wiadomości PKN

NORMALIZACJA

2/2026

2/2026

3 OD REDAKCJI

AKTUALNOŚCI

4 AI potrzebuje zasad. Międzynarodowe forum normalizacyjne

10 Forum Bezpieczeństwa Scenicznego na Politechnice Wrocławskiej

ZE ŚWIATA

12 Opieka zdrowotna – idealny cel dla cyberprzestępców

Z PRAC NORMALIZACYJNYCH

16 Zimowa odzież ochronna w pracy – jakie normy rzeczywiście się liczą?

ORGANY TECHNICZNE – STYCZEŃ

POLSKI KOMITET NORMALIZACYJNY

„**WIADOMOŚCI PKN**" to miesięcznik elektroniczny publikowany cyklicznie na stronie internetowej PKN www.pkn.pl od numeru 9/2011.

ZESPÓŁ REDAKCYJNY
Redaktor prowadzący:
Joanna Skalska – tel. 22 556 74 62
Redaktorzy:
Marta Hejduk – tel. 22 556 77 09
Wiktoria Pomorska – tel. 22 556 76 48
Skład:
Oskar Sztajer – tel. 22 556 77 62
Piotr Jotel – tel. 22 556 75 98

REDAKCJA:
skr. poczt. 411, 00-950 Warszawa 1
e-mail: redakcja@pkn.pl

WYDAWCA:
Polski Komitet Normalizacyjny, ul. Świętokrzyska 14, 00-050 Warszawa

Materiały publikowane w miesięczniku „Wiadomości PKN" są chronione prawami autorskimi. Ich kopiowanie i rozpowszechnianie (w całości lub części) wymaga zgody wydawcy, a cytowanie powołania się na źródło.

Artykuły publikowane w miesięczniku przedstawiają punkt widzenia Autorów i nie zawsze są tożsame z poglądami wydawcy. Redakcja zastrzega sobie prawo do adiustacji tekstów i zmiany tytułów. Materiałów niezamówionych redakcja nie zwraca. Redakcja nie ponosi odpowiedzialności za treść ogłoszeń.

© Copyright by Polski Komitet Normalizacyjny
Zdjęcia - Adobe Stock / PKN, okładka - © Vadym / Adobe Stock

Szanowni Czytelnicy!

Ochrona zdrowia to dziś jeden z najbardziej wrażliwych obszarów funkcjonowania państwa i gospodarki. Łączy w sobie technologię, dane, infrastrukturę krytyczną oraz – przede wszystkim – człowieka. Skala i dynamika zmian w tym sektorze sprawiają, że kwestia bezpieczeństwa nabiera wymiaru systemowego.

Cyberataki na placówki medyczne, rosnąca rola sztucznej inteligencji w diagnostyce, przetwarzanie ogromnych zbiorów danych wrażliwych – to rzeczywistość, która wymaga nie tylko zaawansowanych narzędzi technologicznych, lecz także jasnych i spójnych zasad działania. W artykule poświęconym cyberbezpieczeństwu w ochronie zdrowia przedstawiono, w jaki sposób Normy Międzynarodowe IEC oraz ISO/IEC wspierają budowanie odporności systemów, porządkują odpowiedzialność i pomagają ograniczać ryzyko w środowisku, w którym stawką jest zdrowie i życie pacjentów.

Kwestia zaufania do technologii została podjęta również w relacji ze Światowego Szczytu dotyczącego Międzynarodowych Norm Sztucznej Inteligencji. Debata o AI coraz wyraźniej przenosi się z poziomu ogólnych deklaracji na poziom konkretnych rozwiązań – interoperacyjności, zarządzania ryzykiem, ochrony praw człowieka oraz nadzoru nad systemami. Normy stanowią w tym kontekście wspólny punkt odniesienia, umożliwiający łączenie innowacyjności z odpowiedzialnością.

Ostatecznie to odpowiedzialność stanowi rdzeń poruszanych zagadnień. W świecie przyspieszających zmian technologicznych normy nie są dodatkiem do regulacji ani formalnym wymogiem. Stanowią uporządkowane, uzgodnione międzynarodowo ramy, które wspierają bezpieczne, przejrzyste i możliwe do zweryfikowania projektowanie oraz stosowanie rozwiązań.

Zapraszam do lektury
Joanna Skalska

fot. © Roisa / Adobe Stock

AI potrzebuje zasad

Międzynarodowe forum normalizacyjne

Rola Norm Międzynarodowych w skutecznym wdrażaniu sztucznej inteligencji

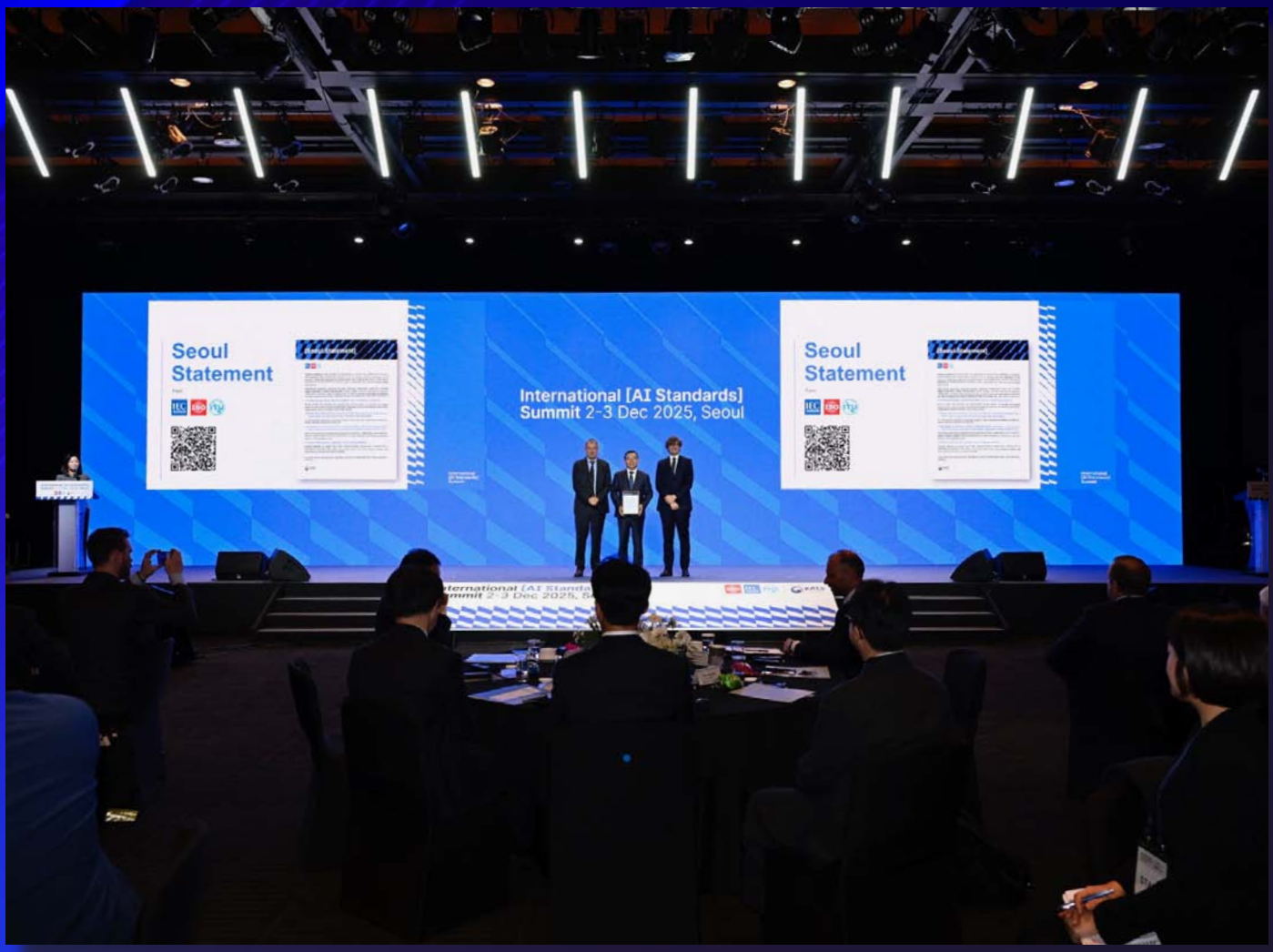
W dniach 2-3 grudnia 2025 r. odbył się Pierwszy Światowy Szczyt poświęcony międzynarodowej normalizacji w obszarze sztucznej inteligencji (AI) – International AI Standards Summit. Szczyt był wspólnym przedsięwzięciem trzech międzynarodowych organizacji normalizacyjnych: ISO (Międzynarodowa Organizacja Normalizacyjna), IEC (Międzynarodowa Komisja Elektrotechniczna) oraz ITU (Międzynarodowy Związek Telekomunikacyjny). Odbył się on przy wsparciu organizacyjnym Koreańskiej Agencji ds. Technologii i Norm (KATS), a także pod honorowym patronatem rządu Republiki Korei.

Międzynarodowe forum normalizacji AI

W wydarzeniu wzięło udział ponad 340 zaproszonych uczestników z 65 krajów. Wśród nich znaleźli się m.in.: przedstawiciele najwyższej kadry zarządzającej organizacji i firm odgrywających kluczową rolę w rozwoju sztucznej inteligencji, pionierzy technologiczni, reprezentanci instytucji państwowych i regulatorów kształtujących polityki wobec AI, liderzy środowisk akademickich, eksperci z instytucji normalizacyjnych i organizacji zarządzających jakością, a także przedstawiciele społeczeństwa obywatelskiego, organizacji międzynarodowych i agend Narodów Zjednoczonych. Kluczowe było zgromadzenie międzynarodowych interesariuszy o istotnym wpływie na globalną debatę, w celu omówienia i przyspieszenia rozwoju globalnych norm dotyczących sztucznej inteligencji.

Ze strony Polskiego Komitetu Normalizacyjnego w Szczycie uczestniczyła Ewelina Szczekocka – Przewodnicząca Komitetu Technicznego 338 ds. Sztucznej Inteligencji, która aktywnie brała udział w prelekcjach, panelach oraz interaktywnych Laboratoriach Wiedzy, umożliwiających wymianę doświadczeń i pogłębioną dyskusję na temat kluczowych wyzwań związanych z globalnym wdrażaniem technologii AI.

Szczyt promował interoperacyjność, zapewnienie przejrzystości oraz poszanowanie praw człowieka



fot. © ISO

w zastosowaniach technologii AI. Zainicjowany w jego ramach dialog ma zmierzać do zapewnienia lepszego zarządzania zastosowaniami AI i współpracy międzynarodowej w tym kluczowym obszarze normalizacji.

W miarę jak sztuczna inteligencja nieustannie zmienia oblicze przemysłu, biznesu i społeczeństw, co wielokrotnie podkreślano podczas obrad, Szczyt stanowił unikalną platformę analizy tej problematyki z perspektywy społeczno-technicznej. Umożliwił on dyskusję nad tym, w jaki sposób Normy Międzynarodowe mogą najskuteczniej zapewnić bezpieczeństwo, interoperacyjność, zrównoważony rozwój i odpowiedzialność we wdrażaniu i użytkowaniu technologii AI w skali światowej.

Uczestnicy Szczytu dyskutowali o roli Norm Międzynarodowych w rozwoju zastosowań sztucznej inteligencji. Wymieniano także doświadczenia z różnych obszarów zastosowania AI, koncentrując się na aspektach społecznych i zrównoważonym rozwoju zastosowań tej technologii.

Zwrócono uwagę, że wraz z pojawianiem się na całym świecie regulacji dotyczących AI, rośnie ryzyko fragmentacji wykorzystania technologii z tego obszaru, co może stwarzać przeszkody w zakresie współpracy dla rządów, społeczeństw, przedsiębiorstw.

Podkreślano rolę Norm Międzynarodowych jako praktycznego narzędzia, wspierającego dostosowywanie rozwiązań do regulacji w skali światowej, umożliwiającego metodyczne zarządzanie ryzykiem i ograniczanie jego wpływu na ludzi, a także budowanie zaufania do technologii AI i redukcję barier handlowych. Wskazano, że Normy Międzynarodowe stanowią solidne i spójne w skali globalnej podejście do projektowania i zarządzania systemami AI.

Oświadczenie Seulskie i globalny kontekst regulacyjny

Podczas inauguracji Szczytu po raz pierwszy zaprezentowano Oświadczenie Seulskie (Seoul Statement), opracowane wspólnie przez ISO, IEC oraz ITU. Dokument ten tworzy podstawy międzynarodowej

współpracy w zakresie rozwoju norm, proponując fundamentalne zasady i kierunki dalszych działań.

Rozpoczęta w ten sposób inicjatywa stanowi odpowiedź na cele Globalnego Paktu Cyfrowego (Global Digital Compact), przyjętego przez państwa ONZ jako element Paktu na rzecz Przyszłości. Realizuje ona również jedną z siedmiu kluczowych rekomendacji Organu Doradczego ONZ ds. Sztucznej Inteligencji, dotyczącą zwołania globalnego szczytu poświęconego normalizacji AI (rekomendacje opublikowane we wrześniu 2024 r. w raporcie Governing AI for Humanity).

Rangę tego spotkania podkreśla uczestnictwo między innymi kadry kierowniczej trzech międzynarodowych organizacji normalizacyjnych, w tym m.in.: Sung Hwan Cho – Prezydenta ISO, Jo Cops – Prezydenta IEC, Tomas Lamanauskas – Zastępcy Sekretarza Generalnego ITU, a także przedstawicieli WTO, WIPO i Rady Europy oraz globalnych firm technologicznych, takich jak Google, Microsoft, Huawei, Alibaba, Samsung czy LG.

Podczas ceremonii otwarcia Premier Republiki Korei Południowej Kim Min-seok podkreślił, że normy umacniają zaufanie i odpowiedzialność społeczności międzynarodowej oraz stanowią kluczowe kryteria zapewniające przejrzystość i bezpieczeństwo technologii AI.

Cztery kierunki globalnej normalizacji sztucznej inteligencji

Następnie Prezydenci ISO, IEC i Zastępca Sekretarza Generalnego ITU przedstawili Oświadczenie Seulskie w sprawie Sztucznej Inteligencji (AI) (ang. The Seoul Statement on Artificial Intelligence) – swoje pierwsze wspólne działanie mające na celu wdrożenie zaleceń ONZ. Oświadczenie przedstawia cztery główne kierunki globalnej normalizacji AI, ustanawiając wspólne zasady bezpiecznego i sprawiedliwego korzystania z rozwiązań z tego obszaru technologicznego.

1) Po pierwsze, normy AI powinny uwzględniać nie tylko aspekty techniczne, ale także szerszy wpływ technologii na ludzi, społeczeństwo i środowisko.

2) Po drugie, w ramach Norm Międzynarodowych AI, należy wzmocnić zabezpieczenia chroniące prawa człowieka – w szczególności przed zagrożeniami, takimi jak naruszenia prywatności i dyskryminacja.

3) Po trzecie, normy AI muszą być sprawiedliwymi i wiarygodnymi normami globalnymi, opracowywanymi przy udziale rządów, przedsiębiorstw, naukowców i społeczeństwa obywatelskiego, a nie kształtowanymi przez pojedynczy kraj lub wyłączną grupę ekspertów.

4) Po czwarte, partnerstwa publiczno-prywatne powinny poszerzać edukację i szkolenia w zakresie AI, aby pomóc w zmniejszeniu różnic w wykorzystaniu AI między krajami i społeczeństwami, umożliwiając wszystkim skuteczne przygotowanie się do ery AI.

Oświadczenie stanowi wspólną wizję i zobowiązania dotyczące sposobu wspierania przez Normy Międzynarodowe rozwoju i wdrażania godnych zaufania systemów AI, przynoszących korzyści społeczeństwu, wpływających pozytywnie na jego dobrostan, napędzających innowacje i chroniących prawa podstawowe. Uznaje ono transformacyjny wpływ AI na społeczeństwo oraz wagę odpowiedzialnego podejścia do sposobu wdrażania i zarządzania AI.

W kolejnych wystąpieniach:

- Kim Dae-ja – Prezes KATS zwrócił uwagę, że „normy AI to coś więcej niż specyfikacje techniczne. Stanowią one podstawę zaufania, które umożliwia ludziom bezpieczne korzystanie z AI". Wspomniał również o dążeniu Korei do bycia globalnym centrum normalizacji AI;
- dr Sung Hwan Cho – Prezydent ISO podkreślił, że „AI ma potencjał, aby przynieść ogromne korzyści ludziom i gospodarkom na całym świecie". Aby jednak zapewnić "sprawiedliwe i odpowiedzialne wykorzystanie tego potencjału", niezbędne jest stosowanie Norm Międzynarodowych i zaangażowanie we wzmacnianie współpracy między organizacjami normalizacyjnymi w celu opracowania odpowiednich, solidnych i zorientowanych na człowieka norm, które będą stanowić wytyczne dla odpowiedzialnego projektowania i wykorzystywania technologii AI";
- Jo Cops – Prezydent IEC zwrócił uwagę na fakt, że „szybki rozwój sztucznej inteligencji potwierdza podstawową prawdę: technologia zawsze dotyczy ludzi". Jednocześnie, wobec stawania się sztucznej inteligencji centralnym elementem globalnej gospodarki, podkreślił pilną potrzebę opracowania ram, które będą towarzyszyć ludziom. Według Prezydenta IEC „to wspólne zobowiązanie podkreśla wartość Norm Międzynarodowych jako wzorca bezpiecznego, godnego zaufania i zorientowanego na ludzi rozwoju sztucznej inteligencji";

fot. © ISO

fot. © ISO

- Seizo Onoe – Dyrektor Biura Normalizacji Telekomunikacji ITU stwierdził, że „normy to narzędzia techniczne służące do podtrzymywania zasad, którymi chcemy się kierować". Natomiast wizja przedstawiona w Oświadczeniu Seulskim wymaga „zróżnicowanej wiedzy specjalistycznej i globalnego zaangażowania we współpracę i konsensus", głównego napędu prac nad normami, które są niezbędnym narzędziem.

Prace merytoryczne Szczytu: panele, laboratoria i zastosowania AI

Szczyt obejmował również szereg sesji roboczych, w tym panele dyskusyjne i Laboratoria Wiedzy, poświęcone zagadnieniom takim jak skuteczne mechanizmy zarządzania wdrażaniem AI, czynniki wpływające na osiągnięcie masowej skali rozwoju zastosowań czy krajowe infrastruktury zarządzania technologiami AI. Omawiano rolę sztucznej inteligencji i norm AI w transformacji kluczowych sektorów, m.in.: globalnych łańcuchów dostaw i handlu, finansów, rolnictwa, energetyki, ochrony zdrowia, automatyzacji przemysłowej, transportu i mobilności oraz telekomunikacji.

Podczas jednego z paneli nt. wspólnego kształtowania odpowiedzialnej sztucznej inteligencji (ang. Shaping Responsible AI Together), Bjørn Berge – Zastępca Sekretarza Generalnego Rady Europy zwrócił uwagę, że Oświadczenie Seulskie odzwierciedla stanowisko Rady Europy: stosowanie sztucznej inteligencji w dobrym celu oraz konieczność współpracy wszystkich interesariuszy dla zapewnienia właściwego wykorzystania AI, w szczególności nienaruszającego praw człowieka, demokracji i praworządności.

W tym kontekście przywołano Ramową Konwencję Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności, przedstawioną do podpisu w 2024 r. jako pierwszy wiążący traktat międzynarodowy, którego celem jest zakotwiczenie tych wspólnych norm w prawie międzynarodowym. Została ona już do tej pory podpisana przez wiele państw, w tym Stany Zjednoczone, Kanadę, Japonię i Urugwaj (traktat ten jest otwarty także dla państw niebędących członkami Rady Europy), jest obecnie na etapie ratyfikacji.

Bjørn Berge mówił również o metodologii HUDERIA opracowanej przez Radę Europy w 2024 r., wspierającej praktyczne stosowanie Konwencji Ramowej. Metodologia ta zapewnia wytyczne i ustrukturyzowane podejście do oceny ryzyka i wpływu systemów sztucznej inteligencji. Została ona opracowana specjalnie z myślą o ochronie i promowaniu praw człowieka, demokracji i praworządności. Może być stosowana zarówno przez podmioty publiczne, jak i prywatne, jako wsparcie w identyfikacji i przeciwdziałaniu zagrożeniom (i ich skutkom) dla praw człowieka, demokracji i praworządności w całym cyklu życia systemów AI. „Ramowa Konwencja Rady Europy o sztucznej inteligencji" wraz z metodologią HUDERIA stanowią kluczowy pomost między prawami człowieka a normami technicznymi na całym świecie.

Rada Europy ściśle współpracuje z Biurem Narodów Zjednoczonych ds. Technologii Cyfrowych i Nowych, Programem Narodów Zjednoczonych ds. Rozwoju, OECD, UNESCO, a także ISO i innymi organizacjami normalizacyjnymi nad zapewnieniem spójności między ramami prawnymi a normami technicznymi.

W trakcie panelu pt. „Budowanie fundamentów globalnego zaufania do AI" (ang. Building Foundations for Global Trust in AI) rozważano wagę norm w budowaniu pomostu pomiędzy szeroko pojętymi regułami wykorzystania AI a praktycznymi implementacjami tej technologii. Poruszano m.in. rolę koncentrowania się na problemach na styku technologii i aspektów społecznych. W panelu uczestniczył Wael William Diab – Przewodniczący Komitetu Technicznego ISO/IEC JTC1/SC 42 ds. Sztucznej Inteligencji. Polski Komitet Normalizacyjny poprzez swoich ekspertów ściśle współpracuje z Komitetem Technicznym SC 42.

Laboratoria Wiedzy gromadziły ekspertów z różnych regionów i sektorów, celem których była wspólna analiza i dyskusja nad pytaniami nurtującymi świat, a dotyczącymi zagadnień na styku technologii, ich implementacji oraz aspektów społecznych.

Eksperci pochylili się m.in. nad analizą znaczenia norm we wspieraniu interoperacyjności i innowacyjności, a także zapewnianiu bezpieczeństwa rozwiązań AI i budowania zaufania do nich.

Omawiano znaczenie rozumienia zależności społeczno-technicznych we właściwym zastosowaniu sztucznej inteligencji, zapewniającym bezpieczeństwo i ochronę podstawowych prawa człowieka.

Szczegółowe zagadnienia poruszane w ramach Laboratoriów Wiedzy to m.in.:

- zarządzanie budowaniem zaufania do AI;
- normy stymulujące rozwój rynku;
- kontekst stosowania AI;
- budowa krajowych infrastruktur dla AI;
- zapewnienie jakości i integralności danych;
- promowanie praw człowieka;
- uwzględnianie wymiaru społeczno-technicznego;
- współpraca między społeczeństwami i sektorami;
- skalowanie możliwości stosowania technologii;
- przyszłe kierunki normalizacji.

Interaktywne sesje umożliwiły wymianę spostrzeżeń między przedstawicielami różnych regionów i branż na temat sposobów zwiększania bezpieczeństwa i zaufania użytkowników.

Istotnym punktem programu było wystąpienie jednego z kluczowych prelegentów, Matiego Bohacka – badacza z Google DeepMind i Uniwersytetu Stanforda pt. „Budowanie zaufania do mediów ery syntetycznej: zagrożenia, normy i drogi do odpowiedzialności".

Bohack omówił szybko rosnące wyzwania związane z fałszywymi informacjami (tzw. deepfake) i mediami

fot. © ISO

syntetycznymi, od dezinformacji i oszustw tożsamościowych po zagrożenia demokracji, a także podzielił się najnowszymi osiągnięciami w zakresie wykrywania i śledzenia pochodzenia oraz audytowalności modeli AI. Jego wystąpienie podkreśliło główne przesłanie Szczytu: zabezpieczenia techniczne muszą być połączone z solidnymi Normami Międzynarodowymi, aby zapewnić przejrzystość, autentyczność i rozliczalność rozwiązań w dobie generatywnej sztucznej inteligencji.

Reasumując, Szczyt koncentrował się na przejściu od zasad teoretycznych do praktyki, kładąc nacisk na zarządzanie, przejrzystość zastosowania technologii i nadzór przez człowieka. Dyskusje dotyczyły m.in. sposobów przekładania polityki na praktyczne wdrożenie technologii z pomocą norm.

Przedstawiono wizje rozwoju zastosowań AI i wzmocnienia wspólnego zaangażowania organizacji normalizacyjnych w promowanie Międzynarodowych Norm sztucznej inteligencji.

Szczyt, który odbył się pod hasłem „Normy kształtujące świat AI", podkreślił kluczową rolę Norm Międzynarodowych w zapewnianiu bezpiecznego i odpowiedzialnego korzystania z AI w przemyśle, administracji publicznej i społeczeństwie. W ciągu dwudniowego programu uczestnicy omówili strategiczne priorytety międzynarodowej normalizacji AI oraz globalny model współpracy.

Ewelina Szczekocka
Przewodnicząca PKN/KT 338 ds. Sztucznej Inteligencji

fot. © Luka / Adobe Stock

Forum Bezpieczeństwa Scenicznego na Politechnice Wrocławskiej

W dniach 19–20 stycznia 2026 roku, w murach Politechniki Wrocławskiej, odbyło się Forum Bezpieczeństwa Scenicznego – wydarzenie poświęcone kluczowym zagadnieniom związanym z bezpieczeństwem techniki scenicznej. Patronat Honorowy nad Forum objął Polski Komitet Normalizacyjny, podkreślając rangę i znaczenie poruszanej tematyki.

Organizatorami wydarzenia były: Agencja Bezpieczeństwa Maszynowego, Fundacja Scena Jutra oraz Katedra Akustyki, Multimediów i Przetwarzania Sygnałów Politechniki Wrocławskiej.

Partnerem wydarzenia była m.in. firma Mikor Inżyniering Sp. z o.o. – członek Komitetu Technicznego PKN/KT 320 ds. Technologii Widowiskowej.

Forum skierowane było przede wszystkim do dyrektorów instytucji kultury, kierowników technicznych, osób odpowiedzialnych za zamówienia publiczne, a także wszystkich zarządzających infrastrukturą sceniczną w obiektach widowiskowych. Dwudniowe spotkanie stanowiło przestrzeń do poszerzenia wiedzy z zakresu praktycznych aspektów bezpieczeństwa techniki scenicznej – zarówno w wymiarze prawnym, technicznym, jak i akustycznym. Prezentowane zagadnienia miały bezpośrednie znaczenie dla funkcjonowania teatrów, filharmonii oraz sal widowiskowych.

Uczestnicy Forum zapoznali się ze zmianami w Dyrektywach Nowego Podejścia, wymaganiami dotyczącymi urządzeń teatralnych obowiązującymi na terenie Unii Europejskiej oraz planowanymi zmianami dyrektywy maszynowej 2006/42/WE.

Program wydarzenia został podzielony na sześć bloków tematycznych. Pierwszy z nich dotyczył odpowiedzialności prawnej osób zarządzających obiektami kultury w kontekście posiadanego wyposażenia oraz jego wpływu na pracowników i użytkowników. W drugim bloku omówiono wymagania zasadnicze i minimalne wynikające z dyrektywy maszynowej. Trzeci blok poświęcono ochronie akustycznej obiektów widowiskowych, natomiast czwarty – zagadnieniom związanym z systemami bezpieczeństwa maszyn.

fot. Olga Pieniążek-Bylewska

fot. Olga Pieniążek-Bylewska

fot. Olga Pieniążek-Bylewska

W piątym bloku przedstawiono normę wieloczęściową PN-EN 17206 oraz proces opracowywania norm. Ostatni, szósty blok tematyczny koncentrował się na nowoczesnych rozwiązaniach dźwiękowych, w szczególności na aktywnej akustyce.

W gronie prelegentów znaleźli się m.in. Radosław Mikołajczyk, Przewodniczący PKN/KT 320 ds. Technologii Widowiskowej, który omówił normy wykorzystywane w branży widowiskowej, a także Piotr Kozłowski, reprezentujący Politechnikę Wrocławską oraz Pracownię Akustyczną Kozłowski. W swoim wystąpieniu przedstawił zagadnienia związane z ochroną akustyczną obiektów widowiskowych oraz zaprezentował nowoczesne rozwiązania dźwiękowe wykorzystywane podczas organizacji wydarzeń artystycznych. Proces powstawania norm oraz zagadnienia normalizacyjne w obszarze technologii widowiskowej przybliżyła Olga Pieniążek-Bylewska, konsultant PKN/KT 320 reprezentująca Sektor Produktów Powszechnego Użytku.

Forum Bezpieczeństwa Scenicznego było okazją do przekazania praktycznych informacji dotyczących obowiązujących przepisów prawa, skierowanych zarówno do użytkowników, jak i producentów maszyn. Spotkanie stworzyło również przestrzeń do dyskusji nad problematycznymi aspektami stosowania systemów bezpieczeństwa, interpretacji wymagań prawnych oraz oceną ryzyka, a także umożliwiło wymianę doświadczeń pomiędzy uczestnikami wydarzenia.

Olga Pieniążek-Bylewska
Sektor Produktów Powszechnego Użytku

fot. © Vadym / Adobe Stock

Opieka zdrowotna – idealny cel dla cyberprzestępców

Monica Heck

Cyberataki na szpitale i firmy z branży opieki zdrowotnej szybko ewoluują. Normy IEC zapewniają niezbędne wytyczne, które pomagają w ochronie tych instytucji.

Opieka zdrowotna to nowa linia frontu w wojnie cybernetycznej. Według badań przeprowadzonych wśród ponad 1000 organizacji związanych z opieką zdrowotną na całym świecie, w ciągu ostatnich 12 miesięcy niemal połowa z nich doświadczyła przynajmniej jednego incydentu związanego z bezpieczeństwem, który wymagał specjalnej reakcji ze strony zespołu ds. bezpieczeństwa. W 2025 r. na całym świecie wykryto blisko 75000 incydentów związanych z opieką zdrowotną, przy czym na czele znalazły się Stany Zjednoczone. Kolejne najczęściej atakowane kraje to Indie, Rosja i Wielka Brytania.

Od naruszeń bezpieczeństwa dokumentacji medycznej po ataki ransomware

Elektroniczna dokumentacja medyczna (electronic health records – EHR) to cyfrowa kopalnia złota zawierająca informacje dotyczące stanu zdrowia, diagnozy i rozliczeń, które składają się na tożsamość medyczną każdej osoby. Mogą być one sprzedawane w dark webie z różnych powodów, od kradzieży tożsamości po oszustwa ubezpieczeniowe i szantaż, co często ułatwia podwójne wymuszenia. W 2024 roku pojedyncza dokumentacja medyczna została sprzedana w dark webie za 250 dolarów, podczas gdy karty kredytowe osiągały cenę zaledwie 5 dolarów. W najgorszym przypadku cyberataki mogą sparaliżować placówki opieki zdrowotnej poprzez ataki typu ransomware, a przez to nawet zagrażać życiu pacjentów.

Rok 2024 był fatalny pod względem liczby osób, które doświadczyły naruszeń bezpieczeństwa dokumentacji medycznych: według niektórych raportów, w USA problem ten dotyczył ponad 80% populacji. W raporcie FBI dotyczącym przestępczości internetowej w 2024 r., opiekę zdrowotną uznano za sektor infrastruktury krytycznej o najwyższej liczbie zgłoszonych cyberzagrożeń, wynoszącej łącznie 444 incydenty, z czego 238 to ataki typu ransomware, a 206 to naruszenia bezpieczeństwa danych. Nie zadowalając się atakowaniem placówek świadczących bezpośrednią opiekę, takimi jak szpitale, hakerzy zwrócili także uwagę na peryferyjnych dostawców usług opieki zdrowotnej, w tym producentów urządzeń medycznych, dostawców usług rozliczeniowych w opiece zdrowotnej i firmy farmaceutyczne.

Atak ransomware na Change Healthcare na początku 2024 r. był przełomowym wydarzeniem, które ujawniło głębokie wady amerykańskiego ekosystemu opieki zdrowotnej. Od tamtego czasu, na całym świecie doszło do setek incydentów o różnej skali. Latem 2025 r. kradzież danych z holenderskiego programu badań przesiewowych w kierunku raka szyjki macicy doprowadziła do naruszenia bezpieczeństwa prawie pół miliona dokumentacji medycznych, natomiast w Wielkiej Brytanii doszło do śmierci pacjenta z powodu opóźnień będących skutkiem ataku typu ransomware na Synnovis – agencję zarządzającą laboratoriami dla funduszu NHS* i lekarzy w południowo-wschodnim Londynie.

Szpitale i placówki związane z opieką zdrowotną są atakowane częściej niż inne branże ze względu na dużą ilość cyfrowych danych narażonych na ataki oraz fakt, że świadczeniodawcy usług opieki zdrowotnej nie mogą narażać zdrowia pacjentów i odmówić zapłacenia okupu za np. ataki ransomware. Połączenie tych dwóch czynników sprawia, że placówki związane z opieką zdrowotną są idealnymi ofiarami. Ponadto, często nie inwestują w najnowsze narzędzia cyberbezpieczeństwa. Wreszcie, coraz powszechniejsze wykorzystywanie sztucznej inteligencji (AI) do diagnozowania i innych czynności medycznych tworzy własne słabe punkty.

Jak sztuczna inteligencja jest wykorzystywana w szwajcarskiej opiece zdrowotnej

Szwajcarski system opieki zdrowotnej nie jest odporny na cyberzagrożenia. Na początku 2025 r., raport przygotowany przez Narodowy Instytut Testów Cyberbezpieczeństwa (National Test Institute for Cybersecurity – NTC) wykazał 40 umiarkowanych lub poważnych luk w zabezpieczeniach trzech najczęściej używanych systemów informatycznych w szwajcarskich szpitalach. Następnie, w czerwcu 2025 r., szwajcarska organizacja non-profit zajmująca się promocją zdrowia i obsługująca różne urzędy federalne padła ofiarą ataku ransomware, w wyniku którego do dark webu trafiło 1,3 TB danych, w tym dokumentacja finansowa i komunikacja wewnętrzna.

W sierpniu 2025 r. 18 szwajcarskich grup zajmujących się opieką zdrowotną, w tym szpitale kantonalne i uniwersyteckie, założyło krajowe centrum cyberbezpieczeństwa, którego zadaniem jest zapewnienie systemów wczesnego ostrzegania przed cyberatakami. Było to mądre posunięcie, biorąc pod uwagę coraz częstsze wykorzystywanie sztucznej inteligencji do usprawnienia diagnostyki, personalizacji leczenia, zwiększania dostępności opieki zdrowotnej i poprawy sprawności operacyjnej. Chociaż sztuczna inteligencja jest coraz częściej wykorzystywana jako narzędzie w szwajcarskiej opiece zdrowotnej, pomaga też cyberprzestępcom w hakowaniu istniejących systemów.

Przykładów coraz częstszego wykorzystania sztucznej inteligencji w szwajcarskiej opiece zdrowotnej jest mnóstwo. W Genewie, publiczny szpital uniwersytecki (HUG) ogłosił niedawno utworzenie centrum sztucznej inteligencji skoncentrowanego na schorzeniach neurologicznych i psychiatrycznych. Natomiast w Bernie, grupa szpitali Insel Gruppe coraz częściej wykorzystuje sztuczną inteligencję w różnych obszarach, aby zwiększyć wydajność i skuteczność swoich działań. „AI nie jest wykorzystywane do podejmowania autonomicznych decyzji klinicznych. Służy ona wyłącznie jako narzędzie wspomagające pracowników opieki zdrowotnej w zapewnieniu optymalnej opieki nad pacjentami" – wyjaśnia Urs Meier, Dyrektor ds. zarządzania IT, ryzyka i zgodności. Dodaje, że AI to zarówno szansa, jak i potencjalne zagrożenie w podjętych działaniach na rzecz ochrony szpitali i usług medycznych przed cyberatakami.

Hakerzy też korzystają z AI

Pomimo obietnic związanych ze sztuczną inteligencją, branża opieki zdrowotnej w większości krajów wciąż pracuje w ramach lub równolegle do istniejących starszych systemów, które działają na przestarzałej infrastrukturze z lukami w zabezpieczeniach: np. portal Citrix, który nie posiadał uwierzytelniania wieloskładnikowego (multi-factor authentication – MFA) był winowajcą katastrofy w Change Healthcare.

Hakerzy wykorzystują asystentów AI lub duże modele językowe do koordynowania ataków, a integracja AI z placówkami medycznymi tworzy nowe wewnętrzne luki w zabezpieczeniach, które mogą wykorzystać cyberprzestępcy. „Korzystanie z zewnętrznych narzędzi AI zwiększa ryzyko wycieku krytycznych danych, co może stanowić również naruszenie prawa" – wyjaśnia Eugene Neelou, pracujący dla zlokalizowanej w San Francisco firmy zajmującej się cyberbezpieczeństwem. „Lokalne narzędzia AI wykorzystywane do uzyskania dostępu do wiedzy wewnętrznej, jak referencje medyczne i dane pacjentów, lub do przetwarzania obrazów medycznych również znacznie zwiększają pole ataku dla cyberprzestępców. Złośliwe wiadomości e-mail lub zaproszenia do kalendarza mogą zawierać pośrednie natychmiastowe ataki, które wykorzystują system AI ofiary, a publicznie dostępne chatboty z dostępem do danych wewnętrznych mogą zostać zmanipulowane w celu ujawnienia danych medycznych lub uzyskania dostępu do systemu back-end w celu dalszej 'eksploatacji'" – dodaje.

„Urządzenia oparte na sztucznej inteligencji mogą być manipulowane za pomocą złośliwych danych wejściowych, co może prowadzić do nadużyć ubezpieczeniowych. Ponadto, zainfekowane oprogramowanie i złośliwe aktualizacje mogą sabotować działania medyczne i skutkować błędnymi diagnozami na dużą skalę, potencjalnie prowadząc do śmiertelnych wypadków" – kontynuuje Neelou.

Przewiduje się, że Agentowa sztuczna inteligencja (Agentic AI) w przyszłości stworzy nowe słabe punkty

Szybkie wprowadzenie agentowej sztucznej inteligencji – autonomicznych "agentów" wchodzących w interakcje z wrażliwymi danymi i systemami bez udziału człowieka – również stanowi poważne zagrożenie. W październiku 2024 r., firma Gartner uznała agentową sztuczną inteligencję za główny trend technologiczny roku 2025 i przewidziała, że 33% aplikacji korporacyjnych będzie obejmować agentową AI do 2028 r. „Incydenty związane z niewłaściwym zachowaniem agentów pokazują, jak po uzyskaniu autonomii agenci AI mogą powodować problemy w środowiskach produkcyjnych, podejmować destruktywne działania lub pozwalać atakującym na przejęcie kontroli nad systemem" – wyjaśnia Neelou.

Chociaż w 2025 r. na całym świecie odnotowano znaczny wzrost liczby cyberataków z wykorzystaniem sztucznej inteligencji, nie odnotowano jeszcze żadnych naruszeń bezpieczeństwa w opiece zdrowotnej, które można bezpośrednio przypisać jej wykorzystaniu, ale według Neelou to tylko kwestia czasu. „Obecnie oprogramowanie ransomware jest wciąż zagrożeniem numer jeden, jednak przestępcy już teraz korzystają ze sztucznej inteligencji do wzmacniania swoich ataków" – wyjaśnia. „Ze względu na stan technologii bezpieczeństwa sztucznej inteligencji, prawdziwe i skuteczne ataki na AI prawdopodobnie przez długi czas pozostaną niewykrywalne. Najprawdopodobniej mają one miejsce już teraz, o czym zagrożone firmy nie mają pojęcia."

Jak normy mogą pomóc?

Według Neelou, nowe procesy oparte na sztucznej inteligencji wymagają specjalnych mechanizmów kontroli środowiska wykonawczego AI. „Dodanie sztucznej inteligencji do systemów zmniejsza ich bezpieczeństwo, ponieważ wiele słabych punktów AI jest nieodłączną cechą tych technologii. Tradycyjne rozwiązania zabezpieczające nie są w stanie sprostać tym wyjątkowym zagrożeniom związanym z AI – konieczne jest stosowanie specjalistycznych rozwiązań zabezpieczających sztuczną inteligencję. Tradycyjne zasady bezpieczeństwa są nadal aktualne, jednak wymagają ponownego przemyślenia w kontekście świata sztucznej inteligencji" – wskazuje.

Open Worldwide Application Security Project (OWASP), w którym uczestniczy firma Neelou, jest fundacją non-profit zajmującą się poprawą bezpieczeństwa oprogramowania. To otwarta społeczność, której celem jest umożliwienie organizacjom tworzenia, rozwijania, nabywania, obsługi i utrzymania aplikacji, którym można zaufać. Opracowywana jest także norma branżowa, która ma chronić przed błędami agentowej sztucznej inteligencji. A2AS: Agentic AI Security Framework ma na celu zdefiniowanie granic bezpieczeństwa, uwierzytelnianie monitów, stosowanie zasad bezpieczeństwa i niestandardowych polityk

oraz kontrolowanie zachowań agentów, umożliwiając zastosowanie strategii ochrony dogłębnej. Jest to również projekt open source, w który angażuje się wiele dużych firm technologicznych.

Międzynarodowe Normy IEC, takie jak ISO/IEC 27001 z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych, również odgrywają ważną rolę w kształtowaniu tego krajobrazu. IEC 62443 dotyczy w szczególności przemysłowych systemów automatyki i sterowania (industrial automation and control systems – IACS) wykorzystywanych w infrastrukturze krytycznej, w tym w opiece zdrowotnej. Podczas gdy bezpieczeństwo IT koncentruje się w równym stopniu na ochronie poufności, integralności i dostępności danych – tak zwana "triada C-I-A"** – w świecie technologii operacyjnej (operational technology – OT), najważniejsza jest dostępność. Priorytety środowisk OT koncentrują się na zdrowiu i bezpieczeństwie oraz ochronie środowiska. W przypadku sytuacji wyjątkowej, bardzo istotne jest, aby operatorzy szpitali otrzymywali dokładne i aktualne informacje oraz mogli szybko podjąć odpowiednie działania, takie jak odcięcie zasilania lub przełączenie się na sprzęt zapasowy w celu ochrony personelu lub pacjentów. Norma IEC 62443 zapewnia kompleksowe wytyczne dotyczące ochrony bezpieczeństwa, integralności, dostępności i poufności w IACS.

Długo oczekiwana czwarta edycja normy IEC 60601-1 zapowiedziana przez komitet techniczny IEC TC 62, zajmujący się normami z zakresu sprzętu medycznego, ma zostać ukończona latem 2029 r. Według eksperta TC 62, Ayuba Yancheshmeha, stanowi ona istotny krok naprzód w zakresie norm bezpieczeństwa urządzeń medycznych. „Po raz pierwszy wprowadza ona formalne wymagania z zakresu cyberbezpieczeństwa i sztucznej inteligencji, odzwierciedlając rosnącą złożoność połączonych i inteligentnych technologii medycznych".

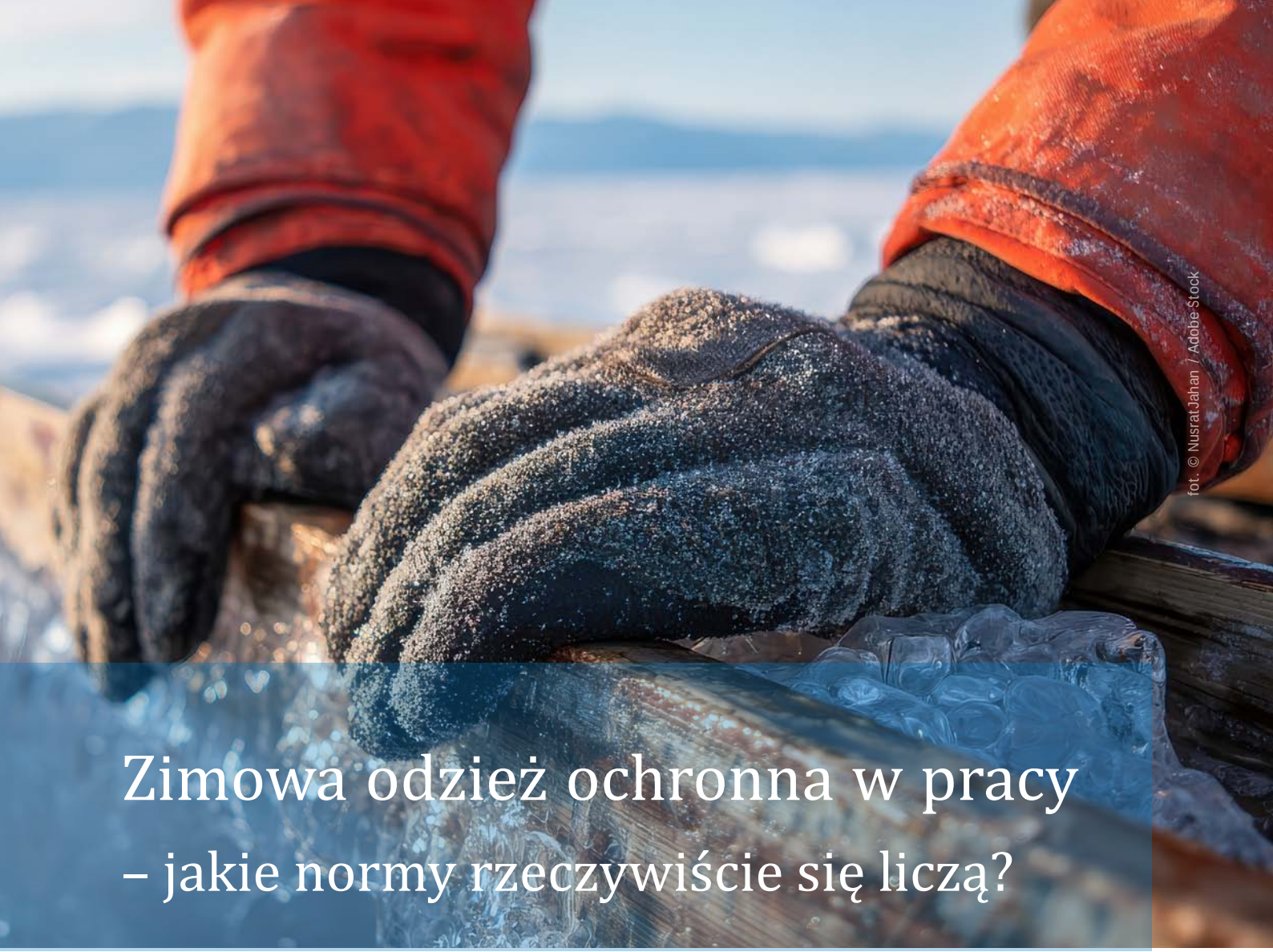
Ta aktualizacja normy IEC 60601-1 kładzie nacisk na zarządzanie ryzykiem cyberbezpieczeństwa poprzez wdrożenie modelowania zagrożeń, testowanie podatności na zagrożenia oraz zapewnienie bezpiecznych instrukcji integracji. Ochrona danych i integralność systemu są teraz uznawane za część podstawowej wydajności. Urządzenia wykorzystujące sztuczną inteligencję muszą także spełniać wymagania dotyczące przejrzystości, wykrywania stronniczości, weryfikacji wydajności i interakcji między człowiekiem a sztuczną inteligencją.

„Ponieważ modele sztucznej inteligencji są złożone i często nieprzejrzyste, subtelne manipulacje mogą zostać niezauważone, szczególnie w urządzeniach połączonych, które opierają się na aktualizacjach w chmurze lub danych zewnętrznych. Ta czwarta edycja odnosi się do tych zagrożeń, włączając modelowanie zagrożeń specyficznych dla sztucznej inteligencji, wymagając od producentów przewidywania sposobów niewłaściwego wykorzystania AI i tworzenia zabezpieczeń, takich jak walidacja danych wejściowych i wykrywanie anomalii" – dodaje Yancheshmeh.

Ponadto, TC 62 zajmuje się sztuczną inteligencją w dziedzinie medycyny poprzez swoją grupę doradczą Software Network and Artificial Intelligence (AG SNAIG). Obecnie trwają prace nad kilkoma projektami, m.in. nad pierwszą edycją normy IEC 63450, która dotyczy testowania urządzeń medycznych wykorzystujących sztuczną inteligencję/uczenie maszynowe. W związku z szybkim rozwojem sztucznej inteligencji i cyberzagrożeń oraz coraz częstszym wykorzystywaniem ich do ataków na szpitale, potrzeba wprowadzania norm cyberbezpieczeństwa w opiece zdrowotnej jest pilniejsza niż kiedykolwiek.

**NHS (national health system) – państwowa opieka zdrowotna*
***C-I-A – confidentiality, integrity, availability*

oprac. I.P.
na podstawie IEC e-tech, Issue 06/2025



fot. © NusratJahan / Adobe Stock

Zimowa odzież ochronna w pracy – jakie normy rzeczywiście się liczą?

Zima to szczególnie wymagający okres dla osób pracujących na zewnątrz, w nieogrzewanych halach czy chłodniach. Niska temperatura, wiatr, wilgoć oraz ograniczona widoczność nie tylko obniżają komfort pracy, lecz przede wszystkim wpływają na bezpieczeństwo. Właśnie dlatego zimowa odzież ochronna nie jest zwykłym ubraniem roboczym, ale elementem środków ochrony indywidualnej, którego jakość i właściwości są precyzyjnie opisane w europejskich normach.

Kluczowe w tym obszarze są normy zharmonizowane, które określają wymagania techniczne, metody badań oraz sposób znakowania odzieży ochronnej. Ubrania spełniające te wymagania mogą być oznakowane znakiem CE i stosowane jako sprzęt ochrony indywidualnej zgodnie z rozporządzeniem UE 2016/425. Dla użytkownika – pracownika lub pracodawcy – oznacza to, że dana kurtka czy kombinezon zostały obiektywnie przebadane, a ich właściwości nie są jedynie deklaracją producenta.

Najważniejszą normą odnoszącą się bezpośrednio do ochrony przed zimnem jest PN-EN 342. Dotyczy ona odzieży przeznaczonej do pracy w bardzo niskich temperaturach, zwykle poniżej –5°C. Norma ta obejmuje zarówno pojedyncze elementy garderoby, jak i kompletne zestawy odzieży, w tym kombinezony. W ramach badań oceniana jest izolacyjność cieplna odzieży, czyli jej zdolność do zatrzymywania ciepła wytwarzanego przez organizm. Analizuje się również przepuszczalność powietrza, ponieważ silny wiatr znacząco przyspiesza wychładzanie ciała. W niektórych przypadkach bada się także odporność na przenikanie wody, co ma duże znaczenie w warunkach śniegu, deszczu lub pracy na mokrym podłożu. Warto podkreślić, że norma PN-EN 342 nie wskazuje konkretnej temperatury, do jakiej odzież „gwarantuje ciepło", lecz posługuje się parametrami liczbowymi, które pozwalają specjalistom dobrać odzież do realnych warunków pracy i poziomu aktywności pracownika.

W sytuacjach, gdy warunki nie są aż tak ekstremalne, zastosowanie znajduje norma PN-EN 14058. Odnosi się ona do odzieży chroniącej przed umiarkowanym chłodem, najczęściej przy temperaturach powyżej –5°C. Tego typu ubrania są powszechnie wykorzystywane w magazynach, chłodniach, halach produkcyjnych oraz podczas pracy na zewnątrz w okresie jesienno-zimowym. Norma ta koncentruje się na oporze cieplnym materiału oraz jego właściwościach użytkowych, takich jak oddychalność czy ochrona przed wiatrem. PN-EN 14058 wypełnia więc lukę pomiędzy standardową odzieżą roboczą a pełnoprawną odzieżą chroniącą przed silnym mrozem.

Ochrona przed zimnem rzadko występuje w oderwaniu od innych zagrożeń, dlatego w praktyce bardzo często znaczenie mają również normy uzupełniające. Jedną z nich jest PN-EN ISO 13688, która określa ogólne wymagania dla odzieży ochronnej, takie jak ergonomia, nieszkodliwość materiałów, trwałość czy czytelne znakowanie. Jest to swego rodzaju fundament, na którym opierają się wszystkie pozostałe normy szczegółowe. W warunkach zimowych istotna bywa także norma PN-EN 343, dotycząca ochrony przed deszczem i wilgocią. Mokra odzież znacznie szybciej traci swoje właściwości termoizolacyjne, dlatego ochrona przed przenikaniem wody jest kluczowa dla zachowania ciepła. Z kolei w miesiącach zimowych, gdy dzień jest krótki, a widoczność często ograniczona przez mgłę lub opady śniegu, ogromne znaczenie ma norma PN-EN ISO 20471, regulująca wymagania dla odzieży o wysokiej widoczności.

Znaczenie normalizacji w przypadku zimowej odzieży ochronnej trudno przecenić. Długotrwałe wychłodzenie organizmu może prowadzić do hipotermii, spadku koncentracji oraz obniżenia sprawności manualnej, co bezpośrednio przekłada się na wzrost ryzyka wypadków. Normy pozwalają w sposób obiektywny ocenić, czy dana odzież rzeczywiście chroni użytkownika, a nie tylko sprawia wrażenie „ciepłej". Dla pracodawców stanowią one narzędzie do właściwego doboru wyposażenia, a dla pracowników – gwarancję, że używana odzież spełnia określone standardy bezpieczeństwa.

Zimowa odzież ochronna to znacznie więcej niż gruba kurtka czy ocieplane spodnie. To element systemu bezpieczeństwa pracy, zaprojektowany i przebadany zgodnie z zapisami konkretnych norm. PN-EN 342 znajduje zastosowanie w warunkach silnego mrozu, PN-EN 14058 sprawdza się przy umiarkowanym chłodzie, a normy takie jak PN-EN ISO 13688, PN-EN 343 czy PN-EN ISO 20471 uzupełniają ochronę o aspekty komfortu, braku wilgoci i dobrej widoczności. Świadomość ich istnienia i znaczenia pozwala lepiej zrozumieć, dlaczego odpowiednia odzież zimowa jest inwestycją w zdrowie i bezpieczeństwo, a nie jedynie dodatkiem do obowiązkowego wyposażenia pracownika.

Źródła:
*https://www.centexbel.be/en/knowledge-hub/depth-articles/ppe-standards/protective-clothing-against-cold?utm_*
https://hydrowear.eu/safety-norms/en-14058?utm
https://www.oxwork.com/en/cold-protective-clothes?utm
https://www.wmwitmar.pl/pl/i/Normy-odziezy-roboczej/19?utm

oprac. W. P.

ORGANY TECHNICZNE

fot. © comzeal / Adobe Stock

STYCZEŃ 2026

Komitety Techniczne

Zmiany zakresów tematycznych Komitetów Technicznych

- KT 341 ds. Technologii Kwantowych rozszerzył współpracę o ETSI/QT, Quantum Technologies

Nowi Przewodniczący Komitetów Technicznych

W styczniu Prezes PKN powołała na 4-letnią kadencję do pełnienia funkcji Przewodniczącego:

- w KT 26 ds. Wyrobów Włókienniczych mgr Agnieszkę Dałek reprezentującą Sieć Badawczą Łukasiewicz – Łódzki Instytut Technologiczny
- w KT 29 ds. Analiz Chemicznych Rud, Koncentratów i Metali prof. dra hab. inż. Andrzeja Wyciślika reprezentującego Politechnikę Śląską
- w KT 107 ds. Technicznych Wyrobów Włókienniczych dr inż. Ewę Witczak reprezentującą Sieć Badawczą Łukasiewicz – Łódzki Instytut Technologiczny
- w KT 214 ds. Wyrobów Bitumicznych i Polimerowych do Izolacji Wodochronnych w Budownictwie dr hab. inż. Barbarę Francke reprezentującą Szkołę Główną Gospodarstwa Wiejskiego w Warszawie

Nowi członkowie Komitetów Technicznych

W styczniu Prezes PKN powołała na członka KT następujące podmioty:

- Certicore Sp. z o.o. do KT 21 ds. Środków Ochrony Indywidualnej Pracowników
- Defor S.A. do KT 169 ds. Okien, Drzwi, Żaluzji i Okuć
- Heat Decor sp. z o. o. do KT 53 ds. Kabli i Przewodów
- Instytut Badawczy Dróg i Mostów do KT 17 ds. Pojazdów i Transportu Drogowego
- Marta Zdunek Doradztwo, Szkolenia, Audyty do KT 157 ds. Zagrożeń Fizycznych w Środowisku Pracy i KT 159 ds. Zagrożeń Chemicznych i Pyłowych w Środowisku Pracy
- Ministerstwo Energii do KT 316 ds. Ciepłownictwa i Ogrzewnictwa
- NORDPEIS Sp. z o.o. do KT 316 ds. Ciepłownictwa i Ogrzewnictwa

- Politechnikę Białostocką do KT 5 ds. Chłodnictwa, Pomp Ciepła, Klimatyzatorów i Sprężarek
- Politechnikę Lubelską do KT 212 ds. Budowy i Utrzymania Dróg
- Sempertrans Bełchatów Sp. z o.o. do KT 186 ds. Gumy i Wyrobów Gumowych
- supnetAI Krzysztof Supowicz do KT 338 ds. Sztucznej Inteligencji
- Uniwersytet Przyrodniczy w Lublinie do KT 93 ds. Mięsa, Jaj i ich Przetworów
- WITPOL Sp. z o.o. do KT 235 ds. Analizy Żywności
- Zakłady Badań i Atestacji ZETOM im. prof. Fryderyka Stauba w Katowicach Sp. z o.o. do KT 280 ds. Jakości Powietrza

Odwołani członkowie Komitetów Technicznych

W styczniu Prezes PKN odwołała z członkostwa w KT następujące podmioty:

- EU-Cert Sp. z o.o. z KT 128 ds. Projektowania i Wykonawstwa Konstrukcji Metalowych i Konstrukcji Zespolonych
- HONEYWELL Sp. z o.o. z KT 5 ds. Chłodnictwa, Pomp Ciepła, Klimatyzatorów i Sprężarek
- Milab Małgorzata Lewandowska z KT 157 ds. Zagrożeń Fizycznych w Środowisku Pracy i KT 159 ds. Zagrożeń Chemicznych i Pyłowych w Środowisku Pracy
- Orange Polska SA z KT 171 ds. Sieci Komputerowych i Oprogramowania
- ZF Automotive Systems Poland Sp. z o.o. z KT 17 ds. Pojazdów i Transportu Drogowego

Komitety Zadaniowe

Nowi członkowie Komitetów Zadaniowych

W styczniu Prezes PKN powołała do KZ następujące podmioty:

- Polskie Towarzystwo Medycyny Sądowej i Kryminologii do KZ 505 ds. Procesów Kryminalistycznych

Podkomitety Techniczne

Nowi członkowie Podkomitetów Technicznych

W styczniu Prezes PKN powołała do PK następujące podmioty:

- Politechnikę Lubelską do PK 2 ds. Asfaltów w KT 222 ds. Przetworów Naftowych oraz Produktów Podobnych Pochodzenia Biologicznego i Syntetycznego

SZKOLENIE ON-LINE PKN

System zarządzania sztuczną inteligencją według ISO/IEC 42001:2023

ZAGADNIENIA

- Wprowadzenie do zagadnień sztucznej inteligencji, systemu zarządzania i normy
- Kluczowe pojęcia i definicje dotyczące systemu zarządzania sztuczną inteligencją ISO/IEC 42001:2023
- System zarządzania sztuczną inteligencją
- Struktura normy ISO/IEC 42001:2023
- Wymagania normy ISO/IEC 42001:2023
- Wymagania i wytyczne wynikające z załączników do normy ISO/IEC 42001:2023

Dowiedz się więcej

wiedza.pkn.pl tel. 22 556 77 66 szkolenia@pkn.pl