wiadomości PKN

• NORMALIZACJA •

6/2019

• CYBERRYZYKO

• NORMALIZACJA W SZKOLE

6/2019

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

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

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

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

Szanowni Czytelnicy,

„Global Risks Report 2018" wśród najważniejszych globalnych zagrożeń oprócz katastrof naturalnych, ekologicznych czy zagrożeń środowiskowych wymienia ataki hakerskie na dużą skalę.

Liczba ataków hakerskich podwoiła się w ciągu ostatnich pięciu lat, a ten trend będzie się utrzymywał, choćby ze względu na upowszechnienie Internetu Rzeczy czy chmury. Szacuje się, że tylko 19% przedsiębiorstw jest odpowiednio przygotowanych do zarządzania cyberryzykiem.

Ryzyka nie można uniknąć, ale można nim skutecznie zarządzać przez wdrożenie odpowiednich norm. Dzięki zastosowaniu rodziny norm SZBI, organizacje mogą opracować i wdrożyć ramy zarządzania bezpieczeństwem ich aktywów informacyjnych i ocenić jej technologiczne potrzeby. Natomiast PN-ISO 31000 pozwoli firmie zrozumieć wartość informacji, a co za tym idzie wdrożyć odpowiedni stopień ochrony technologicznej. Takie podejście zrównoważy koncentrację na technologii z czynnikami ludzkimi. Więcej można przeczytać w bieżącym numerze w artykule „Misja dla cyberzaufania" .

Życzę ciekawej lektury.

Joanna Skalska

fot. © oatawa / Adobe Stock

Normalizacja
w programie nauczania

fot. © peampath / Adobe Stock

Propagowanie wśród młodego pokolenia przekonania o roli norm technicznych i normalizacji w życiu codziennym, a także zachęcenie nauczycieli do wprowadzenia tematyki normalizacyjnej do zajęć lekcyjnych to działania związane z polityką edukacyjną Polskiego Komitetu Normalizacyjnego.

Nowe rozporządzenie

16 maja br. podpisano rozporządzenia Ministra Edukacji Narodowej w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego. Zostały wprowadzone m.in. nowe zawody, a także propozycje dodatkowych umiejętności zawodowych, które szkoła może wybrać jako dodatkową ofertę w danym zawodzie – np. uczniowie zawodów poligraficznych mogą przygotowywać się do modelowania 3D.

Cieszy zatem fakt, że starania PKN dotyczące wprowadzenia elementów normalizacji do programów nauczania również zakończyły się pomyślnie. Oznacza to, że efektem kształcenia absolwentów szkół branżowych będzie umiejętność rozpoznawania norm i procedur oceny zgodności podczas realizacji zadań zawodowych.

Nowe rozporządzenie uwzględnia zatem rozwiązania, które odpowiadają faktycznym potrzebom rynku pracy.

Rozporządzenie wchodzi w życie 1 września 2019 r.

Po co normalizacja?

Kształcenie powinno być spójne z nowoczesną gospodarką oraz rozwojem przedsiębiorczości i kwalifikacji niezbędnych w przyszłej pracy. Treści zawarte w normach są regularnie aktualizowane. Normy zawsze nadążają za postępem naukowo-technicznym, a normalizacja wyznacza perspektywy i możliwości pracy zawodowej w wymiarze krajowym, europejskim i międzynarodowym, uwzględniając jednocześnie różne możliwości osobistego rozwoju i kariery.

Warto podkreślić

Normalizacja obejmuje nie tylko tematykę techniczną, lecz także zagadnienia takie jak: społeczna odpowiedzialność, problemy związane z zarządzaniem środowiskowym, bezpieczeństwo informacyjne. Reaguje na zmieniające się trendy i potrzeby – uwzględnia np. badanie autentyczności żywności czy etykę stosowania sztucznej inteligencji. Zagadnienia te dotyczą całej społeczności, a wszyscy przecież korzystamy z normalizacji.

Uwzględnienie normalizacji na różnych poziomach kształcenia jest zatem konieczne i uzasadnione.

Aleksandra Kurzep

fot. © photon_photo / Adobe Stock

Połączona przyszłość

Rick Gould

W 2018 roku wspólnie z Międzynarodową Komisją Elektrotechniczną (IEC) ISO opublikowało pierwszą na świecie normę (ISO/IEC 30141) harmonizującą architekturę referencyjną Internetu Rzeczy (IoT) – kompleksowego zbioru miliardów inteligentnych urządzeń połączonych za pośrednictwem sieci Internet. Dzięki zastosowaniu normy IoT będzie efektywniejszy, bezpieczniejszy, odporny na zagrożenia i lepiej chroniony.

Niemal 20 lat temu, brytyjski pionier z zakresu technologii, Kevin Ashton, pracujący wówczas dla firmy Procter & Gamble, ukuł nazwę „Internet Rzeczy". Ashton w swojej prezentacji pokazał, jak firma może wykorzystywać identyfikację częstotliwości radiowej (*radio-frequency identification* – RFID) – bezprzewodowej technologii, obecnie szeroko stosowanej w płatnościach zbliżeniowych i inteligentnych kartach ID – do identyfikacji i śledzenia produktów. A nazwa została.

Oficjalna definicja Internetu Rzeczy (IoT) opracowana przez ISO i IEC brzmi: „infrastruktura połączonych podmiotów, osób, systemów i źródeł informacji z usługami przetwarzającymi informacje ze strony świata fizycznego jak i świata wirtualnego". Mówiąc prościej, Internet Rzeczy to sieć skomputeryzowanych, często bezprzewodowych, urządzeń pozwalających nam widzieć, odczuwać bodźce, a nawet kontrolować świat wokół nas – czy to na poziomie jednostkowym, czy w skali globalnej.

Urządzenia i systemy IoT w coraz większym stopniu pojawiają się w wielu, jeśli nie we wszystkich, aspektach współczesnego życia. Niektóre z nich są już dobrze znane i powszechnie używane na rynkach krajowych i konsumenckich, jednak najwięksi użytkownicy Internetu Rzeczy działają w sektorach: przemysłowym, opieki zdrowotnej, komunalnym oraz rolniczym. Krótko mówiąc, dowolna technologia wzbogacona słowem smart/inteligentny najprawdopodobniej zostanie włączona do szybko rosnącej rodziny IoT; na przykład: inteligentne liczniki, inteligentne samochody, inteligentne karty, inteligentne fitness trackery, inteligentne miasta, smartfony, inteligentne zegarki (smartwatche), inteligentne media, inteligentne rolnictwo, inteligentna opieka zdrowotna, a nawet inteligentna produkcja uważana za kolejną rewolucję przemysłową.


fot. © Witthaya / Adobe Stock

Zbliżamy się

Technologia IoT sprawia, że jesteśmy połączeni, kompetentni, wydajni, efektywni i bardziej oszczędni. Jeśli jednak nie będziemy się z nią odpowiednio obchodzić, może się okazać, że nasze sieci komputerowe i dane będą mniej bezpieczne i odporne na zagrożenia. Z uwagi na stosunkową prostotę urządzenia IoT dają nam wiele możliwości, ale stawiają także wyzwania. „Ta technologia to wiele korzyści, jednocześnie najistotniejszymi kwestiami są odporność na zagrożenia i bezpieczeństwo", zauważa Francois Coallier, Przewodniczący ISO/IEC JTC 1 *Information technology*, SC 41 *Internet of Things and related technologies*. ISO i IEC założyły JTC 1/SC 41, aby skupić się na normach obejmujących zagadnienie IoT, podczas gdy JTC 1 jest odpowiedzialne za normalizację międzynarodową w zakresie technologii informacyjnej (IT); od momentu powołania w 1987 r. opublikowano już ponad trzy tysiące norm z tego zakresu.

Wyzwania interoperacyjności – lub możliwości urządzeń IoT do łączenia się między sobą i z innymi systemami w sposób płynny – oraz bezpieczeństwa są ze sobą połączone. „Technologie cały czas rozwijają się w niesamowicie szybkim tempie; uzupełnienie ich połączeniem z siecią jest jednocześnie szybkie i niejednokrotnie doraźne, w miarę pojawiania się nowych rozwiązań", dodaje Coallier. Wzrost w technologii IoT jest wykładniczy, oczekuje się, że do 2020 roku na rynku będzie działać 50 miliardów połączonych urządzeń IoT, a rynek osiągnie wartość trylionów dolarów.

Rok żarówki

Rok 2016, ten sam w którym powołano JTC 1/SC 41, był rokiem żarówki Internetu Rzeczy zarówno w sensie dosłownym, jak i przenośnym; wówczas było głośno o atakach na sieć za pośrednictwem IoT. Na przykład w marcu 2016 roku atak Mirai Botnet sparaliżował większość sieci Internet na wschodnim wybrzeżu USA; był to jak dotąd największy tego typu atak w Internecie. Wiele osób było zaskoczonych szybkością, z jaką rozprzestrzeniał się złośliwy

kod i z jaką łatwością hakerzy uzyskali dostęp do, wydawałoby się, zabezpieczonych sieci. Więc jak to się stało? Był to przypadek najsłabszego ogniwa w łańcuchu, w tej sytuacji mówimy o urządzeniach IoT na końcu sieci.

„Twórca Mirai Botnet za cel obrał urządzenia takie jak bezprzewodowe kamery CCTV* i inteligentne telewizory sprzedawane z ograniczoną liczbą domyślnych nazw i haseł administratora" – wyjaśnia Coallier. Producent wytworzył miliony takich urządzeń. „Atakujący botnet** wypróbowywał każdą kombinację nazwy i hasła administratora po kolei aż do momentu, kiedy atak zakończono sukcesem, tym samym pozwalając botnetowi na przejęcie kontroli nad urządzeniem" – uważa. „Kontrolując ponad sto tysięcy tych urządzeń, atakujący mógł generować intensywne ataki typu odmowa usługi, które mogłyby tymczasowo zakłócać pracę części sieci Internet w USA".

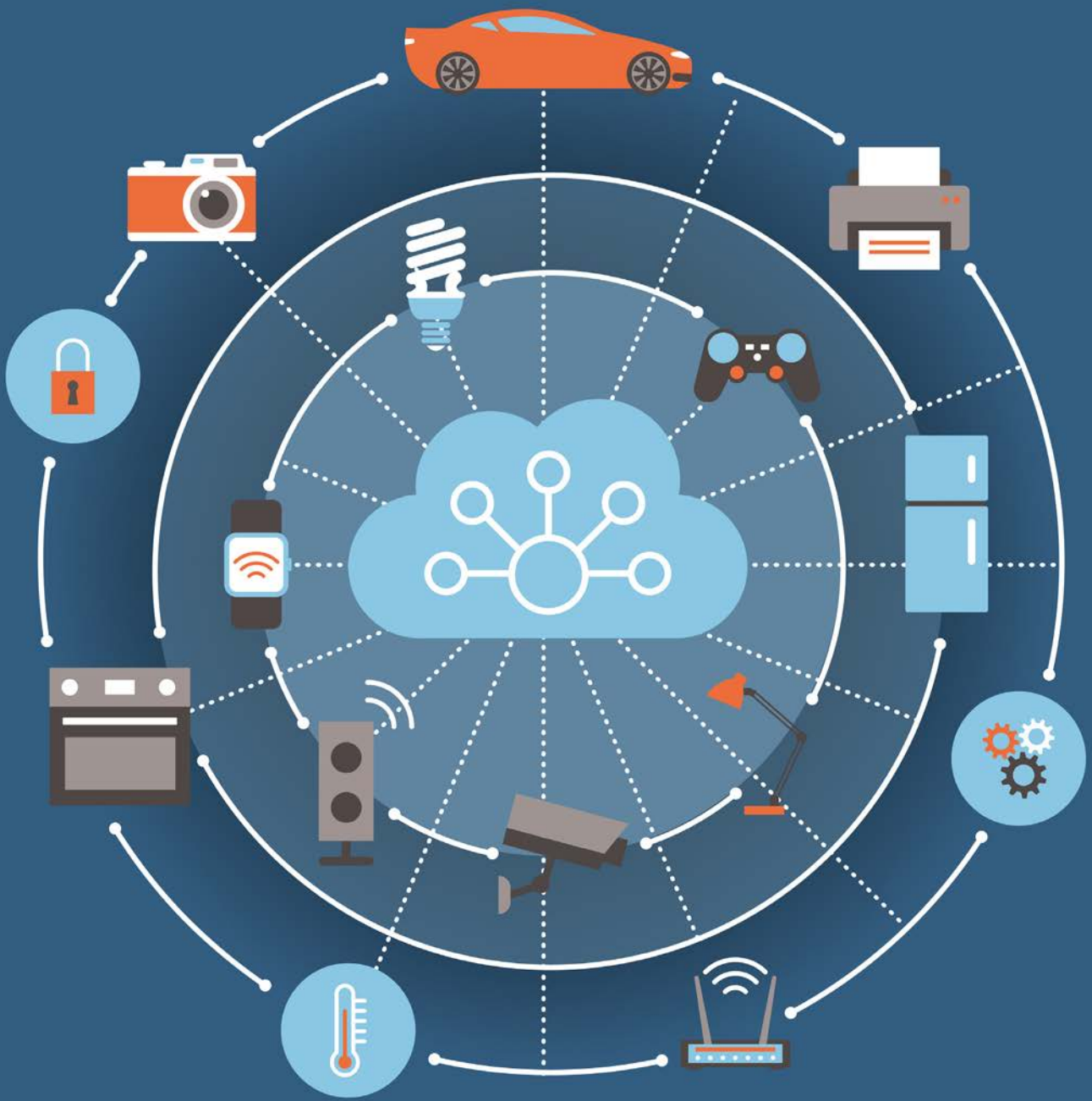
W innym dobrze udokumentowanym ataku, fabryka została zasabotowana przez atak z wykorzystaniem elementów socjotechnik w komputerach osobistych. „W tym przypadku wydaje się, że możliwe było dostanie się przez te komputery do przemysłowych systemów produkcyjnych" – uważa Coallier. „To by się nie wydarzyło, gdyby przemysłowe systemy produkcyjne zostały odseparowane od komputerów działających w sieci dzięki prawidłowej segmentacji". Co ważniejsze, sieć byłaby dużo bezpieczniejsza, gdyby wdrożyć dobrze udokumentowane procesy i procedury opisane już w wielu normach, takich jak seria ISO/IEC 27033 obejmująca techniki zabezpieczania IT; jedna z norm zaleca stosowanie sieci podzielonych w celu zwiększenia poziomu bezpieczeństwa.

W 2016 roku grupa izraelskich badaczy zademonstrowała możliwość włamania się do sieci oświetleniowej za pomocą zmodyfikowanego drona, wykorzystując luki w zabezpieczeniach popularnych inteligentnych żarówek. W prosty sposób obeszli zabezpieczenia w jednej z lamp, a to pozwoliło im zainfekować sąsiednią kompatybilną żarówkę i przejąć nad nimi kontrolę. Badacze zgłosili, że jeżeli w mieście jest wystarczająca liczba inteligentnych żarówek wykorzystujących te same protokoły komunikacyjne, złośliwy atak może bardzo łatwo zająć całą sieć żarówek w kilka minut. Taki obrót sprawy to skrajny przypadek, jednak ta demonstracja wykazała, że ryzyko wykorzystania przeoczonych luk w zabezpieczeniach pozornie bezpiecznych sieci jest wysokie.

Wejście norm IoT

W tym tkwi wyzwanie związane z urządzeniami IoT, w ich prostocie połączonej z niezamierzonym doraźnym i skomplikowanym, jeśli użytkownicy przeoczą kwestię bezpieczeństwa, wdrożeniem. Wiele takich urządzeń jest uproszczonych, minikomputery niskiego poboru mocy wyposażone w kompaktowy system operacyjny oparty na szeroko dostępnym Linuksie, popularnym wśród hakerów. Oznacza to, że urządzenia IoT mają inne wymagania niż komputery i, jeśli użytkownicy nie będą rygorystycznie stosować norm bezpieczeństwa, te czynniki sprawią, że IoT będzie coraz częstszym celem ataków. „To zasada równowagi *yin* i *yang* w IoT. Internet Rzeczy daje nam dużo możliwości, ale musimy je równoważyć ostrożnym stosowaniem i zwracać większą uwagę na kwestie bezpieczeństwa" – uważa Coallier.

Właśnie tutaj Normy Międzynarodowe mogą wesprzeć operacyjność IoT i jego odporność na zagrożenia. W jaki sposób? Na przykład seria norm ISO/IEC 29192 definiuje techniki lekkiej kryptografii, idealnej dla prostszych urządzeń o niskim poborze energii. W przypadku żarówki izraelscy badacze zarekomendowali szczególną technikę zabezpieczającą opisaną w ISO/IEC 29192-5, która określa trzy funkcje skrótu odpowiednie dla aplikacji wymagających wdrożenia lekkiej kryptografii. Jednak, jak w każdym rozwijającym się obszarze, potrzebujemy także nowych norm i tym zajmuje się JTC 1/SC 41, którego zakres prac obejmuje interoperacyjność i przede wszystkim bezpieczeństwo.



fot. © elenabsl / Adobe Stock

Do tej pory podkomitet JTC 1 wydał 18 publikacji obejmujących głównie sieci czujników. Wydano m.in. wytyczne w formie raportu technicznego, ISO/IECTR 22417 *Information technology – Internet of Things (IoT) use cases*, omawiające kontekst wykorzystania norm z zakresu IoT. Te wytyczne obejmują ważne kwestie takie jak podstawowe wymagania, interoperacyjność oraz normy, które wykorzystują użytkownicy. Co ważniejsze, przytoczone przykłady wyjaśniają, gdzie istniejące normy odgrywają ważną rolę i podkreślają, jaki obszar powinien zostać objęty dalszymi pracami normalizacyjnymi.

Tworząc podstawy

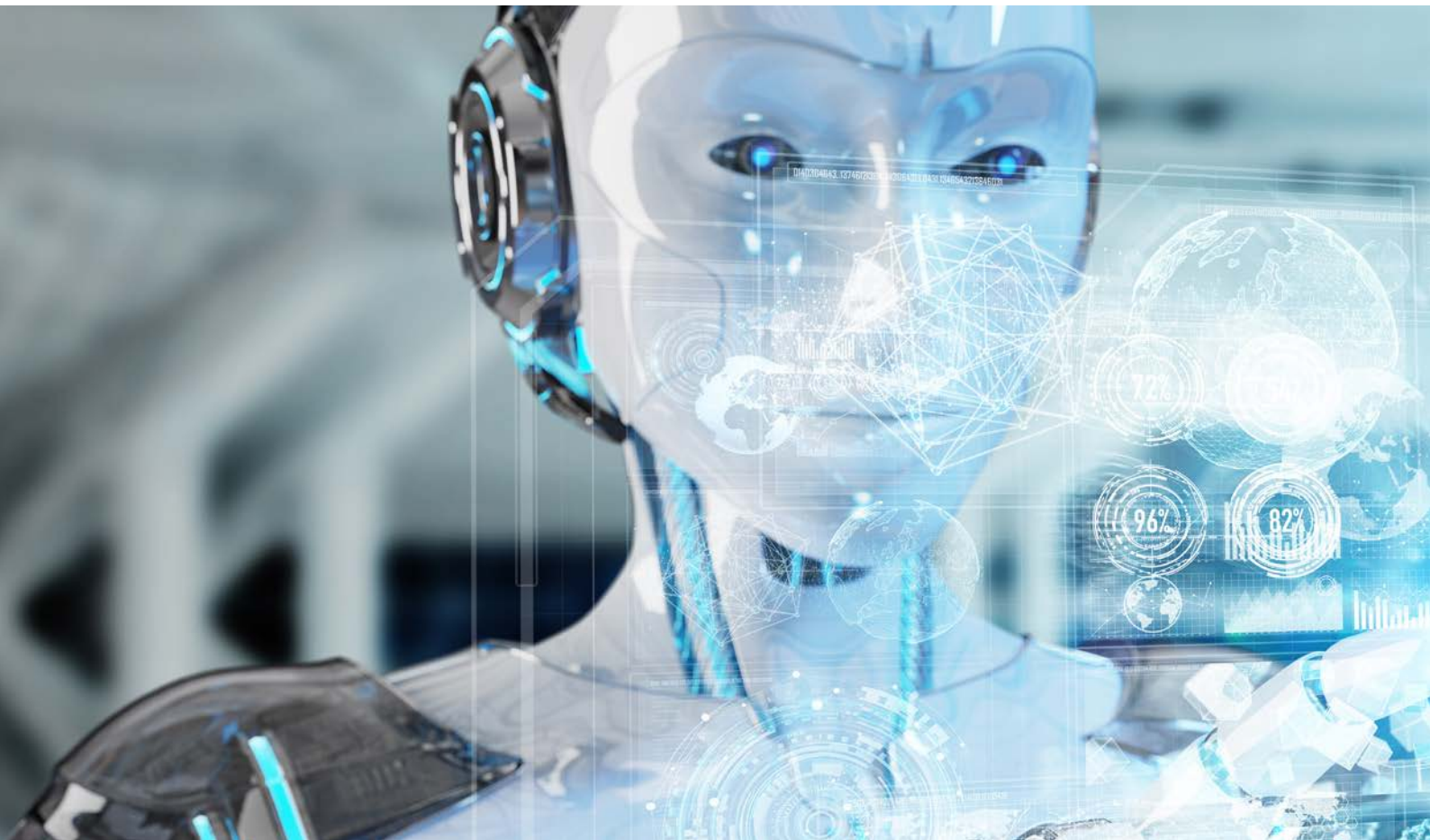
Normy z zakresu Internetu Rzeczy tworzą wspólny grunt dla tematów takich jak terminologia czy architektury referencyjne, które pomogą twórcom rozwinąć interoperacyjny ekosystem. ISO/IEC 30141 zawiera podstawy i ramy odniesienia do wielu norm opracowanych przez JTC 1/SC 41. „Zauważyliśmy potrzebę architektury referencyjnej w celu maksymalizacji korzyści i redukcji ryzyka" – wyjaśnia Coallier, przewodniczący podkomitetu ISO. Inną fundamentalną normą jest ISO/IEC 20924 *Information technology – Internet of Things (IoT) – Definition and vocabulary*. „Bardzo ważne jest, by osoby zajmujące się IoT mówiły tym samym językiem". ISO/IEC 20924 oraz ISO/IEC 30141 zapewniają niezbędne słownictwo.

Grupą roboczą, która pracowała nad ISO/IEC 30141, przewodził dr Jie Shen z Chin; wspierało go dwóch redaktorów współpracujących: Wei Wei z Niemiec oraz Östen Frånberg ze Szwecji. Razem szefowie projektu mają wieloletnie doświadczenie w branży, wspomagane przez 50 innych specjalistów, którzy bezpośrednio przyczynili się do powstania tej normy. „IoT to wiele możliwości, a także wiele zagrożeń" – mówi dr Jie Shen. „Konieczne jest stworzenie idealnego mechanizmu, który pozwoli nam pokonać zagrożenia; to samo w sobie jest kwestią szczegółów".

Większość tych szczegółów zapewnia wiele norm wydanych przez podkomitety JTC 1, natomiast ISO/IEC 30141 dostarcza architekturę referencyjną, która składa je w jedną całość, razem z nowymi normami, nad którymi pracuje JTC 1/SC 41. „ISO/IEC 30141 zapewnia wspólną ramę dla twórców IoT" – wyjaśnia Coallier. „Norma ta opisuje główne cechy charakterystyczne IoT, model konceptualny oraz architekturę referencyjną" – dodaje. Opisy zostały wzbogacone wieloma przykładami.

Łańcuch sześciu domen

ISO/IEC 30141 obejmuje także nowatorską i innowacyjną strukturę znaną jako „Six-Domain Model for IoT reference architecture" (Model sześciu domen dla architektury referencyjnej IoT). Zapewnia ona ramy dla projektantów systemów zapewniające integrację mnogości urządzeń i procesów w ramach IoT. Grupa projektowa doszła do wniosku, że konwencjonalne podejścia nie są odpowiednie dla prostszych sieci. Dr Jie Shen wyjaśnia: „o wiele trudniej jest zbudować ekosystem w IoT, aby połączyć wiele heterogenicznych podmiotów takich jak użytkownicy – ludzie, obiekty fizyczne, urządzenia, platform usługowe, aplikacje, bazy danych, narzędzia zewnętrzne i inne zasoby. Ustaliliśmy, że konwencjonalny warstwowy model od-



niesienia tradycyjnie wykorzystywany w systemach IT jest niewystarczający". Z drugiej strony, *Six-Domain Model* może pomóc podzielić ekosystem IoT w sposób jednoznaczny i poprowadzić użytkowników tak, by mogli stworzyć nowy model biznesowy IoT. Model sam w sobie będzie jeszcze bardziej efektywny, jeśli będzie wspomagany przez technologię *blockchain*, wysoce bezpieczną technikę coraz szerzej stosowaną przy transakcjach finansowych.

Ta norma bardzo wiele mówi o interoperacyjności – lub umożliwianiu różnym typom urządzeń płynnej komunikacji – i o koncepcji wiarygodności IoT. To z kolei definiowane jest jako stopień zaufania, jakie mogą mieć użytkownicy wobec systemu zachowującego się zgodnie z oczekiwaniami, zapewniającego jednocześnie bezpieczeństwo, ochronę, prywatność, niezawodność i odporność w obliczu zakłóceń, takich jak klęski żywiołowe, usterki, błędy ludzkie i ataki z zewnątrz. „Opublikowano już wiele norm dotyczących odporności i bezpieczeństwa, jednocześnie ISO/IEC 30141 zapewnia architekturę referencyjną do ich stosowania" – mówi Coallier. W tym samym czasie, w miarę jak Internet Rzeczy ewoluuje i „rośnie", JTC 1/SC 41 pracuje nad dziewięcioma kolejnymi normami obejmującymi IoT, które zapewnią zwiększenie wiarygodności, interoperacyjności, poziomu bezpieczeństwa oraz nowe specyfikacje techniczne.

**CCTV cameras – kamery telewizyjne w układzie zamkniętym (Closed circuit TV cameras).*

*** Botnet – grupa komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem) pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu.*

Tłum. I. P.
Źródło: ISOfocus

fot. © sdecoret / Adobe Stock

MISJA
DLA CYBERZAUFANIA

Robert Bartram

fot. © vegefox.com / Adobe Stock

Ponieważ technologia staje się coraz bardziej zaawansowana i oferuje zarówno większe możliwości, jak i ujawnia nowe zagrożenia, istnieje niebezpieczeństwo, że różnego typu organizacje pozostaną podatne na złośliwy atak lub naruszenie danych na masową skalę. Zarządzanie ryzykiem jest zatem tak samo ważne w cyberprzestrzeni, jak w świecie fizycznym. Ale jakie są te zagrożenia cybernetyczne? W jaki sposób Normy Międzynarodowe mogą je złagodzić? I czy tak naprawdę jedyną odpowiedzią jest jeszcze bardziej zaawansowana technologia?

Definicja ryzyka w Oxford English Dictionary jest z pewnością wystarczająco jasna: „ryzyko" to „sytuacja wiążąca się z narażeniem na niebezpieczeństwo". Aby osiągnąć wyniki, należy podjąć ryzyko, jednak aby osiągnąć pozytywne rezultaty i uniknąć negatywnych konsekwencji, należy także tym ryzykiem zarządzać.

Unikanie ryzyka nie jest możliwe. Ryzyko musi zostać podjęte; jest to nieunikniona i niezbędna część naszego życia, zarówno prywatnego, jak i zawodowego. Ale ryzyko może być również dobrą siłą napędową. Skuteczne zarządzanie ryzykiem może mieć pozytywne skutki, a firmy muszą podejmować ryzyko, aby osiągać swoje cele. Organizacje potrzebują pewności, zanim podejmą ważne decyzje strategiczne. Ważne jest zrozumienie, że ryzyko to w rzeczywistości prawdopodobny wpływ niepewności na te decyzje. Krótko mówiąc, ryzyko polega na zarządzaniu decyzjami w złożonym, zmiennym i niejednoznacznym świecie, który szybko staje się jeszcze bardziej złożony i niejednoznaczny.

Cyfrowe zagrożenie

Szczególnie odnosi się to do obszaru cyberryzyka. W cyberprzestrzeni wysoki poziom niepewności rutynowo wynika z rozwiązywania problemów bezpieczeństwa narodowego i korporacyjnego. Zagrożenie nie pochodzi z kontekstu i okoliczności rynku, ale ze strony „podstępnych podmiotów" dokonujących poważnych przestępstw. W związku z tym są one niedostrzegalne, co jedynie zwiększa poczucie zagrożenia. Te złośliwe podmioty mają zamiar i możliwość by wyrządzić szkodę, ponadto są zręczne i szybko się dostosowują do sytuacji.

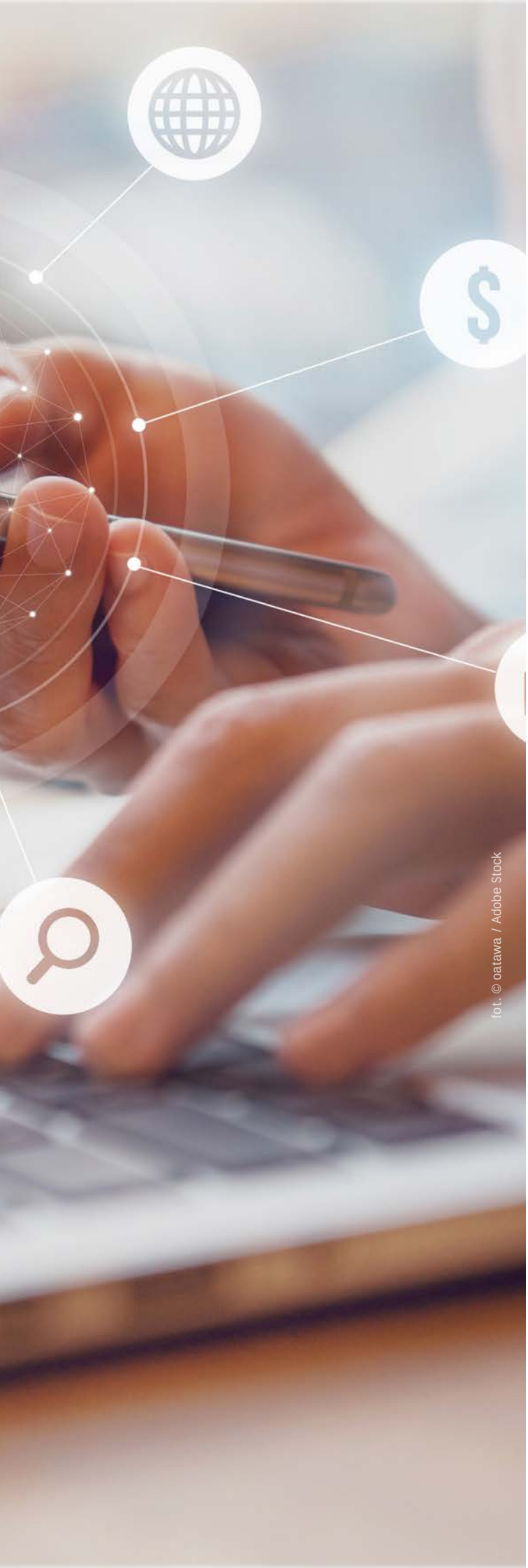
Co więcej, technologia codziennie, jeśli nie co godzinę, staje się coraz bardziej zaawansowana. W przeszłości przestępca przemysłowy mógł ukraść wartościowe dokumenty z teczki, gdyby te zostały pozostawione niedbale na biurku. Obecnie dzięki pamięciom USB oraz wykorzystaniu eksfiltracji danych ten sam przestępca może wykraść gigabajty danych. Nie chodzi tylko o to, że przechowywanie danych wykładniczo jest coraz bardziej zaawansowane – od formy papierowej po cyfrową – lecz także o to, że zmienił się charakter i cel danych. Jeśli przestępca zamierza na przykład wykraść chronione produkty medyczne nie musi już włamywać się do magazynu, wystarczy, że skopiuje dane w formacie cyfrowym i może sklonować produkt za pomocą drukarki 3D.

Dla każdego typu organizacji nieodzowna jest jakaś forma cyberzabezpieczeń. Jednak potrzebują one jeszcze systemu na tyle solidnego, by był zdolny alarmować ich o każdym ataku – realnym lub domniemanym – tak szybko jak to tylko możliwe. Zagrożenia w cyberprzestrzeni dzielimy na dwie obszerne kategorie: wewnętrzne i zewnętrzne. Aby zaprojektować i skutecznie wdrożyć system ochronny przed zagrożeniami zewnętrznymi, należy położyć nacisk na intencje i możliwości zewnętrznych podmiotów szkodliwych – czym są, po co powstały i jakie technologie są dla nich dostępne.

Jednak firmy muszą także przygotować się na zagrożenie zarówno ze strony złośliwych insiderów, jak i osób, które omyłkowo pozostawiły system podatny na ewentualne szkody. Nieostrożne korzystanie z danych osobowych może narazić jednostkę na szantaż i rekrutację przez firmę o złych celach. Firmy mogą mieć najlepsze zapory sieciowe na świecie, jednak nic one nie znaczą w starciu z osobą mającą otwarty dostęp do ważnych danych, których wykradzenie może zostać niezauważone.

Co się naprawdę liczy?

Jak więc rządy, przedsiębiorstwa i osoby fizyczne bronią się przed tymi zagrożeniami? Komitet Techniczny ISO/TC 262 Risk management opublikował normę z zakresu zarządzania ryzykiem ISO 31000, która zawiera zasady i procesy ogólnego zarządzania ryzykiem. Jason Brown, który jest przewodniczącym ISO/TC 262, był odpowiedzialny m.in. za zarządzanie oceną i gwarancją bezpieczeństwa cybernetycznego w australijskim Departamencie Obrony. Wskazuje on, że jeśli firma poważnie myśli o ochronie przed cyberzagrożeniami, musi „wrócić do pierwotnych założeń przedsiębiorstwa i spojrzeć na to, co naprawdę się liczy – innymi słowy, znać swoje największe cyfrowe skarby".



fot. © oatawa / Adobe Stock

Przedsiębiorstwa i rządy muszą bardzo ostrożnie oceniać wartość i charakter tego, co uważają za cenne. Jeśli firma stoi na straży własności intelektualnej o wysokiej jakości technicznej w formie danych, oczywiste jest, że wyciek takich danych lub ich kradzież może wywołać poważne konsekwencje. Następstwa takiego zdarzenia byłyby bardziej destrukcyjne, gdyby te informacje były przechowywane w imieniu podmiotów zależnych od tej organizacji jako części łańcucha dostaw; naruszenie w systemie może skutkować zniszczeniem całego łańcucha. Liczy się zatem przede wszystkim strategiczny przegląd systemowy, a nie ocena samej technologii. Podejście to jest zgodne z podejściem dra Donalda R. Deutscha, wiceprezesa i głównego specjalisty ds. norm w kalifornijskim Oracle oraz przewodniczącego Podkomitetu Technicznego ISO/IECJTC 1 *Information technology*, *SC 38*, *Cloud computing and distributed platforms*. Chmura i jej pozycja w hierarchii ryzyka ma prawdopodobnie największe bezpośrednie znaczenie dla konsumentów. Jeśli korzystamy obecnie z komputera, jest bardzo prawdopodobne, że będziemy również korzystać z chmury. Chmura obliczeniowa, mówi dr Deutsch, „jest bardziej strategią wdrożeniową i biznesową, niż strategią technologiczną". Niewątpliwie istnieją najnowsze udoskonalenia technologiczne związane z zagrożeniami – takie jak automatyczne udostępnianie zasobów obliczeniowych, które są współdzielone przez wielu użytkowników – a jednak „ryzyko jest takie samo, jak w każdym środowisku komputerowym, jednak nasilone i powiększone z uwagi na skalę użycia".

Cena odporności

Normy Międzynarodowe stanowią podstawę tego strategicznego podejścia do cyberryzyka. Jak zauważa Jason Brown, w kwestii zagrożeń cybernetycznych, serię norm ISO 31000 należy oceniać razem z serią ISO/IEC 27000 dotyczącą systemów zarządzania bezpieczeństwem informacji (SZBI). Takie podejście równoważy koncentrację na technologii z czynnikami ludzkimi. ISO/IEC 27000 pomoże firmie ocenić jej czysto technologiczne potrzeby, podczas gdy ISO 31000 pozwoli jej zrozumieć wartość informacji lub produktów, które ma w cyberprzestrzeni, a zatem stopień ochrony technologicznej, której będzie potrzebować, aby zapobiec wszelkim atakom. Innymi słowy, dokładna ocena ryzyka z ISO 31000 może zaoszczędzić każdej firmie znacznych nakładów finansowych na zakup systemu bezpieczeństwa technologicznego. Nieznajomość ryzyka może prowadzić zarówno do zbyt dużego, jak i zbyt małego płacenia za system ochronny.

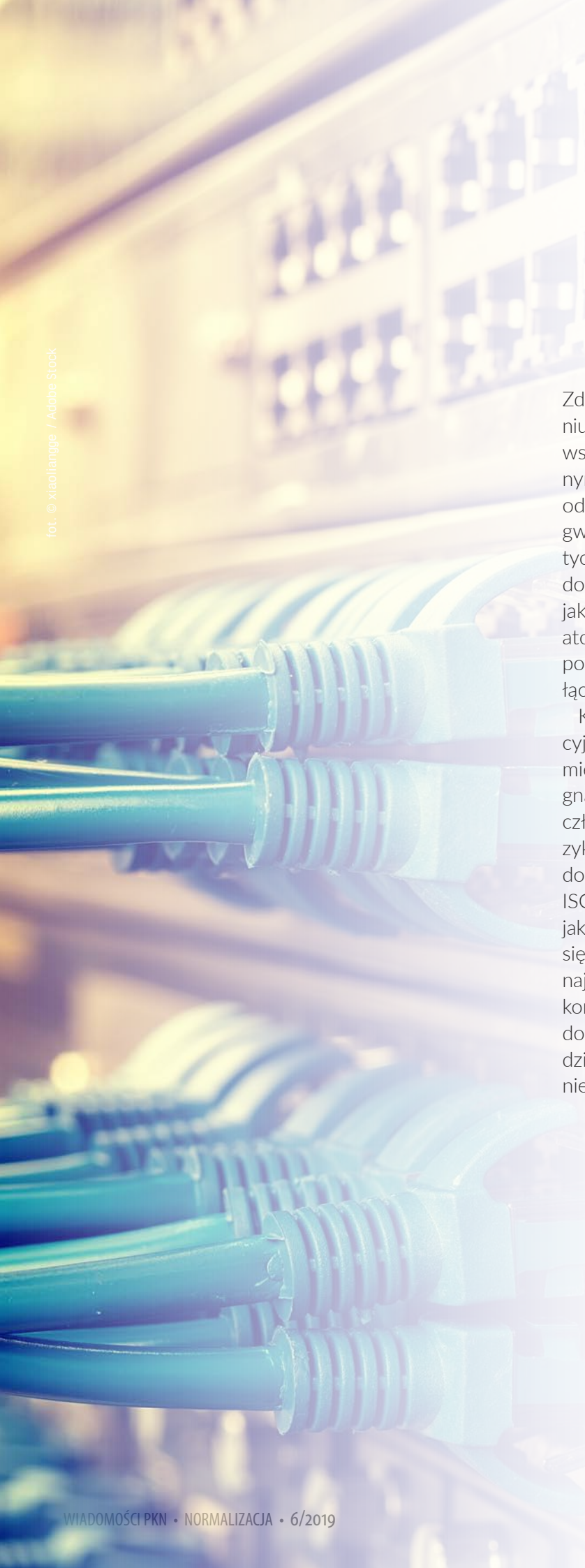
Cyberbezpieczeństwo należy również analizować pod kątem ciągłości biznesowej, a seria ISO 22301 z zakresu zarządzania ciągłością działania obejmuje właśnie te zagadnienia. Ta seria pozwala na „udokumentowany system zarządzania chroniący przed [...] destrukcyjnymi incydentami, kiedy się pojawią" i umożliwia firmie ocenę, w jaki sposób jej system informacyjny i telekomunikacyjny wspiera wyznaczone przez nią cele i jakie byłyby konsekwencje w razie jego upadku. Wysokość inwestycji przedsiębiorstwa w cyberbezpieczeństwo może być wynikiem jej zależności od systemu; mała firma może być w stanie kontynuować rachunkowość w formie papierowej (a nawet do niej całkowicie powrócić), natomiast giganci tacy jak Amazon są dosłownie uzależnieni od łączności.

Podobnie prace ISO/IEC JTC 1/SC 38 pomagają producentom – a tym samym ostatecznie konsumentom – mówić wspólnym językiem dla chmury obliczeniowej. Co istotne, popyt na tę grupę norm nie był napędzany, jak to zazwyczaj bywa, przez samych producentów lub sprzedawców, ale przez klientów i nabywców. Rządy i korporacje wskazywały, że każdy producent posługuje się własną terminologią, uniemożliwiając porównywanie produktów i dokonywanie świadomej decyzji, który z nich wybrać. Doprowadziło to do opublikowania normy ISO/IEC 17789 *Information technology – Cloud computing – Reference architecture*, która ustanowiła architekturę referencyjną i ramy wspólnego słownictwa. Podkomitet SC 38 nadzorował również tworzenie ISO/IEC 19086, czteroczęściowej normy obejmującej umowy usługowe między dostawcami usług w chmurze a ich klientami, z których dwie części są nadal rozwijane.

Skok jakościowy

Nie można wątpić w pozytywny wpływ, jaki wszystkie te normy wywarły na cyberbezpieczeństwo, a w szczególności na cyberzagrożenia. ISO 31000 zostało przyjęte przez około 40 państw jako krajowy system zarządzania ryzykiem. Google w ciągu 0,54 sekundy wyświetla ponad 6,5 miliona wyników po wpisaniu do wyszukiwarki frazy „ISO 31000".

W miarę coraz szybszego tempa rozwoju technologii Normy Międzynarodowe muszą dotrzymywać jej kroku. Działające dziś narzędzia wcale nie muszą działać w przyszłości. Na przykład dzięki uczeniu maszynowemu w kierunku sztucznej inteligencji, prawdopodobnie pojawi się zarówno zdolność adaptacyjnego uczenia się, jak i zdolność „filozoficzna" w systemie, które po prostu nie istnieją w dzisiejszym świecie.



fot. © xiaolianggе / Adobe Stock

Zdolność analityczna danych rozwija się w takim stopniu, że można przeanalizować duże ilości danych w celu wskazania pojawiających się problemów, które w innym przypadku nie byłyby wykrywalne. Niezależnie od tego pojawienie się komputerów kwantowych gwałtownie zwiększy szybkość obliczeń. Połączenie tych trzech zmian w cybernetycznym świecie „prawdopodobnie będzie najbardziej destrukcyjną rzeczą, jaką widzieliśmy od czasu odkrycia elektryczności lub atomu" – mówi Jason Brown. Nawet nie bierze się pod uwagę nanotechnologii ani rosnącej wzajemnej łączności wszystkich rzeczy.

Kiedy te czynniki się połączą, zmiany w konkurencyjnym środowisku dla korzyści w biznesie, korzyści między krajami, a także odbiorcą a zleceniodawcą, ulegną znacznemu przyspieszeniu. Tak bardzo, że wkład człowieka prawdopodobnie nadal będzie określać ryzyko wokół celów, ale rzeczywista zdolność człowieka do zajęcia się cyberprzestrzenią może być znikoma. ISO/TC 262 bada obecnie obszar, który oznaczono jako „Zarządzanie nowymi zagrożeniami", koncentrując się na tych zagrożeniach, które prawdopodobnie będą najbardziej destrukcyjne. Jak wyjaśnia Brown, zarówno konsumenci, jak i producenci muszą inaczej podejść do przyszłości, a my wszyscy „będziemy musieli bardziej otworzyć się na ten bardzo niestabilny i wysoce niejednoznaczny świat".

Tłum. I. P.
Źródło: ISOfocus, January/February 2019

Termomodernizacja 2019

fot. © Roman Babakin / Adobe Stock

90% czasu spędzamy w budynkach. W większości krajów UE około 65% budynków mieszkalnych zostało wybudowanych przed wejściem w życie pierwszych europejskich przepisów dotyczących efektywności energetycznej budynków (tj. przed 1979 r.). Około 65% europejskich i 58% polskich zasobów budowlanych to budynki starsze niż 40 lat. Jedynie 10% budynków ma obecnie świadectwa energetyczne klasy A lub B. Tylko 1-2% budynków rocznie przechodzi renowację. Jak zatem zmierzać do niskoemisyjnego budownictwa?

3 kwietnia 2019 roku w Tower-Service w Warszawie odbyło się „XIX FORUM TERMOMODERNIZACJA 2019" zorganizowane przez Zrzeszenie Audytorów Energetycznych (ZAE). Temat wiodący tegorocznego forum to Odnawialne źródła energii.

Organizowane od wielu lat kolejne edycje FORUM TERMOMODERNIZACJA są bardzo ważnym wydarzeniem, które stwarza możliwość dyskusji i wymiany poglądów na temat efektywności energetycznej budynków.

Prelegenci wyrazili pogląd, że w działaniach dotyczących termomodernizacji powinna nastąpić zmiana priorytetów: poprawa jakości powietrza jest ważniejsza niż zmniejszenie zużycia energii, ponieważ zła jakość powietrza niszczy zdrowie społeczeństwa, a lepsza jakość powietrza – również wewnątrz pomieszczeń – to wyższy standard życia.

Przedstawiciel VELUX Polska przedstawił raport Barometr zdrowych domów, w którym zwrócono uwagę na niezadowalający stan budynków mieszkalnych w Europie i Polsce oraz wynikające stąd zagrożenie dla zdrowia i wzrost ubóstwa energetycznego. Przyznano, że kompleksowa termomodernizacja jest skuteczną metodą oszczędności energii i walki ze smogiem. Omówiono nowoczesne wymagania dla nowych i remontowanych budynków w poszczególnych krajach Europy.

Około 17% Europejczyków twierdzi, że mieszka w niezdrowym budynku.

Stan budynków Polsce:

- 22% mieszkań jest zawilgoconych;
- 23% – niedoświetlonych;
- 26% – niedogrzanych.

Stare budynki stanowią problem społeczny. Następuje wzrost zagrożenia ubóstwem energetycznym ze względu na rosnące ceny energii, niskie dochody oraz fakt, że budynki są nieefektywne energetycznie. Blisko 9 mln Polaków nie jest w stanie ponosić kosztów ogrzewania swoich domów.

Według szacunków możliwa jest oszczędność energii cieplnej dzięki:

- wymianie stolarki okiennej i drzwiowej – 10% do 15%;
- izolacji cieplnej ścian zewnętrznych – 15% do 25%;
- izolacji cieplnej dachu lub stropodachu – 15% do 25%;
- ociepleniu stropu nad nieogrzewaną piwnicą, izolacji podłogi na gruncie 15% do 25%.

Niska efektywność energetyczna budynków jednorodzinnych jest główną przyczyną smogu w Polce. Omówiono dotychczasowe i aktualne działania dotyczące zwalczania zanieczyszczenia powietrza prowadzone przez rząd i samorządy lokalne. Za szczególnie ważne uznano działania w Krakowie, gdzie od września br. będzie obowiązywał całkowity zakaz korzystania z paliw stałych do ogrzewania domów. Przedstawiono kierunki i zakres zmian w systemie świadectw energetycznych budynków. Zmiany te są konieczne w związku z implementacją nowej dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/844 z dnia 30 maja 2018 r. (zmieniającej dyrektywę 2010/31/UE w sprawie charakterystyki energetycznej budynków i dyrektywę 2012/27/UE w sprawie efektywności energetycznej), a także do poprawienia działania systemu świadectw na podstawie doświadczeń ostatnich lat.

W drugiej sesji omówiono m.in. wykorzystanie pomp ciepła jako technologii grzewczej, która ma największy potencjał redukcji CO_2.

Przedstawiciel KAPE S.A. przybliżył zebranym zastosowanie technologii OZE w termomodernizacji budynków, w tym szczególne znaczenie OZE dla zmniejszenia zapotrzebowania na energię pierwotną i redukcję szkodliwych emisji. Prelegent przedstawił możliwości wykorzystania energii promieniowania słonecznego, wiatru, biomasy, pomp ciepła i energii odpadowej, wskazując równocześnie wady w praktyce stosowania. Wynikają one często z nieznajomości specyfiki instalacji OZE, braku doświadczenia oraz nieuwzględniania nowoczesnych technologii i rozwiązań.

Przedstawiciel PORT PC wskazał, że wykorzystanie pomp ciepła jako technologii grzewczej ma największy potencjał redukcji emisji CO_2 w ogrzewnictwie. PORT PC prognozuje, że do 2030 r. liczba instalacji pomp ciepła będzie wynosić około 1 miliona sztuk. Przedstawiono kluczowe innowacje w technologiach budynków, a także zastosowanie wskaźnika SRI oceny budynków zgodnie z nową dyrektywą 2018/844/UE – wskaźnika gotowości SMART dokonywanego według ośmiu kryteriów. Prelegent omówił kampanię informacyjną Dom bez rachunków wskazującą racjonalne rozwiązania w ogrzewaniu budynków.

Podczas trzeciej sesji dyskutowano m.in. o technologii BIM, budownictwie i systemach inteligentnego sterowania węzłem cieplnym.

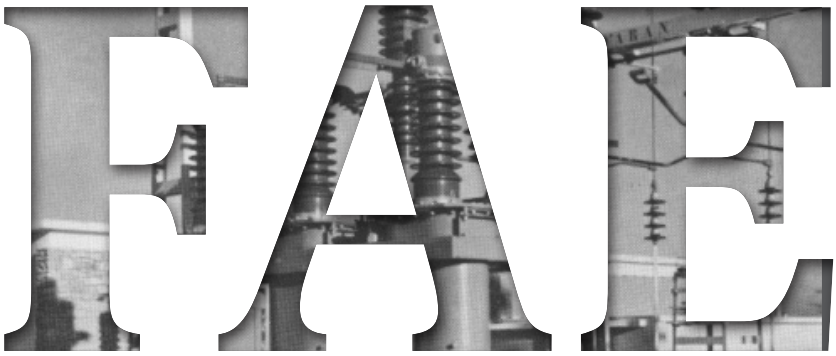
Prelegent EGAIN Polska przedstawił system inteligentnego sterowania węzłem cieplnym, który dzięki danym pogodowym, a także właściwościom cieplnym i lokalizacji budynku z wyprzedzeniem przewiduje sposób ogrzewania budynku przy optymalnym zużyciu. Prelegent przedstawił przypadki, w których zastosowano system uzyskujący 10 – 20% zmniejszenie zużycia energii.

Prelegent z KINGSPAN INSULATION omówił możliwości, jakie stwarza zastosowanie płyt Kooltherm z pianki rezolowej. Dzięki bardzo niskim wartościom współczynnika przewodzenia ciepła (od 0,018 W/m·K do 0,020 W/m·K) możliwe jest wykonanie ociepleń o niewielkiej grubości, co jest bardzo ważne np. przy ocieplaniu ścian od wewnątrz, ścian klatek chodowych, poddaszy i płyt balkonowych.

Andrzej Wiszniewski (NAPE) omówił raport dotyczący rynku budownictwa mieszkaniowego w Polsce opracowany w ramach programu Building Market Briefs. Raport zawiera informacje na temat krajowych uwarunkowań sektora budowlanego i wskaźniki, które można bezpośrednio porównywać pomiędzy krajami. Raporty zawierają porównywalne dane w skali europejskiej, skondensowany wgląd w sektor budowlany, ukazują potencjał rynkowy z wielu perspektyw.

W ostatnim referacie przedstawiciel SANKOM, Politechnika Warszawska, przybliżył zastosowanie technologii BIM w auditingu energetycznym i projektowaniu instalacji sanitarnych w oprogramowaniu w serii AUDYTOR. Oprogramowanie to pozwala na bardzo precyzyjne wykonanie obliczeń cieplnych, import modelu budynku z programu AUTODESK, automatyczne programowanie instalacji i wizualizację przestrzenną instalacji w budynku.

Małgorzata Siemińska
Sektor Budownictwa i Konstrukcji Budowlanych
Sekretarz KT 179 ds. Ochrony Cieplnej Budynków



– historia zakładów inż. Kazimierza Szpotańskiego

Fabryka Aparatów Elektrycznych FAE została założona w 1919 r. w Warszawie przez Kazimierza Szpotańskiego, prekursora polskiego przemysłu elektrotechnicznego, współzałożyciela Stowarzyszenia Elektryków Polskich. Na początku lat 30. w FAE rozpoczęto produkcję liczników energii elektrycznej, przez co fabryka ta stała się poważną konkurencją na rynku polskim dla firmy Siemens.

Historia

Kazimierz Szpotański studiował elektrotechnikę w Niemczech, początkowo w Wyższej Szkole Technicznej w Mittweidzie (1905-07), a następnie na Politechnice w Berlinie-Charlottenburgu (1910-11), gdzie uzyskał dyplom inżyniera elektryka.

Wiedzę zdobytą na studiach uzupełniał praktyką, pracując w latach 1907-10 w fabrykach AEG (Allgemeine Elektricitäts-Gesellschaft) w Niemczech, a po uzyskaniu dyplomu inżyniera powrócił do pracy w AEG. W latach 1911-13 pracował w Berlinie oraz później w oddziałach tej firmy na terenie Rosji, w Charkowie i Rydze. W fabryce w Rydze zorganizował m.in. duży dział produkcji aparatów elektrycznych, zatrudniający około 600 osób, a w Charkowie zaangażował się w działalność społeczną, uczestnicząc w pracach Charkowskiego Oddziału Stowarzyszenia Techników Polskich w Rosji, gdzie w latach 1917-18 pełnił funkcję skarbnika.

Pod koniec I wojny światowej w sierpniu 1918 r. przyjechał do Warszawy i tam otworzył warsztat elektryczny przy ul. Mirowskiej 9 (w XVIII i XIX w. od placu Mirowskiego do Elektoralnej biegła niewielka ulica Mirowska, która do 1879 nosiła nazwę Zatylki, gdyż znajdowała się za tyłami koszar Mirowskich; dziś ulica ta nie istnieje). Swój warsztat nazwał Fabryką Aparatów Elektrycznych K. Szpotański z tym, że w latach 1919-23 K. Szpotański działał w spółce ze Stefanem Ciszewskim. Spółka rozwijała się dobrze i wystawiała swoje wyroby m.in. na krajowych Targach w Poznaniu i Lwowie. Zakład przeniesiony na Kamionek przy ul. Kałuszyńskiej szybko się rozrósł i stał się największym w Polsce przedwojennej zakładem produkującym aparaturę elektryczną. Po dziesięciu latach działalności pracowało w nim już 1100 robotników oraz ok. 100 inżynierów.

K. Szpotański nie zaniedbywał też działalności stowarzyszeniowej i w roku 1918 został członkiem Koła Elektrotechników istniejącym przy Stowarzyszeniu Techników w Warszawie. W marcu został wybrany członkiem 6-osobowego Komitetu Organizacyjnego Ogólnopolskiego Zjazdu Elektrotechników, któremu przewodniczył prof. Mieczysław Pożaryski. Zjazd odbył się w dniach 7-9 czerwca 1919 roku w Warszawie i w ostatnim dniu Zjazdu uchwalono powołanie Stowarzyszenia Elektryków Polskich (SEP). Wybrano też tymczasowy 9-osobowy Zarząd SEP z przewodniczącym prof. M. Pożaryskim, w składzie którego był również inż. K. Szpotański.

W 1924 r. inż. Szpotański przekształcił firmę w spółkę pod nazwą Fabryka Aparatów Elektrycznych K. Szpotański i S-ka, Spółka Akcyjna (FAE). Na początku lat 30. w FAE rozpoczęto produkcję liczników energii elektrycznej, przez co stała się poważną konkurencją na rynku polskim dla firmy Siemens.

Niektóre liczniki wciąż pracują w warszawskich przedwojennych kamienicach na Kamionku

Rozwój produkcji liczników

Liczniki energii produkowane w FAE spełniały wszelkie wymogi międzynarodowe, fabryka uzyskała uprawnienia do ich legalizacji.

Inżynier K. Szpotański był otwarty na współpracę międzynarodową, korzystał też z licencji, zwiększając tym samym dynamikę rozwoju produkcji. Stosował też zasady nowoczesnego marketingu. Produkty wytwarzane przez FAE były prezentowane na wystawach krajowych i zagranicznych (m.in. w Nowym Jorku w 1939 r.), zdobywały liczne wyróżnienia i nagrody, a ponadto FAE prowadziła działalność informacyjną - wydawano katalogi, broszury oraz własne pismo „Informacje dla przyjaciół FAE". Takiemu marketingowi sprzyjała zasada dobrej jakości, gdyż inż. Szpotański wymagał, aby każdy produkt FAE był trwały i spełniał najwyższe wymogi jakości, estetyki i nowoczesności. W 1937 r. za swoje osiągnięcia inż. Kazimierz Szpotański otrzymał od prezydenta Ignacego Mościckiego Krzyż Kawalerski Orderu Odrodzenia Polski. W 1937 roku został też odznaczony nowo ustanowioną Złotą Odznaką Honorową SEP, a w następnym roku wybrano go na prezesa SEP i funkcję tę sprawował do roku 1939.

W tym czasie w FAE podjęto także produkcję aparatury rentgenowskiej, a jej prototypy zyskały akceptację i powszechne uznanie najwybitniejszych radiologów polskich, którzy uznali je za co najmniej równorzędne aparatom zagranicznym.

Produkty FAE były powszechnie stosowane w całym systemie elektroenergetycznym tworzonym w Polsce w okresie międzywojennym.

Po wybuchu II wojny światowej w 1939 r. nowo wybrany prezes SEP kpt. inż. A. Krzyczkowski został zmobilizowany i nie objął tej funkcji. Tym samym funkcję prezesa pełnił inż. K. Szpotański aż do roku 1946.

W okresie okupacji niemieckiej fabryka FAE nadal działała pod kierownictwem inż. Szpotańskiego, który starał się pomagać w różny sposób mieszkańcom Warszawy i członkom ruchu oporu. Sam był represjonowany przez okupanta. W 1942 r. został aresztowany przez Gestapo i więziony na Pawiaku, ale w 1943 r. Niemcy uznali, że jego obecność w fabryce jest niezbędna i został wypuszczony z więzienia.

W 1944 r., w trakcie kończących się działań wojennych w Warszawie, fabryka FAE została celowo zniszczona przez Niemców. Wywieziono maszyny, urządzenia i surowce oraz wysadzono w powietrze kilka budynków fabrycznych.

Zaraz po ustaniu działań wojennych w 1945 r. Kazimierz Szpotański przystąpił do odbudowy fabryki, ale wkrótce została upaństwowiona i nazwana Pierwszą Państwową Fabryką Aparatów Elektrycznych (PPFAE). W sierpniu tegoż roku K. Szpotański został mianowany jej dyrektorem, lecz już w listopadzie 1947 r. został zmuszony przez władze komunistyczne do odejścia.

W 1951 roku, dzięki staraniom swoich kolegów elektryków, inż. Szpotański otrzymał stanowisko naczelnego specjalisty elektryka w Centralnym Zarządzie Biur

Projektów Budownictwa Przemysłowego i pracował tam do grudnia 1960 r.

Po zmianach politycznych, które zaszły w Polsce w 1956 r., inż. Kazimierz Szpotański wznowił swoją aktywną działalność w SEP, a w roku 1959 na Jubileuszowym Zjeździe z okazji 40-lecia SEP odznaczono go Krzyżem Oficerskim Orderu Odrodzenia Polski.

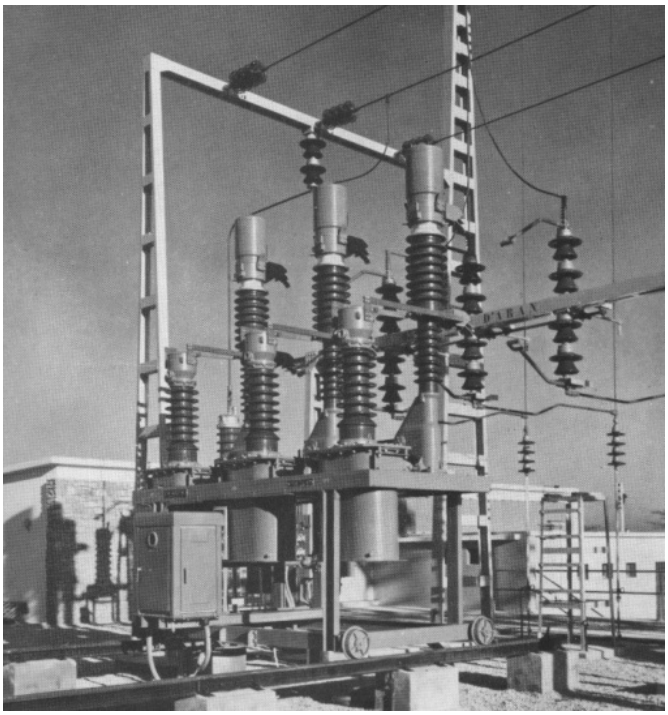
Kazimierz Szpotański zmarł 10 lipca 1966 r. w Warszawie i został pochowany na Starych Powązkach.

W 1969 r. na Zjeździe z okazji 50-lecia SEP Kazimierza Szpotańskiego uhonorowano pośmiertnie najwyższą godnością stowarzyszenia, nadając mu tytuł Członka Honorowego SEP, a w 1986 roku ustanowiono medal im. Kazimierza Szpotańskiego. W Międzylesiu jedną z ulic koło dawnej fabryki FAE nazwano jego imieniem.

Wyłącznik małoolejowy

Fabryka Aparatów Elektrycznych K. Szpotański i Spółka

Fabryka stała się kolebką rodzimych urządzeń elektroenergetycznych. Wytwarzano w niej m.in. łączniki wysokich, średnich i niskich napięć (wyłączniki małoolejowe, jeszcze gdzieniegdzie obecne), urządzenia do pomiarów elektrycznych (w tym użytkowane w całym kraju liczniki energii), aparaty do racjonalnej gospodarki ruchu oraz aparaty rentgenowskie. Kazimierz Szpotański mawiał, że wyroby jego zakładu muszą spełniać kryteria określone w JEEN-ach (skrótowiec powstały od pierwszych liter słów: „Jakość", „Estetyka", „Ekonomiczność" i „Nowoczesność"). Rynkowy sukces zawdzięczał też dużej otwartości na europejskie nowinki technologiczne (sztab inżynierów bacznie obserwował zagranicznych producentów wyrobów elektroenergetycznych) oraz własnemu laboratorium. Fabryka Aparatów Elektrycznych, jako jedna z nielicznych w Polsce międzywojennej, miała specjalne stanowisko projektanta formy ulokowane w Biurze Projektowo-Konstrukcyjnym. Można więc uznać Szpotańskiego za jednego z pionierów wzornictwa przemysłowego. Rzecz jasna, ogromną wagę przywiązywano do jakości. Jej kontrolę przeprowadzono zarówno na poszczególnych stanowiskach pracy (po zakończeniu kolejnych etapów produkcji), jak i po wykonaniu każdego egzemplarza. Taka „polityka jakości" skutkowała znikomą liczbą reklamacji. Jeśli takie się pojawiły, to rozpatrywano je od razu. Katalogi (na bieżąco aktualizowane) z dokładnymi opisami i parametrami technicznymi produktów zawierały pełne informacje o wyrobach FAE. Ponadto fabryka wydawała czasopismo „Informacja dla Przyjaciół FAE", zawierające wiadomości o produkcyjnych nowościach oraz praktyczne rady co do eksploatacji. Wyroby „od Szpotańskiego" często wystawiane były na krajowych i zagranicznych targach, gdzie zdobywały liczne nagrody. Ludzie cenili inż. Szpotańskiego nie tylko za trafność podejmowanych decyzji biznesowych, lecz także za swoisty styl zarządzania przedsiębiorstwem. Rzadko się bowiem zdarza, by fabrykę i zatrudnionych w niej ludzi traktować jak jedną wielką rodzinę. A u Szpotańskiego tak właśnie było - panowała atmosfera wzajemnego zaufania i życzliwości.



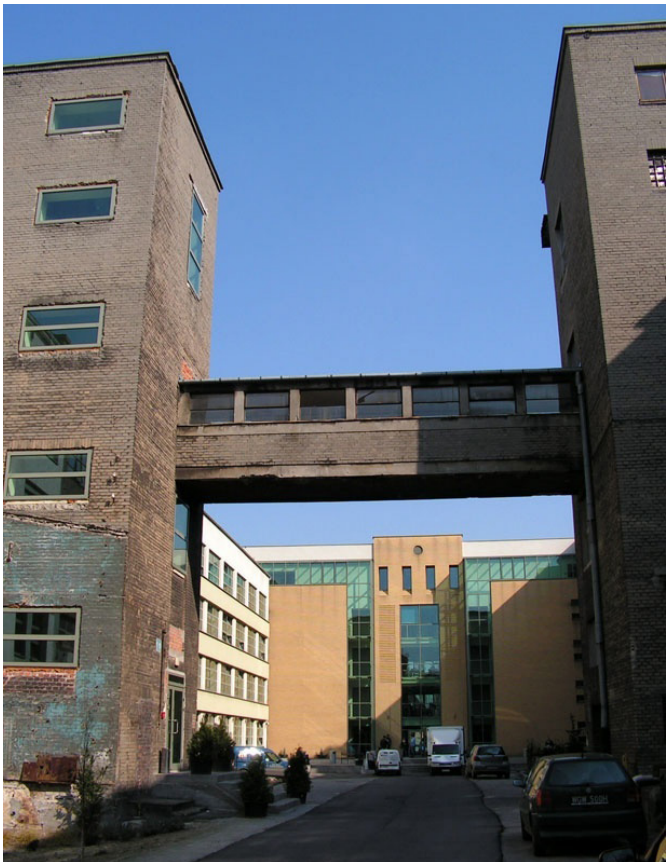
Warszawska fabryka liczników nie zaprzestała działalności nawet podczas okupacji niemieckiej, jednak 20 października 1944 roku została przejęta przez przymusowy zarząd tymczasowy. Gdy tylko zakończyła się okupacja hitlerowska, Kazimierz Szpotański przystąpił do odbudowy zakładu. Zniszczenia w Międzylesiu były niewielkie,

w dużo gorszym stanie znajdowały się obiekty przy ul. Kałuszyńskiej. Po II wojnie już nie FAE tylko ZWAR – Zakład Wytwórczy Aparatury Rozdzielczej – produkował głównie dla byłego ZSRR. W 1997 roku fabryka ZWAR została kupiona przez międzynarodową korporację ABB, w wyniku czego powstała spółka ABB ZWAR (kupiono 2 zakłady w Warszawie, Przasnyszu i Lęborku). Następnie zlikwidowano fabrykę przy ul. Gocławskiej, pozostałą część produkcji przeniesiono do Międzylesia. Działalność ABB ZWAR zawężono do biur konstrukcyjnych i śladowej produkcji, a ABB Przasnysz ograniczyło produkcję głównie do konstrukcji licencyjnych.

Obecnie na terenie fabryki na praskim Kamionku (produkowano tam m.in. liczniki elektryczne) znajduje się Uniwersytet Humanistycznospołeczny SWPS przy ulicy Chodakowskiej, siedziba SWPS mieści się w biurowcu i halach fabrycznych ZWAR.

W listopadzie 2018 roku w 100-lecie Niepodległości Polski i 100-lecie zakładów FAE odbyła się pierwsza konferencja poświęcona Kazimierzowi Szpotańskiemu – TRANSFORMATOR INNOWACYJNOŚCI. W spotkaniu uczestniczyło ok. 100 osób. Wśród nich emerytowani pracownicy ZWAR (Zakładów Wytwórczych Aparatury Wysokiego Napięcia), społeczność akademicka (pracownicy i studenci Uniwersytetu SWPS), lokalni przedsiębiorcy oraz przedstawiciele samorządu lokalnego. W specjalnie przygotowanych warsztatach uczestniczyły również dzieci. Dzięki życzliwości zmarłego niedawno Jacka Szpotańskiego i całej rodziny Szpotańskich historię FAE możemy poznawać także w Muzeum Warszawskiej Pragi.

Ciekawe, czy dzisiejsi studenci pierwszego prywatnego uniwersytetu w Polsce SWPS wiedzą, że w dawnych murach istniała wielka fabryka nie tylko polskiej, lecz także światowej myśli elektrotechnicznej?



SWPS

Sławomir Zieliński
Sektor Elektryki

Bibliografia

1. „Przegląd Elektrotechniczny”.
2. „SEP Kraków Biuletyn” nr 58.
3. Sobiesiak E., *Kazimierz Szpotański (1887-1966)*, [w:] Elektro-Info nr 12 (2013).
4. *Historia Elektryki Polskiej*, tom I, WNT (1976).

ORGANY TECHNICZNE
maj 2019

Komitety Techniczne

Zmiany zakresu tematycznego Komitetów Technicznych

- **KT 37 ds. Ryb i Przetworów Rybnych** rozszerzył zakres o CEN/TC 454 Algae and algae products
- **KT 235 ds. Analizy Żywności** rozszerzył zakres o CEN/TC 460 Food Authenticity

Nowi Przewodniczący Komitetów Technicznych

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

- w **KT 28 ds. Materiałów Ogniotrwałych dra inż. Jerzego Czechowskiego** reprezentującego Sieć Badawczą Łukasiewicz Instytut Ceramiki i Materiałów Budowlanych
- w **KT 56 ds. Maszyn Elektrycznych Wirujących oraz Narzędzi Ręcznych i Przenośnych o Napędzie Elektrycznym dra Konrada Dąbałę** reprezentującego Sieć Badawczą Łukasiewicz Instytut Elektrotechniki
- w **KT 74 ds. Aparatury Rozdzielczej i Sterowniczej Wysokonapięciowej mgra inż. Piotra Piekarskiego** reprezentującego ABB Sp. z o.o.
- w **KT 104 ds. Kompatybilności Elektromagnetycznej mgra inż. Władysława Moronia** reprezentującego Urząd Komunikacji Elektronicznej
- w **KT 138 ds. Kolejnictwa dra inż. Marka Pawlika** reprezentującego Stowarzyszenie na rzecz Interoperacyjności i Rozwoju Transportu Szynowego
- w **KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych dr inż. Elżbietę Andrukiewicz** reprezentującą Polskie Towarzystwo Informatyczne
- w **KT 191 ds. Chemii Gleby dr Bożenę Smreczak** reprezentującą Instytut Uprawy Nawożenia i Gleboznawstwa - Państwowy Instytut Badawczy
- w **KT 198 ds. Szkła mgra inż. Krzysztofa Skarbińskiego** reprezentującego Pilkington IGP Sp. z o.o.

Nowi Zastępcy Przewodniczącego Komitetów Technicznych

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

- w **KT 28 ds. Materiałów Ogniotrwałych dr inż. Katarzynę Stec** reprezentującą Sieć Badawczą Łukasiewicz Instytut Ceramiki i Materiałów Budowlanych

Nowi Sekretarze Komitetów Technicznych

W maju Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w **KT 274 ds. Betonu mgr inż. Małgorzatę Litwę** z Polskiego Komitetu Normalizacyjnego
- w **KT 316 ds. KT 316 ds. Ciepłownictwa i Ogrzewnictwa Jolantę Ryll** z Polskiego Komitetu Normalizacyjnego

Nowi członkowie Komitetów Technicznych

W maju Prezes PKN powołał na członków KT następujące podmioty:

- **AQUER Maciej Dyba, Jarosław Kram Spółka jawna do KT 278** ds. Wodociągów i Kanalizacji
- **ERICO Poland Sp. z o. o. do KT 244** ds. Sprzętu, Środków i Urządzeń Ratowniczo - Gaśniczych
- **GEOMECHANIKĘ Sp. z o. o. do KT 254** ds.Geotechniki
- **H+H Polska Sp. z o.o. do KT 179** ds. Ochrony Cieplnej Budynków i KT 252 ds. Projektowania Konstrukcji Murowych
- **H. CEGIELSKI - Fabrykę Pojazdów Szynowych Sp. z o. o. do KT 138** ds. Kolejnictwa
- **Instytut Techniki Górniczej KOMAG do KT 54** ds. Chemicznych Źródeł Prądu
- **Motorola Solutions Systems Polska Sp. z o. o. do KT 331** ds. Języków Programowania
- **NEWAG IP Management Sp. z o.o. do KT 138** ds. Kolejnictwa
- **NKT SA do KT 53** ds. Kabli i Przewodów
- **NOVOMATIC Technologies Poland S.A. do KT 331** ds. Języków Programowania
- **PRIM-IT Andrzej Niemiec do KT 171** ds. Sieci Komputerowych i Oprogramowania
- **Pałucką Drukarnię Opakowań Sp. z o. o. do KT 133** ds. Opakowań
- **SOLBET Kolbuszowa SA do KT 233** ds. Konstrukcji Murowanych
- **Sieć Badawczą Łukasiewicz - Instytut Włókiennictwa do KT 270** ds. Zarządzania Środowiskowego i **KT 276** ds. Zarządzania Bezpieczeństwem i Higieną Pracy
- **Techplast Sp. z o.o. do KT 130** ds. Aparatury Chemicznej, Zbiorników i Butli do Gazów
- **Trutek Fasteners Polska Sp. z o.o.do KT 236** ds. Części Złącznych i Narzędzi Montażowych
- **ULTRAFOG Sp. z o. o. do KT 244** ds. Sprzętu, Środków i Urządzeń Ratowniczo – Gaśniczych
- **Uniwersytet w Białymstoku do KT 288** ds. Multimediów

Odwołania członków Komitetów Technicznych

W maju Prezes PKN odwołał z członka KT:

- **CERAMIKĘ PILCH Sp. z o.o. Sp. k. z KT 197** ds. Płytek i Sanitarnych Wyrobów Ceramicznych
- **Hufgard Optolith Bauprodukte Polska Sp. z o. o. z KT 252** ds. Projektowania Konstrukcji Murowych
- **Uniwersytet w Białymstoku z KT 256** ds. Języka, Tłumaczeń i Terminologii
- **nkt cables Warszowice Sp. z o.o. z KT 53** ds. Kabli i Przewodów

Podkomitety Techniczne

W maju Prezes PKN powołał do pełnienia funkcji Sekretarza

- **BITUNOVA Sp. z o.o. do PK 2** ds. Asfaltów w KT 222 ds. Przetworów Naftowych i Cieczy Eksploatacyjnych

Dwudniowe szkolenie

Audit wewnętrzny wg znowelizowanej normy PN-EN ISO/IEC 17025:2018-02

Szkolenie skierowane jest do osób pracujących w systemie zarządzania, auditorów wewnętrznych, którzy będą oceniać wdrożenie systemu zarządzania i kompetencje techniczne według wymagań znowelizowanej normy PN-EN ISO/IEC 17025:2018-02.

Zagadnienia:

- Omówienie i interpretacja wymagań znowelizowanej normy PN-EN ISO/IEC 17025:2018-02
- Dokumentowanie systemu zarządzania wg znowelizowanej normy PN-EN ISO/IEC 17025:2018-02
- Dokumenty stanowiące kryteria auditu
- Ogólne wymagania dotyczące kompetencji laboratoriów
- Podejście procesowe, ocena ryzyk i szans
- Ocena wdrożenia nowych elementów
- Dokumentowanie auditów

Miejsce szkolenia:

Polski Komitet Normalizacyjny
ul. Świętokrzyska 14, Warszawa

Cena szkolenia:

690,00 zł netto; 848,70 zł brutto

Więcej szczegółów na stronie wiedza.pkn.pl

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

PKN
POLSKI KOMITET NORMALIZACYJNY