wiadomości PKN

NORMALIZACJA

4/2021

4/2021

„**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!

Zabezpieczenia biometryczne są niewątpliwie odpowiednim wyborem w przypadku ochrony wrażliwych danych lub kontroli dostępu do konkretnych pomieszczeń. Dane biometryczne są unikalne dla osób fizycznych, ale okazuje się, że niczego nie możemy być pewni na 100%.

Karty, hasła i osobiste numery identyfikacyjne można anulować lub zmienić w przypadku utraty, zagubienia lub kradzieży, podczas gdy z odciskami palców, które zostały skopiowane i niewłaściwie wykorzystane, już tak postąpić się nie da. Ponadto informacje biometryczne są przechowywane w bazach, które muszą być chronione przed wszelkimi potencjalnymi naruszeniami bezpieczeństwa.

Chociaż cechy biometryczne są trudniejsze do odtworzenia, to istnieją pewne obawy dotyczące bezpieczeństwa związane z systemami, które ich używają. Jednym z wyzwań związanych z urządzeniami do przechwytywania systemów biometrycznych jest to, że jeżeli ktoś zechce je złamać, nie wymaga się od niego znajomości wewnętrznego systemu operacyjnego.

Ważne jest świadome podejście do tego zagadnienia i wykorzystanie wiedzy zawartej w normach, by zapobiec naruszeniom biometrycznym. Więcej można przeczytać w tym numerze „Wiadomości PKN".

Zapraszam do lektury

Joanna Skalska

fot. © zapp2photo / Adobe Stock

Przyszłość zrównoważonego transportu w miastach

Natalie Mouyal

Rozwiązanie problemu mobilności miejskiej to najważniejsze wyzwanie, przed którym staną miasta w nadchodzącym dziesięcioleciu. Według UNEP transport odpowiada za prawie jedną czwartą światowej emisji CO_2. Populacja miast stale rośnie, tak samo jak liczba samochodów, systemy transportowe są nieefektywne, więc zanieczyszczenie środowiska będzie się tylko nasilać.

W 2020 roku, w wyniku globalnego lockdownu spowodowanego pandemią COVID-19, mobilność spadła. Według IEA transport drogowy w regionach objętych lockdownem spadł o 50-75%, natomiast światowa średnia aktywność w transporcie w marcu 2020 spadła o niemal 50% w stosunku do danych z końca marca 2019 r. Jednak globalny poziom emisji dwutlenku węgla znowu wzrósł; w grudniu 2020 r. poziom emisji był wyższy o 2% niż w grudniu 2019 r.

Odnajdując nową normalność

Dla wielu pandemia może być okazją do lepszego opracowywania ekologicznych rozwiązań dla zrównoważonego rozwoju. W szczytowym okresie lockdownu w Europie, władze miejskie, od Bukaresztu po Helsinki, wprowadziły nową infrastrukturę rowerową z 2300 km ścieżek rowerowych, wydając na to ponad miliard euro.

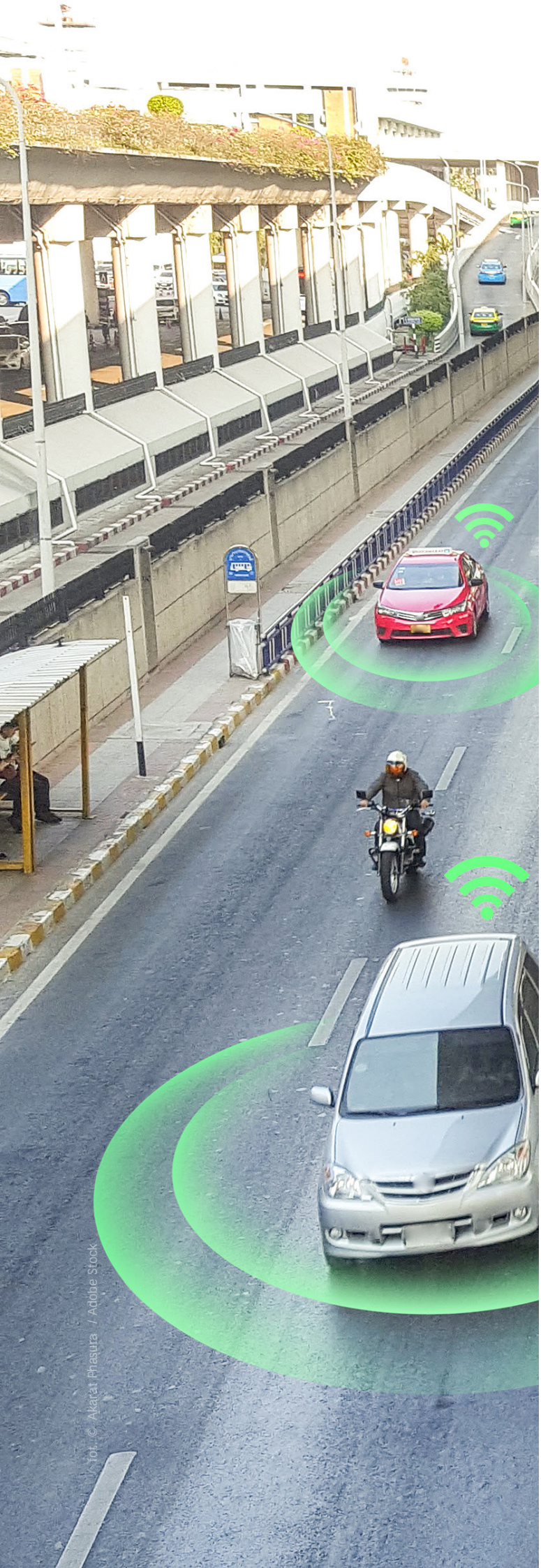
Równocześnie jednak pandemia spowodowała zmniejszenie wykorzystania transportu publicznego, w niektórych miastach odnotowano spadek liczby pasażerów o jedną trzecią, ponieważ mieszkańcy pracowali z domu lub unikali transportu zbiorowego. W innych częściach świata natomiast ruch samochodowy przekroczył poziom sprzed pandemii. W porównaniu z rokiem poprzednim, ruch drogowy w Londynie wzrósł o 20%, a w Perth w Australii o 18%.

Przełomowa innowacja

Transport jest istotnym czynnikiem zapewniającym rozwój. Zrównoważony transport jest wpisany w Cele Zrównoważonego Rozwoju ONZ (SDG), w szczególności w SDG 11, który mówi o uczynieniu miast i osiedli ludzkich bezpiecznymi, odpornymi i zrównoważonymi. Przed pandemią COVID-19 podejmowano wysiłki w celu znalezienia nowych sposobów na ograniczenie negatywnego wpływu transportu na środowisko. Niedawne postępy technologiczne stwarzają potencjalne możliwości w tym zakresie.

Nowe technologie, takie jak sztuczna inteligencja, Internet Rzeczy (IoT), chmura obliczeniowa, mogą wprowadzić inteligencję do sektora transportu. Dzięki inteligentnym systemom transportu (*intelligent transport systems* – ITS) miasta mogą wykorzystać zalety nowych technologii, aby zmniejszyć korki uliczne i zanieczyszczenie, zużycie paliwa i energii elektrycznej oraz zoptymalizować czas podróży. W przypadku transportu publicznego dostępność można dostosować na podstawie zapotrzebowania na podróże i informacje udostępniane pasażerom, by pomóc im w planowaniu podróży.

Będzie to wymagało integracji tych technologii z infrastrukturą obejmującą całe miasto, która może monitorować warunki drogowe i zarządzać nimi, a także opracowywać modele prognostyczne w celu przewidywania ewentualnych zatorów drogowych.



fot. © Akarat Phasura / Adobe Stock

Konieczna będzie wymiana informacji pomiędzy pojazdami a infrastrukturą, co może budzić obawy związane z prywatnością i bezpieczeństwem.

Wiele z tych nowych technologii bazuje na normach opracowanych przez Wspólny Komitet Techniczny IEC i ISO zajmujący się technologią informacyjną (ISO/IEC JTC 1). Jego tematyka obejmuje takie zagadnienia jak inżynieria oprogramowania, sztuczna inteligencja, IoT, biometria i prywatność.

Elektryfikacja transportu

Sprzedaż pojazdów elektrycznych nadal wzrasta, nawet pomimo odnotowania spadku spowodowanego pandemią COVID-19. Przewiduje się (wg Deloitte), że trend dalszego wzrostu utrzyma się przez całą dekadę. Koncentrując się na poprawieniu jakości powietrza, wiele miast takich jak Helsinki, Santiago i Kalkuta, wprowadziło elektryczne autobusy. W 2019 na całym świecie sprzedano rekordową liczbę elektrycznych ciężarówek, a nowe badania nad koncepcjami dynamicznego ładowania rozszerzyły zakres transportu długodystansowego.

Oczekuje się, że także ceny akumulatorów będą niższe. Nowe technologie produkcji akumulatorów sprzyjają upowszechnianiu się elektromobilności. Przykładowo, na początku stycznia 2021 roku izraelska firma ogłosiła, że wyprodukowała akumulatory, które można w pełni naładować w ciągu pięciu minut. Inne firmy na całym świecie również opracowują podobne akumulatory; oczekuje się, że ta technologia będzie dostępna na rynku masowym w ciągu pięciu lat.

Ruch w kierunku elektryfikacji transportu dotyczy prac normalizacyjnych wielu komitetów technicznych IEC m.in.: TC 9 *Electrical equipment and systems for railways*, TC 21 *Secondary cells and batteries*, TC 23 *Electrical accessories*, TC 69 *Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks* oraz TC 125 *Personal e-Transporters*.

Zasilanie inteligentnej sieci

Integracja systemów transportowych z siecią elektryczną jest kolejnym krokiem ku zrównoważonemu transportowi. Sieć elektryczna jest na etapie wdrażania inteligentnych technologii oraz integracji odnawialnych źródeł energii w ramach sieci. Umożliwi to pojazdom elektrycznym dostęp do energii elektrycznej z czystych źródeł, co z kolei przyczyni się do dalszego zmniejszania zanieczyszczenia.

Trwają również prace badawcze nad potencjalnym wykorzystaniem pojazdów elektrycznych do pomocy w zarządzaniu obciążeniem sieci. Według IEA energia może być magazynowana w akumulatorach pojazdów elektrycznych, a tym samym dostarczać energię do sieci w odpowiednim czasie za pośrednictwem rozwiązań typu pojazd – sieć (V2G).

Komitet Systemowy IEC ds. Inteligentnej Energii koordynuje prace kilku komitetów technicznych pracujących nad publikacją norm z zakresu cyfryzacji, automatyzacji i modernizacji sieci, w tym urządzeń i systemów końcowych sieci.

Ponadto, IEC/TC 57 *Power systems management and associated information exchange* opracował serię norm IEC 61850, które uważane są za podstawowe normy technologii cyfrowych związanych z inteligentną energią. Normy te dotyczą integracji energii ze źródeł odnawialnych i energii ze źródeł rozproszonych (*distributed energy resources* – DER) w ramach sieci elektrycznej. IEC/TC 57 wspiera także inteligentne ładowanie pojazdów elektrycznych (EV) w ramach współpracy z IEC/TC 69. PKN/KT 183 ds. Bezpieczeństwa Urządzeń Informatycznych, Telekomunikacyjnych i Biurowych jest komitetem wiodącym w zakresie współpracy z IEC/TC 57, a PKN/KT 61 ds. Elektrycznego Wyposażenia Trakcyjnego z IEC/TC 69.

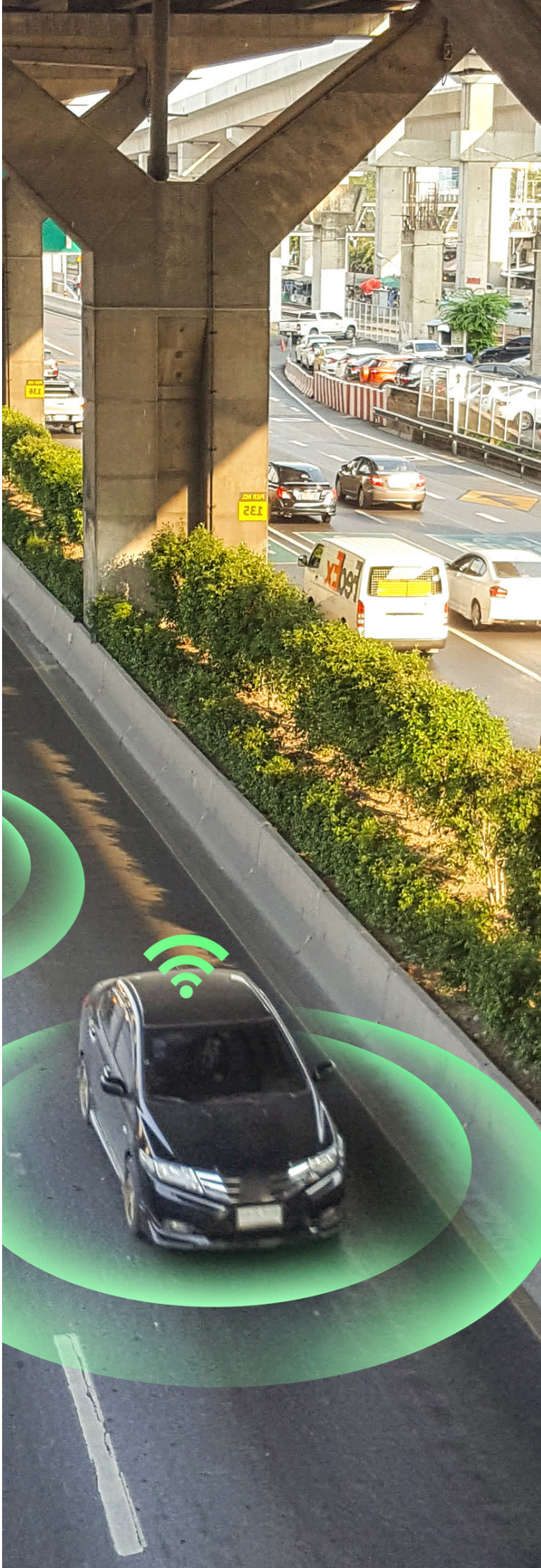
Rola norm

Normy są niezbędne dla rozwoju kolejnych generacji zrównoważonej mobilności. Zapewniają interoperacyjność, wydajność i bezpieczeństwo w obszarach takich jak zabezpieczenia, protokoły komunikacyjne, akumulatory, inteligentne sieci i stacje ładujące.

IEC przyjęła podeście systemowe do inteligentnych miast w celu zapewnienia holistycznego podejścia do rozwiązywania skomplikowanych sytuacji. Komitet Systemowy IEC ds. Inteligentnych Miast aktywnie koordynuje prace normalizacyjne różnych komitetów IEC i innych grup w celu promowania rozwoju norm wspomagających integrację, interoperacyjność i efektywność systemów miejskich.

W 2019 IEC założyła Standardization Evaluation Group, SEG 11, mającą na celu opracowanie studiów przypadku i analizy luk w celu określenia wymagań dotyczących przyszłości zrównoważonego transpotu. SEG 11 ma opublikować raport z rekomendacjami w czerwcu 2021.

Tłum. I. P.
IEC e-tech, Issue 02/2021



Ochrona naszej prywatności w inteligentych miastach

Clare Naden

Chmura obliczeniowa, Internet Rzeczy, sieci mobilne i sztuczna inteligencja to tylko niektóre z narzędzi, których miasta używają do zwiększenia wydajności i poprawy jakości życia swoich obywateli, których wykorzystanie pomoże w rozwiązaniu tych kwestii. Jednak nie zawsze łatwo się między nimi poruszać, kiedy systemy i połączenia są tak złożone, jak wielu jest interesariuszy. Właśnie opublikowano nową specyfikację techniczną, która ma w tym pomóc.

ISO/IEC TS 27570 *Privacy protection – Privacy guidelines for smart cities* zapewnia zalecenia i wytyczne dotyczące zarządzania prywatnością i stosowania norm wspomagających. Zalecenia te mają zastosowanie do organizacji i interesariuszy zainteresowanych dostarczaniem, użytkowaniem lub dostępnością usług w ekosystemie inteligentnego miasta, w którym wiele technologii, systemów i interesariuszy współdziała na wiele złożonych sposobów.

Profesor Kai Rannenberg, lider grupy ekspertów[1], która opracowała specyfikację techniczną, uważa, że ta złożoność może stanowić wyzwanie dla ochrony prywatności, „jednak istnieje wiele różnych norm, które można zastosować, w tym te obejmujące duże zbiory danych, chmurę obliczeniową, zarządzanie IT i wiele innych".

„Najważniejsze to wiedzieć, która norma i w jaki sposób będzie najbardziej odpowiednia. ISO/IEC TS 27570 zawiera wskazówki, w jaki sposób najlepiej zastosować dostępne normy".

Dokument przyjmuje punkt widzenia skupiający się na wielu agencjach i obywatelach, ponadto zawiera wskazówki, jak stosować normy prywatności na poziomie globalnym i organizacyjnym z korzyścią dla obywateli.

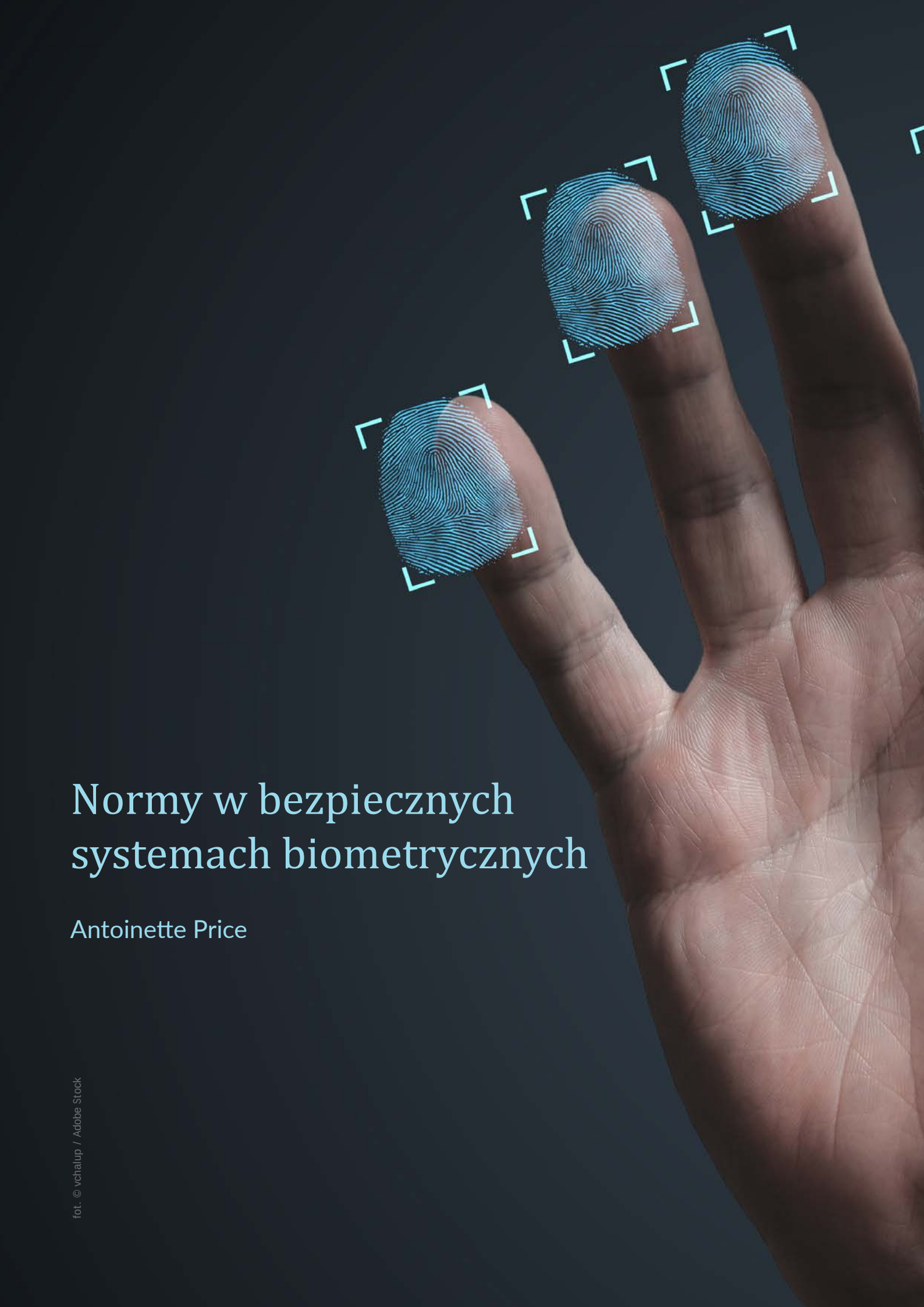
Co więcej, utoruje drogę przyszłym normom prywatności dla inteligentnych miast, w tym tych dotyczących komunikacji, planów zarządzania prywatnością i tworzenia polityki, a także zarządzanie zgodami.

ISO/IEC TS 27570 ma zastosowanie do wszystkich typów i rozmiarów organizacji, włączając w to firmy publiczne i prywatne, jednostki rządowe oraz organizacje not-for-profit, świadczące usługi w środowiskach inteligentnych miast.

Specyfikacja techniczna została opracowana przez podkomitet SC 27 *Information security, cybersecurity and privacy protection* działający w ramach Wspólnego Komitetu Technicznego ISO/IEC JTC 1, stworzonego przez ekspertów z branży IT w ISO oraz ekspertów Międzynarodowej Komisji Elektrotechnicznej (IEC). Sekretariat SC 27 jest prowadzony przez DIN, niemiecką jednostkę normalizacyjną.

Tłum. I. P.
www.iso.org

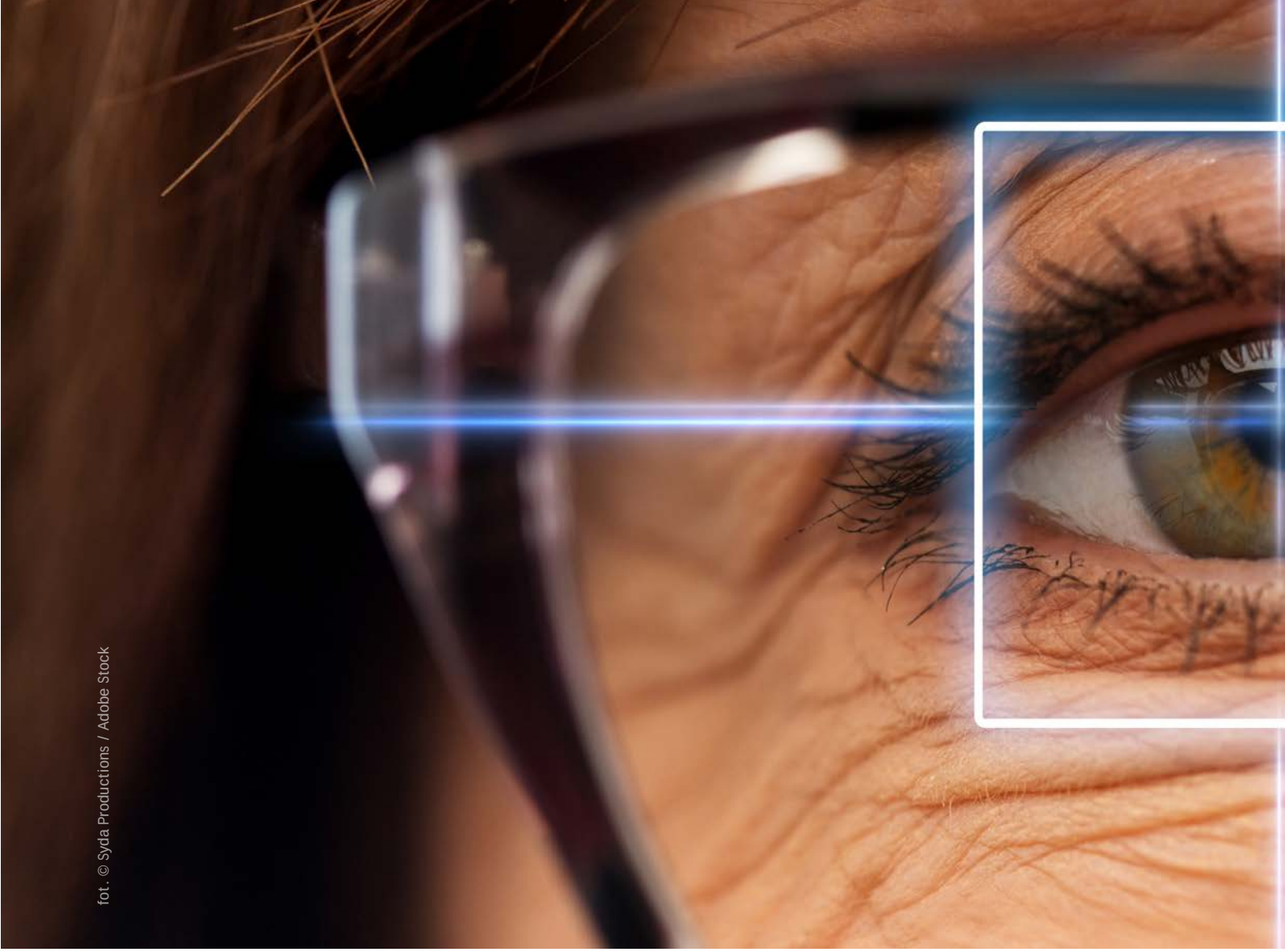
[1] Eksperci Grupy Roboczej WG 5 w ISO/IEC JTC 1/SC 27 *Identity management and privacy technologies*.



Normy w bezpiecznych systemach biometrycznych

Antoinette Price

Biometria obejmuje fizyczne i behawioralne cechy charakterystyczne, takie jak linie papilarne, rysy twarzy, głos czy podpis, unikalne dla każdej osoby.
Mogą być wykorzystywane cyfrowo w celu identyfikacji i umożliwienia odpowiednim osobom uzyskania dostępu do budynków, systemów i urządzeń czy wjazdu na teren kraju.



fot. © Syda Productions / Adobe Stock

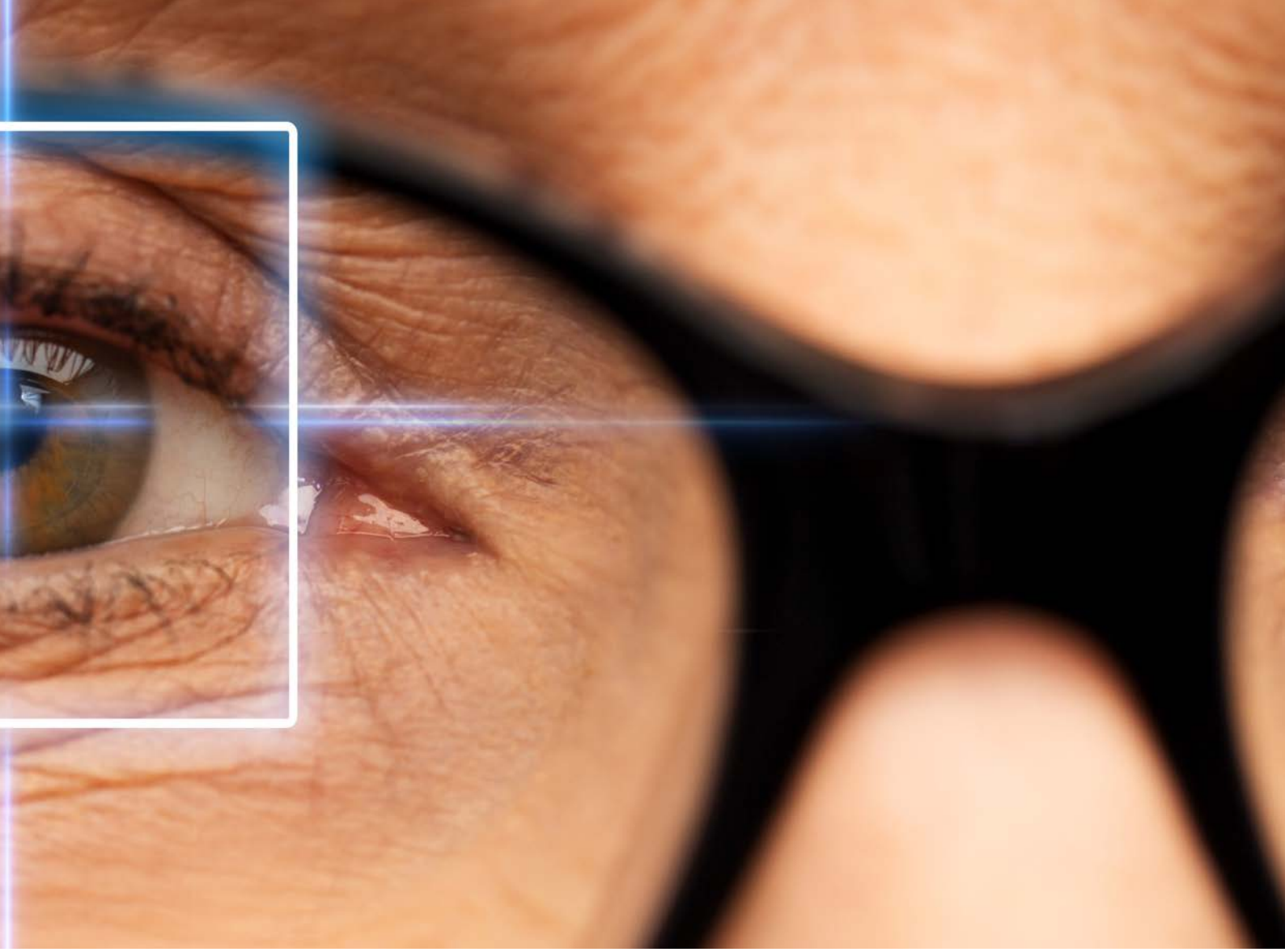
Biometria może znacznie ułatwić życie osobom mającym problemy z zapamiętaniem haseł lub osobom z pewnymi niepełnosprawnościami fizycznymi. Jest wykorzystywana w coraz większej liczbie aplikacji i oferuje rozwiązania bezkontaktowe, co pomaga w powstrzymaniu rozprzestrzeniania się COVID-19.

System rozpoznawania twarzy, wykorzystywany na lotniskach i w systemach kontroli granicznej, identyfikuje obywateli i pozwala im na opuszczenie jednego kraju i wstęp do innego. W innych sytuacjach ta technologia może otwierać drzwi i udostępniać autoryzowanym użytkownikom strefy o wysokim poziomie bezpieczeństwa. W domach systemy rozpoznawania głosu są wykorzystywane do kontrolowania ogrzewania, oświetlenia i systemów multimedialnych, wielu z nas wykorzystuje je do szybkiego wyszukiwania informacji. Czytniki linii papilarnych oferują szybki sposób odblokowania smartfonów i iPadów.

Chociaż cechy biometryczne są trudniejsze do odtworzenia, istnieją pewne obawy dotyczące bezpieczeństwa związane z systemami, które ich używają. Jednym z wyzwań związanych z urządzeniami do przechwytywania systemów biometrycznych jest to, że jeżeli ktoś zechce je złamać, nie wymaga się od niego znajomości wewnętrznego systemu operacyjnego.

Ktoś mógłby np. użyć fałszywych linii papilarnych lub osłonięcia twarzy, aby uzyskać dostęp do systemu. Jest to naruszenie zabezpieczeń biometrycznych (*presentation attack*).

Mike Thieme to edytor/redaktor dwóch Norm Międzynarodowych opracowanych przez Wspólny Komitet Techniczny IEC i ISO zajmujący się biometrią. Wśród dokumentów są: ISO/IEC 30107-3, która uwzględnia testowanie i raportowanie wykrywania naruszeń zabezpieczeń biometrycznych (*biometric presentation attack detection* – PAD) oraz ISO/IEC 30107-4, która przedstawia podejście przyjęte dla nowych wymagań związanych z testowaniem PAD na urządzeniach mobilnych.



Czym jest wykrywanie naruszeń zabezpieczeń biometrycznych?

Wiele osób wie, że fałszywy odcisk palca, maska, a nawet nagranie głosowe mogą posłużyć do uzyskania nieautoryzowanego dostępu do systemu biometrycznego. Przez większość historii komercyjnych technologii biometrycznych, urządzenia biometryczne, takie jak czujniki linii papilarnych, są w stanie wykryć kiedy te ataki mają miejsce. Jednak niektóre urządzenia są lepsze od innych. Zdolność do wykrycia tego typu naruszeń nazywamy wykrywaniem naruszeń zabezpieczeń biometrycznych (*biometric presentation attack detection* – PAD). Przedmiot użyty do naruszenia nazywamy instrumentem naruszenia biometrycznego (*presentation attack instrument* – PAI).

Poza tym, ta koncepcja nie ogranicza się tylko do fałszywych lub sztucznych ataków jak np. maska. Obejmuje to również przypadki, kiedy osoby uszkadzają swoje cechy biometryczne. Klasycznym przykładem są osoby, które niszczą swoje linie papilarne, aby uniknąć wykrycia podczas przeszukiwania bazy danych odcisków palców, np. w sprawach karnych.

Jakie są niektóre z wyzwań?

Atakujący mający dostęp do sprzętu i oprogramowania biometrycznego, dysponujący czasem i pieniędzmi mogą tworzyć wysoce realistyczne fałszywe dane biometryczne, które bardzo trudno wykryć. Na przykład czytnik linii papilarnych może wyszukiwać określone sposoby pochłaniania i odbijania światła przez palce. Mając wystarczająco dużo czasu, atakujący mogą odtworzyć aspekty istotne do wykrywania naruszeń biometrycznych.

Jednak to tylko część wyzwania. Możliwe, że większym problemem jest to, że naruszenia biometryczne są rzadkie. Większość transakcji biometrycznych jest normalna w tym sensie, że z urządzenia korzysta tylko jedna osoba upoważniona (np. próbująca odblokować iPhone'a).

Oznacza to, że programiści systemów biometrycznych nie mogą sprawdzić, czy naruszenie zabezpieczeń biometrycznych będzie zbyt agresywne lub zbyt czułe. Gdyby tak było, uprawnieni użytkownicy byliby odrzucani zbyt często, co byłoby nie do przyjęcia. Znalezienie kompromisu w tej sytuacji jest trudne.

fot. © ryanking999 / Adobe Stock

Czemu ma służyć część 4 normy?

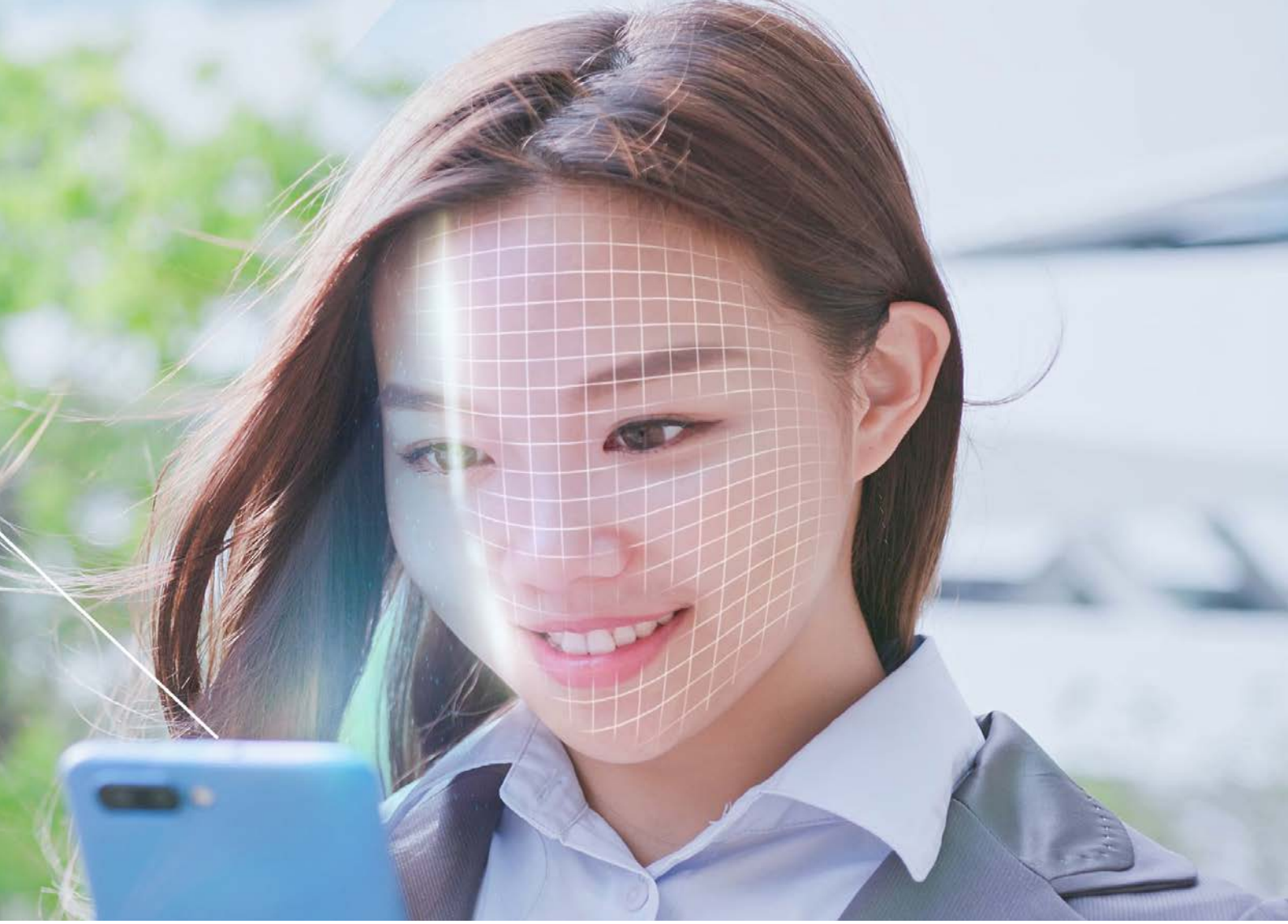
ISO/IEC 30107-3 określa metodologie oceny wydajności wykrywania naruszeń biometrycznych (PAD) dla całej sfery systemów biometrycznych, od krajowych dokumentów potwierdzających tożsamość, po zabezpieczenia komputerów stacjonarnych. Część 3 obejmuje również przypadki, w których wykrywanie naruszeń biometrycznych jest oddzielnym, samodzielnym podsystemem.

Urządzenia mobilne stanowią niewielki, ale bardzo ważny podzbiór ogólnej przestrzeni problemowej PAD. Potrzebowaliśmy profilu, który wyciągnie sekcje i wymagania części 3 mających zastosowanie do urządzeń mobilnych i ułatwi pracę testerom, którzy chcą się skupić na urządzeniach mobilnych.

Urządzenia mobilne to kompletne systemy – nie można ich rozsądnie rozebrać i dowiedzieć się, która część działa dobrze. Test musi ocenić cały system z interakcją w czasie rzeczywistym. To szczególny przypadek.

ISO/IEC 30107-4 robi to i ustanawia dodatkowe wymagania, nieuwzględnione w części 3. Dla każdego wymagania definiuje podejście do testowania PAD w urządzeniach mobilnych.

fot. © Oleg / Adobe Stock



Jakie są dodatkowe wymagania w testach urządzeń mobilnych?

W przypadku urządzeń mobilnych, ze względu na wymagania czasu rzeczywistego, ocena jest prawie zawsze ograniczona do niewielkiej liczby przedmiotów – być może kilkuset. Ta niewielka próbka oznacza, że trudno byłoby zweryfikować wydajność przy niskich poziomach błędu takich jak 0,01%.

Ponadto, jeśli instrument naruszenia biometrycznego (PAI) zawiedzie – to znaczy, że nie pasuje do zamierzonego celu – trudno jest ocenić, czy awaria wystąpiła na skutek niedopasowania biometrycznego, czy wykrycia PAI. Potrzebne są więc konkretne wskaźniki, które łączą te dwa przypadki awarii w jeden.

Czy można mówić o różnych rolach w testowaniu PAD?

Jednym z najbardziej interesujących aspektów testowania PAD są różne role, jakie mogą pełnić poszczególne osoby. Role te mogą być niejednoznaczne i złożone. Osoba prezentująca PAI na urządzeniu mobilnym – prezenter PAI – może wpłynąć na działanie PAD, jeśli jej rzeczywistą charakterystykę biometryczną można wykryć pod PAI lub jeśli nie ma umiejętności posługiwania się urządzeniem mobilnym. Dodatkową rolą jest źródło PAI lub osoba, której cechy biometryczne zostały wykorzystane do stworzenia PAI. Jest to np. dawca fałszywego odcisku palca. Być może najważniejszą rolę odgrywa twórca PAI, który tworzy lub formułuje PAI, wykorzystując zarówno kreatywność, jak i umiejętności inżynieryjne. Każda z ról wpływa na ogólną metodologię oceny i należy ją uważnie rozpatrzeć.

Tłum. I. P.

IEC e-tech, Issue 02/2021

fot. © md3d / Adobe Stock

Znaczenie kontroli dostępu w cyberbezpieczeństwie

Michael A Mullane

Jest taki stary kawał, że najlepsze hasło to „s n o w w h i t e a n d t h e 7 d w a r f s", ponieważ zawiera osiem znaków i cyfrę. Każdy z nas, od czasu do czasu, denerwował się koniecznością aktualizacji danych logowania. Jednak kontrola dostępu to nie powody do śmiechu.

Dwa główne cyberataki w ostatnich miesiącach zaczęły się od słabego hasła i kradzieży danych uwierzytelniających; to podkreśliło znaczenie odpowiednich środków bezpieczeństwa i rozbudowanej procedury cyberbezpieczeństwa. Ludzie są najczęstszą przyczyną naruszeń bezpieczeństwa, niezależnie od tego, czy klikają w link w wiadomości phishingowej, czy przytrzymują otwarte drzwi intruzowi, który wchodzi za nimi do biurowca.

Dlatego właśnie kontrola dostępu jest kluczowym elementem cyberbezpieczeństwa. Polega na tym, że organizacje muszą mieć pewność, że użytkownicy są tymi, za których się podają i że mają pozwolenie na korzystanie z określonych zasobów sieciowych lub wejście do zastrzeżonych obszarów. Kontrola dostępu służy nie tylko do zabezpieczania zasobów, ale może również pomóc w ustaleniu przyczyny cyberataku.

Są dwa rodzaje kontroli dostępu – fizyczna i logiczna. Kontrola fizyczna ogranicza dostęp do pomieszczeń, stacji roboczych i sprzętu IT, natomiast kontrola logiczna tyczy się ograniczenia dostępu do szczególnie istotnych zasobów cybernetycznych. Oba rodzaje są niezbędne dla cyberbezpieczeństwa i bazują na założeniu, że użytkownicy, urządzenia i inne podmioty żądające dostępu są nieznane, dopóki nie zostaną zweryfikowane przez system. Aby tak się stało, muszą mieć unikalny identyfikator, taki jak np. nazwa użytkownika, adres e-mail, który ich zidentyfikuje.

Zasada najmniejszego uprzywilejowania

Słabe i niewystarczające środki bezpieczeństwa są po prostu katastrofą czekającą na swój moment. Amerykańska Agencja Bezpieczeństwa Narodowego dowiedziała się o tym w złych okolicznościach, w momencie gdy Edward Snowden ujawnił mediom dokumenty. Oprócz publicznej reakcji na skandal związany z inwigilacją, agencja starła się także z falą krytyki swojej polityki cyberbezpieczeństwa, szczególnie kontroli dostępu. Koniec końców, NSA ograniczyła dostęp do sieci do poziomu niezbędnego do wykonywania pracy przez poszczególne osoby. Zasada znana jako „zasada najmniejszego uprzywilejowania" jest głównym środkiem bezpieczeństwa rekomendowanym przez IEC 62443-2-1 w celu zabezpieczenia najważniejszej infrastruktury i innych przemysłowych systemów automatyki i sterowania (*industrial automation and control systems* – IACS) przed nieautoryzowanym dostępem. Podobnie, ISO/IEC 27001 rekomenduje zasadę najmniejszego uprzywilejowania w ochronie danych: „Użytkownikom należy zapewnić dostęp tylko do sieci i usług sieciowych, do korzystania z których zostali specjalnie upoważnieni".

Wdrożenie takiej polityki wymaga kompleksowego podejścia do zasad zarządzania tożsamością i aktywami. Oprócz starannego zarządzania uprawnieniami, ważne jest rejestrowanie działań użytkownika, aby stworzyć ścieżkę audytu w przypadku naruszenia. Wreszcie dodawanie i usuwanie praw, zwane nadawaniem i wyłączaniem, nie może mieć negatywnego wpływu na produktywność. Muszą obowiązywać zasady, aby dodawać przywileje w razie potrzeby i odbierać je po zakończeniu projektów lub w przypadku wygaśnięcia umowy o pracę.

Uwierzytelnianie i autoryzacja

Wiele Norm Międzynarodowych dotyczy procesu uwierzytelniania – gdy weryfikowane jest urządzenie i tożsamość użytkownika – oraz autoryzacji, która określa, czy użytkownik może uzyskać dostęp do określonego zasobu na swoim poziomie uprawnień. Należą do nich np. seria norm IEC 62443 oraz seria norm ISO/IEC 27000. IEC 60839-11-5 obejmuje fizyczne kontrole dostępu, w tym dane biometryczne takie jak linie papilarne, skany tęczówki i karty.

Normy IEC przyjmują podejście holistyczne do ograniczania ryzyka, odnosząc się nie tylko do technologii i procedur, lecz także do ludzi. Szkolenia i działania związane z budowaniem potencjału są postrzegane jako niezbędne do podnoszenia świadomości i tworzenia zdrowej kultury cyberbezpieczeństwa. Jest to szczególnie ważne w czasach, gdy z powodu pandemii koronawirusa coraz więcej ludzi pracuje w systemie telepracy. Obecna sytuacja zwiększa złożoność kontroli dostępu z uwagi na fakt, że użytkownicy logują się do wielu aplikacji biznesowych i podsieci z komputerów domowych. Normy IEC pomagają organizacjom w zarządzaniu rolami i wydajnym rozdzielaniu praw sieciowych przy jednoczesnym osiąganiu zadowalającego kompromisu między funkcjonalnością i bezpieczeństwem.

Tłum. I. P.
IEC e-tech, Issue 02/2021

ORGANY TECHNICZNE

fot. © comzeal / Adobe Stock

MARZEC 2021

Komitety Techniczne

Zmiany zakresów tematycznych Komitetów Technicznych

- KT 61 ds. Elektrycznego Wyposażenia Trakcyjnego rozszerzył współpracę o CEN/CLC/JTC 20, Hyperloop systems
- KT 63 ds. Elektrycznego Sprzętu Powszechnego Użytku rozszerzył współpracę o CLC/BTTF 160-1, Recurrent Test of Electrical Equipment
- KT 322 ds. Materiałów Odniesienia rozszerzył współpracę o ISO/TC 334, Reference materials

Zmiany umiejscowienia Sekretariatów Komitetów Technicznych

W marcu prowadzenie sekretariatów:

- KT 13 ds. Maszyn do Robót Ziemnych i Drogowych oraz Żurawi Samojezdnych po rezygnacji Sieci Badawczej Łukasiewicz - Instytutu Mechanizacji Budownictwa i Górnictwa Skalnego przejął Urząd Dozoru Technicznego
- KT 14 ds. Maszyn i Urządzeń dla Budownictwa, Przemysłu Materiałów Budowlanych oraz Górnictwa Skalnego po rezygnacji Sieci Badawczczej Łukasiewicz - Instytutu Mechanizacji Budownictwa i Górnictwa Skalnego przejął Polski Komitet Normalizacyjny

Nowi Przewodniczący Komitetów Technicznych

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

- w KT 5 ds. Chłodnictwa, Pomp Ciepła, Klimatyzatorów i Sprężarek dra hab. inż. Bartosza Zajączkowskiego reprezentującego Politechnikę Wrocławską
- w KT 125 ds. Udostępniania i Eksploatacji Złóż Kopalin dra inż. Sylwestra Rajwę reprezentującego Główny Instytut Górnictwa
- w KT 322 ds. Materiałów Odniesienia prof. dr hab. Ewę Bulską reprezentującą Uniwersytet Warszawski

Nowi Sekretarze Komitetów Technicznych

W marcu Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w KT 13 ds. Maszyn do Robót Ziemnych i Drogowych oraz Żurawi Samojezdnych mgra inż. Piotra Kapicę reprezentującego Urząd Dozoru Technicznego
- w KT 14 ds. Maszyn i Urządzeń dla Budownictwa, Przemysłu Materiałów Budowlanych oraz Górnictwa Skalnego Pana Mateusza Danielewskiego z Polskiego Komitetu Normalizacyjnego
- w KT 62 ds. Sprzętu Elektroinstalacyjnego mgr Patrycję Brzęczkowską reprezentującą Legrand Polska Sp. z o.o.

Nowi członkowie Komitetów Technicznych

W marcu Prezes PKN powołał na członków KT następujące podmioty:

- ELIKO MOŃKA Spółka Jawna do KT 63 ds. Elektrycznego Sprzętu Powszechnego Użytku
- ICR Polska Sp. z o.o. do KT 247 ds. Materiałów Medycznych i Biomateriałów
- IMPACTIS Marcin Bugała do KT 324 ds. Zarządzania w Organizacjach Ochrony Zdrowia
- PCFS Technology Sp. z o.o. do KT 282 ds. Techniki Światłowodowej
- Polskie Domy Drewniane S.A. do KT 100 ds. Wyrobów z Drewna i Materiałów Drewnopochodnych i KT 215 ds. Projektowania i Wykonawstwa Konstrukcji z Drewna i z Materiałów Drewnopochodnych

Odwołani członkowie Komitetów Technicznych

W marcu Prezes PKN odwołał z członka KT następujące podmioty:

- Instytut Żywności i Żywienia im. prof. dra med. Aleksandra Szczygła z KT 200 ds. Koncentratów Spożywczych, Skrobi i Produktów Dietetycznych
- Sieć Badawczą Łukasiewicz - Instytut Obróbki Plastycznej z KT 207 ds. Obróbki Ubytkowej i Przyrostowej oraz Charakterystyki Warstwy Wierzchniej
- Unimetal Recycling Sp. z o.o. z KT 7 ds. Badań Nieniszczących, KT 121 ds. Jakości Wody - Badania Chemiczne – Substancje Nieorganiczne, KT 216 ds. Odpadów i KT 221 ds. Górnictwa, Przeróbki i Analiz Rud

Podkomitety Techniczne

Nowy Przewodniczący Podkomitetu Technicznego

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

- w KT 176/PK 4 ds. Sprzętu i Środków Obrony przed Bronią Masowego Rażenia Pana Maksymiliana Stelę reprezentującego Wojskowy Instytut Chemii i Radiometrii

Nowy członek Podkomitetu Technicznego

W marcu Prezes PKN powołał na członka PK:

- COLAS Polska Sp. z o.o. do KT 222/PK 2 ds. Asfaltów w KT 222 ds. Przetworów Naftowych oraz Produktów Podobnych Pochodzenia Biologicznego i Syntetycznego

Odwołany członek Podkomitetu Technicznego

W marcu Prezes PKN odwołał z członka PK:

- Dowództwo Operacyjne Rodzajów Sił Zbrojnych z KT 176/PK 5 ds. Sprzętu Radiotechnicznego, Środków Łączności, Specjalnych Urządzeń Elektrotechnicznych, Techniki Świetlnej oraz Systemów i Środków Informatyki w KT 176 ds. Techniki Wojskowej i Zaopatrzenia

SZKOLENIA ON-LINE

Zdobywaj wiedzę w wygodnej, interaktywnej formie

Oferta najbliższych szkoleń on-line PKN:

- Podstawy pracy IOD - szkolenie dla początkujących inspektorów
- Wymagania ustawy o krajowym systemie cyberbezpieczeństwa a normy PN-EN ISO 22301:2020-04 i PN-EN ISO/IEC 2700:2017-06
- Zasady przeprowadzania auditów zdalnych pierwszej i drugiej strony zgodnych z normą PN-EN ISO 19011:2018-08
- Rola systemu zarządzania ciągłością działania w skutecznym funkcjonowaniu organizacji
- Metodyka i narzędzia zarządzania ryzykiem na podstawie normy PN-ISO 31000:2018-08, PN-EN IEC 31010:2020-01 oraz PN-EN IEC 60812:2018-12
- PN-EN ISO/IEC 27001:2017-06 Audytor wewnętrzny SZBI - wykład, ćwiczenia, warsztaty
- Powierzenie, współadministrowanie, udostępnienie zgodnie z RODO - jakie warunki należy spełnić, jak uniknąć pułapek

Zapoznaj się z pełną listą szkoleń na naszej stronie wiedza.pkn.pl/web/szkolenia

Polski Komitet Normalizacyjny szkolenia@pkn.pl 22 55 67 766