Terroryzm – studia, analizy, prewencja, 2024, nr 5: 175–194

https://doi.org/10.4467/27204383TER.24.006.19394

Varia

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

Adam Tatarowski

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

Źródła i kontekst współczesnych zagrożeń asymetrycznych i terroryzmu

W latach 30. XX w. Związek Sowiecki, za sprawą koncepcji Georgija Issersona i Władimira Triandafiłłowa, wyznaczał standardy światowe w myśli wojskowej. Isserson jako pierwszy w historii opracował nowatorską doktrynę wojskową opartą na zastosowaniu operacji głębokich, tzn. uderzenia na całej głębokości wojsk wroga, na całej linii frontu[1]. W czasach postalinowskich płk Jewgienij Messner rozwijał koncepcję prowadzenia działań wojennych z wykorzystaniem środków niemilitarnych (tzw. wojen buntowniczych)[2], opisując rolę terroru w prowadzeniu działań zbrojnych,

[1] Г.С. Иссерсон, *Эволюция оперативного искусства*, Москва 1937 (G.S. Issierson, *Ewolucyja opieratiwnogo iskusstwa*, Moskwa 1937).

[2] Е.Э. Месснер, *Хочешь Мира, Победи Мятежевойну!, Творческое наследие Е.Э. Месснера*, Москва 2005 (Je.E. Miessnier, *Choczesz Mira, Pobiedi Miatieżewojnu! Tworczeskoje nasledije Je.E. Miessniera*, Moskwa 2005), s. 110.

wykorzystanie w walkach ludności cywilnej i konkretnych grup społecznych, tworzenie jednostek paramilitarnych w sytuacji zmniejszania różnic między stanem wojny a stanem pokoju. Kontynuatorem tych podejść jest gen. Walerij Gierasimow, Szef Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej. W 2013 r. w szeroko komentowanym w mediach referacie[3] przedstawił założenia wojny hybrydowej opierające się na zsynchronizowanym użyciu militarnych i niemilitarnych środków, za pomocą których będzie możliwe osiągnięcie celów strategicznych i politycznych. Gierasimow omówił takie działania, jak wprowadzanie kontyngentu międzynarodowych sił pokojowych pod pretekstem obrony praw człowieka, izolacja polityczna, sankcje ekonomiczne, blokady szlaków komunikacji lądowej, morskiej i lotniczej, grożenie użyciem siły.

Od 2014 r., od najazdu tzw. zielonych ludzików i aneksji Krymu, można to wszystko obserwować w praktyce – wojna toczy się w zasadzie cały czas i nie jest kontynuacją polityki, o czym pisał Carl von Clausewitz, ale jej elementem[4]. Agresja rosyjska, która w lutym 2022 r. przybrała formę pełnoskalową, dobitnie pokazuje, że ewolucja zagrożeń asymetrycznych znacznie przyspieszyła i ma wpływ nie tylko na obszar stricte militarny, lecz także na całe środowisko bezpieczeństwa. A zatem pojęcie zagrożeń asymetrycznych, zwięźle opisanych w *Słowniku terminów i definicji NATO* jako takich, które wynikają z możliwości zastosowania różnych środków i metod w celu obejścia lub neutralizacji silnych punktów przeciwnika i wykorzystania jego słabości, aby uzyskać niewspółmierne cele[5], należy obecnie rozumieć znacznie szerzej – w wymiarze cywilizacyjnym, społecznym, kulturowym i technologicznym. Co więcej, terroryzm, którego istotą zawsze było celowe i świadome atakowanie niewinnych, postronnych osób czy grup społecznych z zamiarem zastraszenia władz państwowych lub społeczeństwa, przybrał formę znacznie bardziej rozmytą. Collin Powell słusznie zauważył, że chociaż cywilizowany świat przez setki lat dążył do ograniczenia destrukcyjności wojen poprzez np. rozróżnienie cywil – żołnierz, to współczesny terroryzm tę różnicę coraz bardziej zamazuje[6]. Całokształt tych zagrożeń

[3] В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер" 2013 (B. Gierasimow, *Cennost' nauki w priedwidienii*, „Wojenno-promyszlennyj kurjer" 2013), nr 8, s. 2–3.

[4] C. von Clausewitz, *O wojnie*, Warszawa 2022.

[5] *AAP-6 Słownik terminów i definicji NATO*, 2021 r.

[6] Za: J.M. Fish, S.J. McCraw, Ch.J. Reddish, *Fighting in the gray zone: A strategy to close the preemption gap*, Strategic Studies Institute 2004, s. 6.

staje się dziś wyzwaniem dla podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej (dalej: IK) i zapewnienie jej odporności. W niniejszym artykule opisano tendencje legislacyjne w tym obszarze, ze szczególnym uwzględnieniem aspektów standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych wynikających z dyrektywy CER.

Emerging risks w kontekście zagrożeń asymetrycznych i współczesnego terroryzmu – wyzwania w obszarze prawno-normatywnym

Pandemia COVID-19 znacznie przyspieszyła rozpoczęte w 2018 r. prace nad nową specyfikacją techniczną *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*, opisującą sposoby podejścia do oceny i zarządzania nowymi rodzajami ryzyka, które są trudne do przewidzenia i zrozumienia ze względu na brak wystarczającej ilości danych i zweryfikowanych informacji (z ang. *emerging risks*). Ich zaistnienie, z perspektywy jakiejś organizacji, np. podmiotu krytycznego[7], może wynikać z niespodziewanych zmian w obszarze organizacyjnym, z rozwoju technologicznego czy społecznego, procesów globalizacyjnych, zawirowań politycznych, a w szerszym kontekście – z nasilania się zagrożeń asymetrycznych i terroryzmu. Te rodzaje ryzyka charakteryzują się wysokim stopniem niepewności i mogą prowadzić do poważnych konsekwencji w zakresie odporności, bezpieczeństwa oraz ciągłości działania (w wymiarze operacyjnym i biznesowym) organizacji. Zarządzanie nimi wymaga ciągłego monitorowania i gromadzenia informacji oraz elastyczności w podejmowaniu decyzji.

Aktualna koncepcja oceny ryzyka w IK opiera się na założeniach „podstawowej" normy *PN-ISO 31000:2018-08 Zarządzanie ryzykiem – wytyczne* i jest osadzona w skomplikowanym otoczeniu prawno-normatywnym, w którym nadal funkcjonuje podejście „obiektowe" do wyłaniania podmiotów IK. Zgodnie z Narodowym Programem Ochrony Infrastruktury Krytycznej (NPOIK)[8] wyłanianie to odbywa się w trzech etapach. W pierwszym

[7] *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 XII 2022 r.).

[8] *Narodowy Program Ochrony Infrastruktury Krytycznej 2023*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 29 XI 2023].

dokonuje się ustalenia, do którego systemu (według NPOIK – np. łączności, ochrony zdrowia, sieci teleinformatycznych) należy potencjalny obiekt IK (także: urządzenie, instalacja lub usługa) i porównuje się jego cechy z kryteriami danego systemu (kryteria są niejawne). W drugim sprawdza się, czy dany obiekt odgrywa rolę, o której mowa w definicji ustawowej[9]. Następnie analizuje się, czy możliwe skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK spełnią przynajmniej dwa kryteria przekrojowe odnoszące się do społecznych skutków destrukcji lub 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 lub instalacji).

I chociaż równolegle do podejścia „obiektowego" funkcjonuje „usługowy" system wyłaniania operatorów usług kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa[10], to zasięg tej regulacji jest ograniczony, dotyczy bowiem wyłącznie usług ujętych w tej ustawie i tylko takich, które odnoszą się do systemów informacyjnych. Decyzję uznającą podmiot za operatora usługi kluczowej wydaje się, jeśli:

- podmiot świadczy usługę kluczową,
- świadczenie tej usługi zależy od systemów informacyjnych,
- incydent miałby istotny skutek, powodujący zakłócenie świadczenia usługi kluczowej przez tego operatora.

Ten dualizm, z uwagi na wymogi stawiane przez dyrektywę w sprawie odporności podmiotów krytycznych (dyrektywa CER, z ang. *The Critical Entities Resilience Directive*), niebawem zaniknie. W październiku 2024 r. należy oczekiwać uchwalenia krajowych przepisów implementujących tę dyrektywę, wprowadzających „usługowy" model wyznaczania podmiotów IK. Dyrektywa CER wprowadza mechanizm interwencjonizmu państwowego.

[9] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j. DzU z 2023 r. poz. 122).

[10] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (t.j. DzU z 2023 r. poz. 913, ze zm.).

Zgodnie z jej zapisami państwa członkowskie UE stają się współodpowiedzialne za utrzymanie dostępności usługi kluczowej i będą miały możliwość bezpośredniego dotowania podmiotów gospodarczych świadczących takie usługi. Państwa członkowskie będą wyznaczać usługi kluczowe, wskazywać operatorów i egzekwować poziom dostępności usług. To zdecydowana zmiana podejścia nie tylko w relacji obywatel–państwo, lecz także biznes–państwo. Przed IK stoją więc duże wyzwania. Podmiot krytyczny będzie zobowiązany do przeprowadzenia własnej oceny ryzyka, opartej na normie *PN-ISO 31000:2018-08 Zarządzanie ryzykiem – wytyczne*, ale z uwzględnieniem możliwie najszerszego spektrum czynników ryzyka, w tym takich, które są uznawane za *emerging risks*.

Ocena ryzyka w infrastrukturze krytycznej – nowe podejścia

Operatorzy IK stosują różne metodyki zarządzania bezpieczeństwem, w zależności od świadomości, poziomu wiedzy i zrozumienia obszaru, jakim się zajmują. Każda uznana metodyka opiera się na wzorcu, którym jest norma *PN-ISO 31000:2018-08 Zarządzanie ryzykiem – wytyczne*. Zakłada ona realizację procesu zarządzania ryzykiem w trzech krokach:

1) ustalenie kontekstu,
2) ocena ryzyka (identyfikacja zagrożeń, analiza i szacowanie ryzyka),
3) decyzja o postępowaniu z ryzykiem.

Większość metodyk zarządzania bezpieczeństwem stosowanych w Polsce i w krajach, które są uznawane za wiodące w tym obszarze (np. Niemcy, Szwecja, Kanada, USA, Irlandia, Holandia czy Australia), bazuje na tej normie[11]. Autorzy publikacji *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa* szeroko analizują podejścia do oceny i zarządzania ryzykiem stosowane w tych krajach. Prezentują metodykę Zarządzania Sytuacyjnego Bezpieczeństwem Infrastruktury Krytycznej (ZS-BIK) wraz z Integralnym Modelem Bezpieczeństwa Infrastruktury Krytycznej (IM-BIK), który z kolei jest zapleczem narzędziowym metodyki ZS-BIK. Etapy tego zarządzania to:

- powołanie zespołu,
- określenie progów bezpieczeństwa,

[11] M. Kisilowski i in., *Zarządzanie bezpieczeństwem infrastruktury krytycznej i ciągłością usług kluczowych państwa*, Warszawa 2021.

– odwzorowanie charakterystyk IK,
– wygenerowanie scenariuszy zdarzeń niekorzystnych,
– sformułowanie problemu decyzyjnego,
– szacowanie ryzyka,
– wdrożenie zabezpieczeń.

W dobie rosnących zagrożeń asymetrycznych, w tym związanych z działaniami terrorystycznymi, cennym uzupełnieniem (a przede wszystkim pomocą i wsparciem) przy dokonywaniu – w ramach np. metodyki ZS-BIK – oceny ryzyka przez podmioty krytyczne są normy czy specyfikacje techniczne, takie jak:

– *PN-EN IEC 31010:2020-01 Zarządzanie ryzykiem – Techniki oceny ryzyka*,
– *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience*,
– *ISO/IEC 27005:2018 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.

Zdolność podmiotu krytycznego do przewidywania różnych okoliczności, przygotowania się i reagowania na nie powinna być najważniejszym wymogiem w procesie skutecznego zarządzania ryzykiem. Podmiot krytyczny powinien[12] m.in.:

– zoptymalizować komunikację wewnątrz i na zewnątrz organizacji,
– ustanowić skuteczny sposób gromadzenia aktualnych informacji na temat pojawiających się rodzajów ryzyka,
– przeciwdziałać dezinformacji,
– opracować sposób, w jaki osoby odpowiedzialne za zarządzanie ryzykiem mogą wpływać na kierownictwo,
– budować zaufanie w obrębie organizacji i w relacjach z podmiotami współpracującymi, w tym z administracją państwową,
– zachęcać i upoważniać odpowiednie osoby w organizacji do zgłaszania istotnych według nich sygnałów związanych z potencjalnym wystąpieniem nowych rodzajów ryzyka.

Proces identyfikowania ryzyk wymaga od podmiotu krytycznego świadomości dotyczącej dynamicznych zmian zachodzących w środowisku, w którym funkcjonuje. Pomimo wdrożenia struktury identyfikacji ryzyk (opartej na ww. normach czy też innych dokumentach, np. odnoszących się

[12] *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience.*

do zagrożeń związanych z aktami terroru[13]) powinien on korzystać także z niestandardowych, nieustrukturalizowanych metod identyfikacji, gdyż zapewni to bardziej komplementarne podejście do problemu i zwiększy efektywność identyfikacji. Zgodnie z *ISO/TS 31050:2023 Risk management – Guidelines for managing an emerging risk to enhance resilience* organizacja powinna m.in:

- regularnie, kompleksowo i z wielu perspektyw analizować środowisko, w jakim funkcjonuje, lub wykorzystywać odpowiednie metody czy techniki do identyfikacji pojawiających się zmian mogących powodować wystąpienie *emerging risks*,
- analizować trendy i okoliczności, które mogą doprowadzić do powstania nowych *emerging risks*,
- analizować źródła ryzyka i możliwe scenariusze zdarzeń,
- aktualizować w sposób ciągły opisy możliwych rodzajów ryzyka.

Przykładami zmian okoliczności, które mogą być źródłami *emerging risks*, są:

- zagrożenia naturalne, np. klimatyczne, pogodowe,
- zagrożenia związane z nowymi bakteriami, wirusami, grzybami i pasożytami czy z uodparnianiem się tych drobnoustrojów na dostępne leki,
- wyzwania związane z niekontrolowanym rozwojem internetu rzeczy (ang. *internet of things*, IoT),
- wyzwania związane z rozwojem sztucznej inteligencji.

Te ostatnie są coraz bardziej aktualnym problemem i – zdaniem autora niniejszego artykułu – niebawem staną się głównym generatorem *emerging risks*. Po raz pierwszy w historii ludzkości projektuje się urządzenia i systemy, których działanie nie do końca jest zrozumiałe. Nie wiadomo np., jak działa ChatGPT. Twórcy tego narzędzia rozumieją algorytmy uczenia maszynowego, ale nie został poznany dokładnie sposób, w jaki działają sieci neuronowe (a mają one bardzo szybkie tempo rozwoju). Nie wiadomo także, na ile sztuczna inteligencja stanie się samodzielna, a przekazanie możliwości decydowania maszynom, brak przejrzystości i zrozumienia funkcjonowania sztucznej inteligencji oraz brak nadzoru ze strony człowieka może skutkować wystąpieniem nieznanych wcześniej rodzajów ryzyka.

[13] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW* (Dz. Urz. UE L 88/6 z 31 III 2017 r.).

Z *emerging risks* mogą się wiązać również zagrożenia terrorystyczne w szerokim rozumieniu – nie tylko takim, które wynika z przywołanych wcześniej definicji w *Słowniku terminów i definicji NATO* i dyrektywie Parlamentu Europejskiego z 2017 r. w sprawie zwalczania terroryzmu. Należy założyć, że nowa rzeczywistość modelowana przez *emerging risks* będzie miała wpływ na sposób przygotowywania i dokonywania przestępstw terrorystycznych.

Generalnie wyniki systematycznej oceny ryzyka dokonywanej przez podmioty krytyczne powinny zawierać:

- listę dostawców (zasobów, usług) o kluczowym znaczeniu dla podmiotu krytycznego,
- listę procesów, których zaburzenie może wywołać incydent istotny,
- wykaz IK niezbędnej do utrzymania usługi kluczowej.

Ocena ryzyka będzie stanowić punkt wyjścia do opracowania i wdrożenia adekwatnych rozwiązań organizacyjno-technicznych.

Standaryzacja i certyfikacja adekwatnych rozwiązań organizacyjno-technicznych wynikających z dyrektywy CER

Zarys systemu ochrony IK w świetle NPOIK 2023 i dyrektywy CER

W ramach NPOIK funkcjonuje tzw. sześciopak opisujący system ochrony IK. Działania podejmowane na rzecz zapewnienia bezpieczeństwa IK 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 mają 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;
6) plany ciągłości działania i odtwarzania, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK[14].

Ten system koresponduje z art. 13 dyrektywy CER *Środki w zakresie odporności wprowadzane przez podmioty krytyczne.* Pierwszy akapit tego artykułu brzmi:

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;

[14] *Narodowy Program Ochrony Infrastruktury Krytycznej 2023*...

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.

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.

Dyrektywa CER, co jest standardem w prawodawstwie europejskim, umożliwia państwom członkowskim indywidualne regulowanie przepisów prawa krajowego, implementującego jej zapisy w taki sposób, aby poziom odporności podmiotów krytycznych był jak najwyższy i kompatybilny ze specyfiką krajową, ale z uwzględnieniem wykorzystania norm, o czym jest mowa w art. 16 tej dyrektywy.

Norma to dokument normatywny przyjęty przez uznaną jednostkę normalizacyjną. W Polsce jest to Polski Komitet Normalizacyjny. Norma ustala zasady, wytyczne lub charakterystyki dotyczące różnych rodzajów działalności i jej wyników, jest zatwierdzana na zasadzie konsensusu, przeznaczona do powszechnego i wielokrotnego stosowania, zaakceptowana przez zainteresowane strony jako korzyść dla wszystkich oraz wprowadza kodeks dobrej praktyki i zasady racjonalnego postępowania przy aktualnym poziomie techniki[15].

Zastosowanie norm w standaryzacji, a następnie certyfikacji rozwiązań organizacyjno-technicznych jest słusznym krokiem w budowaniu odporności IK na wszelkiego rodzaju zagrożenia. Ułatwia dobór rozwiązań, ich utrzymanie i walidację, a także pozwala na efektywny nadzór i egzekwowanie przepisów, gdyż organ krajowy nadzorujący IK – zgodnie z art. 21 dyrektywy CER – będzie dokonywał kontroli i podejmował decyzje

[15] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej* (Dz. Urz. UE L 316/12 z 14 XI 2012 r.).

na podstawie danych zbieranych przez zewnętrzne, kompetentne podmioty zajmujące się audytowaniem i certyfikacją.

Zakres rozwiązań organizacyjno-technicznych, które powinny zostać zastosowane w podmiocie krytycznym po przeprowadzeniu oceny ryzyka, jest bardzo szeroki. Aby syntetycznie przedstawić zagadnienie standaryzacji i certyfikacji, autor artykułu odwołał się do technicznych środków zapewnienia bezpieczeństwa fizycznego, stanowiących dobry punkt odniesienia w tym temacie, jak również do zapewniania ciągłości działania usług kluczowych.

Standaryzacja i audytowanie – kontekst normalizacji

Zgodnie z koncepcją przedstawioną przez autora artykułu 5 października 2023 r. na Krajowym Forum Ochrony Infrastruktury Krytycznej[16] rozwiązania organizacyjno-techniczne wdrażane przez podmioty krytyczne powinny być tworzone zgodnie z normami, co umożliwia – z uwagi na dostępność rozwiązań prawnych i biznesowych – skuteczne prowadzenie audytów i certyfikacji. Audyt to (...) *systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu obiektywnego oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu*[17]. Audyt ocenia zgodność teraz i w przeszłości, może mieć cel prawno-normatywny i powinien realizować potrzeby biznesowe. Opiera się na siedmiu zasadach:

1) rzetelności, jako podstawie profesjonalizmu,
2) uczciwości przedstawiania wyników,
3) należytej staranności zawodowej,
4) poufności,
5) niezależności,
6) podejściu opartym na dowodach,
7) podejściu opartym na ryzyku.

Istnieją trzy rodzaje audytów (tabela 1).

[16] 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.

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

Tabela 1. Rodzaje audytów według normy PN-EN ISO 19011:2018.

Audit strony pierwszej	Audit strony drugiej	Audit strony trzeciej
Audit wewnętrzny	Audit zewnętrznego dostawcy	Audit dla celów certyfikacji i/lub akredytacji
	Audit innej zewnętrznej strony zainteresowanej	Audit dla celów prawnych, regulacyjnych i podobnych

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

Z perspektywy podmiotów krytycznych najbardziej istotny jest audyt strony trzeciej, który przeprowadzają niezależne organizacje audytujące, takie jak jednostki certyfikujące lub instytucje rządowe. Instytucja rządowa nadzorująca podmioty krytyczne w Polsce (w warunkach prawnych, które nastąpią po implementacji dyrektywy CER) będzie gromadziła dane i podejmowała decyzje na podstawie (...) *dowodów potwierdzających skuteczne wdrożenie tych środków* [tzn. środków z art. 13, omawianych jako rozwiązania organizacyjno-techniczne], *w tym wyników audytu przeprowadzonego na koszt tego podmiotu przez wybranego przez niego niezależnego i wykwalifikowanego audytora.* Dowody w audycie strony trzeciej należy rozumieć jako certyfikaty, czyli dokumenty wydane przez jednostkę oceniającą zgodność (jednostkę certyfikującą), potwierdzające, że wyrób/instalacja/system/proces/usługa są zgodne z wymaganiami. W przypadku implementacji dyrektywy CER – zgodne z wymaganiami zawartymi w odpowiednich normach.

Na marginesie warto wyjaśnić jeden z aspektów, z którego niezrozumieniem autor artykułu spotyka się w swojej działalności zawodowej jako kierujący jednostką certyfikującą. Ocena zgodności zawsze odnosi się do jakiegoś dokumentu, w tym przypadku – normy. Powoływanie się na normy w przepisach prawa, chociaż są to dokumenty do tzw. stosowania dobrowolnego, jest możliwe, co potwierdzają stanowisko prezesa Polskiego Komitetu Normalizacyjnego[18] oraz wyroki sądów[19]. Jeśli więc norma jest przywołana w postanowieniach jakiejś ustawy, to powoływanie się na nią (np. w przypadku audytu czy certyfikacji) jest możliwe i zasadne. Taka

[18] *Dobrowolność stosowania norm*, Polski Komitet Normalizacyjny, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/stanowisko-pkn-w-sprawie-dobrowolnosci-pn [dostęp: 29 XI 2023].

[19] Wyrok Naczelnego Sądu Administracyjnego z 10 IV 2019 r., sygn. akt II OSK 1486/17; wyrok Wojewódzkiego Sądu Administracyjnego w Kielcach z 19 V 2009 r., sygn. akt II SA/Ke 183/09.

praktyka istnieje w polskim prawodawstwie, np. w ustawie o krajowym systemie cyberbezpieczeństwa. Przywołanie norm w przepisach prawa nie ułatwia jednak wglądu w nie. Dostęp do tych norm jest odpłatny.

Ocena zgodności. Uprawnienia jednostek certyfikujących i audytorów do prowadzenia certyfikacji. Certyfikat a deklaracja zgodności

Audyt strony trzeciej może być prowadzony przez jednostkę oceniającą zgodność (jednostkę certyfikującą), akredytowaną na podstawie przepisów ustawy o systemach oceny zgodności i nadzoru rynku[20] – i takie rozwiązanie funkcjonuje już w odniesieniu do audytowania bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[21] – lub przez jednostkę certyfikującą upoważnioną do certyfikacji w imieniu i na rzecz Polskiego Komitetu Normalizacyjnego w rozumieniu przepisów ustawy o normalizacji[22]. Certyfikację należy rozumieć jako działanie jednostki oceniającej zgodność (jednostki certyfikującej), wykazujące, że wyrób/instalacja/system/proces/usługa są zgodne z wymaganiami. Umocowanie jednostek certyfikujących jest bardzo silne. Funkcjonują one jako składowe ogólnego, europejskiego systemu obejmującego ocenę zgodności i nadzór rynku[23]. Ich wykorzystanie w procesie audytowania i certyfikacji rozwiązań organizacyjno-technicznych wdrażanych przez podmioty krytyczne stanie się niezbędne.

Warto zwrócić uwagę, że termin „certyfikat" często jest używany w sposób nieuprawniony (z perspektywy systemu oceny zgodności). Według definicji słownikowej certyfikat to 'oficjalny dokument stwierdzający np. zgodność produktu z normami, autentyczność dzieła sztuki lub ukończenie kursu'[24]. Stanowisko odnośnie do pojęcia certyfikatu zajęła

[20] *Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku* (t.j. DzU z 2022 r. poz. 1854).

[21] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (t.j. DzU z 2023 r. poz. 913, ze zm.).

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

[23] *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 VIII 2008 r.).

[24] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/certyfikat;2553201.html [dostęp: 29 XI 2023].

także Rada Języka Polskiego przy Prezydium Polskiej Akademii Nauk[25]. W kontekście systemu oceny zgodności – tej zgodności, która będzie miała decydujące znaczenie w przypadku IK – certyfikat to zatem, jak już wspomniano, dokument wydany przez jednostkę oceniającą zgodność (jednostkę certyfikującą), potwierdzający, że wyrób/instalacja/system/proces/usługa są zgodne z wymaganiami. Jest to definicja autorska, gdyż to pojęcie w odniesieniu do oceny zgodności z normami niezharmonizowanymi nigdy nie zostało zdefiniowane. Brakuje tej definicji w przepisach dotyczących normalizacji zarówno w przedmiotowej ustawie, jak i w rozporządzeniu Rady Ministrów w sprawie sposobu nadawania i wykorzystywania znaku zgodności z Polską Normą[26], które to rozporządzenie wskazuje nawet wzór certyfikatu. Co więcej, brakuje definicji certyfikatu (w ujęciu wskazanym przez autora artykułu) w ustawie o systemach oceny zgodności i nadzoru rynku. Znajduje się tam jedynie definicja certyfikatu jako dokumentu potwierdzającego zgodność, wydawanego przez jednostkę notyfikowaną, tj. taką, która jest zgłoszona do Komisji Europejskiej i umieszczona w wykazie jednostek notyfikowanych do konkretnych dyrektyw, a więc prowadzącą obligatoryjną ocenę zgodności. Z uwagi na potrzeby wynikające z dyrektywy CER należy spodziewać się doprecyzowania pojęcia certyfikatu w przepisach krajowych.

Deklaracja zgodności została zdefiniowana w ustawie o systemach oceny zgodności i nadzoru rynku. Należy tę deklarację rozumieć jako oświadczenie producenta, instalatora lub ich upoważnionego przedstawiciela albo prywatnego importera (na ich wyłączną odpowiedzialność), że wyrób jest zgodny z wymaganiami.

Jakie podejście do rangi takiej deklaracji można było obserwować w praktyce? Dobrym, modelowym wręcz przykładem branży, w której przez lata działało kilkuosobowe, ale mające siłę przebicia lobby, propagujące tezę, że deklaracja zgodności jest wystarczająca i gwarantuje zgodność z wymaganiami oraz odpowiednią jakość, jest branża technicznych środków zapewnienia bezpieczeństwa fizycznego. Obecnie takie głosy prawie zanikły – z uwagi na zupełnie inną świadomość uczestników rynku i przedstawicieli administracji państwowe. Zmiany nastąpiły pod wpływem negatywnych doświadczeń. Poniżej kilka przykładów ilustrujących, w jaki

[25] *Stanowisko Rady wobec użycia słowa certyfikat,* https://rjp.pan.pl/dokumenty-rady?view=article&id=98:stanowisko-rady-wobec-uycia-sowa-certyfikat&catid=45 [dostęp: 29 XI 2023].

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

sposób funkcjonował – i w pewnych obszarach nadal funkcjonuje – rynek. Dnia 7 września 2010 r. zostało opublikowane rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne[27]. W § 12 tego rozporządzenia znalazł się punkt mówiący o tym, że do przechowywania lub transportowania wartości pieniężnych wykorzystuje się urządzenia (...) *posiadające wydany przez uprawnioną jednostkę certyfikującą certyfikat zgodności albo wydaną przez producenta lub importera deklarację zgodności, potwierdzające zgodność z zasadniczymi lub szczegółowymi wymaganiami w rozumieniu przepisów o systemie oceny zgodności – w przypadku gdy dla danego wyrobu wymagania takie zostały ustalone*. Zapisy te są nadal aktualne. Intuicyjnie wiadomo, że jeśli dostawca urządzeń ma możliwość wprowadzenia na rynek urządzenia mającego deklarację zgodności, którą sam wystawia, a która najczęściej nie ma żadnego pokrycia w stanie faktycznym, to nie będzie przeprowadzał badań w akredytowanym laboratorium i starał się o uzyskanie certyfikatu. Inwestor nie ma w tym przypadku możliwości działania. Nowszym przykładem jest ustawa z 2012 r. o odpadach[28]. Posiadacz odpadów jest obowiązany do prowadzenia wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów. Akt wykonawczy do tej ustawy[29] doprecyzowuje, że: *Parametry urządzeń technicznych systemu kontroli spełniają co najmniej wymagania normy PN-EN 62676-4: 2015-06 Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania lub normy, którą przedmiotowa norma zostanie zastąpiona*. Niestety, większość posiadaczy odpadów (a może nawet żaden) nie ma wdrożonego takiego systemu. Dlaczego tak się dzieje? Pomijając nie najlepszy sposób sformułowania tego zapisu, to brakuje w nim wskazania sposobu potwierdzania zgodności, że zainstalowany system telewizji dozorowej spełnia wymagania. Projektant nie ponosi zatem ryzyka, jeśli zaprojektuje taki system, nie znając nawet przywołanej normy (zjawisko niskiego poziomu kompetencji jest w tej branży powszechne, ale istnieją rozwiązania

[27] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (t.j. DzU z 2016 r. poz. 793).

[28] *Ustawa z dnia 14 grudnia 2012 r. o odpadach* (t.j. DzU z 2023 r. poz. 1587, ze zm.).

[29] *Rozporządzenie Ministra Środowiska z dnia 29 sierpnia 2019 r. w sprawie wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów* (DzU z 2019 r. poz. 1755).

prawno-normatywne, które zaczynają już funkcjonować, co zostanie opisane w dalszej części artykułu), podobnie jak instalator, który zainstaluje taki system i wystawi deklarację jego zgodności z normą. Takie systemy jeśli w ogóle działają, często nie spełniają potrzeb inwestora i wymagań norm, i są, co oczywiste, zawodne. Tak funkcjonuje duży obszar rynku.

W przypadku IK, która zgodnie z dyrektywą CER musi wypracować odporność na zagrożenia asymetryczne, akty terrorystyczne i inne zagrożenia, takie podejście jest niedopuszczalne. System zabezpieczeń technicznych (system sygnalizacji włamania i napadu, system dozoru wizyjnego, system kontroli dostępu) powinien po zainstalowaniu uzyskać certyfikat. Usługi realizowane przez podmioty zewnętrzne (tj. projektowanie, instalowanie, konserwacja) na rzecz IK powinny spełniać najwyższe standardy jakości. Te podmioty powinny posiadać certyfikat zgodności z normą *PN-EN 16763:2017 Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych*, co wypełnia wymogi art. 13 akapit 1 lit. e dyrektywy CER. Dyrektywa ta wychodzi naprzeciw konieczności uporządkowania wymagań wobec usługodawców (w tym w obszarze ochrony przeciwpożarowej), o czym autor artykułu niejednokrotnie mówił na różnych wydarzeniach branżowych i konferencjach[30]. Wspomniana norma została już przywołana jako właściwa przy ocenie kompetencji i kwalifikacji podmiotów działających w tej branży w Załączniku 1 *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje* do NPOIK 2023.

Wdrożenie, utrzymanie i certyfikacja systemu zarządzania ciągłością działania usług kluczowych

Podmiot krytyczny, który dokonał oceny ryzyka i wdraża (lub wdrożył) adekwatne środki organizacyjno-techniczne, powinien zaimplementować system zarządzania ciągłością usługi kluczowej zgodny z normą *PN-EN ISO*

[30] A. Tatarowski, *Nowe sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej i systemów zabezpieczeń technicznych w procesie budowlanym*, IV Międzynarodowa Konferencja N-T „Problemy Inżynierii Bezpieczeństwa Obiektów Antropogenicznych", Warszawa 2021, https://psribs.pl/conferences/iv-miedzynarodowa-konferencja-n-t-problemy-inzynierii-bezpieczenstwa-obiektow-antropogenicznych-wiosna-2021/ [dostęp: 29 XI 2023]; A. Tatarowski, *Nowe sposoby walidacji jakości usług projektantów, instalatorów i konserwatorów systemów ochrony przeciwpożarowej*, XXIX Ogólnopolskie Warsztaty – Sygnalizacja i Automatyka Pożarowa SAP '2023, Żnin 2023, https://www.polon-alfa.pl/pl/aktualnosci/polon-alfa-w-cukrowni-%C5%BCnin [dostęp: 29 XI 2023].

22301:2019 Bezpieczeństwo i odporność. Systemy zarządzania ciągłością działania. Wymagania. System zarządzania ciągłością działania oparty na wspomnianej normie składa się z następujących elementów:

a) polityki,
b) kompetentnych osób z określonymi odpowiedzialnościami,
c) procesów zarządzania dotyczących:
   – polityki,
   – planowania,
   – wdrażania i działań operacyjnych,
   – oceny efektów działania,
   – przeglądu zarządzania,
   – ciągłego doskonalenia,
d) udokumentowanych informacji wspomagających nadzór działań operacyjnych i umożliwiających ocenę efektów działania.

Usług kluczowych zwykle nie realizuje jeden operator. Najczęściej jest to zbiór kilku usług, które funkcjonują niezależnie od siebie i są dostarczane przez różne podmioty. Dobrym przykładem usługi kluczowej – jak wskazują autorzy publikacji *Zarządzanie bezpieczeństwem i ciągłością usług kluczowych państwa* – jest wypłacanie pieniędzy z bankomatu. Aby można było wypłacić gotówkę, muszą być dostępne usługi składowe w postaci:

– dostępności zasilania energetycznego bankomatu,
– dostępności sieci Internet zapewniającej łączność z systemem rozliczeniowym,
– dostępności systemu rozliczeniowego banku, z którego są wypłacane pieniądze,
– zapewniania gotówki w bankomacie, za co obecnie odpowiadają głównie operatorzy sieci bankomatowych.

Zatem (...) *możliwość wypłaty pieniędzy z bankomatu jest więc w rzeczywistości zbiorem relacji, jakie występują między wymienionymi usługami składowymi i może zaistnieć wyłącznie w wyniku równoczesnej dostępności wszystkich usług składowych. W konsekwencji wystarczy niedostępność jednej ze składowych usługi kluczowej, aby ona sama również nie była dostępna*[31].

Mając na uwadze złożoność usług kluczowych, pomocne może okazać się stosowanie IM-BIK uzupełnionego o normy. W literaturze przedmiotu opisano kilka sposobów na zapewnienie nieprzerwanej dostępności. Jest to np.:

[31] M. Kisilowski i in., *Zarządzanie bezpieczeństwem*..., s. 106.

– nadmiar strukturalny, który polega na dublowaniu elementów uznanych za krytyczne,
– nadmiar funkcjonalny, który polega na przystosowywaniu wytypowanych elementów systemu do pełnienia dodatkowych funkcji,
– nadmiar parametryczny, który polega na standardowym zasilaniu systemu w stopniu przewyższającym zapewnianie jego użyteczności[32].

Warto zwrócić uwagę na sposób nazwany nadmiarem funkcjonalnym. Wykorzystując IM-BIK:

> (...) instytucja rządowa, np. RCB, może, posługując się wykazem usług kluczowych, zidentyfikować podmioty, które dostarczają usługi składowe dla usług kluczowych. Usługi składowe można wówczas potraktować jako funkcjonalności rozpatrywanych obiektów IK. W przypadku wystąpienia incydentu ograniczającego lub eliminującego dostępność funkcjonalności IK możliwe jest zidentyfikowanie obiektów IK o podobnych funkcjonalnościach i w ramach PCD (tzn. Planu Ciągłości Działania) uzupełnienie brakującej składowej usługi kluczowej funkcjonalnością realizowaną przez inny obiekt IK[33].

Zagadnienie opracowania, wdrożenia i certyfikacji systemu zarządzania ciągłością działania jest obszerne i ma unikalny charakter w odniesieniu do każdego podmiotu krytycznego. Przytoczone fragmenty zaczerpnięte z literatury przedmiotu mają za zadanie – w intencji autora artykułu – zachęcić czytelników do poszerzenia wiedzy w tym zakresie, gdyż zagadnienie to stanowi najbardziej istotną część w całościowym spojrzeniu na system zarządzania bezpieczeństwem IK.

Podsumowując, z perspektywy podmiotu krytycznego istotnym działaniem będzie nieustanne doskonalenie systemu ciągłości działania poprzez wykorzystanie pomiarów skuteczności, w tym symulacji, monitorowania, systematycznego przeglądu, oceny incydentów i skutecznego ich usuwania

[32] K. Szwarc, *Modelowanie ciągłości działania systemów zarządzania kryzysowego i ocena przydatności rozwiązań na szczeblu lokalnym*, rozprawa doktorska, Warszawa 2019, https://repo.bg.wat.edu.pl/info/phd/WATefc9a9340f3e47cb8141566cdf6e0e53/Record+details+%25E2%2580%2593+Modeling+of+the+continuity+of+crisis+management+systems+and+the+assessment+of+suitability+at+the+local+level+%25E2%2580%2593+Military+Technical+Academy+them.+Jaroslaw+Dabrowski+title?aq=%40status%3Apracownik%2Cauthorprofile%2F%40possitionPL%21%3Aadiunkt%2Cauthorprofile%2F%40possitionPL%21%3Aprofesor%2C%40active%3D%27true%27%2C.%3AWUT84b1c97cce2d442fab1acdc256a5d487&r=author&ps=20&lang=en&pn=1&cid=157628.

[33] M. Kisilowski i in., *Zarządzanie bezpieczeństwem...*, s. 108.

zgodnie z polityką bezpieczeństwa. Jednym z narzędzi pomiaru będzie prowadzenie systematycznych i niezależnych audytów, w tym zakończonych certyfikacją, ale w zakresie niezbędnym do utrzymania świadczenia usługi kluczowej.

Podsumowanie

Rok 2024 będzie dla IK przełomowy. Naglące terminy, zobowiązujące kraje członkowskie do uchwalenia krajowych przepisów implementujących dyrektywę CER, wymagają przygotowania odpowiedniego środowiska do efektywnej pracy legislacyjnej. Rządowe Centrum Bezpieczeństwa, które od wielu lat stwarza warunki sprzyjające poprawie bezpieczeństwa IK i zbudowało unikalne w UE podejście do zarządzania bezpieczeństwem w tym sektorze, oparte na wspomnianym tzw. sześciopaku, stoi obecnie przed dużym wyzwaniem dotyczącym opracowania implementacji dyrektywy CER w Polsce. W niniejszym artykule zostały przedstawione tendencje legislacyjne związane z tą implementacją w aspekcie standaryzacji i certyfikacji rozwiązań organizacyjno-technicznych. Standaryzacja i certyfikacja tych rozwiązań oparta na normach pozwoli na zastąpienie bezpośredniej kontroli ze strony administracji państwowej, umożliwi szybsze, bardziej efektywne i optymalne dostosowanie odporności podmiotów krytycznych na zagrożenia asymetryczne, terrorystyczne i te wynikające z *emerging risks* lub wiążące się z nimi.

W 2024 r. należy spodziewać się intensyfikacji działań hybrydowych mających źródło na wschodzie, ale też w innych regionach świata. To sprawia, że coraz pilniejsza jest potrzeba uporządkowania legislacyjnego nie tylko w odniesieniu do IK, lecz także w szerszym obszarze prawnym, obejmującym: *Ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia*, *Ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, *Ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* oraz *Ustawę z dnia 11 marca 2022 r. o obronie Ojczyzny*.

Adam Tatarowski

Dyrektor Zakładu Rozwoju Technicznej Ochrony Mienia „TECHOM" Sp. z o.o. – wyspecjalizowanej jednostki certyfikującej

oraz placówki kształcenia ustawicznego. W jej ramach kształcą się m.in. osoby funkcyjne zajmujące się ochroną osób i obiektów w służbach mundurowych, pracownicy IK odpowiedzialni za bezpieczeństwo oraz usługodawcy realizujący projekty, instalacje i konserwacje systemów ochrony przeciwpożarowej i technicznych środków zapewnienia bezpieczeństwa fizycznego. Autor jest specjalistą w zakresie oceny zgodności technicznych środków zapewnienia bezpieczeństwa fizycznego (i usług w tym obszarze), ekspertem Komitetów Technicznych nr 52, 264, 306 i 323 w Polskim Komitecie Normalizacyjnym.

Kontakt: tatarowski@techom.com