wiadomości PKN

• NORMALIZACJA •

3/2021

3/2021

„**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!

Bakterie i wirusy są z nami od samego początku. To właśnie one pojawiły się na Ziemi jako pierwsze. Ich obecność jest kluczowa do zachowania prawidłowego funkcjonowania skóry, układu pokarmowego, oddechowego i odpornościowego. Ale 1% z nich stanowi dla nas zagrożenie. Na przestrzeni dziejów nawiedzały nas więc regularnie epidemie i pandemie. Do ok. połowy XX wieku występowały znacznie częściej niż w ciągu ostatnich 100 lat. Z jednej strony – dzięki rozpowszechnieniu zasad higieny i rozwojowi antyseptyki oraz farmakologii (antybiotyków i szczepionek). Jednocześnie z drugiej – powszechne stosowanie antybiotyków wzmogło lekooporność bakterii, ponadto zwiększyła się liczebność populacji i pojawiły się zdobycze technologiczne, dzięki którym podróżujemy daleko. Naukowcy więc od kilku lat przestrzegali przed globalną, dotkliwą pandemią. Czy wiecie, że w 2019 roku przeprowadzono co najmniej dwa projekty wspierane sztuczną inteligencją, których zadaniem była wizualizacja przebiegu globalnej epidemii, opracowanie i przetestowanie strategii działań? Dlaczego więc nie byliśmy gotowi na pandemię koronawirusa? Przestaliśmy bać się infekcji, naszym największym zagrożeniem stał się nowotwór.

Od początku globalnej pandemii COVID-19 przyspieszyła transformacja cyfrowa – świat nadal dostosowuje się do nowych sposobów życia, pracy, nauki i świadczenia najistotniejszych usług, takich jak opieka zdrowotna. W szybkim tempie wzrosło wykorzystanie nowych rozwiązań technologicznych, takich jak teleporady i wideokonsultacje. Algorytmy uczenia maszynowego, lepiej niż ludzie, odnajdują wzorce w dużych zbiorach danych, umożliwiając w ten sposób wczesne wykrywanie chorób i stanów takich jak rak, sepsa, zwyrodnienie plamki żółtej związane z wiekiem czy zawał. Mimo tych korzyści pojawiają się też obawy. Pacjenci muszą zaufać nowym technologiom wykorzystywanym przez pracowników opieki zdrowotnej do diagnozowania i leczenia, mając wciąż na uwadze bezpieczeństwo i poufność ich osobistych danych medycznych. O tym, jak normalizacja może wspomóc te kwestie, można przeczytać w tym numerze.

Życzę ciekawej lektury

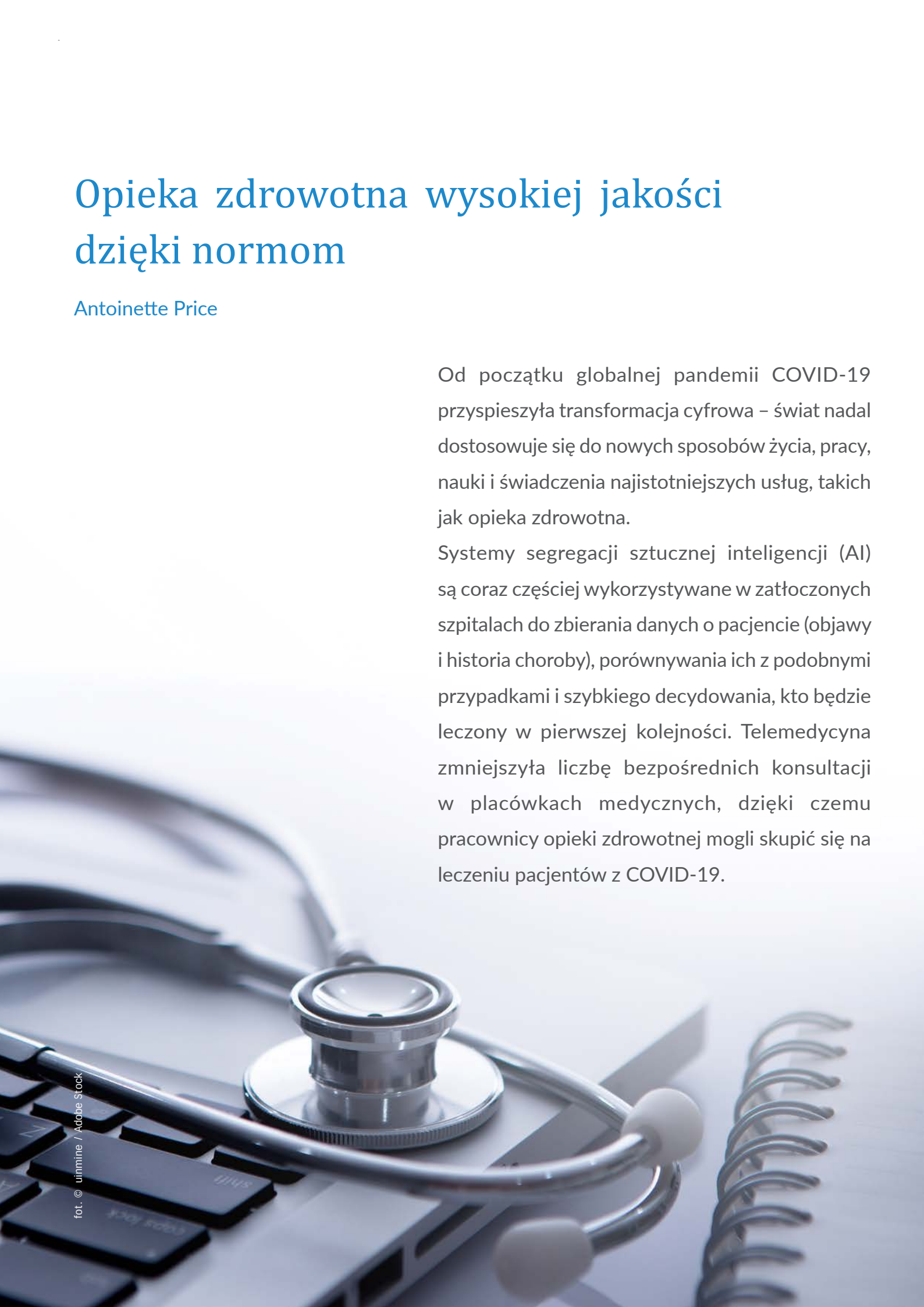
Joanna Skalska

Opieka zdrowotna wysokiej jakości dzięki normom

Antoinette Price

Od początku globalnej pandemii COVID-19 przyspieszyła transformacja cyfrowa – świat nadal dostosowuje się do nowych sposobów życia, pracy, nauki i świadczenia najistotniejszych usług, takich jak opieka zdrowotna.

Systemy segregacji sztucznej inteligencji (AI) są coraz częściej wykorzystywane w zatłoczonych szpitalach do zbierania danych o pacjencie (objawy i historia choroby), porównywania ich z podobnymi przypadkami i szybkiego decydowania, kto będzie leczony w pierwszej kolejności. Telemedycyna zmniejszyła liczbę bezpośrednich konsultacji w placówkach medycznych, dzięki czemu pracownicy opieki zdrowotnej mogli skupić się na leczeniu pacjentów z COVID-19.



fot. © uinmine / Adobe Stock

Technologie AI poprawiają opiekę zdrowotną, ale budzą też obawy

Algorytmy uczenia maszynowego, lepiej niż ludzie, odnajdują wzorce w dużych zbiorach danych, umożliwiając w ten sposób wczesne wykrywanie chorób i stanów takich jak rak, sepsa, zwyrodnienie plamki żółtej związane z wiekiem czy zawał. Oprócz zapewniania dokładniejszych diagnoz i lepiej dostosowanych do pacjenta metod leczenia, istnieje ogromny potencjał dla technologii AI w innych obszarach, takich jak patologia i prace laboratoryjne, w których ogromne zbiory danych pozostają niewykorzystane.

Mimo korzyści pojawiają się też obawy. Pacjenci muszą zaufać nowym technologiom wykorzystywanym przez pracowników opieki zdrowotnej do diagnozowania i leczenia, mając wciąż na uwadze bezpieczeństwo i poufność ich osobistych danych medycznych.

Oto niektóre z wyzwań, przed którymi stoją władze, organy regulacyjne, lekarze, świadczeniodawcy, ubezpieczyciele i pacjenci podczas postępującej cyfryzacji opieki zdrowotnej.

Georg Heidenreich, lider Wspólnej Grupy Roboczej IEC i ISO ds. skutecznego i bezpiecznego oprogramowania medycznego i systemów informatycznych w ochronie zdrowia, w tym tych obejmujących urządzenia medyczne, oraz Martin Meyer, przedstawiciel łącznikowy wspólnego komitetu IEC i ISO ds. sztucznej inteligencji w IEC/TC 62 ds. sprzętu elektrycznego w praktyce medycznej, odpowiadają, jak Normy Międzynarodowe mogą pomóc w rozwiązaniu tych problemów.

Jakie są kluczowe problemy związane z algorytmami w opiece zdrowotnej?

GH: Jak uczą się systemy AI? W jednym typie systemu algorytm jest szkolony z producentem, weryfikowany i wysyłany na rynek jako urządzenie medyczne ze znakiem CE (Certification Europe), co gwarantuje bezpieczeństwo. Ale nawet z tym systemem nie wiemy, dlaczego maszyna robi to, co robi; jej zachowanie nadal będzie pozostawało niejasne.

Co by było, gdyby systemy po wdrożeniu mogły uczyć się w sposób ciągły bez ograniczeń zakresu i jak byłyby kontrolowane? Amerykańska Agencja ds. Żywności i Leków (FDA) rozważa wprowadzenie ram regulacyjnych opartych na całym cyklu życia produktu dla urządzeń medycznych wykorzystujących sztuczną inteligencję i technologie uczenia maszynowego. Pozwoliłoby to na modyfikowanie na podstawie rzeczywistego uczenia się i adaptacji, przy jednoczesnym zapewnieniu bezpieczeństwa i wydajności oprogramowania jako urządzenia medycznego. Uruchomiła także Digital Health Center of Excellence, które ma na celu szybki przegląd, kategoryzację i wyodrębnienie najnowocześniejszych cyfrowych technologii medycznych w USA.

Najważniejsze są zbiory danych. Z jakiego typu danych zostały przeszkolone systemy AI i jakie są ograniczenia? Jeśli na przykład pacjent cierpi na rzadką chorobę, czy dane będą wystarczające do przeszkolenia systemu w rozpoznaniu takiej choroby i jak możemy uniknąć nieodłącznej stronniczości? Patrząc w przyszłość, jaką rolę odegrałby lekarz, gdy systemy AI będą coraz częściej stosowane i coraz bardziej zaawansowane? Czy wkład ludzki byłby wymagany w różnych punktach użytkowania takich systemów?

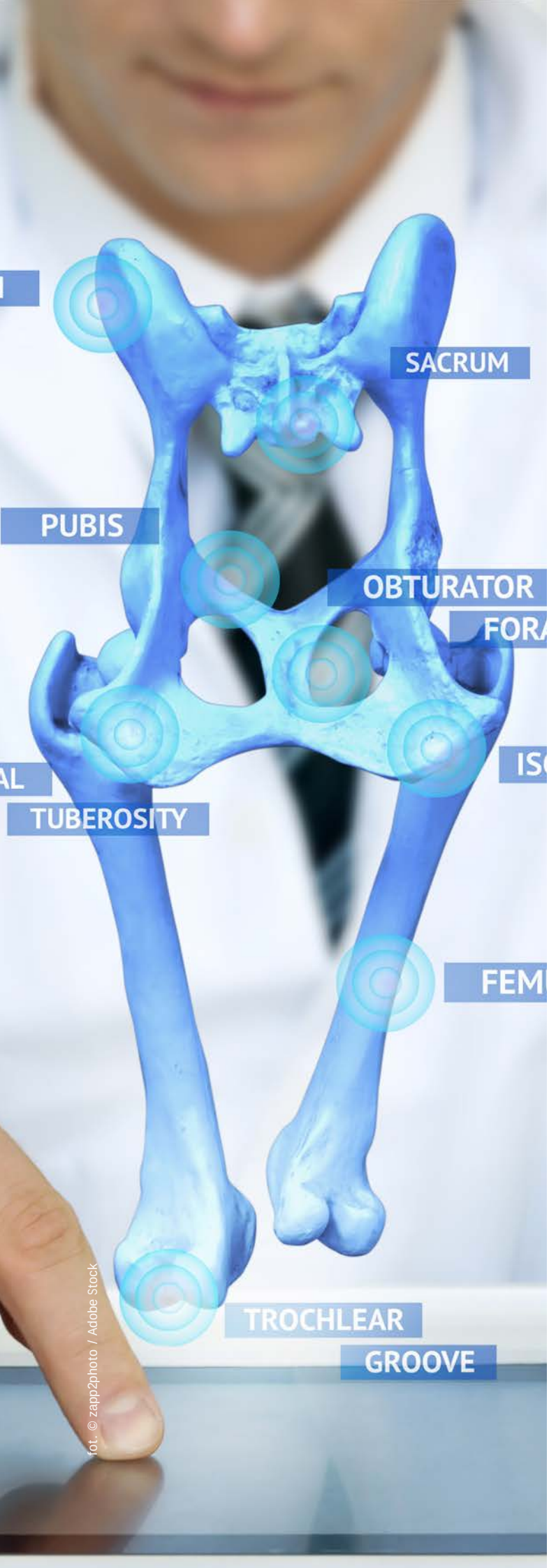
Obecnie, jeśli niektóre algorytmy wciąż się uczą, a później diagnozują więcej pacjentów, to w rzeczywistości pacjenci są poddawani urządzeniu przeszkolonemu bez weryfikacji, która normalnie byłaby zapewniona przez nadzorowane badania kliniczne. Innymi słowy, algorytm został przeszkolony na zestawach danych, które nie zostały sprawdzone pod kątem błędów.

MM: Systemy stale się dostosowujące są technicznie możliwe, jednak stanowią wyzwanie z perspektywy organów regulacyjnych i obaw społecznych. Co społeczeństwo może i chce zaakceptować, co pacjenci uważają za godne zaufania? Wyobraź sobie, że za 10 lat twój lekarz będzie używać tych samych przyrządów sprzed dekady zamiast nowoczesnych technologii – w tej sytuacji można powątpiewać, czy otrzymujemy najlepsze możliwe leczenie.

Jak osiągnąć równowagę między ochroną danych a wdrażaniem innowacyjnej opieki zdrowotnej?

Ogólne rozporządzenie Unii Europejskiej o ochronie danych (RODO) wprowadzone w 2018 r. chroni wszelkie dane związane ze zdrowiem fizycznym lub psychicznym osoby, dane genetyczne, takie jak wyniki laboratoryjne dotyczące analizy próbki biologicznej, dane biometryczne, np. wizerunki twarzy, odciski palców, cechy chodu i nie tylko.

W USA *Ustawa o przenoszeniu i odpowiedzialności za ubezpieczenie zdrowotne* (*Health Insurance Portability and Accountability Act* – HIPAA, ustanowiona w 1966) zapewnia ochronę danych osobowych przechowywanych przez sektor opieki zdrowotnej i ubezpieczeń zdrowotnych przed oszustwami i kradzieżami, obejmuje także ograniczenia w zakresie ubezpieczeń.



fot. © zapp2photo / Adobe Stock

MM: Wiele sprowadza się do tego, jakie dane są dostępne do budowy takiego systemu i umożliwienia jego ewolucji. Choć konsumenci są chronieni przez RODO, dla etycznych firm trudne jest uzyskanie dostępu do danych i zapewnienie, że są wykorzystywane w sposób prawidłowy.

Ponownie to bardziej obawa społeczeństwa. Jakie osobiste dane medyczne chcesz udostępnić i jak bardzo ufasz infrastrukturze? Jeśli zgadzasz się na przesłanie najnowszych wyników badań do pliku historii e-pacjenta – zaufanie jest najważniejsze.

Ubezpieczenie musi obejmować wszystkie poziomy świadczeniodawców opieki zdrowotnej. Oprócz producentów i firm gromadzących i wykorzystujących dane do opracowywania systemów AI opartych na uczeniu maszynowym musi obejmować lekarzy POZ, oddziały szpitalne i przestrzenie danych dotyczących zdrowia, aby uniknąć sytuacji, w których osobiste dane pacjentów mogłyby zostać wykorzystane w sposób niezamierzony.

GH: Ludzie chcą niedrogiej i bezpiecznej opieki zdrowotnej. Aby poprawić opiekę zdrowotną dla świadczeniodawców i pacjentów, społeczeństwo musi znaleźć nową równowagę pomiędzy innowacją a poufnością, co pozwoli technologiom AI na wykorzystanie odpowiednio zanonimizowanych dużych zbiorów danych.

Właściwa anonimizacja może być trudnym zadaniem – jeśli na przykład ze zbioru rekordów usuniemy dane osobowe takie jak imię, nazwisko czy data urodzenia, a grupa uczestników jest wystarczająco mała, inne czynniki takie jak np. kolor włosów, skóry, oczu czy budowa ciała nadal mogą pozwolić na identyfikację osób.

Normy mogą pomóc to osiągnąć dzięki dostarczeniu najlepszych praktyk.

Jakie wnioski wyciągnęliśmy z pandemii?

MM: Pandemia pokazała niektóre niedociągnięcia obecnej infrastruktury i potrzebę dostępu do ważnych danych zdrowotnych, aby móc monitorować choroby, dzielić się odkryciami i – ostatecznie – znaleźć lekarstwo. Na przykład w Niemczech istnieją różne sposoby gromadzenia danych i przenoszenia ich na poziom federalny, co może stanowić wyzwanie. Gromadzenie danych na poziomie europejskim w państwach członkowskich, oprócz przepisów, oznacza rozważanie wdrożenia interfejsów i infrastruktury, które umożliwią porozumienie się we wspólnym języku.

W tym miejscu normalizacja może odegrać rolę w udostępnieniu danych. COVID-19 uwypuklił te kwestie. Jak opracować aplikacje do śledzenia czegoś takiego jak COVID-19 i przekonać populacje do jej używania? Jakie dane zbierać i w jaki sposób to zrobić? Widzieliśmy różne podejścia w różnych krajach oferujące rozwiązania scentralizowane lub zdecentralizowane. Ten prawdziwy scenariusz pokazuje, jak ważne są te tematy.

Normy Międzynarodowe dotyczące poufności danych

Dzięki wspólnemu Komitetowi Technicznemu (ISO/IEC JTC 1) IEC i ISO opracowują Normy Międzynarodowe z zakresu technologii informacyjnych i komunikacyjnych obejmujących AI, zarządzanie danymi, cyberbezpieczeństwo i wiele więcej.

Niektóre z opracowywanych norm AI obejmują wytyczne i wymagania dotyczące zarządzania jakością danych, wiarygodność, zastosowanie AI oraz systemy zarządzania technologią AI.

Trwają prace nad przygotowaniem normalizacyjnych ram danych, aby uwzględnić zagrożenia w całym cyklu życia danych, w tym jakość danych i ich zarządzanie, jak są generowane, wykorzystywane, przechowywane i chronione. Inne kwestie to poziom wrażliwości danych osobowych zawartych w danych, tzw. współczynnik PI (*personal information factor*, *PI factor*).

Seria norm ISO/IEC 27000 składająca się z ponad 40 części obejmuje techniki bezpieczeństwa w systemach zarządzania bezpieczeństwem informacji, w tym poufność, zarządzanie ryzykiem oraz kodeks postępowania w zakresie ochrony danych osobowych w chmurach publicznych działających jako podmioty przetwarzające dane osobowe.

Tłum. I. P.
IEC e-tech, Issue 06/2020

fot. © Africa Studio / Adobe Stock

Pandemia przyspiesza rozwój technologii medycznej i zwiększa liczbę cyberataków

Morand Fachot

Ponieważ pandemia COVID-19 nie ustaje, światowe organizacje normalizacyjne jeszcze ściślej współpracują, aby opracować środki zaradcze zapobiegające jej dalszemu rozprzestrzenianiu się.

Pandemia COVID-19 będzie zapamiętana na długie lata, przede wszystkim ze względu na ogromną liczbę ofiar śmiertelnych sięgającą kilku milionów; dla przypomnienia, na dzień 1 lutego 2021, po upływie roku od wybuchu pandemii, Stany Zjednoczone straciły więcej obywateli z powodu COVID-19 niż w związku z obiema wojnami światowymi i działaniami zbrojnymi w Korei i Wietnamie razem...

Tak jak wcześniej wojny, pandemia będzie zapamiętana jako katalizator postępu w dziedzinie medycyny.

Jednak tym razem postępy wykraczają poza leki, takie jak antybiotyki i sulfonamidy, które z powodzeniem stosowano w leczeniu infekcji podczas II wojny światowej.

Rzeczywiście ta sytuacja zostanie zapamiętana z powodu szybkiego rozwoju niektórych szczepionek, a także z uwagi na znaczący postęp w dziedzinie sprzętu, szczególnie tego elektrycznego wykorzystywanego w medycynie, oraz z powodu wprowadzenia nowych rozwiązań technologicznych jak np. sztuczna inteligencja (AI), uczenie maszynowe, postępu w innych dziedzinach takich jak robotyka i rozwój zdalnej diagnostyki i leczenia za pomocą telemedycyny. Uwidoczniło się to szczególnie podczas ostatnich (wirtualnych) Targów Elektroniki Użytkowej (CES) 2021, gdzie było to jednym z tematów wzbudzających największe zainteresowanie.

COVID-19 jest chorobą wysoce zaraźliwą, zmusza ludzi do pozostania w domach, co z kolei wymogło na sektorze ochrony zdrowia wdrożenie innowacyjnych sposobów diagnozowania, doradzania, a nawet leczenia pacjentów na odległość.

Wideokonsultacje mają jednak swoje ograniczenia. Obiecującym podejściem do tego zagadnienia jest to oferowane przez specjalne urządzenia takie jak system MedWand na smartfony i tablety, urządzenia zdalnie monitorujące, które mogą ocenić i monitorować stan zdrowia pacjentów pod kątem wielu schorzeń i bezpiecznie połączyć z ich lekarzami.

Przełamywanie schematów jest kluczowe dla lepszej opieki zdrowotnej, spójności

Nowością jest bezprecedensowa i bliska współpraca między trzema organizacjami opracowującymi normy z siedzibą w Genewie: Międzynarodową Komisją Elektrotechniczną (IEC), Międzynarodowym Związkiem Telekomunikacyjnym (ITU) oraz Międzynarodową Organizacją Normalizacyjną (ISO). W okresie od marca do czerwca tego roku zaplanowano cykl spotkań poświęconych „skutecznej koordynacji działań normalizacji technicznej w IEC, ISO oraz ITU-T". Działania związane z COVID-19 z dużym prawdopodobieństwem zajmą ważne miejsce w programie.

Przyczyną bliższej współpracy między tymi organizacjami jest fakt, że bardziej niż kiedykolwiek wprowadzana jest interoperacyjność sprzętu, urządzeń i procesów, wiele z nich ma kluczowe znaczenie dla środowiska medycznego, a kwestie związane z COVID-19 nie będą możliwe do rozwiązania bez integracji norm opracowanych przez te trzy organizacje.

Obejmuje to m.in.: wykorzystanie robotów w środowisku medycznym i opiece zdrowotnej, dzięki czemu możemy poradzić sobie z problemami związanymi z pandemią, takimi jak zdalne monitorowanie stanu zdrowia pacjentów, leczenie ich przez dostarczanie leków oraz ochronę personelu medycznego.

Roboty umożliwią także interakcję między pacjentami i personelem medycznym, nawet jeśli pacjent nie znajduje się w placówce ochrony zdrowia; wykonują także czynności, które są zwykle pracochłonne i niebezpieczne np. dezynfekcja i czyszczenie obiektów medycznych.

Roboty, łączące wiele urządzeń i elementów takich jak baterie, czujniki i komponenty elektroniczne, bazują na pracy wielu komitetów technicznych IEC, takich jak IEC/TC 47 *Semiconductor devices*, IEC/TC 21 *Secondary cells and batteries*. Roboty używane do monitorowania i interakcji z pacjentami mogą być wyposażone w ekrany, jak również systemy multimedialne i ich elementy - Normy Międzynarodowe z tego zakresu opracowują IEC/TC 100 *Audio, video and multimedia systems and equipment* oraz IEC/TC 110 *Electronic displays*.

- Zastosowania AI odgrywające ważną rolę w niezliczonych obszarach, m.in. w opiece zdrowotnej w opracowywaniu leków przeciwwirusowych czy spersonalizowanej diagnostyki i sprzętu terapeutycznego. W 2017 roku ISO i IEC powołały wspólny podkomitet ISO/IEC JTC 1/SC42 działający w ramach ISO/IEC JTC 1.
- Telemedycynę, która polega na przesyłaniu danych i informacji, w tym obrazów, pomiędzy pacjentami a personelem medycznym lub między placówkami medycznymi, bazującą na normach połączenia danych i ich transmisji opracowanych głównie przez ITU.

Normy i ocena zgodności

Normy Międzynarodowe obejmujące sprzęt elektryczny w praktyce medycznej są opracowywane przez IEC/TC 62 i jego podkomitety, które w sumie wydały już ponad 300 publikacji.

IECEE, system oceny zgodności IEC dla urządzeń i elementów elektrotechnicznych, oferuje testy i certyfikację w zakresie bezpieczeństwa, jakości, efektywności i ogólnej wydajności zgodnie z Normami

Międzynarodowymi IEC dla 22 kategorii produktów, w tym sprzętu elektrycznego do użytku medycznego. W tym celu powołano Expert Task Force, (ETF) 3 „MEAS, MED", zajmujący się sprzętem pomiarowym i laboratoryjnym (MEAS) oraz sprzętem elektrycznym do użytku medycznego (MED).

Łagodzenie zagrożeń cyberbezpieczeństwa w erze COVID i nie tylko

Rośnie świadomość konieczności utrzymania ochrony poufności dokumentacji pacjentów, integralności danych i dostępu do placówek medycznych, instytutów badawczych i laboratoriów.

Dzieje się tak w następstwie cyberataków na wiele obiektów i naruszeń bezpieczeństwa. Ataki te mogą być przeprowadzane przez podmioty państwowe lub niepaństwowe (czasem w imieniu państw) oraz prze-

stępców. Mogą przybrać formę wtargnięcia „złych podmiotów" próbujących ominąć długie i kosztowne wysiłki badawcze w celu uzyskania informacji na temat szczepionek i leków na COVID-19.

Mogą mieć też na celu wykorzystanie oprogramowania *ransomware*, by zablokować na kilka dni placówki medyczne, w tym szpitalne systemy, szyfrując dane i je deszyfrując (lub nie) za opłatą. Jest to szczególnie poważne w czasie, gdy szpitale są na pierwszej linii frontu walki z pandemią COVID-19 – takie działania mogą mieć bardzo poważne konsekwencje.

Czynnik ludzki najsłabszym ogniwem

Wprowadzenie różnych praktyk pracy, takich jak telepraca po wybuchu pandemii, przyczyniło się do zwiększenia liczby cyberataków.

W październikowym wspólnym raporcie dotyczącym cyberbezpieczeństwa na temat działań *ransomware* wymierzonych w amerykański system opieki zdrowotnej i sektor zdrowia publicznego stwierdzono, że „szpitale i organizacje opieki zdrowotnej stały się celem rosnącej liczby cyberataków".

Międzynarodowa firma Check Point Software 5 stycznia ogłosiła, że liczba ataków na placówki opieki zdrowotnej na całym świecie wzrosła o ponad 45% od 1 listopada 2020, w porównaniu ze średnim 22% wzrostem liczby ataków na inne sektory przemysłu. „Kanada doświadczyła największego, bo 250% wzrostu ataków, następne są Niemcy, które zanotowały 220% wzrost oraz Hiszpania, gdzie zaobserwowano podwojenie liczby ataków", podaje Check Point Software.

Oprócz wzrostu kosztów, ataki te mogą być powodem śmierci, tak jak to miało miejsce w Niemczech we wrześniu 2020, kiedy kobieta zmarła po tym, jak nie została przyjęta do szpitala, który stał się celem cyberataku.

Zbyt często i zbyt długo cyberbezpieczeństwo zajmowało drugie miejsce w placówkach opieki zdrowotnej, które polegały na niezabezpieczonym sprzęcie medycznym i wciąż używały przestarzałego sprzętu i oprogramowania.

Firmy zajmujące się cyberbezpieczeństwem podkreślają znaczenie świadomości, potrzeby edukowania personelu w zakresie złośliwego sprzętu i luk w systemie lub, jeśli jest to niemożliwe, skorzystania z systemu zapobiegania włamaniom z możliwością wirtualnego łatania luk, aby zapobiec próbom wykorzystania słabych punktów we wrażliwych systemach i aplikacjach.

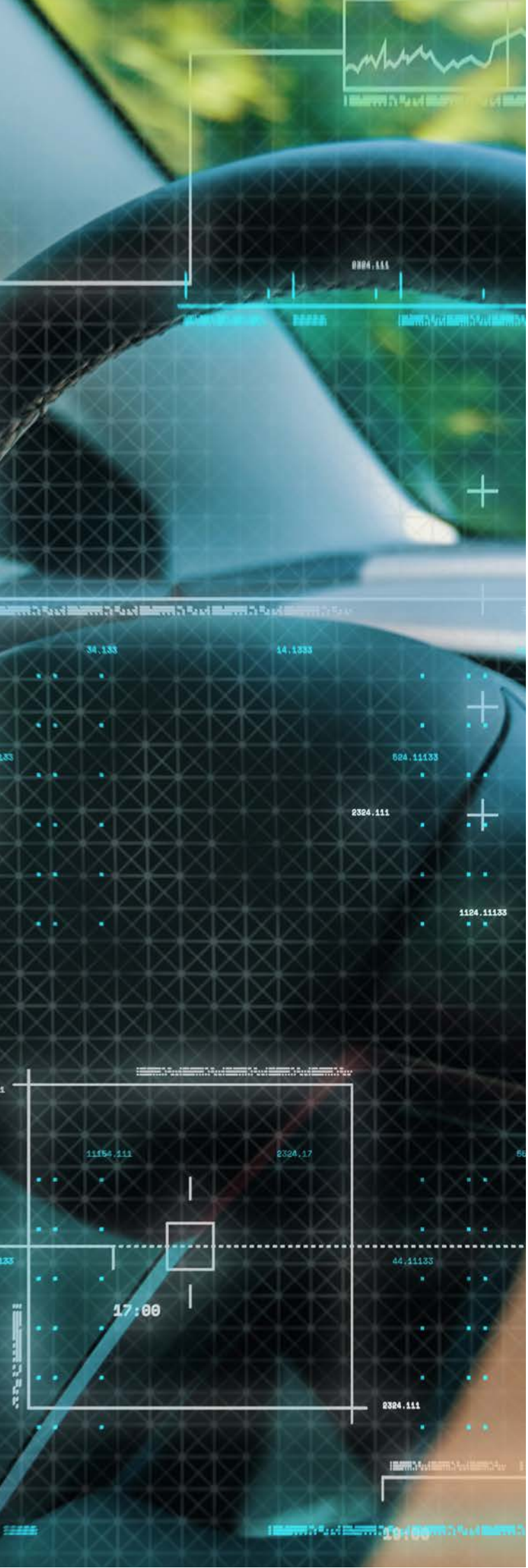
Inną ważną kwestią jest zapewnienie, że producenci urządzeń medycznych projektują i wytwarzają bezpieczne cybernetycznie produkty.

Okaże się, czy środki podjęte w celu zaradzenia globalnej pandemii pomogą zapobiec przyszłym pandemiom lub je złagodzić.

Tłum. I. P.
IEC e-tech magazine, Issue 01/2021

CYBERBEZPIECZEŃSTWO W FOTELU KIEROWCY

Clare Naden



Świat staje się coraz bardziej połączony, więc to samo dzieje się z naszymi samochodami. Jednak większa łączność to więcej danych, które mogą wpaść w niepowołane ręce. Cyberbezpieczeństwo w motoryzacji to pole dynamicznego rozwoju.

Dzięki technologii internetowej nasze samochody umożliwiają wykonywanie połączeń, informują, czy zjeżdżamy na zły pas, zbierają dane o ruchu drogowym lub o położeniu najbliższej stacji paliw. Przemieszczenie się z punktu A do punktu B to kwestia niemal drugorzędna. Jednak wszystkie te możliwości niosą ze sobą ryzyko – od kradzieży danych osobowych po dosłowne zjechanie z drogi.

W różnych eksperymentach sprawdzających odporność systemów cyberbezpieczeństwa w pojazdach „hakerzy w białych kapeluszach" – tj. eksperci ds. bezpieczeństwa komputerowego, którzy celowo włamywali się do systemów, aby przetestować i ocenić ich poziom bezpieczeństwa – pokazali, że możliwe jest zdalne kontrolowanie pojazdów. Na przykład, już w 2015 roku tacy hakerzy udowodnili, że są w stanie przejąć kontrolę nad systemami hamowania i przyspieszania jeepa, jego deską rozdzielczą i nie tylko – to dość przerażająca myśl.

W eksperymencie z Teslą zdołali oszukać oprogramowanie autopilota do jazdy autonomicznej i zjechać na przeciwny pas ruchu. „Inne incydenty, takie jak te nieuwzględniające udziału hakerów w białych kapeluszach, także musiałyby być traktowane z należytą ostrożnością i uwagą" – uważa dr Gido Scharfenberger-Fabian, kierownik projektu w Grupie Roboczej WG 11 zajmującej się cyberbezpieczeństwem elementów elektrycznych i elektronicznych w pojazdach drogowych.

Dlatego cyberbezpieczeństwo to duży biznes, szczególnie, jeśli mówimy o pojazdach. Według różnych szacunków wartość globalnego rynku cyberbezpieczeństwa motoryzacyjnego wzrośnie od 2,4 miliarda dolarów w 2019 roku do około 6 miliardów dolarów w 2025 roku. Mimo że branża bardzo dobrze prosperuje, to dopiero początek wojny z hakerstwem.

Długa historia danych

Dane z naszych samochodów były zbierane już we wczesnych latach 90. XX w. – mówi Jack Pokrzywa, Dyrektor Global Ground Vehicle Standards w SAE International, światowym stowarzyszeniu zajmującym się inżynierią mobilności i kluczowym partnerem ISO. Urządzenia takie jak rejestratory danych o zdarzeniach (*Event Data Recorders*) lub czarna skrzynka samochodu dostarczają informacji np. o działaniach naszego pojazdu przed wypadkiem i po nim.

Oczywiście obecnie technologia jest bardziej zaawansowana. Jej możliwości obejmują zbieranie danych z zewnątrz, np. lokalizacja, pogoda, warunki drogowe; natomiast czujniki wewnątrz pojazdu mogą gromadzić dane o pasażerach, aby w razie wypadku dostarczyć istotnych informacji. „Nie zapominajmy o danych biometrycznych – o możliwości śledzenia na przykład ruchu oczu, by sprawdzić czy kierowca jest skupiony na jeździe, czy zasypia za kółkiem" – dodaje. „Obecnie istnieje wiele aplikacji łączących się z systemem operacyjnym samochodu, co umożliwia np. nagrywanie informacji o połączeniach wykonanych przez samochodowy system głośnomówiący. Płyną z tego korzyści związane z bezpieczeństwem, istnieją także obawy związane z poufnością danych".

W niektórych systemach prawnych, np. w Europie, numer identyfikacyjny pojazdu (VIN) jest postrzegany jako dana osobowa (PII – *personal identifiable information*), ostrzega dr Markus Tschersich, kolejny lider projektu w Grupie Roboczej ekspertów ISO. „W związku z tym, wszystkie dane generowane przez systemy pojazdu i powiązane z VIN mogą być postrzegane jako PII. Są to informacje, które samodzielnie lub w połączeniu mogą zostać wykorzystane do identyfikacji, lokalizacji osoby lub kontaktu z nią. Przykładowo, dane zebrane z układu hamulcowego, kierowniczego i innych elementów samochodu można wykorzystać do uzyskania danych o umiejętnościach i zachowaniach kierowcy". A dopóki istnieje połączenie między samochodem a źródłami zewnętrznymi, istnieje prawdopodobieństwo włamania do systemów.

W dzisiejszym przemyśle motoryzacyjnym każdy etap łańcucha dostaw jest kierowany, monitorowany i analizowany przez zaawansowane technologicznie oprogramowanie.

fot. metamorworks / Adobe Stock

Nadążyć za hakerami

Dzisiejsze samochody są pełne skomplikowanego oprogramowania, oczekuje się, że w niedalekiej przyszłości będą jeszcze bardziej złożone. Według firmy konsultingowej McKinsey & Company mamy współcześnie około stu milionów linijek kodu, uważa się jednak, że do 2030 roku liczba ta będzie trzykrotnie większa. Można to porównać chociażby z samolotem pasażerskim, który ma około 15 milionów linijek kodu i standardowym komputerem osobistym, który ma do 40 milionów linijek kodu. Im bardziej złożona maszyna, tym więcej możliwości wystąpienia cyberataków w całym łańcuchu wartości.

W miarę jak technologia staje się coraz bardziej zintegrowana z samochodami, przemysł motoryzacyjny staje się wyzwaniem dla naszego pokolenia. Chodzi o zabezpieczenie światowej infrastruktury motoryzacyjnej przed cyberprzestępcami, którzy chcą wykraść dane i przejąć kontrolę nad zautomatyzowanymi systemami do złych celów. „Środki cyberbezpieczeństwa należy dostosowywać do kolejnych generacji systemów, a także w systemach w terenie przez aktualizacje", mówi dr Scharfenberger-Fabian. „To niekończące się wyzwanie".

J. Pokrzywa zwraca uwagę, że każde urządzenie działające na oprogramowaniu może zostać zhakowane. Przeciwdziałanie takim problemom wymaga wysokiego poziomu wymiany wiedzy w branży, szczególnie pomiędzy producentami samochodów a ich sieciami dostawczymi. Jak mówi, jedną z organizacji zajmujących się tym w USA jest Automotive Information Sharing and Analysis Center (Auto-ISAC). Przedstawiciele branży analizują informacje o wszelkich potencjalnych zagrożeniach dla pojazdów, przyczyniając się do wzmocnienia technologii cyberbezpieczeństwa. Potrzebne jest jednak podejście holistyczne na całym świecie.

Globalny apel

Ujednolicenie procesów i metod w łańcuchu dostaw jest podstawą do odpowiedniego uwzględnienia kwestii cyberbezpieczeństwa w inżynierii systemów motoryzacyjnych, uważa dr Scharfenberger-Fabian. „Istnieje wiele uznanych Norm Międzynarodowych z zakresu bezpieczeństwa technologii informacyjnych (np. seria ISO/IEC 27xxx) lub branżowych norm bezpieczeń-

stwa (seria IEC 62443 obejmująca systemy kontroli przemysłowych)", mówi, „jednak nie uwzględniają one specyficznych potrzeb przemysłu motoryzacyjnego".

W 2015 roku SAE International utworzyła Komitet ds. Inżynierii Systemów Cyberbezpieczeństwa Pojazdów, aby zająć się tymi zagrożeniami i słabymi punktami na rynku amerykańskim. Rok później, komitet opublikował SAE J3061 *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* definiujący kompletne ramy procesu cyklu życia, które można dostosować i wykorzystać w procesach rozwoju każdej firmy w celu włączenia cyberbezpieczeństwa do cyberfizycznych systemów pojazdów, od fazy koncepcyjnej, przez produkcję, eksploatację i serwis, aż po wycofanie z eksploatacji.

Nowa Norma Międzynarodowa będzie opierać się na wytycznych SAE i tworzyć kompleksowe narzędzie cyberbezpieczeństwa, które odpowie na wszystkie potrzeby i wyzwania branży na poziomie globalnym. Obecnie opracowywana norma ISO/SAE 21434 *Road vehicles – Cybersecurity engineering* ma zostać opublikowana w 2021 roku. Obejmie kwestie cyberbezpieczeństwa w inżynierii systemów elektrycznych i elektronicznych (E/E) w pojazdach drogowych. Stosowanie normy ma pomóc producentom w nadążaniu za zmieniającymi się technologiami i rodzajami cyberataków.

W projekt zaangażowani są dr Scharfenberger-Fabian oraz dr Tschersich, którzy wyjaśniają, że norma ma zastąpić zalecaną praktykę SAE J3061. Umożliwi firmom zdefiniowanie polityki i procesów w zakresie cyberbezpieczeństwa, zarządzanie ryzykiem cyberbezpieczeństwa i wspieranie kultury cyberbezpieczeństwa. Może być także wykorzystana do wdrożenia systemu zarządzania cyberbezpieczeństwem, w tym prawidłowego zarządzania ryzykiem cyberbezpieczeństwa w pojazdach drogowych.

Kwestie bezpieczeństwa

Dla branży przyzwyczajonej do pokonywania skomplikowanych wyzwań i standardowych reakcji, cyberbezpieczeństwo pozostaje nieznormalizowaną anomalią. Czy norma może obiecać prawdziwe cyberbezpieczeństwo? „Niestety nie ma czegoś takiego jak bezpieczna technologia, którą można by znormalizować," mówi dr Tschersich, „więc samo przestrzeganie

fot. © metamorworks / iStock

normy ISO/SAE 21434 nie zapewni bezpieczeństwa samochodów. Procesy w niej opisane mogą z całą pewnością stworzyć podstawy dobrej inżynierii cyberbezpieczeństwa i zacieśnić działania w tym zakresie".

Jak mówi, te procesy obejmują ocenę zagrożeń dla cyberbezpieczeństwa oraz podejścia do identyfikacji i dostosowania rozwiązań cyberbezpieczeństwa dla systemów i komunikacji w całym łańcuchu dostaw. Obejmuje to koncepcje, rozwój, produkcję, eksploatację, serwisowanie i wycofanie z eksploatacji systemów elektrycznych i elektronicznych w pojazdach drogowych, w tym ich części i interfejsów.

Norma ustanawia ramy cyberbezpieczeństwa dla firm motoryzacyjnych i charakteryzuje się wspólnym językiem do komunikacji i zarządzania ryzykiem w cyberbezpieczeństwie.

„Choć norma ISO/SAE 21434 nie odnosi się do technologii i nie promuje jej bezpośrednio, ramy pozwolą na usprawnienie współpracy w zakresie cyberbezpieczeństwa w branży i tym samym doprowadzą do opracowania technologii i rozwiązań,

które lepiej sprostają dzisiejszym i przyszłym problemom związanym z cyberbezpieczeństwem". Pomoże też w rozważeniu kwestii cyberbezpieczeństwa na każdym etapie procesu oraz w terenie, tworząc listę kontrolną dla inżynierów, która obejmie skanowanie w poszukiwaniu błędów, zwiększenie poziomu zabezpieczeń własnych w zakresie cyberbezpieczeństwa pojazdu, oraz opracowanie analizy ryzyka potencjalnych luk w zabezpieczeniach każdej części.

Jak mówi, jest zapotrzebowanie na ISO/SAE 21434, która ma wspierać już istniejące przepisy. Jest postrzegana jako dokument referencyjny dla wdrożenia systemu zarządzania cyberbezpieczeństwem (CSMS), co widać w ostatnio wprowadzonych regulaminach ONZ w zakresie cyberbezpieczeństwa w pojazdach. „Wynika to ze ścisłej współpracy pomiędzy Wspólną Grupą Roboczą ISO/SAE a odpowiednią grupą zadaniową ONZ" – wyjaśnia.

Aby jeszcze bardziej poprawić relację między regulacjami ONZ a normalizacją, niedawno rozpoczęto prace nad publicznie dostępną specyfikacją ISO/PAS 5112, która zawiera wytyczne dotyczące audytów organizacyjnych w zakresie inżynierii cyberbezpieczeństwa. Będzie bazować na ISO/SAE 21434, ma służyć do audytu CSMS zgodnie z definicją ujętą w regulaminie ONZ. Ostatecznym celem jest powszechne wdrożenie normy do codziennych praktyk inżynieryjnych, jednocześnie zwiększając świadomość przez włączenie normy do programu szkolenia inżynierów.

„Jeśli rozwój produktu będzie oparty na solidnych zasadach zawartych w normie ISO/SAE 21434, poziom bezpieczeństwa pojazdów może być jeszcze wyższy", dodaje dr Scharfenberger-Fabian. Przyszła norma ma na celu poprawę cyberbezpieczeństwa motoryzacyjnego i ograniczenie ryzyka w całym łańcuchu dostaw – od momentu zaprojektowania i wyprodukowania pojazdu po jego wycofanie z eksploatacji. Wielu przedstawicieli branży ma w planach zapewnienie jej integracji.

Zatem wojna trwa

Zagrożenia cybernetyczne w samochodach, choć są stosunkowo nowe, pozostaną stałym problemem. W związku z tym producenci samochodów muszą traktować cyberbezpieczeństwo jako integralną część swoich podstawowych funkcji biznesowych i działań rozwojowych. „Nie sądzę, abyśmy kiedykolwiek byli w stanie zapobiec próbom włamania do systemu", uważa Jack Pokrzywa, „ale podnosząc bariery bezpieczeństwa, możemy to ryzyko zmniejszyć". Pozwoli to także kontrolować koszty rozwoju i utrzymania – korzyści dla wszystkich graczy z branży.

Oprócz ISO/SAE 21434, przemysł motoryzacyjny będzie nadal opracowywać własne normy cyberbezpieczeństwa, aby zapewnić łatwe w zarządzaniu i bezpieczne rozwiązania, w tym zapowiadaną normę z zakresu audytu inżynierii cyberbezpieczeństwa. Praca dopiero się zaczyna, jednak dzięki branży zajmującej się bezpieczeństwem systemów samochodowych na każdym etapie produkcji, koła będą się nadal kręcić, a samochody, którymi jeździmy, będą coraz bezpieczniejsze.

Tłum. I. P.
www.iso.org

Specyfikacja Techniczna CEN/TS 17288
International Summary:
Guideline for European Implementation

Komitet Techniczny CEN/TC 251 *Health informatics* opracował ostatnio dwa dokumenty normalizacyjne ustanawiające tzw. *International Patient Summary*[1]: EN 17269:2019 oraz CEN/TS 17288:2020. Dokumenty te obejmują wymagania dotyczące wymiany podstawowego, niezbędnego zbioru danych z zakresu opieki zdrowotnej w celu zapewnienia ciągłości opieki nad pacjentem zawsze i wszędzie gdzie jest ona potrzebna.

W normie EN 17269 *The International Patient Summary* znormalizowano zbiór danych z wytycznych opracowanych i zaktualizowanych przez sieć eHealth (eHealth Network – eHN) w 2016 r. W ramach eHN opracowano „Szczegółowe Wytyczne dotyczące elektronicznej wymiany danych dotyczących zdrowia na mocy Dyrektywy Transgranicznej 2011/24/EU", korzystając z wcześniejszych doświadczeń projektu pilotażowego epSOS, który objął 27 krajów członkowskich UE. Norma EN 17269 jest zatem modelem referencyjnym, który ułatwia tworzenie zgodnych modeli pochodnych do celów wdrożeniowych. Projekt *International Patient Summary* (IPS) zapewnia jeden znormalizowany i trwały szablon przydatnych i użytecznych treści zarówno dla planowanej, jak i nieplanowanej opieki na całym świecie, wspierając w ten sposób utrzymanie ciągłości opieki dla wszystkich.

Zbiór danych IPS ma być minimalny i zwięzły – standardowy wspólny rdzeń ma być adekwatny i zrozumiały dla każdego lekarza prowadzącego w punkcie opieki zdrowotnej. Został zaprojektowany tak, aby można go było łatwo rozszerzać, by umożliwić dodawanie specjalistycznych danych, gdy jest to konieczne przy konkretnych schorzeniach. Ponadto, zakres zbioru danych IPS jasno wskazuje, że może być łatwo wykorzystany w wielu scenariuszach obejmujących zarówno nieplanowaną, jak i planowaną opiekę zdrowotną w sytuacjach transgranicznych i wewnątrzgranicznych. To ostatnie zapewnia elastyczność w jego stosowaniu zarówno na poziomie lokalnym, jak i krajowym, regionalnym czy globalnym. Mówiąc bardziej ogólnie, projekt IPS ma być także wartościowy w sytuacjach transgranicznych, takich jak te wywołane przez systemy organizacyjne i informatyczne wykorzystywane przez różnych świadczeniodawców. Oprócz elastyczności norm, EN 17269 definiuje zestaw bloków danych, które w razie potrzeby można wykorzystać ponownie do innych zastosowań klinicznych.

Na podstawie tych ram, druga – i nowsza – publikacja z tej serii, CEN/TS 17288 *The International Patient Summary – Guideline for European Implementation*, uznaje, że zastosowania transgraniczne to szczególny przypadek, który wymaga większej uwagi, ponieważ obejmują różne jurysdykcje. Docelowi odbiorcy to przede wszystkim programiści i zespoły wdrażające projekty, jednak decydenci i organizacje normalizacyjne mają na celu zapewnienie, że wytyczne są odpowiednie dla określonych okręgów.

Podczas gdy norma EN 17269 formalnie określa zbiór danych eHN i związane z nim zasady, sekcja IPS dotycząca funkcji transgranicznych pozostała „lekka", raczej zastępcza niż sekcja ze szczegółową treścią. Był to celowy zabieg, ponieważ nawet w regionie Europy, poszczególne państwa członkowskie mają różne polityki i przepisy dotyczące opieki zdrowotnej, a tym samym różne wymagania. Ponieważ zamierzeniem IPS jest dostarczenie międzynarodowego standardu, różnice w wymaganiach zwiększyłyby się i mogłyby działać hamująco, jeśli nie stałyby się niemożliwe do opanowania. W tym kontekście CEN/TS 17288 ma wspierać europejskie wdrażanie IPS przez dostarczanie odpowiednich wytycznych. Polityka europejska, dyrektywy, kultura pracy i kultura organizacyjna oraz zróżnicowany rynek wymagają wskazówek dotyczących wdrażania, które są istotne technicznie wrażliwe kontekstowo. CEN/TS 17288 opisuje te aspekty wdrożeniowe z perspektywy europejskiej, wykorzystując *Refined eHealth European Interoperability Framework* (ReEIF)[2] w celu uporządkowania treści w sposób znany europejskim odbiorcom. Po przyjęciu normy EN 17269 przez ISO, CEN/TS 17288 może dostarczyć szablon dla innych regionów na całym świecie do wspierania ich własnego wdrożenia globalnego systemu IPS.

Te dwa dokumenty normalizacyjne zostały opracowane przez CEN/TC 251, którego sekretariat prowadzi NEN, holenderska jednostka normalizacyjna, dzięki wsparciu i finansowaniu ze strony Komisji Europejskiej.

Tłum. I. P.
www.cencenelec.eu/news

---

[1] Dokument *International Patient Summary* (IPS) to elektroniczny wyciąg z dokumentacji medycznej zawierający podstawowe informacje dotyczące opieki zdrowotnej przeznaczony m.in. do wykorzystania w nieplanowanym scenariuszu opieki transgranicznej, zawierającym co najmniej wymagane elementy zbioru danych IPS.

[2] Udoskonalone europejskie ramy interoperacyjności w dziedzinie e-zdrowia.

Zarządzanie jakością oraz bezpieczeństwo w laboratoriach PKN/KT 300 ds. Medycznych Badań Laboratoryjnych In Vitro

Komitet Techniczny PKN/KT 300 ds. Medycznych Badań Laboratoryjnych In Vitro zajmuje się m.in. normalizacją zagadnień związanych z zarządzaniem jakością i zapewnieniem jakości w zakresie diagnostyki *in vitro* oraz bezpieczeństwem laboratoriów.

Działalność PKN/KT 300 pozwala na wdrażanie i rozpowszechnianie w krajowym przemyśle medycznym oraz szeroko rozumianej działalności diagnostycznej *in vitro*, norm opracowanych na poziomie międzynarodowym (ISO) i europejskim (CEN). PKN/KT 300 współpracuje z Komitetami Technicznymi CEN/TC 140 *In vitro diagnostic medical devices* oraz ISO/TC 212 *Clinical laboratory testing and in vitro diagnostic test systems*.

W styczniu bieżącego roku została opublikowana polska wersja językowa PN-EN ISO 15195:2019-04 Medycyna laboratoryjna – Wymagania dotyczące kompetencji laboratoriów wzorcujących, stosujących referencyjne procedury pomiarowe. Norma przedstawia dodatkowe aspekty dotyczące kompetencji laboratoriów wzorcujących w obszarze medycyny laboratoryjnej. Opisano tu kwestie związane z kompetencjami kluczowymi do wykonywania referencyjnych procedur pomiarowych oraz podano dodatkowe wymagania dla laboratoriów wzorcujących, zapewniające prawidłowe wykonywanie przez nie zadań. Warto też wspomnieć o normie PN-EN ISO 15193:2009 Wyroby medyczne do diagnostyki in vitro – Pomiar wielkości w próbkach pochodzenia biologicznego – Wymagania dotyczące zawartości i prezentacji referencyjnych procedur pomiarowych określającej wymagania dotyczące zawartości i formy referencyjnej procedury pomiarowej.

Ogólne wymagania dotyczące kompetencji oraz spójnego funkcjonowania laboratoriów badawczych i wzorcujących podano w dostępnej w języku polskim PN-EN ISO/IEC 17025:2018-02. Wymagania dotyczące jakości i kompetencji laboratoriów medycznych opisano natomiast w dostępnej w języku polskim PN-EN ISO 15189:2013-05 Laboratoria medyczne – Wymagania dotyczące jakości i kompetencji. Dokument może być stosowany zarówno przez laboratoria medyczne rozwijające swoje systemy zarządzania i oceniające swoje kompetencje, jak i klientów laboratoriów, organy ustawodawcze i jednostki akredytujące do potwierdzania i uznawania kompetencji laboratoriów medycznych.

Mówiąc o jakości, nie można pominąć kwestii dotyczących spójności pomiarowej, niezbędnej w celu zapewnienia porównywalności wyników pomiarów w skali kraju, jak i w skali międzynarodowej. Jej zastosowanie i ograniczenia zostały szczegółowo opisane w ISO 17511:2020. Norma przedstawia wymagania techniczne oraz dokumentację niezbędną do ustalania spójności pomiarowej wartości wyznaczonych dla kalibratorów, materiałów kontroli poprawności pomiaru oraz próbek pochodzących od ludzi. Norma zostanie opublikowana jako PN-EN ISO 17511 Wyroby medyczne do diagnostyki in vitro – Wymagania dotyczące ustalania spójności pomiarowej wartości wyznaczonych dla kalibratorów, materiałów do kontroli poprawności pomiaru oraz próbek pochodzących od ludzi.

We wrześniu 2020 opublikowano normę PN-EN ISO 22367:2020-09 Laboratoria medyczne – Zastosowanie zarządzania ryzykiem w laboratoriach medycznych. Dokument stanowi doskonałe narzędzie wspomagające laboratoria diagnostyczne w stosowaniu oceny ryzyka procesów laboratoryjnych. Przedstawia metodę identyfikacji i zarządzania ryzykiem w laboratoriach medycznych w odniesieniu do pacjentów, pracowników i dostawców usług. Uwzględnia identyfikację, szacowanie, ocenę oraz monitorowanie ryzyka. Norma ma zastosowanie do wszystkich aspektów badań i usług laboratoriów medycznych, z uwzględnieniem etapów przedlaboratoryjnych i polaboratoryjnych, przenoszenia wyników badań do systemów elektronicznych oraz innymch procesów technicznych i zarządczych, opisanych we wcześniej wymienionej PN-EN ISO 15189:2013-05. Kolejną normą, stanowiącą swego rodzaju uzupełnienie PN-EN ISO 15189:2013-05, jest PN-EN ISO 22870:2017-02 Badania w miejscu opieki nad pacjentem (POCT) – Wymagania dotyczące jakości i kompetencji. W normie przedstawiono wymagania dotyczące badań wykonywanych w placówkach takich jak: szpitale, kliniki, organizacje opieki zdrowotnej prowadzące opiekę ambulatoryjną.

Więcej informacji dotyczących działalności PKN/KT 300 oraz możliwości współpracy znajduje się na www.pkn.pl.

Elżbieta Siuchta
Sektor Zagadnień Podstawowych
i Systemów Zarządzania PKN

ORGANY TECHNICZNE

fot. © comzeal / Adobe Stock

LUTY 2021

Komitety Techniczne

Zmiana zakresu tematycznego Komitetów Technicznych:

- KT 17 ds. Pojazdów i Transportu Drogowego rozszerzył współpracę o IEC/TC 125, Personal e-Transporters (PeTs)
- KT 40 ds. Pasz rozszerzył współpracę o ISO/TC 331, Biodiversity oraz nastąpiła zmiana zakresu tematycznego na: Terminologia, wymagania jakościowe, pobieranie próbek, metody badań, pakowanie, przechowywanie, transport w zakresie: pasz naturalnych, surowców paszowych, mieszanek paszowych, produktów ubocznych przemysłu spożywczego przeznaczonych na cele paszowe, dodatków do mieszanek paszowych. Normalizacja w dziedzinie różnorodności biologicznej w celu opracowania wymagań, zasad, ram, wskazówek i narzędzi wspierających w holistycznym i globalnym podejściu dla wszystkich odpowiednich organizacji, w celu zwiększenia ich wkładu w zrównoważony rozwój z wyłączeniem normalizacji dotyczącej metod badawczych i pomiarowych dla ekologicznej jakości wody, powietrza, gleby i środowiska morskiego.
- KT 287 ds. Biotechnologii rozszerzył współpracę o ISO/TC 331, Biodiversity (współpraca wiodąca) oraz nastąpiła zmiana zakresu tematycznego na: Biotechnologia, włączając w to aspekty bezpieczeństwa oraz w zakresie produktów żywnościowych modyfikowanych genetycznie oraz normalizacja w dziedzinie różnorodności biologicznej w celu opracowania wymagań, zasad, ram, wskazówek i narzędzi wspierających w holistycznym i globalnym podejściu dla wszystkich odpowiednich organizacji, w celu zwiększenia ich wkładu w zrównoważony rozwój z wyłączeniem normalizacji dotyczącej metod badawczych i pomiarowych dla ekologicznej jakości wody, powietrza, gleby i środowiska morskiego.

Nowi Przewodniczący Komitetów Technicznych

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

- w KT 10 ds. Zastosowań Metod Statystycznych dra inż. Pawła Fotowicza reprezentującego Główny Urząd Miar
- w KT 131 ds. Dźwigów, Schodów i Chodników Ruchomych mgra inż. Pawła Rajewskiego reprezentującego Urząd Dozoru Technicznego
- w KT 161 ds. Jakości Powietrza Wnętrz dra inż. Adama Niesłochowskiego reprezentującego Instytut Techniki Budowlanej
- w KT 257 ds. Metrologii Ogólnej dr Agnieszkę Zoń reprezentującą Główny Urząd Miar
- w KT 306 ds. Bezpieczeństwa Powszechnego i Ochrony Ludności dra inż. Andrzeja Wójcika reprezentującego ES-INSTAL Andrzej Wójcik

Nowi członkowie Komitetów Technicznych

W lutym Prezes PKN powołał na członków KT następujące podmioty:

- CosmetoSAFE Consulting Iwona Białas do KT 334 ds. Produktów Kosmetycznych
- Elbud-Projekt Warszawa Sp. z o.o. do KT 70 ds. Przekaźników Elektrycznych i Elektroenergetycznej Automatyki Zabezpieczeniowej
- Grzegorz Zelek Quality Glob do KT 7 ds. Badań Nieniszczących
- Politechnikę Lubelską do KT 213 ds. Projektowania i Wykonawstwa Konstrukcji z Betonu
- Politechnikę Poznańską do KT 68 ds. Pomiarów i Badań Wysokonapięciowych
- Polski Związek Żeglarski do KT 230 ds. Małych Statków
- QPD Dorota Pierzecka do KT 31 ds. Górnictwa Nafty i Gazu
- TIZ Implements Sp. z o.o. do KT 206 ds. Obrabiarek i Narzędzi Skrawających do Metali oraz Oprzyrządowania Przedmiotowego i Narzędziowego
- Termex-Fiber Sp. z o.o. do KT 211 ds. Wyrobów do Izolacji Cieplnej w Budownictwie
- VdS Schadenverhütung Sp. z o.o. do KT 244 ds. Sprzętu, Środków i Urządzeń Ratowniczo-Gaśniczych i KT 264 ds. Systemów Sygnalizacji Pożarowej

Odwołani członkowie Komitetów Technicznych

W lutym Prezes PKN odwołał z członka KT następujące podmioty:

- Biuro Handlowe BEST Paweł Gawroński z KT 138 ds. Kolejnictwa
- IKEA Purchasing Services Poland Sp. z o.o. z KT 138 ds. Kolejnictwa
- Instytut Ekologii Terenów Uprzemysłowionych z KT 246 ds. Ochrony Radiologicznej
- Janitza Energy Group S.C.z KT 138 ds. Kolejnictwa
- KGHM CUPRUM Sp. z o.o. Centrum Badawczo-Rozwojowe z KT 125 ds. Udostępniania i Eksploatacji Złóż Kopalin
- RAIL TECH PAPLA Sp. z o.o. z KT 138 ds. Kolejnictwa
- Stowarzyszenie Konsumentów Polskich z KT 3 ds. Mikrobiologii Łańcucha Żywnościowego KT 6 ds. Systemów Zarządzania, KT 92 ds. Nasion Roślin Oleistych, Tłuszczów Roślinnych i Zwierzęcych oraz ich Produktów Ubocznych i KT 200 ds. Koncentratów Spożywczych, Skrobi i Produktów Dietetycznych
- TEST-EXPERT Marta Wojas z KT 7 ds. Badań Nieniszczących
- VdS Schadenverhütung GmbH Sp. z o.o. Oddział w Polsce z KT 244 ds. Sprzętu, Środków i Urządzeń Ratowniczo-Gaśniczych i KT 264 ds. Systemów Sygnalizacji Pożarowej

Podkomitety Techniczne

Zmiana umiejscowienia Sekretariatu

W lutym prowadzenie sekretariatu KT 277/PK 3 ds. Przesyłu Paliw Gazowych, po rezygnacji Operatora Gazociągów Przesyłowych GAZ-SYSTEM SA, przejął Instytut Nafty i Gazu – Państwowy Instytut Badawczy

Nowi Sekretarze Podkomitetów Technicznych

W lutym Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w KT 176/PK 8 ds. Eksploatacji Uzbrojenia i Sprzętu Marynarki Wojennej mgra inż. Jarosława Błaszkiewicza reprezentującego Dowództwo Generalne Rodzajów Sił Zbrojnych
- w KT 277/PK 3 ds. Przesyłu Paliw Gazowych mgr Monikę Wojciechowską reprezentującą Instytut Nafty i Gazu – Państwowy Instytut Badawczy

Nowy członek Podkomitetów Technicznych

W lutym Prezes PKN powołał na członka PK

- Fiorentini Polska Sp. z o.o. do KT 277/PK 1 ds. Pomiarów i Oceny Jakości Paliw Gazowych, KT 277/PK 2 ds. Dystrybucji Paliw Gazowych i KT 277/PK 3 ds. Przesyłu Paliw Gazowych

SZKOLENIE ON-LINE

Zapewnienie dostępności podmiotów publicznych zgodnie z ustawą o dostępności

Szkolenie przygotowuje uczestnika do zapewnienia dostępności osobom ze szczególnymi potrzebami oraz do realizowania funkcji koordynatora dostępności.

Omawiane zagadnienia to między innymi:

- Kwalifikacje i obowiązki koordynatora dostępności
- Osoby ze szczególnymi potrzebami
- Uniwersalne projektowanie
- Plan działania na rzecz poprawienia dostępności
- Dostępność architektoniczna, cyfrowa, komunikacyjno-informacyjna
- Wyważenie kosztów i możliwości instytucji w odniesieniu do wymagań przepisów
- Kontrola dostępności w jednostce
- Kary za brak dostępności
- Sprawozdania z dostępności
- Deklaracja dostępności
- Skargi na dostępność