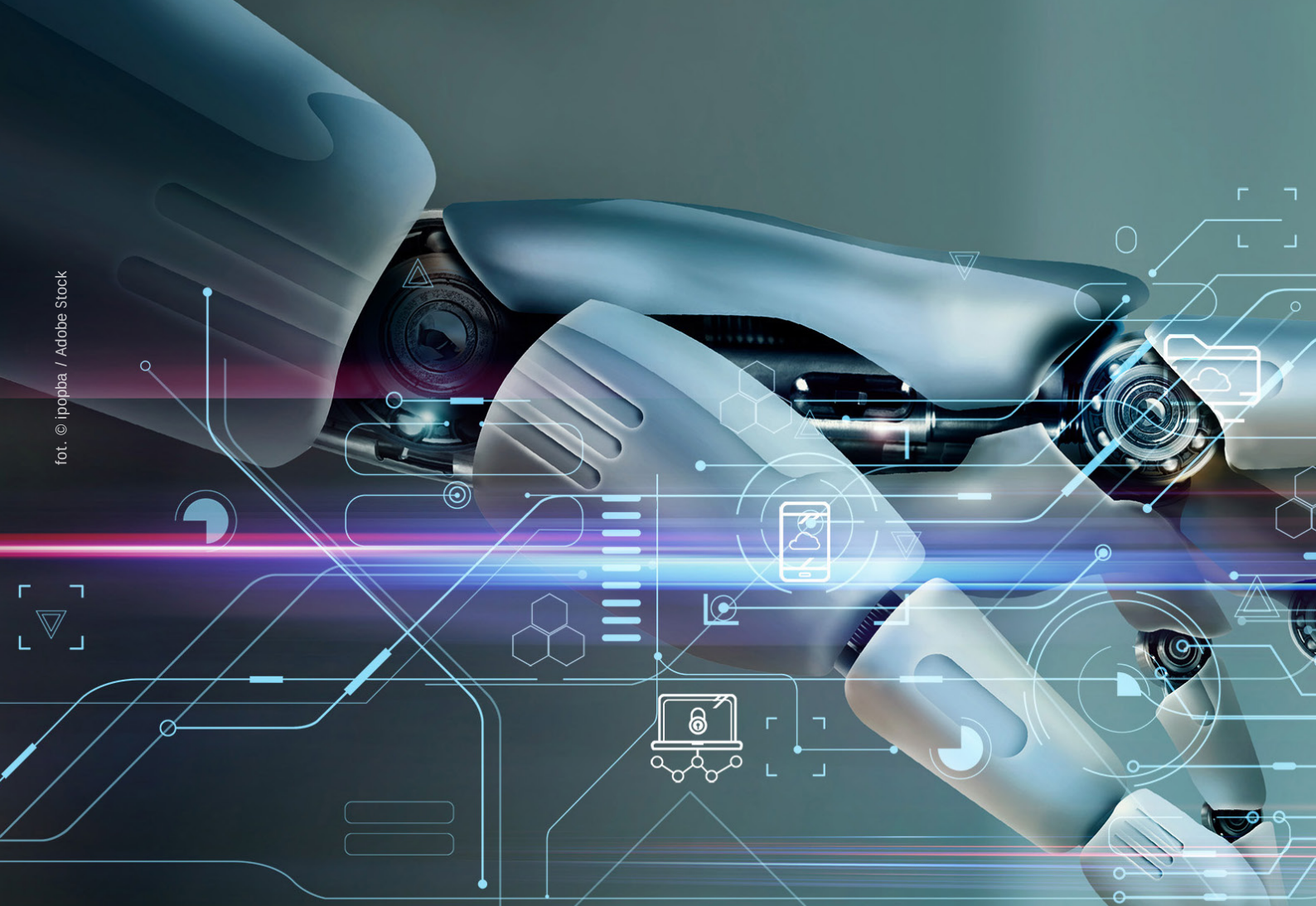

fot. © ipopba / Adobe Stock

Jak zarządzać ryzykiem związanym ze sztuczną inteligencją

Michael A Mullane

W koncepcji zarządzania ryzykiem nie ma niczego nowego. Już w starożytności społeczeństwa rozumiały, że istnieje ryzyko nieodłącznie związane z pewnymi aspektami życia i opracowały strategie mające na celu jego ograniczenie.

Jednym z najwcześniejszych przykładów zarządzania ryzykiem jest zdanie z czasów starożytnego Rzymu – *si vis pacem, para bellum* (tłum. jeśli chcesz pokoju, przygotuj się do wojny).

W czasach współczesnych zarządzanie ryzykiem stało się integralną częścią biznesu i władzy. Firmy zatrudniają specjalistów do spraw ryzyka w celu zidentyfikowania i złagodzenia potencjalnych zagrożeń, począwszy od zagrożeń dla bezpieczeństwa cybernetycznego, po zakłócenia łańcucha dostaw. Pojawienie się nowych technologii zwiększyło potrzebę zachowania czujności i zdolności adaptacyjnych przez osoby zarządzające ryzykiem.

Managerowie ds. ryzyka muszą być w stanie zidentyfikować i ocenić ryzyko związane z nowymi technologiami, a także wdrażać skuteczne strategie zarządzania ryzykiem mające na celu jego ograniczenie. Jednocześnie, muszą być otwarci na nowe rozwiązania oferowane przez pojawiające się technologie, aby wyprzedzać konkurencję i skutecznie zarządzać ryzykiem w szybko zmieniającym się świecie.

Ekspansja sztucznej inteligencji (AI) jest tego przykładem. Przyniosło to rosnącą potrzebę skutecznego zarządzania ryzykiem w celu radzenia sobie z różnymi problemami, od technicznych – takich jak awarie algorytmów, po etyczne – w tym stronniczość w podejmowaniu decyzji. AI ma potencjał, by zrewolucjonizować wiele gałęzi przemysłu i zmienić nasze życie na lepsze, jednak ryzyko związane z jej wykorzystaniem musi być dokładnie przemyślane i zarządzane.

Nowa norma ISO/IEC zapewnia podstawowe wytyczne dotyczące zarządzania ryzykiem dla organizacji wszystkich rozmiarów i typów, które wykorzystują AI w swoich systemach lub procesach. ISO/IEC 23894 pokazuje użytkownikom, jak skutecznie zarządzać ryzykiem związanym z wykorzystaniem AI, aby osiągnąć cele i poprawić wydajność.

„Chociaż systemy AI są pod wieloma względami podobne do tradycyjnych systemów IT, prezentują również nowe aspekty takie jak zdolność uczenia się", twierdzi Wael William Diab, Przewodniczący Wspólnego Komitetu Technicznego IEC i ISO zajmującego się normami z zakresu technologii AI.

„SC 42 przyjął nowatorskie podejście polegające na opracowaniu ram, które wykorzystują ugruntowane techniki zarządzania ryzykiem. ISO/IEC 23894 zapewnia holistyczne i proaktywne podejście do zarządzania ryzykiem związanym z wykorzystaniem AI w celu umożliwienia użytkownikom skutecznego zarządzania ryzykiem i pełnego wykorzystania jej potencjału", dodaje.

Ramy dla zarządzania ryzykiem

Nowa norma dostosowuje i rozwija wytyczne oraz ogólne zasady zarządzania ryzykiem opisane w ISO 31000. Przedstawia ona ramy zarządzania ryzykiem, które wymagają od użytkowników ustalenia kontekstu oraz identyfikacji, analizy, oceny, monitorowania i przeglądu ryzyka.

Ustalanie kontekstu wiąże się z określeniem celów organizacji oraz ryzyka mogącego wpływać na te cele, a także potrzeb i oczekiwań interesariuszy, na których to ryzyko będzie miało wpływ. Identyfikacja ryzyka to wskazanie potencjalnego ryzyka mogącego wpłynąć na cele organizacji, w tym ryzyka związane z działalnością firmy, procesami i czynnikami zewnętrznymi.

Analiza ryzyka oznacza ocenę prawdopodobieństwa i wpływu zidentyfikowanych zagrożeń, a także potencjalnych konsekwencji każdego z nich. Ocena oznacza podjęcie decyzji, którymi ryzykami warto się zająć, na podstawie ich prawdopodobieństwa i potencjalnego wpływu, oraz określenie odpowiedniej reakcji na każde ryzyko.

Postępowanie z ryzykiem polega na wdrożeniu wybranej reakcji na ryzyko, która może obejmować uniknięcie ryzyka, zmniejszenie jego prawdopodobieństwa lub wpływu, przeniesienie go na inną stronę lub zaakceptowanie go. Monitorowanie i przegląd oznacza bieżące monitorowanie ryzyka w celu zapewnienia, że jest ono skutecznie zarządzane oraz przegląd procesu zarządzania ryzykiem w celu określenia wszelkich możliwych usprawnień.

Ustrukturyzowane podejście

„Wdrożenie tej Normy Międzynarodowej nie tylko pomoże organizacjom zapewnić, że systemy AI działają bezpiecznie i przejrzyście, lecz także pomoże im uniknąć potencjalnych zagrożeń i negatywnych konsekwencji", mówi David Filip, przewodniczący grupy roboczej, która opracowała ISO/IEC 23894. „Może pomóc organizacjom zapewnić, że ich wykorzystanie technologii AI jest bezpieczne, etyczne i zgodne z ich celami i wartościami".

fot. © Tongpatong / Adobe Stock

ISO/IEC 23894 zapewnia ustrukturyzowane podejście do zarządzania ryzykiem, które może pomóc organizacjom w identyfikacji ryzyka, jego ocenie i przeciwdziałaniu mu w sposób proaktywny i skuteczny. Oferuje ramy i zasady zapewniające, że systemy AI działają bezpiecznie i przejrzyście, unikając jednocześnie potencjalnych zagrożeń i negatywnych konsekwencji.

„ISO/IEC 23894 opracowano z myślą o wciąż ewoluującej technologii", mówi Peter Deussen, lider projektu ISO/IEC 23894. „Podkreśla znaczenie ciągłego przeglądu, identyfikacji i przygotowania na potencjalne zagrożenia".

ISO/IEC JTC 1/SC 42

Deussen zaprezentował ISO/IEC 23894 na drugim copółrocznym Warsztacie ISO/IEC AI Workshop. Tematy podjęte na spotkaniu obejmowały zastosowania AI, pożyteczne AI, nowatorskie podejścia w normalizacji AI oraz wschodzące trendy technologiczne i wymogi AI.

SC 42 opracowuje Normy Międzynarodowe z zakresu sztucznej inteligencji. Jego unikalne holistyczne podejście rozpatruje cały ekosystem AI, przez analizę możliwości technologicznych i wymogów nietechnicznych, takich jak wymogi biznesowe, regulacyjne i polityczne, potrzeby w dziedzinie zastosowania oraz kwestie etyczne i społeczne.

SC 42 obecnie współpracuje z IEC/TC 65 nad nową funkcjonalną normą bezpieczeństwa dla AI. Jej celem jest zapewnienie, że systemy, środowisko i urządzenia zależne od technologii AI działają bezpiecznie, nawet w przypadku braków i błędów.

IEC/TC 65 jest odpowiedzialny za serię norm IEC 61508 obejmujących projektowanie i wdrażanie zabezpieczeń zapobiegających wypadkom i zmniejszających zagrożenie dla ludzi, własności i środowiska. PKN/KT 50 ds. Automatyki i Robotyki Przemysłowej jest komitetem wiodącym w zakresie współpracy z IEC/TC 65.

Tłum. I. P.
IEC e-tech, Issue 01/2023