Marcin Niedbała

- Akademia Wymiaru Sprawiedliwości (Academy of Justice, Poland)
- e-mail: marcin.niedbala@aws.edu.pl
- ORCID: 0000-0001-9580-9707

DOI: 10.15290/mhi.2025.24.02.11

EWOLUCJA I PRAWNOPORÓWNAWCZA ANALIZA REGULACJI DOTYCZĄCYCH OCHRONY INFRASTRUKTURY KRYTYCZNEJ W POLSCE I NA LITWIE

Abstrakt

Celem opracowania jest analiza wybranych kluczowych norm prawnych regulujących ochronę infrastruktury krytycznej (IK) w Polsce oraz na Litwie, z uwzględnieniem tła historycznego, ewolucji przepisów oraz trwającego procesu harmonizacji ustawodawstw obu państw z regulacjami Unii Europejskiej i NATO. Podjęte rozważania osadzono w kontekście współczesnych zagrożeń, zwłaszcza o charakterze hybrydowym, płynących ze strony Rosji i Białorusi. Asumpt do podejmowanej problematyki stanowiły rzeczywiste incydenty sabotażu w Polsce i na Litwie, które unaoczniły potrzebę skutecznych, przejrzystych i jednolitych ram prawnych w zakresie ochrony IK.

W artykule przedstawiono genezę pojęcia infrastruktury krytycznej, sięgającą doświadczeń amerykańskich z lat 90. XX wieku, a także rozwój międzynarodowych standardów ochrony tej infrastruktury pod wpływem działań NATO oraz regulacji unijnych, takich jak dyrektywa EIK (2008) i dyrektywa CER (2023). Wskazano, że proces harmonizacji przepisów w Polsce i na Litwie trwa nadal i koncentruje się wokół implementacji tych aktów.

W części poświęconej Polsce omówiono obowiązujące ramy prawne – przede wszystkim ustawę o zarządzaniu kryzysowym z 2007 roku oraz Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK). Wskazano na wysoki poziom formalizacji,

przejrzystość obowiązków oraz zaangażowanie zarówno organów publicznych, jak i prywatnych w ochronę IK. W przypadku Litwy scharakteryzowano ustawę z 2002 roku o ochronie obiektów o istotnym znaczeniu dla bezpieczeństwa państwa oraz późniejsze akty wykonawcze i podkreślono ich rozproszenie, brak spójności i dominację aspektów właścicielskich oraz cyberbezpieczeństwa.

W opracowaniu zastosowano metody: dogmatycznoprawną, historycznoprawną, prawnoporównawczą oraz analizy dokumentów i treści. Źródłami analizy były akty normatywne i dokumenty strategiczne obowiązujące w Polsce, na Litwie oraz w ramach UE i NATO. W podsumowaniu wskazano na potrzebę dalszej harmonizacji oraz zacieśnienia współpracy polsko-litewskiej w zakresie ochrony IK jako warunku zwiększenia odporności obu państw na zagrożenia współczesnego świata.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo narodowe, Polska, Litwa, ochrona obiektów strategicznych

EVOLUTION AND COMPARATIVE LEGAL ANALYSIS OF REGULATIONS CONCERNING CRITICAL INFRASTRUCTURE PROTECTION IN POLAND AND LITHUANIA

Abstract

The aim of the study is to analyse selected key legal norms regulating the protection of critical infrastructure (CI) in Poland and Lithuania, taking into account the historical background, the evolution of regulations and the ongoing process of harmonising the legislation of both countries with the regulations of the European Union and NATO. The considerations were placed in the context of contemporary threats, especially those of a hybrid nature, posed by Russia and Belarus. The starting point for the considerations were actual incidents of sabotage in Poland and Lithuania, which highlighted the need for an effective, transparent and uniform legal framework for CI protection.

The article presents the origins of the concept of critical infrastructure, dating back to the American experience of the 1990s, as well as the development of international standards for the protection of this infrastructure under the influence of NATO activities and EU regulations, such as the ECI Directive (2008) and the CER Directive (2023). It is pointed out that the process of harmonising regulations in Poland and Lithuania is still ongoing and focuses on the implementation of these acts.

The section on Poland discussed the existing legal framework, primarily the 2007 Crisis Management Act and the National Programme for the Protection of Critical Infrastructure (NPOIK). The high level of formalisation, transparency of responsibilities and involvement of both public and private authorities in CI protection were

highlighted. In the case of Lithuania, the 2002 Act on the Protection of Objects of Importance to National Security and subsequent implementing acts are characterised, emphasising their fragmentation, lack of consistency and the dominance of ownership and cybersecurity aspects.

The study used the following methods: dogmatic-legal, historical-legal, comparative law, and document and content analysis. The sources of the analysis were normative acts and strategic documents in force in Poland, Lithuania, the EU and NATO. The summary points to the need for further harmonisation and closer Polish-Lithuanian cooperation in the field of CI protection as a prerequisite for increasing the resilience of both countries to the threats of the modern world.

Keywords: critical infrastructure, national security, Poland, Lithuania, protection of strategic facilities

1. Wstęp

Dynamicznie zmieniające się uwarunkowania geopolityczne, agresywna polityka zagraniczna Rosji, szantaż energetyczny, tragiczna w skutkach wojna na Ukrainie, a także próby destabilizacji poszczególnych państw coraz częściej prowadzą do debaty nad nowymi wyzwaniami dla ich bezpieczeństwa. Zagadnienia te w sposób szczególny dotyczą zarówno Polski, jak i Litwy, które muszą bronić się przed wymierzonymi w nie atakami hybrydowymi ze strony Rosji i Białorusi. Co istotne, w ramach tej wojny hybrydowej coraz częściej wykorzystywane są działania o charakterze asymetrycznym. Ich skrajnie niebezpiecznym przykładem są stosunkowo niedawne przypisywane rosyjskim służbom wywiadowczym podpalenia szeregu obiektów, m.in. na terenie Polski i Litwy. Te incydenty prowokują z kolei pytanie o bezpieczeństwo IK[1] przed tego rodzaju działaniami dywersyjnymi.

[1] IK stanowi jeden z sektorów bezpieczeństwa narodowego (Biuro Bezpieczeństwa Narodowego, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, s. 19, https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf (dostęp: 12.06.2025)). Tworzą ją rzeczywiste i cybernetyczne systemy (a w tych systemach obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa. IK pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli (A. Lasota-Jędrzak, *Bezpieczeństwo infrastruktury krytycznej państwa*, „Rocznik Bezpieczeństwa Morskiego" 2013, nr 3, s. 19).

Celem niniejszego opracowania jest dokonanie analizy prawnoporównaczej wybranych norm prawnych obowiązujących w porządkach prawnych Polski i Litwy oraz przyjętych na ich podstawie dokumentów strategicznych, których celem jest zapewnienie ochrony IK obu państw. Cel badawczy zdeterminował zakres podejmowanych rozważań, w ramach których zrezygnowano z analizy problematyki cyberbezpieczeństwa IK, ze względu na specyfikę tego zagadnienia implikującą konieczność odrębnej, kompleksowej analizy w tym przedmiocie. Znajduje to swoje uzasadnienie w przyjętych zarówno w Polsce, jak i na Litwie odrębnych aktach prawnych regulujących ów wymiar bezpieczeństwa IK.

Sformułowano przy tym następujące tezy badawcze:

1. zarówno w przypadku Polski, jak i Litwy dostrzegalna jest zbliżona geneza problematyki ochrony IK zarówno na gruncie normatywnym, jak i strategicznym, wynikająca ze wspólnych doświadczeń, w szczególności na tle członkostwa w NATO i Unii Europejskiej;
2. ochronę IK w Polsce i na Litwie cechują podobieństwa dotyczące przede wszystkim podejścia sektorowego, ograniczeń w zakresie dysponowania obiektami tworzącymi IK, jak też obowiązków ochrony tych obiektów spoczywających na ich właścicielach oraz posiadaczach;
3. różnice pomiędzy przyjętymi w Polsce i na Litwie rozwiązaniami normatywnymi i strategicznymi z zakresu ochrony IK obu państw odnoszą się w szczególności do podmiotów odpowiedzialnych za jej ochronę, a także sposobu formułowania priorytetów, celów, wymagań oraz standardów służących zapewnieniu jej bezpieczeństwa;
4. w przeciwieństwie do przyjętych w Polsce ram prawnych dotyczących systemu ochrony IK rozwiązania litewskie w tym zakresie cechuje znaczny chaos legislacyjny i brak ujednoliconych zasad dotyczących minimalnych standardów bezpieczeństwa obiektów tworzących IK.

Dla celów podejmowanych rozważań posłużono się przede wszystkim metodą dogmatycznoprawną, dzięki której możliwe było ustalenie, jakie normy prawne są obowiązujące zarówno w polskim, jak i litewskim porządku prawnym. Dzięki analizie przepisów poszczególnych aktów prawnych zbadano, jak ukształtowana jest ochrona IK w Polsce i na Litwie. Istotne znaczenie miała przy tym metoda historycznoprawna, w oparciu o którą przedstawiono genezę wskazanych polskich oraz litewskich

norm prawnych i rozwiązań strategicznych. Z kolei przy wykorzystaniu metody prawnoporównawczej zwrócono uwagę na podobieństwa i różnice w tym zakresie w odniesieniu do obu państw. Kluczowe kryteria porównawcze dobrane dla potrzeb podejmowanych rozważań objęły porównanie analogicznych tekstów i instytucji prawnych przyjętych w porządkach normatywnych Polski i Litwy.

W konsekwencji zastosowana metoda umożliwiła z jednej strony przedstawienie różnic w dziedzinie ochrony IK w obu państwach, wynikających po części z ich odmiennej genezy w sensie prawnym. Z drugiej strony pozwoliła ona zwrócić uwagę na stopniowe zbliżanie analizowanych rozwiązań przyjmowanych w Polsce i na Litwie, co stanowi po części konsekwencję harmonizowania badanych przepisów z ustawodawstwem UE.

Posiłkowo posłużono się metodami analizy dokumentów i analizy treści, poprzez które uwzględniono w toku podejmowanych rozważań postanowienia kluczowych przyjętych w Polsce oraz na Litwie dokumentów strategicznych z zakresu bezpieczeństwa IK obu państw. W efekcie przeprowadzono analizę ich najważniejszych założeń odnoszących się w szczególności do metod identyfikowania obiektów tworzących IK, a także obowiązków nakładanych na ich właścicieli lub posiadaczy – lub też braku jasnych bądź wystarczająco uszczegółowionych rozwiązań w tym zakresie.

2. Ochrona infrastruktury krytycznej – rys historyczny

Pojęciem IK zaczęto się posługiwać w latach 90. XX wieku w Stanach Zjednoczonych i Kanadzie[2]. Określenie to po raz pierwszy pojawiło się wprawdzie już w 1989 roku w raporcie Charlesa Lane'a przygotowanym dla Komitetu Spraw Rządowych Senatu Stanów Zjednoczonych dotyczącym kwestii infrastrukturalnych niezbędnych

[2] J. Sadowski, *Ochrona infrastruktury krytycznej. Geneza problemu*, „Autobusy – Technika, Eksploatacja, Systemy Transportowe" 2018, nr 6, s. 1238; B. Cichoń, *System zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego*, [w:] *I Międzynarodowa konferencja naukowa. Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, badań i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007, s. 28.

do przeanalizowania pod względem bezpieczeństwa[3]. Niemniej jednak dopiero tragiczne w skutkach ataki terrorystyczne z 1993 i 1995 roku stanowiły punkt zwrotny[4] i doprowadziły do upowszechnienia się przedmiotowego pojęcia. W reakcji na te zdarzenia Bill Clinton, ówczesny prezydent Stanów Zjednoczonych, podpisał prezydencką dyrektywę decyzyjną nr 39, dotyczącą polityki państwa w zakresie przeciwdziałania terroryzmowi. Jednym z jej założeń było wyznaczenie prokuratora generalnego do przewodniczenia komisji gabinetowej mającej na celu dokonanie przeglądu podatności na terroryzm obiektów rządowych w Stanach Zjednoczonych i krytycznej infrastruktury narodowej[5].

Problematyka ochrony IK stała się obszarem zainteresowania także organizacji międzynarodowych. W przypadku NATO w 2001 roku Komitet Ochrony Cywilnej

[3] Raport wskazywał na kwestie infrastrukturalne, których zbadanie było niezbędne w opinii pionierskiej agencji rządowej, Dyrekcji Ochrony Infrastruktury, prowadzącej prace mające na celu zweryfikowanie potencjalnych podatności i zagrożeń dla bezpieczeństwa państwa polegających na możliwości sparaliżowania jego kluczowych systemów. W samym raporcie posłużono się sformułowaniem: „W styczniu 1986 r. NSC [National Security Council – Rada Bezpieczeństwa Narodowego] wydała NSDD 207 [National Security Decision Directive – Dyrektywa dot. Decyzji ws. Bezpieczeństwa Narodowego], który polecił FEMA [Federal Emergency Management Agency – Federalna Agencja Zarządzania Kryzysowego], pod auspicjami Międzyresortowej Grupy ds. Terroryzmu, określenie stopnia, w jakim różne elementy IK (np. skomputeryzowany system bankowy, sieci energetyczne i sieci komunikacyjne) są podatne na terroryzm, oraz zaproponowanie rozwiązań krótkoterminowych i długoterminowych". K.A. Brown, *Critical Path. A Brief History of Critical Infrastructure Protection in the United States*, Fairfax 2006, s. 71, https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf (dostęp: 12.06.2025).

[4] W dniu 26 lutego 1993 r. grupa terrorystów pod przewodnictwem Ramzi Yousefa doprowadziła do eksplozji wypełnionej materiałami wybuchowymi ciężarówki na podziemnym parkingu World Trade Center. Cel ataku terrorystycznego, jakim było spowodowanie zawalenia się jednej z dwóch wież drapacza chmur na drugą, nie został wprawdzie osiągnięty, lecz wybuch doprowadził do śmierci 6 osób, a ponad 1000 zostało rannych (FBI, *World Trade Center Bombing 1993*, https://www.fbi.gov/history/famous-cases/world-trade-center-bombing-1993 (dostęp: 12.06.2025). Dwa lata później, 19 kwietnia 1995 r., celem podobnego ataku był budynek rządowy położony na przedmieściach Oklahomy. Także w tym przypadku nastąpiła eksplozja ciężarówki wypełnionej materiałami wybuchowymi. Liczba ofiar śmiertelnych była jeszcze bardziej druzgocąca: 168 osób straciło życie, w tym 19 dzieci, a kilkaset zostało rannych (FBI, *Oklahoma City Bombing*, https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing (dostęp: 12.06.2025).

[5] PDD/NSC 39. U.S. Policy on Counterterrorism, https://irp.fas.org/offdocs/pdd39.htm (dostęp: 12.06.2025).

utworzył grupę *ad hoc*, mającą za zadanie rozpoczęcie prac związanych z tematyką ochrony IK[6]. W jej ramach w 2003 roku przyjęty został dokument koncepcyjny zawierający szereg wytycznych i dobrych praktyk adresowanych do państw członkowskich[7].

W ramach UE działania na rzecz ujednolicenia zasad ochrony IK zintensyfikowały się w reakcji na zamachy terrorystyczne w Madrycie z 11 września 2004 roku[8]. W dniu 20 października 2004 roku Komisja Europejska przyjęła komunikat do Rady i Parlamentu Europejskiego pod nazwą *Ochrona infrastruktury strategicznej w walce z terroryzmem*[9], zawierający propozycje przeciwdziałania przez państwa członkowskie atakom terrorystycznym wymierzonym w ich IK. Istotne znaczenie miała także dyrektywa Rady z 8 grudnia 2008 roku, która ustanowiła procedurę identyfikacji i wyznaczania EIK oraz wprowadziła wspólne podejście do oceny potrzeby poprawy jej ochrony[10].

Kolejny etap stanowiło przyjęcie w 2022 roku zalecenia Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności IK[11]. Dokument wskazywał szereg rekomendowanych działań ukierunkowanych na wzmocnienie reagowania na zagrożenia dla IK i zacieśnienie międzynarodowej współpracy w tym obszarze. Niemniej jednak za kluczowy akt prawny w dziedzinie ochrony IK

6 P. Soloch, *NATO a ochrona infrastruktury krytycznej*, [w:] *Przyszłość NATO: konferencja Biura Bezpieczeństwa Narodowego pod Honorowym Patronatem Prezydenta RP Lecha Kaczyńskiego 30 marca 2007 roku*, red. M. Biernat, K. Hołdak, M. Wolańska, Warszawa 2007, s. 78, https://www.bbn.gov.pl/download/1/1030/NATOaochronainfrastrukturykrytycznej.pdf (dostęp: 12.06.2025).

7 NATO Parliamentary Assembly, *The protection of critical infrastructures. Special report by Lord Jopling (United Kingdom) Special Rapporteur 162 CDS 07 E rev 1 Original: English*, s. 12, https://www.nato-pa.int/sites/default/files/documents/2007|-|162|CDS|07|E|REV1||-|CRITICAL|INFRASTRUCTURES|-|JOPLING|REPORT.doc (dostęp: 12.06.2025).

8 J. Sadowski, op. cit., s. 1238.

9 Komisja Wspólnot Europejskich, Komunikat Komisji do Rady i Parlamentu Europejskiego „Ochrona infrastruktury strategicznej w walce z terroryzmem", COM(2004) 702 końcowy.

10 Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (L 345/75, Dz.U. L 345 z 23.12.2008, s. 75–82), dalej „dyrektywa EIK".

11 Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (Tekst mający znaczenie dla EOG) 2023/C 20/01 (Dz.U. C 20 z 20.1.2023, s. 1–11).

w ramach Unii Europejskiej należy uznać przyjętą w 2023 roku dyrektywę Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych (tzw. dyrektywa CER od ang. *The Critical Entities Resilience (CER) Directive*)[12]. Wskazany dokument wyznacza obszerne ramy prawne dotyczące obowiązków państw członkowskich w zakresie zapewnienia bezpieczeństwa i ciągłości działania obiektów zaliczanych do IK.

Przedstawione dokumenty strategiczne i akty prawne przyjęte w ramach organizacji międzynarodowych wywarły znaczący wpływ na kształtowanie się polskich oraz litewskich rozwiązań w zakresie ochrony IK. To z kolei było powiązane ze współpracą Polski i Litwy w dziedzinie bezpieczeństwa w ramach NATO, a także akcesją obu państw do UE w dniu 1 maja 2004 roku[13]. W literaturze przedmiotu wskazuje się, że w przypadku Polski „termin »infrastruktura krytyczna« pojawił się w 2002 roku w związku z pracami prowadzonymi w ramach NATO"[14]. Z kolei w późniejszym czasie, tj. po polskiej akcesji do UE, dodatkowo konieczność integracji krajowej infrastruktury z infrastrukturą innych państw członkowskich stawała się nieodzowna, co znalazło odzwierciedlenie w polityce bezpieczeństwa narodowego oraz w prawodawstwie dotyczącym bezpośrednio ochrony tej infrastruktury[15].

Należy przy tym podkreślić znaczenie zwłaszcza drugiego ze wskazanych czynników, tj. harmonizacji porządku prawnego w Polsce z prawem unijnym. Krajowe normy prawne dotyczące analizowanej problematyki były ubogie, a liczne próby usunięcia

[12] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Tekst mający znaczenie dla EOG) (Dz.U. L 333 z 27.12.2022, s. 164–198), dalej „dyrektywa CER".

[13] Sejm V kadencji, *Projekt ustawy o zarządzaniu kryzysowym wraz z projektami aktów wykonawczych. Druk nr 770*, s. 6, https://orka.sejm.gov.pl/Druki5ka.nsf/0/E28F307439E06431C12571A9003E506D/$file/770.pdf (dostęp: 12.06.2025); B. Cichoń, op. cit., s. 28; R. Vilpišauskas, *Lithuania: regulatory patchwork that evolved in response to external threats, legal approximation and domestic influences*, [w:] *Critical infrastructure in the Baltic States and Norway: strategies and practices of protection and communication*, red. M. Andžāns, A. Sprūds, U. Sverdrup, Riga 2021, s. 61, https://www.liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1 (dostęp: 12.06.2025).

[14] R. Radziejewski, *Ochrona infrastruktury krytycznej. Teoria a praktyka*, Warszawa 2014, s. 51.

[15] Ibidem.

luki legislacyjnej w tym obszarze podejmowane od 1997 roku kończyły się fiaskiem aż do uchwalenia ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym[16], która wprowadzała ramy prawne ochrony IK zbliżone do wynikających z późniejszej dyrektywy EIK[17].

Sytuacja przedstawiała się odmiennie na Litwie, w której porządku prawnym od 2002 roku obowiązywał już akt prawny dotyczący ochrony IK[18] w postaci ustawy z dnia 10 października 2002 roku o przedsiębiorstwach i obiektach o znaczeniu strategicznym dla bezpieczeństwa narodowego oraz innych przedsiębiorstwach mających istotne znaczenie dla zapewnienia bezpieczeństwa narodowego[19]. Jak zaznacza Marie Becker, choć wynikające ze wskazanego aktu prawnego koncepcje nie są zharmonizowane z przyjętymi w prawodawstwie unijnym, to koncentrowanie się na obiektach tworzących IK jest bliskie modelowi wynikającemu z dyrektywy EIK[20].

Implementacja wskazanej dyrektywy przez Polskę i Litwę częściowo zbliżyła krajowe normy prawne obu państw w dziedzinie ochrony ich IK. Należy przy tym zaznaczyć, że proces harmonizacji polskich oraz litewskich rozwiązań w przedmiotowej dziedzinie w dalszym ciągu trwa, w szczególności poprzez podejmowane obecnie przez oba państwa działania zmierzające do stopniowego implementowania dyrektywy CER.

16 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. 2023, poz. 122, z późn. zm.), dalej „u.z.k.".

17 M. Becker, *Transposing EU-Legislation on Critical Infrastructure Protection Legal Implementation Performance in the Baltic Sea Region*, "International Journal of Critical Infrastructure Protection" 2025, s. 12, https://doi.org/10.1016/j.ijcip.2025.100781 (dostęp: 13.06.2025).

18 Termin „infrastruktura krytyczna" nie pojawia się we wskazanym akcie prawnym, lecz należy przyjąć, że dotyczy on tożsamej materii, z uwagi na posłużenie się opisowym synonimicznym określeniem.

19 Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas, 2002 m. spalio 10 d. Nr. IX-1132 (Valstybės žinios, 2002–10-30, Nr. 103–4604), dalej „ustawa nr IX-1132"; wersja w j. ang.: Lietuvos Respublikos Seimas, Law on enterprises and facilities of strategic importance to national security and other enterprises important to ensuring national security, Nr. IX-1132, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.315269?jfwid=-e29oif1nt (dostęp: 13.06.2025).

20 M. Becker, op. cit., s. 12.

3. Ochrona infrastruktury krytycznej w Polsce

Problematyka ochrony polskiej IK znalazła swój wyraz w akcie rangi ustawowej dopiero w 2007 roku wraz z wejściem w życie u.z.k., będącej jednocześnie podstawowym aktem prawnym w tej dziedzinie. W art. 2 pkt 2 przywołanej ustawy sformułowano definicję, zgodnie z którą IK tworzą systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[21].

Dodatkowo na podstawie art. 1 pkt 1 lit. b ustawy z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym[22] do art. 3 u.z.k. dodany został pkt 2a, w którym sformułowano definicję EIK[23], co stanowiło element implementacji dyrektywy EIK do polskiego porządku normatywnego. W ustawie zdefiniowano także pojęcie „ochrony infrastruktury krytycznej" i wskazano, że są to „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie" (w art. 3 pkt 3 u.z.k.).

---

21 Jednocześnie w cytowanym przepisie wskazano, że obejmuje ona systemy: a) zaopatrzenia w energię, surowce energetyczne i paliwa, b) łączności, c) sieci teleinformatycznych, d) finansowe, e) zaopatrzenia w żywność, f) zaopatrzenia w wodę, g) ochrony zdrowia, h) transportowe, i) ratownicze, j) zapewniające ciągłość działania administracji publicznej, k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

22 Ustawa z dnia 29 października 2010 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. 2010 nr 240, poz. 1600).

23 W rozumieniu art. 3 pkt 2a u.z.k. EIK to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach, o których mowa w pkt 2 lit. a i h, w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie.

Przedstawione postanowienia u.z.k. mają charakter wstępny i znajdują swoje doprecyzowanie przede wszystkim w NPOIK, przyjmowanym w drodze uchwały przez Radę Ministrów, którego celem jest stworzenie warunków do poprawy bezpieczeństwa IK (art. 5b ust. 1 u.z.k.). Przedmiotowy dokument jest przygotowywany przez dyrektora RCB we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za wyszczególnione w art. 3 pkt 2 u.z.k. systemy tworzące IK oraz właściwymi w sprawach bezpieczeństwa narodowego (art. 5b ust. 3 u.z.k.).

Wśród licznych postanowień przedmiotowego dokumentu zawarte zostały m.in. kryteria służące identyfikacji IK, które zostały podzielone na systemowe[24] i przekrojowe[25]. W NPOIK znalazły się także informacje dotyczące podmiotów uczestniczących w ochronie IK, w tym ministrów odpowiedzialnych za tworzące ją systemy[26]. W tym kontekście należy wskazać, że wskazani członkowie rządu uczestniczą w procesie sporządzania przez dyrektora RCB (przy zastosowaniu kryteriów zawartych w NPOIK) jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład IK z podziałem na systemy, który ma charakter niejawny (art. 5b ust. 7 pkt 1 u.z.k.).

Właściciele, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń, które zostały ujęte w wykazie, są powiadamiani o tym fakcie przez dyrektora RCB. Są oni zobligowani do ochrony IK, którą zarządzają, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony IK oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia (art. 6 ust. 5 u.z.k.). Istotne znaczenie ma przy tym rozporządzenie Rady Ministrów

[24] Kryteria systemowe charakteryzują ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do IK. Kryteria te przedstawione są dla każdego z systemów IK. RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity*, s. 13, https://www.gov.pl/attachment/b8835aaf-5e7e-4422-a8d8-f02981dfdc86 (dostęp: 13.06.2025).

[25] Kryteria przekrojowe opisują parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria przekrojowe obejmują ofiary w ludziach, skutki finansowe, konieczność ewakuacji, utratę usługi, czas odbudowy, efekt międzynarodowy, unikatowość. Ibidem.

[26] Ibidem, s. 18.

z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej[27], określające strukturę opracowywanych dokumentów, sposób ich przygotowania, niezbędnych uzgodnień, zatwierdzania i aktualizowania.

Tabela 1. Ministrowie odpowiedzialni za systemy IK w Polsce

Systemy infrastruktury krytycznej	Minister odpowiedzialny za system infrastruktury krytycznej
System zaopatrzenia w energię, surowce energetyczne i paliwa	minister właściwy do spraw aktywów państwowych minister właściwy do spraw energii minister właściwy do spraw gospodarki złożami kopalin
System łączności	minister właściwy do spraw informatyzacji minister właściwy do spraw łączności
System sieci teleinformatycznych	minister właściwy do spraw informatyzacji
System finansowy	minister właściwy do spraw budżetu minister właściwy do spraw finansów publicznych minister właściwy do spraw instytucji finansowych
System zaopatrzenia w żywność	minister właściwy do spraw rolnictwa minister właściwy do spraw rynków rolnych
System zaopatrzenia w wodę	minister właściwy do spraw gospodarki wodnej
System ochrony zdrowia	minister właściwy do spraw zdrowia
System transportowy	minister właściwy do spraw transportu minister właściwy do spraw gospodarki morskiej
System ratowniczy	minister właściwy do spraw wewnętrznych
System zapewniający ciągłość działania administracji publicznej	minister właściwy do spraw informatyzacji
System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	minister właściwy do spraw klimatu

Źródło: RCB, op. cit., s. 18.

[27] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83, poz. 542).

Należy dodatkowo zwrócić uwagę na załącznik 1 do NPOIK, tj. *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*. Dokument zawiera obszerne wytyczne dotyczące zapewnienia należytego poziomu ochrony IK, przy czym jego adresatami są zarówno podmioty stosujące różne rodzaje ochrony ze względów biznesowych, jak i takie, które po raz pierwszy zetkną się z takimi zagadnieniami. To z kolei implikuje konieczność zastosowania poziomu szczegółowości, który będzie adekwatny do wszystkich tych odbiorców.

Wypada zauważyć, że w konsekwencji – pomimo znacznej obszerności postanowień wskazanego załącznika – wiele spośród nich ma charakter wysoce ogólnikowy. Sformułowane w załączniku dobre praktyki i rekomendacje zostały podzielone na służące zapewnieniu bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego oraz prawnego, tj. sprowadzające się do działań prewencyjnych. W ostatnim z działów zawarte zostały natomiast wytyczne dotyczące formułowania planów ciągłości działań, których celem jest reagowanie na nagłe i niezależne od organizacji zdarzenia skutkujące przerwaniem realizacji kluczowych procesów.

W oparciu o przedstawione kluczowe akty prawne i dokumenty można sformułować wniosek, iż system ochrony IK w Polsce ma charakter ujednolicony, lecz jednocześnie postanowienia u.z.k. oraz NPOIK cechuje duży stopień nieprecyzyjności. Konkretyzacja standardów w zakresie zapewnienia bezpieczeństwa IK oraz ich wdrażanie w praktyce następuje w szczególności poprzez współpracę sektora publicznego i prywatnego w tym obszarze. Podstawę do tego stanowi m. in. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[28], które „określa sposób realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej […] oraz innymi organami i służbami publicznymi" (§1 RNPOIK).

[28] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. 2010 nr 83, poz. 541), dalej „RNPOIK".

Jak wskazano w §7 ust. 2 tego rozporządzenia, „współpraca w realizacji Programu polega na utrzymywaniu kontaktów pomiędzy jego uczestnikami przez konferencje, seminaria, prowadzenie forum dyskusyjnego, przygotowanie i udział w ćwiczeniach i szkoleniach oraz wymianę informacji". W efekcie istniejące ramy prawne regulujące system ochrony IK w Polsce należy uznać za wystarczające, lecz bezpieczeństwo tej infrastruktury ostatecznie zależeć będzie od ich realizacji w praktyce.

4. Ochrona infrastruktury krytycznej na Litwie

Podstawowym aktem prawnym regulującym ochronę litewskiej infrastruktury krytycznej jest ustawa nr IX-1132. W jej art. 1 ust. 1 wskazano, że celem regulacji jest „zapewnienie ochrony obiektów o istotnym znaczeniu dla bezpieczeństwa narodowego państwa, w tym przedsiębiorstw, obiektów, mienia i sektorów gospodarki oraz mienia i terenu znajdującego się w strefach ochronnych przedsiębiorstw, obiektów i mienia o istotnym znaczeniu dla bezpieczeństwa narodowego (zwanych dalej „strefami ochronnymi"), a także transakcji zarządców niezbędnej infrastruktury informatycznej przed wszystkimi czynnikami ryzyka mogącymi stanowić zagrożenie dla interesów bezpieczeństwa narodowego oraz eliminowanie przyczyn i warunków powstawania takich czynników". Niemniej jednak w cytowanej ustawie nie zdecydowano się na posłużenie się wprost pojęciem „infrastruktury krytycznej". Zamiast tego w art. 2 w ust. 4, 5, 6 sformułowano definicje wymienionych w art. 1 ust. 1 przedsiębiorstw[29], obiektów

[29] Art. 2 ust. 5 ustawy nr IX-1132 – są to przedsiębiorstwa kategorii I, II i III o istotnym znaczeniu dla bezpieczeństwa państwa, przy czym poszczególne kategorie zostały odrębnie zdefiniowane. Do kategorii I zaliczono przedsiębiorstwa państwowe, przedsiębiorstwa komunalne, spółki akcyjne i spółki z ograniczoną odpowiedzialnością wymienione w załączniku nr 1 do ustawy, które ze względu na cel lub charakter działalności mają znaczenie strategiczne dla interesów bezpieczeństwa narodowego i których akcje uprawniające do wszystkich głosów na walnym zgromadzeniu akcjonariuszy są w posiadaniu państwa, gminy lub spółki państwowej, a także przedsiębiorstwa państwowe, którym przeniesiono prawo własności akcji do ww. przedsiębiorstw (art. 2 ust. 8 ustawy nr IX-1132). Do kategorii II zaliczono spółki akcyjne lub spółki z ograniczoną odpowiedzialnością wymienione w załączniku nr 2 do ustawy, które ze względu na cel lub charakter działalności mają strategiczne znaczenie dla interesów bezpieczeństwa państwa i których akcje uprawniające do co najmniej 2/3 głosów na walnym zgromadzeniu akcjonariuszy są w posiadaniu Skarbu Państwa, gminy lub spółki Skarbu Państwa, a także spółki Skarbu Państwa, którym przeniesiono prawo własności akcji należących do Skarbu Państwa w ww. przedsiębiorstwie (art. 2 ust. 1 ustawy nr IX-1132). Do kategorii III zaliczono

i mienia[30] oraz sektorów gospodarki[31] o istotnym znaczeniu dla bezpieczeństwa narodowego. Ich skonkretyzowanie nastąpiło w załącznikach 1–4 do ustawy nr IX-1132 poprzez wymienienie konkretnych przedsiębiorstw, obiektów i mienia[32]. Stanowi to znaczącą różnicę w porównaniu do rozwiązania przyjętego w Polsce, polegającego na umieszczaniu obiektów, instalacji, urządzeń i usług wchodzących w skład polskiej IK w niejawnym wykazie, choć należy zaznaczyć, że wyszczególnienie zawarte w zał. 1–4 do ustawy nr IX-1132 jest ograniczone wyłącznie do nazw lub przedmiotów działalności poszczególnych instytucji, sektorów gospodarki itd.

Ponadto istotne znaczenie dla identyfikacji litewskiej IK ma nowsza regulacja w postaci rezolucji z dnia 5 grudnia 2018 roku w sprawie zmiany rezolucji Rządu Republiki Litewskiej z dnia 13 sierpnia 2018 roku nr 818 „w sprawie zatwierdzenia narodowej strategii cyberbezpieczeństwa”[33]. W dokumencie sformułowano metodologię służącą

spółki akcyjne lub spółki z ograniczoną odpowiedzialnością określone w załączniku nr 3 do ustawy, które ze względu na przedmiot działalności lub charakter działalności mają znaczenie strategiczne dla interesów bezpieczeństwa państwa, a których akcje uprawniające do mniej niż 2/3 głosów na walnym zgromadzeniu akcjonariuszy są w posiadaniu Skarbu Państwa, gminy lub spółki Skarbu Państwa albo nie są w posiadaniu osób prawnych określonych w niniejszym paragrafie (art. 2 ust. 12 ustawy nr IX-1132).

30 Art. 2 ust. 6 ustawy nr IX-1132 – są to projektowane obiekty będące w trakcie budowy oraz istniejące obiekty i mienie określone w załączniku nr 4 do niniejszej ustawy, które zgodnie z przepisami niniejszej ustawy muszą być chronione przed wszystkimi czynnikami ryzyka mogącymi stanowić zagrożenie dla interesów bezpieczeństwa narodowego.

31 Art. 2 ust. 4 ustawy nr IX-1132 – są to obszary działalności o szczególnym znaczeniu narodowym i społecznym dla Republiki Litewskiej, których rozwój, gdyby został przerwany, zakłócony, ograniczony lub zaniechany, mógłby zaszkodzić interesom bezpieczeństwa narodowego.

32 Np. zgodnie z zał. 1 do przedsiębiorstw kategorii I (art. 2 ust. 8 ustawy nr IX-1132) zaliczono m.in. przedsiębiorstwo odpowiedzialne za zarządzanie państwowym portem morskim w Kłajpedzie, przedsiębiorstwo zajmujące się zarządzaniem międzynarodowymi portami lotniczymi w Wilnie, Kownie i Połądze czy też przedsiębiorstwo zajmujące się świadczeniem usług cywilnego transportu lotniczego na lotnisku wojskowym w Szawlach.

33 Lietuvos Respublikos Vyriausybė nutarimas dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo nr. 818 „dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo” pakeitimo, 2018 m gruodžio 5 d. Nr. 1209 (TAR, 2018–12-10, Nr. 20153), https://e-seimasx.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce?jfwid=54ivtoy05 (dostęp: 13.06.2025), dalej „rezolucja nr 1209”.

identyfikacji informacyjnej IK[34], a zarazem definicję wskazanego pojęcia, zgodnie z którą są to obiekty infrastrukturalne świadczące usługi o krytycznym znaczeniu (art. 2.7 Metodologii), tj. takie, których awaria lub wadliwe działanie mogłoby mieć istotny negatywny wpływ na bezpieczeństwo narodowe, gospodarkę kraju lub interesy państwa albo społeczeństwa (art. 2.8 Metodologii).

Pomimo swojej nazwy Metodologia w rzeczywistości reguluje dwie procedury, z których pierwsza służy rozpoznaniu obiektów tworzących IK (Rozdział II Metodologii – identyfikacja obiektów infrastrukturalnych o znaczeniu krytycznym), a druga odnosi się do obiektów tworzących informacyjną IK (Rozdział III Metodologii – identyfikacja krytycznej infrastruktury informacyjnej). Kryteria i schemat działań służących do identyfikacji IK zostały sformułowane w art. 6–7 Metodologii. Zadania w tym zakresie wykonują właściwe organy odpowiedzialne za poszczególne sektory i podsektory IK, zgodnie z załącznikiem nr 1 do Metodologii.

Ministerstwa odpowiedzialne za sektory IK na Litwie[35]

1. Sektor energetyczny – Ministerstwo Energetyki Republiki Litewskiej
   - **1.1.** Podsektor energetyczny
   - **1.2.** Podsektor ropy naftowej i produktów naftowych
   - **1.3.** Podsektor gazu ziemnego
   - **1.4.** Podsektor ciepłownictwa
2. Sektor transportu i poczty – Ministerstwo Transportu i Komunikacji Republiki Litewskiej
   - **2.1.** Podsektor transportu lotniczego
   - **2.2.** Podsektor transportu kolejowego
   - **2.3.** Podsektor transportu wodnego
   - **2.4.** Podsektor transportu drogowego
   - **2.5.** Podsektor pocztowy
3. Sektor finansowy – Ministerstwo Finansów Republiki Litewskiej
   - **3.1.** 3.1. Podsektor instytucji kredytowych
   - **3.2.** 3.2. Podsektor infrastruktury rynku finansowego

[34] Metodologia identyfikacji informacyjnej infrastruktury krytycznej stanowi załącznik do rezolucji nr 1209, dalej „Metodologia".

[35] Rezolucja nr 1209, załącznik nr 1.

4. Sektor opieki zdrowotnej – Ministerstwo Zdrowia Republiki Litewskiej
   - 4.1. Podsektor infrastruktury ochrony zdrowia
5. Sektor zaopatrzenia, dystrybucji i uzdatniania wody pitnej – Ministerstwo Środowiska Republiki Litewskiej
   - 5.1. Podsektor wody pitnej
   - 5.2. Podsektor ścieków
6. Sektor technologii informacyjnych i komunikacji elektronicznej
   - 6.1. Podsektor infrastruktury cyfrowej – Ministerstwo Gospodarki Republiki Litewskiej[36], Ministerstwo Spraw Wewnętrznych Republiki Litewskiej[37]
   - 6.2. Podsektor łączności elektronicznej – Ministerstwo Transportu i Komunikacji Republiki Litewskiej
   - 6.3. Podsektor technologii informatycznych – Ministerstwo Gospodarki Republiki Litewskiej
7. Sektor środowiskowy – Ministerstwo Środowiska Republiki Litewskiej
   - 7.1. Podsektor monitoringu zanieczyszczenia powietrza i meteorologii
   - 7.2. Podsektor monitoringu wód powierzchniowych i morskich
   - 7.3. Podsektor leśny
8. Sektor obrony cywilnej – Ministerstwo Spraw Wewnętrznych Republiki Litewskiej
   - 8.1. Podsektor zarządzania kryzysowego
9. Sektor obrony narodowej – Ministerstwo Obrony Narodowej Republiki Litewskiej
   - 9.1. Podsektor obrony narodowej
10. Sektor spożywczy – Ministerstwo Rolnictwa Republiki Litewskiej
    - 10.1. Podsektor zaopatrzenia i dystrybucji żywności
11. Sektor przemysłowy – Ministerstwo Gospodarki Republiki Litewskiej, Ministerstwo Środowiska Republiki Litewskiej, Ministerstwo Energetyki Republiki Litewskiej
    - 11.1. Podsektor przemysłu chemicznego, jądrowego i innych branż o wyższym ryzyku
    - 11.2. Podsektor przemysłu obronnego
12. Sektor polityki zagranicznej i bezpieczeństwa – Ministerstwo Spraw Zagranicznych Republiki Litewskiej
    - 12.1. Podsektor wdrażania polityki zagranicznej i bezpieczeństwa

[36] Odpowiedzialne za usługi ruchu internetowego i usługi domenowe.
[37] Odpowiedzialne za usługi identyfikacji elektronicznej.

13. Sektor administracji publicznej – Rząd Republiki Litewskiej[38], Ministerstwo Gospodarki Republiki Litewskiej[39]
13.1. Podsektor rządu stanowego
14. Sektor bezpieczeństwa publicznego i porządku publicznego – Ministerstwo Spraw Wewnętrznych Republiki Litewskiej[40], Ministerstwo Sprawiedliwości Republiki Litewskiej[41]
14.1. Podsektor bezpieczeństwa publicznego i egzekwowania praw

To one zwracają się do zarządców instytucji, przedsiębiorstw, obiektów infrastrukturalnych z wnioskiem o przeprowadzenie oceny znaczenia tych podmiotów zgodnie z kwestionariuszem stanowiącym załącznik nr 2 do Metodologii. Na jego podstawie dla każdego ocenianego podmiotu ustalana jest liczba punktów będąca odzwierciedleniem negatywnego wpływu zakłócenia jego działalności dla bezpieczeństwa państwa. Obiekty, które w wyniku tak przeprowadzanej oceny uzyskały co najmniej 16 punktów, są uznawane za obiekty infrastruktury o znaczeniu krytycznym. Identyfikacja krytycznej infrastruktury informacyjnej następuje w tożsamy sposób opisany w art. 8 Metodologii przy wykorzystaniu kwestionariusza stanowiącego załącznik nr 3.

Należy zaznaczyć, że postanowienia ustawy nr IX-1132 i Metodologii ustanawiają *de facto* odrębne i niezależne od siebie ramy służące identyfikacji litewskiej IK. W konsekwencji w literaturze przedmiotu zwraca się uwagę na wysoki stopień skomplikowania kryteriów determinujących to, które obiekty, przedsiębiorstwa, sektory gospodarki stanowią IK[42]. Co więcej, postanowienia ustawy nr IX-1132 w dużej mierze dotyczą metodologii oceny funkcjonowania przedsiębiorstw, ich obiektów i majątku w zakresie inwestycji, transferów i innych transakcji pod kątem ich znaczenia dla bezpieczeństwa narodowego kraju[43].

38 Odpowiedzialny za usługę wykonywania funkcji administracji państwowej.
39 Odpowiedzialne za usługę zarządzania lub przetwarzania zasobów informacyjnych o szczególnym znaczeniu.
40 Odpowiedzialne za służbę bezpieczeństwa publicznego.
41 Odpowiedzialne za funkcjonowania systemu sądowniczego i karnego.
42 R. Vilpišauskas, op. cit., s. 88.
43 Ibidem, s. 87.

Jakkolwiek kwestie związane z bezpieczeństwem fizycznym, cybernetycznym, personelu oraz informacji również znajdują swoje uregulowanie w przywołanym akcie prawnym[44], to można je ocenić jako drugorzędne względem ww. zagadnień o charakterze właścicielsko-finansowym[45]. Świadczy o tym także fakt, że konkretne wymagania w zakresie ochrony litewskiej IK, odnoszące się do jej poszczególnych sektorów, są rozrzucone pomiędzy rozmaite akty prawne i nie mają charakteru kompleksowego, jak w przypadku polskiego NPOIK.

Przykładem są zarządzenie z dnia 15 stycznia 2019 roku w sprawie zatwierdzenia wymogów dotyczących bezpieczeństwa fizycznego i operacyjnego przedsiębiorstw energetycznych o znaczeniu strategicznym lub istotnym dla bezpieczeństwa narodowego oraz infrastruktury energetycznej o znaczeniu strategicznym lub istotnym

44 W szczególności: art. 15 ustawy nr IX-1132, dotyczący minimalnych wymagań, procedury opracowywania i kontrolowania planów bezpieczeństwa w przedsiębiorstwach o znaczeniu krytycznym dla bezpieczeństwa państwa; art. 17 ustawy nr IX-1132, stanowiący delegację ustawową dla rządu i upoważnionych przez rząd instytucji do ustalenia wymagań dla pracowników i osób ubiegających się o zatrudnienie w przedsiębiorstwach o znaczeniu krytycznym dla bezpieczeństwa państwa; art. 19 ustawy nr IX-1132, stanowiący delegację ustawową dla rządu i upoważnionych przez rząd instytucji do ustalenia wymagań dotyczących bezpieczeństwa fizycznego, operacyjnego i/lub cyberbezpieczeństwa przedsiębiorstw o krytycznym znaczeniu dla bezpieczeństwa narodowego oraz obiektów i mienia o krytycznym znaczeniu dla bezpieczeństwa narodowego w zakresie, w jakim wymagania te nie są uregulowane w ustawie Republiki Litewskiej o cyberbezpieczeństwie.

45 Ustawa nr IX-1132 zawiera obszerne postanowienia dotyczące ograniczeń w zakresie reorganizacji, przekształcania, restrukturyzacji lub likwidacji przedsiębiorstw o kluczowym znaczeniu dla bezpieczeństwa państwa (art. 7–9 ustawy nr IX-1132). W zależności od kategorii, do której zaliczane jest przedsiębiorstwo, warunkiem może być uprzednia zgoda sejmu lub komisji do spraw koordynacji ochrony obiektów ważnych dla zapewnienia bezpieczeństwa narodowego. W przypadku Polski zbliżone rozwiązania stanowią uprawnienia przysługujące ministrowi aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej (ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, t.j. Dz.U. z 2025 r. poz. 470).

dla bezpieczeństwa narodowego[46] czy też zarządzenie z dnia 11 września 2019 roku w sprawie realizacji ustawy o ochronie obiektów ważnych dla zapewnienia bezpieczeństwa narodowego Republiki Litewskiej w przedsiębiorstwach ważnych dla zapewnienia bezpieczeństwa narodowego przypisane do właściwości Ministerstwa Finansów Republiki Litewskiej[47]. Z kolei rezolucja nr 1209, mimo że wprowadza Metodologię, służącą identyfikacji obiektów tworzących IK (nie tylko informacyjną), to w pozostałym zakresie ustanawia wymogi organizacyjne i techniczne wyłącznie z zakresu cyberbezpieczeństwa, przy jednoczesnym pominięciu tych odnoszących się do bezpieczeństwa fizycznego.

Na uwagę zasługuje także rola komisji do spraw koordynacji ochrony obiektów ważnych dla zapewnienia bezpieczeństwa narodowego, której podstawą funkcjonowania jest art. 19 ustawy nr IX-1132. Jak wynika z ust. 2 wskazanego przepisu, przedmiotowy organ posiada kompetencje dotyczące m. in. kontroli zgodności struktury właścicielskiej i inwestycji dotyczących obiektów o istotnym znaczeniu dla bezpieczeństwa narodowego Litwy, formułowania na wniosek sejmu lub rządu rekomendacji w sprawie wskazanych obiektów i ich ochrony, przedstawiania informacji, opinii, wniosków i zaleceń oraz egzekwowania obowiązków wobec inwestorów i przedsiębiorstw o istotnym znaczeniu dla bezpieczeństwa państwa, kontrahentów lub osób trzecich dotyczące innych działań niezbędnych do zapewnienia interesów bezpieczeństwa państwa w związku z ochroną obiektów o istotnym znaczeniu dla bezpieczeństwa państwa.

Tym samym poprzez analizę treści art. 19 ust. 2 ustawy nr IX-1132 można wstępnie sformułować wniosek o kluczowej roli tej komisji w obszarze bezpieczeństwa litewskiej IK. Niemniej jednak refleksję należy dodatkowo zweryfikować

[46] Įsakymas dėl nacionaliniam saugumui užtikrinti svarbių energetikos įmonių ir nacionaliniam saugumui užtikrinti strateginę ar svarbią reikšmę turinčios energetikos infrastruktūros fizinės ir veiklos apsaugos reikalavimų patvirtinimo, 2019 m. sausio 15 d. Nr. 1–9 (TAR, 2019–01-17, Nr. 734), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3e560ea01a9411e9bd28d9a28a9e9ad9?jfwid=mw3a6whi4 (dostęp: 13.06.2025).

[47] Įsakymas dėl Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo įgyvendinimo Lietuvos Respublikos Finansų Ministerijos reguliavimo sričiai priskirtose nacionaliniam saugumui užtikrinti svarbiose įmonėse, 2019 m. rugsėjo 11 d. Nr. 1K-267 (TAR, 2019–09-20, Nr. 14910), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/9b43fbd2dbdd11e9a85be81119c7a8fa?jfwid=fhhu5mp5n (dostęp: 13.06.2025).

z uwzględnieniem rezolucji rządu z dnia 25 listopada 2009 roku w sprawie zatwierdzenia procedury komisji do spraw koordynacji ochrony obiektów ważnych dla zapewnienia bezpieczeństwa narodowego[48].

Przeważająca część postanowień przedmiotowego dokumentu dotyczy kwestii związanych ze strukturą właścicielką oraz inwestycjami dotyczącymi obiektów o istotnym znaczeniu dla bezpieczeństwa państwa. Wprawdzie art. 75 rezolucji nr 1540 reguluje postępowanie komisji w sytuacji otrzymania wniosku od rządu, Sejmu Republiki Litewskiej lub innego podmiotu o przedstawienie zaleceń, informacji, opinii, wniosków lub decyzji określonych w art. 19 ust. 2 pkt 2–5, 7 i 9–11 ustawy nr IX-1132[49]. Niemniej jednak kompetencje przedmiotowego organu w tym zakresie mają charakter marginalny w porównaniu do tych związanych z weryfikowaniem zgodności z litewskim bezpieczeństwem narodowym wszelkich inwestycji, transferów i innych transakcji dotyczących obiektów o istotnym znaczeniu dla bezpieczeństwa państwa.

Stanowi to jednocześnie przykład dostrzegalnej na Litwie tendencji do nader restrykcyjnego regulowania decyzji biznesowych przedsiębiorstw, nierzadko arbitralnie uznawanych za mające istotne znaczenie dla funkcjonowania państwa[50]. Pozostaje to w wyraźnym kontraście do znacznego chaosu legislacyjnego i wysokiego stopnia skomplikowania pozostałych uregulowań odnoszących się do ochrony litewskiej IK.

48 Nutarimas dėl nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijos darbo tvarkos aprašo patvirtinimo, 2009 m. lapkričio 25 d. Nr. 1540 (Valstybės žinios, 2009–12-02, Nr. 143–6298), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.359678?jfwid=-6ebzwng8h (dostęp: 13.06.2025), dalej „Rezolucja nr 1540".

49 Tj. także w sprawach związanych z przedstawianiem rekomendacji w zakresie wymagań dotyczących bezpieczeństwa fizycznego i ochrony działalności przedsiębiorstw mających znaczenie dla zapewnienia bezpieczeństwa narodowego lub obiektów i mienia mających znaczenie dla zapewnienia bezpieczeństwa narodowego (art. 19 ust. 2 pkt 9 ustawy nr IX-1132).

50 R. Vilpišauskas, op. cit., s. 88.

5. Podsumowanie

Analiza systemów ochrony IK w Polsce i na Litwie pozwala dostrzec podobieństwa między nimi, których źródłem są w głównej mierze wspólne doświadczenia obu państw wynikające z ich członkostwa w NATO i UE oraz stopniowego harmonizowania ich krajowych przepisów oraz rozwiązań strategicznych z przyjętymi w ramach tych organizacji międzynarodowych. Wymienić tu należy przede wszystkim podejście sektorowe przy jednoczesnym zaliczaniu zbliżonych obszarów funkcjonowania państwa do tych, które są uznawane za kluczowe z punktu widzenia jego bezpieczeństwa. To z kolei implikuje kwalifikowanie analogicznych obiektów, instytucji, przedsiębiorstw i usług jako tworzących IK zarówno w Polsce, jak i na Litwie, choć w tym drugim przypadku dostrzegalne jest znacznie szersze podejście obejmujące większość dziedzin działalności sektora publicznego i prywatnego.

Ponadto w obu państwach wyróżnić można poszczególne systemy tworzące IK, za ochronę których odpowiadają różne organy[51], co w praktyce może prowadzić do trudności na tle współpracy między nimi w tym przedmiocie. Podobieństwa dotyczą również zagadnień właścicielsko-finansowych odnoszących się do obiektów, przedsiębiorstw i instytucji zaliczanych w poczet IK. W Polsce uprawnienia, które można określić jako prawo do ingerowania w przemiany na tle organizacyjnym w tego rodzaju podmiotach, przysługują ministrowi aktywów państwowych. Z kolei na Litwie działania takie jak przeniesienie akcji, reorganizacja, przekształcanie, restrukturyzacja lub likwidacja przedsiębiorstw zaliczanych do mających kluczowe znaczenie dla bezpieczeństwa państwa może wymagać akceptacji sejmu lub komisji do spraw koordynacji ochrony obiektów ważnych dla zapewnienia bezpieczeństwa narodowego.

[51] Np. w Polsce za IK w obszarze systemu łączności odpowiedzialni są minister właściwy do spraw informatyzacji oraz minister właściwy do spraw łączności, tj. minister cyfryzacji (zgodnie z rozporządzeniem Prezesa Rady Ministrów w sprawie szczegółowego zakresu działania Ministra Cyfryzacji, Dz.U. z 2023 r. poz. 2720) oraz minister aktywów państwowych (zgodnie z rozporządzeniem Prezesa Rady Ministrów w sprawie szczegółowego zakresu działania Ministra Aktywów Państwowych, Dz.U. z 2024 r. poz. 741). Na Litwie z kolei za IK w sektorze technologii informacyjnych i komunikacji elektronicznej odpowiedzialne są aż cztery ministerstwa, tj. Ministerstwo Gospodarki Republiki Litewskiej, Ministerstwo Spraw Wewnętrznych Republiki Litewskiej, Ministerstwo Transportu i Komunikacji Republiki Litewskiej i Ministerstwo Gospodarki Republiki Litewskiej.

Warto także zauważyć, że w Polsce tego rodzaju ograniczenia, wynikające z potrzeby zapewnienia bezpieczeństwa prawnego IK[52], stanowią zaledwie jeden z wielu wymiarów jej ochrony wyszczególnionych w NPOIK. Tymczasem analiza litewskich ram prawnych i rozwiązań strategicznych w tym obszarze pozwala sformułować wniosek o koncentrowaniu się na restrykcjach w zakresie decyzji biznesowych przedsiębiorstw uznawanych za istotne dla bezpieczeństwa państwa oraz formułowaniu adresowanych do nich szczegółowych wymogów z zakresu cyberbezpieczeństwa, przy jednoczesnym marginalizowaniu pozostałych wymiarów bezpieczeństwa.

Ponadto analiza systemu ochrony IK na Litwie nakazuje sformułować wniosek o chaosie legislacyjnym na tej płaszczyźnie. Normy prawne determinujące to, które obiekty są zaliczane do IK, a także jakie obowiązki spoczywają na ich właścicielach lub posiadaczach, nie mają charakteru ujednoliconego. W literaturze przedmiotu zwraca się uwagę, że stanowi to wynik stopniowego ewoluowania systemu litewskiego w odpowiedzi na pojawiające się zagrożenia i niedociągnięcia instytucjonalne, a nie na podstawie gruntownego projektu opartego na właściwej ocenie skutków[53].

Pomimo niedoskonałości ram prawnych ochrony IK na Litwie podobieństwa do tych przyjętych w Polsce pozwalają twierdzić, że istnieją podstawy do pogłębiania współpracy obu państw w tym obszarze. Wniosek ten podyktowany jest trwającymi obecnie polskimi i litewskimi pracami zmierzającymi do dalszej harmonizacji krajowych przepisów z prawem unijnym, w szczególności w kierunku implementacji dyrektywy CER.

Na uwagę zasługuje przy tym przede wszystkim procedowany w Polsce projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw[54], zakładający daleko idącą reformę systemu ochrony IK w kierunku zgodnym z wymogami stawianymi przez dyrektywę CER. Pozytywnie należy ocenić proponowaną rezygnację z NPOIK na rzecz Strategii odporności podmiotów krytycznych, która obejmie ogół kwestii związanych z ochroną IK, jak np. rozwiązania strategiczne, procesy identyfikujące IK, a także środki niezbędne do zwiększenia ogólnej odporności

52 Poświęcony jest temu rozdział 2.9 załącznika 1 do NPOIK.
53 R. Vilpišauskas, op. cit., s. 90.
54 RCB, *Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC 47)*, https://legislacja.rcl.gov.pl/projekt/12386961 (dostęp: 24.10.2025).

podmiotów krytycznych. Na szczególną uwagę zasługują natomiast projektowane art. 6ze i nast. u.z.k., które mają określać procedurę wdrażania i kontrolowania rozwiązań w zakresie ochrony IK, w tym poprzez przeprowadzane systematycznie analizy zagrożeń dla IK i wdrażane następnie, adekwatne do tych analiz, konkretne środki. Stanowi to oczekiwane uszczegółowienie i przeniesienie na grunt ustawowy dotychczasowych rozwiązań w tym przedmiocie.

W przypadku Litwy część postanowień dyrektywy CER została już zaimplementowana do krajowego porządku prawnego, m.in. na gruncie przepisów art. 49^1 i n. ustawy z dnia 15 grudnia 1998 roku o zarządzaniu kryzysowym i bezpieczeństwie cywilnym[55], niemniej jednak stanowi to kolejny przykład znacznego rozproszenia litewskich uregulowań w zakresie ochrony IK pomiędzy liczne akty prawne i dokumenty strategiczne. Tymczasem należy skonstatować, że skuteczna współpraca Polski i Litwy w dziedzinie ich bezpieczeństwa, w tym związanego z niezakłóconym funkcjonowaniem ich IK, wymaga w szczególności jasnych i przejrzystych ram prawnych, które wspomagałyby realizację już trwających oraz podejmowanie nowych inicjatyw strategicznych, a także sprawne reagowanie na ewentualne incydenty.

Bibliografia

Akty prawne

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (L 345/75, Dz.U. L 345 z 23.12.2008).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Tekst mający znaczenie dla EOG) (Dz.U. L 333 z 27.12.2022).

Komisja Wspólnot Europejskich, Komunikat Komisji do Rady i Parlamentu Europejskiego „Ochrona infrastruktury strategicznej w walce z terroryzmem", COM(2004) 702 końcowy.

Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (Tekst mający znaczenie dla EOG) 2023/C 20/01 (Dz.U. C 20 z 20.1.2023).

[55] Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymas 1998 m. gruodžio 15 d. nr. VIII-971 (Valstybės žinios, 1998-12-31, Nr. 115-3230), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.69957/vNmLhzzuMH (dostęp: 24.10.2025).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. 2023, poz. 122, z późn. zm.).
Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (t.j. Dz.U. 2025, poz. 470).
Ustawa z dnia 29 października 2010 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz.U. 2010 nr 240, poz. 1600).
Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. 2010 nr 83, poz. 541).
Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. 2010 nr 83, poz. 542).
Rozporządzenie Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz.U. 2023, poz. 2720).
Rozporządzenie Prezesa Rady Ministrów z dnia 16 maja 2024 r. w sprawie szczegółowego zakresu działania Ministra Aktywów Państwowych (Dz.U. 2024, poz. 741).
Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymas 1998 m. gruodžio 15 d. nr. VIII-971 (Valstybės žinios, 1998–12-31, Nr. 115–3230), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.69957/vNmLhzzuMH (dostęp: 24.10.2025).
Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas, 2002 m. spalio 10 d. Nr. IX-1132 (Valstybės žinios, 2002-10-30, Nr. 103-4604), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498?jfwid=136mjqgadn (dostęp: 13.06.2025).
Lietuvos Respublikos Seimas, Law on enterprises and facilities of strategic importance to national security and other enterprises important to ensuring national security, Nr. IX-1132, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.315269?jfwid=-e29oif1nt (dostęp: 13.06.2025).
Lietuvos Respublikos Vyriausybė nutarimas dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo nr. 818 „dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo" pakeitimo, 2018 m gruodžio 5 d. Nr. 1209 (TAR, 2018-12-10, Nr. 20153), https://e-seimasx.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce?jfwid=54ivtoy05 (dostęp: 13.06.2025).
Įsakymas dėl nacionaliniam saugumui užtikrinti svarbių energetikos įmonių ir nacionaliniam saugumui užtikrinti strateginę ar svarbią reikšmę turinčios energetikos infrastruktūros fizinės ir veiklos apsaugos reikalavimų patvirtinimo, 2019 m. sausio 15 d. Nr. 1–9 (TAR, 2019-01-17, Nr. 734), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3e560ea01a9411e9bd28d9a28a9e9ad9?jfwid=mw3a6whi4 (dostęp: 13.06.2025).
Įsakymas dėl Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo įgyvendinimo Lietuvos Respublikos Finansų Ministerijos reguliavimo sričiai priskirtose nacionaliniam saugumui užtikrinti svarbiose įmonėse,

2019 m. rugsėjo 11 d. Nr. 1K-267 (TAR, 2019-09-20, Nr. 14910), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/9b43fbd2dbdd11e9a85be81119c7a8fa?jfwid=fhhu5mp5n (dostęp: 13.06.2025).

Nutarimas dėl nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijos darbo tvarkos aprašo patvirtinimo, 2009 m. lapkričio 25 d. Nr. 1540 (Valstybės žinios, 2009-12-02, Nr. 143-6298), https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.359678?jfwid=-6ebzwng8h (dostęp: 13.06.2025).

Literatura

Becker Marie, *Transposing EU-Legislation on Critical Infrastructure Protection Legal Implementation Performance in the Baltic Sea Region*, "International Journal of Critical Infrastructure Protection" 2025, https://doi.org/10.1016/j.ijcip.2025.100781 (dostęp: 13.06.2025).

Brown Kathi Ann, *Critical Path. A Brief History of Critical Infrastructure Protection in the United States*, Fairfax 2006, https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf (dostęp: 12.06.2025).

Cichoń Bogusław, *System zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego*, [w:] *I Międzynarodowa konferencja naukowa. Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, badań i praktyki*, red. Bogdan Kosowski, Andrzej Włodarski, Warszawa 2007, s. 25–31.

Lasota-Jędrzak Agata, *Bezpieczeństwo infrastruktury krytycznej państwa*, „Rocznik Bezpieczeństwa Morskiego" 2013, nr 3, s. 171–182.

Radziejewski Ryszard, *Ochrona infrastruktury krytycznej. Teoria a praktyka*, Warszawa 2014.

Sadowski Józef, *Ochrona infrastruktury krytycznej. Geneza problemu*, „Autobusy – Technika, Eksploatacja, Systemy Transportowe" 2018, nr 6, s. 1237–1241.

Soloch Paweł, *NATO a ochrona infrastruktury krytycznej*, [w:] *Przyszłość NATO: konferencja Biura Bezpieczeństwa Narodowego pod Honorowym Patronatem Prezydenta RP Lecha Kaczyńskiego 30 marca 2007 roku*, red. Monika Biernat, Katarzyna Hołdak, Marta Wolańska, Warszawa 2007, s. 77–80, https://www.bbn.gov.pl/download/1/1030/NATOaochronainfrastrukturykrytycznej.pdf (dostęp: 12.06.2025).

Vilpišauskas Ramūnas, *Lithuania: Regulatory Patchwork That Evolved in Response to External Threats, Legal Approximation and Domestic Influences*, [w:] *Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication*, red. Māris Andžāns, Andris Sprūds, Ulf Sverdrup, Riga 2021, s. 59–97, https://www.liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1 (dostęp: 12.06.2025).

Źródła internetowe

Biuro Bezpieczeństwa Narodowego, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf (dostęp: 12.06.2025).

FBI, *Oklahoma City Bombing*, https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing (dostęp: 12.06.2025).

FBI, *World Trade Center Bombing 1993*, https://www.fbi.gov/history/famous-cases/world-trade-center-bombing-1993 (dostęp: 12.06.2025).

NATO Parliamentary Assembly, *The protection of critical infrastructures. Special report by Lord Jopling (United Kingdom) Special Rapporteur 162 CDS 07 E rev 1 Original: English*, https://www.nato-pa.int/sites/default/files/documents/2007|-|162|CDS|07|E|REV1||-|CRITICAL|INFRASTRUCTURES|-|JOPLING|REPORT.doc (dostęp: 12.06.2025).

PDD/NSC 39. U.S. Policy on Counterterrorism, https://irp.fas.org/offdocs/pdd39.htm (dostęp: 12.06.2025).

RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej 2023 – tekst jednolity*, https://www.gov.pl/attachment/b8835aaf-5e7e-4422-a8d8-f02981dfdc86 (dostęp: 13.06.2025).

RCB, *Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC 47)*, https://legislacja.rcl.gov.pl/projekt/12386961 (dostęp: 24.10.2025).

Sejm V kadencji, *Projekt ustawy o zarządzaniu kryzysowym wraz z projektami aktów wykonawczych. Druk nr 770*, s. 6, https://orka.sejm.gov.pl/Druki5ka.nsf/0/E28F307439E06431C12571A9003E506D/$file/770.pdf (dostęp: 24.06.2025).

Wykaz skrótów

EIK – europejska infrastruktura krytyczna
IK – infrastruktura krytyczna
NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej
RCB – Rządowe Centrum Bezpieczeństwa

STRESZCZENIE

Ewolucja i prawnoporównawcza analiza regulacji dotyczących ochrony infrastruktury krytycznej w Polsce i na Litwie

W artykule dokonano prawnoporównawczej analizy regulacji prawnych dotyczących ochrony infrastruktury krytycznej (IK) w Polsce i na Litwie, osadzając rozważania w kontekście zmieniającego się środowiska bezpieczeństwa oraz trwających procesów legislacyjnych i instytucjonalnych. Punktem wyjścia była geneza pojęcia IK i rozwój

międzynarodowych standardów ochrony, zapoczątkowanych w Stanach Zjednoczonych w latach 90. XX wieku, a następnie rozwiniętych w ramach NATO oraz Unii Europejskiej. Uwzględniono kluczowe akty, takie jak dyrektywa Rady 2008/114/WE w sprawie identyfikacji i wyznaczania europejskiej infrastruktury krytycznej (dyrektywa EIK) oraz dyrektywa Parlamentu Europejskiego i Rady 2022/2557 w sprawie odporności podmiotów krytycznych (dyrektywa CER), których wpływ na ustawodawstwa krajowe Polski i Litwy oceniono jako istotny, choć wciąż niewystarczająco ujednolicony.

W toku analizy polskiego systemu ochrony IK podkreślono jego względną spójność oraz oparcie na ustawie o zarządzaniu kryzysowym z 2007 roku i Narodowym Programie Ochrony Infrastruktury Krytycznej. Polski model charakteryzuje się jasnym podziałem kompetencji między resorty, obowiązkami właścicieli obiektów IK oraz procedurami tworzenia planów ochrony. System opiera się na współpracy sektora publicznego i prywatnego oraz klasyfikacji IK w ramach niejawnych wykazów. Zwrócono uwagę, że choć dokumenty strategiczne zawierają wiele ogólnych zaleceń, ich wartość polega na standaryzacji praktyk ochronnych.

W odniesieniu do Litwy wykazano, że system prawny jest znacznie bardziej rozproszony i złożony. Kluczową rolę odgrywa ustawa z 2002 roku o ochronie obiektów o istotnym znaczeniu dla bezpieczeństwa państwa oraz szereg aktów wykonawczych. W przeciwieństwie do Polski litewskie podejście kładzie silny nacisk na kontrolę właścicielską i inwestycyjną w odniesieniu do obiektów o znaczeniu strategicznym, często kosztem systemowego ujęcia ochrony IK w innych wymiarach. Przepisy koncentrują się także na cyberbezpieczeństwie, a pomijają spójne uregulowania dotyczące bezpieczeństwa fizycznego i organizacyjnego.

Wyniki dokonanej analizy wskazują na istnienie podobieństw strukturalnych między systemami obu państw, m.in. w podejściu sektorowym i w katalogu instytucji odpowiedzialnych za ochronę IK. Różnice dotyczą przede wszystkim poziomu formalizacji, stopnia centralizacji i kompletności rozwiązań. Polska dysponuje bardziej przejrzystym i zharmonizowanym modelem, natomiast system litewski odznacza się większą fragmentacją i tendencją do arbitralnych ograniczeń w zakresie działalności podmiotów prywatnych.

W konkluzji stwierdzono, że pomimo widocznych mankamentów w litewskich regulacjach istnieją solidne podstawy do dalszego zbliżania rozwiązań obu państw. Harmonizacja nie powinna jednak ograniczać się do formalnego wdrażania unijnych dyrektyw, lecz powinna uwzględniać specyfikę krajową i potrzebę rzeczywistej interoperacyjności systemów ochrony IK w regionie. Skuteczna ochrona IK wymaga nie tylko sprawnych przepisów, ale także konsekwentnej ich implementacji i zdolności reagowania na dynamicznie zmieniające się zagrożenia.

SUMMARY

Evolution and Comparative Legal Analysis of Regulations Concerning Critical Infrastructure Protection in Poland and Lithuania

The article presents a comparative legal analysis of legal regulations concerning critical infrastructure (CI) protection in Poland and Lithuania, placing the discussion in the context of the changing security environment and ongoing legislative and institutional processes. The starting point was the origin of the concept of CI and the development of international protection standards, which began in the United States in the 1990s and were subsequently developed within NATO and the European Union. Key acts such as Council Directive 2008/114/EC on the identification and designation of European critical infrastructure (the ECI Directive) and Directive 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (the CER Directive), whose impact on the national legislation of Poland and Lithuania was assessed as significant, although still insufficiently harmonised.

The analysis of the Polish CI protection system highlighted its relative consistency and its basis in the 2007 Crisis Management Act and the National Critical Infrastructure Protection Programme. The Polish model is characterised by a clear division of competences between ministries, the responsibilities of CI owners and the procedures for drawing up protection plans. The system is based on cooperation between the public and private sectors and the classification of CI in classified lists. It was noted that although strategic documents contain many general recommendations, their value lies in the standardisation of protection practices.

With regard to Lithuania, it was shown that the legal system is much more fragmented and complex. The 2002 Act on the Protection of Facilities of Importance to National Security and a number of implementing acts play a key role. Unlike Poland, the Lithuanian approach places a strong emphasis on ownership and investment control over strategic facilities, often at the expense of a systemic approach to CI protection in other dimensions. The regulations also focus on cybersecurity, neglecting consistent regulations on physical and organisational security.

The results of the analysis indicate structural similarities between the two countries' systems, including in their sectoral approach and the list of institutions responsible for CI protection. The differences mainly concern the level of formalisation, the degree of centralisation and the completeness of the solutions. Poland has a more transparent and harmonised model, while the Lithuanian system is more fragmented and tends to impose arbitrary restrictions on the activities of private entities.

In conclusion, it was found that despite the apparent shortcomings in Lithuanian regulations, there are solid grounds for further convergence of the two countries' solutions. However, harmonisation should not be limited to the formal implementation of EU directives, but should take into account national specificities and the need for genuine interoperability of CI protection systems in the region. Effective CI protection requires not only efficient legislation, but also consistent implementation and the ability to respond to rapidly changing threats.