Terroryzm – studia, analizy, prewencja, 2025, wydanie specjalne: 291–332

https://doi.org/10.4467/27204383TER.25.011.21514

Materiał ekspercki

Rola standaryzacji i oceny zgodności w zapewnianiu bezpieczeństwa i budowaniu odporności infrastruktury krytycznej na zagrożenia hybrydowe

The role of standardisation and conformity assessment in ensuring security and building resilience of critical infrastructure to hybrid threats

Adam Tatarowski
Zakład Rozwoju Technicznej Ochrony Mienia „TECHOM”
https://orcid.org/0009-0007-5503-6819

Wprowadzenie

Podejście do rozumienia bezpieczeństwa ewoluuje w Polsce od okresu transformacji ustrojowej w 1989 r. Dopiero wtedy zaczęły kształtować się potrzeby rynku i administracji państwowej w zakresie usług ochrony i bezpieczeństwa. Do momentu uchwalenia obowiązującej do dzisiaj *Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia* sektor ochrony i bezpieczeństwa funkcjonował w Polsce bez dedykowanych ustawowych regulacji. Rozwijał się na zasadach rynkowych i ulegał zarówno pozytywnym, jak i negatywnym wpływom oddolnym – wewnątrzrynkowym, a także odgórnym – ze strony administracji państwowej oraz zewnętrznym.

Przeszkodą w stworzeniu spójnego i przejrzystego systemu prawnego, który zapewniłby sektorowi ochrony i bezpieczeństwa stabilny fundament, był brak jednoznacznej wizji i decyzyjności państwowych instytucji regulacyjnych na poziomie tworzenia szczegółowych wymagań. Wypracowanie spójnych rozwiązań komplikowały ponadto sprzeczne interesy różnych grup wpływu, których działania miały niekorzystny wpływ na przebieg prac legislacyjnych. Potencjał wynikający z dorobku normalizacyjnego nie został wykorzystany. Kolejne inicjatywy legislacyjne, choć niezbędne i często inspirowane europejskimi rozwiązaniami, nie tworzyły spójnej struktury – pozostawiały istotne luki, hamujące wzrost konkurencyjności, transparentności i jakości świadczonych usług oraz dostarczanych rozwiązań organizacyjno-technicznych. Przykładem bardzo potrzebnego aktu normatywnego, który jednak nie uwzględniał rozwiązań systemowych dotyczących zapewnienia jakości i zgodności, było *Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*, dookreślające zagadnienia ochrony tych obiektów w sytuacji zagrożenia bezpieczeństwa państwa.

Obok „głównego nurtu" prawnego skupionego na ustawie o ochronie osób i mienia zaczęto w Polsce dostrzegać potrzebę utworzenia jednolitego podejścia do ochrony infrastruktury krytycznej (IK) i zapewnienia jej bezpieczeństwa. Choć rozumiano, że pewne systemy i obiekty – takie jak sieci energetyczne, infrastruktura telekomunikacyjna czy systemy transportowe – mają fundamentalne znaczenie dla funkcjonowania państwa, przez długi czas brakowało regulacji, które kompleksowo ujmowałyby ich ochronę. W polskim systemie prawnym brakowało samego pojęcia IK. Jak wskazują Tomasz Szewczyk i Maciej Pyznar[1], polska administracja państwowa spotykała się z tym pojęciem głównie w ramach współpracy międzynarodowej, w strukturach NATO i Unii Europejskiej. Powstające wówczas przepisy koncentrowały się na wybranych sektorach lub odnosiły się do ochrony poszczególnych obiektów, nie tworzyły jednak jednolitego systemu zabezpieczeń. W efekcie działania podejmowane w zakresie ochrony IK były rozproszone, a kwestie odpowiedzialności administracyjnej za jej bezpieczeństwo nie były jasno określone.

[1] T. Szewczyk, M. Pyznar, *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 54.

Dla wielu krajów wzorem w próbie uporządkowania tego zagadnienia stało się podejście amerykańskie, które na przełomie XX i XXI w. kształtowało nowe standardy związane z ochroną IK. Punktem zwrotnym w tym zakresie było wejście w życie dyrektywy Presidential Decision Directive 63 z 22 maja 1998 r.[2], która wprowadziła pojęcie *critical infrastructure* jako systemów niezbędnych do zapewnienia podstawowego funkcjonowania gospodarki i administracji państwowej. Zgodnie z nią są to systemy fizyczne i cyfrowe, których zniszczenie lub zakłócenie mogłoby prowadzić do poważnych konsekwencji społeczno-ekonomicznych i politycznych. Nowością było uznanie, że ochrona tych systemów wymaga skoordynowanego wysiłku zarówno administracji rządowej, jak i sektora prywatnego, który był właścicielem większości zasobów uznawanych za krytyczne dla funkcjonowania państwa. Dyrektywa ta nakładała na poszczególne agencje federalne USA obowiązek opracowania planów ochrony IK oraz stworzenia mechanizmów wymiany informacji między sektorami: publicznym i prywatnym.

Pod wpływem amerykańskich standardów na forum UE rozpoczęto prace nad stworzeniem jednolitych ram ochrony unijnej IK. W Polsce początkowe działania administracji państwowej w tym zakresie koncentrowały się na wybranych sektorach. Wciąż brakowało podejścia, które integrowałoby różne aspekty bezpieczeństwa infrastrukturalnego w jednolitym modelu zarządzania.

Momentem przełomowym w kształtowaniu polskiego systemu ochrony IK było uchwalenie *Ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku*, która w art. 3 pkt 2 po raz pierwszy wprowadziła do polskiego porządku prawnego definicję IK, rozumianej jako:

> (...) 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. Infrastruktura krytyczna obejmuje systemy:
> a) zaopatrzenia w energię, surowce energetyczne i paliwa,
> b) łączności,
> c) sieci teleinformatycznych,
> d) finansowe,

[2] *Presidential Decision Directive/Nsc-63*, The White House, 22.05.1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm [dostęp: 5.03.2025].

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.

W tej ustawie zdefiniowano też pojęcie ochrony IK, czyli (...) *działań zmierzających 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* (art. 3 pkt 3).

Na mocy tej ustawy powstało ponadto Rządowe Centrum Bezpieczeństwa (RCB) – ponadresortowa struktura, podległa bezpośrednio Prezesowi Rady Ministrów, odpowiedzialna za działalność planistyczną i programową z zakresu ochrony IK (art. 10 ust. 1).

Tworzenie europejskich regulacji i ich oddziaływanie na polskie prawodawstwo

Na poziomie unijnym przełom nastąpił po wejściu w życie *Dyrektywy Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*. W rozumieniu tej dyrektywy IK jest definiowana bardziej ogólnie, jako (...) *składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji* (art. 2). Dyrektywa wprowadziła i dookreśliła podejście „obiektowe" do ochrony IK, ponieważ skoncentrowano się w niej na ochronie obiektów i instalacji, których uszkodzenie mogłoby mieć poważne konsekwencje dla funkcjonowania państwa. Polska implementacja dyrektywy uwzględniła ten model bardziej kompleksowo. Wynikało to ze świadomości rosnących zależności między administracją publiczną a sektorem prywatnym oraz dynamicznych zmian w globalnym środowisku bezpieczeństwa. Rozwiązania przyjęte w Polsce nie tylko wzmacniały ochronę obiektów,

lecz także kładły fundament pod pokonywanie przyszłych wyzwań związanych z utrzymaniem ciągłości usług.

Ustawa o zarządzaniu kryzysowym zobowiązywała RCB do utworzenia i systematycznej aktualizacji Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) – przełomowego dokumentu, w którym szczegółowo zdefiniowano proces wyłaniania IK i jej ochronę. Dodano do niego załącznik pt. *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.* Całość stworzyła podbudowę do standaryzacji ochrony IK, opartej na tzw. sześciopaku dotyczącym:

1) ochrony fizycznej,
2) ochrony technicznej,
3) ochrony osobowej,
4) ochrony teleinformatycznej,
5) ochrony prawnej,
6) aspektów związanych z planami odbudowy.

Ustawa i zbiór dokumentów będących jej uzupełnieniem, w tym NPOIK, ewoluowały przez lata. W tym czasie został ugruntowany dość skomplikowany proces identyfikacji IK, składający się z trzech etapów. W pierwszym ustala się, do którego systemu należy potencjalny obiekt IK. Następnie sprawdza się, czy dany obiekt pełni funkcję, o której mowa w definicji ustawowej. Na końcu analizuje się, czy możliwe skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK będą spełnieniem kryteriów przekrojowych odnoszących się do społecznych skutków destrukcji bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria te obejmują:

– ofiary w ludziach,
– skutki finansowe,
– konieczność ewakuacji,
– utratę usługi,
– czas odbudowy,
– efekt międzynarodowy,
– unikatowość (w sensie niemożności zastąpienia i odtworzenia zniszczonego obiektu, urządzenia bądź instalacji)[3].

[3] Zob. szerzej: A. Tatarowski, *Budowanie odporności infrastruktury krytycznej w świetle zagrożeń asymetrycznych i terroryzmu. Tendencje legislacyjne w polskiej implementacji dyrektywy CER ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych*, „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 175–194. https://doi.org/10.4467/27204383TER.24.006.19394.

Od momentu zaimplementowania w Polsce dyrektywy NIS[4] *Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* równolegle do podejścia „obiektowego" funkcjonuje „usługowy" system wyłaniania operatorów usług kluczowych, czyli takich, które mają istotne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i są wymienione w wykazie usług kluczowych, wydanym na podstawie ustawy. Z kolei decyzję uznającą podmiot za operatora usługi kluczowej wydaje się wtedy, gdy:

- podmiot świadczy usługę kluczową,
- świadczenie tej usługi zależy od systemów informacyjnych,
- incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora[5].

Współistnienie podejścia „obiektowego" i „usługowego" doprowadziło do niespójności w całościowym systemie zarządzania IK. Model „obiektowy", bazujący na klasycznej ochronie infrastruktury, nie obejmował perspektywy systemowej i nie uwzględniał istotnych zależności pomiędzy sektorami. Z kolei podejście „usługowe", rozwijane w ramach regulacji dotyczących cyberbezpieczeństwa, miało ograniczony zakres zastosowania. Dualizm ten był szczególnie widoczny w politykach UE, w których obowiązywały dwie odrębne dyrektywy: dyrektywa Rady 2008/114/WE, nakładająca obowiązek ochrony fizycznej infrastruktury, oraz dyrektywa NIS, koncentrująca się na zapewnieniu odporności systemów informatycznych i usług cyfrowych.

Dojrzewanie do nowego modelu ochrony infrastruktury krytycznej

W ciągu kolejnych lat rosło zrozumienie, że tradycyjny model ochrony IK, skupiony wyłącznie na obiektach fizycznych, jest niewystarczający. Wpływ na to miały zarówno przeprowadzane analizy naukowe, jak i wydarzenia, które ujawniły istotne luki w dotychczasowym systemie zarządzania ryzykiem. Doświadczenia wynikające z ataków terrorystycznych (np. 11 września 2001 r.), pandemii COVID-19, cyberataków oraz katastrof naturalnych (np. huragan Sandy)[6] unaoczniły, że duże znaczenie ma nie tyle ochrona

[4] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*.

[5] Zob. szerzej: A. Tatarowski, *Budowanie odporności infrastruktury krytycznej…*, s. 178.

[6] M. Wiśniewski, K. Szwarc, W. Skomra, *Continuity of Essential Services as an Emerging Challenge for Societal Resilience*, „IEEE Access" 2023, t. 11, s. 44615. https://doi.org/10.1109/ACCESS.2023.3271751.

pojedynczych obiektów, systemów czy instalacji, ile zapewnienie nieprzerwanego działania usług istotnych dla stabilności państwa i bezpieczeństwa obywateli. Zakłócenie jednej usługi, np. dostaw paliwa, może wywołać efekt domina i prowadzić do problemów w transporcie, niedoborów żywności czy ograniczonej dostępności opieki medycznej. Ciekawą koncepcją, która miała wpływ na kształtowanie się tego podejścia w Polsce i UE, jest „Six Ways to Die"[7]. Jej najważniejszym założeniem jest to, że celem ochrony nie powinna być sama „fizyczna" IK, lecz zapewnienie nieprzerwanego dostępu do usług, od których zależy bezpieczeństwo obywateli na 3 poziomach: indywidualnym, społecznym i państwowym. Identyfikuje ona 6 fundamentalnych zagrożeń, które mogą prowadzić do śmierci jednostek oraz destabilizacji społecznej i gospodarczej: brak żywności, brak wody, choroby, urazy, ekstremalne zimno i ekstremalne ciepło.

Stany Zjednoczone jako pierwsze szeroko zaimplementowały „usługowy" model ochrony. Amerykańska Cybersecurity and Infrastructure Security Agency (CISA) opracowała dokument *National Critical Functions Set* (NCFS)[8], który definiuje funkcje krytyczne jako działania i procesy niezbędne do utrzymania bezpieczeństwa narodowego, stabilności gospodarki oraz podstawowego funkcjonowania społeczeństwa. W dokumencie wyróżniono 4 główne obszary, w których zidentyfikowano 55 funkcji krytycznych:

1) łączność (*connect*) – zapewnienie sprawnego funkcjonowania systemów telekomunikacyjnych, internetu, transmisji danych i usług pocztowych,
2) dystrybucja i transport (*distribute*) – utrzymanie ciągłości ruchu ludzi, towarów oraz zasobów niezbędnych do funkcjonowania gospodarki i infrastruktury,
3) dostawy i infrastruktura fizyczna (*supply*) – zabezpieczenie kluczowych zasobów, w tym energii, wody pitnej, surowców przemysłowych oraz systemów produkcyjnych,
4) zarządzanie i stabilność społeczna (*manage*) – ochrona systemów administracji publicznej (np. istotna w USA ochrona wyborów), stabilności finansowej, rynków kapitałowych oraz zarządzania kryzysowego.

[7] M. Bennett, V. Gupta, *Dealing in Security Understanding Vital Services and How They Keep You Safe*, 2010, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 22.06.2022].

[8] *National Critical Functions Set*, CISA, https://www.cisa.gov/national-critical-functions-set [dostęp: 24.06.2022].

Zatem w modelu NCFS nie chroni się pojedynczych obiektów czy systemów, lecz usługi, co implikuje np. konieczność wdrażania kompleksowych rozwiązań zapewniających odporność na awarie oraz redundancji zasobów.

Konsekwencją opisywanych działań stało się przyjęcie (14 grudnia 2022 r.) w UE przełomowej dyrektywy CER (o odporności podmiotów krytycznych)[9]. Dyrektywa CER kończy podział na podejście „obiektowe" i „usługowe". Formalizuje nowoczesne podejście do ochrony infrastruktury, z uwzględnieniem zapewnienia odporności podmiotów świadczących niezbędne usługi dla społeczeństwa. Wprowadza kompleksowy model zarządzania ryzykiem na poziomie systemowym, z uwzględnieniem współzależności między sektorami i z naciskiem na odporność całych łańcuchów dostaw. Co znamienne, w tym samym czasie przyjęto dyrektywę NIS 2[10] dotyczącą cyberbezpieczeństwa. Obie dyrektywy są ze sobą kompatybilne i jako takie powinny być wdrożone w systemach prawnych poszczególnych krajów członkowskich.

Przełomowa rola dyrektywy CER – polska perspektywa

Dla Polski implementacja dyrektywy CER jest nie tylko kolejnym wymogiem legislacyjnym, lecz także naturalnym krokiem w kierunku przyjęcia systemowego podejścia do bezpieczeństwa narodowego. Cenne w tym zakresie są doświadczenia związane z ochroną IK, zdobywane zarówno na poziomie krajowym, jak i we współpracy międzynarodowej (np. w ramach NATO i UE). Polska od lat rozwija własne metody zarządzania ryzykiem i ochrony IK, obejmujące wdrożenie NPOIK, budowanie cyberbezpieczeństwa, wprowadzanie mechanizmów służących ochronie ludności[11] i obronie cywilnej czy zwiększanie potencjału militarnego[12]. Są to solidne fundamenty, na których oprze się nowa architektura odporności podmiotów krytycznych i świadczonych przez nich usług.

[9] *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.*

[10] *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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).*

[11] *Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.*

[12] *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny.*

Co więcej, Polska ma unikalne kompetencje do kształtowania standardów ochrony IK na poziomie europejskim. Wieloletnie doświadczenie w łączeniu sektorów publicznego i prywatnego w obszarze bezpieczeństwa, uwzględniające świadomość nowych zagrożeń i ich ciągłej ewolucji oraz rozumienie szerokiego kontekstu społeczno-technologicznego, czynią Polskę ważnym uczestnikiem procesu doskonalenia mechanizmów odporności. Polska prezydencja w Radzie UE, trwająca od 1 stycznia do 30 czerwca 2025 r., koncentruje się na wzmacnianiu 7 wymiarów europejskiego bezpieczeństwa. Są to:

- zdolność do obrony,
- ochrona ludzi i granic,
- odporność na obcą ingerencję i dezinformację,
- bezpieczeństwo i swoboda działalności gospodarczej,
- transformacja energetyczna,
- konkurencyjne i odporne rolnictwo,
- bezpieczeństwo zdrowotne[13].

W Polsce za całość prac merytorycznych związanych z implementacją dyrektywy CER do ustawy o zarządzaniu kryzysowym odpowiada RCB.

Nowy etap w ochronie infrastruktury krytycznej dla Unii Europejskiej i krajów członkowskich

Wdrażanie dyrektywy CER stanowi jedno z największych wyzwań legislacyjnych i operacyjnych dla państw członkowskich UE. Jest to kamień milowy w budowaniu europejskiej odporności na zagrożenia o charakterze systemowym – od cyberataków, przez sabotaż infrastruktury, aż po kryzysy energetyczne, zdrowotne i inne, związane z nieznanymi rodzajami ryzyka. To także wyraźny sygnał, że kraje członkowskie dostrzegają konieczność ewolucji modelu ochrony IK w ujednoliconym, nowoczesnym kierunku. Nowe regulacje pozwolą skuteczniej przeciwdziałać obecnym i przyszłym zagrożeniom i zwiększą odporność zarówno na poziomie państw, jak i całej UE. Jako termin jej pełnego wdrożenia Komisja Europejska wyznaczyła październik 2024 r., jednak do marca 2025 r. jedynie 9 państw ukończyło proces transpozycji przepisów do prawa krajowego, a pozostałe – w tym Polska – prowadzą intensywne prace nad ich finalizacją. Warto dodać, że wspólne wysiłki krajów członkowskich w zakresie wdrażania dyrektywy

[13] *Prezydencja w Radzie UE*, Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/ [dostęp: 28.02.2025].

CER to przejście na nowy poziom integracji i solidarności w zakresie bezpieczeństwa. Dzięki temu UE zyskuje bardziej odporny, elastyczny i skoordynowany system ochrony, który pozwala skutecznie reagować na dynamicznie zmieniające się zagrożenia XXI w.

Źródła założeń polskiej implementacji dyrektywy CER

Prace koncepcyjne nad polską ustawą implementującą dyrektywę CER rozpoczęły się w ramach RCB w pierwszej połowie 2023 r.[14] Ich efekty zostały omówione podczas X Krajowego Forum Ochrony Infrastruktury Krytycznej (2023), a aspekty dotyczące standaryzacji i oceny zgodności przedstawił autor tego artykułu[15]. W I kwartale 2024 r. zapadły formalne decyzje dotyczące zobowiązania RCB jako wykonawcy projektu nowelizacji. W marcu 2024 r. został rozesłany do konsultacji pierwszy projekt, którego nowatorskie rozwiązania zyskały uznanie zarówno administracji państwowej, jak i interesariuszy z rynku, zwłaszcza operatorów IK. Na obecnym etapie prac legislacyjnych (marzec 2025) większość rozwiązań jest już dopracowana, a sama ustawa czeka na wejście do sejmu.

Jednym z najważniejszych obszarów w procesie implementacji dyrektywy CER jest zapewnienie spójnych i skutecznych mechanizmów standaryzacji i oceny zgodności, które umożliwią jednolite podejście do wymagań dotyczących odporności podmiotów krytycznych i ciągłości działania usług kluczowych.

Założeniem niniejszego artykułu jest wkład w dyskusję prowadzoną w ramach polskiej prezydencji w Radzie UE, szczególnie w kontekście prac Grupy Roboczej ds. Ochrony Ludności – Odporność Podmiotów Krytycznych (Working Party on Civil Protection – Critical Entities Resilience, PROCIV CER), Horyzontalnej Grupy Roboczej ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym (Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats) oraz Grupy

[14] Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf [dostęp: 6.04.2025].

[15] A. Tatarowski, *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER*, X Krajowe Forum Ochrony Infrastruktury Krytycznej, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [dostęp: 28.02.2025].

Roboczej ds. Terroryzmu (Working Party on Terrorism, TWP). W artykule przedstawiono, w jaki sposób w projekcie polskiej ustawy przełożono europejskie regulacje na konkretne rozwiązania w zakresie oceny ryzyka, standaryzacji rozwiązań organizacyjno-technicznych i usług świadczonych na rzecz podmiotów krytycznych, a także oceny zgodności (audytowania i certyfikacji). Autor niniejszego opracowania, jako współtwórca koncepcji systemu standaryzacji w polskiej implementacji CER, przedstawił genezę i uzasadnienie przyjętych rozwiązań oraz ich praktyczne konsekwencje dla operatorów IK i administracji publicznej.

Narodowy Program Ochrony Infrastruktury Krytycznej jako fundament zapewniania bezpieczeństwa infrastruktury krytycznej i źródło inspiracji

W ewoluującym przez lata NPOIK system ochrony IK jest oparty na wspomnianym tzw. sześciopaku. Dla porządku zostanie przytoczony aktualny (z 2023 r.)[16] opis tych założeń, które obejmują:

1) zapewnienie bezpieczeństwa fizycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
2) zapewnienie bezpieczeństwa technicznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
3) zapewnienie bezpieczeństwa osobowego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
4) zapewnienie bezpieczeństwa teleinformatycznego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
5) zapewnienie bezpieczeństwa prawnego – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;

[16] *Narodowy Program Ochrony Infrastruktury Krytycznej*, Rządowe Centrum Bezpieczeństwa, 2023. Tekst programu jest dostępny na stronie: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej.

6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK[17].

System ten koresponduje z art. 13 dyrektywy CER, dotyczącym środków w zakresie odporności, które powinny zostać wprowadzone przez podmioty krytyczne. Warto przywołać pierwszy ustęp tego przepisu:

1) Państwa członkowskie zapewniają, aby podmioty krytyczne wprowadzały odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne służące zapewnieniu ich odporności, w oparciu o odpowiednie informacje dostarczone przez państwa członkowskie dotyczące oceny ryzyka państwa członkowskiego oraz wyników oceny ryzyka podmiotu krytycznego, w tym środki niezbędne w celu:
   a) zapobiegania incydentom, z należytym uwzględnieniem środków zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu;
   b) zapewnienia odpowiedniej fizycznej ochrony ich budynków i terenów oraz infrastruktury krytycznej, z należytym uwzględnieniem na przykład zainstalowania ogrodzeń, budowy barier, narzędzi i procedur monitorowania terenu podlegającego ochronie, sprzętu do wykrywania i kontroli dostępu;
   c) odpowiedzi na incydenty, stawiania im oporu i łagodzenia ich skutków, z należytym uwzględnieniem wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych;
   d) odtworzenia po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej;
   e) zapewnienia odpowiedniego zarządzania bezpieczeństwem pracowników, z należytym uwzględnieniem środków takich jak ustanowienie kategorii personelu wykonującego funkcje krytyczne, ustanowienie praw dostępu do budynków i terenów, infrastruktury krytycznej i informacji szczególnie chronionych, ustanowienie procedur sprawdzenia przeszłości zgodnie z art. 14, wyznaczenie kategorii osób podlegających takim procedurom sprawdzenia przeszłości oraz określenie odpowiednich wymogów szkoleniowych i kwalifikacji;
   f) zwiększania świadomości odpowiedniego personelu na temat środków, o których mowa w lit. a)–e), z należytym uwzględnieniem szkoleń, materiałów informacyjnych i ćwiczeń.

[17] *Narodowy Program Ochrony Infrastruktury Krytycznej*..., s. 30–31.

> Do celów akapitu pierwszego lit. e) państwa członkowskie zapewniają, aby podmioty krytyczne uwzględniały personel zewnętrznych dostawców usług przy określaniu kategorii personelu, który wykonuje funkcje krytyczne.

Powyższe zapisy stanowiły punkt wyjścia do prac nad nową strukturą dotyczącą standaryzacji w zakresie zapewnienia bezpieczeństwa i budowania odporności IK w Polsce. Dyrektywa CER, zgodnie z art. 3, opiera się na zasadzie minimalnej harmonizacji, co oznacza, że wyznacza jedynie podstawowe ramy regulacyjne i pozostawia państwom członkowskim możliwość wprowadzenia rozwiązań dostosowanych do krajowych realiów, w tym bardziej rygorystycznych. Takie podejście zapewnia elastyczność i możliwość uwzględnienia specyficznych uwarunkowań krajowych oraz pozwala na stworzenie systemu ochrony IK odpowiadającego rzeczywistym zagrożeniom i wymaganiom operacyjnym. W polskiej implementacji wykorzystano ten margines swobody i zaprojektowano rozwiązania, które nie tylko w pełni realizują unijne wytyczne, lecz także integrują krajowe doświadczenia oraz wnioski płynące z dotychczasowych regulacji i praktyk w zakresie bezpieczeństwa IK.

Normalizacja jako podstawa do wdrożenia optymalnej standaryzacji

Normalizacja, rozumiana jako działalność mająca na celu uzyskanie optymalnego stopnia uporządkowania w określonej dziedzinie przez ustalenie postanowień przeznaczonych do powszechnego wielokrotnego stosowania[18], jest fundamentem sprawnego funkcjonowania społeczeństw i gospodarek, a jej znaczenie sięga początków cywilizacji[19].

[18] J. Łunarski, *Normalizacja i standaryzacja*, Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

[19] Już w świecie starożytnym dążono do ujednolicenia jednostek miar, systemów wag, standardów budowlanych i organizacyjnych, co było ważne nie tylko dla rozwoju handlu i administracji, lecz także dla zapewnienia skuteczności działań militarnych i bezpieczeństwa publicznego. Starożytny Egipt stosował precyzyjne miary przy wznoszeniu monumentalnych konstrukcji, takich jak piramidy, a w Mezopotamii jednolite systemy wag pozwalały na sprawne funkcjonowanie gospodarki i wymiany towarowej. Starożytny Rzym natomiast rozwinął system normalizacji w sposób, który na wiele stuleci ukształtował organizację społeczną i militarną. Standaryzacja uzbrojenia i wyposażenia legionistów zapewniała przewagę operacyjną na polu bitwy i zwiększała efektywność logistyki wojskowej. Rzymianie stosowali również normy w budownictwie – ujednolicone metody wznoszenia dróg, akweduktów i fortów wojskowych umożliwiały sprawną ekspansję i utrzymanie imperium. Rzymianie rozwinęli także pierwsze ustandaryzowane formy straży miejskiej oraz systemy kanalizacyjne, które minimalizowały zagrożenia zdrowotne w miastach.

Normy organizują rzeczywistość, zapewniają przewidywalność i koordynację działań w skali globalnej. Od systemów produkcji i dystrybucji energii, przez transport i telekomunikację, aż po cyberbezpieczeństwo i zarządzanie ryzykiem – normalizacja stanowi fundament interoperacyjności i stabilności. W dobie dynamicznych zmian technologicznych oraz rosnących zagrożeń bezpieczeństwa jej rola jest jeszcze bardziej istotna, ponieważ tworzy spójne ramy dla funkcjonowania państw, gospodarek i instytucji w coraz bardziej złożonym świecie.

Obecnie normalizacja w istotny sposób wspiera unijną legislację. Przełomowym momentem w umocowaniu normalizacji w unijnym ekosystemie społeczno-gospodarczym było przyjęcie i opublikowanie 7 maja 1985 r. Rezolucji Rady WE[20] w sprawie nowego podejścia do harmonizacji technicznej i normalizacji. Jak twierdzą Teresa Idzikowska i Krzysztof Banaszek, (...) *nadanie szczególnie wysokiej rangi normom i specyfikacjom technicznym będącym produktem działalności normalizacyjnej, przy tworzeniu zasad swobodnego przepływu towarów i likwidowaniu barier w handlu, oznaczało radykalną zmianę statusu norm zarówno na szczeblu krajowym, jak i międzynarodowym*[21]. Przyjęty model zakładał, że przepisy prawne powinny określać jedynie podstawowe wymagania dotyczące bezpieczeństwa i jakości, szczegółowe wytyczne techniczne zaś – być opracowywane w ramach dobrowolnych norm europejskich. W praktyce pozwoliło to na elastyczne dostosowanie wymogów do zmieniających się warunków rynkowych i technologicznych, z jednoczesnym ujednoliceniem najważniejszych standardów na poziomie całej Wspólnoty Europejskiej.

Od 1 stycznia 2004 r. Polski Komitet Normalizacyjny (PKN) jest członkiem europejskich organizacji normalizacyjnych: Europejskiego Komitetu Normalizacyjnego i Europejskiego Komitetu Normalizacyjnego Elektrotechniki. Są to stowarzyszenia prywatne, nienakierowane na osiąganie zysku, działające na podstawie belgijskiego prawa. Nie są organami KE. Europejski system normalizacyjny wyróżnia się tym, że Normy Europejskie są uzgadniane przez wszystkie kraje członkowskie, a każdy z nich, niezależnie od zaangażowania w ich opracowanie, ma obowiązek ich oceny i implementacji. W efekcie w Europie istnieje jedna Norma Europejska, dostępna tylko

[20] *Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards.*

[21] T. Idzikowska, K. Banaszek, *Rola i znaczenie normalizacji w bezpieczeństwie transportu*, „Logistyka" 2010, t. 4.

jako implementacja norm krajowych[22]. Dla porządku należy wspomnieć, że norma ma wiele zbieżnych ze sobą definicji[23]. Dość przystępna jest ta ujęta w *Ustawie z dnia 12 września 2002 r. o normalizacji*, zgodnie z którą jest to (...) *dokument przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający – do powszechnego i wielokrotnego stosowania – zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie* (art. 2 ust. 4).

Świadomość roli, jaką odgrywa normalizacja jako instrument wspierający zarządzanie ryzykiem i bezpieczeństwem, znalazła odzwierciedlenie w dyrektywie CER, która umożliwiła państwom członkowskim uwzględnianie norm mających zastosowanie do podmiotów krytycznych. Zgodnie z motywem 34 dyrektywy (...) *proces normalizacji powinien pozostać procesem uzależnionym głównie od czynników rynkowych. Nadal mogą jednak zaistnieć sytuacje, w których należy wymagać przestrzegania określonych norm.* Z kolei art. 16 wskazuje, że (...) *aby wspierać spójne wdrażanie niniejszej dyrektywy, państwa członkowskie zachęcają, w przypadkach gdy może to być przydatne i nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych dla środków w zakresie bezpieczeństwa i w zakresie odporności mających zastosowanie do podmiotów krytycznych.*

Propozycja polskiej implementacji dyrektywy CER w pełni realizuje te założenia. Uwzględnia zarówno europejski dorobek normalizacyjny, jak i krajowe doświadczenia w zakresie standaryzacji systemów bezpieczeństwa w IK (NPOIK wraz z załącznikami).

Wprowadzanie norm do przepisów prawa – polska specyfika

Możliwość powoływania norm w przepisach prawa wynika ze wspomnianej ustawy o normalizacji. Zgodnie z art. 5 ust. 4: *Polskie Normy mogą być powoływane w przepisach prawnych po ich opublikowaniu w języku polskim*, a sposób powoływania uwzględniający dokładność (powołanie datowane, niedatowane, ogólne) i moc (wyłączne lub wskazujące) określa norma PN-EN 45020:2009 *Normalizacja i dziedziny związane. Terminologia ogólna*. Prace legislacyjne związane z osiągnięciem celów wyznaczonych przez

[22] T. Schweitzer, E. Zielińska, *Działalność normalizacyjna*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny, s. 15–18.

[23] *A World Built on Standards: A Textbook for Higher Education*, S.A. Bøgh (red.), Nordhavn 2015, Danish Standards Foundation.

dyrektywę CER musiały oczywiście uwzględniać również szeroko rozumianą dobrowolność stosowania norm, wynikającą nie tyle z samej ustawy, ile z przyjętego systemu normalizacji europejskiej. Zgodnie ze stanowiskiem PKN powoływanie się na Polskie Normy w przepisie prawnym nie zmienia jej dobrowolnego statusu, chyba że ustawodawca chce ten status zmienić, co jest możliwe przez wyraźne wskazanie tylko w postanowieniach innej ustawy[24]. Stanowisko to wykorzystano w pierwszym projekcie implementacji, w którym zostały przywołane normy. W toku pierwszej fazy uzgodnień międzyresortowych, opiniowania i konsultacji społecznych RCB przyjęło argumentację Rządowego Centrum Legislacji (RCL), że normy, jako standardy odpłatne, nie powinny być powoływane w ustawie jako obligatoryjne do stosowania. Co więcej, pomimo jasnego stanowiska PKN względem zmiany statusu normy z dobrowolnej na obligatoryjną w rozumieniu ustawy, w której jest powoływana, zasada dobrowolności stosowania norm mogłaby zostać naruszona. W związku z tym zdecydowano się na alternatywne rozwiązanie – normy będą bezpośrednio przywoływane nie w ustawie, lecz w aktach wykonawczych lub w oficjalnych wykazach publikowanych w Biuletynie Informacji Publicznej (BIP) odpowiednich instytucji. Takie podejście pozwala na zachowanie równowagi między zapewnieniem dostępu do standardów a poszanowaniem zasad normalizacji i regulacji prawnych. Co więcej, w porozumieniu z RCL opracowano konstrukcję przepisów, która uwzględnia dotychczasowe ustalenia z zachowaniem pełnej zgodności z obowiązującymi regulacjami dotyczącymi normalizacji oraz zasadami funkcjonowania systemu normalizacyjnego. W projekcie ustawy dookreślono, że rozwiązania, o których mowa w kolejnych akapitach, (...) *powinny spełniać wymagania określone w normach, wskazanych w akcie wykonawczym*. Ten sposób zapisu wskazuje na konieczność spełnienia wymagań określonych w normie, ale nie narzuca normy jako dokumentu obligatoryjnego do stosowania.

Mentalność i bariery systemowe – geneza problemów. Konieczność twardego podejścia do wykorzystania norm

Doświadczenia państwowych instytucji regulacyjnych, zwłaszcza RCB, operatorów IK oraz całego rynku (w tym innych zamawiających – inwestorów, usługodawców, dostawców rozmaitych rozwiązań organizacyjnych

[24] *Dobrowolność stosowania norm*, Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [dostęp: 28.02.2025].

i technicznych itp.) jednoznacznie wskazują, że ochrona IK w Polsce przez lata była ograniczana przez bariery systemowe, których źródła sięgają początku transformacji ustrojowej. Doprowadziły one do sytuacji, w której zapewnienie odpowiednio wysokich standardów bezpieczeństwa było utrudnione, a w niektórych przypadkach – wręcz niemożliwe.

Jednym z najważniejszych problemów stała się niewłaściwa interpretacja przepisów prawnych regulujących kwestie zamówień publicznych (unijnych i polskich) – najniższa cena była dominującym i czasami jedynym uwzględnianym kryterium. W wielu przypadkach formułowanie wymagań dotyczących jakości sprzętu lub usług napotykało trudności zarówno na poziomie zamawiających, jak i instytucji kontrolujących. Komórki merytoryczne działające u operatorów IK, odpowiedzialne za definiowanie potrzeb w zakresie bezpieczeństwa, często formułowały wymagania odpowiadające rzeczywistym zagrożeniom i wykorzystujące sprawdzone standardy (np. NPOIK) oraz normy. Jednak na kolejnym etapie, na poziomie formalnym, wymagania te były redukowane przez działy zajmujące się zamówieniami (lub zarządy!), które powołując się na przepisy oraz niepisane zasady eliminowania zbędnych kosztów, usuwały dodatkowe wymagania techniczne lub organizacyjne, a pozostawiały wyłącznie te ujęte jednoznacznie w przepisach prawa.

Sytuację dodatkowo komplikowały instytucje kontrolujące, które często utożsamiały wymagania wykraczające poza absolutne minimum prawne z naruszeniem zasad gospodarności. Niejednokrotnie podejmowano działania kontrolne wobec jednostek, które wprowadzały bardziej restrykcyjne wymagania dotyczące bezpieczeństwa. W efekcie osoby odpowiedzialne za zamówienia nie formułowały wysokich standardów z obawy przed oskarżeniami o niegospodarność, a nawet korupcję. W przypadkach, gdy udało się przeforsować wyższe wymagania, kontrole zewnętrzne mogły uznać je za wydatki niezasadne, wzbudzające podejrzenia. Taki układ systemowy doprowadził do błędnego koła:

- operatorzy IK formułują wysokie wymagania dla bezpieczeństwa IK, bazujące na normach i dobrych praktykach,
- komórki zamówień (lub zarządy) odrzucają te wymagania, powołując się na konieczność ograniczenia kosztów i uniknięcia potencjalnych zarzutów o niegospodarność,
- instytucje kontrolujące działają w sposób, który de facto premiuje najniższą cenę, i ignorują realne potrzeby związane z bezpieczeństwem,

– dostawcy wysokiej jakości usług, sprzętu i innych rozwiązań nie mogą skutecznie konkurować, ponieważ nie mają innych argumentów poza ceną,
– dostawcy niskiej jakości usług i sprzętu zdobywają kontrakty przez oferowanie rozwiązań o wątpliwej skuteczności i pochodzeniu.

W tej sytuacji konieczne stało się wprowadzenie regulacji, które uczynią wymagania dotyczące jakości i bezpieczeństwa IK niemożliwymi do ominięcia. Dyrektywa CER w art. 16 oraz motywie 34 jasno wskazuje, że państwa członkowskie powinny zachęcać do stosowania norm, co w przypadku Polski wymagało bardziej stanowczego podejścia. Przyjęcie modelu minimalnej harmonizacji pozwoliło na opracowanie mechanizmów eliminujących możliwość obchodzenia wymagań jakościowych i tym samym na usunięcie luk systemowych, które przez lata utrudniały stosowanie wysokich standardów ochrony.

Co więcej, w projekcie implementacji dyrektywy CER uwzględniono przepisy *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* jako najważniejsze dla zapewnienia odpowiedniego poziomu ochrony wytwarzanej dokumentacji i stosowanych rozwiązań. Dodatkowo zastosowanie tych przepisów pozwala na skorzystanie z regulacji przewidzianych w art. 12 *Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych*, co w określonych przypadkach umożliwia realizację zamówień w trybie innym niż przewidziany w ustawie. To rozwiązanie, wynikające z potrzeby dostosowania procedur do specyfiki IK, wpisuje się w koncepcję podnoszenia standardów bezpieczeństwa oraz kształtowania wymagań względem usług i rozwiązań organizacyjno-technicznych.

Standaryzacja rozwiązań organizacyjno-technicznych oraz wymagań względem usług i osób w polskiej propozycji implementacji dyrektywy CER

Standaryzacja bezpieczeństwa IK to proces systemowego ujednolicania wymagań dotyczących ochrony IK, który bazuje zarówno na normach międzynarodowych, europejskich, jak i na standardach, wytycznych lub rekomendacjach krajowych, takich jak NPOIK. Jest to proces, który czerpie z normalizacji, ale też precyzyjnie określa wymagania, unifikuje je i dostosowuje do specyfiki IK, z uwzględnieniem specyficznych zagrożeń i rosnących współzależności sektorowych. Obejmuje on cały ekosystem interesariuszy:

operatorów IK, podmioty krytyczne, usługodawców, jednostki administracji publicznej, organy nadzoru i kontroli, a także podmioty lub osoby prowadzące walidację (audyty i certyfikacje) zastosowanych rozwiązań.

Proces standaryzacji uwzględnia dynamicznie zmieniające się wyzwania w obszarze bezpieczeństwa. Wymaga elastycznego podejścia do aktualizacji i doskonalenia środków ochrony. Wprowadzenie jednolitych standardów pozwala na skuteczniejsze działanie systemu zarządzania ryzykiem, eliminację jego słabych punktów oraz wzmocnienie interoperacyjności pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo IK. W konsekwencji standaryzacja zapewnia nie tylko wyższy poziom ochrony, lecz także transparentność i przewidywalność w zakresie wymagań i mechanizmów ich realizacji.

Operatorzy IK a podmioty krytyczne

Polska propozycja implementacji dyrektywy CER opisuje wymagania względem operatorów IK i podmiotów krytycznych. Operator IK to zgodnie z projektem ustawy (...) *właściciel lub posiadacz obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług wpisanych do wykazu infrastruktury krytycznej*, z kolei podmiot krytyczny (czyli podmiot wskazany w dyrektywie CER) to (...) *operator IK wpisany do wykazu podmiotów krytycznych, realizujący co najmniej jedną usługę kluczową, prowadzący działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy i prowadzący działalność na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej*. Infrastrukturę krytyczną zaś zdefiniowano jako:

> (...) obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do:
> a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej,
> b) zapewnienia funkcjonowania przedsiębiorstw,
> c) zaspokajania oraz utrzymania potrzeb obywateli, w tym potrzeb o charakterze lokalnym,
> d) zapewnienia świadczenia usług kluczowych.

Podmiot krytyczny to operator IK, który świadczy co najmniej 1 usługę kluczową, a wystąpienie tzw. incydentu istotnego mogłoby spowodować poważne zakłócenia w jej świadczeniu. Wpis do wykazu podmiotów

krytycznych następuje na podstawie analizy progów istotności skutku zakłócającego, które będą określone w akcie wykonawczym Rady Ministrów. Ocena istotności skutków zakłócających uwzględnia m.in.: liczbę użytkowników zależnych od danej usługi, powiązania między sektorami, wpływ incydentu na gospodarkę, społeczeństwo, bezpieczeństwo publiczne oraz środowisko, udział danego podmiotu w rynku, obszar geograficzny dotknięty ewentualnym incydentem oraz dostępność alternatywnych sposobów świadczenia tej usługi.

Standaryzacja wymagań dla operatorów IK. Wymagania ustawowe i minimalne standardy bezpieczeństwa

W projekcie implementacji dyrektywy CER wprowadzono nowe obowiązki dla operatorów IK, obejmujące systematyczną analizę zagrożeń oraz wdrażanie odpowiednich rozwiązań dostosowanych do jej wyników, zgodnie z tzw. sześciopakiem NPOIK.

W toku prac legislacyjnych udało się wypracować podejście, które będzie obligować operatorów IK do wdrażania minimalnych wymagań we wskazanym zakresie. To *game changer* wychodzący naprzeciw opisywanym w poprzednim rozdziale problemom systemowo-operacyjnym, które dotychczas uniemożliwiały wdrażanie odpowiednich rozwiązań pomimo istnienia NPOIK, norm i wielu innych standardów. Minimalne standardy zostaną określone w drodze rozporządzenia i będą dotyczyły całego tzw. sześciopaku. Powstają z uwzględnieniem rekomendacji o charakterze specjalistycznym w zakresie ochrony IK, niezbędnych do wdrażania rozwiązań w zakresie bezpieczeństwa IK, jej lokalizacji i charakterystyki oraz potrzeby podejmowania działań zapewniających jej bezpieczeństwo. Autor niniejszego artykułu jest współautorem tych standardów (są one na etapie uzgodnień). Stanowią one narzędzie do zapewnienia spójnego i jednolitego podejścia do ochrony IK, zgodnego z wymaganiami określonymi w projekcie ustawy. Dokument ten może mocno oddziaływać na całą branżę bezpieczeństwa w Polsce i w Europie oraz stanowić źródło wiedzy i inspiracji nie tylko dla operatorów IK. Warto go zatem szerzej opisać, ze szczególnym uwzględnieniem bezpieczeństwa fizycznego, tak bardzo podkreślanego w dyrektywie CER.

Standardy dookreślają pojęcie ochrony IK jako procesu podzielonego na następujące etapy:

1) wskazanie zakresu działań, celów do osiągnięcia w ramach ochrony IK oraz adresatów tych działań,

2) identyfikacja krytycznych zasobów, funkcji oraz określenie sieci powiązań (zależności) z innymi sektorami IK, w tym podmiotami i organami,
3) określenie ról i odpowiedzialności uczestników procesu ochrony IK,
4) szacowanie ryzyka,
5) wskazanie priorytetów działania i dokonanie ich hierarchizacji w zależności od wyników oceny ryzyka,
6) rozwój i wdrażanie systemu ochrony IK, w tym:
   – określenie kryteriów projektowych oraz instalacja systemów zabezpieczeń technicznych w obiektach IK,
   – opracowanie, stosowanie i bieżąca aktualizacja dokumentacji ochrony IK,
7) testowanie (przez ćwiczenia) i przegląd (przez samoocenę i audyt lub certyfikację) systemu ochrony IK oraz pomiar postępów na drodze do osiągnięcia celu,
8) doskonalenie rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów, pomiarów i wykorzystanie inteligentnych rozwiązań, które powinny obejmować chronione zasoby, zagrożenia dla tych zasobów oraz poziomy ich ochrony przed zidentyfikowanymi zagrożeniami.

Etapami wymagającymi szczególnej uwagi i staranności są: szacowanie ryzyka oraz rozwój i wdrażanie systemu ochrony IK. System ten powinien mieć zastosowanie do wszystkich typów zidentyfikowanych zagrożeń, tak naturalnych, jak i intencjonalnych oraz technicznych, a także być przygotowany do możliwie szybkiego przywrócenia funkcji pełnionych przez daną IK. W związku z tym działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia funkcjonowania IK przez:

– zmniejszanie prawdopodobieństwa wystąpienia zagrożenia,
– zmniejszanie podatności na zagrożenia,
– minimalizowanie skutków wystąpienia zagrożenia.

Standardy wprowadzają ujednolicone definicje pojęć istotnych przy wdrażaniu wszystkich zakresów z tzw. sześciopaku. Przykładowo pojęcia związane z ryzykiem zostały zdefiniowane następująco:

– ryzyko – prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami,
– źródła ryzyka – elementy lub czynniki, które mogą prowadzić do wystąpienia ryzyka, mogą wynikać z zagrożeń, podatności,

charakterystyki i rodzaju aktywów, otoczenia organizacyjnego lub technicznego, zachowań, działań lub błędów osób,
- kryteria ryzyka – zestaw zasad i poziomów odniesienia określających akceptowalność ryzyka, ustalanych z uwzględnieniem celów organizacji, kontekstu wewnętrznego i zewnętrznego oraz obowiązujących przepisów prawa, regulacji i norm,
- identyfikacja ryzyka – proces wyszukiwania, rozpoznawania i opisywania ryzyka, obejmujący określenie zasobów podlegających ryzyku, rozpoznanie jego źródeł oraz potencjalnych skutków,
- analiza ryzyka – proces określania poziomu ryzyka przez ocenę prawdopodobieństwa wystąpienia zdarzeń wynikających z zagrożeń oraz ich potencjalnych skutków, z uwzględnieniem istniejących podatności i zabezpieczeń,
- ocena ryzyka – proces porównania wyników analizy ryzyka z przyjętymi kryteriami ryzyka w celu określenia jego akceptowalności oraz potrzeby podjęcia działań zaradczych,
- szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka.

Definicje zostały opracowane z uwzględnieniem wielu norm z dziedziny ryzyka i kontekstu ich zastosowania w opracowywanych standardach[25]. Warto przypomnieć, że podejście oparte na ryzyku stanowi filozofię zapewnienia bezpieczeństwa IK w Polsce od wielu lat i zostało wzmocnione celami wyznaczonymi przez dyrektywę CER. To podejście umożliwia operatorom IK stosowanie wielu rozwiązań, w zależności od samodzielnie dokonanej oceny ryzyka. Na przykład systemy zabezpieczeń technicznych (czyli systemy sygnalizacji włamania i napadu, systemy kontroli dostępu i systemy telewizji dozorowej) powinny po zainstalowaniu spełnić wymagania Polskiej Normy odpowiedniej dla danego systemu zabezpieczeń technicznych w stopniu zabezpieczenia adekwatnym do oceny ryzyka, przy czym zaleca się stosowanie stopnia nie niższego niż trzeci[26].

[25] PN-ISO 31000:2018-08 *Zarządzanie ryzykiem – Wytyczne*; PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*; PN-EN ISO/IEC 27005:2025-01 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*; PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*; PN-EN IEC 31010:2020-01 *Zarządzanie ryzykiem – Techniki oceny ryzyka*; PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

[26] Według: PN-EN 50131-1 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*; PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące*

W standardach bardzo szczegółowo są opisane minimalne parametry techniczne, które powinny być stosowane dla sprzętu przeznaczonego do ochrony IK.

W projekcie ustawy zawarto również przepis, który wymusza na operatorach żądanie od usługodawców certyfikatów (przy opracowywaniu i zawieraniu umów zapewniających wdrażanie tzw. sześciopaku). W przypadku ich braku są także uwzględniane, zgodnie z zasadami wzajemnego uznawania w UE, inne dokumenty właściwe dla poszczególnych rozwiązań, potwierdzające posiadanie przez usługodawców odpowiednich kompetencji i uprawnień niezbędnych do realizacji tych rozwiązań. W aspekcie bezpieczeństwa fizycznego, w kontekście projektowania, instalowania i konserwacji systemów zabezpieczeń technicznych, można się spodziewać, że będzie to certyfikat zgodności z przywołaną w projekcie standardów PN-EN 16763 *Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych*.

Pierwotna idea standaryzacji wymagań dla podmiotów krytycznych – system zarządzania bezpieczeństwem, audytowanie i certyfikacja

Pierwotną ideą implementacji art. 13 dyrektywy CER było stworzenie dla podmiotów krytycznych systemu zarządzania bezpieczeństwem, który w komplementarny sposób obejmowałby aspekty dotyczące oceny ryzyka, jakości usług, stosowanych rozwiązań organizacyjno-technicznych oraz oceny ich zgodności, a także dotyczące np. wdrażania innych wymagań wynikających z sektorowych aktów prawnych UE. Rozwiązania organizacyjno-techniczne zostały oparte na systemie zarządzania bezpieczeństwem informacji zgodnym z PN-EN ISO/IEC 27001, z uwzględnieniem twardych wymogów w zakresie systemów zabezpieczeń technicznych, które miały być instalowane zgodnie z PN-EN 50131 i/lub PN-EN 60839 i/lub PN-EN 62676. Najbardziej istotnym elementem stało się również utworzenie systemu zarządzania ciągłością działania zgodnego z PN-EN ISO 22301 w zakresie niezbędnym do utrzymania świadczenia usługi kluczowej.

Zwieńczeniem tej idei było sformalizowanie audytów systemu zarządzania bezpieczeństwem podmiotów krytycznych oraz zapewnienie możliwości skorzystania z certyfikacji jako alternatywy dla audytu. Podstawą do tego był art. 21 dyrektywy CER, który umożliwia państwom członkowskim

systemów i komponentów; PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne*.

określenie wymagań dotyczących oceny zgodności wdrażanych rozwiązań organizacyjno-technicznych oraz zobowiązanie podmiotów krytycznych do stosowania odpowiednich środków bezpieczeństwa. W ten sposób system zarządzania bezpieczeństwem zaproponowany w projekcie implementacji miał stanowić spójną, ustandaryzowaną całość i wychodzić naprzeciw zarówno problemom związanym z brakiem jednolitych wymagań, jak i wieloletnim trudnościom z zapewnieniem wysokiej jakości zabezpieczeń w IK.

Zobowiązanie do prowadzenia audytów objęło 3 filary: system zarządzania bezpieczeństwem informacji, system zarządzania ciągłością działania oraz systemy zabezpieczeń technicznych. Podmioty krytyczne mogły realizować te audyty w sposób elastyczny, dostosowany do swojej specyfiki i struktury organizacyjnej. Proponowane rozwiązanie pozwalało na przeprowadzanie audytów w zintegrowany sposób, obejmowało wówczas jednocześnie wszystkie 3 filary, bądź w sposób rozłączny, np. przez certyfikację systemu zarządzania bezpieczeństwem informacji, równoczesne audytowanie zabezpieczeń technicznych oraz przeprowadzenie odrębnego audytu ciągłości działania. Model ten pozwalał na większą swobodę w doborze audytorów lub jednostek certyfikujących, a także dawał w określonym zakresie możliwość zaangażowania audytorów wewnętrznych. Doprecyzowując, część rozwiązań organizacyjno-technicznych mogła podlegać audytowi wewnętrznemu, realizowanemu przez wykwalifikowanych audytorów będących pracownikami podmiotu, podczas gdy część mogła być certyfikowana przez zewnętrzne jednostki certyfikujące. Wprowadzenie obowiązku audytów i możliwości certyfikacji na zgodność z Polskimi Normami miało zapewnić ujednolicenie wymagań i ich egzekwowanie, a także zwiększyć przejrzystość oraz przewidywalność w zakresie stosowanych mechanizmów kontrolnych. Co więcej, bardzo istotnym elementem systemu stało się zobowiązanie podmiotu krytycznego do żądania od usługodawców, mających realizować na rzecz tego podmiotu różne rozwiązania organizacyjno-techniczne, odpowiednich kompetencji potwierdzonych certyfikatem. Zatem już wstępny etap całego procesu wdrażania systemu zarządzania bezpieczeństwem został zabezpieczony pod względem jakości i zgodności z opisywanymi wymaganiami. Zastosowanie takich narzędzi w polskiej implementacji dyrektywy CER miało na celu nie tylko ułatwienie podmiotom krytycznym wdrażania skutecznych środków zarządzania bezpieczeństwem, lecz także przerwanie błędnego koła, które przez lata utrudniało podnoszenie standardów ochrony IK. Opisana koncepcja w toku uzgodnień

międzyresortowych, opiniowania i konsultacji społecznych zyskała uznanie i ewoluowała w dobrym kierunku.

Standaryzacja wymagań dla podmiotów krytycznych – wyewoluowana koncepcja, ujęta w aktualnym projekcie implementacji dyrektywy CER

Podmiot krytyczny zgodnie z projektem ustawy będzie zobowiązany do wdrożenia zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. Filarem tego systemu jest prowadzenie systematycznej oceny ryzyka z uwzględnieniem:

a) zagrożeń i związanych z tym ryzyk wymienionych w Krajowej Ocenie Ryzyka oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych,
b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich,
c) identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej,
d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów.

Ustandaryzowanie podejścia do oceny ryzyka stanowi jeden z celów dyrektywy CER, który w polskiej propozycji został zrealizowany komplementarnie. Warto wskazać, że Krajowa Ocena Ryzyka – dokument, za którego kształt będzie odpowiedzialne RCB – będzie zawierać:

1) zidentyfikowane istotne zagrożenia, w szczególności:
   a) stanowiące katastrofę naturalną lub awarię techniczną w rozumieniu przepisów ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2017 r. poz. 1897),
   b) hybrydowe,
   c) cyberbezpieczeństwa,
   d) o charakterze terrorystycznym,
   e) mogące spowodować niedostępność usług kluczowych,
   f) inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury;
2) zagrożenia niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości;
3) ocenę ryzyka wystąpienia zidentyfikowanych istotnych zagrożeń.

W przeprowadzaniu oceny ryzyka podmiot krytyczny powinien posiłkować się nie tylko „klasycznymi" normami dotyczącymi ryzyka, o których wcześniej wspomniano, lecz także nową specyfikacją techniczną ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*, zgodnie z którą istotne jest wypracowanie podejścia do zarządzania nowymi, nieznanymi dotychczas ryzykami, np. związanymi z rozwojem sztucznej inteligencji[27].

Kolejnym elementem zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej będzie wdrożenie przez podmiot krytyczny odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, zwłaszcza:

a) polityk zarządzania ryzykiem,
b) bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu,
c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z wymogami ochrony infrastruktury krytycznej, o których mowa w przepisach rozdziału 7 ustawy,
d) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
e) cyberbezpieczeństwa, zgodnie z wymogami dotyczącymi podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
f) bezpieczeństwa prawnego świadczenia usługi kluczowej,
g) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie świadczenia usługi kluczowej do czasu jej pełnego odtworzenia,
h) zdolności do ochrony informacji niejawnych w niezbędnym zakresie do zapewnienia świadczenia usługi kluczowej,
i) szkoleń i ćwiczeń personelu w celu jego przygotowania na różnego rodzaju zagrożenia i incydenty,
j) realizacji okresowych audytów i certyfikacji.

Powyższe zapisy zawarte w formie szczegółowych zadań, przygotowane zgodnie z formalnymi wymogami art. 91 ust. 1 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, odpowiadają założeniom normatywnym systemu zarządzania bezpieczeństwem informacji i systemu zarządzania ciągłością działania, z uwzględnieniem aspektów dotyczących

[27] Zob. szerzej: A. Tatarowski, *Budowanie odporności infrastruktury krytycznej*...

bezpieczeństwa fizycznego oraz zabezpieczeń technicznych. Z tego względu wymaga się, aby spełniały wymagania określone w normach, które zostaną wskazane w akcie wykonawczym. Koncepcja RCB przewiduje wskazanie co najmniej następujących norm:

1) PN-EN ISO/IEC 27001 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania*,
2) PN-EN ISO 22301 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania*,
3) PN-EN 50131-1 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe*,
4) PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach. Część 1-1: Wymagania systemowe. Postanowienia ogólne*,
5) PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i komponentów*.

Uzupełnieniem tego aktu wykonawczego będzie możliwość opracowywania i udostępniania przez organ do spraw podmiotów krytycznych (tj. ministra właściwego dla danego sektora lub inny organ, np. Przewodniczącego Komisji Nadzoru Finansowego) dodatkowego wykazu dokumentów normalizacyjnych (czyli norm, specyfikacji technicznych lub innych dokumentów ustalających zasady, wytyczne lub charakterystyki). Wykaz ten, publikowany na stronie podmiotowej BIP, będzie stanowić narzędzie umożliwiające aktualizację i doprecyzowanie niezbędnych wymagań. W konsekwencji podmiot krytyczny przy wdrażaniu odpowiednich rozwiązań organizacyjno-technicznych będzie zobowiązany do uwzględnienia zarówno przepisów aktu wykonawczego, jak i uzupełniającego wykazu, co pozwoli na większą elastyczność w kontekście dynamicznie zmieniającego się otoczenia regulacyjnego i technologicznego. Dobrym przykładem obrazującym zasadność tego rozwiązania są wymagania co do zewnętrznych systemów zabezpieczeń. Obecnie przyjęta przez PKN specyfikacja techniczna[28] funkcjonuje w języku angielskim, co uniemożliwia przywoływanie jej w aktach prawnych. Po przetłumaczeniu na język polski, czego można oczekiwać najwcześniej w 2026 r., łatwiej i zdecydowanie szybciej będzie

[28] PKN-CLC/TS 50661-1:2024-10 *Systemy alarmowe – Zewnętrzne perymetryczne systemy zabezpieczeń – Część 1: Wymagania systemowe*.

można ją uwzględnić w wymaganiach, które będą ponadto ukierunkowane na konkretny sektor lub podsektor.

Sukcesem jest wprowadzenie w projekcie ustawy zobowiązania dla podmiotów krytycznych (przełożonego 1 do 1 z obowiązków określanych dla operatorów IK) do żądania od usługodawców – przy opracowywaniu i zawieraniu umów zapewniających wdrażanie rozwiązań organizacyjno-technicznych – *certyfikatów, uwzględniając równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji*. W założeniach koncepcyjnych wykaz certyfikatów miał być ujęty w akcie wykonawczym, jednak w związku z ewolucją rozwiązań organizacyjno-technicznych i sposobów określania kompetencji niemożliwe jest opublikowanie wykazu satysfakcjonującego wszystkich interesariuszy. Uznano, że optymalnym rozwiązaniem będzie opracowywanie i publikowanie takiego zestawienia przez organy do spraw podmiotów krytycznych na podmiotowych stronach BIP. W tym przypadku organ do spraw podmiotów krytycznych jest zobligowany – przed publikacją wykazu – do zasięgnięcia opinii właściwej sektorowej rady do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 *Ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości*. Ten sam mechanizm jest zastosowany w przypadku operatorów IK. W obszarze bezpieczeństwa fizycznego, uwzględniającego systemy zabezpieczeń technicznych, funkcjonują różne możliwości potwierdzania kompetencji i kwalifikacji. Przykładem jest certyfikacja na zgodność z PN-EN 16763, która dotyczy m.in. projektowania, instalowania i konserwacji systemów zabezpieczeń technicznych. Norma ta, opublikowana w języku polskim, była omawiana na wielu konferencjach (w tym tych poświęconych IK, organizowanych przez RCB) i szkoleniach branżowych, a rynek (firmy zajmujące się zabezpieczeniami technicznymi) jest dostosowany do certyfikacji na zgodność z nią. Taki certyfikat mógłby być wskazany w planowanym pierwotnie akcie wykonawczym. Z kolei normy dotyczące prywatnych usług ochrony dla IK[29], dające możliwość certyfikacji, nie mogłyby być wykorzystane w rozporządzeniu jako dokumenty

[29] PN-EN 17483-1:2021-11 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 1: Wymagania ogólne*; PN-EN 17483-2:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 2: Usługi ochrony portów lotniczych i lotnictwa*; PN-EN 17483-3:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 3: Usługi ochrony morskiej i portowej*.

odniesienia dla oceny kompetencji usługodawców dostarczających usługi ochrony ze względu na brak ich polskiego tłumaczenia.

Wspomniane normy zyskują coraz większe zainteresowanie w UE i krajach członkowskich. Jak wynika z prezentacji Confederation of European Security Services przedłożonej grupie PROCIV CER, normy te powinny odgrywać fundamentalną rolę w przekładaniu zasad bezpieczeństwa wynikających z dyrektywy CER na konkretne wymagania operacyjne. Podkreślono w niej, że prywatne firmy świadczące usługi ochrony stanowią integralną część łańcucha bezpieczeństwa, a jego skuteczność zależy od jakości każdego ogniwa. W tym kontekście normy zostały wskazane jako kluczowe narzędzie do podnoszenia jakości ochrony podmiotów krytycznych oraz zwiększania ich odporności na zagrożenia. Wskazano również, że stosowanie tych norm stanowi rekomendowaną ścieżkę zapewnienia wysokich standardów w obszarze ochrony IK i jest wsparciem realizacji celów dyrektywy CER[30]. Należy zatem podkreślić, że polskie rozwiązania legislacyjne wyróżniają się pragmatyzmem i elastycznością. Umożliwiają sprawne wdrażanie norm jako narzędzia podnoszenia jakości usług. Mechanizm konsultacyjny, uwzględniający opinie sektorowych rad ds. kompetencji, stanowi istotne wsparcie dla organów do spraw podmiotów krytycznych. Rada sektorowa, jako ciało reprezentujące cały sektor (np. sektor ochrony i bezpieczeństwa mienia i osób), zbiera informacje od kluczowych interesariuszy, co pozwala na bieżąco identyfikować potrzeby oraz dostosowywać wymagania kompetencyjne do zmieniających się realiów rynkowych i regulacyjnych.

Dzięki temu mechanizmowi różne dokumenty normalizacyjne mogą zostać włączone do praktyki rynkowej przez publikację zestawień referencyjnych na stronach BIP. To rozwiązanie pozwala na uniknięcie barier formalnych, które mogłyby hamować realizację rozwiązań organizacyjno-technicznych przez kompetentnych usługodawców oraz utrudniać dostosowanie wymagań do ewoluujących wyzwań związanych z bezpieczeństwem. Jednocześnie obowiązek konsultacji z sektorową radą zapewnia, że zestawienia te odzwierciedlają rzeczywiste potrzeby rynku, z uwzględnieniem zarówno praktyki operacyjnej, jak i międzynarodowych trendów w zakresie standaryzacji. Sektorowe rady ds. kompetencji odgrywają rolę w kształtowaniu standardów kwalifikacyjnych i kompetencyjnych w poszczególnych obszarach gospodarki. Są to ciała doradcze, powołane na podstawie

[30] Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV CER Working Party.

ustawy o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, których zadaniem jest identyfikowanie luk kompetencyjnych, rekomendowanie rozwiązań w zakresie kształcenia oraz wspieranie procesów certyfikacji i walidacji umiejętności zawodowych. Ich szczególną wartością jest szeroka reprezentacja kluczowych interesariuszy – administracji publicznej, instytucji edukacyjnych, organizacji branżowych oraz przedsiębiorstw, co pozwala na efektywne dostosowanie kompetencji do rzeczywistych potrzeb rynkowych.

Przedstawione rozwiązania pokazują, że polska implementacja dyrektywy CER nie tylko realizuje jej cele, lecz także wyznacza nowoczesne rozwiązania legislacyjne, dzięki którym zastosowanie norm staje się rzeczywistym mechanizmem podnoszenia jakości usług świadczonych na rzecz podmiotów krytycznych.

Standaryzację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej domyka obowiązek przeprowadzania przez podmioty krytyczne, co najmniej raz na 3 lata, audytu tego systemu na własny koszt. Audyt będzie obejmował zakresy:

1) zarządzanie bezpieczeństwem informacji;
2) zarządzanie ciągłością działania usługi kluczowej;
3) zapewnienie bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

Audyt będzie mógł być prowadzony przez:

1) jednostkę certyfikującą właściwą dla danego zakresu,
2) co najmniej 2 audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego, posiadających certyfikaty określone w akcie wykonawczym i spełniających wymagania bezpieczeństwa osobowego i przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne".

Generalnym założeniem audytu jest ocena zgodności teraz i w przeszłości; audyt może mieć cel prawno-normatywny i powinien realizować potrzeby biznesowe. Opiera się na 7 zasadach, wymienionych we właściwej normie[31]:

1) rzetelności, jako podstawie profesjonalizmu,
2) uczciwości przedstawiania wyników,
3) należytej staranności zawodowej,

[31] PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*.

4) poufności,
5) niezależności,
6) podejściu opartym na dowodach,
7) podejściu opartym na ryzyku.

Pomysł, aby jednostki certyfikujące prowadziły audyty (które przecież nie muszą się kończyć certyfikatem, tylko raportem z audytu), pojawił się już wcześniej i został zaadaptowany z ustawy o krajowym systemie cyberbezpieczeństwa. Jednostki certyfikujące są bowiem instytucjami, których kompetencje, zasady i etyka działania są określone przepisami wynikającymi z europejskiego systemu oceny zgodności (opisany w kolejnym rozdziale). Alternatywą dla jednostki certyfikującej są audytorzy, którzy będą mieli odpowiednie kompetencje oraz dawali rękojmię zachowania tajemnicy, potwierdzoną stosownym poświadczeniem bezpieczeństwa.

Sposób weryfikacji uprawnień audytorów (w tym ich kompetencji) będzie dookreślony w akcie wykonawczym i uwzględni wykaz certyfikatów uprawniających do realizacji audytów, a także zakres wiedzy specjalistycznej i doświadczenie audytorów. W przypadku systemu zarządzania bezpieczeństwem informacji i systemu zarządzania ciągłością działania można spodziewać się przywołania certyfikatów audytora wiodącego w danym zakresie, zresztą bardzo popularnych na rynku. Można przypuszczać, że dla systemów zabezpieczeń technicznych z kolei będzie wymagany certyfikat audytora wiodącego w zakresie systemu zarządzania bezpieczeństwem informacji w specjalizacji systemów zabezpieczeń technicznych, dlatego że nie ma żadnej normy z dziedziny systemów zabezpieczeń, która umożliwiałaby certyfikację audytorów wiodących. Certyfikacja audytora wiodącego dla tej dziedziny czerpie z utrwalonej na rynku metodyki dotyczącej audytowania systemów zarządzania bezpieczeństwem informacji.

Audyty będą mogły być prowadzone przez audytorów wewnętrznych – pracowników podmiotu krytycznego, którzy nie podlegają obowiązkowi posiadania poświadczenia bezpieczeństwa, ale podmiot krytyczny może przeprowadzić ich sprawdzenie. Uwzględnia w nim zwłaszcza informacje pozyskane z rejestrów karnych (Krajowego Rejestru Karnego oraz analogicznych rejestrów w krajach UE). Zakres kompetencji jest jednolity dla audytorów będących pracownikami podmiotu krytycznego i zewnętrznych, zatem audytor wewnętrzny, aby prowadzić audyt wynikający z ustawy, musi mieć kompetencje audytora wiodącego.

Audyt może być zastąpiony przez certyfikację rozwiązań organizacyjno-technicznych przez uprawnioną jednostkę. W takim przypadku

posiadanie certyfikatu przez podmiot krytyczny w odpowiednim zakresie uznaje się za równoznaczne ze spełnieniem obowiązku audytowego.

Dyrektywa CER wyznacza również cele w zakresie kontroli i karania podmiotów krytycznych, które również zostały zrealizowane w polskiej propozycji. Podmioty krytyczne będą podlegać karom pieniężnym w przypadkach, gdy:

- nie przeprowadzają systematycznej oceny ryzyka,
- nie wdrażają rozwiązań organizacyjno-technicznych,
- nie prowadzą dokumentacji dotyczącej wdrożonych rozwiązań,
- nie wykonują zaleceń pokontrolnych,

i innych.

Inspiracje w zakresie audytowania i certyfikacji w implementacji dyrektywy CER. Obligatoryjna i dobrowolna ocena zgodności

Intencją krajów Wspólnoty Europejskiej było wypracowanie takiego modelu systemu oceny zgodności, który ujednolicałby wymagania dla wyrobów na obszarze wspólnego rynku europejskiego. Temu celowi przyświecała zasada wzajemnego uznawania, znana w literaturze jako Cassis de Dijon[32], zgodnie z którą towar wyprodukowany legalnie i wprowadzony do obrotu w jednym państwie UE powinien być dopuszczony na rynki pozostałych państw członkowskich[33]. Przy uwzględnieniu założeń dotyczących zniesienia barier w handlu, z jednoczesnym zapewnieniem bezpieczeństwa konsumentowi i użytkownikowi, producent wyrobu lub upoważniony przez niego przedstawiciel bądź importer tego wyrobu uczestniczy w systemie oceny zgodności w sposób zróżnicowany (obszar obowiązkowy lub dobrowolny), w zależności od rodzaju danego wyrobu. W uproszczeniu, cały zakres przepisów unijnych dotyczących oceny zgodności odnosi się przede wszystkim do bezpieczeństwa wyrobów i dopuszczania ich do obrotu. W unijnych przepisach wprowadzono ramy dla nadzoru rynku produktów, aby zapewnić, że produkty te spełniają wysokie wymagania w zakresie ochrony interesów publicznych, takich jak ogólne zdrowie

[32] Nazwa nawiązuje do orzeczenia Trybunału Europejskiego w sprawie wprowadzenia na niemiecki rynek likieru o tej nazwie.

[33] Judgment of the Court of 20 February 1979. – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. – Case 120/78, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120 [dostęp: 28.02.2025].

i bezpieczeństwo, zdrowie i bezpieczeństwo w miejscu pracy, ochrona konsumentów, ochrona środowiska i bezpieczeństwa publicznego[34]. Zdefiniowano ogólne ramy reguł i zasad w odniesieniu do akredytacji i nadzoru rynku:

1) „akredytacja" oznacza poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności;
2) „krajowa jednostka akredytująca" oznacza jedyną autorytatywną jednostkę w państwie członkowskim, udzielającą akredytacji na podstawie upoważnienia udzielonego jej przez państwo;
3) „ocena zgodności" oznacza proces wykazujący, czy zostały spełnione określone wymagania odnoszące się do produktu, procesu, usługi, systemu, osoby lub jednostki;
4) „jednostka oceniająca zgodność" to jednostka, która wykonuje czynności z zakresu oceny zgodności, w tym wzorcowanie, badanie, certyfikację i inspekcję[35].

W polskim prawodawstwie system oceny zgodności jest uregulowany *Ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku*, która określa przede wszystkim zasady funkcjonowania systemu oceny zgodności w Polsce oraz zasady działania systemu kontroli wyrobów wprowadzanych do obrotu. Jej dwa główne cele to:

– eliminowanie zagrożeń dla życia lub zdrowia użytkowników i konsumentów stwarzanych przez wyroby, a także zagrożeń dla środowiska,

[34] *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93*.

[35] Tamże. Zob. także: *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/515 z dnia 19 marca 2019 r. w sprawie wzajemnego uznawania towarów zgodnie z prawem wprowadzonych do obrotu w innym państwie członkowskim oraz uchylające rozporządzenie (WE) nr 764/2008*; *Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG*; *Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów*.

– stworzenie warunków do rzetelnej oceny wyrobów poprzez ich badania, inspekcję i certyfikację przez kompetentne i niezależne podmioty.

Infrastrukturę systemu oceny zgodności tworzą jednostki notyfikowane, certyfikujące, przeprowadzające badania (laboratoria badawcze, wzorcujące), inspekcyjne oraz akredytujące. W Polsce krajową jednostką akredytującą jest Polskie Centrum Akredytacji.

Wspomniana ustawa, tak jak prawodawstwo europejskie, koncentruje się na obligatoryjnej ocenie zgodności, co jest widoczne już w samych definicjach przywołanych w ustawie, w której to np. certyfikat jest rozumiany jako (...) *dokument wydany przez jednostkę notyfikowaną, potwierdzający, że wyrób, projekt wyrobu lub proces jego wytwarzania są zgodne z wymaganiami* (art. 4 pkt 4). Jednostka notyfikowana to z kolei jednostka oceniająca zgodność (czyli, zgodnie z art. 4 pkt. 11, taka, o której mowa w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008), funkcjonująca w obszarze regulowanym – zgodnie z art. 4 pkt 12. Jak piszą Anna Stankowska, Adam Muszyński i Sławomir Wilczyński[36]:

> (...) tam gdzie prawo określa wymagania w odniesieniu do przedmiotu regulacji, ocena zgodności jest obowiązkowa oraz określone są jednostki/organizacje oceniające zgodność, które z mocy prawa zajmują się taką oceną, jeśli przepis prawa tego wymaga. Biorąca udział w ocenie zgodności jednostka oceniająca zgodność (strona trzecia), wyznaczona w dyrektywie do współuczestniczenia w ocenie zgodności, musi być notyfikowana. Notyfikacja służy formalnemu wykazaniu kompetencji tej jednostki do wykonywania określonych zadań w zakresie oceny zgodności.

Wzorce z obligatoryjnego systemu oceny zgodności, wypracowane na poziomie UE i doprecyzowane w Polsce, były istotnym punktem odniesienia przy formułowaniu rozwiązań legislacyjnych dotyczących audytowania i certyfikacji rozwiązań organizacyjno-technicznych wdrażanych przez podmioty krytyczne. Należy podkreślić, że normy mające zastosowanie do tych rozwiązań nie podlegają obowiązkowej certyfikacji, ale można prowadzić ocenę zgodności z nimi na zasadach dobrowolności. Na potrzeby projektu ustawy przyjęto zatem następujące definicje. Jednostkę certyfikującą określono jako (...) *jednostkę oceniającą zgodność, akredytowaną*

[36] A. Stankowska, A. Muszyński, S. Wilczyński, *System oceny zgodności*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny, s. 169.

zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854) lub upoważnioną do certyfikacji zgodnie z przepisami ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), co nie tylko uwzględnia postanowienia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008, lecz także daje możliwości działania jednostkom certyfikującym, które nie mają akredytacji. Akredytacja bowiem, co należy podkreślić, jest wymagana dla zakresów określonych we wspomnianym rozporządzeniu i ustawie o systemach zgodności i nadzoru rynku. Z kolei jednostki upoważnione do certyfikacji zgodnie przepisami ustawy o normalizacji nie działają w obszarze regulowanym, lecz dobrowolnym i mają możliwość posługiwania się jedynym w Polsce dobrowolnym znakiem certyfikacyjnym umocowanym prawnie, tj. znakiem PN[37].

Certyfikat opisano jako (...) *dokument wydany przez jednostkę certyfikującą potwierdzający, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania.* To bardzo ważna definicja, ponieważ stosowanie pojęcia certyfikatu ma często charakter potoczny i jest ono nadużywane. Powszechne są również przypadki – intencjonalne lub nie – kierowania zainteresowanych na definicję określoną w ustawie o systemach zgodności i nadzoru rynku, co – gdy nie zostanie uwzględniony kontekst – jest mylące i ma ogromny potencjał manipulacyjny i dezinformacyjny. Było to zauważalne zwłaszcza w branży systemów zabezpieczeń technicznych. Certyfikacja z kolei to (...) *działania jednostki certyfikującej, wykazujące, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania.*

W projekcie implementacji dyrektywy CER zaadaptowano istniejące w europejskim i polskim porządku prawnym mechanizmy akredytacji i upoważnienia jako narzędzi do walidacji kompetencji podmiotów zajmujących się oceną zgodności z normami dotyczącymi systemu zarządzania bezpieczeństwem informacji, systemu zarządzania ciągłością działania oraz systemów zabezpieczeń technicznych. Uwzględnienie tych mechanizmów pozwoliło na sprawne wpisanie systemu audytowania i certyfikacji w ugruntowane ramy prawne, już wcześniej regulujące zasady weryfikacji kompetencji jednostek oceniających zgodność.

[37] *Rozporządzenie Rady Ministrów z dnia 11 października 2010 r. w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą.*

Podstawowym celem było zapewnienie wysokiego poziomu rzetelności i wiarygodności procesu oceny zgodności, przy jednoczesnym uniknięciu wprowadzania nadmiernie skomplikowanych, nowatorskich mechanizmów prawnych, które mogłyby generować trudności interpretacyjne i wdrożeniowe. Akredytacja, jako uznana forma formalnego poświadczenia kompetencji jednostek certyfikujących, stanowi gwarancję niezależności, jakości, najwyższego poziomu merytorycznego, organizacyjnego oraz stosowania zasad etyki. Analogicznie jest z upoważnieniem wskazanym w art. 7 ust. 3 ustawy o normalizacji, które otwiera ścieżkę dla podmiotów chcących działać w obszarze certyfikacji na zasadach dobrowolnych. Rozwiązania te korespondują z rynkiem, zapewniają elastyczność systemu i umożliwiają jego sprawne funkcjonowanie. Istotnym elementem, który dopełnia powyższe wyjaśnienia, są funkcjonujące na rynku certyfikaty.

Podsumowanie

Rok 2025 będzie przełomowy dla państw członkowskich UE, które finalizują proces transpozycji dyrektywy CER do krajowych systemów prawnych. Polska, jako jedno z państw najbardziej zaangażowanych w ten proces, wyznacza wysokie standardy w zakresie ochrony IK. Proponowane rozwiązania legislacyjne, oparte na normalizacji, łączące standaryzację i ocenę zgodności, mogą stanowić wzorzec dla pozostałych krajów członkowskich, szczególnie w kontekście narastających zagrożeń antagonistycznych i hybrydowych – a te stanowią dziś jedno z największych wyzwań dla bezpieczeństwa IK. W raporcie dotyczącym sektora ochrony i bezpieczeństwa mienia i osób w Polsce Anna Araminowicz, Piotr Klatta, Tomasz Radochoński i Magda Sierżyńska piszą: *Na poziomie lokalnym udane sabotaże mogą obniżać potencjał gospodarczy, powodując straty osobowe i materialne, jak też stanowić zagrożenie dla życia i zdrowia mieszkańców oraz dla środowiska naturalnego (np. podpalenia wysypisk śmieci). Na poziomie krajowym każdy taki akt, z uwagi na nagłaśnianie go w mediach tradycyjnych i elektronicznych, może wywoływać niepokoje społeczne, panikę i wrażenie chaosu w państwie. Wszystkie te skutki są celami działań w konflikcie hybrydowym*[38].

[38] A. Araminowicz, P. Klatta, T. Radochoński, M. Sierżyńska, *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024, MABEA sp. z o.o., s. 106.

Polska propozycja implementacji wyróżnia się kompleksowym podejściem do ochrony IK, ponieważ integruje system zarządzania bezpieczeństwem świadczenia usługi kluczowej, wymagania normatywne oraz mechanizmy audytowania i certyfikacji. Najważniejszą rolę odgrywa tu obowiązek weryfikacji kompetencji dostawców i usługodawców przez uznane systemy oceny zgodności, co pozwala na eliminację ryzyka związanego z niską jakością rozwiązań organizacyjno-technicznych.

Położenie geopolityczne i doświadczenia wynikające z bezpośredniego sąsiedztwa z regionem objętym konfliktem wojennym wzmacniają pozycję Polski jako państwa, które kształtuje politykę bezpieczeństwa IK na poziomie europejskim. Przyjęte rozwiązania mogą stać się fundamentem przyszłych inicjatyw wzmacniających odporność strategicznych sektorów gospodarki w UE.

Bibliografia

Araminowicz A., Klatta P., Radochoński T., Sierżyńska M., *Ochrona i Bezpieczeństwo Mienia i Osób – analiza sektora. Raport z badania*, Kraków 2024, MABEA sp. z o.o.

A World Built on Standards: A Textbook for Higher Education, S.A. Bøgh (red.), Nordhavn 2015, Danish Standards Foundation.

Confederation of European Security Services, *How standards drive quality and resilience in critical entities security*, 5.02.2025, EU Council PROCIV CER Working Party.

Idzikowska T., Banaszek K., *Rola i znaczenie normalizacji w bezpieczeństwie transportu*, „Logistyka" 2010, t. 4.

Łunarski J., *Normalizacja i standaryzacja*, Rzeszów 2014, Oficyna Wydawnicza Politechniki Rzeszowskiej.

Schweitzer T., Zielińska E., *Działalność normalizacyjna*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny.

Stankowska A., Muszyński A., Wilczyński S., *System oceny zgodności*, w: *Normalizacja*, T. Schweitzer (red.), Warszawa 2013, Polski Komitet Normalizacyjny.

Szewczyk T., Pyznar M., *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 53–59.

Tatarowski A., *Budowanie odporności infrastruktury krytycznej w świetle zagrożeń asymetrycznych i terroryzmu. Tendencje legislacyjne w polskiej implementacji dyrektywy CER ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych,* „Terroryzm – studia, analizy, prewencja" 2024, nr 5, s. 175–194. https://doi.org/10.4467/27204383TER.24.006.19394.

Wiśniewski M., Szwarc K., Skomra W., *Continuity of Essential Services as an Emerging Challenge for Societal Resilience,* „IEEE Access" 2023, t. 11, s. 44614–44635. https://doi.org/10.1109/ACCESS.2023.3271751.

Źródła internetowe

Bennett M., Gupta V., *Dealing in Security Understanding Vital Services and How They Keep You Safe,* http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 22.06.2022].

Dobrowolność stosowania norm, Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [dostęp: 28.02.2025].

Narodowy Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, 2023.

National Critical Functions Set, CISA, https://www.cisa.gov/national-critical-functions-set [dostęp: 24.06.2022].

Prezydencja w Radzie UE, Rada Europejska, Rada Unii Europejskiej, https://www.consilium.europa.eu/pl/council-eu/presidency-council-eu/ [dostęp: 28.02.2025].

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/515 z dnia 19 marca 2019 r. w sprawie wzajemnego uznawania towarów zgodnie z prawem wprowadzonych do obrotu w innym państwie członkowskim oraz uchylające rozporządzenie (WE) nr 764/2008 (Dz. Urz. UE L 91/1 z 29.03.2019).

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218/30 z 13.08.2008).

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 (Dz. Urz. UE L 333/164 z 27.12.2022).

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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) – (Dz. Urz. UE L 333/80 z 27.12.2022).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19.07.2016).

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

Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz. Urz. UE L 11/4 z 3.12.2002).

Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards (Dz. Urz. UE C 136/1 z 4.06.1985).

Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz. Urz. UE L 218/82 z 13.08.2008).

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (DzU z 2024 poz. 1907).

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (t.j. DzU z 2024 poz. 248, ze zm.).

Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. DzU z 2024 poz. 1320).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. DzU z 2024 poz. 1077, ze zm.).

Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. DzU z 2022 poz. 1854, ze zm.).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2024 poz. 632, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2023 poz. 122, ze zm.).

Ustawa z dnia 12 września 2002 r. o normalizacji (t.j. DzU z 2015 poz. 1483).

Ustawa z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. DzU z 2025 poz. 98).

Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (t.j. DzU z 2021 poz. 1995, ze zm.).

Ustawa z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (t.j. DzU z 2024 poz. 1125).

Rozporządzenie Rady Ministrów z dnia 11 października 2010 r. w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą (DzU z 2010 nr 198 poz. 1316).

Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (DzU z 2003 nr 116 poz. 1090).

Presidential Decision Directive/Nsc-63, The White House, 22.05.1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm [dostęp: 5.03.2025].

Tatarowski A., *Standaryzacja i certyfikacja rozwiązań wynikających z Dyrektywy CER*, X Krajowe Forum Ochrony Infrastruktury Krytycznej, Warszawa 2023, https://www.gov.pl/web/rcb/x-krajowe-forum-ochrony-infrastruktury-krytycznej-za-nami [dostęp: 28.02.2025].

Orzecznictwo

Judgment of the Court of 20 February 1979. – Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. – Reference for a preliminary ruling: Hessisches Finanzgericht – Germany. – Measures heaving an effect equivalent to quantitative restrictions. – Case 120/78, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?isOldUri=true&uri=CELEX:61978CJ0120 [dostęp: 28.02.2025].

Inne dokumenty

ISO/TS 31050 *Risk management – Guidelines for managing an emerging risk to enhance resilience*.

PKN-CLC/TS 50661-1:2024-10 *Systemy alarmowe – Zewnętrzne perymetryczne systemy zabezpieczeń – Część 1: Wymagania systemowe*.

PKN-ISO Guide 73:2012 *Zarządzanie ryzykiem – Terminologia*.

PN-EN 16763 *Usługi w zakresie systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych*.

PN-EN 17483-1:2021-11 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 1: Wymagania ogólne*.

PN-EN 17483-2:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 2: Usługi ochrony portów lotniczych i lotnictwa.*

PN-EN 17483-3:2024-03 *Prywatne usługi ochrony – Zabezpieczenie infrastruktury krytycznej – Część 3: Usługi ochrony morskiej i portowej*.

PN-EN 45020:2009 *Normalizacja i dziedziny związane. Terminologia ogólna*.

PN-EN 50131-1 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe*.

PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i komponentów*.

PN-EN 62676-1-1 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne*.

PN-EN IEC 31010:2020-01 *Zarządzanie ryzykiem – Techniki oceny ryzyka*.

PN-EN ISO 19011:2018 *Wytyczne dotyczące audytowania systemów zarządzania*.

PN-EN ISO 22301 *Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania*.

PN-EN ISO/IEC 27001 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. Systemy zarządzania bezpieczeństwem informacji. Wymagania*.

PN-EN ISO/IEC 27005:2025-01 *Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Wytyczne do zarządzania ryzykami w bezpieczeństwie informacji*.

PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*.

PN-ISO 31000:2018-08 *Zarządzanie ryzykiem – Wytyczne*.

PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, https://legislacja.rcl.gov.pl/docs//2/12386961/13069020/13069024/dokument711601.pdf [dostęp: 6.04.2025].

Adam Tatarowski

Przewodniczący Rady ds. Kompetencji w Sektorze Ochrony i Bezpieczeństwa Mienia i Osób przy Polskiej Agencji Rozwoju Przedsiębiorczości. Ekspert Rządowego Centrum Bezpieczeństwa w zakresie standaryzacji i oceny zgodności rozwiązań organizacyjno-technicznych stosowanych w zapewnianiu bezpieczeństwa infrastruktury krytycznej. Prezes Zakładu Rozwoju Technicznego Ochrony Mienia TECHOM – wyspecjalizowanej jednostki certyfikującej i placówki kształcenia ustawicznego działającej w systemie oświaty. Prezes Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM". Członek Rady Normalizacyjnej przy Polskim Komitecie Normalizacyjnym.

Kontakt: tatarowski@techom.com