b).** Konstrukcja osłony zbiornika reaktora. W przypadku stopienia rdzenia woda ze zbiornika IRWST (2 na rys 3a.) zostaje wykorzystana do zalania studni reaktora i chłodzenia zewnętrznej powierzchni zbiornika reaktora.

Fig. 3. ***(a)*** *Passive core cooling system (PXS). 1 – The In-containment Refueling Water Storage Tank (IRWST) is part of the passive residual heat removal system; 2 – Pressure relief valves; 3 – Pressure stabilizer; 4 – Sump; 5 – Shield; 6 – Steam Generator (SG); 7 – Main circulation pumps (MCP); 8 – Circulation node.* ***(b)*** *Reactor vessel shielding construction. In the event of core meltdown, water from the IRWST tank (2 in Fig. 3a.) is used to flood the reactor sump and cool the external surface of the reactor vessel.*

rdzenia. Po podwójnym pęknięciu głównej rury chłodziwa reaktora PXS chłodzi reaktor z dużym marginesem względem limitu maksymalnej temperatury stopienia koszulek prętów paliwowych [18].

W roku 1988 NRC zaktualizowała przepisy dotyczące systemu awaryjnego chłodzenia rdzenia (ECCS), dopuszczając stosowanie kodów komputerowych opartych na metodzie „najlepszego szacunku” (best-estimate) i ustanawiając tym samym standardowe ramy walidacji nowoczesnego oprogramowania z zakresu bezpieczeństwa. W końcu lat 90-tych firma Westinghouse opracowała i przetestowała te kody bezpieczeństwa dla reaktora AP600 (poprzednika modelu AP1000). NRC zatwierdziła te bazowe metodyki w trakcie procesu certyfikacji AP600 w 1999 roku. Komputerowe kody do analizy bezpieczeństwa, wykorzystywane do oceny pasywnego systemu chłodzenia rdzenia (PXS), zostały formalnie zatwierdzone przez NRC w grudniu 2005 roku w ramach procesu certyfikacji projektu reaktora AP1000.

Projekt elektrowni AP1000 obejmuje zawory otwierane wybuchowo, ze względu na ich wysoką niezawodność i przydatność takiego systemu wyposażonego w zapalnik, w sytuacji gdy istnieje jednorazowa potrzeba otwarcia zaworu. To rozwiązanie jest potwierdzone zastosowaniem tego typu zaworów wybuchowych w wielu projektach, w których zawór nie może zawieść w wypełnieniu swojej funkcji. Przykłady takich zastosowań obejmują systemy uzbrojenia i systemy kosmiczne. Konstrukcja zaworu wybuchowego jest prosta (rys. 4) i istnieje niewiele rozwiązań gwarantujących zadziałanie zaworu, jak jest to w tym przypadku.



Rys. 4. Konstrukcja zaworu otwieranego wybuchowo.

Fig. 4. *Valve explosion oppening.*

Tego typu konstrukcja konkuruje z sukcesem z innymi rozwiązaniami, jak np. stosowanie zaworów sterowanych pneumatycznie lub silnikiem, które mają więcej ruchomych części, mogących zawieść i uniemożliwić uruchomienie zaworu. Pasywny system chłodzenia rdzenia elektrowni AP1000TM wymaga jednorazowego ustawienia zaworów do ich uruchomienia. W systemach, w których potrzebna jest bardzo duża niezawodność, w jednorazowym otwarciu w połączeniu ze szczelnością i wysoką niezawodnością zapobiegającą przypadkowemu uruchomieniu, stosuje się zawory otwierane wybuchowo z wykorzystaniem zapalników [19]. Trzeba pamiętać, że zawory zwrotne lub zawory strzałowe (uruchamiane ładunkiem pirotechnicznym) mogą zaciąć się w wyniku nagromadzenia osadów lub produktów korozji, jeśli nie są regularnie testowane.

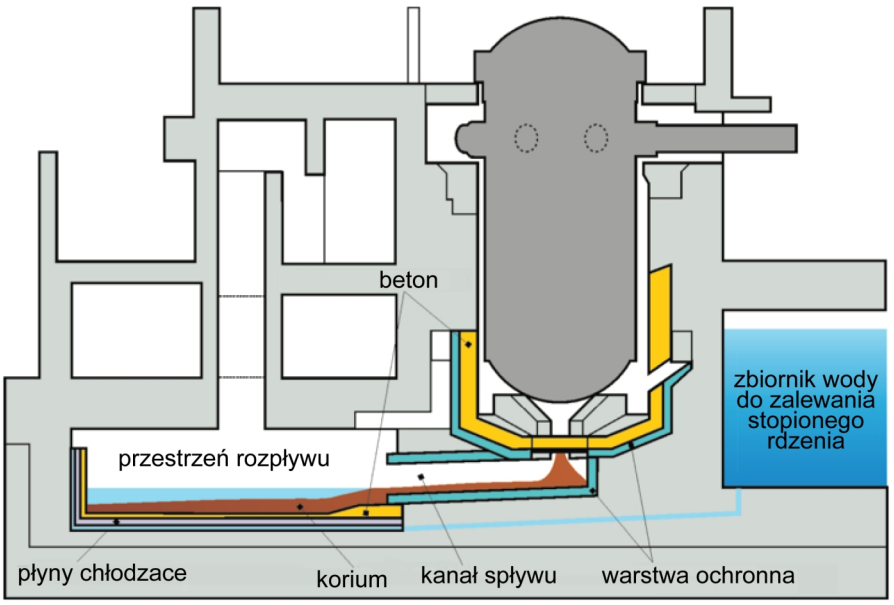
W przypadku AP1000 przyjmuje się, że stopiony rdzeń nie przetopi zbiornika reaktora. Jednak w przypadku reaktora EPR (ang. *European Power Reactor*) ze względu na jego wysoką moc nominalną konieczne było zastosowanie innego podejścia projektowego, niż w przypadku reaktorów APR-1400 czy AP1000. Zatrzymanie stopionego rdzenia (*corium*) wewnątrz zbiornika poprzez chłodzenie zewnętrzne jest uważane za bardzo mało prawdopodobne. Reaktor EPR wyposażony jest w zaawansowaną konstrukcję łapacza rdzenia, która w sposób pasywny zatrzymuje i chłodzi korium w komorze jego rozprzestrzeniania. Osiąga się to dzięki przepływowi wody z systemu IRWST (ang. *In-containment Refualing Water Storage Tank*) pod wpływem siły grawitacji (patrz rys. 5). Woda chłodząca jest następnie odparowywana pod wpływem ciepła wydzielonego przez materiał rdzenia, a następnie skraplana przez zraszacze. System odprowadzania ciepła z obudowy bezpieczeństwa CHRS (ang. *Containment Heat Removal System*) działa w trybie aktywnym i zapewnia ograniczenie ciśnienia wewnątrz obudowy bezpieczeństwa, z jednoczesnym zachowaniem integralności konstrukcji w perspektywie długoterminowej konieczności chłodzenia systemu [20].

5. Badania modelowe

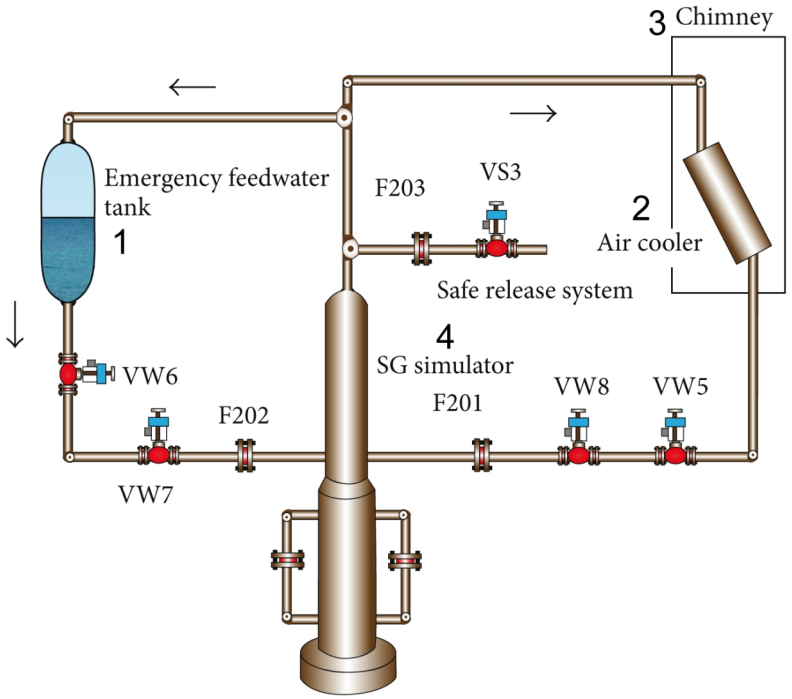
Tak naprawdę systemy pasywne zostały zaproponowane w odniesieniu do istniejących projektów reaktorowych nieco intuicyjne, na podstawie obserwacji istniejących praw natury. Podobnie jak Isaac Newton odkrył prawo ciążenia, obserwując spadające jabłko. Jednak istniejące rozwiązania niekoniecznie ze względów geometrycznych, czy też konstrukcyjnych, muszą być optymalne dla pełnego wykorzystania znanych nam z fizyki i inżynierii zjawisk. I tu wkracza modelowanie z wykorzystaniem narzędzi obliczeniowych lub metod doświadczalnych. Poniżej przykłady tych działań.

Aby poprawić bezpieczeństwo i niezawodność reaktora, niektóre reaktory ewolucyjne i innowacyjne, takie jak AP600/1000, WWER640/407, APR+, SBWR i SMART, wykorzystują pasywne systemy odprowadzania ciepła resztkowego [21]. Jednak większość z tych systemów to podstawowe pasywne systemy chłodzenia, z wyjątkiem WWER640/407 i APR+.

Pasywny system odprowadzania ciepła resztkowego (PRHRS – ang. *Passive Residual Heat Removal System*) dla obiegu wtórnego jest jedną z ważnych cech chińskiego zaawansowanego reaktora wodnego ciśnieniowego (CAPWR – ang. *China Advanced Pressurised Water Reactor*). Aby udowodnić bezpieczeństwo CAPWR, przeprowadzono szereg eksperymentów na specjalnie zaprojektowanym stanowisku testowym PRHRS (ang. *Passive Residual Heat Removal System*). Instalacja testowa została zbudowana zgodnie z zasadami metodyki skalo-



Rys. 5. Widok przekroju chwytacza rdzenia EPR.
Fig. 5. *Cross section view of the EPR core catcher.*



Rys. 6. Schemat stanowiska testowego pasywnego odbioru ciepła powyłaczeniowego wyk(PRHRS). 1- zbiornik wody zasilającej stosowany w przypadku awarii; 2 – chłodnica powietrza; 3 – komin; 4 – wytwornica pary (symulator); VS – zawór bezpieczeństwa (*Safe release system*); VW – zawory wodne; F – złącza kołnierzowe.

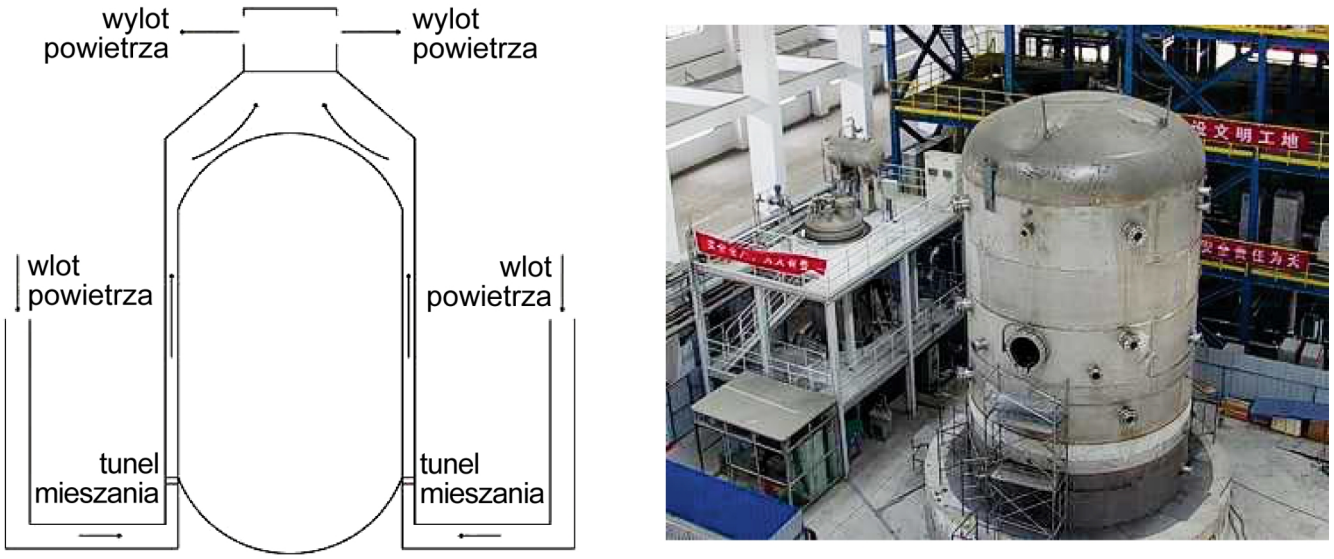
Fig. 6. *Schematic diagram of passive residual heat removal system (PRHRS) test facility. SG – Steam Generator; VS – Safety Valve; VW – Water Valve; F – Flange.*

wania z dwufazową cyrkulacją naturalną. Do ważnych grup podobieństwa należą: podobieństwo geometryczne, współczynnik tarcia, stosunek gęstości, liczba Froude'a, liczba przemian fazowych oraz liczba strumieni konwekcyjnych. Instalacja pilotowa składa się z następujących elementów: pętli cyrkulacji parowo-wodnej, pętli awaryjnego zasilania wodą, pętli cyrkulacji naturalnej powietrza, systemu bezpiecznego upustu pary. [22]. Główne elementy obejmują generator pary, chłodnicę powietrza, awaryjny zbiornika wody zasilającej (EFWT -ang. *Emergency Feed Water Tank*) oraz komina. Obiekt charakteryzuje się współczynnikiem skalowania geometrycznego wynoszącym 1/390 w odniesieniu do objętości, a całkowita wysokość od szczytu komina z regulowaną wysokością do powierzchni dna generatora pary wynosi około 23 m. Maksymalne ciśnienie w obiekcie wynosi 8,6 MPa, a ciepło wydzielane przez stopiony rdzeń jest symulowane przez grzejniki elektryczne o mocy 400 kW (DC). Schemat instalacji przedstawiono na rysunku 6. Jak wspomniano, stanowisko testowe zbudowano zgodnie z prawami skalowania, aby zachować podobieństwo do CAPWR [22].

Łącznie przeprowadzono ponad 300 testów na stanowisku testowym, w 90% przypadków w stanie ustalonym i 10% przypadków w stanie nieustalonym [22]. Na podstawie wyników eksperymentalnych dla przypadków w stanie ustalonym wygenerowano model półempiryczny w celu wyznaczenia funkcji pasywnego odprowadzania ciepła. Charakterystyka dynamiczna i niezawodność pasywnego systemu bezpieczeństwa CAPWR zostały jednoznacznie potwierdzone w przypadkach nieustalonych. Podobne testy prowadzono dla analogicznego reaktora APR+ (ang. *Advanced Power Reactor Plus*). Jest to elektrownia jądrowa generacji III+, rozwijana w Korei. Pasywny pomocniczy system zasilania wodą (PAFS – ang. *Passive Auxiliary Feedwater System*) jest jednym z zaawansowanych rozwiązań bezpieczeństwa wdrażanych w APR+. PAFS ma całkowicie zastąpić konwencjonalny aktywny pomocniczy system zasilania wodą [23]. Pojedynczy układ PAFS jest wymagany do usunięcia maksymalnej mocy cieplnej 129,8 MW przez 240 rur kondensacyjnego wymiennika ciepła PCHX (*ang. Passive Condensation Heat Exchanger*). Badania przeprowadzono na instalacji testowej wykorzystującej konwencjonalne źródło ciepła. W związku z tym dostarczono 540 kW mocy cieplnej, aby wygenerować przepływ pary do pojedynczej rury instalacji badawczej, zgodnie ze współczynnikiem skalowania obiektu (1/240). Poprzedni [22] i ten przykład [23]wskazują, jaki jest wymóg dotyczący skalowania instalacji badawczych (1/240–1/390).

Oczywiście podobne zasady obowiązują w rozwijanych rozwiązaniach SMR. ACP100 to innowacyjny mały reaktor modułowy (SMR) zaprojektowany przez CNNC (*China National Nuclear Corporation)*. Pasywny układ chłodzenia powietrza (PAS – ang. *Passive Air-cooling System*) jest jedną z kluczowych cech technicznych zapewniających bezpieczeństwo w konstrukcji ACP100 [24].

Zgodnie z zasadami skalowania obiekt testowy (rys. 7) został zaprojektowany w taki sposób, aby wymiana ciepła wewnątrz i na zewnątrz zbiornika bezpieczeństwa oraz cyrkulacja/rozwarstwienie gazu w dużej, wolnej przestrzeni w obiekcie testowym były podobne do tych w prototypie



Rys. 7. Schemat dróg przepływu powietrza w urządzeniu ACP100 PAS (po lewej), zdjęcie modelu fizycznego (po prawej).
Fig. 7. *Schematic diagram of ACP100 PAS air flow path (left), physical model photo (right).*

PAS. Po przygotowaniu ogólnego projektu obiektu testowego przeprowadza się analizę skalowaniapolegającego na zmiejszeniu skali obiektu, opartą na przewidywanej reakcji ciśnieniowej systemu w obudowie bezpieczeństwa, magazynowaniu i przewodzeniu ciepła w stalowym zbiorniku bezpieczeństwa, naturalnej cyrkulacji powietrza przepływającego przez kanał na zewnątrz obudowy bezpieczeństwa. Ponadto uwzględnia się cyrkulację/rozpływ gazu w dużej wolnej przestrzeni wewnątrz zbiornika bezpieczeństwa, konwekcyjne i kondensacyjne przenoszenie ciepła wewnątrz zbiornika bezpieczeństwa oraz naturalne przenoszenie ciepła przez konwekcję na zewnątrz obudowy bezpieczeństwa. W ten sposób można uzyskać cechy konstrukcyjne obiektu testowego, uwzględniając podobieństwo parametrów tych ważnych zjawisk. Zgodnie z analizą skalowania prototypu i biorąc pod uwagę ograniczenia finansowe obiektu testowego, zaprojektowano wymiary geometryczne symulatora obudowy bezpieczeństwa. Całkowita wysokość stalowego zbiornika wynosi 9,5 m, co stanowi 1/4,9 prototypu. Średnica stalowego zbiornika wynosi 6 m. Aby uzyskać podobny stosunek powierzchni do objętości obiektu testowego w zmniejszonej skali, wewnętrzna powierzchnia zbiornika poniżej platformy operacyjnej obiektu testowego jest pokryta materiałami termoizolacyjnymi, tak aby wysokość powierzchni wymiany ciepła pionowej części obiektu wynosiła 5,2 m prototypu. Ponadto, w warunkach testu weryfikacyjnego awarii, aby spełnić wymagania dotyczące wolnej objętości obiektu, komory poniżej platformy operacyjnej są częściowo zablokowane, tak by wolna objętość obiektu wynosiła 225 m^3, co stanowi 1/80 skali prototypu.

6. Podsumowanie

Pasywne systemy bezpieczeństwa, zaprojektowane do wyłączania i chłodzenia reaktorów jądrowych przy użyciu sił naturalnych, takich jak grawitacja i konwekcja, zamiast napędzanych pomp, stanowią znaczącą zmianę w projektowaniu reaktorów. Poprawiają bezpieczeństwo poprzez zmniejszenie zależności od elementów aktywnych i interwencji człowieka, stwarzają nowe wyzwania dla operatorów i regulatorów, w tym konieczność wykazania/zweryfikowania niezawodności bez danych operacyjnych, modelowania skomplikowanych zjawisk termohydraulicznych oraz aktualizacji tradycyjnych ram regulacyjnych. MAEA zwraca uwagę na kluczowe kwestie, w tym weryfikację twierdzeń dotyczących bezpieczeństwa, zapewnienie niezawodności, zarządzanie słabymi siłami napędowymi oraz uzyskiwanie licencji na nowatorskie rozwiązania. Kluczowe wyzwania regulacyjne obejmują weryfikację wydajności w szerokim zakresie warunków awaryjnych, ocenę niskich sił napędowych oraz sprawdzanie niezawodności bez udziału człowieka lub aktywnych komponentów. Organy regulacyjne, takie jak we Francji (ASNR)[3], Kanadzie (CNSC)[4] oraz w USA (NRC), aktywnie dokonują przeglądu technik oceny, aby poradzić sobie z oceną bezpieczeństwa wprowadzania tych systemów, koncentrując się na szukaniu rozwiązania problemu braku danych eksploatacyjnych i identyfikacji potencjału wystąpienia awarii o wspólnej przyczynie w zjawiskach naturalnych. Zasady UE dotyczące biernych systemów bezpieczeństwa w reaktorach jądrowych są głównie regulowane przez Dyrektywę o bezpieczeństwie jądrowym (2009/71/Eur-

[3] Francuski urząd ds. bezpieczeństwa jądrowego i ochrony radiologicznej ASNR (*Autorité de sûreté nucléaire et radioprotection*) działa od 1 stycznia 2025; powstał w wyniku scalenia organizacji regulatora – urzędu dozoru jądrowego ASN (*Autorité de sûreté nucléaire*) z instytutem ochrony radiologicznej i bezpieczeństwa jądrowego IRSN (*Institut de radioprotection et de sûreté nucléaire*) pełniącym poprzednio rolę TSO dla ASN (przyp. red).

[4] Kanadyjski urząd dozoru bezpieczeństwa jądrowego CNSC (*Canadian Nuclear Safety Commission*).

atom, zmienioną w 2014 roku), która ustanawia ogólne, prawnie wiążące wymagania dla państw członkowskich w celu zwiększenia bezpieczeństwa, szczególnie po wypadku w Fukushimie Daiichi. Chociaż nie nakładają one obowiązku stosowania konkretnych technologii, przepisy te podkreślają znaczenie wdrażania zaawansowanych funkcji bezpieczeństwa, w tym systemów biernych, w celu zapewnienia długoterminowego chłodzenia i utrzymania układu bez aktywnego, działania ludzkiego lub systemu zasilania elektrycznego. Dużą rolę w ocenie skuteczności i prawidłowości zastosowanych systemów odgrywają zarówno metody obliczeniowe, jak i eksperyment, które są niezbędne do określenia właściwego zastosowania rozwiązań w przypadku wykorzystania pasywnych systemów bezpieczeństwa. Bardzo aktywne w tych działaniach w zakresie wdrażania następnej generacji reaktorów jądrowych (Gen III+ i SMR) są Chiny i Korea Południowa. W Polsce istnieją ośrodki, które są w stanie weryfikować modele i kody przekazywane przez ewentualnych dostawców technologii i takie działania powinny być prowadzone w ramach wsparcia regulatora przez dobrze zorganizowaną strukturę wsparcia technicznego (TSO) [25].

7. Wnioski

- Nowe projekty reaktorów coraz częściej wykorzystują pasywne elementy bezpieczeństwa w różnych celach, na przykład do chłodzenia rdzenia podczas przejściowych stanów pracy, awarii projektowych, a nawet poważnych awarii, a także do chłodzenia obudowy bezpieczeństwa, przyjmując, że systemy pasywne są wysoce niezawodne i zmniejszają koszty związane z instalacją oraz konserwacją systemów wymagających stosowania wielu urządzeń, w tym kosztownych pomp, silników i innych systemów, a też redundantnych źródeł zasilania energią elektryczną.
- Ocena niezawodności systemu pasywnego jest trudnym zadaniem. Wymaga jasnego zrozumienia fizyki zjawisk i możliwego mechanizmu awarii systemu pasywnego, co projektant musi zrobić przed przewidywaniem jego niezawodności.
- Regulatorzy bezpieczeństwa jądrowego na całym świecie stoją przed istotnymi wyzwaniami w ocenie bezpieczeństwa nowych biernych systemów i nowych rozwiązań innowacyjnych projektów reaktorów. Aby wykazać niezawodność systemów biernych lub ich cech zapewnienia bezpieczeństwa eksploatacji reaktora, a także uwzględnić niezależność różnych poziomów „obrony w głąb", wymagania dotyczące projektowania, metod i narzędzi obliczeniowych do analiz zjawisk fizycznych, a również testów eksperymentalnych do weryfikacji mają zasadnicze znaczenie.

Notka o autorach

Prof. dr hab. inż. Andrzej G. Chmielewski jest dyrektorem Instytutu Chemii i Techniki Jądrowej, będącego Collaborating Centre IAEA oraz wiceprzewodniczącym Rady Bezpieczeństwa Jądrowego i Ochrony Radiologicznej przy Prezesie PAA. Przez wiele lat pracował w Politechnice Warszawskiej, University of Tennessee, USA oraz Międzynarodowej Agencji Energii Atomowej, Wiedeń, Austria. W latach 1990–2011 był wiceprzewodniczącym i przewodniczącym Rady ds. Atomistyki przy Prezesie PAA. Pełnił funkcje prezesa PTN i SEREN, a także przez szereg lat był członkiem SAGNA, organu doradczego DDG NA IAEA.

Dr hab. inż. Antoni Rożeń jest adiunktem na Wydziale Inżynierii Chemicznej i Procesowej Politechniki Warszawskiej. Stopień doktora nauk technicznych uzyskał w 1996 r., a stopień doktora habilitowanego w dyscyplinie inżynieria chemiczna w 2008 r.. W latach 1997–1998 odbył staże naukowe w DSM Research w Geleen oraz na University of Groningen (Holandia). Istotnym obszarem jego prac jest problematyka bezpieczeństwa jądrowego, w szczególności modelowanie procesów katalitycznej rekombinacji wodoru z tlenem w pasywnych rekombinatorach stosowanych do ograniczania ryzyka wybuchu wodoru w obudowach bezpieczeństwa reaktorów jądrowych. Badania te obejmują analizę sprzężenia zjawisk transportowych, kinetyki reakcji oraz warunków przepływu, mających kluczowe znaczenie dla skuteczności działania systemów bezpieczeństwa.

Literatura

1. IAEA, Use of Passive Safety Features in Nuclear Power Plant Designs and their Safety Assessment, https://www.iaea.org/topics/design-safety-nuclear -power-plants/passive-safety-features
2. NEA. Survey on the Regulatory Practice to Assess Passive Safety Systems used in New Nuclear Power Plant Designs. NEA/CNRA/R(2017)3; 11 February 2019. https://www.oecd-nea.org/upload/docs/application/ pdf/2020-01/dir1/cnra-r2017-3.pdf
3. Samuel Abiodun Olatubosun, Abiodun Ayodeji, Muritala Alade Amidu, Safety assessment of AP1000: Common transients, analysis codes and research gaps, Nuclear Engineering and Design, Volume 375, 2021, 111100, https://doi.org/10.1016/j.nucengdes.2021.111100.
4. Di Maio, F.; Pedroni, N.; Tóth, B.; Burgazzi, L.; Zio, E. Reliability Assessment of Passive Safety Systems for Nuclear Energy Applications: State-of-the-Art and Open Issues. Energies, 2021, 14, 4688. https://doi.org/10.3390/en14154688
5. S. Ali, K. Qureshi, Rab Nawaz. Safety Assessment of Advanced, 2018 International Conference on Power Generation Systems and Renewable Energy Technologies (PGSRET). https://doi.org/10.1109/PGSRET.2018.8686022, https://www.semanticscholar.org/paper/Safety-Assessment-of-Advanced-PWR-Ali-Qureshi/9a143d342c00557c589b2b3ccdde15673a90c5d7
6. Novikova G.S. and Bogoslovskaya G.P., Development of an Experimental Reactor VVER-SKD 30 MWonSupercritical Water. AtomFuture-2017,XIII International Youth Scientific and Practical Conference "FUTURE OF ATOMIC ENERGY- AtomFuture 2017", Volume 2017, https://doi.org/10.18502/keg.v3i3.1608.
7. Bird R.B., Stewart W.E., Lightfoot E.N., Transport Phenomena, 2nd ed., John Wiley & Sons, New York, 2002.
8. Idelchik I.E., Handbook of Hydraulic Resistance. Begell House, Inc.. NY, 3rd Ed. 1996, https://www.scribd.com/document/511743280/Handbook-of-Hydraulic-Resistance-by-I-E-Idelchik
9. Rohsenow W.M., Hartnett J.P., Cho Y.I. (eds.), Handbook of Heat Transfer, 3rd ed., McGraw-Hill, New York, 1998.
10. Incropera F.P., DeWitt D.P., Bergman T.L., Lavine A.S., Fundamentals of Heat and Mass Transfer, 6th ed., John Wiley & Sons, New York, 2007.

11. Poling B.E., Prausnitz J.M., O'Connell J.P., The Properties of Gases and Liquids, 5th ed., McGraw-Hill, New York, 2001.
12. NEA (2015), Best Practice Guidelines for the Use of CFD in Nuclear Reactor Safety Applications – Revision, OECD Publishing, (NEA/CSNI/R, 2014), Paris, https://www.oecd-nea.org/jcms/pl_19548/best-practice-guidelines-for-the-use-of-cfd-in-nuclear-reactor-s?details =true
13. NEA (2025), Best Practice Guidelines for the Use of CFD in Nuclear Reactor Safety Applications – 2024 Update, OECD Publishing, Paris, https://www.oecd-nea.org/jcms/pl_102607/best-practice-guidelines-for-the-use-of-cfd-in-nuclear-reactor-s upda?details=true
14. International Atomic Energy Agency (1991). Safety Related Terms for Advanced Nuclear Power Plant. Vienna: IAEA. https://www-pub.iaea.org/MTCD/Publications/PDF/te_626_web.pdf
15. Marcin Karol Rowinski, Jiyun Zhao, Timothy John White, Yeng Chai Soh, Safety analysis of Super-Critical Water Reactors–A review, Progress in Nuclear Energy,Volume 106,2018,Pages 87-101, https://doi.org/10.1016/j.pnucene.2018.03.002 https://www.researchgate.net/publication/345672373_Safety_analysis_ of_Super-Critical_Water_Reactors -A_review
16. Arun Kumar Nayak, Amit Chandrakar, Gopika Vinod A Review: Passive System Reliability Analysis – Accomplishments and Unresolved Issues, Front. Energy Res., 10 October 2014, Sec. Nuclear Energy Volume 2 – 2014, | https://doi.org/10.3389/fenrg.2014.00040
17. Status Report on Reliability of Thermal-Hydraulic Passive Systems. Nuclear Safety, NEA/CSNI/R(2021)2, October 2024.
18. Balendra Sutharshan, Meena Mutyala, Ronald P Vijuk and Alok Mishra The AP1000TM Reactor: Passive Safety and Modular Design. Energy Procedia 7 (2011) 293–302,https://doi.org/10.1016/j.egypro.2011.06.038
19. Daniel Freis, Norbert Haspel, Wolfgang Tietsch; AP1000TM Nuclear Power Plant Passive Safety System Actuation using Explosively Opening "Squib Valves" International Conference on Opportunities and Challenges for Water Cooled Reactors in the 21st Century.Vienna, Austria, 27–30 October 2009. BOOK OF EXTENDED SYNOPSES, IAEA-CN-164-3P10.
20. Daniel Hackl, Eileen Langegger, Helmuth Böck. Evolution of Safety Concepts in Pressurized Water Reactors.NENE 2024, 33rd International Conference Nuclear Energy for New Europe, Portož, Slovenia, September 19 – 22, 2024.
21. "Passive safety systems and natural circulation in water cooled nuclear power plants," IAEA-TECDOC-1624, IAEA, Vienna, Austria, 2009.
22. Zhuo Wenbin, Huang Yanping, Xiao Zejun, Peng Chuanxin, and Lu Sansan. Experimental Research on Passive Residual Heat Removal System of Chinese Advanced PWR. Science and Technology of Nuclear Installations. Volume 2014, Article ID 325356, 8 pages http://dx.doi.org/10.1155/2014/325356
23. Seok Kim a, Byoung-Uhn Bae a, Yun-Je Cho a, Yu-Sun Park a, Kyoung-Ho Kang a, Byong-Jo Yun. An experimental study on the validation of cooling capability for the Passive Auxiliary Feedwater System (PAFS) condensation heat exchanger. Nuclear Engineering and Design 260 (2013) 54–63, http://dx.doi.org/10.1016/j.nucengdes.2013.03.016
24. Xing Ji, Yuan Yidan, Han Xu, Yu Mingrui, Liu Zhuo, Wang Hongliang, Feng Yu. An Experimental Program for ACP100 Passive Containment Air Cooling System. International Conference on Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary and Innovative Reactor Designs. Vienna (Austria), 18-21 Oct 2022, https://inis.iaea.org/records/2qqj1-0kp36
25. Sommer S., Palige J., Polkowska H., Zakrzewska-Kołtuniewicz G., Zimek Z., & Chmielewski A. G. (2018). Technical and Scientific Support Organization (TSO) for nuclear power plant in Poland: the view of Research Institute. International Conference on Challenges Faced by Technical and Scientific Support Organizations (TSOs) in Enhancing Nuclear Safety and Security, Brussels (Belgium), 15–18 Oct 2018, https://inis.iaea.org/records/t4khw-dwk36

Ochrona radiologiczna pacjenta w stomatologii wsparta przepisami prawa w Polsce

Radiological protection of the patient in dentistry, based on Polish legal regulations

Karolina Jezierska[1], Paulina Rotter[2], Magdalena Sroczyk-Jaszczyńska[3]
[1] Zakład Fizyki Medycznej, Pomorski Uniwersytet Medyczny w Szczecinie
[2] Katedra i Zakład Pielęgniarstwa, Pomorski Uniwersytet Medyczny w Szczecinie
[3] Katedra i Zakład Radiologii Ogólnej, Stomatologicznej i Zabiegowej, Pomorski Uniwersytet Medyczny w Szczecinie

Streszczenie: Diagnostyka obrazowa z użyciem promieniowania X stanowi nieodłączny element współczesnej stomatologii i jest kluczowym narzędziem w rozpoznawaniu chorób zębów, przyzębia oraz struktur szczękowo-twarzowych. Badania radiologiczne umożliwiają wykrywanie zmian niewidocznych w badaniu klinicznym, ocenę stopnia zaawansowania choroby oraz planowanie i monitorowanie leczenia. W stomatologii najczęściej wykonywane badania obejmują zdjęcia wewnątrzustne, pantomograficzne oraz badania tomograficzne z wykorzystaniem wiązki stożkowej CBCT. Każda z tych metod charakteryzuje się innym zakresem informacji diagnostycznej, inną dawką skuteczną oraz odmiennym profilem ryzyka radiologicznego. Celem niniejszego artykułu jest omówienie zasad ochrony radiologicznej pacjenta w stomatologii z uwzględnieniem aktualnych wymagań prawnych, zaleceń międzynarodowych oraz wytycznych towarzystw naukowych. Ochrona radiologiczna pacjenta nie sprowadza się wyłącznie do redukcji dawki promieniowania ani do stosowania środków ochrony indywidualnej. Istotnym jej celem jest takie zminimalizowanie narażenia, które nie będzie nadmiernie utrudniało lub uniemożliwiało uzyskanie pożądanych i uzasadnionych informacji diagnostycznych lub efektów leczniczych. Współczesna ochrona radiologiczna pacjenta w stomatologii powinna być postrzegana jako proces ciągły, integrujący wymagania prawne, zalecenia naukowe i realia codziennej praktyki klinicznej.

Słowa kluczowe: Diagnostyka rtg, stomatologia, ochrona radiologiczna, prawo energii jądrowej.

Abstract: *X-ray-based diagnostic imaging is an integral part of modern dentistry and a key tool for diagnosing diseases of the teeth, periodontium, and maxillofacial structures. Radiographic examinations enable the detection of abnormalities invisible during clinical examination, the assessment of disease progression, and the planning and monitoring of treatment. The most frequently performed dental examinations include intraoral radiographs, panoramic radiographs, and CBCT scans. Each of these methods offers a different scope of diagnostic information and entails a different effective dose and radiological risk profile. This article aims to discuss the principles of patient radiation protection in dentistry, taking into account current legal requirements, international recommendations, and guidelines from scientific societies. Patient radiation protection is not limited merely to reducing radiation doses or using personal protective equipment. A key objective of it is to minimize exposure in a way that does not unduly hinder or prevent the acquisition of desired and justified diagnostic information or therapeutic outcomes.Modern patient radiation protection in dentistry should be viewed as a continuous process that integrates legal requirements, scientific recommendations, and the realities of daily clinical practice.*

Keywords*: X-ray diagnostics, dentistry, radiation protection, nuclear law.*

Wstęp

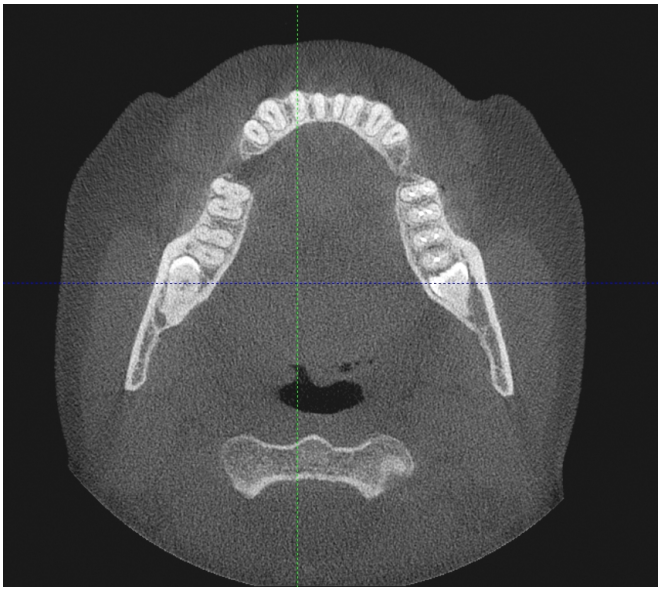
Diagnostyka obrazowa z użyciem promieniowania X stanowi nieodłączny element współczesnej stomatologii i jest kluczowym narzędziem w rozpoznawaniu chorób zębów, przyzębia oraz struktur szczękowo-twarzowych. Badania radiologiczne umożliwiają wykrywanie zmian niewidocznych w badaniu klinicznym, ocenę stopnia zaawansowania choroby oraz planowanie i monitorowanie leczenia. Jednocześnie stomatologia jest dziedziną medycyny, w której wykonuje się jedną z największych liczb ekspozycji medycznych z użyciem promieniowania jonizującego, choć dawki jednostkowe są relatywnie niskie [1]. W wielu krajach badania radiologiczne w stomatologii stanowią znaczną część wszystkich procedur rentgenowskich – np. w Niemczech około 39% wszystkich badań rentgenowskich to badania stomatologiczne, przy czym ich udział w łącznej dawce promieniowania jest niski (około 0,3%) [2].

Niska dawka pojedynczego badania nie zwalnia jednak z obowiązku stosowania zasad ochrony radiologicznej pacjenta. Skumulowana liczba ekspozycji, powszechna dostępność aparatów rentgenowskich oraz rosnące wykorzystanie tomografii wiązki stożkowej CBCT[1] (ang. *Cone Beam Computed Tomography*) sprawiają, że zagadnienie ochrony radiologicznej w gabinecie stomatologicznym pozostaje aktualnym i istotnym problemem klinicznym. Szczególne znaczenie ma to w populacjach wrażliwych, takich jak dzieci i kobiety w ciąży.

Badanie radiologiczne w stomatologii pełni funkcję uzupełniającą badanie kliniczne i nie powinny być traktowane jako procedury rutynowe. Ich głównym celem jest dostarczenie informacji diagnostycznej, której nie można uzyskać innymi metodami, z jednoczesnym zachowaniem możliwie najniższej dawki promieniowania, zapewniającej uzyskanie informacji diagnostycznej [3]. Najczęściej wykonywane badania obejmują zdjęcia wewnątrzustne (fot. 1), pantomograficzne (fot. 2) oraz – coraz częściej – badania CBCT (fot. 3, fot. 4). Każda z tych metod charakteryzuje się innym zakresem informacji diagnostycznej, inną dawką skuteczną oraz odmiennym profilem ryzyka radiologicznego.



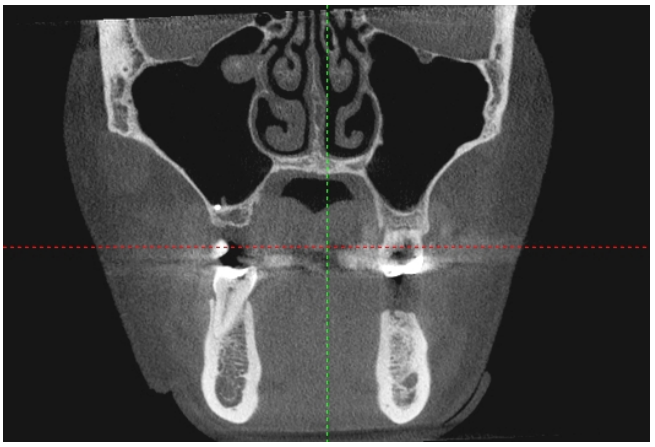
Fot. 2. Zdjęcie pantomograficzne.
Photo 2. *Pantomographic image.*



Fot. 3. Obraz z tomografii wiązki stożkowej (przykład 1).
Photo 3. *Cone-beam computed tomography image (example 1).*



Fot. 1. Zdjęcie wewnątrzustne.
Photo 1. *Intraoral photograph.*



Fot. 4. Obraz CBCT (przykład 2).
Photo 4. *CBCT image (example 2).*

[1] CBCT – tomografia komputerowa z wiązką w kształcie stożka, inne stosowane określenie tomografia wolumetryczna.

Właściwe wykorzystanie diagnostyki obrazowej wymaga nie tylko znajomości możliwości technicznych aparatury, ale przede wszystkim umiejętności krytycznej oceny potrzeby wykonania badania. Decyzja o ekspozycji pacjenta powinna każdorazowo wynikać z konkretnego problemu klinicznego i mieć realny wpływ na dalsze postępowanie diagnostyczno-terapeutyczne. To właśnie na etapie podejmowania decyzji o wykonaniu badania radiologicznego realizuje się najważniejszy element ochrony radiologicznej pacjenta – uzasadnienie ekspozycji, które w stomatologii ma znaczenie większe niż sama optymalizacja parametrów technicznych.

Celem niniejszego artykułu jest omówienie zasad ochrony radiologicznej pacjenta w stomatologii z uwzględnieniem aktualnych wymagań prawnych, zaleceń międzynarodowych oraz aktualnego stanowiska Europejskiego Towarzystwa Endodontycznego. Szczególny nacisk położono na uzasadnienie ekspozycji, optymalizację dawki oraz rolę kontroli jakości i audytu klinicznego. Artykuł koncentruje się na najczęściej wykonywanych procedurach obrazowania w stomatologii, takich jak radiografia wewnątrzustna, pantomograficzna oraz tomografia wiązki stożkowej (CBCT).

Polskie normy prawne

Podstawowymi aktami prawnymi dotyczącymi ochrony pacjenta podczas badania radiologicznego w gabinecie stomatologicznym są: ustawa z dnia 16 czerwca 2023 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. poz. 1675) [4], ustawa z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty (Dz.U. z 2026 r. poz. 37, 203) [5], dwa rozporządzenia Ministra Zdrowia:

1) z dnia 11 stycznia 2023 r. w sprawie warunków bezpiecznego stosowania promieniowania jonizującego dla wszystkich rodzajów ekspozycji medycznej (Dz.U. 2025 poz. 1288) [3],
2) z dnia 8 marca 2023 r. w sprawie szczególnej ochrony niektórych kategorii osób w związku z ekspozycją medyczną w badaniach diagnostycznych, zabiegach i leczeniu (Dz.U. poz. 576) [6].

Oba akty normatywne są aktami wykonawczymi wydanymi na podstawie norm kompetencyjnych ustanowionych w ustawie z dnia 29 listopada 2000 r. – Prawo atomowe[2] (Dz.U. z 2026 r.poz.1, 1097) [7]. W pierwszym z rozporządzeń określa się m.in.: warunki bezpiecznego stosowania promieniowania jonizującego dla wszystkich rodzajów ekspozycji medycznej oraz szczegółowe wymagania dla urządzeń radiologicznych oraz urządzeń pomocniczych. W drugim określa się wymagania w zakresie szczególnej ochrony w związku z ekspozycją medyczną w badaniach diagnostycznych, zabiegach i leczeniu kobiet w wieku rozrodczym, kobiet w ciąży, kobiet karmiących piersią, osób poniżej 16. roku życia, a także opiekunów oraz osób z otoczenia i rodziny pacjentów. Rozporządzenie dotyczy wszystkich rodzajów badań diagnostycznych, w których stosowane jest promieniowanie jonizujące. Nie zawiera odrębnych przepisów dotyczących badań radiologicznych w stomatologii, co oznacza, że lekarz dentysta zobowiązany jest do stosowania ogólnych wymagań dotyczących ochrony radiologicznej pacjenta, analogicznie jak w innych dziedzinach diagnostyki obrazowej.

W Polsce przepisy prawa nie wyszczególniają zasad stosowania badania CBCT. Zalecenia w tej kwestii zawarte są w Publikacji Ochrony Radiologicznej 172 Komisji Europejskiej (zwane jako Sedentexct)[3] [8]. Ponadto zalecenia w zakresie stosowania CBCT są publikowane przez towarzystwa naukowe m.in. Europejskie Towarzystwo Endodontyczne[4] [9]. Zawierają one m.in. uzasadnienia tego badania, optymalizację ekspozycji na promieniowanie, a także określają zakres wymaganych szkoleń dla użytkowników.

Międzynarodowym źródłem prawa w Polsce jest też Dyrektywa Rady 2013/59/EURATOM z dnia 5 grudnia 2013 r. ustanawiająca podstawowe normy bezpieczeństwa w celu ochrony przed zagrożeniami wynikającymi z narażenia na działanie promieniowania jonizującego [10], transponowana do polskich przepisów rangi ustawowej.

Interpretując art. 91 Konstytucji RP, stwierdza się, że źródła prawa międzynarodowego, które wiążą Polskę, mają pierwszeństwo przed ustawą, czyli wewnętrznym źródłem prawa, jeżeli przepisy tej ustawy nie są zgodne z umową międzynarodową [11].

Źródłem prawa międzynarodowego w omawianym obszarze są więc dyrektywa, której przepisy wiążą Polskę oraz zalecenia dotyczące badania radiologicznego. Te ostatnie są dokumentami niewiążącymi, ale można je umieszczać w sferze systemu aktów prawnych i stosować jako swego rodzaju *soft law*.

Zasada ALARA i jej ewolucja

Podstawową zasadą ochrony radiologicznej pacjenta jest zasada ALARA (*As Low As Reasonably Achievable*), zgodnie z którą narażenie na promieniowanie jonizujące powinno być utrzymywane na możliwie najniższym poziomie, osiągalnym w danych warunkach technicznych i organizacyjnych, z uwzględnieniem czynników społecznych i ekonomicznych. Zasada ta znalazła szerokie zastosowanie w radiologii medycznej, w tym w diagnostyce stomatologicznej, i stanowi fundament obowiązujących przepisów prawnych oraz zaleceń międzynarodowych. Prawo-

2 dalej ustawy.
3 SEDENTEXCT (*Safety and Efficacy of a New and Emerging Dental X-ray Modality*). Projekt opracowany przez Konsorcjum SEDENTEXCT, oparty na wieloośrodkowej współpracy określenia zasad pracy dla nowej metody obrazowania (CBCT).
4 European Society of Endodontology Position Statement: *Use of cone beam computed tomography in Endodontics*.

dawca stanowi o tym w § 5 ust. 1 pkt 2 Rozporządzenia Ministra Zdrowia z dnia 11 stycznia 2023 r. w sprawie warunków bezpiecznego stosowania promieniowania jonizującego dla wszystkich rodzajów ekspozycji medycznej [3].

W praktyce klinicznej stomatologii ścisłe stosowanie zasady ALARA wyłącznie w kontekście redukcji dawki może jednak prowadzić do niepożądanych konsekwencji, takich jak pogorszenie jakości obrazu diagnostycznego i ograniczenie jego przydatności klinicznej. Zbyt agresywna redukcja parametrów ekspozycji może skutkować koniecznością powtarzania badań, co w efekcie prowadzi do zwiększenia całkowitej dawki pochłoniętej przez pacjenta i pozostaje w sprzeczności z ideą ochrony radiologicznej.

Z tego względu w ostatnich latach coraz większy nacisk kładzie się na modyfikację klasycznej zasady ALARA w kierunku podejścia bardziej zorientowanego na wartość diagnostyczną badania. W stomatologii znajduje to odzwierciedlenie w koncepcji ALADA (*As Low As Diagnostically Acceptable*), zgodnie z którą dawka promieniowania powinna być możliwie niska, ale jednocześnie wystarczająca do uzyskania obrazu o akceptowalnej wartości diagnostycznej [12, 13, 14, 15]. Podejście to podkreśla, że celem ekspozycji medycznej nie jest minimalizacja dawki sama w sobie, lecz uzyskanie informacji niezbędnej do prawidłowego rozpoznania i leczenia pacjenta.

Dalszym rozwinięciem tej filozofii jest koncepcja ALADAIP (*As Low As Diagnostically Acceptable, Indication-oriented and Patient-specific*), która uwzględnia nie tylko wartość diagnostyczną obrazu, ale również konkretne wskazanie kliniczne oraz indywidualne cechy pacjenta [16]. W tym ujęciu optymalizacja dawki nie polega na stosowaniu jednego, „uniwersalnego" protokołu badania, lecz na dostosowaniu zakresu obrazowania i parametrów ekspozycji do wieku pacjenta, budowy anatomicznej, obszaru zainteresowania oraz celu klinicznego badania. Znaczenie podejścia ALADAIP jest szczególnie istotne w stomatologii, gdzie dostępnych jest wiele metod obrazowania o zróżnicowanym zakresie informacji diagnostycznej i bardzo różnych dawkach promieniowania. Dotyczy to w szczególności tomografii wolumetrycznej CBCT, która – mimo wysokiej wartości diagnostycznej – wiąże się z istotnie większą dawką skuteczną w porównaniu do klasycznych badań wewnątrzustnych czy pantomograficznych [17]. Zastosowanie CBCT powinno być zatem ściśle ograniczone do sytuacji klinicznych, w których informacje uzyskane w badaniach dwuwymiarowych są niewystarczające [9].

W praktyce klinicznej wdrożenie zasad ALADA i ALADAIP wymaga od lekarza dentysty nie tylko znajomości podstaw ochrony radiologicznej, lecz także umiejętności krytycznej oceny wskazań do badania oraz świadomego wyboru metody obrazowania. Optymalizacja dawki rozpoczyna się bowiem na etapie decyzji o wykonaniu badania, a nie w momencie doboru parametrów technicznych aparatu. W tym sensie uzasadnienie ekspozycji stanowi nadrzędny element ochrony radiologicznej pacjenta w stomatologii, a zasady ALARA, ALADA i ALADAIP powinny być traktowane jako wzajemnie uzupełniające się narzędzia wspierające racjonalne wykorzystanie diagnostyki obrazowej.

Sprzęt stosowany w diagnostyce radiologicznej w stomatologii

Sprzęt wykorzystywany w diagnostyce radiologicznej w stomatologii obejmuje urządzenia o zróżnicowanym stopniu zaawansowania technicznego, zakresie obrazowania oraz profilu narażenia radiologicznego pacjenta. Właściwy dobór, eksploatacja i kontrola jakości aparatury stanowią istotny element ochrony radiologicznej pacjenta [18].

Z punktu widzenia ochrony radiologicznej kluczowe znaczenie mają nie tylko parametry nominalne aparatu, ale również jego stan techniczny, sposób użytkowania oraz zgodność z obowiązującymi wymaganiami prawnymi zawartymi przede wszystkim w rozdziale 3 ustawy [7]. Nawet nowoczesne urządzenie, użytkowane niezgodnie z przeznaczeniem lub bez regularnej kontroli jakości, może prowadzić do nieuzasadnionego zwiększenia dawki promieniowania [19].

Jak już wspomniano, aparaty do wykonywania zdjęć wewnątrzustnych (fot. 5) stanowią podstawowe wyposa-



Fot. 5. Aparat do wykonywania zdjęć wewnątrzustnych.
Photo 5. *Intraoral imaging device.*

żenie większości gabinetów stomatologicznych i są najczęściej wykorzystywanym źródłem ekspozycji pacjentów na promieniowanie jonizujące w stomatologii. Charakteryzują się one relatywnie niską dawką jednostkową oraz ograniczonym polem obrazowania, co sprzyja spełnieniu zasad optymalizacji dawki.

Nowoczesne aparaty wewnątrzustne wyposażone są zazwyczaj w:

- stabilne generatory wysokiego napięcia [20],
- krótkie czasy ekspozycji [21],
- kolimację prostokątną bądź okrągłą [22],
- możliwość współpracy z cyfrowymi detektorami obrazu [23].

Zastosowanie cyfrowych systemów obrazowania umożliwia obniżenie dawki promieniowania w porównaniu z klasycznymi filmami analogowymi, jednak samo posiadanie detektora cyfrowego nie gwarantuje optymalizacji dawki. Kluczowe pozostaje właściwe dobranie parametrów ekspozycji, prawidłowe pozycjonowanie pacjenta oraz unikanie powtórzeń badań wynikających z błędów technicznych.

Radiografia panoramiczna umożliwia jednoczesną ocenę obu łuków zębowych oraz struktur szczękowo-twarzowych przy relatywnie umiarkowanej dawce promieniowania. Aparaty pantomograficzne (fot. 6) są powszechnie wykorzystywane w diagnostyce ogólnej, planowaniu leczenia protetycznego, ortodontycznego oraz chirurgicznego.

W kontekście ochrony radiologicznej istotne jest:

- stosowanie programów ekspozycji dostosowanych do wieku i budowy pacjenta,
- ograniczanie pola obrazowania do obszaru zainteresowania klinicznego,
- szczególna ostrożność w badaniach dzieci i młodzieży [24].

Niewłaściwe pozycjonowanie pacjenta w aparacie pantomograficznym jest jedną z najczęstszych przyczyn powtarzania badań, co prowadzi do niepotrzebnego zwiększenia dawki skutecznej [25]. Podkreśla to znaczenie szkolenia personelu oraz bieżącej kontroli jakości obrazu.

Tomografia wolumetryczna CBCT (fot. 6) stanowi najbardziej zaawansowaną technicznie metodę obrazowania stosowaną w stomatologii, umożliwiającą uzyskanie trójwymiarowych obrazów struktur anatomicznych o wysokiej rozdzielczości przestrzennej. Jednocześnie jest to metoda wiążąca się z istotnie wyższą dawką promieniowania w porównaniu do klasycznych badań dwuwymiarowych [26].

Dawka skuteczna w badaniach CBCT zależy od wielu czynników, w tym:

- wielkości pola obrazowania (FOV)[5],
- parametrów ekspozycji,
- zastosowanego protokołu badania,
- konstrukcji i generacji aparatu [27].



Fot. 6. Aparat pantomograficzny.
Photo 6. *Pantomographic unit.*

Analizując przepisy zawarte w rozporządzeniu Ministra Zdrowia z dnia 11 stycznia 2023 r. w sprawie warunków bezpiecznego stosowania promieniowania jonizującego dla wszystkich rodzajów ekspozycji medycznej, wnioskuje się, że nie wprowadzono odrębnej kategorii urządzeń dla tomografii wolumetrycznej CBCT i radiografii pantomograficznej [3]. Z formalnego punktu widzenia aparat pantomograficzny z funkcją CBCT traktowany jest jako jedno urządzenie rentgenowskie, bez rozróżnienia poszczególnych trybów pracy. W praktyce klinicznej oba tryby obrazowania mogą być realizowane w ramach jednego urządzenia radiologicznego, wyposażonego w jedną lampę rentgenowską, posiadającego jeden numer seryjny oraz jedno zezwolenie na użytkowanie (fot. 6). Brak odrębnych regulacji prawnych dla badań CBCT i pantomograficznych nie oznacza jednak ich równoważności z punktu widzenia ochrony radiologicznej pacjenta. Badania te stanowią odmienne procedury diagnostyczne, różniące się geometrią wiązki promieniowania, sposobem akwizycji danych oraz profilem dawki promieniowania. W szczególności tomografia wolumetryczna CBCT wiąże się z istotnie wyższą dawką skuteczną w porównaniu z klasyczną radiografią panoramiczną, co wymaga każdorazowego, odrębnego uzasadnienia klinicznego oraz świadomej optymalizacji parametrów ekspozycji [28]. Tym samym, mimo wspólnej

[5] FOV (*Field of View*) – skanowanie: z dużym polem widzenia pozwala na uzyskanie obrazów całego szkieletu czaszkowo-twarzowego; ze średnim polem widzenia obejmuje szczękę, żuchwę lub obie te struktury; z ograniczonym lub ukierunkowanym polem widzenia dostarcza obrazów o wysokiej rozdzielczości, obejmujących wybrane obszary.

infrastruktury technicznej i formalnej, decyzja o zastosowaniu CBCT powinna być traktowana jako osobna decyzja kliniczna w kontekście ochrony radiologicznej pacjenta.

Raport w sprawie zastosowania badania CBCT wydała Komisja Europejska. Jest on zawarty w publikacji Radiation Protection No 172 [8]. Ponadto Europejskie Towarzystwo Endodontyczne zajęło stanowisko w sprawie korzystania z CBCT i opublikowało wykaz zaleceń [9].

Zgodnie z obowiązującymi przepisami prawa odpowiedzialność za bezpieczne użytkowanie aparatury radiologicznej spoczywa na podmiocie wykonującym działalność leczniczą oraz osobach wykonujących badania. Wynika to z art. 33j ustawy. Obejmuje to nie tylko zapewnienie zgodności urządzeń z wymaganiami technicznymi, lecz także ich właściwą eksploatację, regularną kontrolę jakości oraz dokumentowanie stanu technicznego aparatury [7]. W tym kontekście sprzęt radiologiczny nie może być traktowany wyłącznie jako narzędzie diagnostyczne, lecz jako integralny element systemu ochrony radiologicznej pacjenta, którego właściwe funkcjonowanie warunkuje bezpieczeństwo i skuteczność diagnostyki obrazowej w stomatologii.

Kontrola jakości aparatury radiologicznej i przeglądy okresowe

Kontrola jakości aparatury radiologicznej stanowi integralny element systemu ochrony radiologicznej pacjenta w stomatologii. Jej celem jest zapewnienie, że urządzenia radiologiczne pracują zgodnie z deklarowanymi parametrami technicznymi, umożliwiają uzyskanie obrazu o odpowiedniej wartości diagnostycznej oraz nie prowadzą do nieuzasadnionego zwiększenia dawki promieniowania. Z punktu widzenia ochrony radiologicznej regularna kontrola jakości ma szczególne znaczenie w stomatologii, gdzie pojedyncze dawki są relatywnie niskie, lecz liczba wykonywanych badań jest bardzo duża. Nawet niewielkie odchylenia parametrów ekspozycji, niezauważalne w codziennej praktyce klinicznej, mogą prowadzić do systematycznego wzrostu dawki otrzymywanej przez pacjentów lub do pogorszenia jakości obrazu skutkującego koniecznością powtarzania badań.

Zgodnie z art. 33l ust. 2 ustawy system kontroli jakości aparatury radiologicznej obejmuje kilka poziomów testów, różniących się zakresem i częstotliwością wykonywania:

Testy akceptacyjne wykonywane są przed dopuszczeniem aparatu do użytkowania klinicznego oraz po istotnych naprawach lub modyfikacjach technicznych. Ich celem jest potwierdzenie, że urządzenie spełnia wymagania określone w dokumentacji technicznej oraz przepisach prawa i może być bezpiecznie użytkowane w diagnostyce pacjentów [7].

Testy podstawowe realizowane są okresowo w trakcie eksploatacji aparatury. Obejmują one m.in. kontrolę powtarzalności i odtwarzalności parametrów ekspozycji, ocenę geometrii wiązki promieniowania, funkcjonowania kolimacji oraz podstawowych parametrów jakości obrazu. Regularne wykonywanie testów podstawowych pozwala na wczesne wykrycie nieprawidłowości technicznych i zapobieganie pogorszeniu jakości diagnostycznej badań.

Testy specjalistyczne wykonywane są przez uprawnione podmioty oraz po naprawach aparatury. Obejmują one szczegółową ocenę parametrów fizycznych aparatu, takich jak napięcie lampy, czas ekspozycji, dawka wyjściowa czy jednorodność pola promieniowania [7].

Obowiązek utrzymywania aparatury radiologicznej w należytym stanie technicznym wynika z przepisów ustawy oraz rozporządzenia Ministra Zdrowia z dnia 11 stycznia 2023 r. w sprawie warunków bezpiecznego stosowania promieniowania jonizującego [3, 7]. Choć przepisy nie posługują się wprost pojęciem „przeglądu serwisowego", wymagają zapewnienia sprawności technicznej urządzeń, wykonywania okresowych testów specjalistycznych oraz eksploatacji aparatury zgodnie z instrukcją producenta, co w praktyce oznacza konieczność regularnych przeglądów technicznych. Przeglądy te, wykonywane co najmniej raz w roku, mają na celu potwierdzenie, że urządzenie jest sprawne technicznie i spełnia wymagania w zakresie ochrony radiologicznej pacjenta. Coroczne przeglądy aparatury radiologicznej nie powinny być traktowane wyłącznie jako formalny obowiązek administracyjny. Ich istotą jest zapewnienie ciągłości bezpiecznej eksploatacji urządzeń oraz ograniczenie ryzyka wzrostu dawek promieniowania wynikającego z nieprawidłowej pracy aparatu lub stopniowego pogarszania się jego parametrów technicznych. Wyniki przeglądów i testów kontroli jakości powinny być dokumentowane i analizowane w kontekście jakości uzyskiwanych obrazów oraz liczby powtarzanych badań. Jak wynika z art. 33 1 ust. 14 ustawy, jednostka ochrony zdrowia przechowuje protokoły wyników testów przez okres nie krótszy niż 10 lat, licząc od końca roku kalendarzowego, w którym testy zostały wykonane [7].

Skutecznie funkcjonujący system kontroli jakości aparatury radiologicznej ma bezpośredni wpływ na ochronę radiologiczną pacjenta. Prawidłowo utrzymany aparat umożliwia stosowanie zoptymalizowanych parametrów ekspozycji, zmniejsza ryzyko błędów technicznych oraz ogranicza konieczność powtarzania badań. Kontrola jakości stanowi również istotny element audytu klinicznego i powinna być traktowana jako proces ciągły, obejmujący zarówno aspekty techniczne, jak i organizacyjne [29]. W Polsce obowiązek prowadzenia kontroli jakości jest określony w przepisach ustawy. Jak wynika z art. 33l ust. 10 ustawy, sposób jego realizacji bywa zróżnicowany i zależny od organizacji pracy gabinetu, świadomości personelu oraz dostępności wsparcia inspektora ochrony radiologicznej, fizyka medycznego lub serwisu technicznego [7].

W praktyce klinicznej jednym z najbardziej wymiernych wskaźników jakości aparatury radiologicznej jest liczba

badań powtórnych. Powtarzanie ekspozycji – niezależnie od tego, czy wynika z błędów pozycjonowania pacjenta, niewłaściwych parametrów ekspozycji czy problemów technicznych aparatu – stanowi bezpośredni sygnał zaburzenia systemu kontroli jakości i prowadzi do nieuzasadnionego zwiększenia dawki promieniowania pacjenta. Systematyczna analiza przyczyn badań powtórnych mogłaby w wielu gabinetach stanowić prosty, a jednocześnie skuteczny element optymalizacji ochrony radiologicznej. Doświadczenia praktyczne pokazują również, że tam, gdzie kontrola jakości jest traktowana jako element kultury pracy – a nie wyłącznie obowiązek formalny – możliwe jest skuteczne ograniczenie liczby błędów technicznych oraz poprawa powtarzalności jakości obrazów bez konieczności zwiększania dawek promieniowania. Wymaga to jednak jasno określonych procedur wewnętrznych, regularnych szkoleń personelu oraz współpracy z osobami posiadającymi kompetencje w zakresie ochrony radiologicznej.

Jak wynika z art. 33 l. ust. 2 ustawy, testy kontroli jakości są jednym z warunków ochrony radiologicznej [7]. Niewykonywanie testów kontroli jakości w wymaganych terminach stanowi naruszenie warunków ochrony radiologicznej. Art. 123 ustawy stanowi, że naruszenia te mogą skutkować nałożeniem administracyjnej kary pieniężnej, której wysokość ustalana jest indywidualnie przez organ nadzorczy w zależności od stopnia i czasu trwania naruszenia, a także stwarzanego zagrożenia dla zdrowia pacjentów [7].

Osłony indywidualne pacjenta w stomatologii – przepisy prawa i zalecenia międzynarodowe

Stosowanie osłon indywidualnych u pacjentów poddawanych badaniom radiologicznym w stomatologii od wielu lat stanowi element rutynowej praktyki klinicznej. Współcześnie zagadnienie wymaga jednak krytycznej analizy w świetle aktualnych przepisów prawa, zaleceń międzynarodowych oraz postępu technologicznego w diagnostyce obrazowej. Minister Zdrowia, w rozporządzeniu z dnia 11 stycznia 2023 r. w sprawie warunków bezpiecznego stosowania promieniowania jonizującego dla wszystkich rodzajów ekspozycji medycznej, określił warunki podczas wykonywania medycznych procedur radiologicznych z zakresu rentgenodiagnostyki. Zgodnie z przepisem rozporządzenia zawartym w § 5 ust. 3 stosuje się osłony osobiste chroniące przed promieniowaniem jonizującym części ciała i narządy pacjenta niebędące przedmiotem badania, w szczególności znajdujące się w obrębie wiązki pierwotnej tego promieniowania, a w przypadku wykonywania procedur radiologicznych z zakresu stomatologii – osłony osobiste chroniące w szczególności tarczycę, jeżeli nie umniejsza to diagnostycznych wartości wyniku badania [3]. U dzieci tarczyca jest bardziej wrażliwa niż u dorosłych. W związku z tym pewną ochronę może zapewnić osłona tarczycy. Jednakże w pierwszej kolejności należy stosować kolimator prostokątny i położyć nacisk na właściwą technikę badania [30]. Zalecenia w kwestii osłon w postaci fartucha lub kołnierza ewaluują. Zalecenia wydane w 2024 r. przez ADA (*American Dental Association*) nie rekomendują rutynowego stosowania osłon jako substytutu właściwego uzasadnienia ekspozycji i optymalizacji dawki [31].

W Polsce przepisy nakładają obowiązek zapewnienia szczególnej ochrony wybranych grup pacjentów, w tym dzieci, młodzieży oraz kobiet w ciąży, co zostało doprecyzowane w rozporządzeniu Ministra Zdrowia z dnia 8 marca 2023 r. w sprawie szczególnej ochrony niektórych kategorii osób w związku z ekspozycją medyczną. Minister Zdrowia w rozporządzeniu jednoznacznie wskazuje w § 8, że podczas wykonywania u kobiety w wieku rozrodczym medycznej procedury radiologicznej należy stosować osłony indywidualne chroniące obszar brzucha lub miednicy, chyba że celem badania diagnostycznego, zabiegu lub leczenia są obszary brzucha lub miednicy albo zastosowanie osłon indywidualnych uniemożliwi uzyskanie wyniku badania o założonej jakości diagnostycznej lub terapeutycznej [6].

Aktualne zalecenia międzynarodowych organizacji zajmujących się ochroną radiologiczną pacjenta wskazują, że rutynowe stosowanie osłon indywidualnych u pacjentów w diagnostyce stomatologicznej nie jest konieczne w przypadku prawidłowo przeprowadzonych i zoptymalizowanych badań. Międzynarodowa Komisja Ochrony Radiologicznej (ICRP), Międzynarodowa Agencja Energii Atomowej (IAEA) oraz organizacje radiologiczne[6] podkreślają, że nowoczesne aparaty rentgenowskie, kolimacja wiązki oraz krótkie czasy ekspozycji skutecznie ograniczają dawkę promieniowania do obszaru badanego [30, 32, 33]. W szczególności zwraca się uwagę, że osłony ołowiane stosowane w obrębie jamy ustnej i szyi mogą w niektórych sytuacjach:

- nie wpływać istotnie na zmniejszenie dawki skutecznej,
- prowadzić do artefaktów obrazu,
- zwiększać ryzyko konieczności powtarzania badania,
- zaburzać automatyczne systemy kontroli ekspozycji w nowoczesnych urządzeniach [32].

Zalecenia międzynarodowe akcentują, że kluczowe znaczenie dla ochrony radiologicznej pacjenta ma ograniczenie pola obrazowania do obszaru zainteresowania klinicznego oraz dobór parametrów ekspozycji dostosowanych do wieku i budowy pacjenta, co jest zgodne z zasadą ALADAIP [16].

Szczególną uwagę w literaturze poświęca się stosowaniu kołnierzy ochronnych tarczycy. W starszych systemach obrazowania oraz przy braku precyzyjnej kolimacji stosowanie kołnierza mogło prowadzić do istotnego zmniej-

6 Takie jak np. *European Society of Endodontology*, czy *American Dental Association*.

szenia dawki pochłoniętej przez tarczycę. W nowoczesnej diagnostyce stomatologicznej, zwłaszcza przy radiografii wewnątrzustnej z kolimacją prostokątną oraz w badaniach panoramicznych i CBCT z odpowiednio dobranym polem obrazowania, skuteczność kołnierzy tarczycy jest ograniczona [34, 35, 36]. Międzynarodowe zalecenia wskazują, że stosowanie kołnierza tarczycy może być rozważane indywidualnie, szczególnie u dzieci, pod warunkiem, że nie wpływa negatywnie na jakość obrazu i nie zwiększa ryzyka powtarzania badania [31, 37]. Rutynowe stosowanie kołnierza u wszystkich pacjentów, niezależnie od rodzaju badania i aparatury, nie znajduje jednoznacznego uzasadnienia naukowego. Z punktu widzenia ochrony radiologicznej kluczowe jest, aby decyzja o zastosowaniu osłony była świadoma, uzasadniona i dostosowana do konkretnej procedury diagnostycznej.

Uzasadnienie ekspozycji – kluczowy element ochrony radiologicznej pacjenta. Skierowanie na badanie

Uzasadnienie ekspozycji stanowi podstawowy filar ochrony radiologicznej pacjenta w stomatologii. Oznacza ono, że każde badanie RTG powinno być wykonywane wyłącznie wtedy, gdy oczekiwana korzyść diagnostyczna przewyższa potencjalne ryzyko związane z promieniowaniem, a wynik badania może realnie wpłynąć na decyzje kliniczne. W praktyce gabinetowej zdjęcia bywają zlecane rutynowo (np. „przed leczeniem kanałowym", „przed ekstrakcją", „przed protetyką"), niezależnie od wywiadu i badania klinicznego. Zgodnie z § 3 ust. 2 rozporządzenia Ministra Zdrowia z dnia 11 stycznia 2023 r. badanie diagnostyczne z użyciem promieniowania jonizującego wykonuje się na podstawie skierowania lub zlecenia. Skierowanie poza danymi ogólnymi powinno zawierać m.in.: cel, uzasadnienie badania, wstępne rozpoznanie kliniczne, informacje istotne dla prawidłowego przeprowadzenia medycznej procedury radiologicznej [3].

Powtarzanie badań z powodu braku dostępu do wcześniejszej dokumentacji jest jednym z najczęstszych źródeł ekspozycji nieprzynoszącej pacjentowi dodatkowej wartości. Stosownie do normy art. 33 h ust. 2 ustawy do zadań lekarza należy kliniczna ocena wyniku badania diagnostycznego, zabiegu lub efektu terapeutycznego oraz przekazywanie informacji lub dokumentacji radiologicznej innym lekarzom zaangażowanym w proces badania diagnostycznego, zabiegu lub leczenia [7]. Z punktu widzenia uzasadnienia wykonanie kolejnego badania powinno następować tylko wtedy, gdy:

- poprzednie obrazy są niedostępne lub ich jakość/zakres jest niewystarczający do odpowiedzi na aktualne pytanie kliniczne,
- upłynął czas, w którym zaszły istotne zmiany kliniczne,
- zmienił się cel diagnostyczny.

Co spowodowało, że zmieniły się:

- cel i uzasadnienie badania,
- wstępne rozpoznanie kliniczne,
- informacje istotne dla prawidłowego wykonania procedury.

Zgodnie z § 3 ust. 3 ustawy skierowanie nie jest wymagane w przypadku stomatologicznych zdjęć wewnątrzustnych wykonywanych aparatami służącymi wyłącznie do tego celu [7]. Często bywa to mylnie interpretowane jako brak konieczności uzasadnienia. Uzasadnienie ekspozycji nadal obowiązuje prawnie i klinicznie – zmienia się jedynie jego forma (nie jest elementem skierowania).

W praktyce warto traktować „uzasadnienie" jako krótką, weryfikowalną odpowiedź na pytania:

1. Jaki problem kliniczny rozwiązuję?
2. Czy i dlaczego badanie 2D nie wystarczy?
3. Jak wynik wpłynie na leczenie?

Tak opisane uzasadnienie ogranicza „profilaktyczne" wykonywanie badań i ułatwia obronę decyzji klinicznej w razie kontroli lub sporu.

Wykonanie badania z użyciem promieniowania jonizującego u kobiety w ciąży wymaga szczególnej ostrożności. Przepisy nakładają wówczas obowiązek weryfikacji prawidłowości uzasadnienia przed wykonaniem procedury, a w praktyce oznacza to konieczność sprawdzenia wskazań i rozważenia innych możliwości (jeśli są adekwatne diagnostycznie). Zostało to ujęte w rozporządzeniu Ministra Zdrowia z dnia 8 marca 2023 r., w sprawie szczególnej ochrony niektórych kategorii osób w związku z ekspozycją medyczną w badaniach diagnostycznych, zabiegach i leczeniu [6]. W stomatologii badania nie obejmują jamy brzusznej, jednak decyzja o ekspozycji nadal musi być uzasadniona, a parametry i pole obrazowania – możliwie ograniczone do celu diagnostycznego.

W rozporządzeniach Minister Zdrowia nie określa szczególnej ochrony pacjentów w wieku podeszłym, zatem uzasadnienia ekspozycji pozostają takie same jak w populacji ogólnej, jednak decyzja o wykonaniu badania radiologicznego powinna uwzględniać specyfikę kliniczną tej grupy. Zgodnie z art. 68 Konstytucji RP zwraca się szczególną uwagę na dzieci, kobiety ciężarne, osoby z niepełnosprawnością i osoby starsze w zakresie ochrony zdrowia [11]. Częstsza obecność chorób przewlekłych, leczenia wielolekowego, zmian pourazowych i pozabiegowych oraz zaawansowanych zmian zwyrodnieniowych może zwiększać potrzebę diagnostyki obrazowej, ale jednocześnie sprzyjać wykonywaniu badań o ograniczonej wartości diagnostycznej. W praktyce szczególnego znaczenia nabiera precyzyjne określenie pytania klinicznego oraz dobór najprostszego badania zdolnego na nie odpowiedzieć. U pacjentów w wieku podeszłym potencjalne skutki stochastyczne ekspozycji na promieniowanie jonizujące, ze względu na dłuższy okres latencji nowotworów oraz krótszy oczekiwany czas życia, mają zwykle mniejsze znaczenie kliniczne niż u dzieci i młodych dorosłych, co nie znosi obowiązku uzasadnienia ekspozycji, lecz wpływa na proporcję ryzyka do spodziewanej korzyści diagnostycznej.

Podsumowanie

Ochrona radiologiczna pacjenta w stomatologii nie sprowadza się wyłącznie do redukcji dawki promieniowania ani do stosowania środków ochrony indywidualnej. Należy pamiętać, że ochrona radiologiczna pacjenta, stosownie do art. 3 pkt 21 ustawy, oznacza zespół czynności i ograniczeń zmierzających do zminimalizowania narażenia pacjenta na promieniowanie jonizujące, które nie będzie nadmiernie utrudniało lub uniemożliwiało uzyskanie pożądanych i uzasadnionych informacji diagnostycznych lub efektów leczniczych [7].

Jej fundamentem pozostaje uzasadnienie ekspozycji, rozumiane jako świadoma decyzja kliniczna poprzedzająca wykonanie badania radiologicznego i oparta na realnej potrzebie diagnostycznej. W warunkach powszechnej dostępności aparatów rentgenowskich oraz rosnącego wykorzystania tomografii wiązki stożkowej to właśnie etap podejmowania decyzji o wykonaniu badania ma największy wpływ na ograniczenie ekspozycji nieprzynoszących pacjentowi istotnej korzyści klinicznej.

Przepisy prawa oraz zalecenia międzynarodowe jednoznacznie wskazują, że badania radiologiczne w stomatologii powinny mieć charakter uzupełniający wobec badania klinicznego i być dobierane adekwatnie do postawionego pytania diagnostycznego. Zasady ALARA, ALADA i ALADAIP podkreślają konieczność równoważenia minimalizacji dawki z zachowaniem wartości diagnostycznej obrazu, a ich skuteczna realizacja wymaga nie tylko odpowiedniej aparatury, lecz także wiedzy, doświadczenia i krytycznego myślenia klinicznego.

Istotnym elementem systemu ochrony radiologicznej jest również właściwa eksploatacja sprzętu oraz funkcjonujący system kontroli jakości i regularne przeglądy techniczne. Zaniedbania w tym zakresie mogą prowadzić do pogorszenia jakości obrazów, wzrostu liczby badań powtórnych i w konsekwencji do nieuzasadnionego zwiększenia dawek promieniowania, mimo formalnego spełniania wymogów prawnych.

Dodatkowym problemem w praktycznej realizacji zasad ochrony radiologicznej pacjenta jest brak jednolitej interpretacji przepisów prawa. W praktyce klinicznej obserwuje się, że wymagania stawiane gabinetom stomatologicznym w zakresie ochrony radiologicznej mogą różnić się w zależności od województwa oraz interpretacji przepisów przez właściwe organy nadzorcze. Osłabia to poczucie pewności prawnej po stronie podmiotów wykonujących działalność leczniczą. Niejednolitość interpretacyjna sprzyja traktowaniu ochrony radiologicznej jako zbioru wymagań formalnych, a nie jako spójnego systemu działań ukierunkowanych na realne bezpieczeństwo pacjenta. Z punktu widzenia jakości opieki medycznej pożądane byłoby ujednolicenie praktyk nadzorczych oraz doprecyzowanie wytycznych wykonawczych, tak aby stosowanie przepisów było przewidywalne i spójne na terenie całego kraju, a nacisk kładziony był na rzeczywistą optymalizację ekspozycji, a nie wyłącznie na spełnianie wymogów administracyjnych.

Współczesna ochrona radiologiczna pacjenta w stomatologii powinna być postrzegana jako proces ciągły, integrujący wymagania prawne, zalecenia naukowe i realia codziennej praktyki klinicznej. Jej skuteczność zależy nie tyle od pojedynczych środków technicznych, ile od kultury pracy gabinetu, w której uzasadnienie ekspozycji, optymalizacja dawki i kontrola jakości stanowią spójny element odpowiedzialnego postępowania diagnostycznego.

Notki o autorkach

Karolina Jezierska jest doktorem nauk medycznych, adiunktem w Zakładzie Fizyki Medycznej Pomorskiego Uniwersytetu Medycznego w Szczecinie.
Paulina Rotter jest magistrem prawa o specjalności prawo medyczne, doktorantem w Katedrze i Zakładzie Pielęgniarstwa Pomorskiego Uniwersytetu Medycznego w Szczecinie.
Magdalena Sroczyk-Jaszczyńska jest doktorem nauk medycznych, adiunktem w Katedrze i Zakładzie Radiologii Ogólnej, Stomatologicznej i Zabiegowej Pomorskiego Uniwersytetu Medycznego w Szczecinie.

Literatura

1. Lee H., Badal, A.: *A Review of Doses for Dental Imaging in 2010–2020 and Developmentof a Web Dose Calculator.* Radiol Res Pract 2021, 6924314.
2. Schüler I.M, Hennig C.L, Buschek R., Scherbaum R., Jacobs C., Scheithauer M.: *Radiation Exposure and Frequency of Dental, Bitewing and Occlusal Radiographs in Children and Adolescents*. J Pres Med. 2023 20;13(4):692.
3. Rozporządzenie Ministra Zdrowia z dnia 11 stycznia 2023 r. w sprawie warunków bezpiecznego promieniowania jonizującego dla wszystkich rodzajów ekspozycji medycznej. (Dz.U. 2025 poz. 1288)
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230000195
4. Ustawa z dnia 16 czerwca 2023 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001675/O/D20231675.pdf
5. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20260000037/U/D20260037Lj.pdf
6. Rozporządzenie Ministra Zdrowia z dnia 8 marca 2023 r. w sprawie szczególnej ochrony niektórych kategorii osób w związku z ekspozycją medyczną w badaniach diagnostycznych, zabiegach i leczeniu (Dz.U. 2023 poz. 576)
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230000576/O/D20230576.pdf
7. Ustawa z dnia 29 listopada 2000 r. Prawo atomowe (Dz. U. z 2026 r. poz. 1)
https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20010030018/U/D20010018Lj.pdf
8. https://www.scottishdental.nhs.scot/wp-content/uploads/2015/04/CBCT-radiation_protection_2012.pdf
9. Patel S., Brown J., Semper M., Abella F., Mannocci F.: *European Society of Endodontology position statement: Use of cone beam computed tomography in Endodontics:* European Society of Endodontology (ESE) developed by. Int Endod J. 2019;52(12):1675-1678.
10. Dyrektywa Rady 2013/59/EURATOM z dnia 5 grudnia 2013 r. ustanawiająca podstawowe normy bezpieczeństwa w celu ochrony

przed zagrożeniami wynikającymi z narażenia na działanie promieniowania jonizującego oraz uchylająca dyrektywy 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom i 2003/122/Euratom Dz.U.UE.L.2014.13.1- https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2013-59-euratom-ustanawiajaca-podstawowe-normy-bezpiec https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32013L0059
11. Konstytucja RP.
12. Mendonça R..P., Estrela C., Bueno M.R, Carvalho T.C.A.S.G, Estrela L.R.A, Chilvarquer I.: *Principles of radiological protection and application of ALARA, ALADA, and ALADAIP: a critical review*. Braz Oral Res. 2025,7;39:e14.
13. Berkhout W.E.: *Het ALARA-principe. Achtergronden en toepassing in de praktijk [The ALARA-principle. Backgrounds and enforcement in dental practices].* NedjdschrTandheelkd.2015,122,5:263-70.
14. Jaju P.P, Jaju S.P.: *Cone-beam computed tomography: Time to move from ALARA to ALADA*. Imaging Sci Dent. 2015;45,4:263-5.
15. Clark-Perry D., Berkhout W.E.R, Sanderink G.C, Slot D.E.: *Evaluating cone cut in rectangular collimation in intraoral radiography: application of ALADA and radiation stewardship*. Clin Oral Investig. 2023;27(9):5391-5402.
16. Oenning A.C., Jacobs R., Salmon B.: DIMITRA Research Group (http://www.dimitra.be). *ALADAIP, beyond ALARA and towards personalized optimization for paediatric cone-beam CT.* Int J Paediatr Dent. 2021;31(5):676-678.
17. Kadesjö N., Lynds R., Nilsson M., Shi X.Q.: *Radiation dose from X-ray examinations of impacted canines: cone beam CT vs two-dimensional imaging.* Dentomaxillofac Radiol. 2018;47(3):20170305.
18. European Guidelines on Radiation Protection in Dental Radiology: The Safe Use of Radiographs in Dental Practice. (Publications Office, Luxembourg, 2004).
19. Alahmad H., Alnafea M.: *Survey of quality control of panoramic X-ray machines in private dental clinics in Saudi Arabia*. Journal of Radiation Research and Applied Sciences, 2023,16(2):1–6.
20. Helmrot E., Carlsson G.A, Eckerdal O.: *Effects of contrast equalization on energy imparted to the patient: a comparison of two dental generators and two types of intraoral film.* Dentomaxillofac Radiol. 1994;23(2);83-90.
21. Baechler S., Monnin P., Aroua A., Valley J.F., Perrier M., Trueb P., Verdun F.R.: *Exposure in dental radiology: a comparison between intra-oral, panoramic and tomographic examinations*. Radiat. Prot. Dosim, 2010,*139*(1/3);303-305.
22. Ludlow J.B, Davies-Ludlow L.E, White S.C.: *Patient risk related to common dental radiographic examinations: the impact of 2007 International Commission on Radiological Protection recommendations regarding dose calculation.* J Am Dent Assoc. 2008;139(9):1237-43.
23. Anissi H.D, Geibel M.A.: *Intraoral radiology in general dental practices – a comparison of digital and film-based X-ray systems with regard to radiation protection and dose reduction.* Rofo. 2014;186(8):762-7.
24. Ludlow J.B, Davies-Ludlow L.E, Brooks S.L.: *Dosimetry of two extraoral direct digital imaging devices: NewTom cone beam CT and Orthophos Plus DS panoramic unit.* Dentomaxillofac Radiol. 2003;32(4):229-34.
25. Rondon R.H, Pereira Y.C, do Nascimento G.C.:,*Common positioning errors in panoramic radiography: A review.* Imaging Sci Dent. 2014,44(1):1-6.
26. Benavides E., Benavides E., Krecioch J.R., Allareddy T., Buchanan A, Keels M.A. et al.: *American Dental Association and American Academy of Oral and Maxillofacial Radiology patient selection for dental radiography and cone-beam computed tomography: Clinical recommendations.* J Am Dent Assoc. 2026;157(1):20-35.e5.
27. Horner K., O'Malley L., Taylor K., Glenny A.M.: *Guidelines for clinical use of CBCT: a review.* Dentomaxillofac Radiol. 2015;44(1):20140225.
28. Shin H.S, Nam K.C., Park H., Choi H.U, Kim H.Y, Park C.S.:*Effective doses from panoramic radiography and CBCT (cone beam CT) using dose area product (DAP) in dentistry.* Dentomaxillofac Radiol. 2014;43(5):20130439.
29. Quality control in diagnostic radiology according to national regulations. https://ruj.uj.edu.pl/entities/publication/035a3322-4a3d-462b-8cf7-b713c1621ca7.
30. Hiles P., Gilligan P., Damilakis J., Briers E., Candela-Juan C. et al.: *European consensus on patient contact shielding.* Insights Imaging. 2021,23;12(1):194.
31. Benavides E., Krecioch J.R., Connolly R.T., Allareddy T., Buchanan A,. Spelic D. et al.: *Optimizing radiation safety in dentistry: Clinical recommendations and regulatory considerations*. J Am Dent Assoc. 2024;155(4):280-293.e4.
32. Papolos D.F, Teicher M.H, Post R.M.: *Treatment of Early-Onset Specified and Unspecified Bipolar Disorders: A Systematic Review and Strategies for Identifying and Managing a Thermally Dysregulated Subtype in Children.* Acta Psychiatr Scand. 2025;152(3):156-179.
33. Report of the British Institute of Radiology Guidance on using shielding on patients for diagnostic radiology applications Published March 2020 BIR Registered charity number215869 *https://www.bir.org.uk/media/414334/final_patient_shielding_guidance.pdf*
34. Hoogeveen R.C, Hazenoot B, Sanderink G.C, Berkhout W.E.: *The value of thyroid shielding in intraoral radiography.* Dentomaxillofac Radiol. 2016;45(5):20150407.
35. Johnson K.B, Ludlow J.B.: *Intraoral radiographs: A comparison of dose and risk reduction with collimation and thyroid shielding.* J Am Dent Assoc.2020 ; 151(10): 726-734.
36. Benavides E., Bhula A., Gohel A., Lurie A.G., Mallya S.M., Ramesh A., Tyndall D.A.: *Patient shielding during dentomaxillofacial radiography: Recommendations from the American Academy of Oral and Maxillofacial Radiology.* J Am Dent Assoc. 2023;154(9):826-835.e2.
37. Radiation protection of patients in dental radiology https://www.iaea.org/resources/rpop/health-professionals/dentistry/patients

Model LNT a ochrona radiologiczna w zakresie niskich dawek: stan wiedzy i propozycje zmian regulacyjnych w USA

The LNT Model and Radiation Protection at Low Doses: State of Knowledge and Regulatory Changes Proposals in the USA

Agnieszka Szumska
Instytut Fizyki Jądrowej

Streszczenie: Model liniowy bezprogowy (ang. *LNT – Linear No-Threshold*) od dziesięcioleci stanowi jedno z podstawowych założeń wykorzystywanych w systemie ochrony radiologicznej do oceny i zarządzania ryzykiem skutków stochastycznych przy małych dawkach. Nie jest on jednak tożsamy z całym systemem ochrony radiologicznej, który opiera się przede wszystkim na zasadach uzasadnienia, optymalizacji i ograniczenia dawek [1–3, 9].

Współczesna radiobiologia dostarczyła rozbudowanej wiedzy o odpowiedzi komórkowej na promieniowanie. Poznano dokładniej mechanizmy uszkodzeń i naprawy DNA, procesy eliminacji uszkodzonych komórek, odpowiedzi adaptacyjne, efekty sąsiedztwa czy niestabilność genomową. Mechanizmy te zwiększają złożoność biologicznej odpowiedzi na małe dawki, nie doprowadziły one jednak dotąd do wyznaczenia powszechnie zaakceptowanego, uniwersalnego progu bezpieczeństwa ani alternatywnego modelu ryzyka nowotworowego, który sprawdziłby się we wszystkich zastosowaniach ochrony radiologicznej. Publikacja 99 wydana przez ICRP jasno wskazuje, że przy niskich dawkach występują istotne niepewności, co sprawia, że LNT pozostaje ostrożną i zachowawczą podstawą ochrony radiologicznej [3].

Równolegle rozwija się obszerne badania epidemiologiczne analizujące przewlekłe narażenie na niskie dawki. Wyniki badań wielkich kohort, takich jak *INWORKS* czy *Million Person Study*, dostarczają kolejnych danych o zależnościach dawka–ryzyko, jednak ich interpretacja nie powinna być utożsamiana z bezpośrednim dowodem na to, że ryzyko spada liniowo aż do zera [5, 13].

Szczególnie interesującym przykładem toczącej się dziś debaty regulacyjnej są Stany Zjednoczone. Tamtejsza komisja dozoru jądrowego NRC (ang. *Nuclear Regulatory Commission*) w 2026 roku zaproponowała rewizję ram ochrony radiologicznej, w tym ponowne rozważenie sposobu wykorzystywania modelu LNT i zasady optymalizacji. Mimo że jest to na razie wyłącznie projekt, znaczenie wywołanej nim debaty mocno wykracza poza USA i z pewnością stanie się ważnym punktem odniesienia dla przyszłych dyskusji międzynarodowych [11].

Słowa kluczowe: Model LNT, ochrona radiologiczna, niskie dawki promieniowania, regulacje NRC.

Abstract: *The Linear No-Threshold (LNT) model has for decades been one of the fundamental assumptions used in the radiation protection system to assess and manage the risk of stochastic effects at low doses. However, it is not synonymous with the entire radiation protection system, which is primarily based on the principles of justification, optimization, and dose limitation [1–3, 9].*

Modern radiobiology has provided extensive knowledge about the cellular response to radiation. The mechanisms of DNA damage and repair, processes of eliminating damaged cells, adaptive responses, bystander effects, and genomic instability are now more thoroughly understood. These mechanisms increase the complexity of the biological response to low doses; however, they have not yet led to the establishment of a universally accepted safety threshold or an alternative cancer risk model that would be applicable across all radiation protection applications. ICRP Publication 99 clearly indicates that significant uncertainties exist at low doses, making LNT a cautious and conservative basis for radiation protection [3].

Concurrently, extensive epidemiological research analyzing chronic low-dose exposure is being conducted. The results of large cohorts, such as INWORKS or the Million Person Study, provide further data on dose–risk relationships; however, their interpretation should not be equated with direct evidence that the risk decreases linearly all the way down to zero [5, 13].

The United States serves as a particularly interesting example of the ongoing regulatory debate. In 2026, the US Nuclear Regulatory Commission (NRC) proposed a revision of the radiation protection framework, including a reconsideration of how the LNT model and the optimization principle are utilized. Although this is currently only a regulatory draft, the significance of this debate extends far beyond the US and will certainly become a crucial reference point for future international discussions [11].

***Keywords**: LNT model, radiation protection, low radiation doses, NRC regulations.*

1. Wprowadzenie Paradygmat ochrony radiologicznej



Współczesny system ochrony przed promieniowaniem jonizującym, kształtowany od dziesięcioleci przez rekomendacje Międzynarodowej Komisji Ochrony Radiologicznej (ang. ICRP – *International Commission on Radiological Protection*) (w szczególności publikacja nr 103) oraz Międzynarodowej Agencji Energii Atomowej (MAEA, ang. IAEA – *International Atomic Energy Agency*), opiera się na trzech podstawowych zasadach: uzasadnieniu, optymalizacji i limitowaniu dawek. Należy przy tym zaznaczyć, że ostatnie z tych kryteriów nie ma zastosowania u pacjentów w celach medycznych, gdzie priorytetem jest skuteczność diagnozowania i terapii indywidualnego pacjenta. W prawie europejskim zasady te zostały ujęte w art. 5 dyrektywy 2013/59/Euratom [1, 2].

Ochrona radiologiczna nieustannie poszukuje równowagi pomiędzy korzyściami wynikającymi z wykorzystania promieniowania jonizującego a potencjalnym ryzykiem dla zdrowia i środowiska naturalnego. Ustalenia naukowe przekładają się z czasem na normy prawne w zakresie ochrony radiologicznej, które stanowią część szerszego systemu prawa energii jądrowej.

LNT jest jednym z modeli wykorzystywanych w ocenie ryzyka skutków stochastycznych. Zgodnie z pojęciem całkowitego uszczerbku na zdrowiu, zdefiniowanym w publikacji ICRP 103 [4], kategoria ta obejmuje nie tylko ryzyko nowotworowe (wynikające z mutacji w komórkach somatycznych), ale także stochastyczne efekty dziedziczne (będące następstwem mutacji w linii zarodkowej). Model LNT odnosi się do obu tych zjawisk, jednak trzeba tu podkreślić fundamentalną różnicę w bazie dowodowej. O ile ekstrapolacja ryzyka nowotworowego bazuje na obszernych danych epidemiologicznych u ludzi (np. badanie LSS – *Life Span Study* [3, 6]), o tyle szacunki dotyczące efektów dziedzicznych opierają się na ekstrapolacji wyników z eksperymentów in vivo na zwierzętach. U ludzi – nawet podczas wieloletnich obserwacji kohorty ocalałych z bombardowań w Japonii – nie wykazano dotychczas statystycznie istotnego wzrostu popromiennych efektów dziedzicznych. Warto również przypomnieć, że model ten nie dotyczy odczynów tkankowych (określanych jako skutki deterministyczne, np. zaćmy czy rumienia popromiennego). W ich przypadku współczesna radiobiologia i ochrona radiologiczna posługuje się wartościami progowymi lub zakresami dawek progowych, których wielkość zależy m.in. od rodzaju efektu tkankowego, narażonego narządu, a także czasu czy specyfiki ekspozycji. Model LNT przyjmuje, że na potrzeby ochrony radiologicznej w zakresie małych dawek ryzyko można przybliżać za pomocą zależności liniowej. Nie oznacza to jednak, że każda pojedyncza ekspozycja powoduje mierzalny wzrost zachorowań, który dałoby się bezpośrednio wykryć narzędziami epidemiologicznymi.

LNT należy również odróżnić od zasady optymalizacji. Optymalizacja nie oznacza sprowadzania każdej dawki do minimum bez względu na koszty. Jej celem jest osiągnięcie racjonalnego poziomu ochrony z uwzględnieniem czynników technicznych, ekonomicznych, zdrowotnych i społecznych [1, 2].

1.1. Podstawy biologiczne i kontrowersje wokół niskich dawek

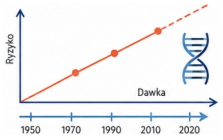
W zakresie dawek powyżej 100 mGy dysponujemy silnymi i spójnymi dowodami epidemiologicznymi (np. z kohorty LSS) potwierdzającymi wzrost ryzyka nowotworowego. Sytuacja komplikuje się jednak wraz ze spadkiem dawki pochłoniętej poniżej wartości 100 mGy. Statystyczne wychwycenie minimalnego przyrostu ryzyka na tle powszechnej, naturalnej zapadalności na nowotwory w społeczeństwie staje się wówczas niemożliwe ze względu na bariery związane z mocą statystyczną badań. Aby skutecznie dowieść nadmiarowego ryzyka przy dawkach rzędu kilku miligrejów (mGy), musielibyśmy badać kohorty o nierealistycznie gigantycznych rozmiarach. Brak bezpośrednich, bezspornych dowodów w rejonie najniższych dawek jest zatem w równej mierze wynikiem statystycznego szumu, co ogromnej złożoności odpowiedzi organizmu. Niemniej jednak, współczesne analizy epidemiologiczne dostarczają nam danych także dla przewlekłego narażenia na relatywnie małe dawki.

Rozwój wiedzy na temat odpowiedzi adaptacyjnej, efektów sąsiedztwa (ang. *bystander effects*), niestabilności genomowej czy zjawiska określanego jako hormeza radiacyjna wyraźnie ukazuje, jak wielowymiarowa jest biolo-

giczna reakcja na małe dawki. Nauka zidentyfikowała szereg procesów modyfikujących odpowiedź tkanek, w tym mechanizmy naprawy DNA, zatrzymania cyklu komórkowego, apoptozy oraz reakcje ze strony układu immunologicznego. Zidentyfikowanie tych zjawisk nie jest jednak równoznaczne z wykazaniem istnienia uniwersalnego progu ryzyka nowotworowego dla człowieka. Brak takich dowodów nie przesądza wprawdzie o liniowości zależności dawka–ryzyko, ale to właśnie zbiorcza ocena dostępnych danych epidemiologicznych, ustaleń radiobiologii i modeli ryzyka stanowi uzasadnienie dalszego stosowania LNT. Zarówno Komitet ONZ ds Skutków Promieniowania Atomowego (ang. UNSCEAR – *United Nations Scientific Committee on the Effects of Atomic Radiation*), jak i ICRP konsekwentnie przypominają, że w obszarze niskich dawek panuje niepewność obejmująca nie tylko samą skalę ryzyka, ale też precyzyjny kształt krzywej dawka-odpowiedź [3, 9].

Wiele emocji w badaniach eksperymentalnych budzi zjawisko hormezy radiacyjnej. Choć w wybranych układach biologicznych rzeczywiście zaobserwowano reakcje adaptacyjne lub stymulujące, nie mamy dziś wystarczających naukowych podstaw, by przyjąć hormezę jako uniwersalny standard ochrony radiologicznej bądź by uznać małe dawki za zjawisko profilaktycznie korzystne dla populacji.

2. Geneza, ewolucja i założenia modelu LNT



Historia LNT nie opiera się na jednym, przełomowym eksperymencie ani na jednej decyzji administracyjnej. Choć wczesne badania Hermanna Mullera nad indukowaniem mutacji u muchówek (*Drosophila*) miały spory wpływ na rozwój koncepcji zależności dawka–efekt, to ostateczny kształt całego systemu ochrony radiologicznej był wynikiem wielu dekad prac eksperymentalnych, epidemiologicznych i regulacyjnych.

2.1. Źródło danych

Jednym z najważniejszych źródeł danych epidemiologicznych pozostaje *Life Span Study* (LSS) ocalałych z wybuchów bomb atomowych w Hiroszimie i Nagasaki. Kohorta ta dostarczyła kluczowych danych o zależności pomiędzy narażeniem na promieniowanie a ryzykiem nowotworowym. Mimo to LSS nie jest gotowym dowodem potwierdzającym trafność LNT „aż do samego zera". Przenoszenie tych wyników na obszar małych dawek staje się w dużej mierze kwestią modelowania statystycznego. Dane z LSS są w pełni miarodajne tam, gdzie liczba przypadków pozwala na pewne oszacowanie parametrów. Im niższa dawka, tym większa niepewność, a jednoznaczne rozstrzygnięcie, który z konkurencyjnych modeli ryzyka jest najtrafniejszy, staje się coraz trudniejsze [3, 6].

2.2. Odpowiedź komórkowa a dane epidemiologiczne

Radiobiologia i epidemiologia odpowiadają na różne pytania. Badania komórkowe pozwalają identyfikować mechanizmy, które mogą wpływać na odpowiedź organizmu. Badania epidemiologiczne pozwalają natomiast oceniać, czy w populacji występuje mierzalny nadmiar zachorowań lub zgonów związany z określonym narażeniem.

Najnowsze analizy kohortowe poszerzają naszą bazę danych o skutki przewlekłego narażenia. W aktualizacji badania INWORKS z 2024 roku dowiedziono istnienia statystycznych zależności między kumulowaną dawką zawodową a ryzykiem zgonu na określone nowotwory (w tym układu krwiotwórczego). Trzeba tu jednak bardzo rygorystycznie oddzielić populacyjną analizę całego trendu od ryzyka indywidualnego. Modele statystyczne rysują obraz dystrybucji ryzyka w dużej grupie, zatem nie można ich traktować jako dowodu na to, że u konkretnego człowieka, który przyjął dawkę rzędu kilkunastu miligrejów (mGy), wystąpi klinicznie mierzalny wzrost ryzyka kancerogenezy [5].

Podobnych wniosków dostarczyło opublikowane w 2025 roku badanie *Million Person Study*, analizujące śmiertelność na nowotwory lite wśród pracowników narażonych na promieniowanie. W tym przypadku sami autorzy zastrzegają obecność istotnych ograniczeń interpretacyjnych, wynikających m.in. z braku pełnych danych o zewnętrznych, niezwiązanych z promieniowaniem czynnikach środowiskowych czy innych źródłach narażenia [13].

3. Wyzwania praktyczne i koszty społeczno-gospodarcze



3.1. Lekcja z Fukushimy

Katastrofa w Fukushima Daiichi pokazuje, że konsekwencje sytuacji radiacyjnej nie ograniczają się wyłącznie do bezpośrednich efektów zdrowotnych wynikających z samego narażenia radiologicznego (otrzymanych dawek). Z raportów UNSCEAR wynika, że w lokalnej populacji nie stwierdzono skutków zdrowotnych, które dałoby się bezpośrednio i jednoznacznie powiązać z napromieniowaniem. Równocześnie jednak działania prewencyjne – takie jak masowa ewakuacja, zerwanie więzi społecznych, długotrwałe przesiedlenia, ogromny stres oraz zakłócenia w funkcjonowaniu opieki zdrowotnej – pociągnęły za sobą bardzo realne, tragiczne konsekwencje zdrowotne [9].

Z tego względu doświadczenie Fukushimy powinno być traktowane przede wszystkim jako argument za proporcjonalnym zarządzaniem ryzykiem i wysoką jakością komunikacji ze społeczeństwem, a nie jako prosty dowód potwierdzający słuszność lub błędy modelu LNT.

3.2. Bariera dla reaktorów energetycznych i medycyny

Wymagania dotyczące ochrony radiologicznej są jednym z elementów wpływających na koszty projektowania i eksploatacji instalacji jądrowych oraz obiektów wykorzystujących promieniowanie jonizujące. Rzeczywisty poziom tych kosztów zależy od wybranej technologii, wymagań lokalnego regulatora i samego procesu optymalizacji. Problem ten doskonale widać przy projektowaniu stałych osłon w nowoczesnych zakładach radioterapii, a w szczególności podczas planowania lokalizacji reaktorów energetycznych w pobliżu dużych aglomeracji miejskich. Dla branży jądrowej fundamentalnym wyzwaniem komercyjnym i społecznym jest możliwość zawężenia strefy planowania awaryjnego (ang. EPZ – *Emergency Planning Zone*) wyłącznie do obrysu fizycznego samego obiektu. W tym kontekście główną przeszkodą nie jest sam model LNT, lecz konieczność zastąpienia skrajnie konserwatywnych założeń (dotyczących np. modeli dyspersji atmosferycznej czy scenariuszy uwalniania radionuklidów) nowym podejściem typu *risk-informed*, które opierałoby się na realistycznych symulacjach zachowania reaktora. Obecne wysokie koszty systemów zabezpieczeń i osłon wynikają z rygorystycznych przepisów, które w obowiązującym stanie prawnym rzadko potrafią sprawiedliwie zróżnicować skalę zagrożenia adekwatnie do innowacyjności i bezpieczeństwa różnych projektów reaktorów włącznie z małymi reaktorami modułowymi (SMR) [7, 8].



4. Debata regulacyjna w USA

Obecnie to w Stanach Zjednoczonych toczą się najważniejsze dyskusje o nowych przepisach i modelach radiologicznych. Wynika to z faktu, że USA mają ogromne zaplecze naukowe i bardzo wpływowe organizacje (takie jak *Health Physics Society* – HPS czy *American Nuclear Society* – ANS). To właśnie tam zwolennicy zmian spierają się z obrońcami dotychczasowych zasad. Przez lata debata ta tkwiła w martwym punkcie, jednak ostatnio doprowadziła do propozycji poważnych reform w prawie.

4.1. Okres stabilizacji i utrzymania status quo (2015–2021)

Spór o model LNT w USA tlił się od lat. Debata w USA nabrała tempa w 2015 r., gdy złożono petycje postulujące całkowite odrzucenie modelu LNT na rzecz rozwiązań uwzględniających zjawisko hormezy. Podnoszono w nich, że LNT ignoruje naturalne procesy ewolucyjne, wywołuje niepotrzebną radiofobię i generuje straty idące w miliardy dolarów.

Analiza tych petycji zajęła regulatorowi długie lata. Ostatecznie, 17 sierpnia 2021 r., U.S. Nuclear Regulatory Commission (NRC) oficjalnie odrzuciła petycje o zmianę przepisów. Komisja uzasadniła to faktem, że choć nauka dostarcza nowych danych z zakresu biologii komórkowej, brakuje twardych podstaw, by zastąpić LNT innym modelem w ramach ogólnego systemu ochrony. Utrzymano wówczas model liniowy jako rozwiązanie najbardziej zachowawcze, zapewniające odpowiedni poziom bezpieczeństwa (ang. *adequate protection*) [10].

4.2. Punkt zwrotny: Dekrety prezydenckie i reformy (2025)

Całkowity zwrot akcji przyniósł rok 2025. Pod presją kryzysu energetycznego, pilnej potrzeby dekarbonizacji gospodarki i fatalnych zatorów administracyjnych uderzających w innowacyjne projekty (zwłaszcza SMR) amerykańska administracja wydała dwa przełomowe dekrety:

- **Executive Order 14300** (ang. *Ordering the Reform of the NRC*), wymuszający na komisji gruntowną rewizję przestarzałych przepisów regulacyjnych,
- **Executive Order 14303** (ang. *Restoring Gold Standard Science*), obligujący do tego, by polityka państwa opierała się wyłącznie na weryfikowalnych dowodach o bezwzględnie najwyższym standardzie empirycznym.

Dokumenty te nadały kierunek reformie regulacyjnej, obejmującej m.in. większe wykorzystanie podejścia *risk-informed* oraz ocenę proporcjonalności wymagań regulacyjnych.

Debata w USA w 2025–2026 roku przesunęła się z pytania „czy LNT jest prawdziwy?" w stronę szerszego pytania: w jaki sposób oceniać ryzyko w codziennych decyzjach administracyjnych i jak proporcjonalnie dopasowywać rygory do rzeczywistego zagrożenia.

Dekrety z 2025 roku i wynikające z nich działania NRC to element szerszej reformy państwowej. Zwrócenie się w stronę podejścia *risk-informed* nie oznacza jednak wykreślenia dotychczasowych modeli radiobiologicznych z ram prawnych ani oficjalnego, urzędowego zatwierdzenia istnienia progu biologicznego.

4.3. Proponowane zmiany regulacyjne i perspektywa 2026 roku

Kulminacją tych procesów było opublikowanie przez NRC 15 lipca 2026 roku projektu *„Reforming and Modernizing the NRC's Radiation Protection Framework"* (Docket ID NRC-2025-1140). Dokument ten ma charakter projektu przepisów (*proposed rule*), podlegającego szerokim konsultacjom społecznym (z terminem zgłaszania uwag przypadającym na 31 sierpnia 2026 r.), a nie gotowego i obowiązującego prawa. W jego treści wprost podnosi się kwestię ponownego przeanalizowania roli LNT i mechanizmów optymalizacji w praktyce administracyjnej [11].

Dla ekspertów z Europy najważniejszy wniosek brzmi: projekt z 2026 roku nie jest naukowym obaleniem dogmatów LNT. To raczej próba przedefiniowania sposobu, w jaki niepewność dotycząca ryzyka ma być przekładana na

twarde wymagania techniczne. Należy zatem ostrożnie operować tezami, że „USA odchodzą od LNT", zaznaczając zawsze, iż dotyczy to przede wszystkim reformowania mechanizmów regulacyjnych i prawnych.

Na dzień przygotowania niniejszej wersji termin zgłaszania uwag do projektu przypada na 31 sierpnia 2026 roku. Ostateczny kształt regulacji może więc jeszcze ulec zmianie [11].



5. Rozwój podejścia ICRP

Debata nad małymi dawkami nie ogranicza się tylko do USA. Międzynarodowa dyskusja toczy się również na forum ICRP. ICRP prowadzi i publikuje prace dotyczące naukowych podstaw oceny ryzyka przy niskich dawkach i niskich mocach dawki. Szczególne znaczenie ma ICRP Publication 99 [3], w której po skrupulatnej analizie zebranych dowodów epidemiologicznych i biologicznych potwierdzono ogromne niepewności w strefie najniższych dawek. Mimo to komisja nie znalazła argumentów za przyjęciem uniwersalnego progu i nadal traktuje model LNT jako racjonalne, ostrożnościowe założenie [3].

Baza naukowa wciąż ewoluuje, o czym świadczą obecne prace ICRP poświęcone m.in. nowotworom litym przy bardzo małym narażeniu oraz tematowi indywidualnej wrażliwości człowieka. Prowadzenie tego typu badań nie oznacza jednak w żadnym wypadku utraty podstaw obecnego systemu bezpieczeństwa jądrowego i ochrony radiologicznej.

6. Co jest dobrze ustalone, a co pozostaje niepewne?



Z perspektywy współczesnej wiedzy:

6.1. Dobrze ustalone:

- wysokie dawki promieniowania jonizującego indukują odczyny tkankowe (po przekroczeniu odpowiednich progów dawki) oraz proporcjonalnie zwiększają prawdopodobieństwo wystąpienia stochastycznych efektów późnych (nowotworów);
- ryzyko zależy m.in. od dawki, rodzaju promieniowania, wieku w chwili ekspozycji, płci, narządu i czasu oraz sposobu narażenia;
- przy niskich dawkach i małych mocach dawki niepewność statystyczna i biologiczna jest większa niż przy wysokich dawkach;
- istnieją epidemiologiczne dane dotyczące przewlekłego narażenia zawodowego na relatywnie niskie dawki, m.in. z badań *INWORKS* i *Million Person Study* [5, 13].

6.2. Niepewne:

- dokładny kształt zależności dawka–ryzyko dla wszystkich nowotworów w najniższym zakresie dawek;
- dokładna wielkość efektu mocy dawki i jego zależność od rodzaju nowotworu oraz sposobu ekspozycji;
- znaczenie indywidualnej podatności genetycznej i innych cech osobniczych dla ryzyka przy małych dawkach;
- istnienie jednego uniwersalnego progu lub uniwersalnego korzystnego efektu małych dawek dla ryzyka nowotworowego w populacji;

Nie istnieje zatem obecnie żaden powszechnie zaakceptowany alternatywny jeden model, który zastąpiłby LNT we wszystkich zastosowaniach ochrony radiologicznej.



7. Znaczenie dla ochrony radiologicznej w Polsce

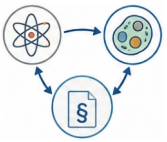
Debata w USA i rozwój prac ICRP stanowią ważny materiał analityczny dla Polski, ale nie oznaczają konieczności automatycznego kopiowania rozwiązań zza oceanu. Krajowy system ochrony radiologicznej funkcjonuje w ramach prawa krajowego oraz prawa europejskiego.

Prezes PAA prowadząc nadzór nad bezpieczeństwem jądrowym i ochroną radiologiczną opiera się na przepisach Prawa atomowego [12], uwzględniającego zarówno dorobek ICRP jak i IAEA, zgodnego także z prawem europejskim, którego ramy dotyczące omawianej kwestii określa dyrektywa 2013/59/Euratom, trzymająca się sprawdzonych filarów: uzasadnienia, optymalizacji i ograniczania dawek [1, 2].



8. Środowisko dozymetryczne w Europie

Europejskie środowisko ochrony radiologicznej i dozymetrii z uwagą śledzi globalne dyskusje na ten temat. Grupa EURADOS (*European Radiation Dosimetry Group*), sieć zrzeszająca obecnie 85 instytucji, głównie europejskich (członków z prawem głosu), oraz ponad 650 naukowców (członków stowarzyszonych), zorganizowała otwarte debaty nad przyszłością LNT i dozymetrii (m.in. w lutym br. podczas corocznego spotkania, które odbyło się w Helsinkach; kolejne spotkanie odbędzie się w lutym 2027 roku i będzie organizowane wspólnie z MAEA), a kolejna szeroka dyskusja pod prowokacyjnym tytułem: *"Are we too conservative in radiation protection?"* zaplanowana jest podczas konferencji *European Radiation Protection Week 2026* (ERPW 2026), która odbędzie się w dniach 5–9 października w Berlinie.



9. Podsumowanie

Model LNT stanowi użyteczny, ale nie jedyny element ochrony radiologicznej. Nie jest on bezpośrednim opisem wszystkich procesów biologicznych zachodzących po ekspozycji na promieniowanie ani nie stanowi samodzielnej zasady prawnej. Jest on w istocie modelem pozwalającym na ostrożne szacowanie ryzyka stochastycznego w przedziałach dawek, dla których nie dysponujemy twardymi dowodami epidemiologicznymi.

O ile mechanizmy działania przy wysokich dawkach rozumiemy dziś bardzo dobrze, o tyle w rejonie dawek najniższych musimy borykać się z poważnymi niepewnościami naukowymi. Radiobiologia nie daje nam dziś pewności, że małe dawki są obojętne lub zawsze korzystne, a jednocześnie sam fakt istnienia drobnych uszkodzeń na poziomie komórkowym nie przesądza jeszcze o liniowym przebiegu krzywej ryzyka w skali całej populacji.

Rozpatrując te kwestie, eksperci powinni ściśle odróżniać trzy wymiary: czysto fizyczną zdolność promieniowania do uszkadzania komórek, epidemiologiczną ocenę zachorowań oraz administracyjno-prawny wymiar wykorzystywania modelu LNT w tworzeniu prawa oraz jego stosowaniu przez organy dozoru jądrowego. Wnioski z rozważań prowadzonych w ramach każdego z tych wymiarów rzadko się wzajemnie pokrywają. Mimo swych niedoskonałości LNT pozostaje ostrożnym standardem, a główną areną naukowej niepewności jest dokładny kształt biologicznej krzywej ryzyka w strefie najniższych narażeń.

Debata regulacyjna w USA jest szczególnie interesująca dlatego, że dotyczy nie tylko samego modelu LNT, lecz także sposobu przekładania niepewności naukowej na wymagania prawne. Projekt NRC z 2026 roku powinien być analizowany jako propozycja reformy regulacyjnej, a nie jako naukowe obalenie LNT.

Dla przyszłości ochrony radiologicznej kluczowa będzie dalsza integracja epidemiologii, radiobiologii, dozymetrii i analizy niepewności. Równie ważne będzie zachowanie proporcjonalności wymagań oraz przejrzyste komunikowanie tego, co jest dobrze ustalone, a co pozostaje przedmiotem badań.

Notka o autorce

Dr inż. Agnieszka Szumska jest od ponad 15 lat związana z Instytutem Fizyki Jądrowej im. Henryka Niewodniczańskiego Polskiej Akademii Nauk (IFJ PAN) w Krakowie, gdzie obecnie pełni m.in. funkcję Inspektora Ochrony Radiologicznej. Jest aktywną uczestniczką, prelegentką oraz współorganizatorką międzynarodowych i ogólnopolskich konferencji, a także autorką i współautorką publikacji poświęconych praktycznym aspektom pomiarów promieniowania jonizującego. Zasiada w Radzie EURADOS, gdzie od ponad dekady uczastniczy w badaniach prowadzonych w grupach roboczych WG1 i WG2 tej organizacji. Pełni funkcję reprezentantki w *European Metrology Network for Radiation Protection* w ramach EURAMET (ang. *European Association of National Metrology Institutes*) oraz jest członkinią Stowarzyszenia Inspektorów Ochrony Radiologicznej (SIOR).



Literatura

1. Council Directive 2013/59/Euratom of 5 December 2013 laying down *basic safety standards for protection against the dangers arising from exposure to ionising radiation*. Official Journal of the European Union. 2014.
2. IAEA. Radiation Protection and Safety of Radiation Sources: *International Basic Safety Standards.* General Safety Requirements Part 3 (GSR Part 3). IAEA, Vienna.
3. ICRP. *Low-dose Extrapolation of Radiation-related Cancer Risk*. ICRP Publication 99. Ann ICRP. 2005;35(4).
4. ICRP. *The 2007 Recommendations of the International Commission on Radiological Protection*. ICRP Publication 103. Ann ICRP. 2007;37(2–4):1–332.
5. Leuraud K. et al. *Leukaemia, lymphoma, and multiple myeloma mortality after low-level exposure to ionising radiation in nuclear workers (INWORKS): updated findings from an international cohort study*. Lancet Haematology. 2024;11(10):e761–e769.
6. National Research Council. *Health Risks from Exposure to Low Levels of Ionizing Radiation*: BEIR VII Phase 2. Washington, DC: National Academies Press; 2006.
7. OECD/NEA. *Unlocking Reductions in the Construction Costs of Nuclear: A Practical Guide for Stakeholders*. NEA No. 7616. OECD Publishing, Paris; 2020.
8. OECD/NEA. *Small Modular Reactors: Challenges and Opportunities.* NEA No. 7560. OECD Publishing, Paris; 2021.40; RIN 3150-AL47.
9. UNSCEAR. Sources, Effects and Risks of Ionizing Radiation. UNSCEAR 2020/2021 Report. Scientific Annex C: *Biological mechanisms relevant for the inference of cancer risks from low-dose and low-dose-rate radiation*. United Nations, New York; 2021, with corrigendum 2022.
10. U.S. Nuclear Regulatory Commission. *Linear No-Threshold Model and Standards for Protection Against Radiation; Denial of Petitions for Rulemaking*. Federal Register. 2021;86:45923. 17 August 2021.
11. U.S. Nuclear Regulatory Commission. *Reforming and Modernizing the NRC's Radiation Protection Framework. Proposed Rule.* Docket ID NRC-2025-1140; RIN 3150-AL47. 15 July 2026.
12. Ustawa z dnia 29 listopada 2000 r. – Prawo atomowe. Dz.U. z 2026 r. poz. 1.
13. Walsh L., Cohen S.S., Dauer L.T., Mumma M.T., Boice J.D. Jr. *Cancer Mortality after Protracted Low-level Radiation Exposure for Early and Contemporary Workers in Two Large Occupational Cohorts in the U.S. Million Person Study.* Radiation Research. 2025;204(5):529–536. doi:10.1667/RADE-24-00271.1.

Computer security of nuclear power plant instrumentation and control systems. IAEA guidance versus the Polish legal framework on the eve of the first unit's construction

Cyberbezpieczeństwo systemów kontrolno-pomiarowych elektrowni jądrowej. Wytyczne MAEA a polskie ramy prawne u progu budowy pierwszego bloku

Artur Chlebicki
Independent Researcher, Gdańsk, Poland (MSc Eng. in Computer Science, Gdańsk University of Technology) · ORCID 0009-0009-7304-0138

Abstract: The instrumentation and control (I&C) systems of a modern nuclear power plant are fully digital, and their compromise may impair nuclear safety functions. The International Atomic Energy Agency has built a dedicated layer of guidance around this problem (the NSS 42-G implementing guide [21] and the NSS 17-T (Rev. 1) [20] and NSS 33-T [17] technical guidance), resting on four interlocking concepts: sensitive digital assets, computer security levels, computer security zones, and the defensive computer security architecture. A parallel family of IEC standards for the nuclear industry has emerged: IEC 62645 [18], IEC 62859 [16] and IEC 63096 [19]. This paper sets that architecture of requirements against the Polish legal order at the moment when the investor has filed its application for a construction licence and the President of the National Atomic Energy Agency has 24 months to decide. Analysis of the legal texts leads to the conclusion that computer security of nuclear I&C is governed in Poland by four regimes that arose independently of one another and have never been reconciled: the design-and-safety regime, in which the design requirements regulation [5] speaks almost exclusively of reliability and devotes a single phrase in § 90(6) to deliberate interference; the classified information regime, to which Article 36c(4) of the Atomic Law [1] refers systems supervising the technological process, together with accreditation carried out by the Internal Security Agency at the "secret" classification level; the physical protection regime, whose statutory design basis threat lists cyber-attack while the 2008 implementing regulation is silent on digital systems; and the national cybersecurity regime, which after the amendment of 23 January 2026 [9] covers the investor holding the principal decision as an important entity and names the operator of a nuclear power facility as an essential entity from the operating licence. Each regime has a different authority, a different logic and a different trigger point in the facility life cycle, and none introduces the concepts on which the IAEA methodology rests. The national cybersecurity regime reaches the project already, but with general management duties only. One practical consequence is singled out: the IAEA cautions that safety analysis is not sufficient to define computer security requirements because it does not address mal-operations caused by malicious acts, yet the Polish design regulation grounds those requirements precisely in reliability analysis. The paper proposes a coverage map of NSS 33-T elements against national provisions and identifies the gaps that can be closed without amending primary legislation. The work is a review and conceptual study based solely on analysis of published documents, standards and legal acts. It contains no original research, measurements or testing. The coverage assessment presented in Figure 5 does not derive from measurement; it is the author's expert judgement, calibrated against the content of the documents analysed.

Keywords: computer security, instrumentation and control systems, I&C, nuclear power plant, IAEA, NSS 33-T, IEC 62645, Atomic Law, national cybersecurity system, NIS 2, design basis threat.

Streszczenie: *Systemy kontrolno-pomiarowe i sterowania (I&C) współczesnej elektrowni jądrowej są w całości cyfrowe, a ich kompromitacja może naruszyć funkcje bezpieczeństwa jądrowego. Międzynarodowa Agencja Energii Atomowej zbudowała wokół tego problemu odrębną warstwę dokumentów (przewodnik wdrożeniowy NSS 42-G [21] oraz wytyczne techniczne NSS 17-T (Rev. 1) [20] i NSS 33-T [17]), opartą na czterech powiązanych pojęciach: wrażliwych aktywów cyfrowych, poziomów bezpieczeństwa komputerowego, stref bezpieczeństwa komputerowego oraz obronnej architektury bezpieczeństwa komputerowego. Równolegle powstała rodzina norm IEC dla przemysłu jądrowego: IEC 62645 [18], IEC 62859 [16] i IEC 63096 [19]. Artykuł zestawia tę architekturę wymagań z polskim porządkiem prawnym w momencie, w którym inwestor złożył wniosek o zezwolenie na budowę, a Prezes Państwowej Agencji Atomistyki ma na decyzję 24 miesiące. Analiza tekstów aktów prawnych prowadzi do wniosku, że cyberbezpieczeństwo I&C obiektu jądrowego jest w Polsce regulowane przez cztery reżimy, które powstały niezależnie od siebie i nie zostały ze sobą uzgodnione: reżim projektowo-bezpieczeństwowy, w którym rozporządzenie o wymaganiach projektowych [5] mówi niemal wyłącznie o niezawodności, a działaniu celowemu poświęca jedno wyrażenie w § 90 pkt 6; reżim ochrony informacji niejawnych, do którego art. 36c ust. 4 Prawa atomowego [1] odsyła systemy nadzorujące proces technologiczny, wraz z akredytacją prowadzoną przez Agencję Bezpieczeństwa Wewnętrznego na poziomie klauzuli „tajne"; reżim ochrony fizycznej, którego ustawowe projektowe zagrożenie wymienia cyberatak, podczas gdy rozporządzenie wykonawcze z 2008 r. milczy o systemach cyfrowych; oraz reżim krajowego systemu cyberbezpieczeństwa, który po nowelizacji z 23 stycznia 2026 r. [9] obejmuje inwestora posiadającego decyzję zasadniczą jako podmiot ważny, a operatora obiektu energetyki jądrowej wymienia jako podmiot kluczowy od chwili uzyskania zezwolenia na eksploatację. Każdy z tych reżimów ma inny organ, inną logikę i inny moment uruchomienia w cyklu życia obiektu, a żaden nie wprowadza pojęć, na których opiera się metodyka MAEA. Reżim krajowego systemu cyberbezpieczeństwa obejmuje przedsięwzięcie już dziś, ale wyłącznie ogólnymi obowiązkami zarządczymi. Osobno wskazano konsekwencję praktyczną: MAEA zastrzega, że analiza bezpieczeństwa nie wystarcza do zdefiniowania wymagań bezpieczeństwa komputerowego, ponieważ nie obejmuje wadliwych działań spowodowanych aktami złośliwymi, a polskie rozporządzenie projektowe opiera te wymagania właśnie na analizie niezawodnościowej. Artykuł proponuje mapę pokrycia elementów NSS 33-T przez przepisy krajowe i wskazuje miejsca, w których lukę można zamknąć bez zmiany ustawy. Praca ma charakter przeglądowo-koncepcyjny: opiera się wyłącznie na analizie opublikowanych dokumentów, norm i aktów prawnych. Nie zawiera badań własnych, pomiarów ani testów. Zestawienie pokrycia przedstawione na rysunku 5 nie pochodzi z pomiaru, lecz jest oceną ekspercką autora, skalibrowaną względem treści analizowanych dokumentów.*

Słowa kluczowe: *cyberbezpieczeństwo, systemy kontrolno-pomiarowe, I&C, elektrownia jądrowa, MAEA, NSS 33-T, IEC 62645, Prawo atomowe, krajowy system cyberbezpieczeństwa, NIS 2, podstawowe zagrożenie projektowe.*

1. Introduction

The Polish nuclear programme has entered a phase in which questions about computer security stop being theoretical. On 31 March 2026 the investor, Polskie Elektrownie Jądrowe (PEJ), filed an application with the President of the National Atomic Energy Agency (Państwowa Agencja Atomistyki, PAA) for a licence to construct a nuclear facility [24]. Under Article 39a(1)(1) of the Atomic Law, the President of the Agency issues a decision in such a case within 24 months of the day the application is filed together with the required documents [1]. The proceedings are under way as this text is being written.

The investment concerns the Lubiatowo-Kopalino site in the municipality of Choczewo, where three AP1000 reactors supplied by Westinghouse are to stand, with a total capacity of up to 3750 MWe. The schedule in the 2025 draft update of the Polish Nuclear Power Programme, directed to public consultation, foresees construction licences and the start of construction work, that is the first nuclear concrete, in 2028, with commercial operation of the successive units beginning in 2036, 2037 and 2038 [23]. The road to this point was long and has been described in the literature [37, 49], but only now is the programme passing from planning into design.

A preliminary safety report accompanies the construction licence application. Under Article 36d(1) and (2) of the Atomic Law, the investor first carries out safety analyses, submits them to verification in which entities involved in developing the facility design may not take part, and draws up the report on the basis of their results [1]. This is the document in which the requirements placed on I&C systems take binding form, and this is the moment when they can still be shaped.

Why these dates matter for the subject of this article follows from a simple property of instrumentation and control systems: their security architecture is settled at the design stage, not during operation. The division into zones, the directions of data flow, the choice of platforms, the way boundaries between systems of different safety significance are realised: all of this is, in practice, irreversible once the design is closed. If computer security requirements are not set now, then in ten years they can at best be approximated with compensatory measures, in a facility where every modification of a safety-relevant system is a heavy, costly procedure requiring regulatory consent.

The starting point is the IAEA's observation that new nuclear facilities use highly integrated digital I&C systems to handle very large volumes of process data simultaneously, with less human involvement than in previous-generation designs [17]. The same feature that yields the efficiency gain creates an attack surface that facilities designed in the 1970s simply did not have.

The aim of this article is to set the architecture of requirements that the IAEA and the IEC have built around I&C computer security against what Polish law says on the matter, and to point to the places where the two layers fail to meet. The thesis I put forward is this: Polish regulation addresses the computer security of a nuclear facility in four places, but each of those places speaks a different language and answers to a different authority. Together they do not add up to a coherent computer security programme in the sense that NSS 42-G gives that term [21].

2. Scope, method and limitations

This article is a review and conceptual study. Its material consists of published documents: IAEA guidance from the Nuclear Security Series, standards of the International Electrotechnical Commission, Polish legal acts together with their consolidated texts, and peer-reviewed literature. I checked every act of Polish law in the official ELI repository maintained by the Chancellery of the Sejm, which records the title, the promulgation address, the status in force and the full text. The quoted passages of statutes and regulations were read in the original, not through secondary accounts.

What this text does not contain needs saying at the outset. There are no original studies, measurements, penetration tests or analyses of specific installations. Nor is there any information about vulnerabilities of the Polish project, partly because none is public, and partly because publishing such things would be irresponsible regardless of their availability. Every number in the text comes from a cited document and is marked as such.

One point requires a separate reservation. Figure 5, discussed in section 8, presents the elements of the NSS 33-T guidance set against their coverage by national provisions. It is not the result of measurement or of a computational method. It is the author's expert judgement, calibrated against the content of the documents analysed, and as such it is open to debate. I offer it because without such a juxtaposition the scale of the difference is hard to show, but the reader should treat it as an argument, not as a measurement.

The author is a cybersecurity practitioner, not a nuclear engineer. The perspective of this text is that of protecting industrial process control systems, carried over onto the ground of nuclear regulation with all the caution such a transfer demands.

3. Why nuclear facility I&C is a special case

Transplanting office IT practice into control systems ends badly, and the industry literature has described this many times [30, 50]. In a nuclear facility the differences are sharper still.

The first difference is that the order of protection goals reverses. In information systems, confidentiality usually comes first. In I&C, what matters above all is the integrity of the signal and the availability of the function: a false temperature reading, or a blocked reactor trip signal, is a problem of a different category from a leaked document. The IAEA states this outright, listing the consequences of compromise of an I&C function in order from the worst: the function remains undetermined, with the effects of compromise producing an unnoticed change in the design or operation of the system; the function behaves unexpectedly but observably for the operator; the function fails; the function performs as expected, meaning the compromise does not affect it adversely [17, para. 2.21]. The worst case is not failure but a silent change in system behaviour that nobody notices. Detecting precisely such changes is a research strand of its own, covering methods for detecting falsified process signals [46, 53].

The second difference is the length and rigidity of the life cycle. An I&C platform chosen at the design stage operates for decades. A software update in a protection system is not a routine action but a modification that requires verification and validation to be repeated. The "patch fast" habit of general IT is here not so much difficult as formally prohibited without the proper procedure. This also shapes the way security testing can be performed, which must be subordinated to the operational regime of the facility [47].

The third difference, the least obvious one, is that a security measure can itself become a hazard to nuclear safety. The IAEA devotes a separate block of guidance to it. A badly designed protective measure can introduce new failure modes into the system, increase the probability of spurious actuation and undermine the system's ability to perform its safety function reliably; the example given is improperly implemented antivirus protection inside an I&C system, which adds complexity, adds latency and itself creates a new attack path [17, para. 3.37]. The guidance distils this into a rule: neither normal nor abnormal operation of any computer security measure should adversely affect the ability of the I&C system to perform its safety function [17, para. 3.44]. The failure modes of the protective measures themselves are to be identified, documented and included in the system hazard analyses [17, para. 3.45]. The OECD Nuclear Energy Agency reached similar conclusions when analysing the impact of cybersecurity features on digital safety systems [48].

The resolution of the conflict is unambiguous, and it is sometimes quoted inaccurately, so I quote it precisely. If

a conflict arises between nuclear safety and security, the solutions adopted for nuclear safety are maintained, but the operator is to seek a solution that complies with the computer security requirements; compensatory measures reducing the risk to an acceptable level are to be implemented, supported by full justification and risk analysis, and they should not rest solely on administrative measures for an extended period. The sentence closing that paragraph reads: the absence of a security solution should never be accepted [17, para. 3.49]. Nuclear safety wins the dispute over a particular measure, but it releases no one from the duty to secure the system.

This relationship has a standard of its own. IEC 62859 [16] deals exclusively with coordinating nuclear safety and cybersecurity: it is meant to optimise the introduction of cybersecurity provisions into I&C architectures and systems, to prevent conflicts between the two, and to help identify and exploit synergies. It is built of three parts: the I&C architecture as a whole, the level of the individual system, and organisational and procedural matters.

4. The IAEA requirements architecture

4.1. The document hierarchy

The IAEA guidance on computer security is layered. I reconstruct the layers here, because they decide which document governs what (Fig. 1).

At the top stand the Nuclear Security Fundamentals and the Recommendations. These include above all NSS 13, the recommendations on the physical protection of nuclear material and nuclear facilities known as INFCIRC/225/Rev. 5 [11], and NSS 20, which defines the objective and essential elements of a state's nuclear security regime [12]. Below them sits the implementing guide NSS 42-G [21], issued in 2021. It is the first IAEA document to cover computer security as a whole: the roles of the state and of entities, the national strategy, the elements of computer security programmes and the sustaining activities. Lower still lie the technical guidance documents: NSS 17-T (Rev. 1) on computer security techniques for nuclear facilities [20], issued in 2021 as a revision of the 2011 document, and NSS 33-T of 2018 [17], devoted solely to I&C systems. The division of labour between these two is distinct: NSS 17-T (Rev. 1) describes computer security risk management at the level of the whole facility, from defining the scope and characterising the facility, through threat characterisation, to the specification of requirements [20, para. 4.10]. NSS 33-T descends to the level of the individual I&C system and its life cycle. NSS 42-G itself describes this relationship, referring the reader to NSS 33-T and NSS 17-T (Rev. 1) for more detailed guidance, examples of the technical implementation of measures, and risk management. The set is completed by NSS 23-G on the security of nuclear information [13] and by the documents on the design basis threat [22] and on nuclear security culture [10].

For a practitioner the most important document is NSS 33-T, because it is the only one in this family written specifically for instrumentation and control systems. Its guidance is arranged in four chapters: key concepts, the risk-informed approach, the I&C system life cycle, and activities in the individual phases of that cycle; the last of these chapters alone runs to 226 numbered paragraphs. Its counterpart on the nuclear safety side is SSG-39, on the design of I&C systems for nuclear power plants [14], and on the management side, GSR Part 2 [15].

One thing has to be noted here, and it matters to anyone who wants to rely on these documents in licensing

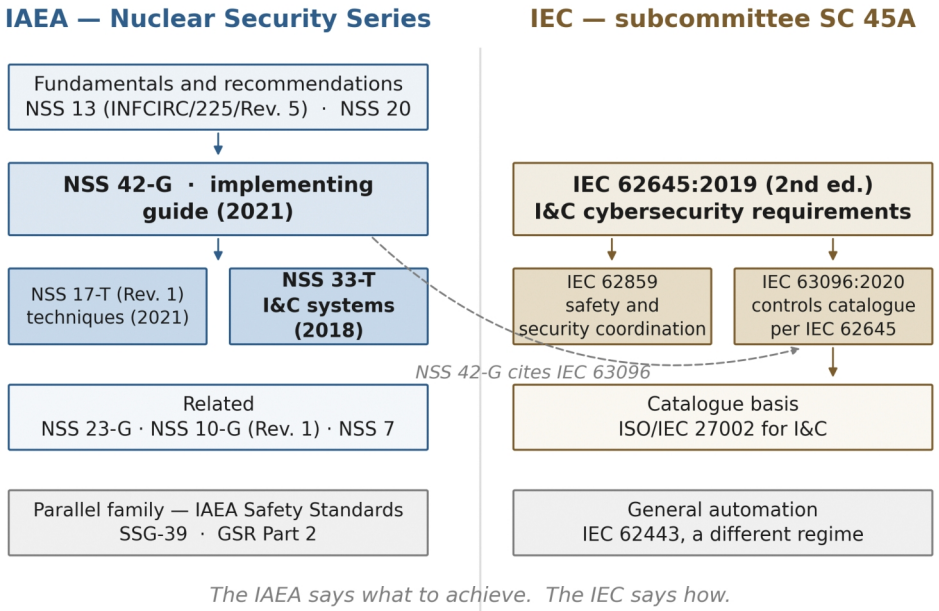


Fig. 1. The hierarchy of IAEA documents and IEC standards on the computer security of nuclear facilities. Author's own elaboration based on the content and reference lists of NSS 42-G [21] and NSS 33-T [17] and on the descriptions of IEC 62645 [18], IEC 62859 [16] and IEC 63096 [19].

proceedings. NSS 33-T dates from 2018, and its reference list still cites NSS 17 of 2011 and IEC 62645:2014, both of which have since been superseded. A revision of NSS 33-T is in preparation. Invoking this document in design documentation therefore requires checking that the standards it cites onward are not already outdated. The earlier edition of NSS 17 was, for that matter, the subject of a critical analysis of attack scenarios, which pointed to the limitations of the approach as it then stood [27].

4.2. Four load-bearing concepts

The whole IAEA methodology rests on four concepts that hold one another up. I give the definitions after the NSS 42-G glossary [21].

Sensitive digital assets (SDA) are sensitive information assets that are computer-based systems or parts of such systems. Sensitive information assets comprise any equipment or components used to store, process, control or transmit sensitive information, including control systems, networks and information systems. Identifying SDAs is the first step: until it is known what is being protected, the later stages have no foundation.

A **computer security level** is the strength of protection required to meet the computer security requirements for a function associated with physical protection, nuclear safety, nuclear material accounting and control, or the management of sensitive information. NSS 17-T (Rev. 1) gives a concrete scale: levels are numbered from 5, requiring the weakest protection, to 1, requiring the strongest, with systems containing sensitive digital assets placed at levels 1 to 3, and the remaining digital assets at levels 4 and 5 [20, para. 3.24]. Requirements attach to the level, while the choice of a specific measure remains a design decision, dependent on the architecture and technology of the asset concerned [20, para. 3.23]. NSS 33-T stresses at the same time that computer security levels and nuclear safety classes are distinct, though related, concepts [17, para. 2.24]. The operator assigns the level on the basis of the potential consequences of failure or malfunction of the system, including behaviour departing from the design or from the failure modes assumed in the safety analysis. The level is a property of the system itself and does not depend on its environment [17, para. 2.27]. Practical experience of categorising I&C systems by level has been described by the Ukrainian nuclear regulator in a series of articles [28, 32, 35, 42], one of the few public accounts of this process from a regulator's perspective.

A **computer security zone** is a group of systems with common physical or logical boundaries that have been assigned a common computer security level in order to simplify administration, communication and the application of protective measures. All systems in a zone are protected at the most stringent level present in that zone [17, para. 2.28]. The consequence is practical: a communication device performing functions of low significance, but placed in the zone of the reactor protection system, receives that system's level, because it can be used to compromise it [17, para. 2.30].

The **defensive computer security architecture** binds the above into a design solution. The operator is to define an overall defensive architecture in which every I&C system has an assigned level and is protected in accordance with the corresponding requirements [17, para. 4.132]. The

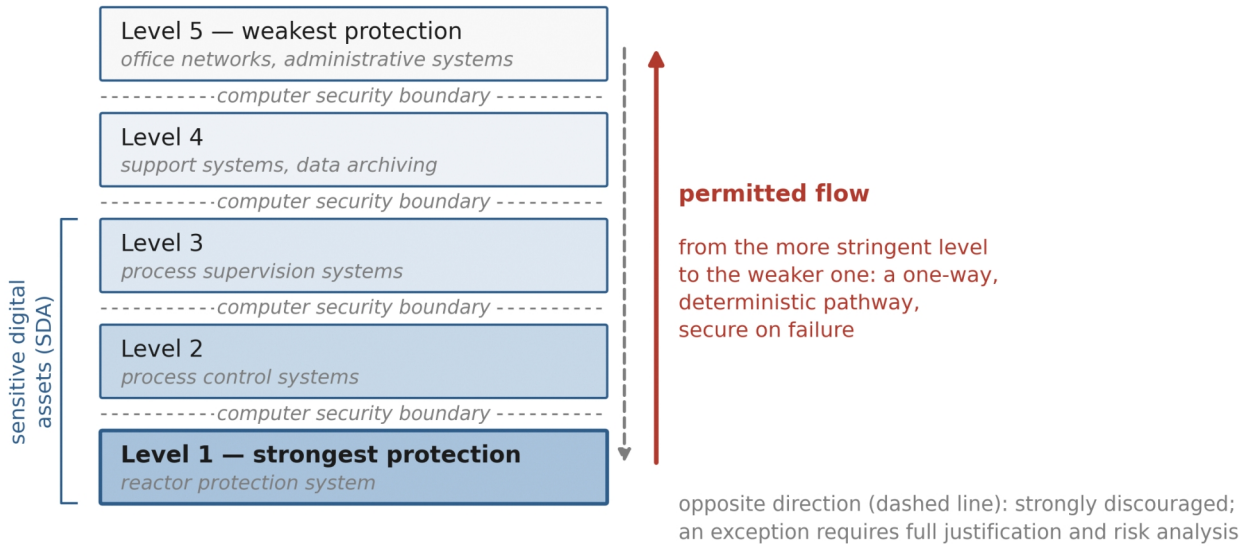


Fig. 2. Computer security levels, zones and data flow rules in the defensive computer security architecture. A conceptual diagram based on NSS 17-T (Rev. 1) [20], para. 3.24 (the five-level scale and the placement of sensitive digital assets), and NSS 33-T [17], paras 2.28–2.30 and 4.132–4.143 (zones, boundaries, flow rules). The assignment of specific systems to levels is an example illustrating the rule, not a depiction of any real installation.

architecture is to make it possible to prevent attacks, detect them, delay them, mitigate their consequences and recover from them [17, para. 4.133].

4.3. Architecture rules and defence in depth

Several construction rules follow from the architecture chapter. They are what translates the concepts into design decisions (Fig. 2).

Computer security boundaries are introduced between systems of different levels [17, para. 4.134], and data flow between zones of different levels, as well as between systems within the same level, is subject to control based on risk assessment [17, para. 4.135]. Systems at the highest level are connected to systems at lower levels only through one-way, deterministic communication pathways operating in a fail-secure mode, with the direction of flow restricted to transmission from higher-level systems to lower-level systems; exceptions are strongly discouraged and may be considered only case by case, with full justification and risk analysis [17, para. 4.136]. The document notes on this occasion that some Member States take the view that exceptions should not be allowed at all. Remote access to systems at the highest level is impossible in this construction, which follows directly from the one-way restriction on outbound traffic.

Technical measures applied inside a zone or at its boundary are to use technologies different from those applied at neighbouring levels and boundaries, which provides diversity of protection [17, para. 4.140]. Wireless communication in systems at the most stringent level is considered problematic, because a secure boundary is difficult to assure for it [17, para. 4.138].

Defence in depth against compromise is, in this methodology, more than technical layering. It consists of multiple layers of measures that must fail or be bypassed for an attack to progress, but it also includes maintaining a programme of measures that assess, prevent, detect, protect, respond, mitigate and recover [17, para. 4.142]. The requirement closing this block is a strong one: no single failure within or between the defensive layers should invalidate the protection as a whole [17, para. 4.143]. This carries over to security the same principle that nuclear safety described long ago and in detail [31], with the difference that here the layers face an adversary rather than a probability distribution. The design of systems robust against compromise has also received dedicated treatment [44].

4.4. The graded approach

The IAEA requires requirements to be graded according to risk, and it says what is to be taken into account: the significance of the I&C system's function both for nuclear safety and for security; the identified and assessed threats to the facility; the attractiveness of the system to a potential adversary; the vulnerabilities of the system; the operating environment; and the potential consequences that compromise of the system could cause, directly or indirectly [17, para. 2.20]. Requirements are defined in proportion to the potential consequences of an attack [17, para. 2.21].

Two items on that list have no counterpart in purely reliability-based thinking: attractiveness to an adversary, and threat assessment. Reliability asks how often something fails. Security asks who would want to break it, and why. These are different questions, and they lead to different designs.

The IAEA says as much directly when listing the inputs to computer security risk management for a facility. Among them is the safety analysis of the facility's computer systems, with a caveat: that analysis may serve to define computer security requirements, but it is not sufficient for the purpose, because it does not cover all mal-operations, in particular those caused by malicious acts [20, para. 4.9]. I return to this caveat in section 7, in assessing the Polish design regulation. The literature supplies tools for ordering this second perspective: a taxonomy of attacks on the digital environment of a nuclear power plant [40] and a framework for assessing attack scenarios by relative difficulty of execution and consequence [41].

5. The IEC family of standards

The IAEA guidance describes what is to be achieved. The IEC standards describe how to do it in engineering terms, and they form a coherent family prepared by subcommittee SC 45A (Fig. 1). Their genesis and mutual relations are discussed at greater length in the literature [43, 51].

IEC 62645 [18] is the base document. The second edition, of November 2019, replaced the 2014 edition and changed the title along the way: from requirements for security programmes for computer-based systems to cybersecurity requirements for instrumentation, control and electrical power systems of nuclear power plants. The standard establishes requirements and guidance for developing and maintaining computer security programmes for programmable digital I&C systems, and it defines measures for preventing, detecting and responding to malicious acts committed by digital means. It is the source of the concept of security degrees, to which the other standards of the family refer.

IEC 62859 [16] is responsible for coordinating nuclear safety and cybersecurity, as discussed above.

IEC 63096 [19], of October 2020, supplies a catalogue of security controls, recommended and optional, graded according to the security degrees defined in IEC 62645. The catalogue builds on the controls of ISO/IEC 27002, with the original requirements modified, refined or sup-

plemented where this proved necessary from the perspective of programmable digital I&C systems. The standard addresses both the I&C of new plants and the modernisation of existing facilities. It is also the standard the IAEA cites in NSS 42-G when discussing security measures.

The construction of this family has one distinct advantage: it avoids carrying over wholesale the provisions of IEC 62443, which was written for industrial automation in general [26]. The zone-based approach is similar in both families [57], but the nuclear requirements take account of safety classification, qualification requirements and a modification regime that general automation does not have. A separate issue, beyond the scope of this article, is the interface between a nuclear power plant and the power system, and the couplings that follow from it [45].

6. What the documented incidents teach

Incidents call for caution, because accounts circulate in this field that do not survive confrontation with the source. I confine myself to what the operator confirmed or what peer-reviewed analysis established (Fig. 3). A broader treatment of the cases from a nuclear security perspective can be found in a handbook chapter [52].

Stuxnet (2010) remains the reference case, because it showed that malicious software can be written for a specific configuration of industrial controllers and can alter the behaviour of the process while presenting the supervision system with a picture of normal operation [25]. Its significance for nuclear regulation is twofold. It demonstrated that separating a network from the Internet is not a safeguard in itself. It also enacted precisely the worst-case scenario the IAEA describes as an unnoticed change in the operation of a system. The IAEA cites an analysis of this case as the first item in the NSS 33-T reference list.

Korea Hydro and Nuclear Power (2014) is the case in which reactor documentation, manuals and employees' personal data leaked, the entry vector being the phishing of people connected with the operator and its subsidiaries. Control systems were not breached [33]. The lesson is therefore not a direct threat to unit operation but something subtler: the design documentation of I&C systems is itself a sensitive asset, because it shortens an adversary's path to preparing an attack. That is exactly how the IAEA defines sensitive information and sensitive information assets [13, 21].

Kudankulam (2019) supplied the case of malicious software present in the administrative network of a power plant. The operator, Nuclear Power Corporation of India, confirmed on 30 October 2019 that malware had been detected. It concerned, according to the operator, a single computer connected to the administrative network; the operational networks controlling the two 1000 MW units are entirely separate from it [36]. With all due caution towards operators' statements, the case illustrates the IT–OT boundary as the real point at which the scale of an incident is decided, and it is an argument for that boundary being designed rather than assumed.

The common lesson of these three cases is that network separation works exactly as well as it was designed and is maintained. The literature has described mechanisms for carrying data across the boundaries of networks assumed to be isolated [34]. The IAEA addresses this directly, requiring that removable media, portable devices and other temporary equipment that needs access to a system be used only within a single zone or a defined set of zones [17, para. 2.29]. A separate thread, not developed here, is the insider threat, which has its own literature [29, 54] and its own IAEA documents.

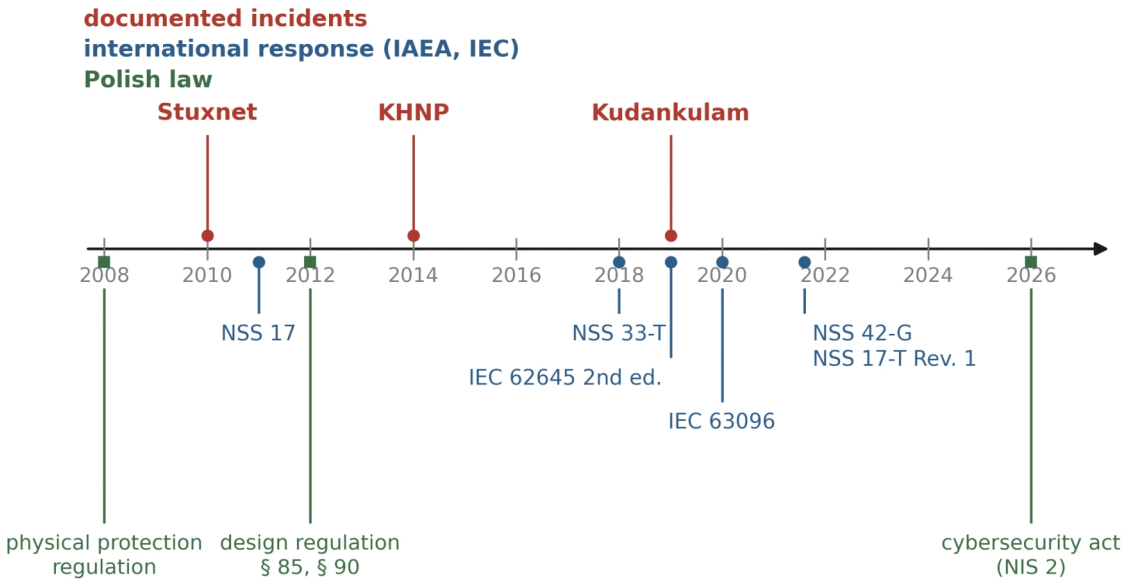


Fig. 3. Chronology of documented incidents relevant to the computer security of nuclear facilities and of the regulatory response. The compilation includes only incidents confirmed by the operator or described in peer-reviewed literature [25, 33].

7. The Polish legal framework

Set against the above, national law can be summarised in one sentence: the computer security of nuclear facility I&C is regulated in Poland in four places, which came into being independently and have never been reconciled with one another (Fig. 4).

7.1. The first regime: design requirements

The basis is the Regulation of the Council of Ministers of 31 August 2012 on the nuclear safety and radiological protection requirements to be taken into account in the design of a nuclear facility [5]. It devotes two provisions to ICT systems (systemy teleinformatyczne).

Paragraph 85 concerns the situation in which the correct operation of a system important to nuclear safety and radiological protection depends on the reliable functioning of an ICT system. It then requires appropriate standards and procedures to be implemented and applied throughout the period of the system's use, in particular in the software development cycle. Subparagraph 2 requires the reliability level of the hardware and software to be commensurate with the importance of the system for the fulfilment of safety functions. Subparagraph 3 requires the adopted reliability level to include safety margins compensating for the uncertainties of analysis arising from the complexity of the system.

Paragraph 90 adds six requirements for ICT systems used in safety systems, in particular in the protection system: high quality requirements commensurate with the significance of the system; systematic documentation and review of the development process, together with the control, testing and acceptance of design changes; confirmation of high reliability by a specialist independent of the designer and the supplier; diverse technical solutions where safety functions are of fundamental significance for reaching and maintaining safe shutdown; consideration of common cause failures caused by software errors; and, in point 6, the introduction of protection against accidental or deliberate interference (zabezpieczenia przed przypadkową lub rozmyślną ingerencją) with the operation of the system.

The proportions of these provisions speak for themselves. Five of the six requirements of § 90, and the whole of § 85, concern quality and reliability: the development cycle, documentation, independent verification, common cause failures. That is the language of safety engineering, and on its own terms it is sound. Intentional action receives a single expression: the word "deliberate" (rozmyślną) in point 6, in a sentence that places it beside accidental interference. For comparison, NSS 33-T develops the same subject matter across four chapters of numbered guidance, of which the chapter on life-cycle activities alone contains 226 paragraphs, and IEC 63096 supplies a full catalogue of controls. I am not arguing that the design regulation should contain such a catalogue; that is not its role. I am arguing that a single adjectival aside does not create a basis on which a regulator could assess a defensive computer security architecture, because it defines neither the concepts nor the criteria.

Here the IAEA caveat quoted in section 4.4 returns. Safety analysis of a facility's computer systems is not sufficient to define computer security requirements, because it does not cover mal-operations caused by malicious acts [20, para. 4.9]. The Polish design regulation does exactly what that paragraph warns against: it builds the requirements for ICT systems solely on the ground of reliability analysis. This bears directly on the licensing proceedings, because the preliminary safety report is drawn up precisely

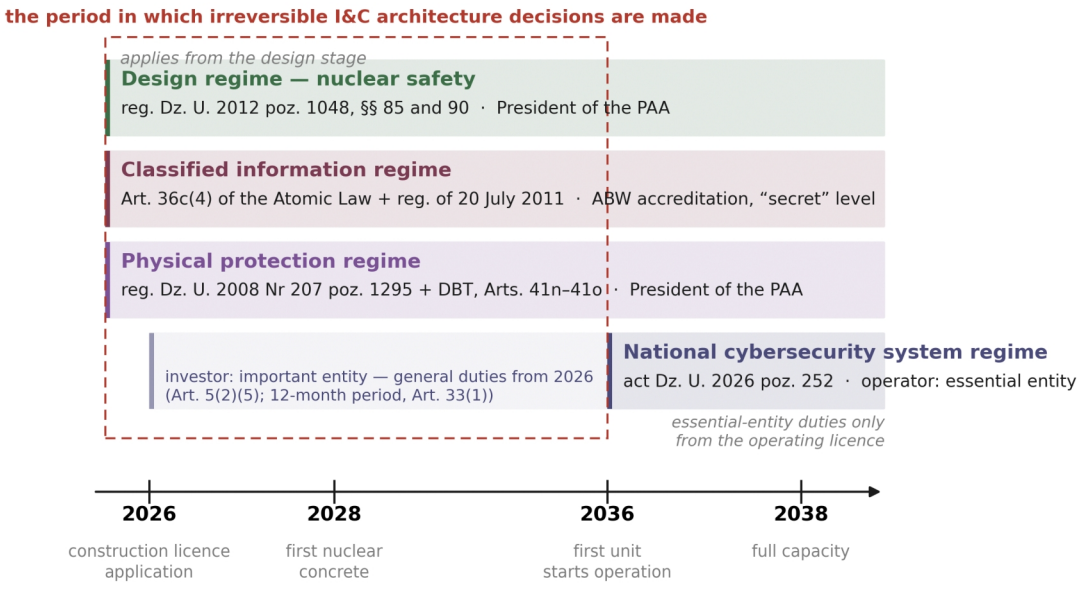


Fig. 4. The four regulatory regimes applicable to the computer security of nuclear facility I&C in Poland, set against the phases of the facility life cycle. Author's own elaboration based on the texts of the legal acts [1, 2, 5, 9]. Schedule dates after the 2025 draft update of the Polish Nuclear Power Programme [23].

on the basis of the safety analyses conducted under Article 36d(1) of the Atomic Law [1].

What these provisions do not contain is telling as well. There are no computer security levels, no zones, no requirement to identify sensitive digital assets, no one-way data flow rule, no requirement of diverse technologies at zone boundaries. There is also no obligation to take a threat assessment into account when defining the requirements for a system, and that is precisely the element that distinguishes security from reliability.

7.2. The second regime: protection of classified information

The second place is Article 36c(4) of the Atomic Law [1]. The provision states that ICT systems forming elements of the critical ICT infrastructure (teleinformatyczna infrastruktura krytyczna) intended for supervising the course of the technological or production process in nuclear facilities are designed, built and operated in a manner meeting the ICT security requirements laid down in the provisions on the protection of classified information for systems and networks used to process classified information bearing the "secret" (tajne) classification. The authority competent for the accreditation of these systems and networks is the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW).

This is the only provision in Polish nuclear law that places real, enforceable ICT security requirements on the systems supervising the technological process, together with a procedure for confirming them. Its construction deserves attention, though, because it has three consequences.

The first concerns the logic of the requirements. The classified information regime exists to prevent disclosure, but its technical layer is broader than confidentiality alone. The requirements to which Article 36c(4) refers are laid down in the Regulation of the Prime Minister of 20 July 2011 on basic ICT security requirements [4]. Its § 5(1) obliges the protection of confidentiality, integrity and availability alike; § 5(2) requires risk management, limited trust towards other systems, layered protection and security testing; § 18 spans the entire period of the system's operation; and § 20 requires the identification of resources, threats, vulnerabilities and safeguards. Read together with the accreditation procedure, this is a real security-management regime, not an access-control annex. What it is not is an I&C regime. It grades nothing by the consequences of a compromised control function, and it knows none of the NSS 33-T concepts: no levels, no zones, no defensive architecture, no one-way data flows. Accreditation at the "secret" level therefore covers more of the NSS 33-T problem than a confidentiality-only reading would suggest; it still does not cover the whole of it.

The second concerns scope. The provision covers systems intended "for supervising the course of the technological or production process". The IAEA methodology covers all systems whose compromise could adversely affect nuclear safety or security, together with the principle of assigning auxiliary devices to the level of the zone in which they are placed [17, para. 2.30]. A scope based on the supervisory function and a scope based on the potential consequences of compromise do not coincide.

The third concerns the authority. Accreditation is carried out by the ABW, an authority other than the President of the PAA, who approves the physical protection system and issues licences. NSS 42-G discusses the division of roles between the state and the operator and underlines the need for coherence of the whole regime [21]; the dispersal of competences is not a defect in itself, but it calls for a coordination mechanism.

7.3. The third regime: physical protection and the design basis threat

Physical protection is a regime in its own right: it has its own authority, its own approval moment and its own logic. It is also where the IAEA places computer security: NSS 13 treats it as an element of facility protection [11].

The Polish Regulation of the Council of Ministers of 4 November 2008 on the physical protection of nuclear material and nuclear facilities [2], still in force, contains not a single reference to ICT, computer or information systems. I checked this directly in the text of the act. The regulation dates from 2008, which is to say before Stuxnet, before NSS 17 and before the entire layer of IAEA documents described in section 4. This is the most direct gap and, at the same time, the easiest to close, because closing it does not require amending the statute.

The statute itself is more modern in this respect than its implementing act. The definition of the design basis threat contained in the Atomic Law includes the characteristics of entities that may seek to commit acts such as theft, unauthorised use, cyber-attack, an act of terror or sabotage, and this threat is taken into account in developing the physical protection system [1]. The statute requires the design basis threat to be taken into account in the development, approval and review of physical protection systems (Article 41n), and it is drawn up by the President of the PAA in consultation with the competent authorities (Article 41o), which corresponds to the construction recommended by the IAEA [22]. The current revision of that guidance, NSS 10-G (Rev. 1) of 2021, matters here in its own right: it brings computer security into the national threat assessment and sets out, step by step, how a design basis threat that includes cyber threats is developed, maintained and used [22]. The bridge between the statutory mention of cyber-attack and a working, cyber-inclusive design basis threat therefore already exists at the method-

ological level. The President of the PAA also has, within the scope of oversight, the right to demand access for inspection to the networks or ICT systems used in the physical protection system of the inspected facility.

We therefore have a situation in which the statute lists cyber-attack among the design basis threats and gives the regulator an inspection tool, while the implementing act defining the content of physical protection is silent about digital systems. The statutory basis for filling this gap already exists.

7.4. The fourth regime: the national cybersecurity system

The fourth place is the newest. The Act of 23 January 2026 amending the Act on the National Cybersecurity System and certain other acts [9], promulgated on 2 March 2026, implements the NIS 2 Directive [8] by amending the 2018 statute [7]. Under its Article 49, it enters into force one month after the day of promulgation, that is on 3 April 2026.

Three of its elements matter for the subject of this article. In Annex 1, covering the essential sectors, a subsector "Nuclear energy" has been distinguished within the Energy sector. The type of entity indicated is an entity operating a nuclear power facility within the meaning of the Act on the preparation and implementation of investments in nuclear power facilities and associated investments [3]. The statute also fixes the moment at which the operator of a nuclear power plant becomes an essential entity. It is the day it obtains the operating licence referred to in Article 4(1)(2) of the Atomic Law, or the day it obtains a concession for the generation of electricity or heat under the Energy Law, whichever comes first.

The operator is not the only addressee. Under Article 5(2)(5) of the amended statute, an investor for a nuclear power facility which has obtained the principal decision is an important entity, regardless of its size, and Annex 2 lists the corresponding sector, investments in nuclear power. Article 8 attaches the obligations of chapter 3 to essential and important entities alike, and under Article 33(1) of the amending act an entity that met the criteria on the day the amendment entered into force has twelve months to implement them. The investor obtained the principal decision in July 2023, before filing the construction licence application [24], so it met those criteria on 3 April 2026 and its general cybersecurity obligations fall due within a year of that date.

The nuclear programme thus enters the national cybersecurity regime explicitly, on two tracks: the investor as an important entity now, the operator as an essential entity from the operating licence. That is a qualitative change from the previous state. It does, though, raise the question of what each track carries, and when.

The two tracks differ in content. The investor's obligations are the general management duties of chapter 3: a security management system, risk analysis, incident handling, documentation. They bind the investor as an organisation, and none of them speaks the language of I&C: no sensitive digital assets, no computer security levels or zones, no defensive architecture, no data flow rules. The operator's obligations, attached to the essential-entity status, arrive with the operating licence or the concession, which on the current schedule means around 2036 [23]. By then the facility will have gone through commissioning, whose requirements a separate regulation governs [6], and the I&C systems will already be installed and tested. So the regime reaches the project today, but what reaches it is a general management toolkit; the I&C architecture being settled now, at the design stage, is addressed by neither track.

The relation to the other regimes has not been settled either. The investor is already an important entity under the national cybersecurity system; the operator will simultaneously be an essential entity under that system, the addressee of the ABW accreditation requirements under Article 36c(4) of the Atomic Law, and an entity overseen by the President of the PAA as regards physical protection and nuclear safety. Each of these regimes has its own authority, its own procedure for confirming conformity and its own reporting duties. The literature on the implementation of NIS 2 in the energy sector describes this type of regime overlap as a recurring problem [56], as do analyses of cybersecurity standards in the electricity sector [38, 39]. In the Polish setting, the relation between cybersecurity and the protection of critical infrastructure has already been the subject of legal analysis [55].

8. Coverage map and gaps

The juxtaposition in Figure 5 puts the above in order. I took the elements of the NSS 33-T methodology as the axis and checked whether, and where, each finds a counterpart in national law. I repeat the reservation from section 2: this is an expert judgement based on a reading of the texts, not a measurement.

Five elements have no counterpart in national law at all. There is no obligation to identify and inventory sensitive digital assets. There are no computer security levels as a normative category, and no computer security zones. There is no requirement to present a defensive computer security architecture as an element of the documentation. There are no rules for data flow between levels, including the one-way rule for connections with systems at the highest level.

Three elements are covered in part. Grading of requirements exists, but in its reliability version: § 85(2) of the design regulation ties the reliability level to the importance

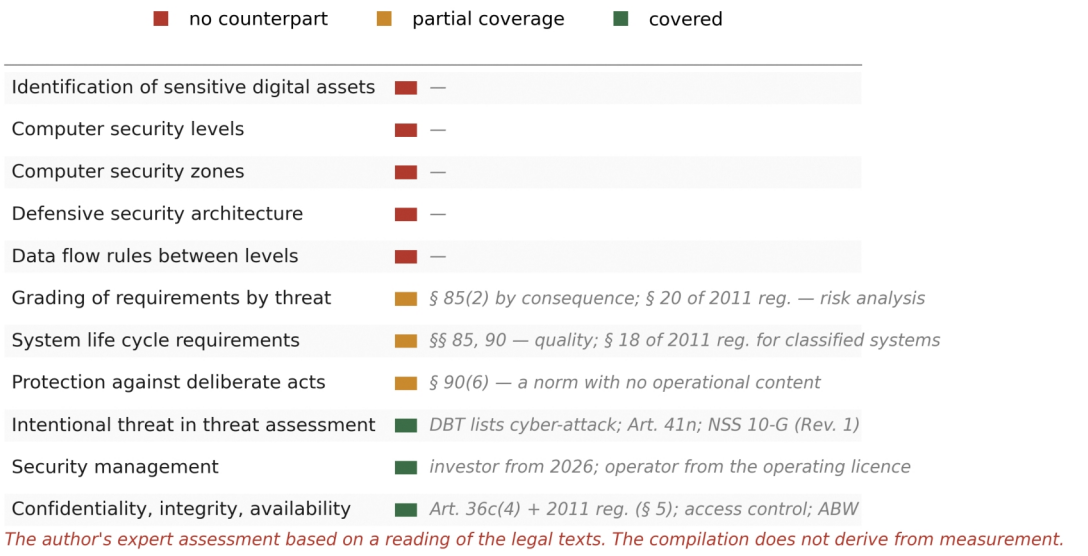


Fig. 5. Coverage of the elements of the NSS 33-T methodology [17] by Polish provisions — an expert assessment. The compilation does not derive from measurement; it is the author's judgement based on a reading of the texts of the legal acts and guidance.

of the safety function, which is grading by consequence, not by threat. Life cycle requirements are present and quite developed, except that they concern the quality of production, not resistance to attack; for the systems under Article 36c(4), § 18 of the 2011 regulation adds security duties spanning the system's whole period of operation [4]. Protection against intentional action exists as a norm, in § 90(6), but without operational content.

Three elements are covered in a way I consider sufficient at the statutory level. The inclusion of intentional threats in threat assessment is ensured by the definition of the design basis threat, which lists cyber-attack, and by Article 41n, with the methodology for a cyber-inclusive threat assessment supplied by NSS 10-G (Rev. 1) [22]. Security management on the organisational side is covered by the national cybersecurity regime: for the investor, as an important entity, already now, with the twelve-month implementation period of Article 33(1); for the operator, from the operating licence. Access control and the protection of confidentiality are covered by Article 36c(4) and the classified information regime, whose 2011 implementing regulation reaches beyond confidentiality to integrity, availability, risk management and security testing [4].

Four practical conclusions follow from this pattern.

First, the gap is largest where decisions are hardest to reverse. The elements not covered at all (assets, levels, zones, architecture and data flows) are settled in the design. The elements covered well (management, reporting, access control) can be introduced later. The distribution of the gaps is the inverse of the distribution of urgency.

Second, the shortest remedial path does not run through the statute. The delegation in Article 36c(3) of the Atomic Law directs the Council of Ministers to lay down the design requirements taking into account the recommendations of the IAEA and WENRA. The delegation concerning physical protection allows the content of the protection system to be regulated. The design basis threat lists cyber-attack, and the President of the PAA draws it up. Introducing the concepts of computer security into the implementing regulations, or into regulatory guidance, sits within the existing authorisations.

Third, the regulator has a tool already. The construction licence application comes with safety analyses and documentation, and the President of the PAA approves the physical protection system and may attach conditions concerning the assurance of its effectiveness. Requiring the documentation to contain an identification of sensitive digital assets, an assignment of levels and a description of the defensive architecture calls for no new provision, only for that expectation to be stated in the proceedings. The Ukrainian regulator went down this road, working out a catalogue of computer security justification documents for I&C systems [35] and a methodology for assessing the computer security of those systems [42].

One more place deserves a note: the programme document itself. In the Polish Nuclear Power Programme the word "cybersecurity" occurs once, and not among the requirements for the facility, but in the list of fields of university study relevant to the nuclear programme [23]. The document that frames the whole undertaking treats cybersecurity as a staffing question, not a design question.

Fourth, Polish terminology is needed. The four load-bearing concepts of the IAEA methodology have no established Polish equivalents in normative texts. Until they exist, every set of documentation will translate them anew, and the regulator will be assessing things that go by different names. The Polish renderings proposed here (wrażliwe aktywa cyfrowe, poziom bezpieczeństwa komputerowego, strefa bezpieczeństwa komputerowego, obronna architektura bezpieczeństwa komputerowego) are offered as a starting point for discussion, not as a settlement.

9. Conclusions

Poland is building its first nuclear power plant at a moment when the international methodology for the computer security of I&C systems is mature and available. The IAEA has issued a complete set of guidance: NSS 42-G, NSS 17-T (Rev. 1) and NSS 33-T. The IEC has supplied a family of standards with a catalogue of controls. The material on which requirements can be based exists and is public.

The Polish legal order addresses this subject in four places, but it does so in four different languages. The design regulation speaks of reliability and mentions deliberate interference exactly once, although the IAEA warns in plain terms that safety analysis is not sufficient to define computer security requirements [20, para. 4.9]. The Atomic Law refers the systems supervising the process to the classified information regime, whose 2011 implementing regulation reaches beyond confidentiality to integrity, availability and risk management, with accreditation carried out by the ABW. The amended Act on the National Cybersecurity System, in force since 3 April 2026, covers the investor holding the principal decision as an important entity, with general duties enforceable within twelve months, and names the operator of a nuclear power facility as an essential entity only from the moment of obtaining the operating licence, roughly a decade away from the design decisions those obligations would be meant to secure. The physical protection regulation, still that of 2008, does not mention digital systems at all.

The national cybersecurity regime therefore reaches the investor already, but it operates with general management instruments alone and contains none of the I&C-specific concepts of the NSS 33-T methodology: sensitive digital assets, computer security levels, zones, the defensive architecture, the data flow rules. The other regimes do not introduce them either. Without them, design documentation and regulatory assessment lack a common language, and the grading of requirements remains grading by the consequence of failure, not by the intentional threat.

The conclusion is not alarmist, and it is not meant to be. The statutory framework contains everything needed to close these gaps: a definition of the design basis threat that lists cyber-attack, a delegation to lay down design requirements with an instruction to take IAEA recommendations into account, and the competence of the President of the PAA to approve the physical protection system and to set conditions for its effectiveness. What is missing are the implementing acts and the guidance that would translate the international methodology into the language of Polish regulatory practice. The moment for that is now, during the construction licence proceedings, not after them.

Limitations

This article relies on publicly available documents. I had no access to the design documentation of the Polish plant, or to internal regulatory guidance, if any has been produced. It is therefore possible that some of the identified gaps are being closed at the level of supervisory practice that is not public. The coverage assessment in Figure 5 is an expert judgement and open to debate. The analysis reflects the legal position as at 11 September 2026; given the pace of change in cybersecurity regulation and the ongoing revision of NSS 33-T, that position needs to be rechecked at every later use of this text. I did not analyse the United States requirements, which may carry practical significance given the choice of the AP1000 technology. That is a natural direction for further work.

Declarations

Funding: this work received no external funding.
Conflict of interest: the author declares no conflict of interest.
Statement on the use of artificial intelligence: No generative artificial intelligence tools were used in the preparation, drafting, editing, analysis, or review of this article. All content, analyses, conclusions, and figures were created by the author. The author personally verified all information presented in this work and bears full responsibility for its content. Artificial intelligence is not an author or co-author of this work.
Nature of the work: a review and conceptual article. It contains no original research, measurement data or experimental results.

About the author

Artur Chlebicki — MSc Eng. in Computer Science (Gdańsk University of Technology), independent researcher. Works professionally in the security of ICT systems. Areas of interest: security of industrial process control systems, cybersecurity regulation of critical infrastructure, assessment of the maturity of security processes. Contact: contact@chlebicki.art.

References

I. Legal acts (in chronological order)

1. Ustawa z dnia 29 listopada 2000 r. — Prawo atomowe (tekst jedn. Dz. U. z 2026 r. poz. 1).
2. Rozporządzenie Rady Ministrów z dnia 4 listopada 2008 r. w sprawie ochrony fizycznej materiałów jądrowych i obiektów jądrowych (Dz. U. Nr 207, poz. 1295).
3. Ustawa z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (tekst jedn. Dz. U. z 2025 r. poz. 1156).
4. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).
5. Rozporządzenie Rady Ministrów z dnia 31 sierpnia 2012 r. w sprawie wymagań bezpieczeństwa jądrowego i ochrony radiologicznej, jakie ma uwzględniać projekt obiektu jądrowego (Dz. U. poz. 1048).

6. Rozporządzenie Rady Ministrów z dnia 11 lutego 2013 r. w sprawie wymagań dotyczących rozruchu i eksploatacji obiektów jądrowych (Dz. U. poz. 281).
7. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2026 r. poz. 20).
8. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (Dz. Urz. UE L 333 z 27.12.2022, s. 80).
9. Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252).

II. IAEA documents and technical standards (in chronological order)

10. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
11. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
12. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
13. INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
14. INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).
15. INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).
16. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Coordinating Safety and Cybersecurity, IEC 62859:2016, IEC, Geneva (2016), with amendment IEC 62859:2016/AMD1:2019; consolidated version IEC 62859:2016+AMD1:2019 CSV (ed. 1.1), IEC, Geneva (2019).
17. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
18. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Cybersecurity Requirements, IEC 62645:2019, 2nd ed., IEC, Geneva (2019).
19. INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Security Controls, IEC 63096:2020, IEC, Geneva (2020).
20. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).
21. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).
22. INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

III. Programme documents

23. Program polskiej energetyki jądrowej — projekt aktualizacji z 2025 r. skierowany do konsultacji publicznych [Polish Nuclear Power Programme, draft 2025 update, public consultation version], Rada Ministrów, Warszawa (2025).
24. POLSKIE ELEKTROWNIE JĄDROWE sp. z o.o., Złożenie wniosku o wydanie zezwolenia na budowę obiektu jądrowego [Filing of the application for a licence to construct a nuclear facility], press release of 31 March 2026, Warszawa (2026).

IV. Secondary literature (in chronological order)

25. LANGNER, R., Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Security & Privacy 9 (2011) 49–51, doi: 10.1109/msp.2011.67.
26. PIGGIN, R., Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security, IET Conference on Control and Automation, Birmingham (2013), doi: 10.1049/cp.2013.0001.
27. SEMA, P., ZAVARSKY, P., RUHL, R., A critical review of attack scenarios on the IAEA Technical Guidance NSS 17 Computer Security at Nuclear Facilities, World Congress on Internet Security (WorldCIS-2014), IEEE (2014) 87–90, doi: 10.1109/worldcis.2014.7028173.
28. KLEVTSOV, A., SYMONOV, A., TRUBCHANINOV, S., Computer Security of NPP Instrumentation and Control Systems: Categorization, Nuclear and Radiation Safety 4(72) (2016) 65–70, doi: 10.32918/nrs.2016.4(72).10.
29. HEALEY, A.N., The insider threat to nuclear safety and security, Security Journal 29 (2016) 23–38, doi: 10.1057/sj.2015.42.
30. LITHERLAND, P., ORR, R., PIGGIN, R., Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security, 11th International Conference on System Safety and Cyber-Security, IET (2016), doi: 10.1049/cp.2016.0856.
31. OECD NUCLEAR ENERGY AGENCY, Implementation of Defence in Depth at Nuclear Power Plants, OECD Publishing, Paris (2016), doi: 10.1787/9789264253001-en.
32. SYMONOV, A., KLEVTSOV, A., TRUBCHANINOV, S., Computer Security of NPP Instrumentation and Control Systems: Protective Measures against Computer Threats, Nuclear and Radiation Safety 2(74) (2017) 46–50, doi: 10.32918/nrs.2017.2(74).09.
33. BIAN, Y., LI, J., YIN, B., Analysis of Cyber Security Incident in South Korean Nuclear Power Plant and Cyber Security Solutions for Nuclear Power Industry, Proceedings of ICONE25, ASME (2017), doi: 10.1115/icone25-67577.
34. GURI, M., MONITZ, M., ELOVICI, Y., Bridging the Air Gap between Isolated Networks and Mobile Phones in a Practical Cyber-Attack, ACM Transactions on Intelligent Systems and Technology 8 (2017) 1–25, doi: 10.1145/2870641.
35. SYMONOV, A., KLEVTSOV, O., TRUBCHANINOV, S., LAZURENKO, O., Computer Security of NPP Instrumentation and Control Systems: Computer Security Justification Documents, Nuclear and Radiation Safety 4(84) (2019) 73–81, doi: 10.32918/nrs.2019.4(84).09.
36. ROBBINS, M., Cyberattack Hits Indian Nuclear Plant, Arms Control Today, December 2019.
37. JAKÓBIK, W., NOWAK, Z., NOWAKOWSKI, R., Energetyka jądrowa w Polsce [Nuclear power in Poland], Sprawy Międzynarodowe 72 (2019) 245–255, doi: 10.35757/sm.2019.72.3.08.
38. LESZCZYNA, R., Cybersecurity in the Electricity Sector, Springer, Cham (2019), doi: 10.1007/978-3-030-19538-0.
39. LESZCZYNA, R., Cybersecurity Standards Applicable to the Electricity Sector, in: Cybersecurity in the Electricity Sector, Springer, Cham (2019) 59–86, doi: 10.1007/978-3-030-19538-0_3.
40. KIM, S., HEO, G., ZIO, E., SHIN, J., Cyber attack taxonomy for digital environment in nuclear power plants, Nuclear Engineering and Technology 52 (2020) 995–1001, doi: 10.1016/j.net.2019.11.001.
41. PARK, J.W., LEE, S.J., A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence, Annals of Nuclear Energy 142 (2020) 107432, doi: 10.1016/j.anucene.2020.107432.
42. KLEVTSOV, O., SYMONOV, A., TRUBCHANINOV, S., Computer Security of NPP Instrumentation and Control Systems: Computer Security Assessment, Nuclear and Radiation Safety 4(88) (2020) 69–76, doi: 10.32918/nrs.2020.4(88).09.

43. TRUBCHANINOV, S., International Standard Bases, in: Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems, IGI Global, Hershey (2020) 27–55, doi: 10.4018/978-1-7998-3277-5.ch002.
44. JOHNSON, G., Cyber Robust Systems, in: Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems, IGI Global, Hershey (2020) 163–174, doi: 10.4018/978-1-7998-3277-5.ch006.
45. BREZHNIEV, E., IVANCHENKO, O., NPP-Smart Grid Mutual Safety and Cyber Security Assurance, in: Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems, IGI Global, Hershey (2020) 349–380, doi: 10.4018/978-1-7998-3277-5.ch014.
46. ZHANG, F., COBLE, J.B., Robust localized cyber-attack detection for key equipment in nuclear power plants, Progress in Nuclear Energy 128 (2020) 103446, doi: 10.1016/j.pnucene.2020.103446.
47. XI, W., GU, P., LIU, W., Discussions on Information Security Test Strategy for Digital Industrial Control System in Nuclear Power Plant, Lecture Notes in Electrical Engineering, Springer, Singapore (2020) 83–89, doi: 10.1007/978-981-15-1876-8_9.
48. GARCIA, I., Nuclear Energy Agency's Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Safety Systems, NPIC&HMIT 12 (2021) 1437–1444, doi: 10.13182/t124-34209.
49. STRUPCZEWSKI, A., Energetyka jądrowa koniecznym elementem elektroenergetyki polskiej [Nuclear power as a necessary element of the Polish electricity system], ACADEMIA. Magazyn Polskiej Akademii Nauk (2021) 88–97, doi: 10.24425/academiapan.2021.136854.
50. YANG, A., Discussion on Functional Safety and Cyber Security of I&C System in Nuclear Facilities, Proceedings of ICONE29, ASME (2022), doi: 10.1115/icone29-90807.
51. YANG, A., Research on Cyber Security Standards of Nuclear Power Industry Control System, Lecture Notes in Electrical Engineering, Springer, Singapore (2022) 75–84, doi: 10.1007/978-981-19-1181-1_8.
52. AGHARA, S., SPIRITO, C., Cyber Security for Nuclear Facilities, in: The Oxford Handbook of Nuclear Security, Oxford University Press, Oxford (2023) 309–324, doi: 10.1093/oxfordhb/9780192847935.013.29.
53. HUANG, Y., WANG, J., GU, H., ZHOU, X., False data injection attack detection for nuclear reactor based on chaotic time/frequency-hopping spread spectrum watermarking, Process Safety and Environmental Protection 176 (2023) 841–851, doi: 10.1016/j.psep.2023.06.068.
54. KHRIPUNOV, I., Nuclear Security Culture as a Tool to Address Insider Threat, in: Advanced Sciences and Technologies for Security Applications, Springer, Cham (2023) 115–126, doi: 10.1007/978-3-031-20278-0_8.
55. CZURYK, M., Cybersecurity and Protection of Critical Infrastructure, Studia Iuridica Lublinensia 32 (2023) 43–52, doi: 10.17951/sil.2023.32.5.43-52.
56. TEICHMANN, F., Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus, International Cybersecurity Law Review 6 (2025) 207–220, doi: 10.1365/s43439-025-00154-4.
57. JAATUN, M.G., LUNDTEIGEN, M.A., THIEME, C.A., FLÅ, L.H., Security Aspects of Zones and Conduits in IEC 62443, Journal of Cybersecurity and Privacy 6 (2026) 52, doi: 10.3390/jcp6020052.

Biuletyn „Bezpieczeństwo Jądrowe i Ochrona Radiologiczna” wydawany jest od 1989 r. Do 2013 r. był drukowany i kolportowany (ostatnio w nakładzie 700 egzemplarzy) wśród osób i instytucji zainteresowanych zagadnieniami dozoru nad bezpieczeństwem jądrowym i ochroną radiologiczną. Od 2014 r. biuletyn wydawany jest w nowej, elektronicznej formie. Każdy numer biuletynu zamieszczany jest na stronie internetowej.

Biuletyn „Bezpieczeństwo Jądrowe i Ochrona Radiologiczna” znajduje się w wykazie czasopism naukowych Ministerstwa Edukacji i Nauki. Kwartalnik wydawany przez PAA otrzymał 40 pkt. w następujących dyscyplinach naukowych:

- nauki o bezpieczeństwie,
- nauki fizyczne,
- nauki chemiczne,
- nauki prawne,
- nauki medyczne,
- inżyniernia bezpieczeństwa,
- biologia medyczna.

Informacja dla autorów

Wydawca przyjmuje artykuły naukowe, których tematyka jest związana z zapewnieniem i kontrolą bezpieczeństwa jądrowego i ochrony radiologicznej, w tym również związane z zabezpieczeniem i ochroną fizyczną materiałów jądrowych i obiektów jądrowych, technologiami jądrowymi i technikami radiacyjnymi, fizyką i chemią oraz inżynierią jądrową, naukami prawnymi, geologią i geofizyką czy bezpieczeństwem narodowym.
Każdy artykuł zamieszczony w biuletynie jest recenzowany przez dwóch recenzentów.

Zasady ogólne

Tekst artykułu powinien prezentować aktualny stan wiedzy na poruszany temat oraz najnowsze dane. Artykuł powinien być podzielony na mniejsze logiczne fragmenty redakcyjne, opatrzone śródtytułami. Artykuł nie może być wcześniej publikowany ani zgłoszony do publikacji w innym czasopiśmie. Wydawca zastrzega sobie prawo nieprzyjęcia artykułu do publikacji, dokonywania skrótów, wprowadzania poprawek stylistycznych i redakcyjnych oraz zmian w tytule artykułu. Autorzy są zobowiązani do współpracy z Wydawcą w całym procesie przygotowywania artykułu do publikacji, w tym do terminowej korekty autorskiej.

Zgłoszenie dzieła

Egzemplarze artykułu wraz z pełnym zestawem ilustracji mogą być przesyłane na adres:

Biuletyn „Bezpieczeństwo Jądrowe i Ochrona Radiologiczna”
Państwowa Agencja Atomistyki
ul. Nowy Świat 6/12,
00-400 Warszawa, Polska
E-mail: biuletyn@paa.gov.pl

Zachęcamy do przesyłania artykułów drogą elektroniczną na wyżej wskazany adres e-mail.
Szczegółowe informacje można uzyskać na stronie internetowej:
https://www.gov.pl/web/paa/biuletyn-bezpieczenstwo-jadrowe-i-ochrona-radiologiczna

Państwowa Agencja Atomistyki
ul. Nowy Świat 6/12, 00-400 Warszawa
www.gov.pl/web/paa