wiadomości PKN
NORMALIZACJA
5/2022

DZIEŃ NORMALIZACJI POLSKIEJ

5/2022

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

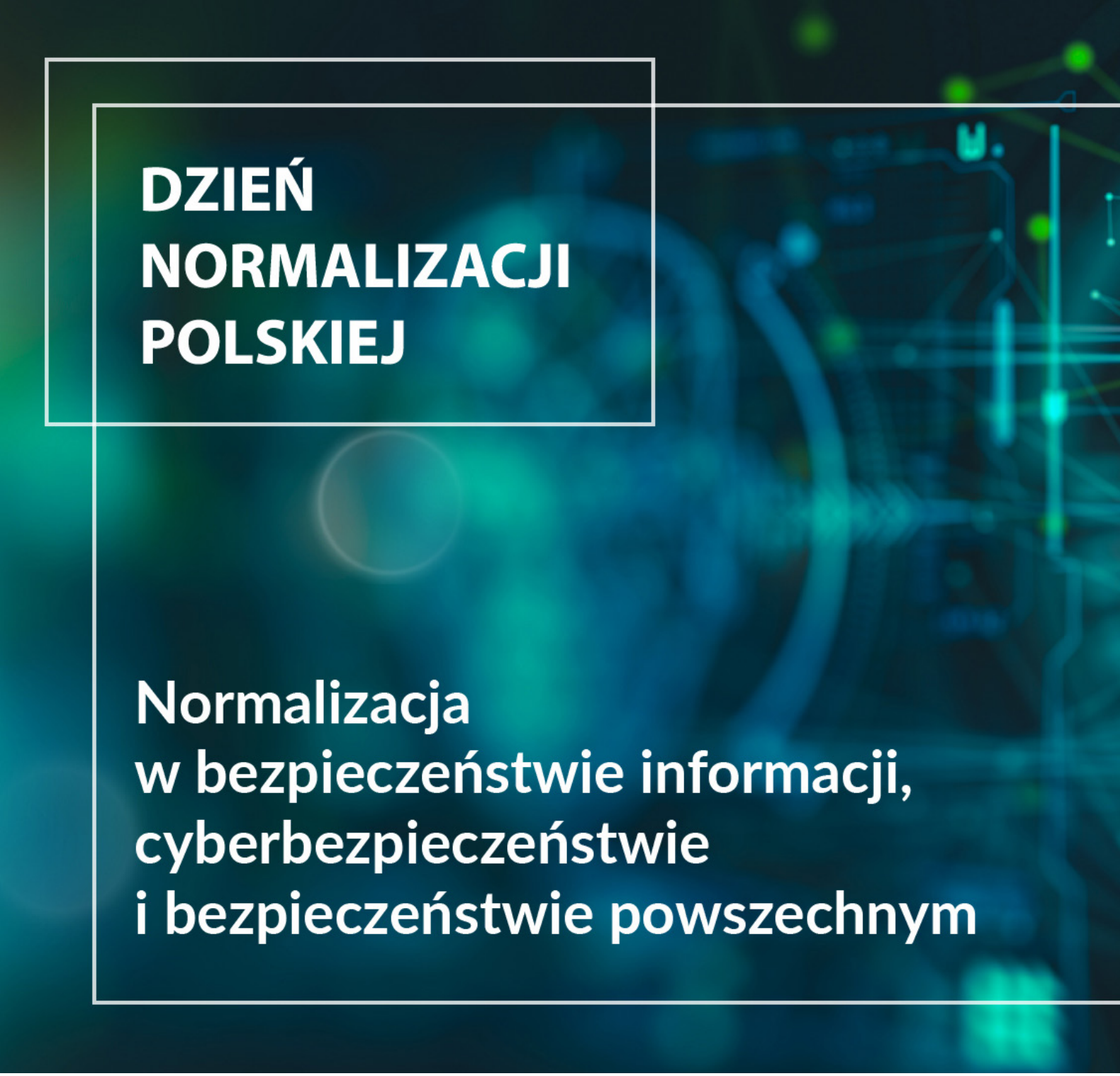
ZESPÓŁ REDAKCYJNY
Redaktor prowadzący:
Joanna Skalska – tel. 22 556 74 62
Redaktorzy:
Marta Hejduk – tel. 22 556 77 09
Aleksandra Kurzep – tel. 22 556 75 07
Skład:
Oskar Sztajer – tel. 22 556 77 62
Piotr Jotel - tel. 22 556 75 98

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

Z okazji Dnia Normalizacji Polskiej
wszystkim osobom
zaangażowanym w rozwój normalizacji
życzymy wielu sukcesów,
inspiracji i motywacji
do wyznaczania jej nowych kierunków.

Polski Komitet Normalizacyjny



DZIEŃ NORMALIZACJI POLSKIEJ

Normalizacja w bezpieczeństwie informacji, cyberbezpieczeństwie i bezpieczeństwie powszechnym

Zależność od cyfrowych narzędzi stawia wiele firm przed zagrożeniem ze strony cyberprzestępców. Solidna wiedza jest kluczowa, ponieważ ataki cybernetyczne stają się coraz bardziej zaawansowane. Bezpieczeństwo, zarówno cybernetyczne, jak i ogólne, obejmuje wszystkie obszary, operacje i działy każdej firmy lub organizacji. Ale tak naprawdę wszystko zaczyna się od wejścia do budynku. Z okazji Dnia Normalizacji Polskiej 19 maja 2022 r. zorganizowaliśmy webinar „Normalizacja w bezpieczeństwie informacji, cyberbezpieczeństwie i bezpieczeństwie powszechnym”, aby dowiedzieć się więcej.

Nie przytrzymuj drzwi intruzowi!

Ochrona informacji firmowych przed naruszeniami danych i włamaniami jest coraz bardziej złożoną kwestią, często wymagającą wielu systemów, narzędzi i ludzi. I jak się sami przekonaliśmy – norm.

Znaczenie normalizacji w bezpieczeństwie informacji i bezpieczeństwie powszechnym omówiła Teresa Sosnowska, Zastępca Prezesa PKN. W swojej prezentacji przywołała wyzwania w zakresie bezpieczeństwa, tj. zagrożenia i zapobieganie im dzięki systemowi normalizacji europejskiej i międzynarodowej. Wskazała na budowanie zintegrowanych rozwiązań w zakresie bezpieczeństwa w Europie przez tworzenie jednolitego rynku produktów i usług bezpieczeństwa, powszechne zaangażowanie w normalizację wśród zainteresowanych stron, realizację prac normalizacyjnych w sposób jak najbardziej zrównoważony, pozwalający na wzajemne wzmacnianie i uwzględnianie wspólnych celów wszystkich zainteresowanych.

Ludzie są najczęstszą przyczyną naruszeń bezpieczeństwa, niezależnie od tego, czy klikają w link w wiadomości phishingowej, czy przytrzymują otwarte drzwi obcej osobie, wchodzącej za nimi do biurowca.

Normy z zakresu bezpieczeństwa informacji i bezpieczeństwa powszechnego

Joanna Skwarek, Pełnomocnik Zintegrowanego Systemu Zarządzania PKN, omówiła m.in. zmiany, jakie wprowadzono do norm dotyczących bezpieczeństwa informacji, a także prace w zakresie bezpieczeństwa powszechnego na poziomie międzynarodowym i europejskim. W swojej prezentacji podkreśliła, że gwarancją bezpieczeństwa jest wiedza, zrozumienie i budowanie świadomości. Normy dotyczące zarządzania bezpieczeństwem informacji (seria norm ISO 27000) uważa się obecnie za najważniejsze dla tej dziedziny. Ich wykorzystanie pozwala nam budować skuteczny system bezpieczeństwa i zabezpieczeń. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji daje nam świetne narzędzie do skutecznego i efektywnego zarządzania tym obszarem w organizacji. Wdrożenie wymagań normy w sposób świadomy i ze zrozumieniem uczy nas, jak skutecznie budować bezpieczeństwo w organizacji.

Prelegentka przybliżyła także współpracę międzynarodowych, europejskich i regionalnych komitetów technicznych w dziedzinie bezpieczeństwa. Międzynarodowy komitet ISO/TC 292 *Security and resilience*, łączący wszystkie do tej pory mocno

fot. © greenbutterfly / Adobe Stock


fot. Jacob1123 / Adobe Stock

rozproszone obszary bezpieczeństwa, odpowiada za normalizację obejmującą wytyczne i wymagania w zakresie bezpieczeństwa, systemów zarządzania w dziedzinie bezpieczeństwa oraz m.in. (ale nie wyłącznie): terminologię, zarządzanie ciągłością działania, zarządzanie kryzysowe, bezpieczeństwo łańcucha dostaw, infrastrukturę krytyczną, przeciwdziałanie oszustwom, usługi bezpieczeństwa. Na poziomie krajowym funkcjonują PKN/KT 306 ds. Bezpieczeństwa Powszechnego i Ochrony Ludności oraz PKN/KT 323 ds. Usług w Ochronie Osób i Mienia.

Systemy zarządzania a cyberbezpieczeństwo

Tadeusz Zawistowski, Konsultant w zakresie systemów zarządzania, mówił o tym, kto może lub powinien korzystać z norm dotyczących systemów zarządzania, a także jak te normy wspierają cyberbezpieczeństwo. System Zarządzania Bezpieczeństwem Informacji zgodny z Normą Międzynarodową jest rozwiązaniem systemowym jako odpowiedź na zagrożenia cybernetyczne.

Normy osadzają cyberbezpieczeństwo w środowisku systemowym i układają w logiczną i kompletną całość, a także w kontekście, w tym w relacji ze stronami zainteresowanymi, zapewniają zaangażowanie najwyższego kierownictwa (m.in. spójność polityki ze strategią i celami biznesowymi, cele, zasoby), dostarczają narzędzi (m.in. monitorowanie, audyty, zarządzanie ryzykiem, działania doskonalące), nie pozwalają pominąć aspektów „nietechnicznych" (np. świadomość, kompetencje, środowisko fizyczne).

Niezależność cyfrowa

Temu zagadnieniu swoje wystąpienie poświecił Tomasz Mazur – Kierownik Sektora Technik Informacyjnych i Komunikacji PKN.

W lipcu zeszłego roku CEN i CENELEC powołały Komitet Warsztatowy – CEN/CLC/WS DS *Digital Sovereignty* – przed którym stoją dosyć poważne wyzwania. Cele tego Komitetu Warsztatowego to m.in.: wypracowanie wspólnego, jednoznacznego rozumienia i struktury pojęcia „autonomii cyfrowej", stwierdzenie jakie normy powinny być opracowane, aby dążyć do osiągnięcia niezależności cyfrowej, ustalenie wymaganych współzależności między normalizacją a legislacją, wskazanie, jak europejska autonomia cyfrowa może być zrozumiana w szerszym międzynarodowym kontekście, ponieważ normalizacja jest narzędziem do znoszenia barier technicznych i handlowych. PKN/KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych

jest komitetem wiodącym we współpracy z CEN/CLC/WS DS *Digital Sovereignty*.

Wkład w osiągnięcie autonomii cyfrowej będzie możliwy, jeśli będziemy dysponować odpowiednio wykształconymi kadrami. Kompetencje cyfrowe stają się coraz większym wyzwaniem zarówno dla pracowników, jak i pracodawców. Technologie to część codziennego życia zawodowego większości pracowników. Wielu z nas korzysta w pracy z urządzeń, specjalistycznego oprogramowania, mediów społecznościowych czy rozwiązań chmurowych. Ich wykorzystywanie wymaga odpowiednich kompetencji cyfrowych.

E-kompetencje są podstawowym elementem strategii Unii Europejskiej na rzecz e-umiejętności w XXI wieku.

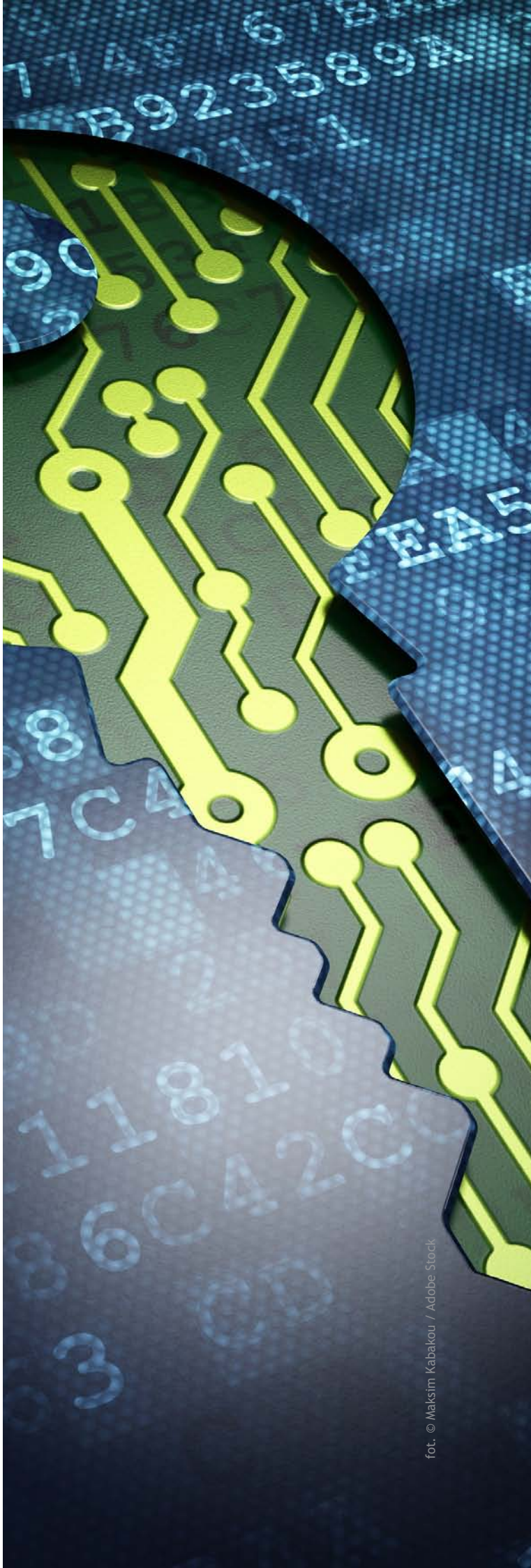
Dlaczego aktywne uczestnictwo w normalizacji na poziomie międzynarodowym jest ważne?

Ewa Zielińska – p.o. Prezes PKN – przedstawiła m.in. cele normalizacji. Jednym z nich jest działanie na rzecz uwzględnienia interesów krajowych w normalizacji europejskiej i międzynarodowej. Dzięki czynnemu udziałowi w normalizacji przedsiębiorca: może wpływać na ustalenie postanowień norm zgodnie z własnymi uwarunkowaniami, otrzymuje informacje o przewidywanych zmianach z odpowiednim wyprzedzeniem, uzyskuje potencjał do kreowania innowacji. Uczestnictwo w normalizacji przekłada się na ułatwiony dostęp do rynku światowego, legalny dostęp do nowoczesnych rozwiązań, zgodnych z aktualnym poziomem światowym.

Każdy z nas może zaangażować się w opracowywanie norm na różne sposoby w zależności od własnych potrzeb i możliwości. Dzięki czynnemu udziałowi w normalizacji można m.in. wpływać na ustalenie postanowień norm zgodnie z własnymi uwarunkowaniami oraz uzyskać informacje o nadchodzących zmianach na rynku w określonej branży.

Ochrona w świecie wirtualnym nie jest prosta. Cyberprzestępcy mogą wejść w posiadanie Twoich danych na wiele sposobów. Mogą nawet przekonać Cię do przesłania ich dobrowolnie, jeśli nie zdajesz sobie sprawy, że właśnie padasz ofiarą oszustwa. Jeśli chcesz pogłębić swoje kompetencje, być świadomym i być na bieżąco, to zapraszamy na szkolenia PKN: https://wiedza.pkn.pl/web/szkolenia/start.

Redakcja



fot. © Maksim Kabakou / Adobe Stock

Przeciwdziałanie atakom cybernetycznym

Ataki cybernetyczne są kosztowne, uciążliwe i stanowią coraz większe zagrożenie dla działalności gospodarczej, rządów oraz społeczeństwa. Na szczęście dzięki normom można stawić im czoła.

Ann Brady

Cyberprzestępczość rośnie. W erze cyfrowej, tzw. czwartej rewolucji przemysłowej, przestępczość ta staje się coraz bardziej wyrafinowana i groźna, co pociąga za sobą poważne konsekwencje. W miarę jak cyberprzestępcy stają się coraz bardziej skuteczni, cyberprzestępczość, w taki czy inny sposób, dotyka każdego z nas.

Cyberataki mogą dotyczyć włamania do systemów i mediów społecznościowych, ataków phishingowych, złośliwego oprogramowania, w tym *ransomware*, kradzieży tożsamości, socjotechniki oraz ataków typu „odmowa usługi". Jest to dotkliwe zarówno pod względem osobistym, jak i finansowym – powoduje niewyobrażalne szkody i zniszczenia, a także naraża społeczeństwo i obywateli na niebezpieczeństwo. Według McAfee, firmy produkującej oprogramowanie zabezpieczające komputery, koszty tych cyberataków rosną – w 2020 r. wyniosły już 1 bilion dolarów.

Rosnące światowe zagrożenie

W związku z pandemią COVID-19, która jeszcze bardziej ugruntowała naszą zależność od systemów cyfrowych, nie dziwi fakt, że zagrożenia dla cyberbezpieczeństwa zostały po raz kolejny wymienione w Global Risks Report 2022 jako rosnące zagrożenia dla świata. W raporcie stwierdzono, że błędy w zakresie cyberbezpieczeństwa znacznie się pogłębiły i zagrażają długoterminowemu dobrobytowi.

Ale jak być krok do przodu? Budowa dobrego systemu cyberobrony oraz przewidywanie zagrożeń to bardzo istotne elementy walki z cyberprzestępczością, jednak ani odporność, ani zarządzanie nie są możliwe bez wiarygodnych i zaawansowanych planów zarządzania ryzykiem cybernetycznym. „Cyberprzestępczość jest zjawiskiem zarówno krajowym, jak i międzynarodowym rozprzestrzeniającym się z ogromną prędkością, wpływającym na przedsiębiorstwa, rządy i całe społeczeństwo. Skala i złożoność tej działalności przestępczej ma dalekosiężne i szkodliwe konsekwencje, a sytuacja jest niejasna, ponieważ cyberprzestępcy działają, wykorzystując infrastrukturę techniczną ponad granicami państw" – twierdzi ekspert ds. cyberbezpieczeństwa dr Edward Humphreys.

W związku z tym – dodaje – współpraca międzynarodowa jest konieczna, a Normy Międzynarodowe niezbędne do zapewnienia globalnej ochrony. Dr Humphreys wypowiada się na podstawie swojego wieloletniego doświadczenia biznesowego. Jest on również starszym pracownikiem naukowym specjalizującym się w badaniach nad ryzykiem cybernetycznym, bezpieczeństwem i cyberpsychologią oraz innowacyjnością systemów zarządzania bezpieczeństwem informacji (SZBI), a także przewodniczącym grupy roboczej ISO/IEC odpowiedzialnej za zarządzanie, utrzymanie i rozwój ISO/IEC 27000, grupy norm obejmujących systemy zarządzania bezpieczeństwem informacji.

Rozwiązania i sterowanie

Normy Międzynarodowe dostarczają rozwiązań, umożliwiając organizacjom ustanowienie ram i systemów oceny sytuacji i zarządzania nią – w celu ochrony informacji, zabezpieczenia aplikacji i usług oraz infrastruktury krajowej.

Pierwszym krokiem w walce z cyberprzestępczością jest poznanie zagrożeń, na jakie narażona jest dana organizacja oraz określenie środków kontroli, które należy wdrożyć w celu ograniczenia tych zagrożeń. Humphreys wskazuje na normy z serii ISO/IEC 27000 jako właściwy wybór dla każdej organizacji pragnącej wprowadzić solidne rozwiązania w walce z cyberprzestępczością. Pakiet Norm Międzynarodowych określa system zarządzania, który obejmuje proces zarządzania ryzykiem polegający na ocenie zagrożeń, a następnie na określeniu środków kontroli niezbędnych do ich eliminacji.

„Istnieje wiele norm wspierających ISO/IEC 27001, jak np. ISO/IEC 27005 dot. zarządzania ryzykiem w zakresie bezpieczeństwa informacji oraz wytycznych wdrażania ISO/IEC 27003", mówi. „Funkcjonuje też wiele innych norm zapewniających wsparcie techniczne dla normy ISO/IEC 27001, np. w zakresie zabezpieczania sieci i wbudowywania zabezpieczeń w technologie, usługi i aplikacje".

Być przygotowanym

Dr Humphreys powtarza, że firmy muszą być przygotowane i gotowe do stawienia czoła takim atakom. „Ataki cybernetyczne mogą mieć miejsce zawsze i wszędzie. To, że takie ataki nastąpią, jest pewne, nie możemy być jednak pewni kiedy i gdzie", mówi. „Bycie gotowym i przygotowanym jest podstawowym działaniem biznesowym umożliwiającym przetrwanie. Wiąże się to z wprowadzeniem przez firmę procesu umożliwiającego przewidywanie i identyfikowanie, wykrywanie i zgłaszanie incydentów, a także analizowanie tych incydentów w celu podjęcia decyzji o sposobie reagowania na

nie". Wszystko to należy robić szybko i terminowo, by ograniczyć skutki zaistniałego incydentu.

Jak przedsiębiorstwa mogą być lepiej przygotowane? Im szybciej firma wykryje atak z wykorzystaniem złośliwego kodu lub atak typu „odmowa usługi", tym większa szansa na ograniczenie rozprzestrzeniania się takich ataków, a także na ograniczenie ich skutków i szkód. Jak mówi dr Humphreys, istnieją normy, które pomagają przedsiębiorstwom w osiągnięciu gotowości i lepszego przygotowania do reagowania na incydenty, jak choćby norma ISO/IEC 27035 obejmująca zarzadzanie incydentami, norma ISO 22301 z zakresu zarządzania ciągłością działania oraz norma gotowości ICT – ISO/IEC 27031.

Wspólne działania

W już i tak niepewnym świecie cyberprzestępczość może przynosić straty finansowe, zakłócać działalność przedsiębiorstw i infrastrukturę krajową, a także wpływać na obywateli i społeczeństwo. Na przykład atak na jedną część łańcucha dostaw może się rozprzestrzenić, zakłócić i uszkodzić inne jego części. Dr Humphreys twierdzi, że aby zwiększyć bezpieczeństwo i odporność systemów bezpieczeństwa cybernetycznego, zarządzanie łańcuchem dostaw jest dobrym przykładem sytuacji, w której niezbędne jest wspólne działanie wszystkich uczestników łańcucha w celu zapewnienia jego bezpieczeństwa.

„Istnieją normy, które pomagają w zapewnieniu bezpieczeństwa łańcucha dostaw, np. ISO 28000 oraz ISO/IEC 27036. Wspólne działania są również potrzebne w różnych scenariuszach obejmujących relacje biznesowe i komunikację z innymi organizacjami. Istnieje grupa norm zarządzania, która pomoże w budowaniu odporności na zakłócenia w działalności biznesowej, zapewnieniu przetrwania oraz system administrowania. Należą do nich normy ISO 22301 (systemy zarządzania ciągłością działania), ISO/IEC 27001 (systemy zarzadzania bezpieczeństwem informacji) oraz ISO/IEC 27014 (zarządzanie bezpieczeństwem informacji)".

Wraz z rozwojem i uzależnieniem od łączności w biznesie, infrastrukturą ją obsługującą oraz korzystaniem z Internetu i urządzeń mobilnych wzrasta potrzeba zapewnienia bezpieczeństwa i odporności systemu. Dr Humphreys przyznaje, że normy muszą ewoluować, aby dostosować się do szybkiego postępu technologicznego. „W pierwszym kwartale 2022 roku opublikowano np. trzecie wydanie normy ISO/IEC 27002.

fot. © Song_about_summer / Adobe Stock

Ta głośna norma dotyczy kontroli bezpieczeństwa informacji i została zaktualizowana w celu dostosowania jej do postępu technologicznego, rozwoju praktyk biznesowych oraz nowych przepisów i regulacji".

Dodaje, że w 2021 nastąpiło wiele innych zmian w normalizacji, w tym w zakresie bezpieczeństwa Internetu Rzeczy (IoT), bezpieczeństwa i poufności dużych danych, bezpieczeństwa i poufności sztucznej inteligencji oraz ochrony informacji biometrycznej. Wszystkie te zagadnienia są uzupełniane przez najnowsze specyfikacje techniczne takie jak ISO/IEC TS 27570, zawierającą wytyczne dotyczące ochrony prywatności ekosystemu inteligentnego miasta oraz ISO/IEC TS 27100, która określa, jak tworzyć lub udoskonalać systemy cybernetyczne w celu ochrony przed cyberatakami. Cała grupa norm ISO/IEC 27000 i te specyfikacje skupione na technologii stanowią podstawę do budowy i zarządzania bezpieczną przyszłością.

Tłum. I. P.
www.iso.org

fot. © Blue Planet Studio / Adobe Stock

Certyfikacja – warunek konieczny dla ISO/IEC 27001

Claire Marchand

Cyberataki mnożą się na całym świecie. Ich celem są nie tylko zakłady przemysłowe, lecz także władze na szczeblu lokalnym, regionalnym i krajowym, organizacje pozarządowe, a także operatorzy usług takich jak opieka zdrowotna, turystyka, bankowość, transport, handel i wiele innych.

Według Check Point, izraelskiej firmy zajmującej się cyberbezpieczeństwem, rok 2021 był rekordowy pod względem liczby cyberataków, przy wzroście liczby ataków o 50% tygodniowo w porównaniu do roku 2020. W 2021 największej liczby cyberataków doświadczył sektor edukacyjny/badawczy (wzrost o 75% w stosunku do roku 2020), a w dalszej kolejności: sektor rządowy/wojskowy (+47%), komunikacyjny (+51%), opieki zdrowotnej (+71%), usług komunalnych (+46%) oraz produkcji (+41%).

Luki w zabezpieczeniach są liczne

Dlaczego firmy i organizacje są tak narażone na ataki? Istnieją oczywiste powody jak otwieranie wiadomości e-mail od nieznanych nadawców, posiadanie słabych danych uwierzytelniających, pozostawianie haseł na karteczkach samoprzylepnych, posiadanie dostępu do wszystkiego, niewystarczające przeszkolenie

pracowników lub jego brak, nieaktualizowanie programu antywirusowego lub korzystanie z niezabezpieczonych urządzeń mobilnych. Według Computer Weekly 84% ofiar wskazuje, przynajmniej częściowo, błąd ludzki jako przyczynę cyberataku.

Jednak w kwestii bezpieczeństwa, komputery i osoby prywatne nie są jedynymi winowajcami. Bezpieczeństwo zarówno cybernetyczne, jak i ogólne obejmuje wszystkie obszary, działania i oddziały każdej firmy lub organizacji. Tak naprawdę zaczyna się ono od momentu wejścia do budynku.

Bezpieczeństwo zaczyna się u drzwi

Istnieje wiele pytań, które każdy zespół zarządzający powinien sobie zadać i odpowiedzieć na nie, aby zapewnić jak najwyższy poziom bezpieczeństwa:

- W jaki sposób uzyskuje się dostęp do pomieszczeń? Czy używa się kluczy, identyfikatorów, haseł, kodów czy danych biometrycznych?
- Kto ma dostęp do pomieszczeń? Czy istnieją obszary o ograniczonym dostępie, do których może wejść tylko upoważniony personel?
- Na jakich warunkach do budynku mogą wejść firmy zewnętrzne np. sprzątające, serwisowe itp.? W jaki sposób przeprowadza się weryfikację osób odwiedzających? Czy przed budynkiem znajdują się kamery? Czy istnieje zasada zamykania akt na noc, aby pracownicy ochrony i osoby sprzątające nie mogli zobaczyć poufnych informacji na biurkach?
- Jaka jest procedura zgłoszenia zagubionych lub skradzionych dokumentów firmowych, komputerów, telefonów, kart kredytowych? Co się dzieje z informacjami przechowywanymi na urządzeniu? W jaki sposób informacje są zabezpieczane? Podobnie, jak zabezpieczone są informacje o klientach?
- W jaki sposób utylizuje się stare dokumenty – papierowe i elektroniczne?
- Co się dzieje z dyskami twardymi komputerów, które są wyrzucane i wymieniane?

I można tak dalej. To lista podstawowych pytań niewyczerpujących tematu, a które każda firma powinna sobie zadać.

SZBI jest odpowiedzią

Odpowiedzią na te wszystkie pytania jest wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), który będzie chronił zasoby firmy. SZBI może zapobiec uszkodzeniu lub zniszczeniu poufnych danych i zapewni, że nie dostaną się one w niepowołane ręce.

fot. © Maksim Kabakou / Adobe Stock

SZBI to zestaw polityk, procedur i mechanizmów kontrolnych, które chronią integralność, bezpieczeństwo i dostępność poufnych danych firmy. Obejmuje on procesy, dane i technologie, a także zachowania pracowników. Jeśli jest egzekwowany w sposób kompleksowy, staje się on częścią kultury organizacyjnej firmy.

Tylko skuteczne wdrożenie SZBI, czyli włączenie zarządzania informacją do kultury firmy i przeszkolenie personelu w zakresie jego przestrzegania, zapewni wysoki stopień zabezpieczenia przed naruszeniami bezpieczeństwa danych.

Zwiększenie bezpieczeństwa informacji dzięki ISO/IEC 27001

Wspólny Komitet Techniczny ds. informacji ISO/IEC JTC 1, poprzez jeden ze swoich podkomitetów, SC 27, opublikował normę ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*.

Ta Norma Międzynarodowa określa wymagania dotyczące ustanawiania, wdrażania, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w kontekście organizacji, jak również oceny i postępowania z ryzykiem związanym z bezpieczeństwem informacji dostosowanego do potrzeb organizacji/firmy. Wymagania te mają charakter ogólny i powinny być stosowane we wszystkich organizacjach, bez względu na ich typ, wielkość czy charakter. Zawiera zalecenia dotyczące przywództwa, zaangażowania i polityki, a także działań mających na celu reakcję na ryzyko zagrożenia i inne perspektywy. Norma obejmuje także kwestie pomocnicze, takie jak zasoby, kompetencje, świadomość, komunikację, planowanie i kontrolę operacyjną, ocenę ryzyka związanego z bezpieczeństwem informacji oraz kwestie dotyczące postępowania i wydajności.

Norma ISO/IEC 27001 wykracza poza cyberbezpieczeństwo i obejmuje sposób, w jaki firma zarządza bezpieczeństwem posiadanych informacji, pochodzących zarówno z działalności własnej, jak i ze źródeł zewnętrznych takich jak dostawcy, klienci itd. Norma ISO/IEC 27001 obejmuje również zagrożenia wynikające z celowych cyberataków.

Stosowanie holistycznego podejścia normy ISO/IEC 27001 przynosi wiele korzyści: zgodność z przepisa-

mi krajowymi i/albo regionalnymi; odporność i lepsze reagowanie na zagrożenia cybernetyczne; redukcję kosztów dzięki centralnie zarządzanemu systemowi, który pozwala na pozbycie się wielu nieefektywnych procedur; dobrze poinformowanych pracowników świadomych swoich obowiązków w zakresie bezpieczeństwa.

Certyfikacja IECQ dla ISO/IEC 27001

Uzyskując certyfikat ISO/IEC 27001, firma udowadnia swoim interesariuszom i klientom, że jest zaangażowana w bezpieczne zarządzanie informacjami. Mówiąc krótko: tej firmie można zaufać.

Certyfikacja na zgodność z ISO/IEC 27001 istnieje od czasu opublikowania normy w 2013 roku, jednak dopiero w ostatnich latach IECQ (IEC *Quality Assessment System for Electronic Components*) ustanowiło prawdziwie jednolity ustandaryzowany sposób oceny i certyfikacji SZBI z ISO/IEC 27001.

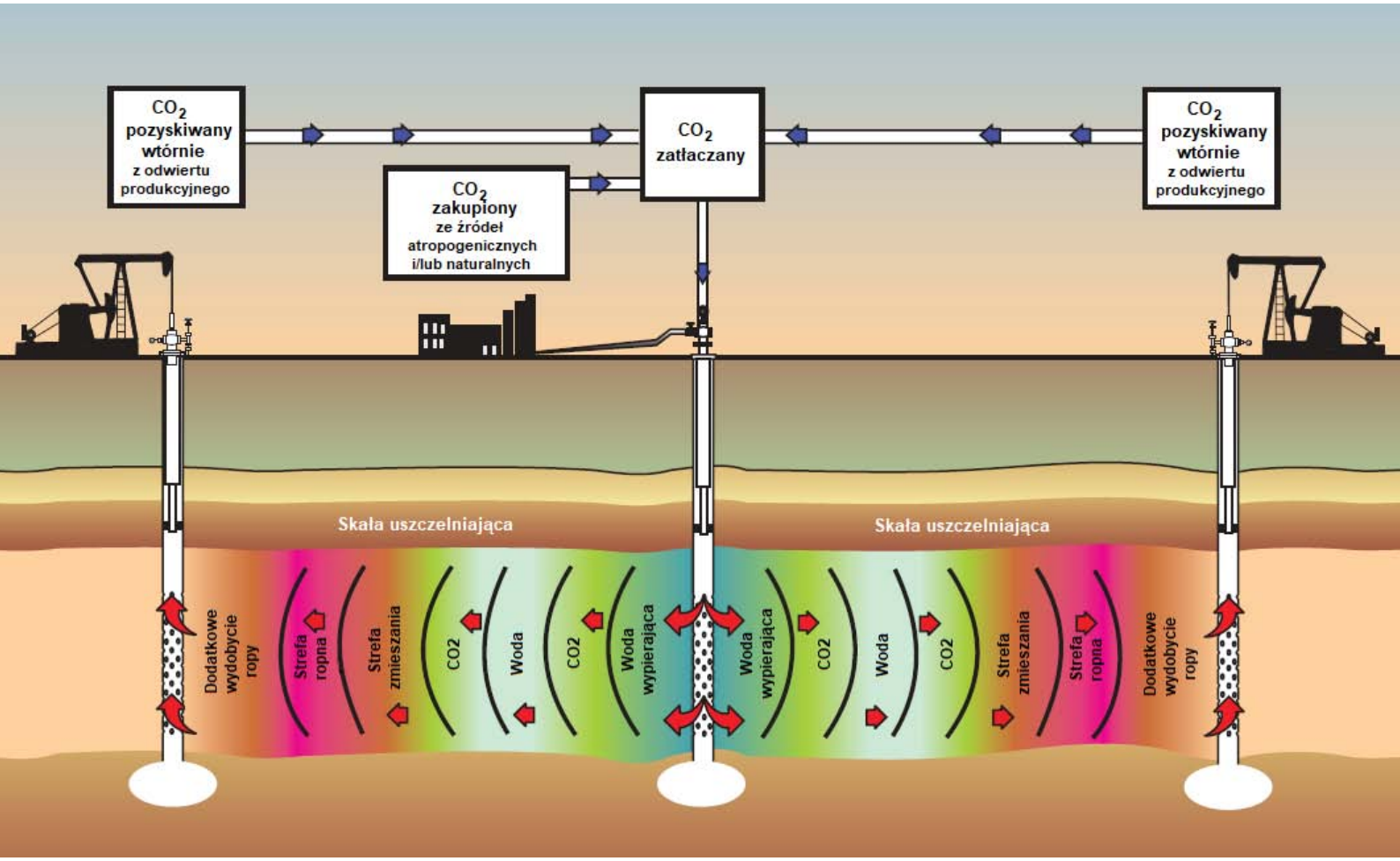
Stale rosnąca potrzeba dostarczenia przez firmy niezależnego dowodu zgodności z normą ISO/IEC 27001 dla ich SZBI doprowadziła do tego, że branża zwróciła się do jednostek certyfikujących IECQ z prośbą o możliwość przeprowadzenia oceny i certyfikacji na zgodność z ISO/IEC 27001 w ramach zatwierdzonego schematu procesu (approved process scheme – AP scheme) podczas przeprowadzania innych ocen IECQ, np. w zakresie awioniki lub zarządzania procesami związanymi z substancjami niebezpiecznymi.

To co w ostatnim czasie skłoniło przemysł do zwrócenia się do IECQ, to brak harmonizacji pomiędzy wieloma jednostkami certyfikacyjnymi oferującymi własne certyfikaty i stosującymi własne interpretacje normy ISO/IEC 27001. Z czasem doprowadziło to do powstania różnych podejść i różnic w tym, co jest akceptowane przez różne jednostki certyfikujące. W związku z tym przemysł uznał, że IECQ jest w stanie zaoferować jednolite podejście do stosowania normy ISO/IEC 27001. Wszystkie certyfikaty można znaleźć na stronie internetowej IECQ.

Tłum. I. P.
IEC e-the, Issue 01/2022

WYCHWYTYWANIE, TRANSPORT I GEOLOGICZNE SKŁADOWANIE DWUTLENKU WĘGLA

W 2022 roku do programu prac KT 31 ds. Górnictwa Nafty i Gazu po raz pierwszy wprowadzono normy dotyczące wychwytywania, transportu i geologicznego składowania dwutlenku węgla. Pierwszą z wprowadzanych norm jest ISO 27917:2017 Wychwytywanie, transport i geologiczne składowanie dwutlenku węgla – Terminologia – Terminy przekrojowe.



Schemat CO_2-EOR z wykorzystaniem metody naprzemiennego zatłaczania wody i gazu (źródło: ISO 27916)

Celem wprowadzenia tego dokumentu do zbioru Polskich Norm jest dostarczenie wyczerpującego wykazu terminów w języku polskim i ich definicji dotyczących wychwytywania, transportu i geologicznego składowania dwutlenku węgla, w tym operacji składowania powiązanego ze wspomaganiem wydobycia ropy naftowej (EOR), w celu ułatwienia komunikacji między ekspertami zaangażowanymi w rozwój tych technologii oraz innymi interesariuszami.

Terminy sklasyfikowano według pięciu obszarów związanych z:

- wychwytywaniem, transportem i składowaniem dwutlenku węgla – 9 terminów;
- dwutlenkiem węgla – 14 terminów;
- monitoringiem i efektywnością pomiarów w zakresie wychwytywania, transportu i geologicznego składowania dwutlenku węgla – 11 terminów;
- ryzykiem – 15 terminów;
- relacjami z interesariuszami – 6 terminów.

Drugą z wprowadzanych norm jest ISO 27916:2019 Wychwytywanie, transport i geologiczne składowanie dwutlenku węgla – Składowanie dwutlenku węgla z wykorzystaniem wspomagania wydobycia ropy naftowej (CO_2-EOR).

Wspomaganie wydobycia ropy z wykorzystaniem dwutlenku węgla (CO_2-EOR) to metoda pozwalająca na zwiększanie sczerpania węglowodorów z pola naftowego.

Proces ten polega na wykorzystaniu odwiertów do zatłaczania CO_2 przy ciśnieniach, w których zatłoczony CO_2 zwykle miesza się z ropą, zmieniając właściwości ropy i umożliwiając jej swobodniejszy przepływ do odwiertów wydobywczych. W większości przypadków projekt CO_2-EOR jest zaprojektowany jako system o obiegu zamkniętym, w którym część zatłoczonego CO_2 jest wydobywana razem z ropą, a następnie jest oddzielana w napowierzchniowych instalacjach przed powrotnym zatłoczeniem do złoża ropy. CO_2 zatłaczany do złoża objętego projektem jest uwięziony jako nieodłączny element zatłaczania i wydobycia. CO_2, który jest zatłaczany i pułapkowany w złożu objętym projektem (lub w kompleksie EOR) w trakcie i po zakończeniu działań związanych z wydobyciem ropy, nie jest uwalniany do atmosfery, a takie pułapkowanie określa się mianem składowania powiązanego. W Załączniku A do tej normy zawarto szczegółowy opis obecnie stosowanego procesu CO_2-EOR oraz składowania powiązanego, który jest nieodłączną częścią tych operacji. Dodatkową kwestią jest metan i mimo że jest on często obecny w złożach objętych projektem EOR, to norma ta nie odnosi się konkretnie do metanu ani gazów cieplarnianych. Wymagania demonstracyjne dotyczące bezpiecznego i długotrwałego uwięzienia dotyczą jednak oceny możliwości pułapkowania i potencjalnych dróg wycieku, które prawdopodobnie zapewniłyby uwięzienie dla metanu jak i CO_2. CO_2-EOR jest stosowany na świecie od kilku dziesięcioleci i ma potencjał do rozwoju. CO_2-EOR ma obecnie znaczenie komercyjne, ponieważ pozwala na dodatkowe sczerpanie zasobów węglowodorów, przy jednoczesnym pułapkowaniu zatłoczonego CO_2, z zachowaniem bezpiecznego i długotrwałego uwięzienia jako części procesu.

Normy PN-ISO 27916 i PN-ISO 27917 będą dokumentami ze wszech miar ważnymi i potrzebnymi dla znacznej części podmiotów, dla których szeroko rozumiana tematyka dwutlenku węgla jest istotna oraz przyczynią się do stosowania rozwiązań zgodnych z najwyższymi światowymi standardami.

Krzysztof Rakowski
Sektor Górnictwa PKN

Czy Ziemia przetrwa inwazję człowieka?

Zygfryd Witkiewicz, Waldemar Wardencki,
Anna Świercz

To recenzowana praca popularno-naukowa przeznaczona dla szerokiego grona odbiorców, którym bliski jest los naszej planety.

Zagadnienia poruszane w książce mają charakter uniwersalny, dotyczą zagrożeń egzystencjalnych dla naszej planety. Zagrożenia te związane są z działalnością człowieka, a ich skutkiem są przede wszystkim groźne zmiany klimatu i utrata bioróżnorodności. Sytuację pogarsza ciągle wzrastająca liczba ludności, która wymaga coraz większych ilości energii, nie chce ograniczać produkcji dóbr konsumpcyjnych, a jednocześnie wprowadza do środowiska coraz więcej zanieczyszczeń, głównie chemicznych. Coraz większym problemem stają się zanieczyszczenia tworzywami sztucznymi i odpadami komunalno-przemysłowymi.

Autorzy książki pokazują, jak w wyniku aktywności *homo sapiens* zachodziły zmiany w ekosystemach wywołane przez działalność przemysłowo-gospodarczą człowieka – gatunku inwazyjnego. W książce przedstawione są najnowsze teorie dotyczące przyczyn i następstw ocieplenia klimatu, konsekwencji niepohamowanego wzrostu liczby ludności, problemów z dostępem do wody i żywności, skali chorób o charakterze pandemii. Autorzy pokusili się także o przedstawienie propozycji odwrócenia niepokojących trendów zmierzających do jeszcze większej dewastacji zasobów środowiska. Przedstawili w sposób skłaniający do refleksji i dyskusji problemy dotyczące polityki państw oraz organizacji pozarządowych w zakresie zmian klimatu.

Choć publikacji o zbliżonej tematyce jest dużo, to mało jest takich, które są pisane w sposób przystępny, językiem czytelnym dla przeciętnego czytelnika. Niniejsza książka może też być wartościową pomocą dydaktyczną dla studentów różnych kierunków studiów, w tym ochrony środowiska, geografii, biologii, chemii. Książka, ze względu na interdyscyplinarność zagadnień, może być pomocna przy omawianiu wielu zagadnień środowiskowych podczas zajęć konwersatoryjnych, laboratoryjnych, a także na zajęciach z etyki i podstaw filozofii. Jej nadrzędnym celem jest popularyzacja wiedzy w sposób ogólnie zrozumiały, ale mający solidne podstawy naukowe.

Zapraszamy do lektury!
Autorzy

„Czy Ziemia przetrwa inwazję człowieka?" – książka wydana przez Bogucki Wydawnictwo Naukowe (Poznań, 2022), której autorami są Zygfryd Witkiewicz (WAT, Warszawa) – wieloletni przewodniczący PKN/KT 280 ds. Jakości Powietrza, Waldemar Wardencki (PG, Gdańsk) i Anna Świercz (UJK, Kielce).

ORGANY TECHNICZNE

fot. © comzeal / Adobe Stock

KWIECIEŃ 2022

Komitety Techniczne

Zmiana zakresu tematycznego Komitetu Technicznego

- KT 55 ds. Instalacji Elektrycznych i Ochrony Odgromowej Obiektów Budowlanych rozszerzył zakres współpracy o CLC/SR LVDC, *Low Voltage Direct Current and Low Voltage Direct Current for Electricity Access* i IEC/PC 128, *Operation of electrical installations*

Nowi Przewodniczący Komitetów Technicznych

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

- w KT 126 ds. Rur Stalowych mgra inż. Dariusza Chromika reprezentującego TÜV SÜD Polska Sp. z o.o.
- w KT 132 ds. Silników Spalinowych dra inż. Andrzeja Sucheckiego reprezentującego Instytut Badań i Rozwoju Motoryzacji BOSMAL Sp. z o.o.
- w KT 141 ds. Tworzyw Sztucznych dr hab. inż. Reginę Jeziórską reprezentującą Sieć Badawczą Łukasiewicz – Instytut Chemii Przemysłowej im. prof. Ignacego Mościckiego
- w KT 230 ds. Małych Statków mgra inż. Adama Dunikowskiego reprezentującego Polski Rejestr Statków SA
- w KT 246 ds. Ochrony Radiologicznej dra Pawła Krajowskiego reprezentującego Centralne Laboratorium Ochrony Radiologicznej
- w KT 285 ds. Górniczych Maszyn i Urządzeń Dołowych dra inż. Edwarda Pieczorę reprezentującego Instytut Techniki Górniczej KOMAG
- w KT 302 ds. Zastosowania Informatyki w Ochronie Zdrowia mgra inż. Edwarda Byczyńskiego reprezentującego Stowarzyszenie e-Polska+

Nowi Zastępcy Przewodniczącego Komitetów Technicznych

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

- w KT 285 ds. Górniczych Maszyn i Urządzeń Dołowych mgr inż. Romanę Zając reprezentującą Instytut Techniki Górniczej KOMAG
- w KT 290 ds. Technik Specjalnych w Elektryce dra inż. Wojciecha Sokólskiego reprezentującego Specjalistyczne Przedsiębiorstwo Zabezpieczeń Przeciwkorozyjnych CORRPOL Sp. z o.o.

Nowi Sekretarze Komitetów Technicznych

W kwietniu Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w KT 14 ds. Maszyn i Urządzeń dla Budownictwa, Przemysłu Materiałów Budowlanych oraz Górnictwa Skalnego mgr inż. Bożennę Mrówkę z Polskiego Komitetu Normalizacyjnego
- w KT 81 ds. Przekładników i Transformatorów Małej Mocy Pana Bartłomieja Sylwestrzuka z Polskiego Komitetu Normalizacyjnego
- w KT 108 ds. Kruszyw i Kamienia Budowlanego mgr Katarzynę Sieńczewską z Polskiego Komitetu Normalizacyjnego

Nowi członkowie Komitetów Technicznych

W kwietniu Prezes PKN powołał na członka KT:

- ARMACELL Poland Sp. z o.o. do KT 179 ds. Ochrony Cieplnej Budynków
- Greenlite Media Sp. z o.o. do KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych
- Instytut Innowacji Przemysłu Mleczarskiego Sp. z o.o. do KT 235 ds. Analizy Żywności
- SAFCON Sp. z o.o. do KT 158 ds. Bezpieczeństwa Maszyn i Urządzeń Technicznych oraz Ergonomii – Zagadnienia Ogólne
- TÜV SÜD Polska Sp. z o.o. do KT 123 ds. Badań Własności Metali, KT 138 ds. Kolejnictwa, KT 165 ds. Spawania i Procesów Pokrewnych i KT 168 ds. Wyrobów z Tworzyw Sztucznych
- i2 Analytical Limited Sp. z o.o. Oddział w Polsce do KT 108 ds. Kruszyw i Kamienia Budowlanego

Odwołani członkowie Komitetów Technicznych

W kwietniu Prezes PKN odwołał z członkostwa w KT następujące podmioty:

- Adama Zalewskiego z KT 304 ds. Aspektów Systemowych Dostawy Energii Elektrycznej
- Armstrong Building Products B.V. Sp. z o.o. Oddział w Polsce z KT 169 ds. Okien, Drzwi, Żaluzji i Okuć
- Biuro Techniczne ALSTA – Stanisław Koślacz z KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych
- Canon Polska Sp. z o.o. z KT 170 ds. Terminologii Informatycznej, Kodowania Informacji i Techniki Biurowej
- Instytut Badawczy Materiałów Budowlanych Sp. z o.o. w likwidacji z KT 108 ds. Kruszyw i Kamienia Budowlanego
- Kopalnie Gipsu i Anhydrytu NOWY LĄD Sp. z o.o. z KT 194 ds. Gipsu i Wyrobów z Gipsu
- Marcin Trylski SAFCON z KT 158 ds. Bezpieczeństwa Maszyn i Urządzeń Technicznych oraz Ergonomii – Zagadnienia Ogólne
- Polimex Mostostal SA z KT 14 ds. Maszyn i Urządzeń dla Budownictwa, Przemysłu Materiałów Budowlanych oraz Górnictwa Skalnego
- Pomorską Izbę Rzemieślniczą Małych i Średnich Przedsiębiorstw z KT 239 ds. Jubilerstwa
- Radę Stołeczną Naczelnej Organizacji Technicznej z KT 14 ds. Maszyn i Urządzeń dla Budownictwa, Przemysłu Materiałów Budowlanych oraz Górnictwa Skalnego
- Stowarzyszenie Włókienników Polskich z KT 20 ds. Skóry i Obuwia

- Uczelnię Techniczno-Handlową im. Heleny Chodkowskiej z KT 304 ds. Aspektów Systemowych Dostawy Energii Elektrycznej
- Uniwersytet w Białymstoku z KT 3 ds. Mikrobiologii Łańcucha Żywnościowego, KT 120 ds. Jakości Wody – Badania Mikrobiologiczne i Biologiczne i KT 235 ds. Analizy Żywności
- Vedag Polska Sp. z o.o. z KT z KT 214 ds. Wyrobów Bitumicznych i Polimerowych do Izolacji Wodochronnych w Budownictwie

Komitety Zadaniowe

Nowy Przewodniczący Komitetu Zadaniowego

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

- w KZ 505 ds. Procesów Kryminalistycznych Pana Artura Dębskiego reprezentującego Centralne Laboratorium Kryminalistyczne Policji

Podkomitety Techniczne

Nowi Przewodniczący Podkomitetów Technicznych

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

- w KT 176/PK 2 ds. Sprzętu Pancernego i Wojskowego Sprzętu Samochodowego oraz w zakresie Ochrony Sprzętu Technicznego przed Korozją i Starzeniem mgra inż. Przemysława Wachowiaka reprezentującego Wojskowy Instytut Techniki Pancernej i Samochodowej
- w KT 222/PK 3 Środków Smarowych mgra Janusza Fudałę reprezentującego ORLEN OIL Sp. z o.o.

SZKOLENIA ON-LINE

Oferta najbliższych szkoleń on-line PKN:

Zarządzanie działaniami korekcyjnymi, korygującymi i doskonalącymi zgodne z normami ISO dotyczącymi systemów zarządzania

Analiza ryzyka zgodnie z RODO - krok po kroku

Audyt zgodności z RODO - praktyczne warsztaty

Zasady przeprowadzania auditów zdalnych pierwszej i drugiej strony zgodnych z normą PN-EN ISO 19011:2018-08

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

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