wiadomości
• NORMALIZACJA •
PKN
1/2019

CYBERBEZPIECZEŃSTWO

1/2019

„**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
Aleksandra Kurzep – tel. 22 556 75 07
Skład:
Oskar Sztajer – tel. 22 556 77 62
Piotr Jotel - tel. 22 556 75 98

REDAKCJA:
00-950 Warszawa, skr. poczt. 411
ul. Świętokrzyska 14
e-mail: redakcja@pkn.pl

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

Szanowni Czytelnicy,

Internet Rzeczy z miliardami połączonych urządzeń i systemów stał się nieodłącznym elementem naszego życia. I dobrze. Inteligentne systemy sprawiają, że miasta, transport i krytyczna infrastruktura energetyczna są solidniejsze i wydajniejsze. Inteligentna technologia w budynkach i domach zapewnia efektywniejsze zużycie energii i wody oraz oferuje niepełnosprawnym i starzejącym się społeczeństwom niezależność niezbędną do wykonywania codziennych czynności w ich domach. Trzeba jednak pamiętać, że te same urządzenia są narażone na cyberataki. A to już jest poważny problem. W 2017 roku byliśmy świadkami rozprzestrzenienia się szkodliwego oprogramowania ransomware Wannacry. Efektem był paraliż wielu systemów szpitalnych. Zagrożone atakami mogą być też ratujące życie urządzenia wszczepiane pacjentom jak np. implanty mózgowe pomagające w chorobie Parkinsona. Cyberprzestępcy mogą na przykład zmienić ustawienia neurostymulatorów tak, aby zwiększyć napięcie sygnałów wysyłanych w trybie ciągłym do mózgu pacjenta. Może to spowodować nieodwracalne zmiany w mózgu pacjenta, a nawet zagrozić życiu.

A co z prywatnością gromadzonych danych? Kto jest ich właścicielem i jak je przetwarza?

To są problemy, z którymi trzeba się zmierzyć. W tym numerze piszemy, jak normy przyczyniają się do zwiększenia bezpieczeństwa cybernetycznego wielu branż.

Joanna Skalska

fot. © panandrii / Adobe Stock

Ochrona łańcuchów dostaw przed cyberatakami

Mike Mullane

Odporność cybernetyczna może zostać osiągnięta jedynie dzięki skupieniu się na technologii informacyjnej i operacyjnej

W ostatnich miesiącach w wielu badaniach i raportach podkreślano alarmujący wzrost liczby cyberataków na łańcuchy dostaw. Jedno z takich badań, przeprowadzonych w obu Amerykach, Azji i Europie, sugeruje, że w ostatnim roku dwie trzecie firm doświadczyło cyberataku na ich łańcuch dostaw.

Łańcuch dostaw to droga, jaką produkty i usługi muszą przejść od dostawcy do klienta. To system, który obejmuje organizacje, ludzi, działania, informacje i zasoby. Łańcuchy dostaw są szczególnie wrażliwe ze względu na ich złożone interakcje m.in. z działaniami zakładu, pracownikami, klientami i spedytorami. Trudno poznać te mechanizmy, nie mówiąc już o ich kontroli oraz procedurach bezpieczeństwa wykorzystywanych wzdłuż całego łańcucha.

Inną kwestią wskazaną przez raport Departamentu Obrony Stanów Zjednoczonych jest to, że bezpieczeństwo w przemyśle wytwórczym koncentruje się na usługach w chmurze, zarządzaniu danymi i innych rodzajach technologii informacyjnych (IT), jednocześnie nie uwzględniając bezpieczeństwa łańcucha dostaw, z których wiele działa na podstawie technologii operacyjnej (OT). Głównym problemem Pentagonu jest oczywiście amerykański przemysł obronny, ale kwestie uwzględnione w raporcie dotyczą wszystkich sektorów przemysłowych i infrastruktury krytycznej na całym świecie.

Cyberbezpieczeństwo IT i OT

Programy cyberbezpieczeństwa zbyt często bazują na rozwiązaniach IT. W rzeczywistości ograniczenia operacyjne w sektorach przemysłu takich jak produkcja, energetyka, ochrona zdrowia i transport oznaczają, że podejście zaadaptowane w kwestii cyberbezpieczeństwa wymaga zabezpieczenia OT.

IT koncentruje się głównie na danych i ich zdolności do swobodnego i bezpiecznego przepływu. Istnieje w świecie wirtualnym, w którym dane są przechowywane, pobierane, przesyłane i edytowane. IT jest płynny i ma wiele ruchomych części i bram, co czyni go podatnym na ataki. Obrona przed nimi polega na zabezpieczeniu każdej warstwy oraz ciągłym identyfikowaniu i korygowaniu słabości, aby zapewnić ciągłość przepływu danych.

OT przeciwnie, należy do świata fizycznego. Podczas gdy dział IT musi chronić każdą warstwę systemu, OT obejmuje utrzymanie kontroli nad systemami: włączania i wyłączania, zamykania lub otwierania. OT zapewnia poprawne wykonanie wszystkich działań. Wszystko w OT jest nastawione na fizyczny ruch i kontrolę urządzeń i procesów, aby system działał zgodnie z przeznaczeniem, ze szczególnym naciskiem na bezpieczeństwo i zwiększoną wydajność. Na przykład OT pomaga zagwarantować, że generator włącza się w tryb online, w sytuacji wzrostu zapotrzebowania na energię elektryczną lub że zawór przelewowy otwiera się, gdy zbiornik chemikaliów jest pełny, aby uniknąć wycieków niebezpiecznych substancji.

W przeszłości IT i OT miały odrębne role. Zespoły OT pracowały z zamkniętymi systemami zależnymi od fizycznych mechanizmów bezpieczeństwa zapewniającymi ciągłość działania. Wraz z pojawieniem się Przemysłowego Internetu Rzeczy (Industrial Internet of Things - IIoT) oraz integracją fizycznych maszyn z czujnikami i oprogramowaniem w sieci, granice między tymi dwoma technologiami zacierają się. Ponieważ coraz więcej obiektów łączy się, komunikuje ze sobą i wchodzi w interakcje, nastąpił wzrost liczby punktów końcowych i potencjalnych sposobów dostępu cyberprzestępców do sieci i systemów infrastruktury.

Ochrona łańcuchów dostaw

To prowadzi nas z powrotem do łańcuchów dostaw, skąd prawdopodobnie bierze się ogromna większość cyberprzestępstw. I znowu, istnieją istotne różnice pomiędzy IT i OT.

Łańcuch dostaw IT definiuje się jako „zbiór organizacji z powiązanymi zbiorami zasobów i procesami, z których każdy działa jako nabywca, dostawca lub obie te osoby, aby tworzyć kolejne relacje z dostawcami ustanowione w momencie złożenia zamówienia, podpisania umowy lub innej formalnej umowy zaopatrzeniowej".

Definicja łańcucha dostaw dla inteligentnych zakładów produkcyjnych obejmowałaby nie tylko IT, lecz także łańcuch dostaw OT. Dotyczy to osób (programistów, dostawców, sprzedawców i pracowników pracujących w OT) oraz procesów i produktów: elementów i systemów centralnych dla OT, takich jak automatyka przemysłowa i systemy kontroli (IACS), a także coraz częściej elementy Internetu Rzeczy (IoT).

W ochronie łańcucha dostaw kluczowe znaczenie ma zainstalowanie bezpiecznej technologii. Stara technologia jest poważnym problemem, zwłaszcza gdy zagrożone urządzenia stają się bramą do systemów kontroli przemysłowej lub kontroli nadzorczej i systemów gromadzenia danych (SCADA). Naukowcy niedawno korzystali z linii faksu, aby uzyskać dostęp do urządzeń sieciowych podłączonych do drukarki wielofunkcyjnej.

Znaczenie zarządzania ryzykiem

Bezpieczna technologia stanowi tylko część wyzwania; sama w sobie nie zapewni odporności. Najbezpieczniejsze podejście polega na zrozumieniu i zmniejszeniu ryzyka w celu zastosowania właściwej ochrony w odpowiednich punktach systemu. Dotyczy to zarówno IT, jak i OT.

Istotne jest, że ten proces jest ściśle powiązany z celami organizacyjnymi, ponieważ decyzje dotyczące ograniczeń mogą mieć poważny wpływ na działalność. Idealnie byłoby, gdyby proces bazował na podejściu systemowym angażującym interesariuszy z całej organizacji.

fot. © Alex / Adobe Stock

Gdy organizacja zrozumie system i określi, co jest wartościowe i potrzebuje największej ochrony, należy podjąć trzy kroki, aby poradzić sobie z ryzykiem i konsekwencjami ataku cybernetycznego:

- zrozumieć znane zagrożenia poprzez modelowanie zagrożeń i ocenę ryzyka;
- zająć się zagrożeniami i wdrożeniem ochrony za pomocą Norm Międzynarodowych odzwierciedlających najlepsze światowe praktyki;
- zastosować odpowiedni poziom oceny zgodności – testowanie i certyfikacja – wobec wymogów.

Podejście oparte na analizie ryzyka zwiększa zaufanie wszystkich zainteresowanych stron, demonstrując nie tylko stosowanie środków bezpieczeństwa uwzględniających najlepsze praktyki, lecz także skuteczne wdrożenie odpowiednich środków przez organizację.

Normy i ocena zgodności w ochronie łańcuchów dostaw

IEC opracowało wiele norm w celu ochrony infrastruktury przemysłowej i krytycznej, mające zastosowanie do wielu różnych sytuacji oraz wyspecjalizowanych norm, na przykład dla elektrowni jądrowych lub ochrony zdrowia. Jednocześnie IEC pracuje także nad oceną zgodności (CA) oraz globalnymi schematami certyfikacji poprzez grupy robocze (WG) powołane przez Radę ds. Oceny Zgodności (CAB) oraz Komitet ds. Zarządzania Certyfikacją (Certification Management Committee - CMC) w IECEE.

Oprócz grupy norm ISO/IEC 27000 obejmującej zarządzanie usługami IT oraz serii norm IEC 62443 horyzontalnych publikacji obejmujących przemysłowe sieci komunikacyjne oraz IACS, wiele komitetów (TC) i podkomitetów technicznych (SC) IEC opracowało normy, specyfikacje techniczne (TS) oraz wymagania dla poszczególnych sektorów.

IEC CAB powołało WG 17, aby prześledzić potrzeby rynku i ramy czasowe usług CA (globalnych schematów certyfikacji) dla produktów, usług, personelu i zintegrowanych systemów w obszarze cyberbezpieczeństwa. Nie obejmuje to automatyki przemysłowej, którą zajmuje się IECEE CMC WG 31. CAB WG 17 informuje również inne sektory przemysłu o ogólnym podejściu w zakresie cyberbezpieczeństwa przyjętym przez IECEE CMC WG 31 oraz jak może ono dotyczyć tych sektorów.

Głównym zadaniem IECEE CMC WG 31 jest „stworzenie wyjątkowego podejścia CA do serii norm IEC 62443". W tym celu powstał OD-2061 opublikowany w czerwcu 2018 roku przewodnik *Operational Document* (Dokument Operacyjny), opisujący jak ocena zgodności może być wykorzystywana i stosowana wobec niektórych norm z serii IEC 62443.

OD-2061 wyjaśnia również, pod jakimi warunkami można uzyskać IECEE *Cyber Certificates of Conformity – Industrial Cyber Security Capability*. Certyfikaty są ważne tylko gdy „podpisze je uznane Laboratorium Certyfikujące oraz dołączone do certyfikatu wydanego przez krajową jednostkę certyfikującą (NBC – National Certification Body)".

Obecnie te certyfikaty są określone dla następujących ocen, z których każda ma zastosowanie do jednej lub więcej norm z serii IEC 62443:

- wydajności produktu (*Product capability*);
- wydajności procesu (*Process capability*);
- możliwości zastosowania produktu (*Product application of capabilities*);
- możliwości zastosowania procesów (*Process application of capabilities*);
- możliwości zastosowania rozwiązań (*Solution application of capabilities*).

Wraz z normami IEC obejmującymi bezpieczeństwo cybernetyczne niedawne wprowadzenie kompleksowych systemów certyfikacji CA powinno zapewnić lepszą ochronę systemów bazujących na przemysłowych sieciach komunikacyjnych oraz IACS (w tym łańcuchów dostaw) przed cyberzagrożeniami.

Źródło: IEC e-tech magazine, Issue 6/2018
Tłum. I. P.

Jak bezpieczne jest twoje urządzenie medyczne?

Antoinette Price

Dynamicznie rozwijający się przemysł

Rozwój połączonych przenośnych urządzeń medycznych, *wereables* (urządzeń do noszenia) i aplikacji oraz implantów rozwija się dzięki pojawieniu się Internetu Rzeczy (IoT) i zaawansowaniu w rozwoju sztucznej inteligencji (AI).

Producenci muszą więc bezwzględnie zagwarantować, że urządzenia te będą zabezpieczone przed cyberatakami, zachowując przy tym prywatność wszystkich danych osobowych, które gromadzą, przechowują i udostępniają operatorom i usługodawcom opieki zdrowotnej.

Światowy rynek inteligentnych urządzeń medycznych błyskawicznie rośnie, do 2025 r. osiągnie 24,46 mld USD, jak wynika z raportu Grand View Research.

Rola norm

Od 1968 r. IEC opracowuje Normy Międzynarodowe dot. bezpieczeństwa i wydajności urządzeń elektrycznych stosowanych w praktyce medycznej. Seria IEC 60601 obejmuje szerokie spektrum medycznych urządzeń elektrycznych, systemów i domen. Normy są opracowywane przez ekspertów z branży medycznej, przemysłu, zakładów opieki zdrowotnej, informatyki i oprogramowania oraz organów regulacyjnych.

Michael Appel, anestezjolog i szef Patient Safety Officer w Northeast Georgia Health System, przewodniczy pracom IEC w tej dziedzinie, mówi o wyzwaniach, przed którymi stoi branża medyczna. Musi ona przestrzegać coraz większej liczby przepisów dotyczących aspektów bezpieczeństwa sprzętu i systemów medycznych:

„Cyberbezpieczeństwo i prywatność danych osobowych to najważniejsze zagadnienia, które należy rozwiązać. W USA bardzo rygorystyczne przepisy dotyczące prywatności i prawa, takie jak RODO w UE, mogą utrudniać gromadzenie tak dużej ilości danych. Należy wypracować odpowiednie rozwiązania w tej kwestii, a kolejne ważne pytanie, na które musimy znaleźć odpowiedź to: kto jest właścicielem danych zgromadzonych przez te urządzenia?".

Od transportu i zakwaterowania po magazynowanie i dystrybucję towarów firmy technologiczne zmieniają sposób działania różnych branż dzięki innowacyjnym oprogramowaniom, które oferują nowe sposoby prowadzenia działalności.

„Jeśli nie będziemy szybsi, nowi gracze wejdą do branży, zakłócą ją i zrobią to, czego wymaga rynek. Już teraz mówi się o kompletnej reorganizacji całej branży urządzeń medycznych i opieki zdrowotnej przez podmioty, które nie są uważane za klasyczne firmy medyczne. Te duże firmy technologiczne wymyślą sposób wykorzystania danych, tradycyjnie uważanych za obszar opieki zdrowotnej, więc jeśli nie przyznamy, że rewolucja odbywa się na naszych oczach i nie dostosujemy się do niej, tak się stanie".

Zmieniająca się globalna demografia

Światowa demografia się zmienia. Z danych WHO wynika, że w ciągu nadchodzących 35 lat liczba osób 60+ w skali światowej wzrośnie niemal o sto procent: z dotychczasowych 900 mln do ok. 2 mld. Co ciekawe, populacja osób starszych będzie większa niż liczba dzieci do lat pięciu. Dodatkowo już wkrótce 80 proc. starszych osób stanowić będą mieszkańcy państw o niskich płacach i średnich dochodach. Starzejące się populacje, obniżające się współczynniki płodności, zwiększona średnia długość życia i coraz częstsze występowanie chorób przewlekłych stanowią poważne wyzwania dla rządów, które muszą wdrażać polityki w celu zaspokojenia potrzeb osób starszych, w tym mieszkalnictwa, zatrudnienia, ochrony socjalnej i opieki zdrowotnej.

fot. © panandrii / Adobe Stock

Medtech jest istotną częścią rozwiązania opieki zdrowotnej

Urządzenia medyczne odgrywają coraz ważniejszą rolę w odciążaniu opieki zdrowotnej, zmniejszając liczbę wizyt lekarskich i obniżając koszty. Przykładowo pacjenci mogą monitorować swoje parametry w czasie rzeczywistym i przesyłać te informacje do swoich placówek opieki zdrowotnej, gdzie zostanie podjęta decyzja, czy leczenie jest konieczne. Poprawiają one także jakość życia od aparatów słuchowych, aplikacji dla niedowidzących i mających wszczepiony rozrusznik serca, po implanty ortopedyczne i urządzenia do ciągłego monitorowania glukozy, które sprawdzają odczyty glukozy w czasie rzeczywistym i usprawniają leczenie niektórych postaci cukrzycy.

Inne szybko ewoluujące technologie sztucznej inteligencji, takie jak algorytmy, pomagają lekarzom poprawić diagnostykę i leczenie. Mogą być stosowane na oddziałach intensywnej terapii, gdzie uruchamiają w pełni autonomiczne systemy monitorujące pacjentów krytycznych, zastępując zespoły specjalistów.

Zapewnienie prywatności danych, ochrony i bezpieczeństwa w połączonym świecie

Nie ma bardziej osobistych i wrażliwych danych niż dane medyczne. Jeśli bezpieczeństwo inteligentnych urządzeń medycznych zostanie naruszone, może to być śmiertelne dla użytkowników. W tym kontekście seria norm IEC 80001, opracowana w celu zastosowania zarządzania ryzykiem w sieciach informatycznych zawierających urządzenia medyczne, oferuje także wskazówki dotyczące ujawniania i komunikowania potrzeb, zagrożeń i kontroli bezpieczeństwa urządzeń medycznych. Normy mogą być stosowane przez producentów urządzeń medycznych, a także wspierać organizacje dostarczające usługi opieki zdrowotnej z zarządzaniem ryzykiem w sieciach informatycznych za pomocą jednego lub więcej łączy bezprzewodowych.

Georg Heidenreich, koordynator Technical Regulations and Standardizations w Siemens Healthcare i przewodzący grupie IEC/ISO pracującej w szczególności nad bezpieczeństwem, ochroną i skutecznością oprogramowania medycznego, podkreśla specyficzne role i obowiązki związane z urządzeniami medycznymi: „Opracowane dokumenty będą obejmowały nowe rozwiązania, ale będą niezależne od konkretnych technologii. Niektóre obszary objęte są nową

architekturą: *fog* i *cloud* (architektura mgły i chmury) i aplikacjami w dziedzinie cyfrowego zdrowia, sztucznej inteligencji i analizy danych. Oczekujemy również przeprowadzenia kolejnej analizy strategicznej wymagań nowych technologii - w szczególności AI do końca pierwszego kwartału 2019".

Tworzenie zaufania poprzez testowanie i certyfikację

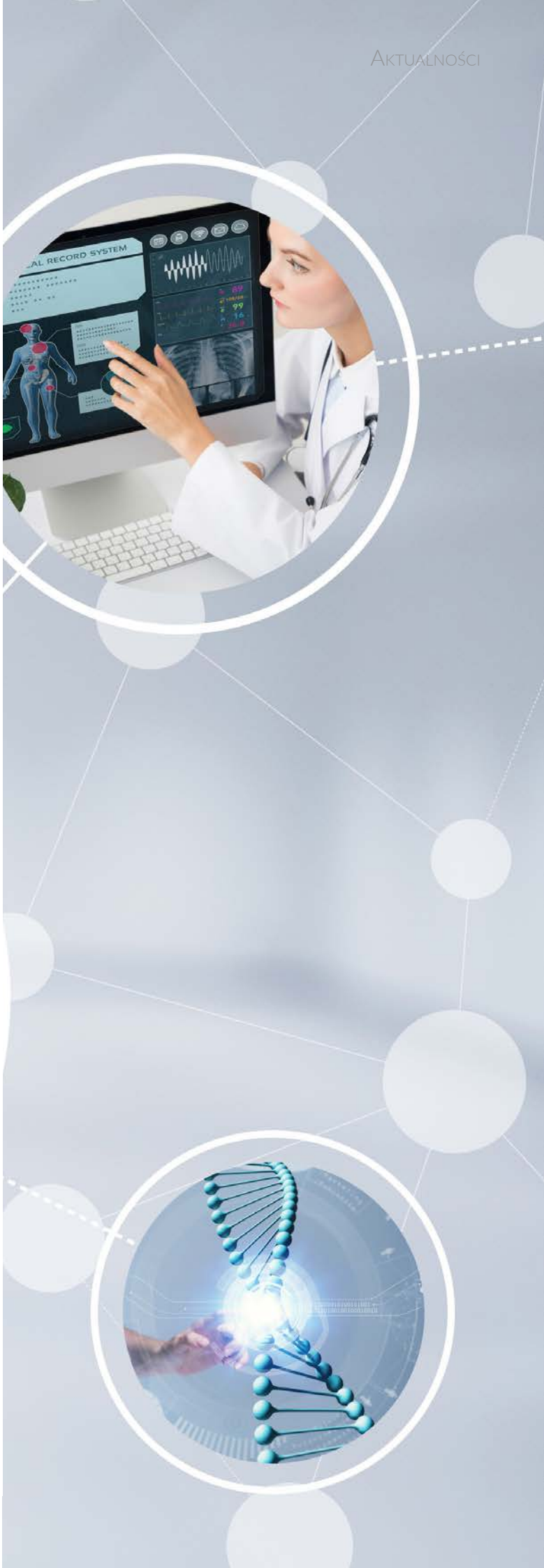
Ludzie będą niechętnie korzystać z technologii medycznej, jeśli nie będą mieć pewności, że jest to bezpieczne, a ich osobiste dane medyczne pozostaną prywatne. Jednym ze sposobów rozwiązania tego problemu jest testowanie i certyfikacja.

IECEE - system IEC zgodności badań i certyfikacji sprzętu elektrotechnicznego - zapewnia, że urządzenia i sprzęt elektryczny i elektroniczny spełniają oczekiwania pod względem wydajności, bezpieczeństwa, niezawodności i innych kryteriów, przez testowanie i certyfikację zgodnie z Normami Międzynarodowymi opracowanymi przez IEC.

System uwzględnia również ryzyko w odniesieniu do pacjentów, osób, które obsługują sprzęt - na przykład lekarzy, pielęgniarek i techników - oraz pracowników obsługi technicznej.

Ponieważ liczba inteligentnych urządzeń medycznych rośnie, to zarówno Rada ds. Oceny Zgodności IEC (CAB), jak i IECEE rozszerzyły zakres swoich działań o te związane z cyberbezpieczeństwem dla branży medycznej, aby zapewnić bezpieczeństwo użytkowników przed potencjalnymi zagrożeniami cybernetycznymi i ochronić ich dane wrażliwe.

Oprac. na podstawie www.iec.ch
IEC e-tech, Issue 6/2018
J. S.



fot. © exclusive-design / Adobe Stock

Jak zadbać o bezpieczeństwo dzieci?

Natalie Mouyal

Normy Międzynarodowe pomagają rodzicom w radzeniu z zagrożeniami ze strony inteligentnych zabawek

Jak co roku, w okresie przedświątecznym rodzice wyruszają na poszukiwania idealnego prezentu dla swoich pociech. Wyprawa do działu zabawek w każdym sklepie pokazuje, że wybór ten jest w zasadzie nieograniczony.

Inteligentne zabawki a nieoczekiwane niebezpieczeństwa

Od gier i lalek po modele samochodów i pluszowych misiów – współczesne zabawki nie różnią się znacząco od tych dostępnych poprzednim pokoleniom, poza jednym – połączeniem z Internetem. Lalki prowadzą rozmowy, pluszaki wysyłają wiadomości, a smartwatche pozwalają rodzicom zlokalizować ich dzieci. Gry mogą być wykorzystywane jako narzędzia edukacyjne poprzez wprowadzanie nowych umiejętności, takich jak kodowanie czy gra interaktywna.

Popularność zabawek z dostępem do Internetu rośnie. Według firmy Zion, zajmującej się badaniem rynku, światowy rynek inteligentnych zabawek, o wartości 3,87 mld USD w 2017 r., ma wzrosnąć do 5,41 mld USD do roku 2024. I nie tylko zakup inteligentnych zabawek napędza wzrost. Przewiduje się, że zakupy w aplikacji staną się głównym czynnikiem wzrostu w przypadku zabawek podłączonych do smartfonów.

Chociaż te zabawki mogą przynieść wiele korzyści, to ich zabezpieczenie pozostaje wątpliwe. Niektóre kraje ostrzegają konsumentów przed zagrożeniami związanymi z utratą prywatności.

W Niemczech urzędnicy rządowi zakazali sprzedaży mówiącej lalki podłączonej do Internetu, ponieważ można ją było łatwo zhakować i szpiegować dzieci. Niedawno naukowcy zajmujący się bezpieczeństwem odkryli, że do smartwatcha z opcją śledzenia lokalizacji, z którego korzystają tysiące dzieci, można się włamać i uzyskać dostęp do danych osobowych oraz możliwość śledzenia i podsłuchiwania użytkownika.

Rodzice powinni czuć się również zaniepokojeni faktem, że sporo nowoczesnych zabawek zbiera dane i udostępnia je producentom. Niektóre zabawki zbierają dane domyślnie i dla wielu osób nie jest jasne, w jaki sposób są one gromadzone, a tym bardziej, w jaki sposób są wykorzystywane. W Europie ogólne rozporządzenie o ochronie danych (RODO) nakłada rygorystyczne wymagania dotyczące gromadzenia, przechowywania i udostępniania danych osobowych. Jednak takie przepisy nie zostały wdrożone w innych częściach świata.

Normy Międzynarodowe mogą pomóc

Jak dalece rodzice mogą ufać producentowi w kwestii podjęcia przez niego środków niezbędnych do zabezpieczenia danych i prywatności? To właśnie zaufanie będzie determinować ich decyzję o zakupie urządzenia z dostępem do Internetu dla dziecka. Ale najpierw sami będą musieli dowiedzieć się więcej na temat tych produktów, żeby ustalić, czy producent wprowadził wystarczające zabezpieczenia.

Normy Międzynarodowe zawierają wymagania dotyczące gromadzenia, przechowywania i przetwarzania danych szczególnie chronionych w kontekście różnych wymogów prawnych. Producenci mogą korzystać z wielu norm dotyczących cyberbezpieczeństwa i ochrony danych, w tym dobrze znanej normy ISO/IEC 27000, opracowanej przez ekspertów ze wspólnego podkomitetu technicznego ISO/IEC *IT Security*. Normy identyfikują potencjalne zagrożenia i ułatwiają organizacjom wdrożenie odpowiedniej kontroli w celu ich ograniczenia. Zapewniają nie tylko kompletny zestaw narzędzi i metodologii zarządzania bezpieczeństwem danych, lecz także pokazują najlepsze praktyki wykorzystywane na rynku.

IEC utworzyła Komitet Doradczy ds. Bezpieczeństwa Danych i Poufności Danych (ACSEC), który opracowuje wytyczne dla wszystkich komitetów technicznych IEC w obszarach bezpieczeństwa informacji i prywatności danych, dzięki czemu wszystkie opracowywane normy uwzględniają kwestie cyberbezpieczeństwa. ACSEC na bieżąco śledzi i analizuje również działalność badawczą i trendy w środowisku akademickim. W czerwcu 2018 r. został opublikowany przewodnik IEC 120 zawierający wytyczne dotyczące zagadnień cyberbezpieczeństwa, które należy uwzględnić w publikacjach IEC, a także sposoby ich wdrożenia.

Chociaż inteligentne zabawki zawsze mogą być zhakowane, to stosowanie Norm Międzynarodowych jest ważnym krokiem w kierunku ochrony prywatności naszych dzieci.

Oprac. na podstawie www.iec.ch
IEC e-tech, Issue 6/2018
M. H.


PKN
ISO
praktyczny
przewodnik
dla MŚP
ISO 14001:2015
Systemy zarządzania środowiskowego

ISO 14001
– Praktyczny przewodnik dla MŚP

System zarządzania środowiskowego (SZŚ) jest narzędziem zarządzania umożliwiającym organizacji identyfikowanie i nadzorowanie wpływu działań, wyrobów i usług organizacji na środowisko; doskonalenie środowiskowych efektów działalności; wdrożenie systematycznego podejścia do ustalania i osiągania celów środowiskowych.

Natomiast norma ISO 14001 ułatwia wdrożenie tego systemu. Zawiera bowiem wymagania dotyczące systemu zarządzania środowiskowego, dzięki czemu ułatwia organizacji ustanowienie polityki i celów uwzględniających wymagania prawne i inne, do których spełniania organizacja się zobowiązała.

Według stanu na koniec 2014 r. ponad 324 000 organizacji na świecie było certyfikowanych na zgodność z ISO 14001. Dzięki wykorzystaniu systematycznego podejścia przyjętego w ISO 14001 wiele firm udoskonaliło swoje działania operacyjne przez zmniejszenie niekorzystnych wpływów swoich działań, procesów, wyrobów i usług na środowisko.

Ważne jest, że wdrożenie ISO 14001 może mieć miejsce w organizacji każdej wielkości lub każdego rodzaju, ponieważ wymagania SZŚ są takie same dla wszystkich, chociaż sposób wdrożenia będzie różny w zależności od wielkości i działalności organizacji.

Poradnik dla MŚP

Aby małe i średnie przedsiębiorstwa mogły skutecznie wdrożyć SZŚ z uwzględnieniem ich indywidualnych potrzeb i czerpać różnorodne korzyści, opracowano poradnik, który podaje praktyczne wskazówki. Wyjaśnia m.in. odpowiednie wymagania i techniki wdrażania systemu, uwzględnia również przydatne informacje na temat środowiska. Pozwala zrozumieć wymagania dotyczące systemu zarządzania środowiskowego, aby właściwie zidentyfikować obszary wymagające poprawy.

Korzyści

Korzyści z pozytywnego uwzględnienia czynników środowiskowych są związane nie tylko z ochroną środowiska, lecz także z wynikami biznesowymi i rentownością. Mogą one obejmować poprawę wizerunku firmy, rozszerzenie dostępu do rynków eksportowych, poprawę relacji z klientami, organami władzy, społecznością, innymi interesariuszami itp.

Polska wersja językowa poradnika jest dostępna w sklepie PKN.

A.K.

fot. © Vasyl / Adobe Stock

Czy suplementy diety sportowców są bezpieczne?

Można założyć, że odpowiednia i zróżnicowana dieta w normalnych warunkach będzie dostarczać konsumentom wszystkich substancji odżywczych niezbędnych do prawidłowego rozwoju i zachowania zdrowego stylu życia. Jeśli jednak to nie wystarcza, to konsumenci mogą zdecydować się na uzupełnianie spożycia substancji odżywczych suplementami żywnościowymi.

Substancje chemiczne stosowane jako źródło witamin i minerałów w produkcji suplementów żywnościowych powinny być bezpieczne i przyswajalne przez organizm, dlatego konieczne było stworzenie wykazu takich substancji. Mając to na uwadze, Parlament Europejski i Rada Unii Europejskiej przyjęły Dyrektywę 2002/46/WE Parlamentu Europejskiego i Rady z dnia 10 czerwca 2002 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do suplementów żywnościowych.

Zgodnie z tą dyrektywą „suplementy żywnościowe" oznaczają środki spożywcze, których celem jest uzupełnienie normalnej diety i które są skoncentrowanym źródłem substancji odżywczych lub innych substancji wykazujących efekt odżywczy lub fizjologiczny, pojedynczych lub złożonych, sprzedawanych w postaci dawek, a mianowicie w postaci kapsułek, pastylek, tabletek, pigułek i w innych podobnych formach, jak również w postaci saszetek z proszkiem, ampułek z płynem, butelek z kroplomierzem i tym podobnych postaciach płynów lub proszków przeznaczonych do przyjmowania w niewielkich odmierzanych ilościach jednostkowych, natomiast „substancje odżywcze" oznaczają witaminy i minerały.

Nawiązując do powyższych informacji, chciałabym skupić się na nowej grupie konsumentów związanych z rozwojem branży fitness oraz modą na aktywność fizyczną, która jest ukierunkowana na określony rodzaj żywności, w tym suplementy żywnościowe.

Niestety, różne badania wskazują, że produkty spożywcze dla tej grupy konsumentów – a w szczególności suplementy żywnościowe – mogą zawierać substancje dopingujące i w konsekwencji prowadzić do pozytywnych wyników w testach antydopingowych przeprowadzanych przez właściwe organy i wywoływać negatywne dla zdrowia skutki. Biorąc pod uwagę negatywny wpływ substancji dopingujących na zdrowie, żywność dla sportowców jest ważnym aspektem zdrowia publicznego, znacznie wykraczającym poza samych sportowców, w tym sportowców rekreacyjnych.

Przyłączając się do działalności organizacji, których celem jest zapewnienie wysokich standardów jakości w sektorze fitness i związanym z aktywnością fizyczną, Rada Techniczna CEN/BT od 12 grudnia 2016 r. do 14 maja 2017 r. uruchomiła wśród członków CEN głosowanie w sprawie francuskiej propozycji utworzenia nowego komitetu technicznego (CEN/TC) w zakresie żywienia i suplementacji kompatybilnej z zapobieganiem dopingowi - powołano CEN/TC 453 *Dietary supplements and sports food free of doping substances*. Pierwsze posiedzenie tego TC odbyło się we wrześniu 2017 r., a jego sekretariat umiejscowiono w AFNOR.

Zakres działania CEN/TC 453 obejmuje normalizację żywności dla sportowców i suplementów diety wolnych od substancji dopingujących, do spożycia przez osoby uprawiające sport w ramach zróżnicowanej i dobrze zbilansowanej diety. Suplementy żywnościowe są określone w ww. dyrektywie 2002/46/WE (wraz z późniejszymi zmianami), a substancje dopingujące znajdują się na liście zabronionych substancji Światowej Agencji Antydopingowej (WADA).

Współpraca z tym TC w PKN została przypisana do KT 200 ds. Koncentratów Spożywczych, Skrobi i Produktów Dietetycznych.

Dzięki wsparciu oferowanemu wspólnie przez CEN/TC 453 i zainteresowane strony przygotowano już pierwszy projekt normy, który ma być narzędziem pomagającym konsumentom w identyfikacji suplementów diety i żywności wolnych od substancji dopingujących: *Doping prevention in sport – Good development and manufacturing practices aimed at ensuring the absence of prohibited substances in food supplements and sports food* (Zapobieganie dopingowi w sporcie – Dobre praktyki rozwojowe i produkcyjne mające na celu zapewnienie braku substancji zabronionych w suplementach diety i żywności dla sportowców).

Niniejszy dokument określa wymagania dotyczące rozwoju i produkcji żywności i suplementów żywnościowych przeznaczonych dla sportowców z zamiarem skutecznego wykluczania żywności z substancjami zabronionymi przez Światową Agencję Antydopingową (WADA). Określa ramy dobrych praktyk w celu zapewnienia braku substancji zabronionych w sporcie w produktach przetworzonych wprowadzanych do obrotu. Nie uwzględniono w nim tak zwanych „napojów energetycznych". Dokument jest na etapie opiniowania w CEN/TC na poziomie „activation of Preliminary Work Item" – do 20 stycznia 2019 r.

Zapobieganie dopingowi opiera się na różnych ukierunkowanych akcjach. Jednym z działań zapobiegawczych jest zapewnienie uczestnikom zajęć sportowych suplementacji niezawierającej substancji dopingujących.

Alina Marczuk
Sektor Żywności, Rolnictwa i Leśnictwa
Sekretarz KT 200

fot. © nasakid12 / Adobe Stock

KT 5 ds. Chłodnictwa, Pomp Ciepła, Klimatyzatorów i Sprężarek

W 2018 r. w KT 5 opracowano polskie wersje językowe bardzo ważnych dla środowiska związanego z chłodnictwem dwóch części normy
PN-EN 378 Instalacje chłodnicze i pompy ciepła - Wymagania dotyczące bezpieczeństwa i ochrony środowiska:

- **Część 1: Wymagania podstawowe, definicje, klasyfikacja i kryteria wyboru;**
- **Część 2: Projektowanie, konstrukcja, badanie, znakowanie i dokumentowanie.**

W normie tej określono wymagania dotyczące bezpieczeństwa osób i mienia, dostarczono wskazówek w zakresie ochrony środowiska oraz określono procedury dotyczące działania, konserwacji i napraw instalacji chłodniczych oraz odzysku czynników chłodniczych.

Norma ma zastosowanie do nowych instalacji chłodniczych, części składowych, a także modyfikacji już istniejących systemów, również przeniesionych i obsługiwanych w nowym miejscu. Ma zastosowanie również w przypadku konwersji systemu na inny typ czynnika chłodniczego.

Normę stosuje się do:

- instalacji chłodniczych stacjonarnych lub przenośnych, wszystkich rozmiarów, z wyjątkiem systemów klimatyzacji pojazdów objętych szczegółową normą wyrobu, np. ISO 13043;
- pośrednich instalacji chłodzenia lub ogrzewania;
- lokalizacji instalacji chłodniczych;
- części wymienionych i części składowych dodanych po przyjęciu niniejszej normy, jeżeli nie są one identyczne.

W Części 1 w Załączniku C przedstawiono, w jaki sposób wyznaczyć ilość czynnika chłodniczego dozwoloną w danej przestrzeni, która po jej przekroczeniu wymaga dodatkowych środków ochronnych w celu zmniejszenia ryzyka. W Załączniku E określono kryteria bezpieczeństwa i ochrony środowiska różnych czynników chłodniczych stosowanych w chłodnictwie i klimatyzacji.

Część 2 ma zastosowanie do projektowania, konstrukcji i instalowania instalacji chłodniczych, w tym rurociągów, części składowych i materiałów. Określono w niej również wymagania dotyczące badania, uruchamiania, znakowania i dokumentacji. Wykluczone są wymagania dotyczące obiegów pośredniczących w wymianie ciepła, z wyjątkiem wszelkich wymagań ochronnych związanych z instalacjami chłodniczymi. Ta część obejmuje również wyposażenie pomocnicze, na przykład wentylatory, silniki wentylatorów oraz silniki elektryczne i zespoły skrzyni biegów w systemach ze sprężarkami otwartymi.

Warto wspomnieć, że Część 2 PN-EN 378 jest normą zharmonizowaną, związaną z dwiema dyrektywami nowego podejścia: dyrektywą 2006/42/EC Maszyny oraz 2014/68/EU Urządzenia ciśnieniowe, co gwarantuje, że spełnienie wymagań normy daje domniemanie zgodności z odpowiednimi zasadniczymi wymaganiami tych dyrektyw.

Prace nad tymi normami skłoniły KT 5 do odświeżenia terminologii z zakresu chłodnictwa, z czego najistotniejsza jest zmiana podejścia do tłumaczenia terminu „refrigerating", który do tej pory tłumaczony był jako „ziębnicze", a obecnie przyjęto formę „chłodnicze".

Warto zwrócić uwagę, że w br. opracowane będą polskie wersje językowe dwóch pozostałych części:

- Część 3: Usytuowanie instalacji i ochrona osobista
  oraz
- Część 4: Obsługa, konserwacja, naprawa i odzysk.

Część 3 tej najważniejszej normy chłodniczej określa wymagania związane z bezpieczeństwem instalacji, a w szczególności maszynowni. Budowanie instalacji chłodniczych pośrednich (główne elementy zawierające czynnik chłodniczy znajdują się w wyodrębnionej maszynowni) stanowi widoczny trend w branży chłodniczej. Niniejsza część precyzuje wymagania bezpieczeństwa w takich pomieszczeniach oraz wymagania bezpieczeństwa w zakresie ochrony osobistej obsługi pracującej w tych pomieszczeniach.

Część 4 natomiast wprowadza wymagania dotyczące obsługi, kontroli, utrzymania i demontażu urządzeń zawierających czynniki chłodnicze, które to czynności nabrały szczególnego znaczenia w związku z nowymi przepisami (m.in. dyrektywą gazową). Obejmuje również temat odzysku i przechowywania czynników chłodniczych.

Anna Zielonka
Sektor Maszyn i Inżynierii

ORGANY TECHNICZNE
grudzień 2018

Komitety Techniczne

Zmiany zakresu tematycznego Komitetów Technicznych

- **KT 276 ds. Zarządzania Bezpieczeństwem i Higieną Pracy** rozszerzył zakres o ISO/TC 283, Occupational health and safety management

Nowi Sekretarze Komitetów Technicznych

W grudniu Prezes PKN powołał do pełnienia funkcji Sekretarza

- w **KT 65 ds. Prób Środowiskowych Wyrobów Elektrycznych mgr Aleksandrę Wąsowską** z Polskiego Komitetu Normalizacyjnego

Nowi członkowie Komitetów Technicznych

W grudniu Prezes PKN powołał na członków KT następujące podmioty:

- **Eltrim Kable Sp. z o.o. do KT 80** ds. Ogólnych w Sieciach Elektroenergetycznych
- **Firma Doradcza ISOTOP S.C. A. Wilczyńska-Piliszek, S. Piliszek do KT 157** ds. Zagrożeń Fizycznych w Środowisku Pracy i **KT 159** ds. Zagrożeń Chemicznych i Pyłowych w Środowisku Pracy
- **Instytut Technologiczno-Przyrodniczy do KT 56** ds. Maszyn Elektrycznych Wirujących oraz Narzędzi Ręcznych i Przenośnych o Napędzie Elektrycznym
- **Politechnika Poznańska do KT 78** ds. Elektrotermii Przemysłowej
- **Stowarzyszenie Polskie Forum Zarządzania Bezpieczeństwem i Higieną Pracy ISO 45000 do KT 276** ds. Zarządzania Bezpieczeństwem i Higieną Pracy

Odwołania członków Komitetów Technicznych

W grudniu Prezes PKN odwołał z członka KT:

- **HASCO POLSKA Sp. z o.o**. z **KT 240** ds. Maszyn i Urządzeń do Przetwórstwa Tworzyw
- **Instytut Meteorologii i Gospodarki Wodnej - Państwowy Instytut Badawczy** z **KT 249** ds. Analizy Chemicznej
- **LZMO S.A.** z **KT 318** ds. Kominów
- **Ministerstwo Infrastruktury i Budownictwa** z **KT 297** ds. Informacji Geograficznej i **KT 307** ds. Zrównoważonego Budownictwa
- **Politechnikę Warszawską** z **KT 56** ds. Maszyn Elektrycznych Wirujących oraz Narzędzi Ręcznych i Przenośnych o Napędzie Elektrycznym
- **Stowarzyszenie Elektryków Polskich** z **KT 78** ds. Elektrotermii Przemysłowej

Podkomitety Techniczne

Nowi Przewodniczący Podkomitetów Technicznych

W grudniu Prezes PKN powołał na 4-letnią kadencję do pełnienia funkcji Przewodniczącego

- w **KT 277/PK 1 ds. Pomiarów i Oceny Jakości Paliw Gazowych dr inż. Elizę Dyakowską** reprezentującą Operatora Gazociągów Przesyłowych GAZ-SYSTEM S.A.

Nowi Sekretarze Podkomitetów Technicznych

W grudniu Prezes PKN powołał do pełnienia funkcji Sekretarza

- w **KT 277/PK 1 ds. Pomiarów i Oceny Jakości Paliw Gazowych Panią Marzenę Kwiecińską** reprezentującą Polskie Górnictwo Naftowe i Gazownictwo S.A.
- w **KT 277/PK 2 ds. Dystrybucji Paliw Gazowych Panią Marzenę Kwiecińską** reprezentującą Polskie Górnictwo Naftowe i Gazownictwo S.A.
- w **KT 277/PK 4 ds. Użytkowania Gazu Panią Marzenę Kwiecińską** reprezentującą Polskie Górnictwo Naftowe i Gazownictwo S.A.

Szkolenie

Podejście procesowe w normach ISO na przykładzie ISO 9001:2015

Szkolenie jest skierowane do kadry kierowniczej, pełnomocników ds. systemów zarządzania, specjalistów ds. systemów zarządzania, specjalistów ds. zarządzania procesami, właścicieli procesów oraz konsultantów i audytorów systemów.

Celem szkolenia jest nabycie umiejętności interdyscyplinarnego rozumienia i stosowania podejścia procesowego w ramach funkcjonowania systemów zarządzania opartych na wymaganiach norm serii ISO.

Szkolenie składa się z wykładów, warsztatów, ćwiczeń oraz dyskusji.

Zagadnienia:

- Cechy składowe procesów
- Architektura procesów
- Identyfikacja procesów
- Korelacje pomiędzy procesami
- Mapowanie procesów
- Modelowanie procesów
- Pomiar procesów
- Optymalizacja procesów
- Klient wewnętrzny
- Zarządzanie zmianą

Miejsce szkolenia:

Polski Komitet Normalizacyjny
ul. Świętokrzyska 14, Warszawa

Cena szkolenia:

490,00 zł netto; 602,70 zł brutto

Więcej szczegółów na stronie wiedza.pkn.pl

Kontakt: szkolenia@pkn.pl; tel. 22 55 67 766

POLSKI KOMITET NORMALIZACYJNY