PARP
PFR Group

Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo

Kompetencje, edukacja i rynek pracy w sektorze telekomunikacja i cyberbezpieczeństwo – dziś i jutro

Kompetencje, edukacja i rynek pracy w sektorze telekomunikacja i cyberbezpieczeństwo – dziś i jutro

SPIS TREŚCI

Publikacja realizowana w ramach Projektu pn. „Utworzenie i funkcjonowanie Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo”.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza, Edukacja, Rozwój.

Koncepcja merytoryczna: Dariusz Chełstowski, Tomasz Klekowski, Beata Ostrowska, Adam Sanocki, Maciej Wnuk, Irmina Zakrzewska

Redaktor: Anna Wojda

Korekta: Maria Węcowska

Skład: Igor Nowak

ISBN 978-83-967447-3-9

Warszawa 2023

WSTĘP

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo (SRTCB) w ciągu ostatnich ponad trzech lat podejmowała liczne aktywności. To konferencje, webinaria, ale też przygotowanie ważnych wskazówek i rekomendacji dla biznesu i edukacji. Jak bardzo potrzebne są działania Rady, pokazują wypowiedzi osób, które zostały do niej zaproszone. W wielu przypadkach po początkowym zdziwieniu spektrum aktywności Rady i jej członków, przeradzało się w prawdziwą fascynację.

Jest wiele korzyści ze współpracy: poza podnoszeniem kwalifikacji to także kreowanie przestrzeni do wymiany doświadczeń

Zainteresowanie działalnością Rady nie powinno dziwić. Prowadzi ona wiele badań i analiz, by potem przygotować ciekawe raporty. Dzięki temu możliwe jest poznanie potrzeb biznesu i zidentyfikowanie koniecznych kompetencji w sektorach informatycznym i telekomunikacyjnym. Dzięki temu Rada ułatwia współpracę biznesu i edukacji, podejmuje działania włączające przedstawicieli sektora do współpracy, monitoruje zmiany na rynku pracy. Pozwoliło to choćby na szybkie zarekomendowanie potrzeb kompetencyjnych w związku z pandemią COVID-19.

Duża część działalności Rady dotyczy również edukacji. Dzięki jej działalności możliwe było dopasowanie programów nauczania do potrzebnych kompetencji czy zauważenie, że potrzebne są nowe kierunki studiów. Nie tylko zresztą nowe kierunki, ale przede wszystkim zmiana sposobu myślenia o kształceniu: pokazanie studentom, gdzie w praktyce mogą się przydać umiejętności, które zdobyli na uczelni.

W branżach telekomunikacja i cyberbezpieczeństwo pojawia się coraz więcej nie tylko nowych zagrożeń, ale również nowych regulacji prawnych, a co za tym idzie – coraz więcej nowych obowiązków. Kształcenie z tych dziedzin zdaje się zyskiwać coraz większe znaczenie. Ignorowanie zagrożeń nie sprawi, że one znikną. Dlatego właśnie doświadczenie i kompetencje Rady mogą być – zwłaszcza tu – niezwykle przydatne w najbliższym czasie.

Rada ma jeszcze dużo do zrobienia i do zaoferowania. Upowszechnianie wiedzy o możliwościach rozwoju i podnoszenia poziomu kompetencji, umożliwienie wymiany doświadczeń przedstawicieli biznesu, edukacji i administracji publicznej oraz współpraca z rynkiem pracodawców i pracowników sektora – to zadania dla Rady na kolejne lata. Pozwólmy jej działać. Będzie to z korzyścią dla nas wszystkich: przedsiębiorców, szeroko rozumianej edukacji, pracowników, ale i – w szerszym ujęciu – całej polskiej gospodarki.

RADA TO CAŁE SPEKTRUM ZADAŃ

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo może się pochwalić licznymi efektami swojej działalności. To nie tylko raporty, webinaria czy podcasty, lecz także konkretne wskazówki ważne i dla edukacji, i dla biznesu.

Adam Sanocki
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne

Rynek pracy stale ewoluuje. To efekt zmieniającej się sytuacji gospodarczej i stałego rozwoju przedsiębiorstw. Nie pozostaje to bez wpływu na kompetencje pracowników, jakich oczekują potencjalni pracodawcy. Z badań Polskiej Agencji Rozwoju Przedsiębiorczości wynika, że choć ponad 50 proc. Polaków posiada wyższe wykształcenie, większość przedsiębiorców wciąż ma trudności z pozyskaniem kandydatów, którzy posiadaliby oczekiwane kwalifikacje. Dlatego tak ważne jest istnienie odpowiednich systemów i narzędzi wspierających współpracę jednostek naukowych z przedsiębiorcami. Pozwala to na bieżące badanie i definiowanie potrzeb poszczególnych sektorów gospodarki i dostosowywanie do nich systemu kształcenia. Niebagatelną rolę odgrywają tu Sektorowe Rady ds. Kompetencji.

Na zdjęciu (od lewej): Beata Ostrowska, Wiesław Paluszyński i Andrzej Dulka podczas jednego z posiedzeń Rady

Telekomunikacja i cyberbezpieczeństwo

Sektorowe rady ds. kompetencji powstały w związku z pogłębiającymi się problemami z pozyskiwaniem odpowiednio wykwalifikowanej kadry. Chodziło również o zmniejszenie luki kompetencyjnej poprzez kształcenie i merytoryczne przygotowanie pracowników już obecnych na rynku, a także tych, którzy dopiero będą na rynek wchodzić.

Pierwsze sektorowe rady powstały w 2016 r. Obecnie jest ich siedemnaście, w takich sektorach jak: moda i innowacyjne tekstylia; nowoczesne usługi biznesowe; opieka zdrowotna i pomoc społeczna; handel; budownictwo; usługi rozwojowe; komunikacja marketingowa; przemysł lotniczo-kosmiczny; przemysł chemiczny; finanse; turystyka; odzysk materiałowy surowców; informatyka; rekultywacja i gospodarka wodno-ściekowa; żywność wysokiej jakości; motoryzacja i elektromobilność oraz telekomunikacja i cyberbezpieczeństwo.

Nad pracami rad sektorowych czuwa Rada Programowa złożona z przedstawicieli ministerstw właściwych do spraw rozwoju, edukacji, szkolnictwa wyższego, pracy, przedstawicieli sektora edukacji formalnej i pozaformalnej, a także organizacji przedsiębiorców oraz partnerów społecznych i gospodarczych. Każda rada sektorowa to oddolna inicjatywa branży, tworzona przez osoby oraz instytucje wprost związane z daną branżą, zaczynając od przedsiębiorców, poprzez różne organizacje, na przedstawicielach świata nauki kończąc.

Zadania i inicjatywy

Do podstawowych zadań wszystkich działających rad sektorowych należy przede wszystkim inicjowanie współpracy przedsiębiorców z uczelniami, pozyskiwanie wiedzy od przedsiębiorców na temat potrzeb kwalifikacyjno-zawodowych występujących na rynku pracy w danym sektorze gospodarki, upowszechnianie informacji na temat tych potrzeb, a także formułowanie rekomendacji w zakresie dostosowania kadr do aktualnych potrzeb przedsiębiorców. W zależności od branży, trendów oraz wyzwań, z jakimi dany sektor gospodarki musi się mierzyć, różni się także zakres działalności oraz inicjatywy podejmowane przez poszczególne rady.

Dobrze rozbudowana infrastruktura telekomunikacyjna ma wpływ na transformację cyfrową całej gospodarki, a to jedno z ważniejszych wyzwań dla branży

Sektor telekomunikacji i cyberbezpieczeństwa (TCB) ma kluczowe znaczenie dla funkcjonowania całego państwa i gospodarki. Nowoczesna, stabilna i odpowiednio zabezpieczona infrastruktura telekomunikacyjna zapewnia nieprzerwane i efektywne funkcjonowanie struktur państwa oraz możliwość prowadzenia biznesu. Sieci telekomunikacyjne stały się głównym medium wymiany informacji. Dobrze rozbudowana infrastruktura telekomunikacyjna ma wpływ na transformację cyfrową całej gospodarki, a to jest jednym z ważniejszych wyzwań, przed jakimi stoi branża.

Do sektora telekomunikacji zalicza się m.in. działalność w zakresie telekomunikacji przewodowej, bezprzewodowej, satelitarnej oraz wszelkie aktywności związane z zapewnieniem cyberbezpieczeństwa. Specyfiką sektora

telekomunikacji i cyberbezpieczeństwa jest ścisły związek z technologią informacyjno--komunikacyjną. Sektor ten cechuje się wysoką podatnością na czynniki ekonomiczne, które mają wpływ na kształtowanie rynku usług zarówno w grupie dostawców, jak i odbiorców. Jego funkcjonowanie jest determinowane ogólną sytuacją gospodarczą i silnie powiązane z potencjałem inwestycyjnym przedsiębiorstw. W ostatnich kilkunastu latach obserwujemy ogromny postęp technologiczny, który miał wpływ na dynamiczne zmiany na rynku pracy w tym sektorze, zwłaszcza gdy chodzi o zapotrzebowanie na określone kwalifikacje i kompetencje. W obliczu pandemii COVID-19, trwającego ciągle kryzysu gospodarczego i społecznego, a także wojny w Ukrainie, obserwujemy niezmiennie ważną rolę sektora TCB m.in. w zapobieganiu wzrostom bezrobocia. Wszystko dzięki ułatwianiu zdalnego dostępu do przeróżnych zasobów, a co za tym idzie – umożliwieniu większości pracowników wykonywania ich obowiązków zawodowych.

Edukacja i kadry

Sektorową Radę ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo (SRTCB) powołano 12 lutego 2020 roku na podstawie art. 4c i 4e Ustawy z 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości. Współfinansowana jest ze środków Unii Europejskiej w ramach Programu Operacyjnego Wiedza Edukacja Rozwój. Projekt realizowany jest wspólnie przez Polskie Towarzystwo Informatyczne oraz Polską Izbę Informatyki i Telekomunikacji.

Do zadań Sektorowej Rady ds. Kompetencji Teleinformatyka i Cyberbezpieczeństwo należy przede wszystkim zapewnienie przepływu informacji o zapotrzebowaniu na kompetencje między kadrami sektora TCB a szeroko rozumianym HR, instytucjami edukacyjnymi, rynkiem pracy, w tym agencjami zatrudnienia oraz wojewódzkimi i powiatowymi urzędami pracy. Wpływa to w dużym stopniu na wzrost skuteczności działań z zakresu pośrednictwa pracy i poradnictwa zawodowego.

Rada ma doprowadzić do transferu najlepszych w tym obszarze praktyk programów kształcenia, specjalizacji oraz zapotrzebowania na poszczególne grupy specjalistów TCB. Jej celem jest dostosowanie procesów edukacyjnych do potrzeb i problemów kadrowo-zawodowych, a działania ukierunkowane są głównie na kompleksową identyfikację i prognozowanie potrzeb kwalifikacyjno-zawodowych sektora TCB w Polsce. W tym celu Rada nawiązała w 2020 roku współpracę z Akademią Leona Koźmińskiego. Chodziło o przygotowanie w ramach partnerstwa programu i organizacji nowego kierunku studiów podyplomowych w zakresie zarządzania cyberbezpieczeństwem. Głównym celem studiów było przekazanie praktycznej wiedzy ze wspomnianego zakresu w organizacjach z sektora publicznego i prywatnego. Podjęta współpraca wiąże się ściśle ze współpracą rad z sektorem edukacji w zakresie dostarczania nowych kompetencji i kwalifikacji osobom zainteresowanym pracą w tej dziedzinie.

Działania Rady skupiają się także na osiągnięciu innego celu – PO WER, Programu Operacyjnego Wiedza Edukacja Rozwój. Ma on poprawić politykę i działania publiczne na rzecz rynku pracy, edukacji i całej gospodarki. Dzięki dotacjom unijnym jest szansa wzmocnienia szkolnictwa wyższego w takich aspektach, jak potrzeba rozwoju, promocja innowacji społecznych i współpraca ponadnarodowa. Rada określa obszary badawcze i inicjuje badania kompetencji pracowników sektora, gromadzi i przekazuje informacje o potrzebach sektora TCB partnerom społecznym, rekomenduje rozwiązania i zmiany systemowe oraz legislacyjne w obszarze edukacji i wskazuje konieczność jej dostosowania do potrzeb rynku pracy, w tym zmiany sektorowych ram kwalifikacji.

Kto za tym stoi

W skład Sektorowej Rady wchodzą przedstawiciele najważniejszych organizacji z sektora TCB (czyli telekomunikacja i cyberbezpieczeństwo), przedstawiciele firm oraz środowiska edukacyjnego.

Prezydium Rady tworzy ośmiu członków: przewodniczący Rady Wiesław Paluszyński (Polska Izba Informatyki i Telekomunikacji) oraz wiceprzewodniczący – Tomasz Chomicki (Samsung Electronics Polska Sp. z o.o.), Paweł Kostkiewicz (NASK – Państwowy Instytut Badawczy, nadzorowany przez Kancelarię Prezesa Rady Ministrów), Wojciech Maciejczak (Orange Polska S.A.), Beata Ostrowska (Wojewódzka Rada Rynku Pracy w Łodzi, BROst Centrum Edukacji i Technologii Komputerowej), Jarosław Pazgrat (MCX Pro), Magdalena Polak (Zespół Szkół Licealnych i Technicznych nr 1) oraz Grażyna Szpor (Uniwersytet Kardynała Stefana Wyszyńskiego). Prezydium koordynuje całokształt prac Rady i podejmuje kluczowe decyzje w zakresie uprawnień regulaminowych Rady.

> **Do podstawowych obowiązków sektorowej rady należy udział jej członków w cyklicznych posiedzeniach plenarnych**

Dodatkowo w ramach Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo utworzone zostały merytoryczne Komitety Rady. Realizują one jej cele i zadania w zakresie analiz i badań luk kompetencyjnych, systemu edukacji i kształcenia, rozwiązań legislacyjnych, rozwoju i certyfikacji kompetencji branżowych. Obecnie komitetom przewodniczą: Beata Ostrowska, Grażyna Szpor, Sławomir Smugowski, Jarosław Pazgrat, Bogusław Dębski.

Do podstawowych obowiązków Sektorowej Rady należy udział jej członków w posiedzeniach plenarnych. Są one organizowane cyklicznie od 2020 roku. Jak te spotkania przebiegają, można się dowiedzieć ze sprawozdań z posiedzeń publikowanych na stronie https://srtcb.radasektorowa.pl/o-radzie/sprawozdania.

Raporty i badania

Rada to także działalność badawcza i analityczna. W ramach tej działalności publikowane są raporty oraz opracowywane formalne rekomendacje rozwojowe, będące praktyczną wskazówką do wykonywanych na szeroką skalę działań rozwojowych. Działania badawczo-analityczne skupiają się na ocenie aktualnej sytuacji gospodarczej, która przekłada się na funkcjonowanie całego sektora. Zdarzeniem, które miało bardzo duży wpływ i na gospodarkę, i na branżę, była pandemia COVID-19 oraz wprowadzony w Polsce lockdown. Zaowocowało to dwiema edycjami raportu pt. „Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa" wypracowanego wspólnie przez Sektorową Radę ds. Kompetencji – Informatyka oraz Sektorową Radę ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo. Efektem prac są również zbiorcze wyniki z badania w 2021 i 2022 roku dotyczące działań antyCOVIDowych w sektorach: informatyka oraz telekomunikacja i cyberbezpieczeństwo. Pandemia wywołała nieodwracalne zmiany. Mają one wpływ na życie, zdrowie i zachowania społeczeństwa. Rządzący na całym świecie musieli dokonywać wielu zmian w ustawodawstwie, były one często nagłe i restrykcyjne. Skutki wielu

z nich są odczuwalne do dziś. Dla licznych sektorów gospodarki pandemia poskutkowała kryzysem. Firmy powoli wracają na właściwe tory i ich biznesy zaczynają działać jak dawniej. Niezaprzeczalnie jednak pandemia była wyzwaniem nie tylko dla firm, lecz także dla sektorów IT oraz telekomunikacji i cyberbezpieczeństwa. Wszyscy musieli sprostać niespotykanemu wcześniej zapotrzebowaniu na usługi.

W II edycji badania największą reprezentację firm miały przedsiębiorstwa z sektora telekomunikacji i cyberbezpieczeństwa (TCB), które prowadzą działalność w zakresie komunikacji przewodowej (26 proc.) oraz firmy z sektora informatyki (IT) zajmujące się oprogramowaniem, doradztwem w zakresie informatyki i pozostałą działalnością usługową w zakresie technologii informatycznych i komputerowych (25 proc.). W badaniu wskazano m.in. zakres kompetencji mających największe znaczenie dla sektora, jak: tworzenie, rozwój i zarządzanie oprogramowaniem oraz integracją systemów, zarządzanie zasobami własnymi, jak również utrzymanie i rozwój infrastruktury ICT. Z drugiej edycji badania wynika, że w najbliższym czasie najważniejszymi kompetencjami będą: utrzymanie i rozwój infrastruktury ICT, zapewnienie bezpieczeństwa kanałów komunikacji elektronicznej oraz zarządzanie zasobami danych. Najnowsza edycja raportu dostępna jest na stronie internetowej: https://srtcb.radasektorowa.pl/publikacje-raporty/raporty/454-raport-potrzeby-kompetencyjne-w-kontekscie-skutkow-pandemii-koronawirusa-edycja-ii.

Moc warsztatów, uchwał i rekomendacji

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo w latach 2020 i 2021 roku przeprowadziła cykl ośmiu warsztatów. Ich celem było opracowanie dobrych praktyk, idealnego modelu współpracy między biznesem, instytucjami akademickimi oraz administracją i określenie ekosystemu pozyskania informacji o tych potrzebach kompetencyjnych na rynku. Warsztaty są tworzone wspólnie przez organizacje i firmy, które są również członkami SRTCB, co pozwala realnie określić potrzeby rynku.

Na zdjęciu (od lewej): Tomasz Kulisiewicz, Beata Ostrowska, Wiesław Paluszyński i Andrzej Dulka podczas jednego z posiedzeń Rady

W 2020 roku przeprowadzono cztery warsztaty. Temat potrzebnych na rynku kompetencji pojawił się już podczas pierwszego warsztatu pt. „Ekosystem Kompetencyjny i potrzeby biznesu w kształceniu przyszłych kadr dla branży TCB". W czasie tego warsztatu wypracowano wstępną listę ponad 100 kompetencji (twardych, miękkich oraz transferowalnych). By dopracować szczegółowo wyniki warsztatów, wśród przedsiębiorców oraz ekspertów rynkowych zostało przeprowadzone badanie. Jego celem było wskazanie kluczowych kompetencji w branży TCB, a także wstępne określenie jakościowo-ilościowych potrzeb kompetencyjnych oraz uchwycenie tendencji na rynku pracy w tym sektorze.

Badanie pozwoliło zidentyfikować kompetencje, których poszukują działający w branży przedsiębiorcy. Udało się też oszacować zapotrzebowanie na kwalifikacje w sektorze TCB w dłuższej perspektywie czasu (trzy do pięciu lat).

Podczas panelu dyskusyjnego na EduMixer 2022 (od lewej): Małgorzata Ganczar, Maciej Rogalski, Piotr Grzybowski, Marcin Wysocki

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo podejmuje również uchwały, publikuje rekomendacje SRTCB. Jedna z pierwszych rekomendacji, opracowana na podstawie analiz sektora telekomunikacja i cyberbezpieczeństwo, zalecała udzielanie wsparcia szkoleniowo-doradczego w ramach Działania 2.21 PO WER. Ideą jest dopasowanie kompetencji do zdiagnozowanych potrzeb sektora – poprzez realizację usług rozwojowych wspierających zdobycie, uzupełnienie lub aktualizację kompetencji, których szczegółowy zakres jest określony w rekomendacji nr 2/2020 Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

Bardzo ważna jest też rekomendacja dotycząca utworzenia/aktualizacji sektorowej ramy kwalifikacji przyjętych uchwałą Rady nr 15e/SRTCB/2021 z 16 grudnia 2021 r. na podstawie przeprowadzonych analiz aktualnej Sektorowej Ramy Kwalifikacji dla Sektora Telekomunikacji (SRK Tele) oraz wniosków wypracowanych w toku prac eksperckich. SRK Tele opisuje kwalifikacje w branży telekomunikacyjnej, pomaga również w stworzeniu nowoczesnych, przejrzystych i porównywalnych form kształcenia oraz walidacji i certyfikacji kwalifikacji w branży telekomunikacyjnej. Szczegóły dotyczące rekomendacji znajdują się na stronie internetowej: https://srtcb.radasektorowa.pl/publikacje-raporty/rekomendacje-rady-przeglad.

Kwalifikacje

Do zadań sektorowych rad ds. kompetencji należy również inicjowanie przeglądu włączonych kwalifikacji rynkowych oraz wnioskowanie o przywrócenie kwalifikacji archiwalnej statusu kwalifikacji funkcjonującej. Inicjatywy takie trafiają do Zintegrowanego Systemu Kwalifikacji (ZSK), czyli systemu będącego zbiorem rozwiązań, których celem jest integracja polskiego systemu kształcenia.

W 2022 roku Rady Sektorowe przy Polskim Towarzystwie Informatycznym, w tym także Rada Sektorowa ds. kompetencji Telekomunikacja i Cyberbezpieczeństwo, opracowały pięć wniosków o włączenie kwalifikacji rynkowych do ZSK. Pod koniec poprzedniego roku minister cyfryzacji rozpoczął procedurę włączania kwalifikacji rynkowych do systemu, obecnie wnioski są na etapie konsultacji środowiskowych.

Zaproponowane przez Rady Sektorowe kwalifikacje obejmują przede wszystkim zarządzanie usługami chmurowymi w organizacji, czyli m.in. wdrażanie rozwiązań chmurowych zgodnie z projektem,

w tym np. zamawianie usług chmurowych czy ich konfigurowanie, a także kwalifikacje dotyczące zapewniania cyberbezpieczeństwa takich rozwiązań. Osoby z odpowiednimi kwalifikacjami identyfikują wynikające z regulacji prawnych specyfiki działalności oraz wymagania w zakresie bezpieczeństwa, jakim muszą odpowiadać wykorzystywane rozwiązania chmurowe. W zakresie usług chmurowych kwalifikacja opracowana przez Rady Sektorowe dotyczy samego projektowania takich usług w organizacji, co ma pozwolić odpowiednio opracować koncepcje usług z uwzględnieniem potrzeb danej organizacji.

Kolejna kwalifikacja dotyczy obsługi incydentów w obszarze cyberbezpieczeństwa. Sprowadza się ona do tego, by wykwalifikowane osoby wykonywały zadania związane z obsługą zdarzeń będących incydentami naruszającymi cyberbezpieczeństwo i rozpoznawały takie zdarzenia. Ostatnia kwalifikacja dotyczy pozyskiwania, przetwarzania i wykorzystywania otwartych danych publicznych. Odpowiednia analiza pozwoli na ocenę przydatności na rynku pracy.

Skutki wojny

Działania Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo skierowane zostały także na jedno z najważniejszych wydarzeń polityczno-społeczno-gospodarczych na świecie, tj. wojnę w Ukrainie. Zadaniem sektorowych rad jest analizowanie takich wydarzeń, jak wojna za naszą wschodnią granicą. Jej wpływ na sytuację gospodarczą w Polsce jest ogromny, jeszcze większy jednak na polski rynek pracy.

W 2022 roku powstały dwie opinie wspólnych roboczych zespołów ekspertów Sektorowej Rady ds. Kompetencji – Informatyka i Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo w sprawie sytuacji na rynku pracy w związku z wydarzeniami w Ukrainie oraz w sprawie działań na rzecz wsparcia uchodźców z Ukrainy lub przedsiębiorców odczuwających skutki wojny w Ukrainie.

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo wydała nadzwyczajną rekomendację i dwie opinie

Pierwsza przedstawiona opinia w dużej mierze skupiała się na specyfice poszczególnych sektorów, ponieważ zupełnie inaczej konsekwencje wojny w Ukrainie odczuwa sektor budownictwa czy logistyki, a inaczej branża ICT. W opinii wskazano na potencjalne zagrożenia związane z aktualną sytuacją w Ukrainie, chociażby w zakresie polskich firm, które korzystały z usług specjalistów (np. programistów) mieszkających w Ukrainie, wykonujących pracę dla polskich przedsiębiorstw w formie zdalnej. Zwrócono także uwagę na możliwość wykorzystania potencjału kadry specjalistów ICT z Ukrainy, jednak w tym zakresie problemem mogą być ustawowe wymogi posiadania w wielu sytuacjach poświadczenia bezpieczeństwa. Pojawiają się też oddolne inicjatywy środowiskowe służące wspieraniu uchodźców czy osób pozostających w Ukrainie (np. TechForUkraine, Startupy dla Ukrainy itp.). Przy okazji publikowanej opinii zwrócono uwagę na konieczność podniesienia świadomości cyberzagrożeń we wszystkich

sektorach gospodarki i zapewnienie ochrony przed nimi w związku z nasilającymi się atakami cybernetycznymi. Cała opinia dostępna jest na stronie SRTCB.

W drugiej opinii sektorowe rady podtrzymały stanowisko wyrażone w pierwszym dokumencie, a mianowicie, że podstawowym i najważniejszym problemem w planowaniu racjonalnych działań skierowanych do uchodźców z Ukrainy jest brak wiarygodnych, miarodajnych informacji na temat potencjału zawodowego osób przybywających do Polski. Dlatego konieczne jest przeprowadzenie badań sektorowych oraz zapewnienie dostępu do informacji na ten temat.

Ważny cel: komunikacja

Kolejnym aspektem działalności Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo jest aktywne komunikowanie się ze społeczeństwem oraz uczestnikami rynku sektora TCB. Dotyczy to przede wszystkim edukacji w zakresie funkcjonowania rynku oraz istotnych aspektów związanych z tym obszarem nie tylko w kontekście kompetencji pracowników, lecz także zagadnień związanych z cyfrową transformacją, cyberbezpieczeństwem w sieci w zakresie budowania nowoczesnego i bezpiecznego społeczeństwa cyfrowego. Powstaje platforma do dyskusji na temat potrzeb, możliwości, szans oraz wyzwań, jakie mogą się pojawić w kolejnych latach.

Przedstawiciele Sektorowej Rady organizują i biorą czynny udział w konferencjach, webinariach czy debatach branżowych, komunikując w ten sposób potrzeby rynku i jego przedstawicieli. Jednym z takich wydarzeń jest Forum Współpracy Edukacji z Biznesem – EduMixer – organizowane przez Polską Izbę Informatyki i Telekomunikacji (PIIT) we współpracy z Polskim Towarzystwem Informatycznym (PTI) w ramach dwóch rad sektorowych: Sektorowej Rady ds. Kompetencji – Informatyka oraz Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

Celem konferencji jest wypracowanie propozycji zmian w programach kształcenia uwzględniających rozwój technologiczny oraz potrzeby dynamicznego rynku pracy, wymiana doświadczeń i transfer praktyk między sektorem edukacji, przedsiębiorcami i instytucjami. Ważna jest także poprawa współpracy i zbudowanie partnerstwa między podmiotami kształtującymi rynek pracy, a to będzie możliwe dzięki identyfikacji potrzeb kompetencyjnych poszczególnych grup specjalistów z obszarów informatyki, telekomunikacji i cyberbezpieczeństwa.

Działania Sektorowej Rady zostały skierowane na jedno z najważniejszych wydarzeń, tj. wojnę w Ukrainie

Pierwsza konferencja zorganizowana została w 2017 roku, zaś ubiegłoroczna była szóstą edycją EduMixera. Jej tematem przewodnim było „Bezpieczeństwo w teleinformatyce. Wyzwanie dla edukacji, rynku pracy i przedsiębiorców”.

Porozmawiajmy na forum

Kolejną inicjatywą, skierowaną wprost do przedstawicieli sektora, jest Forum Teleinformatyki, które w 2022 roku

miało swoją XXVIII edycję. Wydarzenie organizowali BizTech Konsulting SA i Polska Izba Informatyki i Telekomunikacji. Forum gromadzi najlepszych specjalistów i praktyków aktywnie zaangażowanych w modernizację funkcjonowania państwa, umożliwiając publiczną wymianę doświadczeń i poglądów poprzez czynny udział w dyskusjach panelowych czy rozmowach kuluarowych.

W ramach sesji i paneli eksperckich omawiane są pożądane kierunki rozwoju systemu informacyjnego państwa, m.in. zagadnienia związane z: koniecznością redefinicji zagrożeń w obszarze bezpieczeństwa informacyjnego (cyberbezpieczeństwa), potrzebą pełniejszego wykorzystania metod i narzędzi sztucznej inteligencji, niezbędną identyfikacją barier połączoną z poszukiwaniem innowacyjnych sposobów wspierania eksportu polskich rozwiązań informatycznych.

Informując o aktywności Rady, warto wspomnieć o webinarium pt. „Cyberzagrożenia – czego boją się Polacy?", które odbyło się w lipcu ubiegłego roku. Podczas spotkania poruszane były kwestie związane m.in. z wyciekiem danych osobowych, atakiem hakerskim czy wyłudzeniami danych, czyli problemami cyberprzestępstw, z którymi może się mierzyć w swoim życiu każdy z nas.

W obszarze działalności komunikacyjnej Rady warto wskazać również filmy informacyjne. Przedstawiają one zadania i kompetencje rady, a także prowadzone i inicjowane badania rynku. Ciekawą inicjatywą jest cykl podcastów pt. „Wyzwania dla edukacji i rynku pracy w dobie transformacji cyfrowej". Pokazują one najciekawsze wyzwania i trendy związane z rozwojem kompetencji i rynku pracy w obszarze telekomunikacja i cyberbezpieczeństwo oraz IT. Punktem wyjścia do dyskusji jest kwestia transformacji cyfrowej i wyzwań, jakie stoją przed przedsiębiorstwami czy sektorem edukacji wobec dynamicznej rzeczywistości społecznej i biznesowej, szczególnie po pandemii SARS-CoV-2. Więcej informacji na stronie podcastów: https://anchor.fm/radasektorowa.

Rada jest ciągle potrzebna

Należy zdać sobie sprawę, że odczuwalne do tej pory skutki pandemii COVID-19, a także trwająca wojna w Ukrainie mają ogromny wpływ na funkcjonowanie i rozwój poszczególnych sektorów gospodarki. Branża ICT w Polsce należy do najbardziej dynamicznych sektorów. Jej stały rozwój, ale także nowe wyzwania i niebezpieczeństwa związane z cyberzagrożeniami, przekładają się bezpośrednio na duże zapotrzebowanie na wyspecjalizowane kadry. Sektorowe Rady ds. kompetencji w obszarze ICT, w tym właśnie Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo pełniły, pełnią i nadal mogą odgrywać ważną rolę, rekomendując kierunki kształcenia kadr i umożliwiając pracownikom zdobycie niezbędnych kwalifikacji i kompetencji, przyczyniając się tym samym do rozwoju krajowej gospodarki.

Na zdjęciu (od lewej): Arwid Mednis, Grażyna Szpor, Maciej Rogalski, Sławomir Kumka i Wiesław Paluszyński podczas panelu na 28. Forum Teleinformatyki 2022

CZŁONKOWIE RADY O RADZIE

WIESŁAW PALUSZYŃSKI

Przewodniczący Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, prezes Polskiego Towarzystwa Informatycznego

Rada jest potrzebna; widać to przez pryzmat jej zainteresowań i tego, co robi

Efekty pracy Rady są widoczne

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo skończyła trzy lata. Taki mały jubileusz. Jeśli środki unijne pozwolą przedłużyć kontrakt, będziemy działali w kolejnych latach. Rada jest potrzebna. Widać to przez pryzmat jej zainteresowań i tego, co robi. Najciekawszym efektem, który zostanie po trzech latach, będzie opracowanie nowych kompetencji zgłoszonych do Zintegrowanego Systemu Kwalifikacji właśnie w obszarze cyberbezpieczeństwa, dopasowanie programów nauczania do tych kompetencji, uruchomienie kursów i egzaminów. Słabością naszego systemu, przynajmniej do tej pory, jest opieranie się na certyfikatach kwalifikacji międzynarodowych, głównie amerykańskich. Tymczasem niezbędne są polskie i Rada włożyła wiele wysiłku w to, by polskie kwalifikacje powstały. Co dalej, zobaczymy. Nasze działanie jest potrzebne, nie zmógł nas COVID, pracowaliśmy zdalnie i wszyscy w tym czasie byli zaangażowani. Mam nadzieję, że skończą się w tym roku prace nad ustawą o cyberbezpieczeństwie i że dzięki temu kwalifikacje, które wypracowaliśmy, będą oparte na solidnych podstawach prawnych.

Spektrum działania Rady jest bardzo szerokie, to m.in. identyfikacja potrzeb przedsiębiorców z sektora

BEATA OSTROWSKA

Wiceprzewodnicząca Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, wiceprezes Polskiego Towarzystwa Informatycznego

Ważny element: komunikacja

Rady sektorowe prowadzą wiele działań, których celem jest nawiązanie współpracy między edukacją i biznesem. Aby jednak wiedzieć, jakie są potrzeby biznesu, prowadzimy badania i analizy oraz przygotowujemy raporty z tych badań. Pokazują one, jakie są potrzeby kompetencyjne w sektorach: zarówno informatycznym, jak i telekomunikacyjnym. Badania wykorzystujemy do tego, by przygotować rekomendacje potrzeb kompetencyjnych dla sektora. Szkolenia z obszarów rekomendowanych przez rady sektorowe są realizowane przez operatorów.

Ważnym elementem w działaniach Rady jest komunikacja. Wykorzystujemy do tego wiele kanałów informacyjnych, jak YouTube, Facebook czy Linkedin – po to, by komunikować i informować o działaniach Rady i zapraszać na wydarzenia realizowane przez Radę. Spektrum działania Rady jest bardzo szerokie. Identyfikacja potrzeb przedsiębiorców z sektora, ułatwianie współpracy edukacji i biznesu, integrowanie interesariuszy sektora, działania włączające przedstawicieli sektora do współpracy, organizowanie warsztatów, debat eksperckich, seminariów, webinariów, konferencji, prace eksperckich zespołów roboczych, udział w konsultacjach publicznych, włączanie się jako partner merytoryczny w wiele wydarzeń, informowanie interesariuszy sektora o działaniach rady i wydarzeniach związanych z sektorem, opiniowanie wniosków o włączenie kwalifikacji do ZSK, opiniowanie programów studiów, bieżące monitorowanie zmian na rynku pracy – co pozwoliło na szybką rekomendację potrzeb kompetencyjnych w związku z pandemią COVID-19, współpraca z Ministerstwem Edukacji i Nauki w zakresie wypracowywania rekomendacji dotyczącej zmian w podstawach programowych szkół branżowych oraz tworzenia nowych kierunków kształcenia, prowadzenie działań upowszechniających wiedzę o możliwościach rozwoju i podnoszenia poziomu kompetencji, prowadzenie własnych badań identyfikujących potrzeby sektora, luki kompetencyjne.

Działalność Rady powinna być kontynuowana, by mogła dbać o aktualność programów kształcenia i dostępność odpowiednich kompetencji

WOJCIECH MACIEJCZAK

Dyrektor bezpieczeństwa regulacyjnego Orange Polska SA, członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Platforma wymiany wiedzy i doświadczeń

W mojej codziennej pracy u operatora telekomunikacyjnego zajmuję się zagadnieniami związanymi z bezpieczeństwem w dosyć szerokim ujęciu: od zarządzania ryzykiem, ciągłością działania, poprzez bezpieczeństwo fizyczne i realizację ustawowych obowiązków na rzecz obronności i bezpieczeństwa państwa i bezpieczeństwa publicznego, do organizacji ochrony informacji niejawnych.

Obszary te pełnią istotną rolę w tworzeniu bezpiecznego środowiska do prowadzenia biznesu i niezakłóconego świadczenia usług telekomunikacyjnych.

Tym chętniej przyjąłem zaproszenie do Rady, traktując uczestnictwo jako możliwość współpracy z wybitnymi przedstawicielami branży oraz sektora edukacji przygotowującego przedsiębiorcom przyszłe kadry. Rada była doskonałą platformą wymiany wiedzy i doświadczeń. Organizowane wydarzenia, konferencje dawały możliwość poznania różnych punktów widzenia, a sama Rada wydała wiele ważnych rekomendacji, w szczególności w zakresie niezbędnych na rynku nowych kompetencji.

W ostatnich czasach daje się zauważyć rosnący nacisk na zapewnienie wysokiego poziomu odporności sektora telekomunikacji na zagrożenia i, w konsekwencji, dostępności usług. Przed nami kolejne wyzwania związane z transpozycją regulacji unijnych, takich jak NIS2 czy CER. W związku z tym wydaje się, że Rada w swoim kształcie powinna pracować w trybie ciągłym, dbając o aktualność programów kształcenia i dostępność odpowiednich kompetencji wraz ze zmieniającymi się warunkami otoczenia.

Spotkanie się w jednym zespole osób o różnych perspektywach spowodowało ciekawą, dyskusję

ADAM DZWONKOWSKI

Dyrektor Microsoft Technology Center,
członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Cyberbezpieczeństwo: jeden z głównych priorytetów państwa

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo już w momencie powołania była świetnym pomysłem, a dziś idealnie wpasowuje się w sytuację, której organizatorzy zapewne nie przewidzieli. Cyberbezpieczeństwo stało się jednym z głównych priorytetów państwa, a zapotrzebowanie na specjalistów dramatycznie wzrosło. Spotkanie się w jednym zespole osób o różnych perspektywach na tę dziedzinę spowodowało ciekawą, merytoryczną dyskusję i na pewno dało mi możliwość poznania różnych spojrzeń na tę tematykę.

Szczególnie zderzenie podejścia firmy, która jest globalnym i do tego kluczowym „graczem" na rynku cyberbezpieczeństwa, z oczekiwaniami i potrzebami mniejszych podmiotów, w tym ośrodków odpowiadających za edukację krajowych zasobów, pozwoliło mi i firmie, którą reprezentuję, lepiej dostosować i zidentyfikować potrzeby rynku, w tym poczynić konkretne inwestycje w powszechne szkolenie organizacji i przedsiębiorstw będących partnerami i klientami firmy Microsoft.

Cieszę się, że miałem okazję być członkiem Rady, doceniam profesjonalizm i zaangażowanie organizatorów i liczę, że w takiej czy innej formie współpraca będzie kontynuowana, ponieważ krajowa cyberprzestrzeń stała się obszarem działań, który jest krytyczny dla funkcjonowania polskiej przestrzeni biznesowej oraz publicznej.

Na wydziałach prawa trzeba wprowadzać elementy kształcenia z innych dziedzin, w tym z zakresu nowoczesnych technologii

ARWID MEDNIS

Wydział Prawa i Administracji Uniwersytetu Warszawskiego, członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, radca prawny

Otwórzmy oczy na odpowiednie kształcenie

Nie sposób przecenić roli sektorowych rad ds. kompetencji. Jeśli jednak mają pomóc w dopasowaniu sposobu kształcenia do potrzeb gospodarki, to same muszą składać się z osób reprezentujących szeroko rozumianą edukację i biznes w danej dziedzinie. I wydaje mi się, że w naszej Radzie taka reprezentacja jest.

Dla mnie uczestnictwo w Radzie, która zajmuje się telekomunikacją i cyberbezpieczeństwem, jest nie tylko wyróżnieniem, lecz także wyzwaniem. Jest też doświadczeniem otwierającym oczy na kwestie odpowiedniego kształcenia. Nauczyciele akademiccy mają tu również ważną rolę do odegrania. Ktoś może oczywiście zapytać, jakie znaczenie ma kształcenie prawników. Otóż ma, ponieważ w branżach takich jak telekomunikacja i cyberbezpieczeństwo mamy coraz więcej coraz bardziej skomplikowanych regulacji prawnych, z którymi wiążą się nowe obowiązki. Na przykład współczesne regulacje prawne z zakresu cyberbezpieczeństwa, ochrony danych osobowych, itp. są oparte o tzw. risk-based approach, a więc podejście, które zakłada, że ostateczny, konkretny kształt obowiązku z zakresu bezpieczeństwa zależy od dokonanej uprzednio oceny ryzyka. Prawo nie reguluje zatem tego, co trzeba konkretnie zrobić w ramach np. zabezpieczenia systemów informacyjnych, tylko opisuje „procedurę dojścia" do tych konkretów. I to jest między innymi rola prawników, którzy wspólnie ze specjalistami z innych dziedzin powinni określać, co konkretnie dana organizacja musi zrobić. Pamiętajmy, że ocena ryzyka i realizacja obowiązków podlega często kontroli różnych organów (np. organów właściwych do spraw cyberbezpieczeństwa czy Prezesa Urzędu Ochrony Danych Osobowych) oraz sądów. A przecież w tych organach i sądach zasiadają absolwenci takich wydziałów jak mój. Jako radca prawny, a więc praktyk prowadzący wiele różnych postępowań, mam wrażenie, że sędziowie często nie mają dostatecznej wiedzy w danej dziedzinie, żeby poprawnie ocenić daną kwestię. Zarówno w wygranej, jak i przegranej sprawie, chciałbym żeby wyrok był jakościowo dobry, tzn. wydany z pełną merytoryczną znajomością rzeczy.

Zmaterializowanych korzyści wynikających z prac Rady mogłoby być więcej, gdyby zdecydowano się na poszerzenie jej kompetencji

BOGUSŁAW DĘBSKI

Dyrektor Centrum Certyfikacji Kompetencji i Potwierdzania Kwalifikacji Polskiego Towarzystwa Informatycznego, członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Doświadczenie współpracy gwarantem sukcesu

Mówi się, że prawdziwa praca zespołowa oznacza współpracę, komunikację i uznanie wspólnego celu. Dokładnie tak było w przypadku Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

W mojej ocenie Rada ta stała się nie tylko efektywną platformą realizacji założonych w projekcie celów, lecz była także miejscem inspirującej dla mnie wymiany doświadczeń przedstawicieli edukacji, biznesu i administracji publicznej.

W konsekwencji powstawały zarówno wysoko oceniane przez rynek analizy i rekomendacje w zakresie oferowanych usług edukacyjnych, jak i rozwiązania wybiegające poza schematyczne działania przyporządkowane do tego typu gremiów.

Przykładem może być decyzja Rady o konieczności rozszerzenia oferty dostępnych na rynku kwalifikacji z obszaru cyberbezpieczeństwa. Rada doprowadziła do opracowania nowych kwalifikacji rynkowych Zintegrowanego Systemu Kwalifikacji (ZSK), w szczególności dotyczących bezpieczeństwa rozwiązań chmurowych.

Opisy tych kwalifikacji mają szansę na trwałe wpisać się w krajobraz wartościowych kwalifikacji wspierających procesy uczenia się przez całe życie oraz stać się inspiracją dla uczelni, szkół, oraz ośrodków szkoleniowych w Polsce. Moim zdaniem podobnych zmaterializowanych korzyści wynikających z prac Rady mogłoby być znacznie więcej, gdyby zdecydowano się na poszerzenie jej kompetencji o funkcje decyzyjne, m.in. w zakresie zasadności procedowania wniosków o włączenie kwalifikacji rynkowych ZSK na wstępnym etapie ich procedowania.

W Radzie udało się zebrać przedstawicieli małych, średnich i dużych przedsiębiorstw, a tym samym osiągnąć pełne spektrum spojrzenia na sektor

JAROSŁAW PAZGRAT

Członek zarządu MCX PRO Sp. z o.o., członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Zagadka przerodziła się w fascynację

Zaproszenie do Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo z jednej strony traktowałem jako wyróżnienie, a z drugiej jako swoistą zagadkę. Pomimo ponad 20-letniego doświadczenia w sektorze ICT było to moje pierwsze zetknięcie z radą sektorową. Zagadka przerodziła się w fascynację, która wynikała z głównych założeń dotyczących działalności rady oraz ze składu osobowego rady. Sądziłem, że ciężko będzie zbudować reprezentatywne grono przedstawicieli biznesu, nie koncentrując się tylko i wyłącznie na wielkich korporacjach i ich potrzebach.

W W Sektorowej Radzie ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwoj udało się zebrać przedstawicieli małych, średnich i dużych przedsiębiorstw, a tym samym osiągnąć pełne spektrum spojrzenia na sektor i jego kompetencyjne potrzeby. W związku z tym, że w skład Rady wchodzili nie tylko przedstawiciele biznesu, lecz także przedstawiciele środowiska akademickiego oraz zawodowych szkół średnich, dawało to możliwość poznania realnych uwarunkowań dotyczących kształtowania programów nauczania, potrzeb i bolączek naszego szkolnictwa. Osobiście podczas realizacji zadania „Kluczowe kompetencje zarządcze w branży telekomunikacja i cyberbezpieczeństwo z uwzględnieniem wpływu COVID-19 na zmiany sposobu zarządzania” miałem okazję poznać i rozmawiać z przedstawicielami zarządów wszystkich czołowych firm w sektorze, co pozwoliło mi uzyskać unikatową wiedzę na temat perspektywy ewolucji tych kompetencji na przestrzeni kolejnych lat, a także zrozumieć, jakie kompetencje są kluczowe do osiągnięcia sukcesu zawodowego.

Dobrym przykładem działań Rady były zawierane porozumienia sektorowe czy organizowane przez nią konferencje

ADAM
SIEWICZ

Prezes zarządu krajowego Stowarzyszenia Budowniczych Telekomunikacji, członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Nieodzowna jest współpraca

To, co dla Stowarzyszenia Budowniczych Telekomunikacji (SBT) – które to reprezentuję w Radzie – jest istotnym w działaniach Rady, to współpraca z reprezentantami rynku telekomunikacyjnego, tj. przedsiębiorcami, jednostkami edukacyjnymi, organizacjami pozarządowymi, administracją państwową, w tym legislatorem i regulatorem rynku. SBT w ramach tych prac opiniowało wiele projektów i przedsięwzięć Rady, w tym w zakresie aktów legislacyjnych, projektów kwalifikacji rynkowych zgłaszanych do rejestru ZSK czy samych ram kwalifikacji sektorowych (np. analizy SRK Tele). Naszym zdaniem dobrym przykładem działań Rady były zawierane porozumienia sektorowe czy konferencje organizowane przez Radę (np. Forum Teleinformatyki, EduMixer 2022). Jesteśmy zainteresowani dalszą współpracą w tym zakresie.

Co do rozwoju kwalifikacji rynkowych w sektorze telekomunikacji – zdaniem SBT istotna jest stała współpraca z rynkiem pracodawców i pracowników sektora, bieżące śledzenie zmian na tym rynku oraz rozwoju legislacji Unii Europejskiej i w ślad za tym, krajowej. Mamy tu na myśli nowy horyzont wymagań i warunków, regulacji na rynku infrastruktury, usług i urządzeń. A jest to konsekwencją wprowadzenia nowych regulacji UE, m.in. w sprawie: środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, jednolitego rynku usług cyfrowych (akt o usługach cyfrowych „DSA”), kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych). Wynikają z nich nowe obowiązki przedsiębiorców, a zatem i potrzeby nowych kwalifikacji dla pracowników. Współpraca Rady z rynkiem pracodawców, podmiotami edukacyjnymi i pozarządowymi oraz regulatorem sektora jest tu nieodzowna.

EUROPA POTRZEBUJE KOMPETENTNYCH KADR

Wciąż zmieniający się rynek pracy w Polsce i na świecie wymaga od pracowników uzupełniania kwalifikacji. Dlatego konieczna jest koordynacja działań inicjatyw sektorowych – tak na szczeblu europejskim, jak i krajowym – która pozwoli na wspólne wypracowanie narzędzi zwalczających niedopasowanie kwalifikacji.

Adam Sanocki
Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo,
Polskie Towarzystwo Informatyczne

To, jakie kompetencje i kwalifikacje są aktualnie potrzebne na rynku, zmienia się wraz z sytuacją gospodarczą czy rozwojem technologicznym związanym z automatyzacją i cyfryzacją przedsiębiorstw. Do zmian w funkcjonowaniu przedsiębiorstw na całym świecie w dużej mierze przyczyniła się również pandemia COVID-19.
Dla pracodawców istotne jest dostosowanie kwalifikacji pracowników do aktualnej sytuacji panującej na rynku pracy.
Stąd konieczność współpracy jednostek naukowych z przedsiębiorcami. Dzięki niej możliwe jest dopasowanie systemu edukacji do potrzeb gospodarki. Dlatego tak ważne jest, by absolwenci szkół wyższych, czyli przyszli pracownicy, mieli dostęp do praktycznej wiedzy odpowiadającej potrzebom rynku. Nie można też zapominać o zapewnieniu im możliwości rozwijania tzw. kompetencji miękkich, jak skuteczna komunikacja czy umiejętność współpracy w zespole.

Z zainicjowanego przez PARP badania „Bilans Kapitału Ludzkiego" wynika, że ponad 50 proc. Polaków ma wyższe wykształcenie. Mimo to ¾ przedsiębiorców nie może znaleźć kandydatów o pożądanych kwalifikacjach.
Stąd powołanie Rad ds. Kompetencji. Mają być one odpowiedzią na lukę w zapotrzebowaniu na wiedzę, kompetencje i umiejętności na rynku pracy. Rady mają ułatwić współpracę między partnerami społecznymi – przedsiębiorstwami, związkami zawodowymi, izbami handlowymi, instytucjami badawczymi, edukacyjnymi i szkoleniowymi oraz władzami publicznymi na poziomie krajowym, regionalnym i lokalnym. Rady powołano w sektorach kluczowych dla gospodarki, jak opieka zdrowotna i pomoc społeczna, budownictwo, finanse, turystyka czy IT. Ma to pozwolić dostosować system kształcenia do realnego zapotrzebowania przedsiębiorców z poszczególnych branż.

Nie tylko polski problem

Brak kadr z odpowiednimi kompetencjami to nie tylko nasz lokalny problem, dotyczy to również innych krajów Unii Europejskiej. Z danych opublikowanych przez urząd statystyczny UE wynika, że stopa bezrobocia w strefie euro w grudniu 2022 r. wyniosła 6,6 proc., a w krajach UE 6,1 proc. W Europie ciągle obserwuje się niedobór siły roboczej i niedopasowanie kwalifikacji do wymagań,

jakie stawia przed przedsiębiorcami i pracownikami rynek pracy. Europejskie Centrum Rozwoju Kształcenia Zawodowego (CEDEFOP) wskazuje, że w Unii Europejskiej około 75 mln ludzi – czyli niemal jedna trzecia osób w tzw. wieku produkcyjnym – ma niskie kwalifikacje lub nie ma żadnych. Z danych CEDEFOP z 2018 roku wynika, że czterech na dziesięciu pracodawców w UE miało trudności ze znalezieniem pracowników spełniających ich oczekiwania. Z kolei około 39 proc. dorosłych pracowników zajmowało stanowiska pracy poniżej swoich kwalifikacji, a jeden na pięciu Europejczyków podejmował pracę, która wymagała niższych kwalifikacji niż te, które posiadał.

Na europejskim rynku pracy obserwowane są też inne trendy. Starzenie się społeczeństw powoduje, że coraz częściej konieczność przekwalifikowania się czy podnoszenia kompetencji dotyczyć będzie dorosłych, także aktywnych zawodowo. Zmiany demograficzne powinny wpłynąć na zakres beneficjentów inicjatyw sektorowych. W tym kontekście znaczenia nabiera promowanie uczenia się przez całe życie. Komisja Europejska ogłosiła rok 2023 „Europejskim Rokiem Umiejętności". Ma to dać obywatelom możliwość nauki, podnoszenia kwalifikacji zawodowych czy udziału w szkoleniach dzięki dofinansowaniu z Funduszy Europejskich. Program ma się skupiać na daniu pracownikom możliwości podnoszenia swoich kwalifikacji przez całe życie. Unia ma kierować na ten cel środki finansowe, ujęte m.in. w EFS+, „Cyfrowej Europie" czy programie „Erasmus+".

Na lokalnych podwórkach

Kraje członkowskie UE tworzą własne projekty wsparcia systemów szkolenia i kształcenia zawodowego, w niektórych przypadkach także szkolnictwa wyższego i edukacji dorosłych. Systemy te są dostosowane do aktualnej sytuacji na rynku pracy oraz umiejętności i wykształcenia mieszkańców danego kraju. Odpowiedzią na lukę w zapotrzebowaniu na wiedzę, kompetencje i umiejętności wymagane od pracowników w określonych kategoriach są Europejskie Rady ds. Umiejętności Sektorowych (European Sector Skills Councils). W 2022 roku zakończyły one swoją działalność, przekształcając się w Sojusze na Rzecz Umiejętności Sektorowych (Sector Skills Alliances).

> **Konieczność przekwalifikowania się czy podnoszenia kompetencji dotyczyć będzie dorosłych, także aktywnych zawodowo**

Zakres funkcjonowania i zadania powierzone ESSC są zbliżone do zadań rad sektorowych funkcjonujących w Polsce. Oczywiście pojawiają się różnice dotyczące branż i sektorów – państwa UE szczegółowo określają te, w których brakuje wykwalifikowanych pracowników. Są to m.in. przemysł morski, rolnictwo czy przemysł drzewny i papierniczy.

Europejskie systemy opierają się na aktualizowaniu i tworzeniu programów nauczania tak, by dostarczać odpowiednich kwalifikacji i umiejętności. Ważnym obszarem jest również tworzenie odpowiednich profili zawodowych opartych na monitoringu umiejętności. Różnice w funkcjonowaniu rad sektorowych w Polsce i tych działających na terenie innych państw UE można zauważyć przede wszystkim w skali projektów. Polskie rady sektorowe skupiają się na kształceniu pracowników, którzy mają wzmocnić pozycję polskich firm i rynek pracy w Polsce. Z kolei europejskie programy kompetencyjne, oprócz poprawiania sytuacji wewnątrz państw członkowskich, nastawione są także na wymianę pracowników między

krajami Unii, co gwarantuje przenikanie się specjalistów między państwami i daje większe prawdopodobieństwo znalezienia przez pracodawców idealnych kandydatów do swoich firm.

Poniżej kilka przykładów działania rad sektorowych w innych krajach

Łotwa – Eksperckie Rady Sektorowe
Eksperckie Rady Sektorowe na Łotwie skupiają się przede wszystkim na polepszeniu kwalifikacji osób, które po ukończeniu szkół średnich nie kontynuują już nauki, co powoduje, że pozostają bez potwierdzonych umiejętności. To powód, dla którego tak mocno jest rozwinięte w tym kraju szkolenie zawodowe i dopasowanie go do poszczególnych sektorów gospodarki. Szczególny nacisk kładziony jest na te branże gospodarki, w których pracownicy mogą zdobyć praktyczną wiedzę i umiejętności, np. przemysł chemiczny, farmacja, przemysł tekstylny, produkcja skór i wyrobów skórzanych, budownictwo, ale także energetyka czy finanse i księgowość.

Malta – Karta Umiejętności Branży Budowalnej
Ciekawym przykładem działalności rad sektorowych jest rada działająca na Malcie. Jest ona skupiona na jednym sektorze gospodarki – budownictwie. Głównym celem The Construction Industry Skill Card (CISC) jest umożliwienie pracownikom sektora budowlanego zdobycie nowych umiejętności, które pomogą im się przystosować do zmieniającego się rynku pracy oraz poprawić jakość oferowanych przez branżę usług.

Hiszpania – Wspólne Komitety Sektorowe
Głównym problemem hiszpańskiego systemu kształcenia jest brak możliwości dofinansowania szkoleń dla pracowników niewykwalifikowanych w ramach umów krajowych. W Hiszpanii dominują małe firmy, które działają zgodnie z tradycyjnymi systemami zarządzania. Zastosowanie nowych zasad zarządzania zasobami ludzkimi zwykle ogranicza się do pracowników o kluczowych umiejętnościach w większych, korporacyjnych przedsiębiorstwach. Rady Sektorowe ds. Umiejętności mają za zadanie stworzyć odpowiednie warunki do zniwelowania luki prawnej, która do tego doprowadziła. Sytuację komplikuje to, że sektory gospodarki są bardzo zróżnicowane, są to m.in. hotelarstwo, turystyka, przemysł chemiczny, przemysł metalurgiczny czy działalność morska i portowa.

Sojusze na Rzecz Umiejętności

Na koniec warto wspomnieć o Sojuszach na Rzecz Umiejętności Sektorowych (Sector Skills Alliances – SSA), które – podobnie jak Rady Sektorowe – są inicjatywami stworzonymi przez UE w celu dopasowania umiejętności pracowników poszczególnych sektorów do zapotrzebowania rynku pracy. SSA szczególną uwagę zwracają na umiejętności cyfrowe, przydatne zarówno dla pracowników, jak i pracodawców. W Polsce działa Sektorowa Rada ds. Kompetencji w obszarze Telekomunikacji i Cyberbezpieczeństwa. Jej celem jest kompleksowa identyfikacja i prognozowanie potrzeb kwalifikacyjno-zawodowych sektora telekomunikacyjnego oraz cyberbezpieczeństwa (TCB). Radę tworzą najważniejsze instytucje oraz firmy mające realną wiedzę na temat funkcjonowania i potrzeb sektora TCB.

Wciąż zmieniający się rynek pracy w Polsce i na świecie wymaga zarówno od przyszłych, jak i obecnych pracowników podwyższania swoich kompetencji i uzupełniania kwalifikacji. Aktualne doświadczenia pokazują, że niezbędna jest odpowiednia koordynacja działań inicjatyw sektorowych, tak na szczeblu europejskim, jak i krajowym. Dzięki temu można będzie wspólnie wypracować narzędzia, które będą efektywnie zwalczać niedopasowanie kwalifikacji.

WIEDZA I KOMPETENCJE RAD SĄ JAK LATARNIA MORSKA

Musimy sprostać zmianom, a to można tylko zrobić, budując elastyczne rozwiązania – mówi Daniel Nowak, ekspert w Departamencie Rozwoju Kadr w Przedsiębiorstwach, w rozmowie z Beatą Ostrowską, wiceprzewodniczącą Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

Beata Ostrowska: Jaka była idea powstania Systemu Rad ds. Kompetencji i powołania przez Polską Agencję Rozwoju Przedsiębiorczości rad sektorowych?

Daniel Nowak: Inspiracją dla nas były rady umiejętności, które działały w Wielkiej Brytanii. Kilka lat temu działało ich w tym kraju około 20 i były one nadzorowane przez instytucję publiczną. Przy okazji prac nad Zintegrowanym Systemem Kwalifikacji, w trakcie kuluarowych spotkań, zawiązaliśmy nieformalną współpracę z kilkoma sektorami. Dzięki temu udało się nam przekonać przedstawicieli Komisji Europejskiej do tego, żeby zgodziła się na dofinansowanie kilku pierwszych rad sektorowych. Później Komisja zgodziła się na sfinansowanie kolejnych i w ten sposób teraz mamy ich 17.

W jaki dokładnie sposób funkcjonowały powołane rady sektorowe? Jakie były ich zadania i kompetencje?

Rady przede wszystkim analizują sytuację w danej branży i na tej podstawie przygotowują rekomendacje, w których wskazują, jakich kwalifikacji brakuje w sektorze.

Sektorowe Rady ds. Kompetencji przygotowują ramy prawne dla efektywnego i praktycznego kształcenia specjalistów. Zachęcają przedsiębiorców do angażowania się w kształcenie, np. poprzez organizację praktyk i staży oraz współtworzenie podstawy programowej dla kształcenia w zawodach

czy oddziaływanie na instytucje szkoleniowo-rozwojowe w przygotowaniu oferty dopasowanej do zidentyfikowanych potrzeb sektora.

Ekspercki i szeroki skład rad pozwalają na rzetelną identyfikację luk kompetencyjnych w sektorze i ich prognozowanie. Są one podstawą do podejmowania przez administrację publiczną decyzji opartych na dowodach, przy zachowaniu współpracy wszystkich uczestników systemu.

Trzeba też dodać, że PARP za pośrednictwem Bazy Usług Rozwojowych dofinansowuje usługi szkoleniowe bądź doradcze wynikające z rekomendacji rad.

Sektorowe Rady ds. Kompetencji przygotowują ramy prawne dla efektywnego i praktycznego kształcenia specjalistów

Rady sektorowe powołane zostały w określonych sektorach takich, jak m.in. IT, finanse, budownictwo czy opieka zdrowotna, branże kluczowe dla funkcjonowania polskiej gospodarki. W jaki dokładnie sposób zostały wybrane poszczególne sektory i jaki wpływ na ich późniejsze funkcjonowanie miały powołane rady?

Rady zostały wyłonione w konkursach w ramach Programu Operacyjnego Wiedza Edukacja Rozwój. Żeby je przeprowadzić, musieliśmy podzielić gospodarkę na sektory, zdefiniować je i dopiero ogłosić konkurs. Wybierając rady sektorowe, musieliśmy zwracać szczególną uwagę na potencjał podmiotów, które je będą prowadzić. Trzeba pamiętać, że Komisja na początku zgodziła się na wsparcie tylko kilku rad sektorowych i od powodzenia ich działania zależała zgoda na dofinansowanie kolejnych.

Jaki wpływ na funkcjonowanie przedsiębiorstw miały powołane siedem lat temu Rady Sektorowe? Czy możemy także wskazać, jaki miały wpływ na funkcjonowanie systemu edukacji w Polsce?

Ciężko oszacować, jaki miały wpływ. Jest trudny do uchwycenia. Jednak można powiedzieć, że rady to pierwszy podmiot, któremu wprost zostały przyznane środki publiczne tylko i wyłącznie na działania związane z identyfikowaniem luk kompetencyjnych w sektorach i działania związane z ich zmniejszaniem. Dzięki temu wielu przedsiębiorców zaczęło zwracać uwagę na to, jak ważne jest planowanie rozwoju firmy czy branży także w kontekście rozwoju pracowników i planowania wspólnie z instytucjami publicznymi działań, które przyczyniają się do zmniejszania luki kompetencyjnej. Stąd tak ważna współpraca rad sektorowych ze szkołami, uczelniami i innymi podmiotami edukacyjnymi.

Jak do tej pory możemy podsumować prace rad sektorowych?

Najbardziej wymiernym rezultatem pracy rad sektorowych są rekomendacje rad. Każda z nich takie wydała i są one dostępne publicznie. PARP na ich podstawie ogłosiła konkursy dla przedsiębiorców i dofinansowała dla nich usługi edukacyjne. Do tej pory wsparliśmy ponad 14,5 tys. pracowników, są to dane według stanu na 31 grudnia 2022 roku.

Rady prowadzą też własne badania, których wyniki publikują na swoich stronach

internetowych, organizują konferencje, debaty społeczne dotyczące luk kompetencyjnych, rozwoju sektora i potrzebnych kompetencji w przyszłości, współpracują ze szkołami i ministerstwami, żeby system edukacji – ten formalny i pozaformalny – odpowiadał potrzebom przedsiębiorców.

W jaki sposób Rady Sektorowe ds. Kompetencji wpłynęły w ciągu tych kilku lat na funkcjonowanie rynku pracy oraz na pracowników?

Niewątpliwie liczba szkoleń i innych usług edukacyjnych, o których mówiliśmy wcześniej, przyczyniła się do tego, że luki kompetencyjne w sektorach zmniejszyły się, a przedsiębiorcy zwrócili większą uwagę na to, że podnoszenie kompetencji pracowników nie jest tylko kosztem, ale inwestycją w rozwój firmy.

W obliczu wzrastających zagrożeń oraz sytuacji społeczno-gospodarczej w Polsce i na świecie należy podkreślić kluczową rolę, jaką w naszej gospodarce odgrywa sektor ICT. Jakie będą w najbliższym czasie wyzwania, a także nowe możliwości w kontekście rozwijania kompetencji, umiejętności i rynku pracy w obszarze telekomunikacji, cyberbezpieczeństwa oraz IT?

Tu należy zwrócić uwagę na nowy program Fundusze Europejskie dla Rozwoju Społecznego, w skrócie FERS. Polska przeznaczy bardzo dużo środków na wsparcie transformacji cyfrowej i tzw. zielonej, ekologicznej. Już to jest ogromnym wyzwaniem, biorąc pod uwagę kontekst, w jakim jesteśmy. Bardzo mało polskich firm korzysta z rozwiniętych rozwiązań cyfrowych. Polska ze swoim wskaźnikiem DESI (indeks gospodarki cyfrowej i społeczeństwa cyfrowego) plasuje się na 24. pozycji wśród wszystkich państw członkowskich Unii Europejskiej. DESI uwzględnia cztery obszary: kapitał ludzki, łączność, integrację technologii cyfrowej oraz cyfrowe usługi publiczne. W obszarze kapitału ludzkiego widać, że tylko 43 proc. osób posiada podstawowe umiejętności cyfrowe.

> **Zaangażowanie Rad jest nieocenione w sytuacjach nagłej zmiany rynkowej, przykład to wybuch pandemii COVID-19 albo wojny w Ukrainie**

Czy możemy wskazać przykłady dobrych praktyk na podstawie funkcjonowania rad sektorowych oraz w zakresie współpracy sektora edukacji z biznesem? Czy w ciągu siedmiu lat działania rad sektorowych zauważa Pani także pewne złe praktyki, które trzeba wyeliminować?

Bardzo dobrze obrazuje to Sektorowa Rada ds. Kompetencji Informatyka i Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo. W szczególności w zakresie upowszechniania wiedzy na temat luk kompetencyjnych sektora i angażowania swojego środowiska do współpracy. Przywołam choćby konferencje EduMixer, na których poruszane są ważne tematy z zakresu aktualnych trendów w sektorze oraz potrzeb kompetencyjnych. Bardzo dobrym przykładem jest Rada Sektorowa Mody i Innowacyjnych Tekstyliów, która podejmuje wiele działań na rzecz wspierania edukacji sektorowej w szkołach branżowych. Nie można też zapomnieć o Radzie Odzysku Materiałowego Surowców, która wspólnie z Ministerstwem Klimatu i Środowiska pracuje nad wprowadzeniem zmian do podstawy programowej szkół branżowych, żeby te w większym stopniu odpowiadały sektorowi.

W ramach nowej perspektywy finansowej mają powstać kolejne Rady Sektorowe. Czy możemy wskazać, jakie powstaną, i określić sektory gospodarki oraz obszary, w których zostaną powołane?

Tego jeszcze nie wiemy. Pracujemy intensywnie nad identyfikacją takich sektorów i potencjalnych podmiotów, które mogłyby prowadzić taką radę. Przez kilka lat funkcjonowania rad sektorowych zbieraliśmy zgłoszenia zainteresowanych podmiotów i mamy taką listę, ale nie wypełnia ona naszych możliwości wsparcia projektów rad sektorowych w FERS. Dlatego też, jeśli ktoś jest zainteresowany prowadzeniem nowej rady, zapraszamy do kontaktu z PARP. Wtedy zorganizujemy konkurs.

Najbardziej wymiernym rezultatem pracy rad sektorowych są rekomendacje rad

Jakie wyzwania oraz zagrożenia możemy wskazać dla nowo powołanych rad w obliczu aktualnej sytuacji gospodarczej Polski oraz trudnej sytuacji firm i samych przedsiębiorców?

Obecnie naszą gospodarkę, a także gospodarkę Unii Europejskiej dotyka wiele wyzwań i trudności. Myślę, że dla rad sektorowych zarówno tych starych, jak i nowych, są one takie same. Borykamy się z wysokimi cenami energii, ciągłymi zmianami i trudnościami w łańcuchach dostaw, inflacją, zmniejszeniem akcji kredytowej banków i ciągłym niedoborem pracowników o poszukiwanych kompetencjach. Wiele firm musi podjąć w związku z tym trudne decyzje, które nie są obojętne dla poszukiwanych kompetencji. Choćby skracanie łańcuchów dostaw zwiększy wymagania dotyczące powierzchni magazynowej i jej obsługi. Do tego są potrzebne zarówno rozwiązania logistyczne, jak i cyfrowe. Ciągły rozwój sztucznej inteligencji także będzie wpływał na to, jak przebiegają różne procesy: produkcyjne, sprzedażowe, relacji z klientami i inne.

Pewna jest tylko zmiana i musimy umieć jej sprostać. A to można zrobić, tylko budując elastyczne rozwiązania – co też jest wyzwaniem.

Przed radami wiele wyzwań i konieczność szybkiej, w wielu sytuacjach, reakcji. To zresztą było już widać.

Tak. Wiedza i kompetencje członków Rady, jak również innych rad sektorowych, na co dzień są dla nas jak latarnia morska, która wskazuje kierunek wsparcia przedsiębiorców i pracowników przedsiębiorców. Zaangażowanie Rad jest także nieocenione w sytuacjach nagłej zmiany rynkowej. Przypomnieć wystarczy wybuch pandemii COVID-19 albo wojny w Ukrainie. Rady sektorowe natychmiast zareagowały, przygotowując specjalne rekomendacje dotyczące tego, jakie szkolenia i doradztwo są konieczne w sektorach, aby mogły dalej sprawnie funkcjonować i szybko dostosować się do dynamicznie zmieniającej się rzeczywistości.

PLANOWANE ZMIANY W PRAWIE A POTRZEBY KOMPETENCYJNE

Nie jest tajemnicą, że w Polsce brakuje specjalistów zarówno w dziedzinie telekomunikacji, jak i cyberbezpieczeństwa. A zapotrzebowanie na nich w najbliższym czasie jeszcze wzrośnie.

Arwid Mednis
członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Uniwersytet Warszawski

Postępująca cyfryzacja i rosnąca liczba zagrożeń w cyberprzestrzeni powodują, że tylko w zakresie cyberbezpieczeństwa potrzeby te sięgają już około 18 tysięcy osób. Oprócz stałych potrzeb kompetencyjnych pojawiły się w ostatnim czasie nowe wyzwania, jak choćby wzrost liczby ataków hakerskich, częściowo niewątpliwie powiązany z atakiem Rosji na Ukrainę (ataki te dotyczą nie tylko instytucji publicznych, ale również podmiotów sektora prywatnego, m.in. banków). Dodatkowo, pandemia SARS-CoV-2 wymusiła zajęcie się taki kwestiami, jak bezpieczeństwo pracy zdalnej.

I tu pojawia się ważne pytanie: skoro dziś w tych konkretnych okolicznościach mamy takie braki kadrowe, jak zamierzamy sobie poradzić w najbliższych latach nie tylko w obliczu liczby zagrożeń, która z pewnością nie będzie maleć, ale również w kontekście nowych regulacji prawnych zarówno w sektorze łączności elektronicznej (telekomunikacji), jak i cyberbezpieczeństwa?

Patrzmy w przyszłość

Na pojawianie się nowych cyberzagrożeń nie mamy wielkiego wpływu, ale nad regulacjami prawnymi prace trwają zwykle dłuższy czas i w tym zakresie można przewidzieć jakich kompetencji będzie wymagało stosowanie nowego prawa. W przypadku projektów przepisów unijnych prace trwają nierzadko kilka lat, a w przypadku dyrektyw należy

doliczyć jeszcze czas na ich implementację do krajowego porządku prawnego.

Dobrym przykładem jest RODO, które jest rozporządzeniem, a więc nie wymaga implementacji: od chwili opublikowania projektu do uchwalenia upłynęły cztery lata, a mieliśmy jeszcze dwuletni okres dostosowawczy. Przepisy o ochronie danych osobowych funkcjonowały już wcześniej, ale przynajmniej w Polsce zaczęliśmy poważnie traktować ochronę danych, dopiero gdy wraz z RODO pojawiła się perspektywa wysokich kar pieniężnych. Pomimo to można odnieść wrażenie, że do dziś rynek specjalistów w tej dziedzinie nie jest nasycony.

Brakuje nam zdecydowanie kierunków interdyscyplinarnych, tak aby np. osoby zajmujące się telekomunikacją nabyły potrzebną wiedzę obejmującą prawo

Nie chodzi tu jednak tylko o zbyt małą liczbę specjalistów w danej dziedzinie, ale o jakość przekazywanej wiedzy. Struktury edukacyjne są w Polsce nadal skostniałe, tworzy się wprawdzie nowe kierunki studiów, ale nadal osoby o określonym wykształceniu muszą ratować się różnymi kursami i studiami podyplomowymi, żeby uzupełnić wiedzę w innej dziedzinie. Brakuje nam zdecydowanie kierunków interdyscyplinarnych, tak aby np. osoby zajmujące się telekomunikacją nabyły potrzebną wiedzę obejmującą prawo, ekonomię (regulowanie rynku takiego jak telekomunikacyjny wymaga tego typu wiedzy), wiedzę techniczną o funkcjonowaniu sieci i urządzeń.

Tymczasem przed nami zmiany w regulacjach prawnych w obu interesujących nas dziedzinach. Wydaje się, że planowane zmiany nie kreują potrzeb w zakresie nowych kompetencji, natomiast zwiększą zapotrzebowanie na specjalistów posiadających wiedzę w dotychczasowym zakresie. Stanie się to głównie za sprawą zastosowania nowych przepisów do szerszego kręgu podmiotów. Zapewne część skorzysta z formuły outsourcingu, ale to z kolei oznacza zwiększenie popytu na specjalistów w firmach powiązanych.

Nowe regulacje prawne

W dziedzinie telekomunikacji (komunikacji elektronicznej) procedowany jest obecnie w Sejmie projekt ustawy – Prawo komunikacji elektronicznej.

Ustawa ma stanowić długo oczekiwaną implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11 grudnia 2018 r. ustanawiającej europejski kodeks łączności elektronicznej (Dz. Urz. UE L 321 z 17.12.2018, str. 34, z późn. zm.). Implementacja dyrektywy w poszczególnych państwach UE zakończy jeden z najważniejszych etapów realizacji strategii Jednolitego Rynku Cyfrowego.

Z jednej strony nowa regulacja zawiera wiele uaktualnionych przepisów dotyczących sieci łączności elektronicznej (sieci telekomunikacyjnych), usług telekomunikacyjnych oraz towarzyszących urządzeń i usług, z drugiej – rozszerza się w niej zakres podmiotowy stosowania przepisów. Prawo komunikacji elektronicznej, wzorem wspomnianej dyrektywy, poza tradycyjnymi przedsiębiorcami telekomunikacyjnymi, obejmie również podmioty pozostające dotąd poza regulacją pakietu dotychczasowych dyrektyw telekomunikacyjnych oraz Prawa

telekomunikacyjnego, tj. podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów.

Zmiana ta z pewnością wymusi zapotrzebowanie na specjalistów od regulacji rynku telekomunikacyjnego, z uwagi na to, że znaczna część „nowych" usług jest obecnie świadczona przez podmioty niebędące tradycyjnymi przedsiębiorcami telekomunikacyjnymi.

Wzrośnie zapotrzebowanie na specjalistów

Sporo zmian czeka nas także w przepisach dotyczących cyberbezpieczeństwa. Spowodują one niewątpliwie wzrost popytu na specjalistów zajmujących się różnymi aspektami tego zagadnienia.

W pierwszej kolejności warto wspomnieć o planowanej nowelizacji ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Prace nad nowelizacją trwają już bardzo długo i w chwili obecnej trudno przesądzić o jej dalszych losach, ponieważ słychać coraz częściej postulaty, aby w nowelizacji wziąć pod uwagę uchwaloną niedawnoe dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 („Dyrektywa NIS 2"). Niezależnie od tych kontrowersji warto odnotować, że gdyby nowelizacja weszła w życie, to miałaby również wpływ na rozwój kompetencji i rynek specjalistów od cyberbezpieczeństwa ze względu m.in. na dołączenie do krajowego systemu cyberbezpieczeństwa kilku nowych podmiotów, a ponadto pojawienie się na rynku nowej instytucji, tj. tzw. ISAC, czyli centrów wymiany informacji i analiz (*Information Sharing and Analysis Center*). Zwykle są one tworzone w formule partnerstwa publiczno-prywatnego i najczęściej są wykorzystywane w kwestiach związanych z bezpieczeństwem, w tym cyberbezpieczeństwem. W USA instytucje te sprawdzają się już od jakiegoś czasu w poszczególnych sektorach gospodarki. Skupiają m.in. wysokiej klasy analityków, specjalistów od data science itp.

Niektóre akty prawne powinny zawierać dodatkowe wymogi kwalifikacyjne na wyższe stanowiska, co służyłoby większemu popytowi na zdobywanie odpowiednich kwalifikacji

Zgodnie z projektem nowelizacji – ISAC byłyby centrami wymiany i analizy informacji na temat podatności cyberzagrożeń i incydentów funkcjonującymi w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa. Stworzenie ISAC będzie miało dobrowolny charakter, niewątpliwie jednak wzmocni popyt na specjalistów w zakresie analityki cyberzagrożeń.

Kluczowe i ważne

Wspomniana już dyrektywa NIS 2 będzie kolejnym wyzwaniem dla rynku. W stosunku do stanu obecnego zmieni ona wiele kwestii, ale w kontekście kompetencji warto odnotować przede wszystkim zmianę klasyfikacji podmiotów będących adresatami nowych przepisów oraz rozszerzenie zakresu podmiotowego na nowe dziedziny. W dyrektywie NIS2 porzucono dotychczasowy

podział na operatorów usług kluczowych i dostawców usług cyfrowych na rzecz rozgraniczenia na podmioty kluczowe i ważne.

Co istotne, rozszerzeniu ulega katalog sektorów objętych działaniem dyrektywy. Wśród sektorów objętych dyrektywą pojawi się m.in. administracja publiczna, sektory żywności, odprowadzania ścieków, zarządzania odpadami oraz przestrzeń kosmiczna. Ponadto, w obrębie dotychczasowych sektorów (takich jak zdrowie, infrastruktura cyfrowa) dojdzie do rozszerzenia stosowania obowiązków na nowe kategorie podmiotów. Zwiększą się także wymagania w zakresie zabezpieczeń systemów informacyjnych. Dyrektywa musi zostać zaimplementowana do krajowego porządku prawnego do 17 października 2024 r., niemniej możemy już zaobserwować zainteresowanie przedsiębiorców wdrożeniem jej postanowień w firmach.

DORA i certyfikacja

Dużym zainteresowaniem cieszy się również rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011), znane jako „DORA". Zawiera ono szczegółowe wymogi odnośnie do cyberbezpieczeństwa w instytucjach finansowych. DORA jako rozporządzenie nie wymaga implementacji w prawie krajowym, ale zastosowanie znajdzie od 17 stycznia 2025 r. Ze wstępnych analiz wynika, że w pewnej części dużych podmiotów finansowych jego wdrożenie nie będzie stanowiło większego problemu, jednak z pewnością znajdą się w sektorze takie firmy, które będą musiały zwiększyć środki i wzmocnić kadry, aby spełnić wszystkie szczegółowe wymagania.

Dodajmy jeszcze, że na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) rozwija się obecnie nowy mechanizm certyfikacji produktów, usług i procesów ICT w kontekście cyberbezpieczeństwa. W tym celu planuje się odpowiednie zmiany w ustawie o krajowym systemie cyberbezpieczeństwa. Wprawdzie certyfikacja będzie dobrowolna, ale w mojej ocenie waga certyfikacji wzrośnie w kolejnych latach (np. poprzez wymogi przetargowe i in.), a ponadto na szczeblu unijnym planuje się wprowadzenie obowiązku certyfikacji niektórych elementów internetu rzeczy.

Powyższe zmiany legislacyjne to tylko wycinek planowanej regulacji gospodarki cyfrowej w dwóch dziedzinach, którymi zajmuje się Sektorowa Rada ds. kompetencji Telekomunikacja i Cyberbezpieczeństwo. Nie ulega jednak wątpliwości, że wszystkie te zmiany znacząco wpłyną na rynek powiązanych z tymi dziedzinami zawodów i pożądanych kompetencji. Rola Rady jest w tym zakresie nie do przecenienia, Rada podejmowała wiele działań związanych z poszerzaniem kompetencji w obu dziedzinach, zabierała również głos w procesach legislacyjnych. Wydaje się w związku z tym zasadne „automatyczne" włączanie Rady w prace nad projektami dotyczącymi telekomunikacji i cyberbezpieczeństwa. Słuszny jest, moim zdaniem, również postulat, aby niektóre akty prawne zawierały dodatkowe wymogi kwalifikacyjne na wyższe stanowiska w obu dziedzinach. Służyłoby to większemu popytowi na zdobywanie odpowiednich kwalifikacji.

TRENDY W PRAWIE I ICH WPŁYW NA SEKTOR ICT

Coraz większą wagę należy przykładać do edukacji cyfrowej, by lepiej dopasować kompetencje do współczesnego rynku pracy oraz przygotować do bezpiecznego, etycznego i umiejętnego korzystania z szans stwarzanych przez technologie.

Agnieszka Besiekierska,
Beata Zbarachewicz
Ekspertki Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Uniwersytet Kardynała Stefana Wyszyńskiego

W ostatnich latach obserwujemy wzmożoną aktywność zarówno w obszarze prawodawstwa europejskiego, jak i polskiego w zakresie technologii informacyjno-komunikacyjnych (ICT). Wynika to niewątpliwie z rozwoju technologii, zmian społecznych zachodzących m.in. wskutek pandemii, która wymusiła częstsze korzystanie z narzędzi ICT, a także przyzwyczaiła i zwiększyła oczekiwania pracowników związane z szerszym zastosowaniem pracy zdalnej lub pracy w modelu hybrydowym, jak również umożliwiła odkrycie możliwości, jakie dają w edukacji. Obok pozytywnych efektów związanych z zastosowaniem nowych technologii, nasiliły się zjawiska negatywne, takie jak zwiększenie aktywności cyberprzestępców, dezinformacja czy niczym nieskrępowana dominacja dużych graczy w cyberprzestrzeni.

Obowiązkowa certyfikacja

Reakcją na cyberprzestępczość jest obserwowany wzrost świadomości, przywiązywanie większej wagi do działań skierowanych na poprawę cyberbezpieczeństwa i co za tym idzie – nowe prawo. Pod koniec 2022 roku została przyjęta nowa dyrektywa NIS2 rozszerzająca katalog podmiotów objętych obowiązkami w obszarze cyberbezpieczeństwa. Do dotychczasowych podmiotów dołączyły podmioty z sektora produkcyjnego (m.in. producenci komputerów, wyrobów

elektronicznych i optycznych, producenci urządzeń elektrycznych i maszyn), dostawcy publicznie dostępnych usług komunikacji elektronicznej, dostawcy usług zarządzanych ICT (managed ICT services) oraz operatorzy platform sieci społecznościowych. Istotną zmianą jest uprawnienie Komisji Europejskiej oraz państw członkowskich do wprowadzenia obowiązkowej certyfikacji w odniesieniu do niektórych produktów ICT, usług ICT i procesów ICT, z których będą korzystać podmioty kluczowe.

W najbliższej przyszłości można się spodziewać kolejnych europejskich aktów prawnych dotyczących cyberbezpieczeństwa, w tym przede wszystkim w obszarze internetu rzeczy (projekt rozporządzenia EU Cyber Resilience Act został opublikowany we wrześniu 2022 roku), co sprawi, iż krajobraz regulacji cyberbezpieczeństwa będzie jeszcze bardziej złożony. Tym samym jeszcze bardziej wzrośnie znaczenie kompetencji w obszarze cyberbezpieczeństwa, przy czym będzie to obejmowało wiedzę i umiejętności techniczno-organizacyjne, jakie wymagane będą na przykład w obszarze certyfikacji, ale również kompetencje z obszaru nauk społecznych niezbędne do walki z socjotechnikami i inżynierią społeczną.

> **Obok pozytywnych efektów związanych z zastosowaniem nowych technologii, nasiliły się zjawiska negatywne, takie jak zwiększenie aktywności cyberprzestępców, czy dezinformacja**

Kompetencje o charakterze społecznym są również konieczne w walce z innym negatywnym zjawiskiem, jakim jest dezinformacja. Zgodnie z definicją Komisji Europejskiej, zawartą w komunikacie w sprawie zwalczania dezinformacji, dezinformacja to „możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną". Również i w tym obszarze podejmowane są działania, które zaowocowały przepisami rozporządzenia – tzw. Akt o usługach cyfrowych z 2022 r. – i mogą zaowocować nowymi rozwiązaniami prawnymi na poziomie krajowym. Z różnym efektem w walkę z dezinformacją zaangażowały się w ramach Kodeksu Dobrych Praktyk w zakresie dezinformacji m.in. platformy sieci społecznościowych, które w dzisiejszych czasach w znaczącym stopniu wpływają na życie społeczne, wybory polityczne i ekonomiczne wielu milionów użytkowników.

Nie sposób pominąć przepisów prawnych dotyczących platform internetowych (Akt o rynkach cyfrowych), również przyjętych w 2022 r., których celem jest wprowadzenie wyższych standardów działania platform internetowych. Konieczność przyjęcia tych aktów prawnych wskazuje, iż pojawianie się nowych modeli biznesowych, będące następstwem rozwoju nowych technologii, wymaga szerszego spojrzenia i oceny, na ile zachodzące zmiany i ich konsekwencje społecznie, a być może w ostatecznym rozrachunku również ekonomicznie, są korzystne.

Wspólne standardy – ESG

Można przyjąć, iż regulacje prawne dotyczące graczy internetowych stanowią wyraz większego trendu, jakim jest podniesienie rangi pozaekonomicznych aspektów biznesu. Pod koniec 2022 roku została uchwalona dyrektywa

2022/2464 zmieniająca dotychczasowe przepisy dotyczące sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju. Zgodnie z dyrektywą wszystkie duże jednostki oraz małe i średnie spółki giełdowe będą przedstawiać w swoim sprawozdaniu z działalności informacje na temat: kwestii środowiskowych, społecznych i praw człowieka oraz ładu korporacyjnego według wspólnych europejskich standardów sprawozdawczości, dzięki czemu zainteresowani otrzymają dostęp do porównywalnych, wiarygodnych, wysokiej jakości danych dotyczących zrównoważonego rozwoju. Da to lokalnym społecznościom możliwość wpłynięcia na politykę środowiskową przedsiębiorców, a konsumentom pozwoli podejmować decyzje zakupowe w oparciu o przesłanki wykraczające poza parametry samego produktu takie, jak różnorodność w miejscu pracy czy poszanowanie praw pracowniczych i praw człowieka. Aby sprostać zadaniu, firmy z ICT będą musiały zbudować długoterminowe strategie w obszarze zrównoważonego rozwoju. Czasu nie jest wiele, gdyż dyrektywa powinna zostać zaimplementowana do porządków prawnych poszczególnych państw członkowskich do 6 lipca 2024 roku, a jej przepisy znajdą zastosowanie w odniesieniu do dużych podmiotów już za rok 2024. Tym bardziej, iż jak wskazują wyniki zeszłorocznego raportu „Szanse i zagrożenia – odpowiedzialność społeczna i środowiskowa firm IT" przygotowanego przez INSPIRED oraz InCredibles, większość firm z sektora ICT nie przywiązuje wagi do ESG.

Sztuczna inteligencja i edukacja cyfrowa

Pisząc o trendach w prawie, nie sposób pominąć tematu sztucznej inteligencji, która prawdopodobnie w najbliższej przyszłości stanie się przedmiotem regulacji prawnej. Celem jest zapewnienie, aby systemy sztucznej inteligencji wprowadzane na rynek UE i używane w Unii były bezpieczne i zgodne z obowiązującym prawem w obszarze praw podstawowych oraz zgodne z unijnymi wartościami. Przedstawiony w 2021 roku projekt rozporządzenia wskazuje na zakazane praktyki związane ze sztuczną inteligencją i, bazując na podejściu opartym o ocenę ryzyka, wprowadza pojęcie systemów sztucznej inteligencji wysokiego ryzyka, których użycie będzie obwarowane dodatkowymi wymogami. Tym samym warunek stosowania rozwiązań opartych o sztuczną inteligencję nie będzie oparty wyłącznie o postęp technologiczny i kompetencje techniczne, ale będzie również uwzględniać czynniki prawno-społeczne.

Niezbędne jest podejmowanie działań w celu podniesienia poziomu kompetencji cyfrowych obywateli

Branżę ICT czekają liczne wyzwania związane ze sprostaniem wymogom prawnym, a kluczowym zasobem są odpowiednio przygotowani merytorycznie ludzie. Przegląd trendów w obszarze regulacji prawnych pokazuje, iż kompetencje z obszaru cyfryzacji są potrzebne nie tylko osobom o wykształceniu technicznym, ale również humanistom czy przedstawicielom nauk społecznych, od których będzie wymagane większe zaangażowanie w osiągnięcie zgodności nowych rozwiązań technicznych z przepisami prawa. Coraz większą wagę należy przykładać do edukacji cyfrowej, aby lepiej dopasować kompetencje do współczesnego rynku pracy oraz przygotować

do bezpiecznego, etycznego i umiejętnego korzystania z szans stwarzanych przez technologie cyfrowe, jak również rozwijać korzystanie z e-usług i zasobów kultury, nauki i wiedzy.

Kluczowym „zasobem" niezbędnym do powodzenia procesu transformacji są ludzie, ponieważ to oni są inicjatorami i liderami innowacji. Niestety brak kadr umożliwiających wdrożenia i mogących funkcjonować w gospodarce cyfrowej jest widoczny i odczuwalny już dziś. Wśród siedmiu największych barier wskazanych w Białej Księdze Rozwoju Przemysłu, opublikowanej przez Ministerstwo Rozwoju i Technologii 10 marca 2021 r., dwie bezpośrednio łączą się z brakiem kadr i ich niedostatecznym wykształceniem. Niezbędne jest zatem podejmowanie działań w celu podniesienia poziomu kompetencji cyfrowych obywateli. Program Rozwoju Kompetencji Cyfrowych wskazał, że główną barierą dla obywateli w korzystaniu z technologii cyfrowych nie są koszty, które wymienia 22 proc. gospodarstw domowych nieużywających sieci, 68 proc. obywateli jako główną barierę wskazuje brak potrzeb, a 52 proc. brak umiejętności.

Dodatkowym impulsem do działania w sferze podnoszenia kompetencji cyfrowych w wymiarze społecznym powinny być wyniki raportów EU DESI na 2022. Polska zajmuje 24. miejsce wśród 27 krajów Unii Europejskiej pod względem kapitału ludzkiego społeczeństwa cyfrowego, jest to identyczny wynik jak w roku 2021. Za Polską znalazły się tylko Grecja, Bułgaria i Rumunia.

Priorytety

Należy zauważyć, że potrzeby kompetencyjne obywateli są różne w zależności od etapu ich życia, pełnionych ról społecznych, wykształcenia, zamożności, a nawet miejsca zamieszkania. Specyficzne grupy wiekowe i społeczne wymagają innego rodzaju wsparcia przy projektowaniu interwencji w zakresie rozwoju kompetencji cyfrowych, a działania powinny być dostosowane do grup odbiorców pod względem ich możliwości. Należy wziąć pod uwagę to zróżnicowanie przy projektowaniu adekwatnych rozwiązań. W lipcu 2022 Kancelaria Prezesa Rady Ministrów przedstawiła projekt Programu rozwoju kompetencji cyfrowych. W dokumencie wskazano pięć priorytetów istotnych dla rozwoju kompetencji cyfrowych i przewidziano je w ramach działań. Jako priorytety określono: rozwój edukacji cyfrowej (dotyczy dzieci w wieku przedszkolnym, uczniów, studentów, nauczycieli i edukatorów), zapewnienie każdemu możliwości rozwoju kompetencji cyfrowych (użytkownicy technologii cyfrowych, osoby stawiające pierwsze kroki w świecie cyfrowym), wsparcie kompetencji cyfrowych pracowników różnych sektorów (pracownicy, osoby zarządzające, przedsiębiorcy, pracownicy sektora publicznego), rozwój zaawansowanych kompetencji cyfrowych (specjaliści ICT) oraz wzmocnienie zarządzania rozwojem kompetencji cyfrowych. Działania zaproponowane w programie w obszarze edukacji cyfrowej są dostosowane do poszczególnych grup docelowych z uwzględnieniem ich potrzeb i przedstawiają konkretne rozwiązania i działania.

Kompetencje cyfrowe

W systemie oświaty na poziomie szkół podstawowych i średnich od 2017 roku podjęto dużo wysiłków mających na celu rozwój i zmiany edukacji informatycznej. Na etapie szkoły podstawowej i ponadpodstawowej kształtowane są zarówno podstawowe, jak i bardziej zaawansowane kompetencje cyfrowe, co jest szczególnie ważne w szybko zmieniających się warunkach. Wobec mnogości dostępnych narzędzi technologicznych, nowych sposobów

nauczania, konieczna jest edukacja uczniów, ale również aktualizacja wiedzy nauczycieli. Nauczyciele ubiegający się o stopnie awansu zawodowego zobligowani byli do podnoszenia swoich kompetencji cyfrowych oraz do wykazania się umiejętnością korzystania w swojej pracy z ICT. Potwierdzają to wyniki raportu NIK z 2021 roku „Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa".

> **Nieodzowne są działania zarówno w obszarze prawodawstwa w zakresie technologii informacyjno-komunikacyjnych, jak również rozwój edukacji cyfrowej**

Ważne jest ciągłe doskonalenie wszystkich elementów systemu edukacji, aby młodzi ludzie byli jak najlepiej przygotowani do życia w społeczeństwie cyfrowym. Przepisy nowej podstawy programowej odnoszą się również do respektowania prywatności informacji, ochrony danych, praw własności intelektualnej oraz bezpiecznego poruszania się w cyberprzestrzeni. Należy zadbać również o kształtowanie umiejętności związanych z szeroko pojętą higieną cyfrową, etyką cyfrową oraz bezpiecznym korzystaniem z rozwiązań cyfrowych.

Jeśli chodzi o edukację akademicką, NIK zwraca uwagę, że do tej pory nie zostały przeprowadzone przez ministra właściwego do spraw szkolnictwa wyższego analizy potrzeb w zakresie podnoszenia poziomu kompetencji cyfrowych kadry akademickiej. Nie zostały również przyjęte standardy kształcenia. Absolwenci szkół wyższych, niezależnie od kierunku studiów, wchodząc na rynek pracy, powinni być wyposażeni w kompetencje zawodowe, ale również w uniwersalne kompetencje cyfrowe dotyczące cyberbezpieczeństwa, ochrony danych osobowych oraz wykorzystania nowych technologii w nauce i pracy. Jak wskazuje raport NIK, minister nie opracował koncepcji dotyczącej przygotowania i wykorzystania cyfrowych materiałów edukacyjnych na uczelniach oraz podnoszenia kompetencji cyfrowych kadry akademickiej, powołując się na tzw. autonomię uczelni. Uczelnie powinny spełniać rolę liderów rozwijających kompetencje cyfrowe. Przedstawiony przez Kancelarię Prezesa Rady Ministrów w lipcu 2022 roku Projekt Programu Rozwoju Kompetencji Cyfrowych w obszarze szkół wyższych zakłada dostosowanie standardów kształcenia, w tym standardów kształcenia nauczycieli, do wymogów współczesnego świata i rozwoju technologii cyfrowych oraz wsparcie rozwoju zaawansowanych kompetencji cyfrowych w szkołach wyższych. Wprowadzenie zaproponowanych rozwiązań będzie wymagało od środowiska akademickiego zmian przepisów powszechnie obowiązujących oraz wewnętrznych na uczelniach.

Obserwujemy dynamiczny rozwój w zakresie technologii informacyjno-komunikacyjnych, a pandemia i konieczność przejścia na pracę i nauczanie zdalne pokazały, jak ważne, a wręcz niezbędne, jest korzystanie z narzędzi ICT. Nieodzowne są działania zarówno w obszarze prawodawstwa w zakresie technologii informacyjno-komunikacyjnych, jak i rozwój edukacji cyfrowej.

Skuteczne korzystanie z kompetencji cyfrowych ma umożliwić obywatelom wykorzystywanie technologii cyfrowych w różnych obszarach oraz odnoszenie dzięki kompetencjom korzyści i podnoszenie jakości życia. Celem edukacji rozwoju kompetencji cyfrowych jest budowanie społeczeństwa cyfrowego świadomego korzyści, ale i zagrożeń płynących z wykorzystania technologii cyfrowych.

EDUMIXER, CZYLI JAKICH KOMPETENCJI NAM POTRZEBA

Forum Współpracy Edukacji i Biznesu to konferencja, która na stałe wpisała się w kalendarz wydarzeń branżowych dla sektora IT oraz telekomunikacji i cyberbezpieczeństwa, skupiając zarówno praktyków, jak i przedstawicieli środowiska akademickiego.

Irmina Zakrzewska
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne

EduMixer, czyli Forum Współpracy Edukacji i Biznesu, to jedno z najważniejszych cyklicznych wydarzeń dla branży informatycznej, telekomunikacji i cyberbezpieczeństwa odbywających się w Polsce. Konferencja organizowana jest przez Polską Izbę Informatyki i Telekomunikacji (PIIT) we współpracy z Polskim Towarzystwem Informatycznym (PTI) w ramach Sektorowej Rady ds. Kompetencji Informatyka oraz Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

Konferencja, od początku organizowana przez PTI oraz PIIT, jest flagowym elementem spotkania środowisk, które są reprezentowane w Radach Sektorowych, czyli biznesu, edukacji, placówek zainteresowanych edukacją teleinformatyczną i administracji publicznej. Wspólny dialog jest niezbędny, aby przygotować programy szkolenia formalnego i pozaformalnego w sposób spójny i odpowiadający potrzebom rynku pracy. Problem z inicjatywami i przedsięwzięciami edukacyjnymi, które mają podnosić poziom kompetencji w obszarze technologii cyfrowych, jest ciągle obecny. Cykliczne spotkanie w gronie ekspertów i praktyków jest niezwykle istotne i przyczynia się do zmian w poszczególnych segmentach działań edukacyjnych.

Dopasujmy programy i praktyki

EduMixer to bardzo ważne wydarzenie dla przyszłości rynku teleinformatycznego, telekomunikacyjnego i obszarów cyberbezpieczeństwa. Jest związane z kompetencjami, czyli z tym, czego najbardziej potrzebują przedsiębiorcy i przyszłość rynku telekomunikacyjnego

w Polsce. Jest to platforma współpracy biznesu i edukacji, w tym edukacji wysokiej. Podczas konferencji eksperci zastanawiają się, jakie kompetencje będą potrzebne w przyszłości, jakie umiejętności należy rozwijać, a także co będzie decydowało o przyszłości, skuteczności i efektywności polskiej gospodarki opartej o teleinformatykę.

Głównym celem Forum Współpracy Edukacji i Biznesu jest dialog pomiędzy biznesem a instytucjami naukowo-dydaktycznymi, aby jak najlepiej dopasować przyszłe programy i praktyki do potrzeb współczesnego rynku pracy. Współpraca w obu tych sektorach jest niezbędna do dalszego rozwoju uczelni oraz wzmacniania konkurencyjności polskich przedsiębiorców poprzez możliwości zatrudniania dobrze wyspecjalizowanych kadr.

Co można zyskać

Korzyści wynikające z udziału w konferencji EduMixer to:

- spotkania z profesjonalistami w dziedzinie informatyki oraz telekomunikacji
- zdobycie nowej wiedzy i aktualizowanie obecnej w zakresie współpracy edukacji z branżą teleinformatyczną
- wymiana doświadczeń poprzez udział w dyskusjach i rozmowy w kuluarach
- zapoznanie się z dobrymi praktykami współpracy edukacji z biznesem
- nawiązywanie nowych znajomości z przedstawicielami różnych środowisk
- możliwość nawiązania współpracy ze szkołami oraz uczelniami

EduMixer jest skierowany do reprezentantów firm z sektorów IT oraz telekomunikacji i cyberbezpieczeństwa, a także przedstawicieli uczelni, szkół zawodowych i branżowych oraz reprezentantów edukacji, uczniów i studentów, studenckich biur karier, kół naukowych i innych ekspertów czy praktyków rynkowych. Chodzi o to, by pomóc w wypracowaniu wzajemnego modelu współpracy tych sektorów oraz wskazać kluczowe potrzeby w branży ICT.

Początkowo wydarzenie było organizowane przez PIIT i PTI w ramach Sektorowej Rady ds. Kompetencji Informatyka, jednakże od rozpoczęcia działalności SRTCB Rada ta włączyła się w aktywny sposób w organizowanie i promowanie tej konferencji.

Pierwsza edycja konferencji EduMixer zorganizowana przez Radę ds. Kompetencji Sektora IT odbyła się w 2017 roku. Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo zainaugurowała swoje działania w lutym 2020 roku i w naturalny sposób stała się współorganizatorem tej cyklicznej imprezy łączącej edukację i biznes. Od tej edycji program EduMixera ma przewidywalny charakter. Pierwszy dzień to tematy związane z zagadnieniami sektora IT. Podczas drugiego dnia poruszane są tematy dotyczące sektora telekomunikacji i cyberbezpieczeństwa. Z kolei trzeciego dnia odbywają się warsztaty merytoryczne, podczas których uczestnicy mają szansę wysłuchać ciekawych prelekcji, a w formule warsztatowej porozmawiać o ważnych dla nich i dla sektora kwestiach, zmianach w ustawodawstwie czy o dobrych praktykach wynikających ze współpracy na linii edukacja – biznes.

W dalszej części omówione zostaną edycje, które współorganizowała Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

IV edycja konferencji

EduMixer 2020 to pierwsza edycja współorganizowana przez Sektorową

Radę ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, a czwarta już edycja Forum Współpracy Edukacji i Biznesu. Wydarzenie odbyło się w trudnym pandemicznym roku, i podobnie jak wiele innych, jako konferencja online. Łącznie w IV edycji EduMixera wzięło udział blisko 200 osób.

Uczestnicy konferencji – przedstawiciele administracji, specjaliści, reprezentanci firm oraz uczelni i placówek edukacyjnych rozmawiali o współpracy nauki z biznesem. Głównym tematem dyskusji podczas drugiego dnia konferencji poświęconego obszarom telekomunikacji i cyberbezpieczeństwa była identyfikacja potrzeb kompetencyjnych, budowanie partnerstwa i poszukiwanie modelu współpracy środowiska naukowego i edukacyjnego z firmami technologicznymi.

Podczas paneli dyskutowano o nowych potrzebach kompetencyjnych, jakie pojawią się w wyniku zmian w Krajowym Systemie Cyberbezpieczeństwa oraz w nowym prawie komunikacji elektronicznej, a także o tym, jak uczestnicy konferencji wyobrażają sobie idealny, trójstronny model funkcjonowania między szkołami średnimi, uczelniami wyższymi i firmami.

Uczestnicy wysłuchali wystąpień ekspertów i praktyków branżowych, którzy przybliżyli m.in.:

- Krajowy System Certyfikacji Cyberbezpieczeństwa i system certyfikacyjny urządzeń szkieletu sieci i urządzeń końcowych;
- zmiany w potrzebach rekrutacyjnych i kompetencyjnych w firmie telekomunikacyjnej oraz
- cyberbezpieczeństwo w zderzeniu z mentalnością ogółu, czyli jak turniej Cybersecurity Challenge PL2020 doprowadził do powstania Wojewódzkich Cyber Labów.

Ważnym elementem obu dni EduMixera było wystąpienie Animatora Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo o istocie podpisywania sektorowych porozumień między edukacją a biznesem oraz prezentacje o obszarach takiej współpracy i korzyściach z niego płynących dla zaangażowanych stron. Swoim doświadczeniem na tym polu podzielił się Tomasz Królikowski – Prorektor ds. Studenckich z Politechniki Koszalińskiej i Piotr Bartkiewicz – dyrektor w firmie GlobalLogic. A o swoich przyszłych planach opowiedzieli Grzegorz Mazurek, rektor Akademii Leona Koźmińskiego i Tomasz Stojek, technical services director w Senetic S.A.

Trzeci dzień to, zgodnie z ramowym planem konferencji, warsztaty merytoryczne. Pierwszy warsztat przygotowała i poprowadziła firma IS-Wireless, która przybliżyła potrzeby kompetencyjne w projektowaniu i budowie sieci 5G. W czasie drugiego warsztatu na temat cyberbezpieczeństwa w obszarze internetu rzeczy uczestnicy zastanawiali się wspólnie z NASK i NASK SA nad koniecznością certyfikacji rozwiązań i urządzeń.

V edycja konferencji

W 2021 r. od 1 do 3 grudnia odbywała się, również online, V edycja konferencji EduMixer. Pierwsze dni grudnia upłynęły pod hasłem: „Transformacja cyfrowa. Wyzwanie dla edukacji, rynku pracy i przedsiębiorców”. Podczas V Forum Współpracy Edukacji z Biznesem EduMixer zostały omówione zagadnienia związane z potrzebami kompetencyjnymi na dynamicznie zmieniającym się rynku IT oraz telekomunikacji i cyberbezpieczeństwa. Swoją wiedzą podzielili się specjaliści, reprezentanci firm oraz uczelni i placówek edukacyjnych.

Dyskusja panelowa „Jak zmiany w Krajowym Systemie Cyberbezpieczeństwa oraz nowym

prawie komunikacji elektronicznej wpłyną na potrzeby kompetencyjne?" otworzyła dzień poświęcony wyzwaniom w sektorze telekomunikacji i cyberbezpieczeństwa.

Następnie odbyły się prezentacje dotyczące:

- Krajowego Systemu Certyfikacji Cyberbezpieczeństwa – sposobu na weryfikację najbardziej wrażliwego ogniwa w systemie bezpieczeństwa,
- roli sektorowych porozumień w rozwoju współpracy pomiędzy edukacją a biznesem TCB,
- tego, jakich pracowników potrzebujemy w nowoczesnej firmie telekomunikacyjnej i jakie działania podejmujemy, żeby mieć wpływ na edukację naszych przyszłych kadr,
- systemu certyfikacyjnego urządzeń szkieletu sieci i urządzeń końcowych – jaki powinien być i czy kompetencje w tym zakresie są wystarczające,
- współpracy uczelni z biznesem – ramowe porozumienie i case study,
- cyberbezpieczeństwa w zderzeniu z mentalnością ogółu – od turnieju Cybersecurity Challenge PL2020 do Wojewódzkich Cyber Labów.

Andrzej Dulka (z lewej) z Grzegorzem Karasiewiczem, dziekanem Wydziału Zarządzania podczas EduMixera 2022 na Uniwersytecie Warszawskim

Podczas konferencji odbyła się dyskusja panelowa dotycząca transformacji edukacji. W poszukiwaniu idealnego, trójstronnego modelu współpracy, omówiono główne wnioski płynące z raportu o potrzebach kompetencyjnych, który został przygotowany przez Sektorową Radę ds. Kompetencji Informatyka oraz Sektorową Radę ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo w kontekście skutków pandemii, a także trendy i wymagania, które będą kreować najbliższą przyszłość sektora ICT.

Trzeci dzień EduMixera, podobnie jak w poprzednim roku, poświęcony był warsztatom merytorycznym dla sektora Telekomunikacja i Cyberbezpieczeństwo. Dwa główne tematy, wokół których przeprowadzono rozmowy, to: „Sektorowa Rama Kwalifikacji – rekomendacje w obszarze aktualizacji Ramy Kwalifikacji dla sektora Telekomunikacji" oraz „Zmiany w ustawie o Krajowym Systemie Cyberbezpieczeństwa".

EduMixer, jak co roku, został skierowany do reprezentantów firm z sektorów IT oraz telekomunikacji i cyberbezpieczeństwa, a także przedstawicieli uczelni, szkół zawodowych i branżowych, reprezentantów edukacji nieformalnej, uczniów i studentów, studenckich biur karier, kół naukowych i innych ekspertów oraz praktyków rynkowych, aby pomóc w wypracowaniu wzajemnego modelu współpracy tych sektorów, jak również wskazać kluczowe potrzeby w branży ICT.

VI edycja konferencji

Kolejna, VI już, edycja Forum Współpracy Edukacji i Biznesu, odbywała się między 18 a 20 października 2022 r. Konferencję prowadzono w sposób hybrydowy: stacjonarnie na Wydziale Zarządzania Uniwersytetu Warszawskiego, a dla pozostałych uczestników – online.

Tematem przewodnim tej edycji było „Bezpieczeństwo w teleinformatyce. Wyzwanie dla edukacji, rynku pracy i przedsiębiorców". Eksperci po raz kolejny

rozmawiali o współpracy nauki z biznesem, a także wyzwaniach kompetencyjnych, których efektem będzie stworzenie modelu współpracy środowiska naukowego z firmami technologicznymi.

Głównym celem konferencji było wypracowanie propozycji zmian w programach kształcenia, uwzględniających rozwój technologiczny oraz potrzeby dynamicznego rynku pracy, wymiana doświadczeń i transfer najlepszych praktyk pomiędzy sektorem edukacji formalnej i pozaformalnej czy przedsiębiorcami i instytucjami. Na konferencji zauważono, jak istotna jest poprawa współpracy i zbudowanie partnerstwa pomiędzy podmiotami kształtującymi rynek pracy, co jest możliwe dzięki identyfikacji potrzeb kompetencyjnych poszczególnych grup specjalistów z obszarów informatyki, telekomunikacji i cyberbezpieczeństwa. Końcowym efektem są rekomendacje konkretnych rozwiązań, które zapewnią potrzebne kompetencje zainteresowanym podmiotom.

Podczas drugiego dnia konferencji rozmawiano o wyzwaniach dla sektora telekomunikacji i cyberbezpieczeństwa oraz o bezpieczeństwie w komunikacji elektronicznej. Paneliści dyskutowali m.in. o:

- wyzwaniach, jakie stawiają nowe technologie przed biznesem w obszarze telekomunikacji;
- usługach telekomunikacyjnych w obliczu sytuacji kryzysowych;
- bezpieczeństwie informacji i dezinformacji;
- sposobach zarządzania ryzykiem w sektorze telekomunikacji i cyberbezpieczeństwa.

W trakcie warsztatów merytorycznych dla sektora telekomunikacji i cyberbezpieczeństwa, które tradycyjnie odbyły się ostatniego dnia konferencji, omówiono kwestie obowiązków związanych z Krajowym Systemem Bezpieczeństwa, a także nowe obowiązki przedsiębiorców związane z Digital Services Act (DSA) i Digital Markets Act (DMA) oraz ich wpływ na nowe potrzebne kompetencje.

Dr Agnieszka Besiekierska – adwokat i adiunkt w Katedrze Prawa Informatycznego Wydziału Prawa przedstawiła obowiązki związane z Krajowym Systemem Cyberbezpieczeństwa. Z kolei Bartosz Lech – Head of Location-Based Services Department w Globema zaprezentował warsztat dobrych praktyk współpracy biznesu z uczelnią.

Nad nowymi obowiązkami przedsiębiorców wynikającymi z Digital Services Act (DSA) oraz tym, jakie kompetencje będą potrzebne w świetle nadchodzących zmian, pochylili się dr Piotr Wasilewski – adwokat i partner w Traple Konarski Podrecki i Wspólnicy oraz Arkadiusz Baran, adwokat i counsel w tej samej kancelarii.

O dobrych praktykach współpracy pomiędzy biznesem a edukacją na przykładzie działalności Sektorowych Rad ds. Kompetencji (Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo) opowiadał Maciej Wnuk, animator warsztatów Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.

Na stałe w krajobrazie

EduMixer to konferencja, która na stałe wpisała się w kalendarz wydarzeń branżowych dla sektora IT oraz telekomunikacji i cyberbezpieczeństwa. Skupia wokół siebie zarówno praktyków z sektora, jak i przedstawicieli środowiska akademickiego, szkół średnich i wyższych. Panelistami i moderatorami są również przedstawiciele ministerstw i urzędów, które w swojej bieżącej pracy zajmują się tematyką cyberbezpieczeństwa. Uczestnikami są też reprezentanci firm z sektora ICT,

przedstawiciele administracji, samorządów, uczelni, szkół zawodowych i branżowych.

Warto podkreślić olbrzymią rolę konferencji EduMixer jako platformy do rozmowy, wymiany informacji i generowania pomysłów, czyli miejsca idealnego do rozwoju, wymiany doświadczeń i nawiązania współpracy, również dzięki realizowanym podczas wydarzenia sesjom networkingowym, które cieszą się dużym zainteresowaniem. Dynamika zmian w dziedzinie rozwoju nowych technologii wymaga nabywania oraz ciągłego doskonalenia kompetencji, a EduMixer poprzez liczne debaty eksperckie w znacznym stopniu to ułatwia.

O wysokiej randze konferencji świadczą instytucje, które objęły ją patronatami honorowymi. Są wśród nich: Urząd Komunikacji Elektronicznej (2020), Przemysław Czarnek, minister edukacji i nauki; Janusz Cieszyński, sekretarz stanu w Kancelarii Prezesa Rady Ministrów ds. Cyfryzacji; Piotr Nowak, minister rozwoju i technologii; Jacek Oko, prezes Urzędu Komunikacji Elektronicznej oraz Polska Agencja Rozwoju Przedsiębiorczości (2021), Ministerstwo Rozwoju i Technologii, Urząd Komunikacji Elektronicznej czy Polska Agencja Rozwoju Przedsiębiorczości (2022). Wśród patronów medialnych edycji 2020-2022 znaleźli się: Personel Plus, Digital&more, Radio Kampus, My Company Polska (2020); Digital&more, IT Reseller, ITWiz, My Company Polska, Personel Plus, Radio Kampus oraz Teleinfo24 (2021); Teleinfo24, My Company Polska, Digital&more, Radio Kampus, ITWiz, Personel Plus oraz Brands IT (2022).

To wydarzenie, podczas którego rozmawia się o wyzwaniach, szansach i zagrożeniach dla branży, o tym, co ważnego dzieje się w najnowszych rozwiązaniach technologicznych, jak przeciwdziałać cyberzagrożeniom, a także wymienia się doświadczeniami. Co najważniejsze, EduMixer to prawdziwa platforma współpracy edukacji i biznesu, gdzie można nawiązać relacje, które mogą być podstawą do dalszej współpracy dla branży, rozwoju kompetencji oraz w sposób naturalny być platformą zapoznawczą dla firm i szkół, które dzięki współpracy mogą kreować przydatne programy nauczania, a te przyczynią się do lepszej synergii i wyższego poziomu świadczonych usług.

Sektorowa Rada ds. Kompetencji Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo – inicjując i biorąc udział w wielorakich przedsięwzięciach związanych przede wszystkim z tematyką kompetencji w obszarze informatyki, telekomunikacji i cyberbezpieczeństwa – pomaga harmonizować ofertę edukacyjną z wymaganiami rynku pracy IT i TCB. Członkowie Rady reprezentują wszystkich interesariuszy sektora i zapewniają możliwość dotarcia do różnych środowisk, zarówno w obszarze biznesu, jak i edukacji.

Kolejna, już VII, edycja konferencji EduMixer odbędzie się w maju 2023 r. W chwili wysyłania publikacji do druku nie ma jeszcze ogłoszonego programu wydarzenia. Po wszelkie szczegóły oraz najnowsze informacje dotyczące projektu zapraszamy na stronę wydarzenia www.edumixer.pl oraz do mediów społecznościowych projektu.

Współpraca Joachim Łącki

Wojciech Maciejczak (z lewej) i Piotr Bartosiak podczas EduMixera 2022

RYNEK PRACY W KONTEKŚCIE SKUTKÓW PANDEMII KORONAWIRUSA

Jakie potrzeby kompetencyjne w firmach teleinformatycznych ujawniła pandemia koronawirusa? Jakie kwalifikacje będą potrzebne? Informacji na ten temat dostarczają wyniki wspólnego badania Rad Sektorowych – Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo.

Dariusz Chełstowski
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne
Andrzej Gontarz
Sektorowa Rada ds. Kompetencji – Informatyka, Polskie Towarzystwo Informatyczne

Pandemia koronawirusa zmusiła prawie wszystkie przedsiębiorstwa i organizacje do zmiany niemalże z dnia na dzień sposobów swojego działania. Szczególne wyzwania pojawiły się przed firmami z sektora ICT, na których usługi i produkty wzrosło mocno zapotrzebowanie. Informatyka i telekomunikacja stały się w warunkach pandemicznych podstawą funkcjonowania całej gospodarki. Intensyfikacja procesów cyfryzacji skutkowała jednocześnie większymi wyzwaniami w obszarze cyberbezpieczeństwa.

Sektorowa Rada ds. Kompetencji – Informatyka (IT) oraz Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo (TCB) sprawdziły, w jaki sposób pandemia i jej skutki wpłynęły na potrzeby kompetencyjne w organizacjach z reprezentowanych przez obie Rady sektorów. Zorganizowane wspólnie badanie miało na celu identyfikację kluczowych obszarów działań podejmowanych w warunkach pandemicznych i związanych z nimi strategicznych potrzeb kompetencyjnych. Chodziło o zdefiniowanie zarówno potrzeb ujawnionych już przez pandemię, jak i oczekiwanych w związku z prognozowanymi skutkami sytuacji pandemicznej.

Wyniki badania mogą stanowić podstawę do tworzenia scenariuszy dla przyszłych działań szkoleniowych, edukacyjnych i doradczych w kontekście zapewnienia potrzebnych kwalifikacji i kompetencji, umożliwiających sprawne funkcjonowanie biznesu w obliczu istniejących zakłóceń oraz prognozowanych skutków pandemii. Celem badania było ustalenie, czy i jakie kompetencje okazały się niezbędne, a których brakuje, bądź będzie brakować w najbliższym czasie, w kontekście spodziewanych konsekwencji pandemii dla sektorów IT oraz TCB.

Prezentujemy wybrane wyniki badania w obu sektorach. Było ono realizowane w dwóch edycjach. Pierwsza miała miejsce w czerwcu 2021 roku, a druga na przełomie lutego i marca 2022 r. Z raportami zawierającymi pełne wyniki badania można się zapoznać na stronach rad: srit.radasektorowa.pl, srtcb.radasektorowa.pl.

TABELA 1. Jak duże znaczenie mają dla funkcjonowania firmy poszczególne obszary zadań obecnie – dane zbiorcze (sektory IT i TCB razem: suma odpowiedzi „kluczowe" + „duże znaczenie") dla ogółu badanych z I i II tury badania*

Obszary zadań	I tura badania („kluczowe znaczenie" + „duże znaczenie")	II tura badania („kluczowe znaczenie" + „duże znaczenie")
Utrzymanie ciągłości działania firmy	69%	81% ↑
Zapewnienie bezpieczeństwa danych, aplikacji i sieci (połączeń) w związku z wprowadzeniem pracy zdalnej, zdalnej obsługi klientów i świadczenia usług na odległość	65%	79% ↑
Zapewnienie odpowiednich zasobów technicznych dla realizacji pojawiających się zadań	57%	79% ↑
Dostosowanie podejmowanych działań do regulacji prawnych	55%	79% ↑
Obsługa klientów w trybie zdalnym, współpraca z klientami w zakresie realizacji projektów, dostarczania produktów, świadczenia usług, wywiązywania się z umów	61%	76% ↑
Zapewnienie odpowiednich zasobów ludzkich dla realizacji pojawiających się zadań, w tym pozyskanie kompetencji odpowiednich dla działań wynikających ze skutków pandemii	58%	76% ↑
Organizacja pracy zdalnej w firmie	55%	70% ↑

** Strzałki w górę wskazują na wyższy odsetek sumy odpowiedzi „zdecydowanie tak" i „raczej tak" w stosunku do pierwszej edycji badania.*
Źródło: Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa. Raport zbiorczy z badania dotyczącego działań antycovidowych w sektorach: Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo, Edycja II, Warszawa 2022.

Sektor informatyczny (IT)

Chociaż firmy informatyczne, jak wszystkie inne, odczuły bezpośrednio i wyraźnie skutki pandemii, to z badania wynika, że wprowadzane przez nie zmiany nie były zbyt radykalne. 42 proc. uczestniczących w pierwszej edycji badania podmiotów określiło wymuszone przez sytuację pandemiczną zmiany dotychczasowego modelu działania jako umiarkowane. Dla 25 proc. firm zmiany te były duże i bardzo duże, a dla 22 proc. małe i bardzo małe. Na taką ocenę sytuacji wpłynęły z pewnością doświadczenia z wcześniej już stosowanej na znaczną skalę pracy zdalnej i realizacji licznych projektów w rozproszonych zespołach.

Prawie połowa (49 proc.) respondentów w pierwszej edycji badania była jednak zdania, że wprowadzone w wyniku pandemii zmiany sposobu funkcjonowania firmy będą już miały trwały charakter. Jednym z ważnych, podlegających takim przekształceniom, obszarów są kompetencje pracownicze. Większość odpowiadających (62 proc.) uważała, że modyfikacje wprowadzone wskutek pandemii wpłynęły na zmianę kompetencji pracowników co najmniej w umiarkowanym lub większym stopniu. Dla 34 proc. odpowiadających zmiany były małe lub bardzo małe, ale jednak również zauważalne. Natomiast w drugiej edycji badania trzy czwarte respondentów

(75 proc.) nie zauważało już wpływu pandemii na konieczność zmiany kompetencji pracowników. Około połowa (47 proc.) firm, które taką potrzebę wskazywały, była zdania, że pandemia wpływa na ten obszar działalności w raczej dużym zakresie, a druga połowa (53 proc.) była zdania, że w umiarkowanym.

W chwili pojawienia się pandemii koronawirusa w 2020 roku firmy z sektora IT, jak pokazały wyniki pierwszej edycji badania,

Informatyka i telekomunikacja stały się w warunkach pandemicznych podstawą funkcjonowania całej gospodarki

skupiły się przede wszystkim na zapewnieniu bezpieczeństwa danych, aplikacji i sieci w związku z wprowadzeniem pracy zdalnej. To był obszar działań o największym – dużym i kluczowym – znaczeniu dla zdecydowanej większości, bo aż 72 proc. uczestników pierwszej edycji badania. Równie ważne było zapewnienie ciągłości działania firmy – na to zadanie wskazało 71 proc. respondentów.

W odpowiedzi na zaistniałą sytuację nieco ponad połowa (52 proc.) przedsiębiorstw dokonała aktualizacji polityki cyberbezpieczeństwa. Zostały opracowane i wdrożone procedury bezpieczeństwa dostosowane do wymogów sytuacji pandemicznej i jej skutków. W 43 proc. przypadków firmy zajęły się również zapewnieniem adekwatnych do warunków pandemicznych, technicznych środków bezpieczeństwa firmowych zasobów.

Natomiast po ponad roku od wprowadzenia stanu pandemii, czyli w momencie przeprowadzania ankiety do pierwszej edycji badania (czerwiec 2021), najważniejszym zadaniem dla trzech czwartych członków sektora IT (76 proc. odpowiedzi) było utrzymanie ciągłości działania firmy. 72 proc. respondentów wskazało również na priorytetowe nadal traktowanie zapewnienia bezpieczeństwa danych, aplikacji i sieci w związku z prowadzeniem pracy zdalnej. Z kolei w planach rozwoju firm strategicznymi kierunkami działań były przede wszystkim: zapewnienie klientom elastycznego dostępu do sieci, zasobów i usług (71 proc.) oraz identyfikacja technologii i rozwiązań z największym potencjałem na przyszłość (69 proc.).

Natomiast w chwili realizacji drugiej edycji badania (luty/marzec 2022) za najważniejsze zadanie dla funkcjonowania przedsiębiorstw zostało uznane dostosowanie podejmowanych działań do regulacji prawnych – 87 proc. dla połączonych odpowiedzi „duże znaczenie” i „kluczowe znaczenie”. Za istotne dla sprawnego działania firm uznano również: zapewnienie odpowiednich zasobów technicznych dla realizacji pojawiających się zadań (85 proc. odpowiedzi) oraz zapewnienie bezpieczeństwa danych, aplikacji i sieci (połączeń) w związku z wprowadzeniem pracy zdalnej, zdalnej obsługi klientów i świadczenia usług na odległość (84 proc.). Najmniejsza grupa respondentów (77 proc.) za ważny obszar funkcjonowania przedsiębiorstwa w pierwszym kwartale 2022 roku uznała organizację pracy zdalnej w przedsiębiorstwie. W porównaniu z pierwszą edycją badania w znaczący stopniu wzrosło znaczenie dostosowania podejmowanych działań do regulacji prawnych – o 17 proc. więcej wskazań dla tego obszaru. Jednocześnie na znaczeniu, chociaż już w mniejszym stopniu, zyskały również wszystkie inne wymienione w ankiecie obszary funkcjonowania firm z sektora IT.

TABELA 2. Jak duże znaczenie mają dla funkcjonowania firmy poszczególne obszary zadań obecnie – dane zbiorcze (sektor IT: suma odpowiedzi „kluczowe" + „duże znaczenie") dla ogółu badanych z I i II tury badania*

Obszary zadań	I tura badania („kluczowe znaczenie" + „duże znaczenie")	II tura badania („kluczowe znaczenie" + „duże znaczenie")
Dostosowanie podejmowanych działań do regulacji prawnych	60%	87% ↑
Zapewnienie odpowiednich zasobów technicznych dla realizacji pojawiających się zadań	58%	85% ↑
Zapewnienie bezpieczeństwa danych, aplikacji i sieci (połączeń) w związku z wprowadzeniem pracy zdalnej, zdalnej obsługi klientów i świadczenia usług na odległość	72%	84% ↑
Obsługa klientów w trybie zdalnym, współpraca z klientami w zakresie realizacji projektów, dostarczania produktów, świadczenia usług, wywiązywania się z umów	64%	82% ↑
Utrzymanie ciągłości działania firmy	76%	82% ↑
Zapewnienie odpowiednich zasobów ludzkich dla realizacji pojawiających się zadań, w tym pozyskanie kompetencji odpowiednich dla działań wynikających ze skutków pandemii	60%	81% ↑
Organizacja pracy zdalnej w firmie	55%	77% ↑

** Strzałki w górę wskazują na wyższy odsetek sumy odpowiedzi „zdecydowanie tak" i „raczej tak" w stosunku do pierwszej edycji badania. Źródło: Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa. Raport zbiorczy z badania dotyczącego działań antycovidowych w sektorach: Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo, Edycja II, Warszawa 2022.*

Największe znaczenie miały dla przedsiębiorstw w połowie 2021 roku kompetencje związane z: zapewnieniem bezpieczeństwa kanałów komunikacji elektronicznej (średnia: 3,94 na skali 1-5), zarządzaniem informacją (3,92), tworzeniem, rozwojem i zarządzaniem oprogramowaniem (3,91) oraz z zarządzaniem zasobami danych (3,88) i integracją systemów (3,86). Z kolei w perspektywie najbliższych 12 miesięcy największe znaczenie również będzie miało zapewnienie bezpieczeństwa kanałów komunikacji elektronicznej (3,88), a także obsługa klienta, w tym m.in. świadczenie pomocy technicznej w trybie zdalnym (3,85).

Natomiast w pierwszym kwartale 2022 roku największe znaczenie firmy z sektora IT przypisywały kompetencjom związanym z tworzeniem, rozwojem i zarządzaniem oprogramowaniem (średnia ocen 4,28 na skali 1-5). W dalszej kolejności wskazywano: utrzymanie i rozwój infrastruktury (4,25), zarządzanie zasobami danych (4,25 oraz integrację systemów – 4,21), jak również implementowanie, konfigurowanie, administrowanie i zabezpieczanie systemów obiegu dokumentów (4,21).

TABELA 3. Kluczowe kompetencje w kontekście skutków pandemii COVID-19 – sektor IT: obecnie i w ciągu najbliższych 12 miesięcy*

Kompetencje kluczowe w kontekście skutków pandemii COVID-19	Obecnie (wśrednia)	W najbliższych 12 miesiącach (średnia)
Tworzenie, rozwój i zarządzanie oprogramowaniem	4,28 ↑	4,19 ↑
Utrzymanie i rozwój infrastruktury ICT	4,25 ↑	4,18 ↑
Zarządzanie zasobami danych	4,25 ↑	4,23 ↑
Integracja systemów	4,21 ↑	4,11 ↑
Implementowanie, konfigurowanie, administrowanie i zabezpieczanie systemów obiegu dokumentów	4,21 ↑	4,10 ↑
Zarządzanie procesami ICT na styku technologii i biznesu	4,20 ↑	4,14 ↑
Obsługa klienta, w tym również świadczenie usług pomocy technicznej, w trybie zdalnym	4,20 ↑	4,10 ↑
Tworzenie i wdrażanie nowych metod zapewnienia ciągłości działania firmy w sytuacji nagłych zagrożeń	4,19 ↑	4,09 ↑
Zestawianie łączy do bezpiecznej transmisji dźwięku, obrazu i danych	4,17 ↑	4,17 ↑
Zapewnienie bezpieczeństwa kanałów komunikacji elektronicznej, w tym należyta weryfikacja tożsamości stron komunikacji	4,17 ↑	4,22 ↑
Zarządzanie informacją	4,17 ↑	4,16 ↑
Projektowanie, implementacja, administrowanie i zabezpieczanie rozwiązań chmurowych oraz migracja danych do chmury	4,16 ↑	4,14 ↑
Implementowanie, konfigurowanie, administrowanie i zabezpieczanie platform e-learningowych	4,14 ↑	4,07 ↑
Zarządzanie zmianą	4,14 ↑	4,14 ↑
Instalowanie, konfigurowanie, administrowanie i zabezpieczanie systemów do pracy zdalnej i telekonferencji	4,14 ↑	3,99 ↑
Analiza ryzyk w zmiennym, niestabilnym środowisku pracy i prowadzenia biznesu	4,10 ↑	4,16 ↑
Analiza danych i jej wykorzystanie do wspomagania decyzji	4,10 ↑	4,21 ↑
Zarządzanie procesem digitalizacji	4,08 ↑	4,06 ↑
Zarządzanie kryzysowe	4,07 ↑	4,11 ↑
Stosowanie regulacji prawnych związanych z pracą zdalną i hybrydową	4,06 ↑	3,98 ↑
Edukacja pracowników i interesariuszy w zakresie pracy zdalnej i cyberbezpieczeństwa	4,06 ↑	4,06 ↑
Zarządzanie projektami w trybie pracy zdalnej i hybrydowej	4,02 ↑	3,87 ↑
Zarządzanie projektami w trybie pracy zdalnej	3,98 ↑	3,99 ↑
Automatyzacja i robotyzacja procesów	3,97 ↑	4,02 ↑
Organizacja pracy zdalnej i hybrydowej w firmie	3,86 ↑	3,86 ↑

** Strzałki w górę wskazują na wyższą średnią ocenę poszczególnych kluczowych kompetencji w stosunku do pierwszej edycji badania.*
Źródło: Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa. Raport zbiorczy z badania dotyczącego działań antycovidowych w sektorach: Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo, Edycja II, Warszawa 2022.

W obu edycjach badania prawie wszystkie firmy z sektora IT (po 98 proc. odpowiedzi) deklarowały, że pozyskują potrzebne im kompetencje poprzez utrzymanie, szkolenie i przekwalifikowanie własnych pracowników. Dla 42 proc. uczestników pierwszej edycji i 47 proc. uczestników drugiej edycji sposobem na zdobycie potrzebnych kompetencji było również pozyskanie doświadczonych specjalistów z rynku pracy. 42 proc. respondentów pierwszej ankiety i 42 proc. drugiej twierdziło, że pozyskuje potrzebne kadry poprzez zatrudnianie młodych specjalistów i wyszkolenie ich u siebie. W obu edycjach po 25 proc. firm z sektora IT deklarowało korzystanie przy pozyskiwaniu potrzebnych specjalistów ze współpracy ze szkołami i uczelniami (staże, praktyki).

Sektor telekomunikacji i cyberbezpieczeństwa (TCB)

Sektor telekomunikacji i cyberbezpieczeństwa, w porównaniu z innymi, nietechnologicznymi, sektorami gospodarki stosunkowo łagodnie został dotknięty skutkami pandemii, podobnie jak sektor informatyczny. Zdaniem ankietowanych w pierwszej edycji badania pandemia wpłynęła więc w umiarkowanym stopniu na zmianę dotychczasowego modelu działania firm. Tak twierdziło najwięcej, bo 40 proc. respondentów, a w co dziesiątym przedsiębiorstwie koronawirus nie wymusił żadnych zmian w modelu działania. Bardzo duże i duże zmiany oraz małe i bardzo małe odnotowano odpowiednio w 24 proc. i 26 proc. firm z tego sektora.

Połowa przedsiębiorców przewidywała, że wprowadzone w modelu działania zmiany będą trwałe, a ponad połowa (55 proc.) uważała, że zmiana dotychczasowego modelu działania wpłynęła na zmianę kompetencji pracowników co najmniej w umiarkowanym stopniu. Jedynie 9 proc. ankietowanych w ogóle nie widziało konieczności zmiany kompetencji pracowników. Z kolei zdecydowana większość respondentów (67 proc.) uważała, że w ciągu najbliższych 12 miesięcy pandemia i jej skutki nie zmienią nic w aspekcie potrzeb kompetencyjnych w ich firmach. Zaledwie 8 proc. badanych było zdania, że w tym czasie pojawi się zapotrzebowanie na nowe kompetencje.

Natomiast w drugiej edycji badania ponad połowa respondentów wskazała, że pandemia nie wywiera już wpływu na funkcjonowanie ich przedsiębiorstw (62 proc.). Z kolei 37 proc. badanych z sektora TCB wskazało na występowanie takiego wpływu.

Jakie zatem kompetencje miały w pandemii największe znaczenie dla telekomunikacji i cyberbezpieczeństwa? Według badanych w pierwszej edycji były to kompetencje związane z obsługą klienta, w tym również świadczeniem usług pomocy technicznej w trybie zdalnym (średnia: 3,58 w skali 1-5), zarządzaniem projektami w trybie pracy zdalnej (3,57) oraz z instalowaniem, konfigurowaniem, administrowaniem i zabezpieczaniem systemów obiegu dokumentów i organizacją pracy zdalnej i hybrydowej w firmie (po 3,55).

Z kolei największe znaczenie w kolejnej edycji miały kompetencje związane z integracją systemów (średnia: 3,99), analizą ryzyka w zmiennym, niestabilnym środowisku pracy i prowadzeniem biznesu (średnia: 3,98), zarządzaniem informacją (średnia: 3,94) oraz analizą danych i jej wykorzystaniem do wspomagania decyzji (średnia: 3,93). Zaś najmniejsze znaczenie miała automatyzacja i robotyzacja procesów (średnia: 3,69), zarządzanie procesem digitalizacji (średnia: 3,72) oraz zarządzanie kryzysowe (średnia: 3,73).

TABELA 4. Kluczowe kompetencje w kontekście skutków pandemii COVID-19 – sektor TCB: obecnie i w ciągu najbliższych 12 miesięcy*

Kompetencje kluczowe w kontekście skutków pandemii COVID-19	Obecnie (wśrednia)	W najbliższych 12 miesiącach (średnia)
Integracja systemów	3,99 ↑	4,00 ↑
Analiza ryzyk w zmiennym, niestabilnym środowisku pracy i prowadzenia biznesu	3,98 ↑	3,82 ↑
Zarządzanie informacją	3,94 ↑	3,97 ↑
Analiza danych i jej wykorzystanie do wspomagania decyzji	3,93 ↑	3,86 ↑
Projektowanie, implementacja, administrowanie i zabezpieczanie rozwiązań chmurowych oraz migracja danych do chmury	3,92 ↑	3,88 ↑
Tworzenie, rozwój i zarządzanie oprogramowaniem	3,91 ↑	3,94 ↑
Utrzymanie i rozwój infrastruktury ICT	3,91 ↑	3,95 ↑
Zarządzanie zasobami danych	3,90 ↑	3,90 ↑
Stosowanie regulacji prawnych związanych z pracą zdalną i hybrydową	3,88 ↑	3,76 ↑
Implementowanie, konfigurowanie, administrowanie i zabezpieczanie systemów obiegu dokumentów	3,88 ↑	3,89 ↑
Zarządzanie procesami ICT na styku technologii i biznesu	3,87 ↑	3,84 ↑
Zapewnienie bezpieczeństwa kanałów komunikacji elektronicznej, w tym należyta weryfikacja tożsamości stron komunikacji	3,86 ↑	3,92 ↑
Implementowanie, konfigurowanie, administrowanie i zabezpieczanie platform e-learningowych	3,85 ↑	3,81 ↑
Tworzenie i wdrażanie nowych metod zapewnienia ciągłości działania firmy w sytuacji nagłych zagrożeń	3,85 ↑	3,89 ↑
Instalowanie, konfigurowanie, administrowanie i zabezpieczanie systemów do pracy zdalnej i telekonferencji	3,85 ↑	3,90 ↑
Zarządzanie projektami w trybie pracy zdalnej i hybrydowej	3,84 ↑	3,89 ↑
Obsługa klienta, w tym również świadczenie usług pomocy technicznej, w trybie zdalnym	3,82 ↑	3,83 ↑
Edukacja pracowników i interesariuszy w zakresie pracy zdalnej i cyberbezpieczeństwa	3,82 ↑	3,87 ↑
Zarządzanie zmianą	3,80 ↑	3,73 ↑
Organizacja pracy zdalnej i hybrydowej w firmie	3,80 ↑	3,79 ↑
Zestawianie łączy do bezpiecznej transmisji dźwięku, obrazu i danych	3,77 ↑	3,73 ↑
Zarządzenie projektami w trybie pracy zdalnej	3,75 ↑	3,73 ↑
Zarządzanie kryzysowe	3,73 ↑	3,83 ↑
Zarządzanie procesem digitalizacji	3,72 ↑	3,63 ↑
Automatyzacja i robotyzacja procesów	3,69 ↑	3,60 ↑

** Strzałki w górę wskazują na wyższą średnią ocenę poszczególnych kluczowych kompetencji w stosunku do pierwszej edycji badania.*
Źródło: Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa. Raport zbiorczy z badania dotyczącego działań antycovidowych w sektorach: Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo, Edycja II, Warszawa 2022.

Wyniki znaczenia kompetencji w firmach znacząco różniły się pomiędzy I a II edycją badania. W I edycji najczęściej określane jako mające kluczowe lub duże znaczenie dla działalności firm z sektora TCB były kompetencje zorientowane na pracę zdalną oraz wszelkie procesy z nią związane. Z kolei wyniki II edycji wskazywały na kompetencje posiadające kluczowe lub duże znaczenie dotyczące głównie systemów oraz oprogramowania. Wśród kompetencji o znacznym wzroście znaczenia na przestrzeni dwóch przeprowadzonych edycji występują kompetencje dotyczące integracji systemów (I edycja: 53 proc., II edycja: 79 proc.) oraz tworzenia, rozwoju i zarządzania oprogramowaniem (I edycja: 53 proc., II edycja: 73 proc.).

Jeśli chodzi o dostępność na rynku pracy specjalistów z określonymi kompetencjami, to z pierwszego badania wynika, że najłatwiej dostępni byli pracownicy zajmujący się: obsługą klienta, w tym również świadczeniem usług pomocy technicznej w trybie zdalnym, tworzeniem i wdrażaniem nowych metod zapewniania ciągłości działania firmy w sytuacji nagłych zagrożeń, a także implementowaniem, konfigurowaniem, administrowaniem i zabezpieczaniem systemów obiegu dokumentów i zarządzaniem zasobami danych (po 84 proc. dla połączonych odpowiedzi „zdecydowanie tak" i „raczej tak"). Kompetencją, z którą wiązała się najmniejsza dostępność specjalistów, była analiza ryzyk w zmiennym, niestabilnym środowisku pracy (74 proc.).

W drugiej edycji badania kompetencjami uznanymi za najłatwiej dostępne były: integracja systemów (78 proc. wskazań dla połączonych odpowiedzi „zdecydowanie tak" i „raczej tak"), projektowanie, implementacja, administrowanie i zabezpieczanie rozwiązań chmurowych oraz migracja danych do chmury (75 proc.), implementowanie, konfigurowanie, administrowanie i zabezpieczanie platform e-learningowych (73 proc.), analiza ryzyk w zmiennym i niestabilnym środowisku pracy i prowadzenia biznesu (72 proc.) oraz tworzenie, rozwój i zarządzanie oprogramowaniem (72 proc.).

Z przeprowadzonych badań wynika, że w co dziesiątym przedsiębiorstwie koronawirus nie wymusił żadnych zmian w modelu działania

Z badania wynika też, że niemal wszystkie badane firmy zdobywały potrzebne kompetencje poprzez utrzymanie, szkolenie lub przekwalifikowanie własnych pracowników. W obu edycjach tak właśnie odpowiedziało 95 proc. respondentów. 62 proc. badanych z pierwszej edycji i 74 proc. z drugiej korzystało również z pozyskiwania doświadczonych specjalistów z rynku, a odpowiednio 47 proc. i 54 proc. z zatrudniania młodych specjalistów, absolwentów uczelni i przygotowywania ich do zadań w firmie. Z kolei odpowiednio 29 proc. ankietowanych w połowie 2021 roku i 42 proc. w pierwszym kwartale 2022 roku stwierdziło, że ich firmy pozyskują potrzebne kompetencje dzięki współpracy ze szkołami lub uczelniami.

Współpraca Maria Węcowska

TABELA 5. Czy Pani/Pana zdaniem są obecnie na rynku pracy specjaliści dysponujący wymienionymi kompetencjami? – sektor TCB: dane zbiorcze dla odpowiedzi „zdecydowanie tak" + „raczej tak" dla I i II tury badania*

Kompetencje specjalistów	I tura badania („zdecydowanie tak" + „raczej tak")	II tura badania („zdecydowanie tak" + „raczej tak")
Integracja systemów	81%	78% ↓
Projektowanie, implementacja, administrowanie i zabezpieczanie rozwiązań chmurowych oraz migracja danych do chmury	77%	75% ↓
Implementowanie, konfigurowanie, administrowanie i zabezpieczanie platform e-learningowych	83%	74% ↓
Analiza ryzyka w zmiennym, niestabilnym środowisku pracy i prowadzenia biznesu	74%	72% ↓
Tworzenie, rozwój i zarządzanie oprogramowaniem	83%	72% ↓
Zarządzanie informacją	80%	72% ↓
Zarządzanie procesami ICT na styku technologii i biznesu	82%	71% ↓
Zarządzanie projektami w trybie pracy zdalnej i hybrydowej	81%	71% ↓
Tworzenie i wdrażanie nowych metod zapewnienia ciągłości działania firmy w sytuacji nagłych zagrożeń	84%	70% ↓
Zarządzanie procesem digitalizacji	79%	70% ↓
Zestawianie łączy do bezpiecznej transmisji dźwięku, obrazu i danych	79%	70% ↓
Analiza danych i jej wykorzystanie do wspomagania decyzji	77%	69% ↓
Instalowanie, konfigurowanie, administrowanie i zabezpieczanie systemów do pracy zdalnej i telekonferencji	78%	69% ↓
Obsługa klienta, w tym również świadczenie usług pomocy technicznej, w trybie zdalnym	85%	69% ↓
Stosowanie regulacji prawnych związanych z pracą zdalną i hybrydową	76%	68% ↓
Zarządzanie zasobami danych	84%	68% ↓
Implementowanie, konfigurowanie, administrowanie i zabezpieczanie systemów obiegu dokumentów	84%	67% ↓
Zarządzanie kryzysowe	79%	67% ↓
Utrzymanie i rozwój infrastruktury ICT	79%	66% ↓
Edukacja pracowników i interesariuszy w zakresie pracy zdalnej i cyberbezpieczeństwa	80%	64% ↓
Automatyzacja i robotyzacja procesów	83%	62% ↓
Zarządzanie zmianą	82%	62% ↓
Zarządzanie projektami w trybie pracy zdalnej	77%	62% ↓
Zapewnienie bezpieczeństwa kanałów komunikacji elektronicznej, w tym należyta weryfikacja tożsamości stron komunikacji	79%	61% ↓
Organizacja pracy zdalnej i hybrydowej w firmie	75%	60% ↓

** Strzałki w dół wskazują na niższy odsetek sumy odpowiedzi „zdecydowanie tak" i „raczej tak" w stosunku do pierwszej edycji badania.*
Źródło: Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa. Raport zbiorczy z badania dotyczącego działań antycovidowych w sektorach: Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo, Edycja II, Warszawa 202.

Między biznesem a edukacją

Ponad połowa (59 proc.) firm z całej branży ICT (informatyka oraz telekomunikacja i cyberbezpieczeństwo) uczestniczących w drugiej edycji badania stwierdziła, że współpracuje ze szkołami i/lub uczelniami. W grupie tej 62 proc. dobrze oceniło tę współpracę. Z drugiej strony, niemal połowa (48 proc.) firm, które nie współpracowały wówczas ze szkołami czy uczelniami, twierdziła, że nie ma takiej potrzeby.

Najczęściej wymienianymi formami współpracy między przedsiębiorstwami a placówkami edukacyjnymi były: oferowanie przez firmę kursów praktycznych (praktyk) oraz stażów dla uczniów/studentów (49 proc. odpowiedzi dla całej branży ICT), udział przedstawicieli firmy w spotkaniach w szkole/na uczelni w celu pokazania specyfiki pracy w branży (38 proc.), zaangażowanie studentów do pisania branżowych prac magisterskich na potrzeby firmy (36 proc.).

Również ponad połowa (57 proc.) wszystkich respondentów z sektorów informatyka oraz telekomunikacja i cyberbezpieczeństwo w pierwszym kwartale 2022 roku deklarowała chęć pogłębienia współpracy ze szkołami i uczelniami. Za największą korzyść ze współpracy z placówkami edukacyjnymi firmy uznały wzrost konkurencyjności (49 proc. wskazań). W dalszej kolejności wskazano: poszerzenie obszarów kompetencyjnych firmy (40 proc.), rozwój kompetencji pracowników wchodzących na rynek pracy (36 proc.) oraz wzrost prestiżu firmy (34 proc.).

Za główną barierę współpracy ze szkołami i uczelniami firmy z branży ICT uznały nadmierną formalizację i procedury w szkołach/uczelniach (38 proc. wskazań). Po stronie trudności wymieniono również: brak czasu na zaangażowanie w dodatkowe aktywności przez którąś ze stron (26 proc.), brak elastyczności i adaptacji świata nauki do wymogów rynku w branży (26 proc.) oraz niechęć do współpracy naukowców z przedstawicielami przedsiębiorstw (18 proc.).

Ankietowani zostali również zapytani, czy powinny być wprowadzone jakieś zmiany w systemie edukacji. Dla 33 proc. ogółu respondentów zmiany te powinny być wdrożone jak najszybciej, jednak blisko połowa (46 proc.) uważała, że w ogóle nie ma takiej potrzeby. Natomiast aż 22 proc. pytanych nie miało swojego zdania, czy wprowadzanie takich zmian jest konieczne – ich zdaniem warto poczekać na ustabilizowanie się sytuacji i wykrystalizowanie w miarę stałych trendów.

Ciekawe wnioski można zaobserwować, analizując wyniki w podziale na sektory. Przedstawiciele firm z sektora informatyka dużo częściej twierdzili, że wprowadzenie zmian w systemie edukacji jest konieczne i należy zrobić to jak najszybciej (44 proc.). Natomiast w przypadku tego sektora znaczna część odpowiedzi wskazywała na konieczność poczekania na ustabilizowanie się sytuacji (28 proc.). Tyle samo ankietowanych nie widziało również potrzeby wprowadzenia istotnych zmian. Z kolei respondenci z firm z sektora telekomunikacja i cyberbezpieczeństwo dużo częściej podkreślali, że nie ma potrzeby wprowadzania tego rodzaju zmian w systemie edukacji (64 proc.), a jedynie 22 proc. pytanych uważało, że zmiany należy wprowadzić jak najszybciej. Zdaniem 15 proc. ankietowanych warto poczekać na ustabilizowanie się sytuacji na rynku pracy.

Porównując połączone odpowiedzi dla całego rynku ICT z konkretnymi propozycjami zmian w systemie edukacji, można zaobserwować, że mimo iż tylko co trzeci badany uznał, że zmiany w systemie edukacji powinny zostać wprowadzone jak najszybciej, to aż 67 proc. respondentów uważało, że warto już teraz aktualizować i dostosowywać programy kształcenia na studiach, a także w szkołach ponadpodstawowych – 65 proc. wskazań. Niewiele mniej osób wskazało na potrzebę udostępnienia środków na przekwalifikowanie pracowników (64 proc.) i zwiększenie liczby (zdalnych) szkoleń i kursów dla pracowników w sektorze (61 proc.).

Wprowadzanie zmian w systemie edukacji było kwestią mocno różnicującą odpowiedzi przedstawicieli firm z obu sektorów. Przedsiębiorcy z sektora informatyka byli zdecydowanie bardziej przekonani o konieczności wprowadzenia wszystkich wymienionych zmian w systemie edukacji – wyniki mieściły się w zakresie 81-71 proc.

MIĘDZYNARODOWE NARZĘDZIA OPISU KOMPETENCJI CYBERBEZPIECZEŃSTWA – NIE WYMYŚLAJMY KOŁA OD NOWA

NIST Cybersecurity Framework i ENISA European Cybersecurity Skills Framework to stale aktualizowane dokumenty reprezentujące najwyższą jakość oraz pełny stan wiedzy w całym międzynarodowym ekosystemie zapewniania cyberbezpieczeństwa. Są one weryfikowane przez setki i dziesiątki tysięcy specjalistów i wykorzystywane przez miliony fachowców z całego świata.

Tomasz Klekowski
Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo,
Polskie Towarzystwo Informatyczne

Wysiłek i wiedza włożone w ich przygotowanie są ogromne. Nie jest zasadne i możliwe przygotowanie dokumentów o podobnej jakości bez wielomilionowych inwestycji i wieloletnich ciągłych prac olbrzymich zespołów ekspertów o najwyższych kompetencjach.

Polski ekosystem cyberbezpieczeństwa powinien skupić się na wykorzystywaniu tych światowych i europejskich zasobów, aby zapewnić odpowiedni do wyzwań poziom wsparcia w zakresie cyberbezpieczeństwa.

Palące wyzwania

Wraz z postępującym procesem transformacji cyfrowej szybko rośnie wykorzystanie różnorodnych technologii informatycznych, zarówno w obszarze infrastruktury oprogramowania firm, jak i w obszarze internetu rzeczy, gdzie następuje połączenie rozwiązań cyfrowych z innymi urządzeniami.

Obydwa te obszary wymagają ochrony cybernetycznej, ponieważ wraz z rozwojem technologii rosną również zagrożenia związane z atakami cybernetycznymi.

Tempo rozwoju technologii i zagrożeń stawia duże wyzwania z perspektywy rozwoju kompetencji dla tworzenia, wdrożeń i utrzymania narzędzi i procesów związanych z cyberbezpieczeństwem.

W Polsce z racji rozdrobnionej struktury gospodarki, w której dominują małe i średnie firmy, wyzwania związane z cyberbezpieczeństwem są jeszcze bardziej palące. Wiele firm nie posiada kompetencji potrzebnych do zdefiniowania swoich potrzeb w zakresie cyberbezpieczeństwa, podaż specjalistów jest niewystarczająca, a ich kształcenie nie jest odpowiednio ustrukturyzowane.

Zintegrowany System Kwalifikacji definiuje podstawowe wymagania kompetencyjne w obszarze cyberbezpieczeństwa, odnosząc się do trzech kwalifikacji, specjalisty zarządzania cyberbezpieczeństwem, eksperta zarządzania cyberbezpieczeństwem i managera zarządzania cyberbezpieczeństwem.

Tempo rozwoju technologii i zagrożeń stawia duże wyzwania z perspektywy rozwoju kompetencji, dziś nie ma jednego rodzaju specjalisty cyberbezpieczeństwa

Takie podejście było właściwe w początkowej fazie rozwoju domeny cyberbezpieczeństwa, ale wraz z upływem czasu, rozwojem technologii cyfrowych, wzrostem palety zastosowań i integracji technologii w każdym obszarze działania przedsiębiorstw i gospodarki przestaje być wystarczające.

Procesy i narzędzia cyberbezpieczeństwa się rozrastają, dywersyfikują, wzrasta ich złożoność i w związku z tym następuje dywersyfikacja i specjalizacja w ramach realizacji poszczególnych funkcji cyberbezpieczeństwa.

Dzisiaj już nie ma jednego rodzaju specjalisty cyberbezpieczeństwa obejmującego całe spektrum wymagań i zastosowań technologii, ale pojawia się wiele węższych specjalizacji. Przy okazji rosną wyzwania związane z zarządzaniem całym systemem bezpieczeństwa firm i organizacji.

Wyzwanie to jest widoczne na całym świecie. Z tempem rozwoju i różnicowania specjalności w obszarze cyberbezpieczeństwa mierzą się wszystkie kraje i wszystkie systemy rozwoju kompetencji.

Dlatego warto spojrzeć na działania podejmowane w tym zakresie w Stanach Zjednoczonych i Europie, tam gdzie rozwijana jest technologia i tam, gdzie definiuje się procesy i praktyki związane z zarządzaniem cyberbezpieczeństwem oraz ustala standardy w tym obszarze z uwzględnieniem wymagań i standardów rozwoju kompetencji.

Wykorzystanie międzynarodowych standardów i ich dostosowanie do polskich wymogów jest konieczne do utrzymania spójności z rozwojem technologii, zapewniania odpowiedniego tempa dostosowania zmian w wymaganiach kompetencyjnych do szybkości i złożoności rozwoju technologii i zagrożeń, zapewnienia stałej aktualności wymagań kompetencyjnych.

Matryce porządkują i standaryzują opisywane obszary, pozwalają na normalizację języka opisu, a do tego ułatwiają edukację i współpracę specjalistów oraz komunikację z szerokimi grupami interesariuszy.

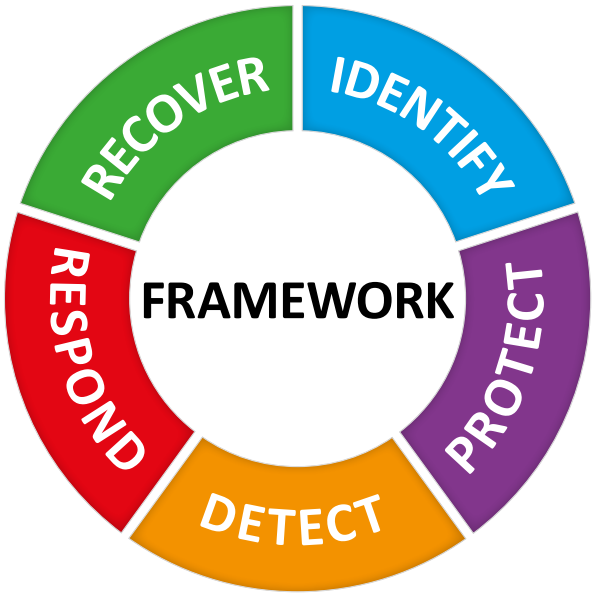
The National Institute of Standards and Technology (NIST) i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Obszarem rozwoju i standaryzacji opisów wymagań dla cyberbezpieczeństwa zajmuje się w światowym ekosystemie wiele organizacji. Również te, które zajmują się opisami kompetencji dla ról w obszarze tworzenia, wdrażania i wykorzystywania rozwiązań informatycznych. Odniesienie do ról cyberbezpieczeństwa można znaleźć zarówno w Skills Framework for the Information Age, jak i e-competence framework. Jednak najbardziej wartościowe prace zostały wykonane w ramach amerykańskiego

The National Institute of Standards and Technology (NIST) – www.nist.gov oraz w ramach prac Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) – www.enisa.europa.eu.

NIST od wielu lat rozwija i przygotowuje wymagania dotyczące cyberbezpieczeństwa. Pierwsze zalecenia w postaci Cybersecurity Framework zostały opublikowane w 2013 roku.

Według danych z sierpnia 2021 matryca Cybersecurity Framework jest wykorzystywana w ponad stu krajach i została pobrana ponad półtora miliona razy. Niemal każdy specjalista cyberbezpieczeństwa zna grafikę NIST opisującą funkcje cyberbezpieczeństwa.



Matryca skupia się głównie na stronie organizacji procesów i wymagań w zakresie cyberbezpieczeństwa i umieszcza odpowiedzialność za poszczególne działania w pięciu funkcjach:

- Zidentyfikuj
- Ochroń
- Wykryj
- Odpowiedz
- Odbuduj

Każdy z tych obszarów składa się z kategorii działań, a kategorie podzielone są na bardziej szczegółowe podkategorie. Opis każdego działania w podkategorii jest wsparty konkretnymi dokumentami, pochodzącymi przykładowo z normy ISO 27001, NIST SP 800-53 rev4.

Cała matryca składa się z 23 kategorii i 108 podkategorii opisujących całe spektrum działań w zakresie cyberbezpieczeństwa. W konkretnych zastosowaniach wykorzystuje się profile dotyczące konkretnego rodzaju zastosowania, odnoszącego się do branży lub rodzaju zagrożenia.

Obecnie przygotowane są na przykład profile związane z zapewnianiem cyberbezpieczeństwa elektroenergetycznych sieci przesyłowych – smart grid, ochrony procesów i infrastruktury produkcyjnej w fabrykach czy ochrony pojazdów podłączonych do internetu.

Przykładami profili odnoszących się do typów zagrożeń są profile dotyczące zarządzania ryzykiem ataków typu ransomware czy ataków DDoS z sieci botów.

Matryca ta nie skupia się bezpośrednio na kompetencjach, ale na działaniach i z tego powodu ma bardzo praktyczny charakter, i jest szeroko wykorzystywana w branży.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) podjęła wysiłek przygotowania ramy odnoszącej się bezpośrednio do kwalifikacji i ról, jakie są pełnione przez specjalistów w obszarze cyberbezpieczeństwa.

Matryca ENISY to European Cybersecurity Skills Framework (ECSF), została finalnie przedstawiona kilka miesięcy temu – we wrześniu 2022 roku – i wnosi do dyskusji o kształtowaniu i strukturze kompetencji dla cyberbezpieczeństwa bardzo dużo wartości.

Matryca szczegółowo opisuje wymagania dla 12 ról w obszarze cyberbezpieczeństwa:

1. CHIEF INFORMATION SECURITY OFFICER (CISO)
2. CYBER INCIDENT RESPONDER
3. CYBER LEGAL, POLICY & COMPLIANCE OFFICER
4. CYBER THREAT INTELLIGENCE SPECIALIST
5. CYBERSECURITY ARCHITECT
6. CYBERSECURITY AUDITOR
7. CYBERSECURITY EDUCATOR
8. CYBERSECURITY IMPLEMENTER
9. CYBERSECURITY RESEARCHER
10. CYBERSECURITY RISK MANAGER
11. DIGITAL FORENSICS INVESTIGATOR
12. PENETRATION TESTER

Role pokrywają szerokie spektrum pracy specjalistów z zakresu zapewniania cyberbezpieczeństwa, zarządzania cyberbezpieczeństwem, jak również wsparcia procesów cyberbezpieczeństwa, np. cybersecurity educator czy cybersecurity researcher.

Każda rola jest precyzyjnie opisana i zawiera:

- podsumowanie
- misję, jaką realizuje osoba w tej roli
- główne rezultaty pracy (deliverables)
- główne zadania
- główne wymagane umiejętności
- wymagany zakres posiadanej wiedzy
- odniesienie do opisu kompetencji w ramie e-competence framework (e-CF) z podaniem poziomu, jaki osoba pełniąca rolę powinna posiadać

Opis roli zawiera również odniesienie do alternatywnych nazw, jakie są wykorzystywane w różnych organizacjach dla osób z takim zakresem pracy i odpowiedzialności, co jest bardzo przydatne w praktyce wykorzystywania matrycy.

Wykorzystanie matryc

Zdefiniowane matryce z opisem wymagań dla poszczególnych ról, zagregowane w odpowiednie ramy kwalifikacji, mogą pomóc w wielu obszarach:

- tworzeniu opisów stanowisk, zakresów odpowiedzialności i profili ról w obszarze cyberbezpieczeństwa
- planowaniu docelowych modeli pracy oraz struktur organizacyjnych dla zapewniania cyberbezpieczeństwa oraz planowaniu potrzeb w zakresie zasobów ludzkich w tym obszarze
- pomocy w pozyskiwaniu i rekrutacji pracowników o odpowiednich umiejętnościach poprzez standaryzację języka opisu i używanie określeń zrozumiałych dla branży i aplikujących specjalistów
- pomocy w opisie wymagań dla zaangażowania poddostawców
- alokacji pracowników o odpowiednich kompetencjach do odpowiednich zadań i projektów
- ocenie umiejętności pracowników, poddostawców i potencjału organizacji
- analizie dla projektowania rozwoju kompetencji działu i organizacji
- rozwoju kompetencji pracowników
- ustaleniu zasad wynagradzania i szeregowania pracowników w domenie cyberbezpieczeństwa

W związku z tym takie matryce mogą być szeroko wykorzystywane w organizacjach przez:

- pracowników, kierowników i managerów
- zarządzających i liderów organizacji
- specjalistów ds. zasobów ludzkich oraz specjalistów ds. wynagrodzeń
- specjalistów ds. szkoleń i rozwoju
- działów zakupów zajmujących się kontraktowaniem usług i poddostawców

Nazwa profilu	Manager Zarządzania Ryzykiem Cybernetycznym
Inne nazwy profilu	Analityk Ryzyka Bezpieczeństwa Informacyjnego Konsultant ds. Zapewniania Bezpieczeństwa Cybernetycznego Konsultant ds Ryzyk Cyberbezpieczeństwa Analityk Wpływu Zagrożeń Cybernetycznych Manger Ryzyk Cyberbezpieczeństwa
Podsumowanie roli	Zarządza ryzykiem związanym z cyberbezpieczeństwem organizacji w odniesieniu do realizacji jej strategii. Opracowuje, utrzymuje i wdraża procesy zarządzania ryzykiem pochodzącym z zagrożeń cybernetycznych i informacyjnych
Opis misji	Zarządza (identyfikuje, analizuje, ocenia, szacuje, odpowiada na) ryzyka związane z cyberbezpieczeństwem w zakresie infrastruktury, systemów i usług ICT poprzez planowanie, stosowanie, raportowanie i komunikowanie analizy, oceny i przetwarzania ryzyka. Ustanawia strategię zarządzania ryzykiem dla organizacji i zapewnia, że ryzyko pozostaje na akceptowalnym dla organizacji poziomie poprzez wybór i wdrażanie działań zapobiegawczych i kontrolnych
Przykładowe rezultaty	▪ Raport oceny ryzyka dla cyberbezpieczeństwa ▪ Plan działania na rzecz usuwania ryzyka cybernetycznego
Główne zadania	▪ Opracowanie strategii zarządzania ryzykiem cyberbezpieczeństwa w organizacji ▪ Zarządzanie inwentaryzacją zasobów organizacji ▪ Identyfikacja i ocena zagrożeń i podatności systemów teleinformatycznych związanych z cyberbezpieczeństwem ▪ Identyfikacja krajobrazu zagrożeń, w tym profili atakujących i oszacowanie potencjału ataków ▪ ocena zagrożeń dla cyberbezpieczeństwa i zaproponowanie najodpowiedniejszych opcji zarządzania ryzykiem ▪ w tym środków kontroli oraz ograniczania i unikania ryzyka, w odniesieniu do realizacji strategii organizacji ▪ Monitorowanie skuteczności kontroli cyberbezpieczeństwa i poziomów ryzyka ▪ Zapewnienie, że wszystkie zagrożenia dla cyberbezpieczeństwa pozostaną na akceptowalnym poziomie dla organizacji ▪ Opracowanie, utrzymanie, raportowanie i komunikowanie działań pełnego cyklu zarządzania ryzykiem
Główne umiejętności	▪ Umiejętności wdrożenia ram, metodologii i wytycznych dotyczących zarządzania ryzykiem w cyberbezpieczeństwie oraz zapewnienie zgodności z przepisami i standardami ▪ Umiejętności analizy i wykorzystania praktyk zarządzania jakością i ryzykiem w organizacji ▪ Umożliwienie właścicielom procesów i obszarów biznesowych, kadrze kierowniczej i innym interesariuszom podejmowania decyzji ze świadomością ryzyka i możliwością zarządzania nim ▪ Umiejętności budowy środowiska rozumienia ryzyka w zakresie cyberbezpieczeństwie ▪ Umiejętności komunikacji, prezentowania i raportowania do odpowiednich interesariuszy w organizacji ▪ Umiejętności definiowania opcji zarządzania ryzyka
Najważniejsze obszary wiedzy	▪ Zna i rozumie standardy, metodologie i ramy zarządzania ryzykiem ▪ Zna i rozumie narzędzia zarządzania ryzykiem ▪ Zna i rozumie zalecenia i najlepsze praktyki w zakresie zarządzania ryzykiem ▪ Zna i rozumie zagrożenia cybernetyczne ▪ Zna i rozumie luki w zabezpieczeniach systemów komputerowych Zna zasady kontroli procesów i stosowania rozwiązań w zakresie cyberbezpieczeństwa ▪ Zna i rozumie zagrożenia dla cyberbezpieczeństwa ▪ Zna i rozumie zasady monitorowania, testowania i oceny skuteczności kontroli bezpieczeństwa cybernetycznego ▪ Zna u rozumie zakres korzyści i wykorzystania certyfikatów związanych z cyberbezpieczeństwem ▪ Zna i rozumie technologie związane z cyberbezpieczeństwem
Wymagane kompetencje z ramy kompetencji e-CF	▪ E.3. Risk Management – poziom 4 ▪ E.5. Process Improvement – poziom 3 ▪ E.7. Business Change Management – poziom 4 ▪ E.9. IS-Governance – poziom 4

Oraz przez zewnętrzne organizacje działające w ekosystemie, w tym przez:

- rekruterów
- edukatorów, twórców szkoleń i programów kształcenia
- konsultantów organizacji
- organizacje branżowe

Omówione matryce pokazują duże zaawansowanie i szczegółowo strukturyzują opisywane przez siebie zagadnienia z perspektywy realizowanych procesów i potrzebnych kompetencji.

Są to dokumenty reprezentujące najwyższą jakość oraz pełny stan wiedzy w całym międzynarodowym ekosystemie zapewniania cyberbezpieczeństwa. Są to dokumenty weryfikowane przez setki i dziesiątki tysięcy specjalistów i wykorzystywane przez miliony specjalistów z całego świata. I co najważniejsze, są to dokumenty stale aktualizowane.

Polski ekosystem cyberbezpieczeństwa powinien skupić się na wykorzystywaniu tych światowych i europejskich zasobów, aby zapewnić odpowiedni do wyzwań poziom wsparcia w zakresie cyberbezpieczeństwa.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) podjęła wysiłek przygotowania ramy odnoszącej się bezpośrednio do kwalifikacji i ról, jakie są pełnione przez specjalistów w obszarze cyberbezpieczeństwa

Opisywane ramy NIST, ECSF i e-CF są obszernymi i złożonymi dokumentami. Już sama ich lokalizacja i odniesienie do lokalnych warunków jest ważnym i dużym zadaniem, które powinny podjąć organizacje zajmujące się wsparciem rozwoju kompetencji dla specjalistów cyberbezpieczeństwa w Polsce.

KTO I CZEGO POWINIEN SIĘ UCZYĆ W ŚWIETLE WYZWAŃ CYFROWEJ TRANSFORMACJI

Dbanie o bezpieczeństwo podczas korzystania z sieci jest umiejętnością, która powinna należeć do najszerzej rozpowszechnionych kompetencji cyfrowych.

Joanna Mazur
analityczka DELab Uniwersytet Warszawski

Patrząc na wyniki *Digital Economy and Society Index* (DESI) dla Polski za 2022 rok, można by stwierdzić, że znowu nam nie wyszło. Znów zajmujemy jedno z ostatnich miejsc w rankingu państw członkowskich Unii Europejskiej mających na celu ułatwienie oceny poziomu zaawansowania w zakresie korzystania z cyfrowych usług, rozwoju infrastruktury, wdrażania cyfrowych rozwiązań przez przedsiębiorstwa czy poziomu kompetencji cyfrowych w społeczeństwie. Jednym z obszarów, w których poradziliśmy sobie najgorzej, był „Kapitał ludzki": „Jedynie 43 proc. osób w wieku od 16 do 74 lat posiada podstawowe lub wyższe umiejętności cyfrowe (UE – 54 proc.), a 57 proc. – co najmniej podstawowe umiejętności tworzenia treści cyfrowych (UE – 66 proc.). Specjaliści w dziedzinie ICT stanowią w Polsce nieco niższy odsetek siły roboczej niż średnia UE"[1].

Pytanie, które nasuwa się w świetle tych danych, dotyczy tego, na ile i jakiego rodzaju działaniami możliwe i potrzebne jest upowszechnianie wiedzy i umiejętności, które pozwoliłyby większemu gronu osób w bardziej świadomy sposób posługiwać się cyfrowymi technologiami?

1 *DESI Country Profile PL*, s. 3, dostęp: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (22.02.2023 r.).

Kształtowanie dobrych nawyków

Wśród kwestii branych pod uwagę przy wyliczaniu poziomu kompetencji cyfrowych są m.in. zagadnienia dotyczące dbania o bezpieczeństwo podczas korzystania z urządzeń cyfrowych. W świetle zbieranych do wyliczania DESI danych jedynie nieco ponad połowa Polaków w wieku między 16. a 74. rokiem życia ma podstawowe lub wyższe umiejętności w zakresie dbania o bezpieczeństwo podczas korzystania z sieci.

Chociaż trudno się nie zgodzić z tym, że zdobywanie wiedzy może pomagać w radzeniu sobie z licznymi wyzwaniami, to w kontekście korzystania z nowych technologii warto się zastanowić nad tym, w jakim zakresie użytkownikom przydałoby się więcej wiedzy

Tymczasem jest to niezwykle ważna umiejętność, która powinna należeć do najszerzej rozpowszechnionych kompetencji cyfrowych. Troska o bezpieczeństwo naszych danych osobowych i ostrożność w korzystaniu z podejrzanych stron czy aplikacji powinna być promowana wśród wszystkich grup demograficznych. Każdy z nas może paść ofiarą prób wyłudzenia danych osobowych, zwłaszcza w związku z używaniem coraz bardziej wysublimowanych technik wyciągania od użytkowników internetu wrażliwych informacji.

Stąd działania dotyczące budowania świadomości możliwych zagrożeń i sytuacji, które powinny budzić naszą podejrzliwość, powinny być kierowane do jak najszerszego grona odbiorców i obejmować nie tyle etap szkolnej edukacji, co ogólnopolskie kampanie informacyjne np. dotyczące możliwości zgłaszania podejrzanych linków przysyłanych SMS-ami o nieodebranych paczkach, za które użytkownik ma uiścić zapłatę.

Transformacja a edukacja trwająca całe życie

Zmieniające się wyzwania w zakresie dbania o bezpieczeństwo danych pokazują również inną specyfikę kompetencji cyfrowych: konieczność ich ciągłego aktualizowania w związku ze zmieniającymi się technologiami. Tym samym postrzeganie edukacji jako pewnego etapu w życiu przestaje odpowiadać temu, jaką rolę kształcenie pełni obecnie i może pełnić w najbliższej przyszłości: dla wielu z nas staje się ono elementem towarzyszącym nam przez dużą część życia.

Tendencja ta dotyczy nie tylko zawodów ściśle związanych z technologiami teleinformatycznymi, lecz również prac, których wykonywanie jeszcze do niedawna nie wiązało się z korzystaniem z technologii cyfrowych. Stąd wynika coraz większa waga otwartości na naukę nowych umiejętności, zwłaszcza w zakresie czynności wymagających współpracy z urządzeniami cyfrowymi. Chociażby szybko postępujący rozwój rozwiązań z zakresu generowania tekstów oraz tłumaczeń wykonywanych w sposób zautomatyzowany pokazuje, że przynajmniej w odniesieniu do części zawodów charakter wykonywanych w ich ramach czynności może się zmienić, np. z tłumaczenia na redagowanie tekstów przetłumaczonych w sposób zautomatyzowany.

Obecność tych mechanizmów na współczesnym rynku pracy wiąże się z pytaniami o rolę zinstytucjonalizowanej edukacji wyższej w czasach tak szybkich zmian stosowanych technologii, powstających nowych zawodów czy postępujących możliwości w zakresie automatyzacji różnych czynności. Z jednej strony pojawiają się głosy mówiące o jej nieprzystawalności – przynajmniej w obecnej formie – do zmieniających się realiów. Z drugiej jednak strony można bronić studiowania jako sposobu zdobywania bardziej uniwersalnych umiejętności, które dotyczą uczenia się i łatwości opanowywania kolejnych, coraz to nowych, technologii.

Waga niecyfrowych kompetencji

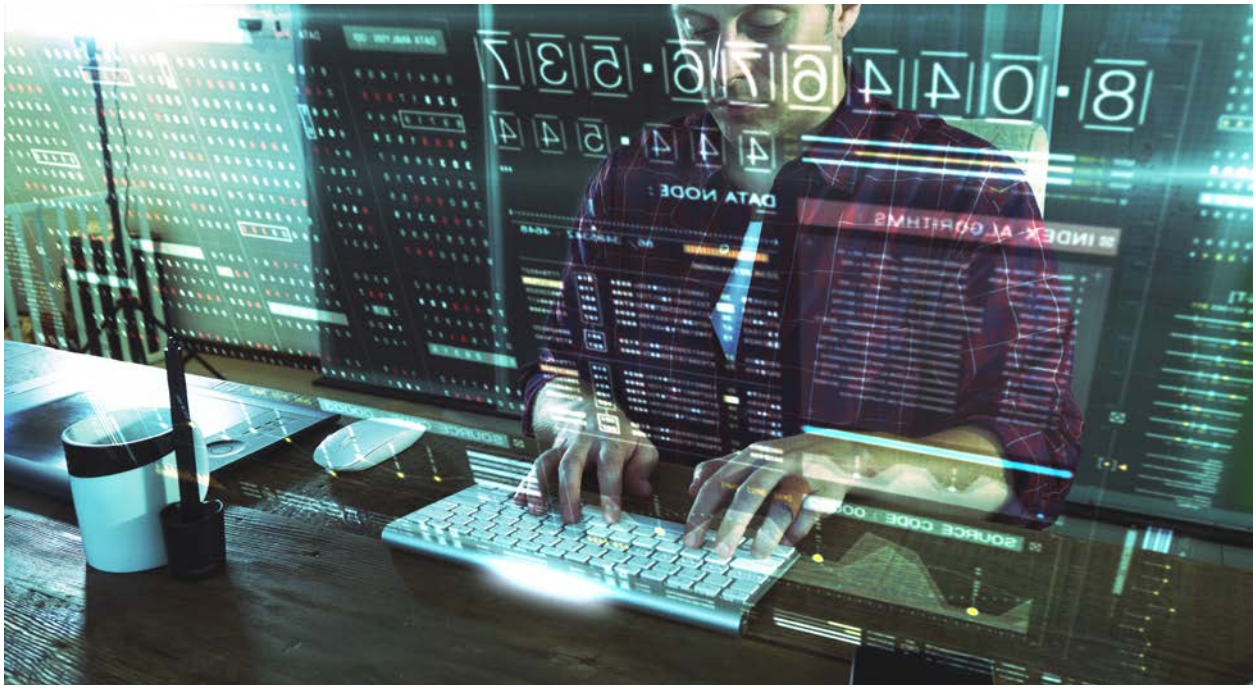
Innym uniwersalnym aspektem kompetencji potrzebnych do aktywnego i świadomego korzystania z technologii jest waga, którą mają kompetencje niemające ściśle cyfrowego charakteru. Przykładem w tym zakresie jest chociażby krytyczne podchodzenie do źródeł informacji. Nie jest to umiejętność ściśle należąca do kompetencji cyfrowych, a jednocześnie jest ona kluczowa, jeśli chodzi o poruszanie się po środowisku cyfrowym, w którym ocena wiarygodności wiadomości bywa trudna.

> **Większa liczba ekspertów powinna uczyć i siebie, i nas, jak zmieniać rzeczywistość cyfrową tak, aby pozwalała osobom mającym niższy poziom kompetencji cyfrowych bezpieczniej się w niej czuć i świadomiej z niej korzystać**

W tym zakresie istotne jest uzupełnianie zdobywanych kompetencji o specyfikę wymiaru cyfrowego. Wiedza o mechanizmach działania sieci społecznościowych czy platform, na których użytkownicy umieszczają filmy wideo, mające na celu podsuwanie użytkownikom angażujących treści i tym samym skłanianie ich do spędzania większej ilości czasu przed ekranem, może pomóc zachować większy dystans i czujność w odniesieniu do treści sugerowanych użytkownikowi na danej platformie.

ym, że zdobywanie wiedzy może pomagać w radzeniu sobie z licznymi wyzwaniami, to w kontekście korzystania z nowych technologii warto się zastanowić nad tym, w jakim zakresie użytkownikom przydałoby się więcej wiedzy na temat tego, jak one działają i więcej kompetencji dotyczących sposobów korzystania z nich, a w jakim zakresie przydałoby się więcej i skuteczniej egzekwowanych regulacji w zakresie przeciwdziałania zagrożeniom generowanym za pośrednictwem tych technologii.

Przedstawmy to zagadnienie przez analogię: wyobraźmy sobie, że podczas poruszania się rowerem po mieście zachowujemy odpowiedni poziom ostrożności i uważności na to, co się dzieje w naszym otoczeniu, jednak co chwilę na ścieżkę rowerową podrzucana zostaje elektryczna hulajnoga, której obecności nie mogliśmy się spodziewać. Czy oznacza to, że nie umiemy jeździć na rowerze, czy że hulajnogi nie powinny być wrzucane na ścieżkę? Zbieranie i wykorzystywanie danych, które nie są niezbędne do świadczenia danej usługi, niewystarczające zabezpieczenia w zakresie ich ochrony, wycieki danych – to nie tylko wynik braku kompetencji cyfrowych i wiedzy – czy to użytkowników internetu, czy osób pracujących w danych podmiotach – ale też ram prawnych umożliwiających przetwarzanie danego typu danych.



Jakich ekspertów brakuje

Takie przesunięcie akcentów w zakresie tego, kto i za co powinien być odpowiedzialny, żeby uczynić internet bezpieczniejszym miejscem, łączy się ze zmianą perspektywy w zakresie tego, jakiego rodzaju kompetencje cyfrowe powinny być rozwijane. O ile chodzi o kompetencje dotyczące korzystania z technologii cyfrowych: powinny one być jak najpowszechniejsze i jak najbardziej pogłębione, co osiągnąć można nie tylko przez działania koncentrujące się na rozwijaniu samych kompetencji cyfrowych, lecz także przez rozwijanie bardziej uniwersalnych umiejętności dotyczących chociażby krytycznego podejścia do treści, na które natykamy się w sieci.

Jeśli natomiast chodzi o bardziej aktywny sposób kształtowania rzeczywistości cyfrowej, zarówno wyniki DESI, jak i inne analizy ciągle wskazują na niewystarczającą liczbę specjalistów od technologii informacyjnych w Polsce. Pytanie, które rzadko jest jednak zadawane w tym kontekście, dotyczy tego, czy problem na pewno leży w liczbie specjalistów, czy może jednak w zajęciach, których wykonywaniu poświęcają czas osoby posiadające te szczególnie wysokie kompetencje[2]? Jak długo uwaga dużej części z nich skierowana będzie na kreowanie rozwiązań mających na celu zachęcenie użytkowników do klikania sponsorowanych reklam czy tworzenia algorytmów, które coraz głębiej będą nas wciągać w meandry ekstremistycznych treści, można by zaryzykować stwierdzenie, że użytkownicy internetu raczej czerpią korzyści z niewystarczającej liczby tego typu ekspertów na rynku.

Dlatego na pytanie, kto i czego powinien się uczyć w świetle wyzwań cyfrowej transformacji w odniesieniu do ekspertów, można by odpowiedzieć, że większa ich liczba powinna uczyć i siebie, i nas, jak zmieniać rzeczywistość cyfrową tak, aby pozwalała osobom mającym niższy poziom kompetencji cyfrowych bezpieczniej się w niej czuć i świadomiej z niej korzystać.

2 Tekst poruszający ten temat to np. artykuł: H. Walczyński, *O nędzy analityków*, „Nowy Obywatel", 16 listopada 2022 r., dostęp: https://nowyobywatel.pl/2022/11/16/o-nedzy-analitykow/ (22.2.2023).

JAK IDENTYFIKOWAĆ ZAGROŻENIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

Przepisy prawa zobowiązują, zwłaszcza przedsiębiorców, do zabezpieczenia systemów informacyjnych.

Grzegorz Cenkier
Członek Izby Rzeczoznawców Polskiego Towarzystwa Informatycznego, członek zarządu ISSA Polska

Historia ataków cybernetycznych nie jest długa. Pierwszy poważny globalny atak miał miejsce 2 listopada 1988 r. Spowodowany został przez Morris Worm – kod liczący 3 tys. linijek, który został wprowadzony do internetu przez Roberta Morrisa. Wirus ten zainfekował ponad 6 tys. komputerów (ok. 10 proc. całego ówczesnego internetu), a jego usunięcie zajęło ponad osiem dni ze względu na to, że duża część serwerów została odłączona od sieci. Dopiero 10 listopada udało się przywrócić normalne funkcjonowanie – łączne straty szacowano na kilkadziesiąt milionów dolarów.

Na świecie i w Polsce

Obecnie ataki są znacznie większe, a dotyczą nie tylko urządzeń komputerowych, lecz także infrastruktury przemysłowej, powodując straty finansowe sięgające setek milionów dolarów i dotykają użytkowników na całym świecie. Jeden z największych cyberataków ransomware w 2021 r. na infrastrukturę miał miejsce 7 maja, gdy został zainfekowany skomputeryzowany sprzęt zarządzający rurociągiem Colonial Pipeline, amerykańskiego systemu rurociągów naftowych, który transportuje benzynę i paliwo lotnicze z Houston w Teksasie głównie do południowo-wschodnich Stanów Zjednoczonych. Aby zablokować atak, Colonial Pipeline Company wstrzymała wszystkie operacje rurociągu i przy pośrednictwie FBI zapłaciła żądany okup (75 bitcoinów, wtedy około 4 milionów dolarów) w krótkim czasie po ataku. Okazało się jednak, że oprogramowanie dostarczone przez hakerów, które miało przywrócić prawidłowe funkcjonowanie rurociągu działa niezwykle wolno, co zmusiło właściciela rurociągu do odtworzenia systemów z kopii zapasowych (backupów). Eksploatacja rurociągu została wznowiona dopiero 12 maja o godzinie 17, kończąc sześciodniowe zamknięcie, jednak powrót do pełnej wydajności systemu nastąpił dopiero 15 maja. Koszt tego ataku to częściowe zamknięcie lotnisk Charlotte Douglas i Hartsfield-Jackson w Atlancie oraz wzrost cen paliw od 9 do 16 centów w Karolinie, Tennessee, Wirginii i Georgii i brak benzyny na 10 600 stacji benzynowych. Incydenty bezpieczeństwa dotyczą również naszego kraju.

W Polsce duży atak cybernetyczny miał miejsce między 27 a 28 czerwca 2017 roku, kiedy to wirus NotPetya w ciągu kilku godzin od ujawnienia się, dotarł z Ukrainy do wielu

punktów na świecie, w tym do jednej z polskich spółek giełdowych, która musiała zatrzymać swoje działanie. Początkowo wirus uważany był za ransomware, ale okazało się, że to wiper (wycieraczka), czyli mimo zapłacenia okupu, dane i systemy nie zostaną odzyskane, bo exploit je wymazuje. Odzyskanie danych z systemów zapasowych zajęło spółce kilka dni, przynosząc ogromne straty. W wyniku tego ataku ucierpiały światowe koncerny: Merck, FedEx, Saint-Gobain i wiele innych, w tym rosyjska spółka naftowa Rosnieft. Straty oszacowano na kilkadziesiąt milionów dolarów.

Regulacje prawne

Wspomniane zdarzenia pokazują, jak istotne jest bezpieczeństwo systemów informacyjnych. Czy wobec takich incydentów jesteśmy bezradni? Na pewno nie, ponieważ możemy się przygotować na takie zdarzenia, do czego zobowiązują, zwłaszcza przedsiębiorców bez względu na skalę działania, przepisy prawa. W Polsce 28 sierpnia 2018 r. weszła w życie ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC), która nakłada wiele zadań na operatorów usług kluczowych oraz dostawców usług cyfrowych. W skład systemu wchodzi również administracja publiczna, zarówno szczebla rządowego, jak i samorządowego, a także uczelnie i instytuty badawcze. Obowiązująca ustawa o KSC zostanie zapewne wkrótce zmieniona, ponieważ 27 grudnia 2022 roku uchwalona została nowelizacja europejskiej dyrektywy NIS w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.

Zrewidowana dyrektywa NIS, nazywana NIS 2, rozszerza zakres sektorów objętych dotychczasową dyrektywą m.in. o administrację publiczną, sektor żywności, telekomunikację, ścieki, przemysł, zarządzanie odpadami i przestrzeń kosmiczną, rozszerza także zakres infrastruktury cyfrowej. Sektory te zostały uznane za podmioty kluczowe (essential entities). Lista ta uległa powiększeniu o podmioty ważne (important entities), do których zaliczono: usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcję wyrobów medycznych, produkty komputerowe, elektroniczne i optyczne, sprzęt elektryczny, maszyny i wyposażenie, pojazdy samochodowe, przyczepy i naczepy oraz produkcję i dystrybucję chemikaliów, a także przetwarzanie i dystrybucję żywności. Ponadto NIS 2 wprowadza obowiązek raportowania incydentów, odpowiedzialność kierownictwa firmy za zgodność ze środkami zarządzania ryzykiem w cyberbezpieczeństwie, nakłada większe wymagania w zakresie zarządzania, obsługi i ujawniania luk w zabezpieczeniach, testowaniu poziomu cyberbezpieczeństwa oraz efektywnym wykorzystywaniu szyfrowania.

Ataki są znacznie większe, a dotyczą nie tylko urządzeń komputerowych, lecz także infrastruktury przemysłowej, powodując gigantyczne, sięgające milionów straty finansowe

Powstanie europejska sieć zarządzania kryzysowego w cyberprzestrzeni (European Cyber Crisis Liaison Organization Network, EU-CyCLONe), której zadaniem będzie koordynacja zarządzania incydentami

na wielką skalę na poziomie Unii Europejskiej. NIS 2 wprowadza koordynację w zakresie ujawniania podatności (vulnerability disclosure), a także wzmacnia rolę ENISA – Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, która po przyjęciu propozycji będzie odpowiedzialna za przygotowanie „Sprawozdania o stanie cyberbezpieczeństwa w Unii".

Pierwszy powstały w Polsce zespół reagowania na incydenty cyberbezpieczeństwa, zarejestrował w 2021 roku prawie 30 tys. unikalnych incydentów

Na mocy dotychczas obowiązującej ustawy o KSC w systemie cyberbezpieczeństwa działają trzy zespoły CSIRT odpowiedzialne za poszczególne obszary funkcjonowania państwa. CSIRT GOV zbiera informacje o incydentach zaistniałych w jednostkach administracji rządowej i u operatorów infrastruktury krytycznej, CSIRT MON w podmiotach podległych Ministrowi Obrony Narodowej, do CSIRT NASK incydenty zgłasza większość operatorów usług kluczowych, dostawcy usług cyfrowych, organy samorządu terytorialnego, a także podmioty sektora bankowości i infrastruktury rynków finansowych. Incydenty mogą także zgłaszać zwykli obywatele.

W projekcie nowej ustawy KSC zapisano, że przybędzie jeszcze CSIRT INT podległy szefowi Agencji Wywiadu, który ma wspierać obsługę incydentów zgłaszanych przez jednostki podległe ministrowi spraw zagranicznych (w tym placówki zagraniczne RP) oraz przez samą Agencję. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa, który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze. Szczegółowej analizie podlegają systemy niezbędne do świadczenia usługi kluczowej lub cyfrowej.

Jako kryteria oceny zostaną przyjęte wymagania ustawy, normy i standardy w zakresie bezpieczeństwa: ISO/IEC 27001, ISO 22301, NIST SP 800-82, NIST SP 800-53 oraz wymagania i wytyczne Rządowego Centrum Bezpieczeństwa. Normy NIST ułatwiają ocenę usługi w obszarze Industrial Control Systems (ICS) – Systemów Kontroli Przemysłowej, a norma 27001 pozwala na efektywną ocenę takich obszarów, jak: kontrola dostępu, kryptografia czy ochrona przed szkodliwym oprogramowaniem. W zakresie ciągłości pomocą służy norma ISO 22301.

Wszystkie działania podejmowane są, aby utrudnić lub uniemożliwić atak hakerski, jeśli zaś nastąpi – szybko zlikwidować jego skutki. A ataków jest dużo. CERT Polska, funkcjonujący w strukturach Państwowego Instytutu Badawczego NASK, pierwszy powstały w Polsce zespół reagowania na incydenty cyberbezpieczeństwa, zarejestrował w 2021 roku prawie 30 tys. unikalnych incydentów. Ponad 75 proc. obsłużonych incydentów bezpieczeństwa stanowił phishing. Oznacza to prawie dwustuprocentowy wzrost w kategorii takich zdarzeń w porównaniu z poprzednim rokiem. Na stronę z listą ostrzeżeń przed niebezpiecznymi stronami CERT Polska trafiło blisko 42 tys. złośliwych domen, z czego aż 33 tys. w 2021 r. Z ostrzeżeniami można zapoznać się na stronie: https://www.cert.pl/news/single/ostrzezenia_phishing/.

Jak rozpoznać phishing

Nie jest to łatwe, bo czasem zarówno tekst, jak i grafika odzwierciedlają rutynowe e-maile od znanych dostawców. W przypadku faktury zawsze warto sprawdzić adres nadawcy i/lub adres konta bankowego, na które należy wpłacić pieniądze, bo może być fałszywe. Należy również przeczytać, jakich działań oczekuje nadawca e-maila i ewentualnie potwierdzić telefonicznie żądanie, jeśli budzi wątpliwości, lub skontaktować się z administratorem systemu, czy nie zaobserwował dużego napływu e-maili od tego samego nadawcy. Nie należy otwierać załączników, jeśli treść e-maila budzi wątpliwości, bo załącznik może być zainfekowany i zawierać np. ransomware, a jego otwarcie może spowodować np. zaszyfrowanie całego dysku.

Poniżej podajemy siedem elementów, które warto sprawdzać w przypadku otrzymania wątpliwego e-maila:

- **Nieprawidłowa nazwa w adresie nadawcy**

  Zagrożeniem może być e-mail, który zawiera błędnie zapisaną nazwę nadawcy, np. polska_poczta.pl lub w ogóle nie zawiera nazwy firmy/instytucji. Najprawdopodobniej oznacza to, że pochodzi od nieznanej domeny (firmy/instytucje przeważnie mają własne, zarejestrowane domeny) i jest wynikiem oszustwa.

- **Brak Twojego adresu w polu DO: (lub TO:)**

  Podejrzenia może wzbudzić zarówno brak Twojego adresu mailowego, jak i komunikat „undisclosed recipients” (chociaż nie jest to warunek wystarczający, bo czasem np. zaproszenia na wydarzenie rozsyła się do wielu adresatów, a niekoniecznie chcemy ujawniać adresy innych zaproszonych gości) w polu DO: (TO:) – fałszywe e-maile wysyłane są do wielu potencjalnych ofiar jednocześnie. E-maile od zaufanych nadawców skierowane są tylko i wyłącznie do Ciebie.

- **Nieprawidłowy adres strony internetowej nadawcy – URL**

  W treści fałszywego e-maila możesz np. znaleźć link do strony, przez którą np. masz dokonać aktualizacji swoich danych. Nigdy nie korzystaj z linków podawanych w e-mailach, a jeśli chcesz sprawdzić URL, wklej adres do nowego okna przeglądarki i zobacz, czy zawiera poprawną nazwę firmy/instytucji (może się różnić jedną literą od oryginalnej, jak np. http://mrbank.pl) oraz czy jej adres wymusza szyfrowaną certyfikatem SSL komunikację z serwerem (https://).

- **Błędy w temacie i treści wiadomości**

  Popularną techniką stosowaną przez hakerów jest używanie w tytułach e-maili słów z błędami ortograficznymi i gramatycznymi, a także cyframi zamiast liter i dużymi literami w środku wyrazów. Ma to na celu ominięcie filtrów antyspamowych. Celowe jest także zamieszczanie błędów w treści e-maila. Hakerzy stosują tę metodę, aby trafić do mniej doświadczonych użytkowników, ponieważ często prowadzą rozpoznanie przy wyborze potencjalnych ofiar ataku. Wiedzą, że jeśli otrzymają odpowiedź na e-mail z błędami, to będą mogli włożyć mniej wysiłku w pozyskanie od niego informacji istotnych dla ich procederu.

- **Brak logo instytucji w treści e-maila**

  Może się zdarzyć, że w sfałszowanym e-mailu nie będzie grafiki i logo firmy/instytucji, pod którą podszywa się nadawca. Obecnie to już rzadkość, ale czasem znajduje się w niej sam tekst.

Wiadomość też znacznie różni się od tych przesyłanych do tej pory przez zaufanego nadawcę krojem czcionki lub kolorem tła.

- **Prośba o podanie informacji**

  Często e-maile od fałszywych nadawców zawierają polecenia do natychmiastowego wykonania jakiejś czynności, np. „musisz kliknąć w ten link teraz". Mogą też zawierać prośbę o podanie i/lub aktualizację informacji osobistych np. numeru PESEL lub numeru konta bankowego albo haseł dostępu do bankowości internetowej. Należy pamiętać, że instytucje finansowe, w tym banki, nie będą żądać podania osobistych informacji pocztą elektroniczną.

- **Podejrzane załączniki**

  Jeśli otrzymałeś e-mail z załącznikiem, to sprawdź, czy ten załącznik nie zawiera pliku z rozszerzeniem: .exe, .scr, .zip, .com, .bat. Jeśli otrzymasz taki załącznik – nie otwieraj go. To prawdopodobne, że zawiera wirusa.

<u>Jeśli otrzymałeś fałszywy e-mail, to:</u>

1. **Prześlij załącznik do wiadomości do producenta oprogramowania antywirusowego i powiadom odpowiedni CSIRT:**
   - https://incydent.cert.pl/ – dla osób fizycznych oraz większości operatorów usług kluczowych, dostawców usług cyfrowych, organów samorządu terytorialnego, a także podmiotów sektora bankowości i infrastruktury rynków finansowych.
   - https://csirt.gov.pl/cer/zglaszanie-incydentu/16,Zglaszanie-incydentu.html – zbiera informacje o incydentach zaistniałych w jednostkach administracji rządowej i u operatorów infrastruktury krytycznej.
2. **Poproś swojego informatyka o stworzenie reguł filtrujących korespondencję pod kątem nazwy zainfekowanego załącznika.**
3. **Jeśli to był e-mail od rzekomo uznanego dostawcy (np. banku), prześlij informację do tej firmy oraz poinformuj współpracowników o takim wydarzeniu.**

Na zakończenie działań sprawdź, czy na stronie https://haveibeenpwned.com/ Twój e-mail nie jest dostępny dla innych, ponieważ pojawił się w którymś z wycieków danych. Jeśli tak było, to powinieneś natychmiast zmienić hasło, ale pamiętaj nigdy nie używaj tego samego hasła do różnych zasobów. Jeśli tak zrobisz, to kompromitacja jednego z nich spowoduje zagrożenie wszystkich serwisów, w których takiego hasła użyłeś. Hasło powinno mieć długość przynajmniej 12 znaków (rekomendacje CERT Polska można znaleźć pod adresem https://cert.pl/hasla/).

Stosuj wieloskładnikowe uwierzytelnianie – MFA (Multi Factor Authentication) użytkownika, co oznacza nie tylko podanie nazwy i hasła dostępu, ale też dodatkowego elementu, np. SMS-a otrzymanego na smartfon, biometrii, klucza Yubikey lub użycia aplikacji takiej jak „Google Authenticator" czy „Microsoft Authenticator". Zabezpieczenie biometryczne, zwłaszcza odcisk palca, jest stosunkowo łatwo złamać. Jedno dobre zdjęcie dłoni wystarczy, by przechwycić

wzór odcisku palca i przetworzyć go na klucz biometryczny, który posłuży do złamania zabezpieczeń. Znacznie pewniejszym zabezpieczeniem jest obraz tęczówki, czy układu naczyń krwionośnych w dłoni. Trzeba też pamiętać, że cech biometrycznych, które dostały się w niepowołane ręce – skompromitowana osoba nie może, w przeciwieństwie do hasła, zmienić.

Socjotechniczna ucieczka

28-letni Neil Moore z Londynu odsiadywał wyrok w więzieniu Wandsworth za kradzież blisko 2 milionów funtów. Kradzieży dokonywał, podszywając się pod pracowników znanych banków (Barclays, Lloyds, Santander) i kradnąc ich tożsamości. Podobną technikę wykorzystał, aby uciec z więzienia. W niejasny sposób, którego władze więzienia nie potrafią wyjaśnić, zdobył smartfon. Wykorzystując zdalny dostęp do internetu, kupił domenę o nazwie podobnej do sądowej. W ramach tej domeny zbudował pocztę elektroniczną, która posłużyła mu do wysłania do komendanta więzienia e-maila z informacją, że należy niezwłocznie wypuścić więźnia Moore'a. Nadawcą e-maila był rzekomo jeden z prowadzących jego sprawę, powiedzmy, urzędników. Polecenie wykonano i Moore wyszedł na wolność. Ucieczka wyszła na jaw dopiero po kilku dniach. Moore'a złapano po jakimś czasie i osadzono z powrotem w więzieniu. Sprawa była szeroko komentowana w mediach brytyjskich. Szczegóły wydarzenia: http://www.bbc.com/news/uk-england-london-32095189.

WAŻNE RADY

Jak wyłączyć skradziony telefon komórkowy?

Aby sprawdzić numer seryjny swojego telefonu komórkowego, wciśnij następujące klawisze w telefonie:

* # 06 #
15-cyfrowy kod (IMEI) pojawi się na ekranie.

Możesz też sprawdzić kod na kartonie Twojego telefonu (zwykle w formie naklejki).

Ten numer jest unikalny dla Twojego telefonu. Zapisz go i schowaj w bezpieczne miejsce.

Gdy telefon zostanie skradziony, możesz zadzwonić do swojego providera (dostawcy usług telefonicznych) i podać mu ten kod. Najpierw jednak powinieneś zgłosić fakt kradzieży na policji.

Operator będzie miał możliwość zablokowania Twojego telefonu, nawet jeśli złodziej zmieni kartę SIM. Telefon będzie całkowicie bezużyteczny.

Prawdopodobnie nie otrzymasz swojego telefonu z powrotem, ale przynajmniej będzie wiadomo, że ktoś, kto go ukradł, nie będzie mógł z niego korzystać ani sprzedać go dalej.

Przed przystąpieniem do pracy należy upewnić się, czy:

- Twoja przeglądarka internetowa jest w aktualnej wersji
- Twoja poczta elektroniczna nie została przejęta przez nieuprawnione osoby
- Twój system antywirusowy jest zaktualizowany

Aktualizacja systemu i przeglądarek jest konieczna, ponieważ często atakujący uzyskują dostęp do prywatnych danych, wykorzystując luki w systemach operacyjnych urządzeń (komputerów, telefonów) lub w oprogramowaniu takim, jak np. przeglądarki internetowe. Zazwyczaj systemy same informują o konieczności aktualizacji i warto wyrazić na to zgodę. Najpopularniejsze przeglądarki aktualizują się same, ale dobrze jest sprawdzać, czy zainstalowane w nich wtyczki nie wymagają odświeżenia.

DEZINFORMACJA ONLINE: JAK JĄ ROZUMIEĆ I JAKIE SĄ ŚRODKI PRAWNE JEJ ZWALCZANIA

Konieczne jest systemowe uregulowanie dezinformacji na poziomie prawa unijnego. Służyć temu ma unijny akt o usługach cyfrowych. Nie wyklucza to równoległego przyjmowania krajowych regulacji w tym zakresie.

Xawery Konarski
członek Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Kancelaria Traple Konarski Podrecki i Wspólnicy

Dezinformacja, czyli świadome rozpowszechnianie nieprawdziwych lub wprowadzających w błąd informacji, ma na celu podważanie zaufania do instytucji, społeczeństw i konkretnych ludzi. Towarzyszy nam ona od początku ludzkości (pisał już o niej m.in. starożytny teoretyk sztuki wojny – Sun Zi), jednak rozwój technologii cyfrowych, w tym przede wszystkim komunikacyjnych, spowodował, że nigdy wcześniej rozpowszechnianie tego rodzaju informacji nie było tak łatwe, umożliwiając tym samym wpływ na opinie i decyzje podejmowane nie tylko przez jednostki, ale wręcz ogół społeczeństwa.

W konkretnych celach

Działania dezinformacyjne podejmowane są z różnych powodów – głównie dla realizacji celów politycznych i/lub chęci osiągnięcia zysku ekonomicznego. Ich wynikiem może być zarówno wywołanie szkody publicznej (np. naruszenie demokratycznego procesu wyborczego), jak i szkody osobowej (np. naruszenie dobrego imienia konkretnej osoby).

Na przestrzeni ostatnich latach byliśmy świadkami kampanii dezinformacyjnych dotyczących tak kluczowych społecznie kwestii, jak skuteczność szczepień na COVID-19 czy szkodliwość dla zdrowia sieci komórkowej piątej generacji (5G). W zgodnej opinii dezinformacja wpłynęła również na wynik referendum w Wielkiej Brytanii w sprawie Brexitu, a także wybory prezydenckie w Stanach Zjednoczonych (2016).

Mimo powszechnej świadomości negatywnych konsekwencji, jakie niesie ze sobą dezinformacja, stosunkowo mała jest wiedza o tym, jakie regulacje prawne mające na celu jej zwalczanie obowiązują w Unii Europejskiej, a także jakie zasady odpowiedzialności zostały w tym zakresie ustanowione. Akty prawne dotyczące dezinformacji nieraz mylone są z regulacjami mającymi na celu zwalczanie

innych niekorzystnych zjawisk w internecie, takich jak np. mowa nienawiści. Warto w związku z tym dokonać przeglądu tych przepisów.

Dezinformacja na gruncie prawa unijnego

Najbardziej znanym aktem prawnym, mającym na celu zwalczanie dezinformacji, jest opublikowany przez Komisję Europejską we wrześniu 2018 r. kodeks postępowania w zakresie zwalczania dezinformacji (dalej „kodeks" lub „kodeks unijny o dezinformacji"). Przystąpienie do kodeksu jest dobrowolne, a jego sygnatariuszami są największe firmy internetowe (m.in. Facebook, Google, Microsoft, Tik-Tok, Twitter), jak również organizacje branżowe. Podmioty te zobowiązały się do podjęcia określonych działań ograniczających wpływ dezinformacji m.in. w takich obszarach jak: transparentność sponsorowanych treści, identyfikacja fałszywych kont i botów, przejrzystość i możliwość weryfikacji algorytmów, czy dostęp do różnorodnych źródeł informacji. Jedyną sankcją za naruszenie kodeksu jest wykluczenie danego podmiotu jako jego sygnatariusza, nie wprowadzono w nim natomiast np. możliwości nakładania kar za jego nieprzestrzeganie.

Zgodnie z kodeksem, za dezinformację uważa się „możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, które są tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub zamierzonego wprowadzenia w błąd opinii publicznej oraz w swoim zamyśle mogące wyrządzić szkodę publiczną".

W świetle tej definicji na dezinformację składają się łącznie cztery elementy. Po pierwsze, obejmuje ona nie tylko informacje fałszywe, ale również „wprowadzające w błąd". Po drugie, informacja nieprawdziwa to taka, która ma „zdatność" do jej zweryfikowana pod kątem rzetelności. Po trzecie, informacje te muszą być świadomie rozpowszechniane w celu uzyskania korzyści gospodarczych lub wyrządzenia szkody publicznej. Pojęcie „szkody publicznej" rozumiane jest w kodeksie jako „zagrożenie dla demokratycznych procesów politycznych i kształtowania polityki oraz dla dóbr publicznych, takich jak ochrona zdrowia obywateli UE, środowisko naturalne lub bezpieczeństwo". Po czwarte, dla przypisania danemu działaniu cechy rozpowszechniania dezinformacji wystarczy już sam stan zagrożenia, nie jest natomiast konieczne stwierdzenie wystąpienia szkody nią spowodowanej (np. w postaci wypaczenia wyniku wyborów).

W ostatnich latach byliśmy świadkami kampanii dezinformacyjnych dotyczących tak kluczowych społecznie kwestii, jak skuteczność szczepień na COVID-19, czy szkodliwość dla zdrowia sieci komórkowej piątej generacji

W tym kontekście należy podkreślić, że nie każde rozpowszechnianie informacji nieprawdziwych lub wprowadzających w błąd będzie dezinformacją w rozumieniu prawnym. Istotne jest bowiem, aby działanie takie było wykonywanie świadomie, w celu osiągnięcia zysku ekonomicznego lub niekorzystnego wpływu na procesy społeczne. W kodeksie unijnym, mówiąc o dezinformacji, skoncentrowano się wyłącznie na zapobieżeniu wystąpieniu szkody publicznej,

poza zakresem tego pojęcia znalazła się natomiast szkoda osobowa ponoszona przez konkretne jednostki (a nie całe społeczeństwo) w wyniku rozpowszechniania informacji tego rodzaju.

Polskie regulacje

W chwili obecnej w Polsce brak jest jednego aktu prawnego wprowadzającego środki prawne zwalczania dezinformacji.

Jeżeli chodzi o szkody osobowe spowodowane tego rodzaju działaniami, to dotknięte nimi osoby mogą przede wszystkim skorzystać z możliwości, jakie dają im przepisy Kodeksu cywilnego dotyczące ochrony dóbr osobistych (np. dobrego imienia), określone w art. 23 i n. k.c., względnie przepisy kodeksu karnego dotyczące zniesławienia (art. 212 k.k.). W przypadku, gdy źródłem tego rodzaju informacji jest dziennikarz, zastosowanie mogą ewentualnie znaleźć również przepisy prawa prasowego, w szczególności art. 12. Zgodnie z nim „dziennikarz jest zobowiązany zachować szczególną staranność i rzetelność przy zbieraniu i wykorzystaniu materiałów prasowych, a w szczególności sprawdzać zgodność z prawdą uzyskanych wiadomości lub podać ich źródło".

Jeżeli chodzi o szkody publiczne wywołane dezinformacją, obecnie w Polsce obowiązują jedynie przepisy zwalczające rozpowszechnianie nieprawdziwych informacji w związku z kampanią wyborczą. Zgodnie z art. 111 § 1 kodeksu wyborczego, kandydatowi przysługuje m.in. prawo do wniesienia do sądu okręgowego wniosku o wydanie orzeczenia zakazu rozpowszechniania takich informacji. Wniosek taki ma zostać rozpoznany w ciągu 24 godzin w postępowaniu nieprocesowym. Równie szybki jest termin na wniesienie zażalenia na takie rozstrzygnięcie i jego rozpatrzenia przez sąd apelacyjny, a publikacja sprostowania, odpowiedzi lub przeprosin powinna nastąpić najpóźniej w ciągu 48 godzin, na koszt zobowiązanego (art. 111 § 3 i 4).

Publiczne i wyrządzone konkretnym osobom

Pojęcie „dezinformacji", a także środków jej zwalczania, zostało również określone w opracowanym przez Ministerstwo Sprawiedliwości projekcie ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych (dalej „ustawa wolnościowa"). Zgodnie z art. 3 pkt 5 projektu za dezinformację należy uważać „fałszywą lub wprowadzającą w błąd informację, wytworzoną, zaprezentowaną i rozpowszechnioną dla zysku lub naruszenia istotnego interesu publicznego albo wyrządzającą krzywdę osobową lub szkodę majątkową".

W projekcie jednoznacznie przesądzono, że dezinformacja ma charakter bezprawny (art. 3 pkt 6). W odróżnieniu od kodeksu unijnego o dezinformacji, polski projektodawca uwzględnił nie tylko szkody publiczne, lecz także wyrządzone konkretnym osobom. Zgodnie z projektem adresatami obowiązków określonych w ustawie wolnościowej są tylko najwięksi dostawcy serwisów społecznościowych (np. Facebook, Twitter). Przesądza o tym treść art. 3 pkt 1 projektu, zgodnie z którym przez „internetowy serwis społecznościowy" rozumie się usługę świadczoną drogą elektroniczną, z której na terytorium Rzeczypospolitej Polskiej korzysta co najmniej milion użytkowników. Podmioty te są zobowiązane do rozpatrzenia zgłoszeń rozpowszechniania treści o charakterze bezprawnym i podjęcia decyzji o ograniczeniu dostępu do treści lub ograniczeniu dostęp do profilu użytkownika albo odmowie ograniczenia dostępu do treści lub ograniczenia dostępu

do profilu użytkownika. Za naruszenie tego obowiązku ma grozić odpowiedzialność karna, a na usługodawców serwisów społecznościowych może zostać nałożona kara grzywny. W chwili przygotowywania niniejszej publikacji projekt ustawy wolnościowej nie został jeszcze przyjęty przez Radę Ministrów i trudno w związku z tym ocenić, czy i w jakim ostatecznie kształcie zostanie on przyjęty. Niewątpliwie jednak jego znaczenie już teraz wyraża się w próbie zdefiniowania „dezinformacji" i uznania jej bezprawnego charakteru.

W innych państwach

Środki prawne zwalczania dezinformacji zawarte zostały również w ustawodawstwach kilkunastu państw Unii Europejskiej. Różnią się one przy tym przyjętą metodą regulacyjną, przedmiotem ochrony oraz zasadami odpowiedzialności za rozpowszechnianie tego rodzaju informacji.

W niektórych państwach Unii Europejskiej wprowadzono regulację horyzontalną, tzn. zakazano rozpowszechniania dezinformacji w każdym kontekście, o ile tylko istnieje zagrożenie szkodą publiczną. Przykładem jest Malta. Z kolei w innych krajach UE przyjęto rozwiązania wertykalne, czyli ustanowiono przepisy prawne zwalczające dezinformację tylko w kontekście konkretnych obszarów nią dotkniętych, takich jak COVID-19 (np. Węgry), czy organizacja procesu wyborczego (np. Francja).

Jeżeli chodzi o zasady odpowiedzialności, dominują dwa podstawowe modele: odpowiedzialność karna (np. Cypr, Czechy, Grecja, Litwa, Malta) albo odpowiedzialność administracyjna (np. Francja).

Przedstawiona krótka analiza stanu prawnego odnośnie do zwalczania dezinformacji na podstawie prawa Unii Europejskiej, czy poszczególnych ustawodawstw państw członkowskich, pozwala na poczynienie kilku uwag o charakterze generalnym.

Adresatami obowiązków określonych w ustawie wolnościowej są tylko najwięksi dostawcy serwisów społecznościowych (np. Facebook, Twitter)

Po pierwsze, z uwagi na bardzo dużą fragmentaryzację tych rozwiązań, konieczne jest systemowe uregulowanie dezinformacji na poziomie prawa unijnego. Cel ten ma być osiągnięty poprzez uchwalenie unijnego aktu o usługach cyfrowych (AUC), nad którym obecnie trwają intensywne prace. Z uwagi na charakter prawny aktu (rozporządzenie unijne), przyjęte rozwiązania będą obowiązywały na terytorium całej Unii. Główne zadania w zwalczaniu nielegalnych treści, w tym również dezinformacji, nałożone zostały na platformy internetowe.

Po drugie, ewentualne uchwalenie AUC nie wyklucza równoległego przyjmowania krajowych regulacji w zakresie dezinformacji. W tym kontekście szczególnie istotne wydaje się uchwalenie przepisów mających na celu zapobieżeniu szkodzie publicznej wyrządzonej w wyniku rozpowszechniania tych informacji (np. wypaczenie wyników wyborów).

Po trzecie, w ramach dyskusji o uchwalaniu regulacji zwalczających dezinformację, trzeba również pamiętać o tym, że przyjęcie zbyt rygorystycznych środków w tym zakresie może powodować tzw. *chilling effect* wśród podmiotów zagrożonych tego rodzaju odpowiedzialnością i skutkować zagrożeniem dla wolności słowa.

STRUKTURA SYSTEMU CYBERBEZPIECZEŃSTWA

Ochrona internetu jest wspólną odpowiedzialnością, która jest oparta na koordynacji działań między wieloma podmiotami.

Tomasz Klekowski
Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo,
Polskie Towarzystwo Informatyczne

Rządy i organy ścigania odgrywają ważną rolę w ochronie internetu przed cyberprzestępczością. Są odpowiedzialne za opracowywanie i egzekwowanie przepisów i regulacji związanych z cyberbezpieczeństwem oraz za prowadzenie dochodzeń i ściganie cyberprzestępców. W Polsce najważniejszą regulacją jest ustawa o krajowym systemie cyberbezpieczeństwa uchwalona w lipcu 2018[1] i później nowelizowana, która jest zharmonizowana z europejską dyrektywą NIS. Obecnie trwają prace nad wdrożeniem zaleceń uaktualnionej dyrektywy NIS2.

Rola organizacji

Dużą rolę w zapewnianiu bezpieczeństwa cybernetycznego odgrywają organizacje odpowiedzialne za utrzymanie infrastruktury internetowej. Należą do nich trzy główne grupy podmiotów: właściciele sieci szkieletowej, (Network Service Providers), operatorzy punktów wymiany ruchu internetowego (Internet Exchange Points) oraz dostawcy usług internetowych (Internet Service Providers).

W Polsce funkcjonuje ponad 30 podmiotów zajmujących się utrzymaniem sieci szkieletowej i organizacją wymiany ruchu internetowego, w tym 18 punktów wymiany ruchu internetowego[2]. Podmioty utrzymujące infrastrukturę internetu i dostawcy usług internetowych są odpowiedzialni za zapewnienie dostępu do internetu i jako tacy odgrywają kluczową rolę w ochronie internetu przed cyberprzestępczością. Dostawcy usług internetowych mogą monitorować swoje sieci pod kątem podejrzanej aktywności, blokować złośliwy ruch oraz współpracować z organami ścigania i innymi organizacjami w celu reagowania na zagrożenia cybernetyczne.

Zarządzanie incydentami

Kolejnym ważnym elementem systemu cyberbezpieczeństwa są zespoły reagowania na incydenty komputerowe (CERT). CERT-y to organizacje odpowiedzialne za zarządzanie incydentami cyberbezpieczeństwa i reagowanie na nie. Współpracują ze sobą i innymi organizacjami, aby dzielić się informacjami o zagrożeniach, koordynować reagowanie na incydenty i promować najlepsze praktyki w zakresie reagowania na incydenty. Ustawa o krajowym systemie cyberbezpieczeństwa

1 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220001863

2 https://datacatalog.worldbank.org/search/dataset/0037932

ustanawia trzy główne – organizowane na poziomie krajowym – zespoły reagowania na incydenty bezpieczeństwa komputerowego:

- CSIRT GOV prowadzony przez Agencję Bezpieczeństwa Wewnętrznego,
- CSIRT NASK prowadzony przez Naukową i Akademicką Sieć Komputerową
- oraz CSIRT MON prowadzony przez resort obrony narodowej.

W Polsce funkcjonują również CERT-y prowadzone przez firmy i organizacje działające w różnych sektorach, głównie telekomunikacji, ale również w bankowym i akademickim.

W organizacji systemu cyberbezpieczeństwa ważną rolę odgrywają również organizacje międzynarodowe np. Międzynarodowy Związek Telekomunikacyjny (ITU), Internet Governance Forum czy Cloud Security Alliance, międzynarodowe organizacje branżowe, jak np. Tech Accord, jak i krajowe organizacje, w tym Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, których rolą jest promowanie najlepszych praktyk i standardów w zakresie cyberbezpieczeństwa w swoich obszarach działania. Współpracują one również z innymi podmiotami w celu promowania świadomości i edukacji w zakresie cyberbezpieczeństwa.

ENISA i jej zadania

Ważną rolę w organizowaniu cyberbezpieczeństwa w Unii Europejskiej odgrywa Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Do jej obowiązków należy wspieranie państw członkowskich UE w opracowywaniu i wdrażaniu krajowych strategii cyberbezpieczeństwa, zapewnianie państwom członkowskim UE wytycznych i wiedzy fachowej w zakresie opracowywania i wdrażania krajowych strategii cyberbezpieczeństwa, opracowanie ram i wytycznych dotyczących cyberbezpieczeństwa.

Pomagają też firmy

Dużą rolę w działaniu systemu cyberbezpieczeństwa odgrywają również firmy. Największe, które posiadają wysoce wyspecjalizowane organizacje, zajmują się współpracą z rządami i różnymi podmiotami w celu koordynacji działań ochrony cybernetycznej na całym świecie. Przykładem takiej organizacji jest Microsoft Digital Crime Unit[3], która współpracuje z instytucjami państwowymi ponad trzydziestu krajów.

Rola CERT-ów

CERT (Computer Emergency Response Team) to grupa ekspertów ds. cyberbezpieczeństwa odpowiedzialnych za zarządzanie i reagowanie na incydenty cyberbezpieczeństwa. CERT-y są zazwyczaj tworzone przez organizacje lub rządy w celu zapewnienia scentralizowanego punktu kontaktowego dla incydentów cyberbezpieczeństwa i koordynowania reakcji na te incydenty.

Podstawową rolą CERT-ów jest zapobieganie cyberatakom, wirusom komputerowym i innym formom cyberzagrożeń oraz reagowanie na nie. Obejmuje to identyfikowanie, analizowanie i ograniczanie zagrożeń cyberbezpieczeństwa, a także udzielanie wskazówek i wsparcia osobom i organizacjom dotkniętym incydentami cyberbezpieczeństwa.

CERT-y zazwyczaj działają 24 godziny na dobę, siedem dni w tygodniu i utrzymują bliskie relacje z innymi zespołami CERT i organizacjami cyberbezpieczeństwa na całym świecie.

3 https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/

Powinny się również angażować w szkolenia i edukację na temat najlepszych praktyk w zakresie cyberbezpieczeństwa oraz działania na rzecz promowania świadomości problemów związanych z cyberbezpieczeństwem wśród obywateli i organizacji.

Krajowy CERT i CERT-y sektorowe

CERT-y są zorganizowane na różne sposoby w zależności od ich celu. Krajowy CERT jest ustanawiany przez rząd, aby służyć jako główny punkt kontaktowy w zakresie zarządzania incydentami cybernetycznymi, które mają wpływ na kraj, i reagowania na nie. Krajowe zespoły CERT zazwyczaj ściśle współpracują z innymi agencjami rządowymi i dostawcami infrastruktury krytycznej.

CERT-y sektorowe są zorganizowane w celu rozwiązania problemów dotyczących cyberbezpieczeństwa w określonej branży lub sektorze, takim jak opieka zdrowotna, finanse lub transport. Zespoły te dysponują specjalistyczną wiedzą na temat unikalnych wyzwań stojących przed ich sektorem.

W Polsce do najważniejszych CERT-ów należą:

- **CERT Polska (CSIRT GOV):** krajowy zespół reagowania na incydenty komputerowe w Polsce, odpowiedzialny za zarządzanie i reagowanie na incydenty cybernetyczne, które dotykają kraj. Działa w ramach ABW.
- **NASK-CERT (CSIRT NASK)**: prowadzony przez Naukową i Akademicką Sieć Komputerową (NASK), odpowiedzialny za koordynację reakcji na incydenty cyberbezpieczeństwa dotykające ogólnopolską sieć badawczo-akademicką.
- **CSIRT.PL:** prowadzony przez Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS)[4], odpowiedzialny za zarządzanie i reagowanie na incydenty cyberbezpieczeństwa dotykające sieć akademicką i badawczą.
- **CERT Orange Polska:** prowadzony przez Orange Polska, odpowiedzialny za zarządzanie i reagowanie na incydenty cyberbezpieczeństwa mające wpływ na sieć i usługi firmy.
- **CERT T-Mobile:** odpowiedzialny za zarządzanie i reagowanie na incydenty cyberbezpieczeństwa mające wpływ na sieć i usługi spółki[5].
- **CERT Poczta Polska**, który rozwija się i włącza we współpracę z CERT-ami rządowymi.
- **Bank Pekao CERT:** - prowadzony przez Bank Pekao, odpowiedzialny za zarządzanie i reagowanie na incydenty cyberbezpieczeństwa mające wpływ na sieć i usługi banku.

Współpraca ważna dla CERT-ów

CERT-y w celu przeciwdziałania cyberatakom współpracują ze sobą i innymi organizacjami na kilka sposobów. Zespoły CERT udostępniają informacje o zagrożeniach i lukach w zabezpieczeniach sobie nawzajem i innym organizacjom. Może to obejmować udostępnianie raportów, analizy zagrożeń, próbek złośliwego oprogramowania i innych informacji, które mogą pomóc innym zespołom CERT wykrywać cyberataki i reagować na nie.

CERT-y mogą koordynować działania ze sobą i innymi organizacjami, aby reagować na cyberataki. Może to obejmować współpracę w celu zbadania incydentów, dzielenie się najlepszymi praktykami w zakresie reagowania na incydenty i koordynowanie komunikacji z zainteresowanymi stronami.

4 https://www.pcss.pl/cyberbezpieczenstwo/

5 https://cert.t-mobile.pl/

NIEOCZYWISTE DZIAŁANIA POCZTY POLSKIEJ W ZAKRESIE CYBERBEZPIECZEŃSTWA

Bezpieczeństwo w cyberprzestrzeni, w przypadku tak dużej firmy, jak Poczta Polska, to nieoczywisty, ale istotny obszar działalności spółki bezpośrednio wpływający na stabilność biznesu.

Dzięki intensyfikacji – w ostatnich latach – budowania zdolności w obszarze cyberbezpieczeństwa, Poczta Polska osiągnęła dojrzałość w trzech aspektach: osobowym, procesowym i technologicznym. Pozyskiwanie specjalistów do struktur nie jest łatwe, jednak udało się stworzyć zespół o bardzo wysokich kompetencjach.

Bardzo ważnym elementem cyberbezpieczeństwa jest obszar procesowy dotyczący strategii, polityk, procedur i procesów. W 2021 roku w Poczcie Polskiej opracowano nową Politykę Bezpieczeństwa Informacji. Pozwoliło to na uruchomienie prac nad dostosowaniem istniejących regulacji do nowej PBI. W tym zakresie realizowano działania związane z opracowaniem kilkudziesięciu regulacji, tj. wewnętrznych aktów prawnych lub procedur z obszaru cyberbezpieczeństwa. Większość dokumentów zostało już wprowadzonych do stosowania, a ostatnie z nich weszły w końcowy etap wewnętrznej legislacji.

W Poczcie Polskiej działa również CERT, pracujący w trybie 24/7/365. To zespół nadzoru i raportowania stanu cyberbezpieczeństwa spółki, którego odbiorcami jest kierownictwo Centrum Transformacji Cyfrowej oraz zarząd spółki. Jednocześnie w I kwartale 2022 roku CERT rozpoczął realizację przedsięwzięć wynikających z sytuacji międzynarodowej i z wprowadzonego na terenie Rzeczpospolitej Polskiej stanu alarmowego Charlie CRP.

W ramach współpracy międzynarodowej CERT Poczty Polskiej uzyskał status „Listed" w organizacji TF-CSIRT Trusted Introducer, który powoduje umieszczenie informacji o tej jednostce w globalnym katalogu zespołów reagowania na incydenty naruszenia bezpieczeństwa teleinformatycznego. Obecnie CERT Poczta Polska prowadzi prace techniczno-organizacyjne związane z przygotowaniem do przystąpienia do stowarzyszenia zespołów reagowania na incydenty cyberbezpieczeństwa FIRST.org oraz osiągnięcia statusu „Accredited" w organizacji TF-CSIRT Trusted Introducer.

Funkcjonowanie systemu związanego z zapewnieniem bezpieczeństwa teleinformatycznego w tak dużej firmie, jak Poczta Polska, wymaga posiadania odpowiedniej technologii. W związku z tym, na przestrzeni ostatnich dwóch lat, zmodernizowano system cyberbezpieczeństwa, czyli zrealizowano bardzo istotne i dostrzegalne działania. Stopniowo pozyskiwano urządzenia oraz odpowiednie systemy.

ORANGE: JESTEŚMY O KROK PRZED PRZESTĘPCAMI

Nie wydadzą polecenia zarażonemu komputerowi, nie zajrzą do jego zawartości, nie uzyskają wykradzionych danych, czy nie wydadzą polecenia zaszyfrowania plików.

CERT Orange Polska (ang. Computer Emergency Response Team, zespół reagowania na zagrożenia cyberbezpieczeństwa) to specjalistyczna jednostka, odpowiedzialna za bezpieczeństwo użytkowników internetu.

A po ludzku? Nasza codzienna działalność to przede wszystkim coś, co zbiorczo można określić mianem CyberTarczy. Grupa systemów, rozwiązań, procedur i mechanizmów uczenia maszynowego. Nierzadko pozwalają nam one blokować domeny, zanim zostaną po raz pierwszy wykorzystane przez przestępców! A to przekłada się na realne ustrzeżenie internautów przed ryzykiem utraty loginów, haseł i oszczędności całego życia. CyberTarcza uniemożliwia też komunikację zainfekowanych już urządzeń ze złośliwą infrastrukturą. Dzięki temu przestępcy nie wydadzą polecenia zarażonemu komputerowi, nie zajrzą do jego zawartości, nie uzyskają wykradzionych danych.

W codziennej pracy eksperci CERT Orange Polska spotykają się z wieloma przykładami czy to braku wiedzy, czy zwykłej niefrasobliwości. Każdy z nas, kto zdawał na prawo jazdy, uczył się zasady ograniczonego zaufania. Skoro zdajemy sobie sprawę, jak ważna jest ona na ulicy, dlaczego w sieci dla wielu nie jest to tak oczywiste? W sytuacji, gdy strefy online i offline przenikają się w każdej sferze życia, zagapienie się przy korzystaniu z telefonu może zakończyć się włamaniem do firmowej sieci czy utratą oszczędności życia.

Dzisiejszy świat cyberzagrożeń to, w lwiej części, świat phishingu i socjotechnicznych sztuczek. Dlatego kluczowa jest edukacja internautów. Przemyślana edukacja, ukierunkowana na zagrożenia jako takie, a nie potencjalne ryzyko dla sieci korporacyjnej czy zasobów przedsiębiorstwa. Jeśli nauczymy pracownika, na co generalnie powinien uważać, nie zapomni o tym przecież, gdy zaloguje się do pracy? Edukując internautę (przez pryzmat zagrożeń dla domu, dzieci, seniorów, osób mniej świadomych cyfrowo, no i wreszcie własnych danych czy pieniędzy), zyskamy wdzięcznego i świadomego pracownika.

Na ogólnodostępnych stronach cert.orange.pl czy blog.orange.pl, a także na naszym Twitterze @cert_opl ostrzegamy o nowych zagrożeniach i często do znudzenia przypominamy te same, stosowane przez przestępców schematy. Dlatego pojawiamy na konferencjach – nie tylko branżowych. Dlatego też nie odmawiamy prośbom o prelekcje, ucząc o zagrożeniach zarówno klasy nauczania początkowego szkół podstawowych, jak i uczestniczących w zajęciach Uniwersytetu Trzeciego Wieku. Świadomy internauta to bezpieczniejszy internauta. A nas mało rzeczy satysfakcjonuje bardziej niż świadomość, że sieciowemu oszustowi znów się nie udało.

DLACZEGO WAŻNA JEST WSPÓŁPRACA NA LINII EDUKACJA – BIZNES

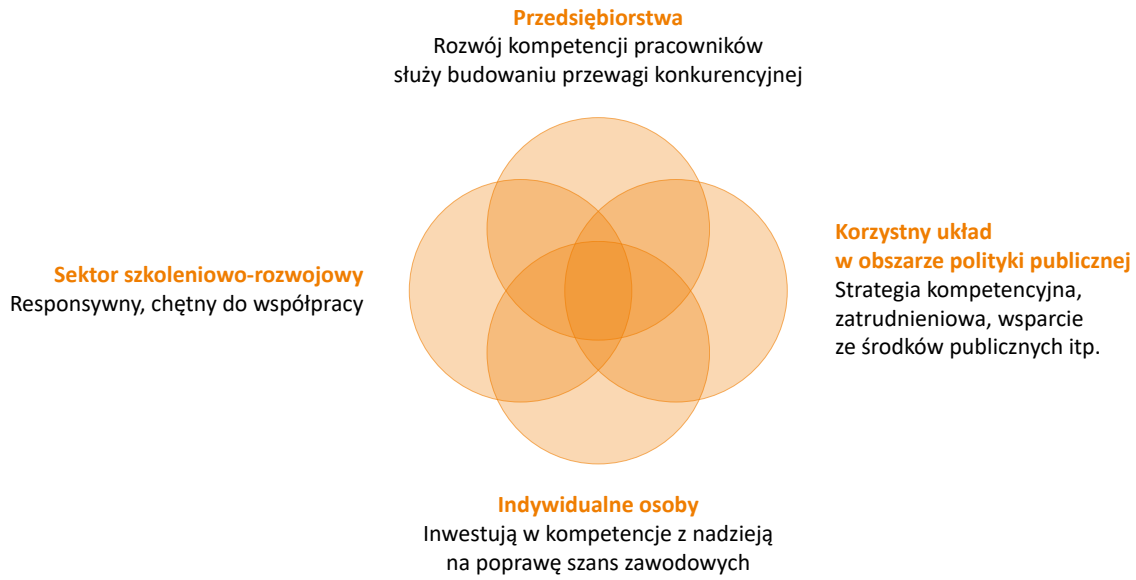
Jest wiele korzyści ze współpracy. Poza oczywistym celem, jakim jest podnoszenie kwalifikacji obecnych oraz przyszłych kadr, istnieją inne: kreowanie przestrzeni dla bezpośredniej wymiany doświadczeń między uczelniami i potencjalnymi pracodawcami z branży.

Maciej Wnuk
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polska Izba Informatyki i Telekomunikacji

Pandemia koronawirusa oraz rosyjska agresja na Ukrainę pokazała, jak ważną rolę pełni branża teleinformatyczna w niemalże każdym sektorze gospodarki. Wraz ze zwiększonym zapotrzebowaniem na coraz to nowsze rozwiązania technologiczne powstało zapotrzebowanie na nowe kompetencje u pracowników, którzy te rozwiązania tworzą. Szybki wzrost zapotrzebowania na nowe kompetencje wiąże się z potrzebą zmian systemowych oraz zwiększonej, efektywnej współpracy edukacji z biznesem.

Steve Whiddett i Sarah Hollyforde w swojej książce pt. „Modele kompetencyjne w zarządzaniu zasobami ludzkimi" zdefiniowali kompetencje w zakresie wykonywanej pracy jako „[…] zespół cech danej osoby, na który składają się charakterystyczne dla tej osoby elementy, jak motywacja, cechy osobowości, umiejętności, samoocena związana z funkcjonowaniem w grupie oraz wiedza, którą ta osoba sobie przyswoiła i którą się posługuje" (S. Whiddett, S. Hollyforde, 2003).

Dr Magdalena Jelonek w swojej publikacji pt. „Kompetencje, potrzeby pracodawców a współodpowiedzialność za zasoby kompetencyjne regionów" przedstawia, stworzony przez Paula Dalziela, model ekosystemu kompetencyjnego jako wpływ relacji i interakcji między aktorami (pracownikami, pracodawcami, związkami zawodowymi, przedstawicielami sektora szkoleniowo-rozwojowego [w tym ze szkołami i uczelniami] oraz decydentami) na aktualną sytuację rynkową lub każdego aktora z osobna (M. Jelonek, 2019).



Źródło: P. Dalziel, „Education and qualifications as skills" (za: M. Jelonek)

Powyższy model ekosystemu kompetencyjnego zakłada potrzebę współpracy czterech aktorów przy rozwoju wymaganych kompetencji przez biznes z branży teleinformatycznej: administracja (ustawodawca i regulator), przedsiębiorcy z sektora teleinformatycznego, sektor szkoleniowo-rozwojowy oraz indywidualne osoby.

John Buchanan i Richard Hall w swoim raporcie pt. *Beyond VET: The Changing Skill Needs of the Victorian Services Industries* stawiają tezę, że poprzez współpracę administracji z biznesem powstają nowe możliwości inwestycyjne, a za tym nowe miejsca pracy (Buchanan, Hall 2003). Jednocześnie decyzje ustawodawców i regulatorów mające wpływ na funkcjonowanie przedsiębiorstw z branży teleinformatycznej dodatkowo wpływają na zmiany w potrzebnych kompetencjach u kadr, aby firmy mogły dostosować się do przepisów prawa. Wiąże się to z kosztami ponoszonymi w dużej części przez biznes.

Decyzje administracji wpływają także na sektor szkoleniowo-rozwojowy i jego obłożenie, ponieważ podstawowym zadaniem tego sektora jest uzupełnianie braków kompetencyjnych na rynku. Jeżeli powstają nowe potrzeby kompetencyjne w związku z regulacjami oraz innowacjami, to sektor szkoleniowo-rozwojowy musi wziąć na swoje barki rozwój kompetencji u swoich uczniów i studentów, czyli przyszłych kadr.

Współpraca między sektorem szkoleniowo-rozwojowym a biznesem jest kluczowa w modelu ekosystemu kompetencyjnego, ponieważ to rynek sygnalizuje, jakich kompetencji potrzebuje, a sektor szkoleniowo-rozwojowy odpowiada za wypracowanie tych kwalifikacji i kompetencji, biznes natomiast powinien wspierać szkoły i uczelnie w ich rozwoju.

Czwartym, ostatnim z aktorów współodpowiedzialnych za rozwój kompetencji jest indywidualna osoba, jej kompetencje (twarde i miękkie) oraz motywacja do ich rozwoju.

Cztery płaszczyzny

Jednym z podstawowych impulsów wzrostu gospodarki są innowacje oparte na bazie wiedzy, edukacji oraz działalności badawczo-rozwojowej. Współpraca oraz wymiana wiedzy między aktorami odpowiedzialnymi za rozwój

kompetencji w branży teleinformatycznej pozwala na szybkie reagowanie na zmieniające się potrzeby kompetencyjne.

W trakcie prac warsztatowych Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo zidentyfikowano cztery płaszczyzny potencjalnej współpracy na linii edukacja – biznes: merytoryczna, projektowa, technologiczna i wizerunkowa. Te płaszczyzny współpracy zidentyfikowane w branży mogą być zastosowane jako model w innych sektorach gospodarki.

Współpraca merytoryczna dotyczy wspólnych działań między biznesem a edukacją, które mają na celu zwiększenie wiedzy w zakresie najnowszych trendów na rynku pracy. Zwiększenie wiedzy nie powinno być skierowane jedynie do uczniów i studentów, ale także do kadry nauczającej.

Współpraca merytoryczna to m.in. współtworzenie programów nauczania oraz podstaw programowych. To działanie pozwala na wskazanie kierunków edukacyjnych dostosowanych do potrzeb kompetencyjnych na rynku pracy. Wraz ze współtworzeniem programów nauczania oraz podstaw programowych, kolejnym działaniem jest oddelegowanie przez biznes specjalistów i ekspertów do prowadzenia zajęć w szkołach. Jest to o tyle istotne działanie, że wiedza może być przekazana bezpośrednio przez pracodawców.

Uczestnicy warsztatów wskazali na dwie kluczowe bariery dotyczące pracy ekspertów przy wykładach czy lekcjach. Jedną z tych barier jest brak możliwości zasobowych do wyznaczenia osoby do prowadzenia takich zajęć (brak czasu pracownika względem innych obowiązków w firmie). Z drugiej strony przedstawiciele szkół technicznych spotykają się z brakiem odpowiednich środków finansowych do zatrudnienia eksperta w danej dziedzinie. Te same problemy pojawiają się przy potrzebie współpracy z ekspertem przy tworzeniu programów naukowych.

Gdy powstanie nowy program nauczania, kolejnym krokiem jest prowadzenie zajęć oraz lekcji. Tutaj potrzebne jest zapewnienie szkoleń dla kadry nauczającej. Bardzo często wiąże się to z potrzebą finansowania. Ten trend powoli się zmienia, ponieważ wielu przedsiębiorców w branży zaczyna oferować darmowe szkolenia oraz webinaria dla kadr nauczających. Istnieją także programy współpracy, oferujące szkolenia i wsparcie. Wraz z wyszkoloną kadrą nauczającą realizacja współtworzonych programów nauczania będzie efektywniejsza.

Pozyskiwanie wiedzy i rozwijanie kompetencji nie musi się odbywać tylko na terenie szkoły i uczelni, podczas zajęć. Jednym z najczęściej stosowanych działań są praktyki dla studentów organizowane przez pracodawców. Niestety, jest to rzadko oferowane uczniom szkół technicznych i firmy skupiają się na takiej współpracy z uczelniami. Szkoły techniczne odgrywają, obok uczelni, jedną z podstawowych ról w rozwijaniu kompetencji i przygotowywaniu przyszłych kadr do rynku pracy w Polsce, w branży.

Współpraca projektowa ma na celu przekazanie praktycznej wiedzy uczniom i studentom. Uczestnicy warsztatów, w tym przedstawiciele firm pracujących w sektorze cyberbezpieczeństwa, wskazali na potrzebę współpracy projektowej, w tym przy projektach badawczo-rozwojowych. Taka współpraca otwiera możliwości długoterminowej współpracy między biznesem i edukacją. Jednocześnie zaangażowanie nauczycieli, wykładowców, uczniów i studentów wspiera rozwój nowych kompetencji. Przedsiębiorcy czerpią z takiej współpracy korzyści poprzez dostęp do przyszłych pracowników, a szkoły i uczelnie przygotowują przyszłych pracowników według potrzeb rynkowych. W wielu przypadkach działania projektowe kończą się na wspólnej komercjalizacji rozwiązań.

W celu rozwoju potrzebnych kompetencji w branży współpraca między biznesem a edukacją powinna mieć również **wymiar technologiczny**. Bez dostępu do nowych technologii i laboratoriów rozwój kompetencji zatrzyma się na poziomie przygotowania teoretycznego. Już teraz pojawiają się oferowane przez firmy platformy certyfikujące pewne kompetencje, które mogą być wykorzystane przez uczniów i kadry nauczające w dalszym rozwoju. Wiele z tych certyfikowanych szkoleń online udostępnianych jest szkołom za darmo. W ten sposób przyszłe kadry mogą zdobyć odpowiednie kompetencje jeszcze na poziomie szkoły średniej, zanim zostaną wypuszczone na rynek pracy. Wielu przedsiębiorców podejmuje się także budowy laboratoriów na uczelniach – w celu testowania rozwiązań i innowacyjnych pomysłów.

Kolejną płaszczyzną jest **współpraca wizerunkowa**, w ramach której przedsiębiorcy i instytucje akademickie organizują wspólne konferencje oraz przyznają patronaty nad swoimi wydarzeniami. Do współpracy wizerunkowej zakwalifikowano także wykłady ekspertów. Takie działania stanowią motywację dla uczniów i studentów do pogłębiania kompetencji. Wykłady eksperckie pokazują możliwości rozwoju zawodowego oraz specjalizacji.

W ramach współpracy wizerunkowej szkół i biznesu powinny być częściej podpisywane listy intencyjne czy porozumienia o współpracy w celach informujących o takim działaniu. Działanie to powinno zachęcić więcej podmiotów rynkowych do współpracy przy rozwoju idealnego modelu kształtowania kompetencji.

Lista korzyści

Jest wiele korzyści ze współpracy na linii edukacja – biznes. Poza oczywistym celem, jakim jest podnoszenie kwalifikacji obecnych oraz przyszłych kadr, istnieją inne korzyści, tj. kreowanie przestrzeni do bezpośredniej wymiany doświadczeń między uczelniami i potencjalnymi pracodawcami z branży.

Platforma wymiany doświadczeń umożliwia działania, czyli wspólne tworzenie ram programowych. Umożliwia również przedsiębiorstwom dostęp do potencjalnych przyszłych pracowników, którzy są w trakcie nauki lub są absolwentami z już posiadanymi, wymaganymi przez rynek, kompetencjami. Z takiej współpracy korzystają wszyscy aktorzy w ekosystemie, ponieważ uczelnie otrzymują możliwość kontaktu z rynkiem, dostępu do nowoczesnych technologii, czy wsparcie dydaktyczne. Biznes otrzymuje możliwość dostępu do rynku pracowników na wczesnym etapie ich rozwoju, możliwość popularyzacji rozwiązań technologicznych lub możliwość budowania marki. Na koniec studenci otrzymują szanse na poznanie potencjalnego rynku pracy, szanse na zdobycie nowej wiedzy wartościowej komercyjnie czy po prostu kontakt z nowymi technologiami, które umożliwiają łączenie teorii z praktyką.

DOBRE PRAKTYKI – JAK MOGĄ WYGLĄDAĆ

W Polsce funkcjonuje wiele przykładów dobrych praktyk, lecz nadal nie jest to wystarczające, aby sprostać zapotrzebowaniu gospodarki na innowacje.

Maciej Wnuk
Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polska Izba Informatyki i Telekomunikacji

W projektach Sektorowych Rad ds. Kompetencji (Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo) jednym z celów jest podejmowanie i realizowanie inicjatyw w obszarze edukacji poprzez animowanie porozumień o współpracy między edukacją a biznesem. Celem takiego porozumienia jest deklaracja współpracy nowej oraz aktualnej. Skupione jest ono na swobodnej wymianie wiedzy i transferze doświadczeń w zakresie prowadzonych przez strony porozumienia działań, których celem będzie wzajemny rozwój i lepsze dopasowanie do oczekiwań otoczenia zewnętrznego (w tym rynku pracy).

Program P-Tech

Celem Rady Sektorowej jest również pokazanie aktualnych dobrych praktyk oraz zainspirowanie innych podmiotów do takiej współpracy. Jednym z programów, który był przedstawiony podczas prac Rady, jest program P-Tech, który jest partnerstwem szkół technicznych i firm z rozwijających się branż, w tym teleinformatycznej. Projekt P-Tech jest globalnym programem IBM. W Polsce został on ogłoszony w 2019 r., przez trzy firmy partnerskie (Fujitsu, IBM, Samsung) oraz trzy szkoły średnie (ZS nr 1 im. Powstańców Wielkopolskich we Wronkach, ZSTiO nr 2 w Katowicach oraz Śląskie Techniczne Zakłady Naukowe w Katowicach). Jest on realizowany we współpracy merytorycznej z Instytutem Badań Edukacyjnych. Od czasu ogłoszenia do programu dołączyli ING Bank Śląski oraz Zespół Szkół Politechnicznych w Łodzi.

W ramach programu P-Tech szkoły partnerskie i klasy w tych szkołach mogą skorzystać z kursów obejmujących cyberbezpieczeństwo, sztuczną inteligencję, data science, blockchain czy design thinking.

Program realizowany jest na zasadzie partnerstwa, gdzie zarówno szkoły, jak i biznes coś wnoszą w kształcenie kompetencji u przyszłych kadr. Określa on w dużej mierze merytoryczną płaszczyznę współpracy, ale nie tylko. Oferowany jest wachlarz rozwiązań, w tym również szkolenia dla kadry nauczającej poprzez moduły edukacyjne w programie. Przewiduje on nie tylko merytoryczny wkład ekspercki na lekcjach, ale także praktyki i płatne staże dla uczniów. P-Tech przygotowuje uczniów do dalszego pogłębiania kompetencji na poziomie uniwersyteckim i daje możliwość zatrudnienia zaraz po maturze.

Udostępniana jest także platforma z możliwością zdobywania certyfikatów online przez uczniów, co pomaga im pogłębiać i dokumentować wiedzę. Jedną z zalet tego programu jest możliwość realizacji wspólnych projektów partnerskich z udziałem biznesu, kadry nauczającej oraz uczniów.

Więcej szczegółowych informacji o programie oraz o możliwości współpracy można znaleźć na poświęconej programowi stronie https://www.ptech.org/pl/

Szkolenia na temat procesu Design Thinking

Kolejnym, bardzo dobrym, przykładem współpracy jest globalny program Samsung Electronics – Solve For Tomorrow, który realizowany jest również w Polsce. Celem tego programu jest wspieranie rozwoju kompetencji przyszłości młodego pokolenia poprzez tworzenie projektów odpowiadających na wyzwania otaczającego świata przy zastosowaniu metody STEAM. Trzonem programu są szkolenia obejmujące proces Design Thinking, zorientowane na rozwiązywanie problemów. Podczas nich uczestnicy programu uczą się pracy projektowej, rozwijając kompetencje: kreatywność, komunikację, kooperację i krytyczne myślenie. Najlepsze pomysły, które powstaną w trakcie procesu, są prezentowane na gali programu.

W pierwszej edycji polskiego programu Solve For Tomorrow (2021/2022) organizatorzy skupili się na tematach związanych ze zdrowiem, z bezpieczeństwem oraz klimatem.

Więcej o programie można się dowiedzieć na stronie: https://solvefortomorrow.pl

Samsung Electronics Polska jednocześnie współpracuje ze Szkołą Główną Handlową. Uczelnia poszerzyła oraz wzmocniła ofertę dla studentów polsko- i anglojęzycznych w ramach następujących kierunków:

- Global Business, Finance and Governance
- International Business
- Technological Environment of International Business
- International Business Environment

Red Hat Academy

Kolejnym przykładem wzorcowej współpracy z uczelniami jest program firmy Red Hat pn. Red Hat Academy. Firma Red Hat to kolejny, po markach IBM oraz Samsung, światowy lider technologiczny, który prężnie rozwija swoją działalność w Polsce. W ramach tego programu uczelnie, które nawiązały współpracę z Red Hat, otrzymują bezpłatny dostęp do szkoleń z innowacyjnych rozwiązań informatycznych, w szczególności w zakresie open source, zakończonych egzaminami oraz certyfikatami. Akademia ma na celu nauczenie studentów podstawowych umiejętności w obszarach Linux, cloud i dev.

Istnieje również możliwość współpracy z globalnymi partnerami oferującymi infrastrukturę pod laboratoria, które są dostępne dla użytkowników platformy. Oferowane jest także miejsce do wymiany doświadczeń oraz dostęp do Red Hat Portal, który łączy studentów z potencjalnymi pracodawcami.

W Polsce program Red Hat Academy jest dostępny w Wojskowej Akademii Technicznej i na Politechnikach: Warszawskiej, Lubelskiej oraz Krakowskiej.

Więcej o programie można się dowiedzieć na stronie: https://www.redhat.com/en/services/training/red-hat-academy

Polskie firmy

Współpraca na linii edukacja – biznes odbywa się nie tylko z globalnymi firmami. Jest również wiele przykładów dobrych praktyk polskich firm takich, jak Globema, Systemics-PAB czy GlobalLogic.

Świetnym przykładem współpracy na linii edukacja – biznes może się pochwalić Globema, która jest sygnatariuszem jednego z porozumień sektorowych zainicjowanych przez Sektorową Radę. Firma nawiązała współpracę z Wydziałem Geodezji i Kartografii na Politechnice Warszawskiej. Początkiem tej współpracy były merytoryczne zajęcia dotyczące metod przetwarzania danych z wykorzystaniem produktu FME oraz tworzenia aplikacji w oparciu o Google Maps Platform. Te początki dały sposobność dalszej współpracy w zakresie organizacji Hackathonów, wspólnych konferencji oraz umożliwienia studentom odbycia praktyk. Realizowana jest także współpraca w kontekście badawczo-rozwojowym w zakresie energetyki rozproszonej.

Realizowane projekty B+R obejmują również inne uczelnie poza Politechniką Warszawską:

- Uniwersytet Warszawski (Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego ICM Meteo) – współpraca w obszarze OZE (wpływ warunków atmosferycznych na sieci energetyczne)
- Politechnika Łódzka – współpraca w obszarze energetyki (symulacje pracy sieci)
- Akademia Górniczo-Hutnicza – współpraca w obszarze energetyki (testy wysokich napięć)

Od 2009 roku Globema jako Centrum Badawczo-Rozwojowe zrealizowała kilkanaście projektów B+R.

Przykłady współpracy z innymi podmiotami to m.in. zdalne warsztaty dla studentów oraz prowadzących zajęcia, dostawa licencji edukacyjnych, kursy wideo, a także kształcenie kadr w ramach programu „Train the Trainer”.

Kolejnym przykładem współpracy polskich firm jest Systemics-PAB, która od początku swojej działalności współpracuje z wyższymi uczelniami technicznymi w Polsce. Ta współpraca opiera się m.in. na informowaniu i dzieleniu się wiedzą praktyczną o trendach rozwojowych w obszarze narzędzi do pomiarów/testów dla szeroko rozumianych środowisk ICT oraz realizacji badań, analiz bieżącego stanu i QoS/QoE sieci mobilnych; prezentacjach produktów i rozwiązań liderów; omawianiu nietypowych przypadków użycia tzw. use case’ów; organizacji i wspieraniu PoC’ów i trialów rozwiązań HW i SW (przykład działania można znaleźć pod tym linkiem https://www.wojsko-polskie.pl/wat/articles/nauka-i-technologia-4/technologia-5g-w-zastosowaniach-wojskowych/).

Systemics-PAB może się także pochwalić ważnymi osiągnięciami, które wpisują się w płaszczyzny współpracy: stała obecność firmy na konferencjach naukowych – KSTiT, KKRRiT (współpraca wizerunkowa); organizacja konferencji naukowo-technicznej „Jakość w sieciach mobilnych” (współpraca wizerunkowa/merytoryczna); współtworzenie kierunku „Informatyka techniczna i telekomunikacja” na uczelniach (współpraca merytoryczna); przygotowywanie projektów R&D z obszaru QoS/QoE w sieciach mobilnych, „big data”, GNSS oraz bezpieczeństwa sieciowego (współpraca technologiczna/projektowa); a także udział w testowaniu technologii przełomowych – 5G w zastosowaniach krytycznych (współpraca projektowa).

Ciekawym przykładem współpracy na linii edukacja – biznes może się pochwalić również kolejna polska firma, GlobalLogic. Realizuje ona program „Student Development Program", który ma na celu aktualizację wiedzy studentów oraz prowadzących zajęcia w zakresie nowych trendów technologicznych. Eksperci firmy prowadzą kursy poza zajęciami na uczelniach, które przeznaczone są dla studentów. Kursy dotyczą nie tylko kwestii technicznych np. nauki języków Java, C#, C++, lecz także skupiają się na szkoleniach z zakresu zapewnienia jakości oprogramowania oraz zarządzania projektami. Mają one na celu uzupełnienie wiedzy na dane tematy, wprowadzenie do dalszych działań związanych z programem oraz innymi aktywnościami prowadzonymi wspólnie z uczelniami. Kolejnym etapem współpracy są staże i praktyki oraz Akademie GL przeznaczone dla studentów ostatniego roku oraz absolwentów. GlobalLogic współpracuje również z uczelniami partnerskimi w zakresie aktualizacji ram programowych oraz budowy laboratoriów dla badań nad internetem rzeczy.

Przykładem wielopłaszczyznowej kooperacji GlobalLogic z edukacją jest współpraca z Uniwersytetem Szczecińskim w ramach porozumienia podpisanego w 2022 roku. Planowane są wspólne badania naukowe, konsultacje badawcze oraz praktyki i staże dla studentów. Firma, jak stwierdziła, chce realizować wiele projektów, ale brakuje jej wykwalifikowanych kadr.

Więcej informacji na temat tej współpracy można znaleźć pod tym linkiem: https://usz.edu.pl/uniwersytet-szczecinski-bedzie-wspolpracowal-z-globallogic/.

Współpraca edukacji z biznesem skupia się nie tylko na tworzeniu nowych rozwiązań, lecz także na badaniach społecznych czy upowszechnianiu nauki. W Polskiej Izbie Informatyki i Telekomunikacji funkcjonuje Grupa Robocza Operatorów Telekomunikacyjnych (GROT), która stara się edukować rynek w zakresie nieszkodliwości pól elektromagnetycznych. Współpraca GROT z sektorem edukacyjnym polega na walce z dezinformacją oraz wspólnych działaniach badawczo-rozwojowych w kontekście społecznym.

Na przykład, w ramach projektu edukacyjnego zajmującego się polami elektromagnetycznymi, PIIT współpracował z Katolickim Uniwersytetem Lubelskim i firmą Kantar, aby przeprowadzić badanie na temat nastawienia Polaków do pola elektromagnetycznego oraz nowych technologii. Badanie dostępne jest pod linkiem https://www.piit.org.pl/__data/assets/pdf_file/0014/19031/Postawy-Polakow-wobec-pola-elektromagnetycznego-oraz-nowych-technologii_Raport-PIIT_FINAL.pdf.

Eksperci naukowi oraz praktycy łączą siły w celu upowszechniania działań CSR w biznesie oraz walki z dezinformacją związaną z nowymi technologiami. Model współpracy GROT z uczelniami jest korzystny dla wszystkich stron, ponieważ polega na trzech fundamentach: specjaliści z uczelni szkolący biznes, praktycy z biznesu szkolący studentów oraz zapewnienie miejsca dla praktykantów i stażystów.

Podane przykłady stanowią tylko niewielką listę doskonałych modeli współpracy na linii edukacja – biznes. W Polsce funkcjonuje wiele przykładów dobrych praktyk, lecz nadal nie jest to wystarczające, aby sprostać zapotrzebowaniu gospodarki na innowacje. Współpraca edukacji z biznesem jest kluczowa w celu zachowania wzrostu innowacyjności nowych rozwiązań teleinformatycznych, które wspierają rozwój gospodarki oraz walkę z różnego rodzaju kryzysami. Zadaniem Sektorowych Rad ds. Kompetencji jest aktywna komunikacja potrzeby takiej współpracy, zachęcanie do niej i pokazanie zainteresowanym, jak ta współpraca mogłaby wyglądać.

Studenci mogą zobaczyć, gdzie w praktyce przydadzą się umiejętności, które zdobywają na uczelni

BARTOSZ LECH

Dyrektor Pionu Aplikacji i Usług Lokalizacyjnych, Globema

Porozumienie sektorowe: Politechnika Warszawska i Globema

Zależy nam na wymianie doświadczenia pomiędzy światem nauki, a światem biznesu – który reprezentujemy. Z jednej strony chcielibyśmy mieć wpływ na kształt programu nauczania i na to, z jakimi umiejętnościami studenci opuszczają uczelnię. Z drugiej, jako przedstawiciele biznesu, chcemy podzielić się wiedzą o tym, jak wygląda praca w Globemie i jakie umiejętności wśród studentów i absolwentów uczelni poszukiwane są na rynku pracy.

W firmie prowadzimy też liczne projekty B+R. Pracujemy przede wszystkim nad rozwiązaniami wykorzystującymi sztuczną inteligencję – m.in. dla sektora energetycznego, w tym sektora energii odnawialnych.

Porozumienie ma na celu ułatwienie przepływu wiedzy i doświadczeń pomiędzy uczelnią, a biznesem. Jest to więc szansa na zmniejszenie rozbieżności pomiędzy tym, co swoim studentom oferują uczelnie, a tym, czego oczekuje od nich rynek pracy. To także szansa na lepsze wykorzystanie potencjału badań naukowych prowadzonych na uczelniach oraz gromadzonej przez nie wiedzy.

Globema tworzy specjalizowane rozwiązania geoprzestrzenne, dostarcza także szereg innych produktów i usług IT między innymi dla przedsiębiorstw z sektora telekomunikacyjnego, ciepłowniczego, elektroenergetycznego i wielu innych. Współpracujemy z największymi firmami z tych branż.

Studenci wydziału Geodezji i Kartografii Politechniki Warszawskiej dysponują umiejętnościami, które wykorzystujemy w pracy nad naszymi projektami.

Podczas studiów pracują m.in. z platformą do integracji i przetwarzania danych FME, której jesteśmy oficjalnym dystrybutorem i wdrażamy projekty z jej wykorzystaniem u klientów w Polsce i za granicą.

Oprac. JŁ

Można stworzyć korzystne warunki dla rozwoju zarówno edukacji, jak i biznesu

SŁAWOMIR KUMKA

Dyrektor Centrum Oprogramowania IBM w Krakowie

IBM: korzyści dla obu stron

Jedną z najbardziej i najszybciej rozwijających się dziedzin współczesnego świata jest technologia. Ten postęp niejednokrotnie wyprzedza edukację. Dlatego też dobre praktyki na linii współpracy edukacji i biznesu mogą przynieść wiele korzyści dla obu stron.

Przykładem takiej działalności może być zaangażowanie firm w tworzenie kwalifikacji zawodowych. IBM jako lider technologiczny ma to wpisane w swoje wartości i realizuje inicjatywy edukacyjne jako jedną ze swoich misji.

W Polsce przykładem wspomnianej działalności jest stworzenie przez IBM kwalifikacji zawodowej w pionierskiej dziedzinie nauki i rozwoju technologicznego, jaką są komputery kwantowe. W oparciu o technologię IBM Quantum Computing IBM stworzył kwalifikację „Programowanie komputerów kwantowych" dostępną w ZSK (Zintegrowany System Kwalifikacji) od lutego tego roku, i umożliwiającą kształcenie i pozyskanie ekspertów w tej dziedzinie w ciągu najbliższych kilku lat. Co ważne, kwalifikacja (dostępna na poziomie piątym ZSK) jest dostępna już dla młodzieży szkół ponadpodstawowych i daje solidne podstawy do wykonywania zawodu technika programisty komputerów kwantowych, stwarza też mocne podstawy do kontynuowania nauki na poziomie uniwersyteckim.

Podsumowując, dobre praktyki na linii współpracy edukacji i biznesu opierają się na partnerskim podejściu, planowaniu działań, praktykach studenckich, programach edukacyjnych, współpracy z lokalnymi przedsiębiorcami oraz wymianie doświadczeń. Dzięki takiemu podejściu można stworzyć korzystne warunki dla rozwoju zarówno edukacji, jak i biznesu, co przyczynia się do wzmocnienia całego społeczeństwa.

Oprac. JŁ

KSZTAŁCENIE KOMPETENCJI CYFROWYCH NAUCZYCIELI – WYZWANIE DLA SYSTEMU EDUKACJI W EPOCE CYFROWEJ

To nauczyciele są szczególną grupą społeczną i zawodową, która zdecyduje o powodzeniu procesu zmiany cywilizacyjnej. To od nich wymaga się aktualnej wiedzy merytorycznej i metodycznej, by mogli zapewnić uczniom wykształcenie kompetencji niezbędnych w cyfrowym świecie.

Danuta Morańska
Wyższa Szkoła HUMANITAS,
członek zespołu eksperckiego ds. edukacji
Sektorowej Rady ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwa

Kiedy w 2006 r. po raz pierwszy opublikowano zalecenie Parlamentu Europejskiego i Rady z 18 grudnia 2006 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie (2006/962/WE), w sposób jasny sprecyzowano komunikat dotyczący zadań stojących przed systemami edukacji poszczególnych krajów członkowskich UE odnośnie do podjęcia działań ukierunkowanych na zapewnienie społeczeństwu możliwości ich rozwoju. Wskazując kierunki koniecznych zmian w edukacji, zwrócono uwagę na potrzebę przygotowania kadry pedagogicznej, odpowiedzialnej za realizację nowych wyzwań. Zadania te są nadal aktualne, tym bardziej, że obserwowane zmiany cywilizacyjne ciągle stawiają społeczeństwo europejskie wobec nowych wyzwań kompetencyjnych (zalecenie Rady z 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie; tekst mający znaczenie dla EOG – 2018/C 189/01).

Sprawne funkcjonowanie w społeczeństwie informacyjnym wymaga dynamicznych i zintegrowanych działań w obszarze rozwoju edukacji cyfrowej społeczeństw (KE, 2020). Edukację cyfrową postrzega się dwojako. Jednym z kierunków jest rozwój kompetencji cyfrowych osób uczących się oraz pedagogiczne wykorzystanie technologii cyfrowych w celu transformacji i ulepszania nauczania. Realizacja tych zadań stawia przed kadrą pedagogiczną szczególne wyzwania w zakresie kompetencji cyfrowych, gdyż to właśnie ona odgrywa szczególną rolę w realizowaniu priorytetowego celu strategicznego opisanego w planie działania w dziedzinie edukacji cyfrowej na lata 2021–2027, który polega na tworzeniu ekosystemu edukacji cyfrowej (KE, 2020). Stąd tak ważne są kompetencje nauczycieli w tym zakresie. Stanowią oni szczególną grupę społeczną i zawodową, która zdecyduje o powodzeniu procesu zmiany cywilizacyjnej. To właśnie od nauczycieli wymaga się aktualnej wiedzy merytorycznej i metodycznej, by mogli zapewnić swoim uczniom wykształcenie kompetencji niezbędnych w cyfrowym świecie.

Kształcenie kompetencji cyfrowych nauczycieli

W Polsce posiadanie kompetencji cyfrowych jest nie tylko nieodzownym elementem codziennej pracy nauczyciela, lecz także warunkiem uzyskania kwalifikacji do wykonywania tego zawodu. *Standardy przygotowania do zawodu nauczyciela* (MNiSW, 2019) zakładają kształcenie w obszarze technologii informacyjnej lub informatyki kandydatów do zawodu nauczyciela niezależnie od wybranego przez nich kierunku i specjalności. Zawarte tam zapisy odnośnie kompetencji cyfrowych są dość ogólne i dotyczą przede wszystkim promowania odpowiedzialnego i krytycznego wykorzystywania mediów cyfrowych oraz w pierwszej kolejności poszanowania praw własności intelektualnej podczas studiowania, a następnie do działań na rzecz własnego rozwoju zawodowego. Wskazują także na potrzebę stosowania nowoczesnych technologii w pracy dydaktycznej.

Jak wskazuje raport *Edukacja cyfrowa w szkołach w Europie* (Euridice, 2019), w około dwóch trzecich europejskich systemów edukacji (w tym w Polsce) kompetencje cyfrowe są traktowane jako podstawowe kompetencje zawarte w ramach kwalifikacji związanych z tym zawodem, przy czym poziom opisu szczegółowości obszarów i umiejętności jest zróżnicowany. Wspólną cechą jest wymóg posiadania przez nauczycieli

- wiedzy na temat tego, jak włączać technologie cyfrowe do swojej praktyki nauczania i uczenia się
- umiejętności skutecznego wykorzystania technologii w procesie dydaktycznym.

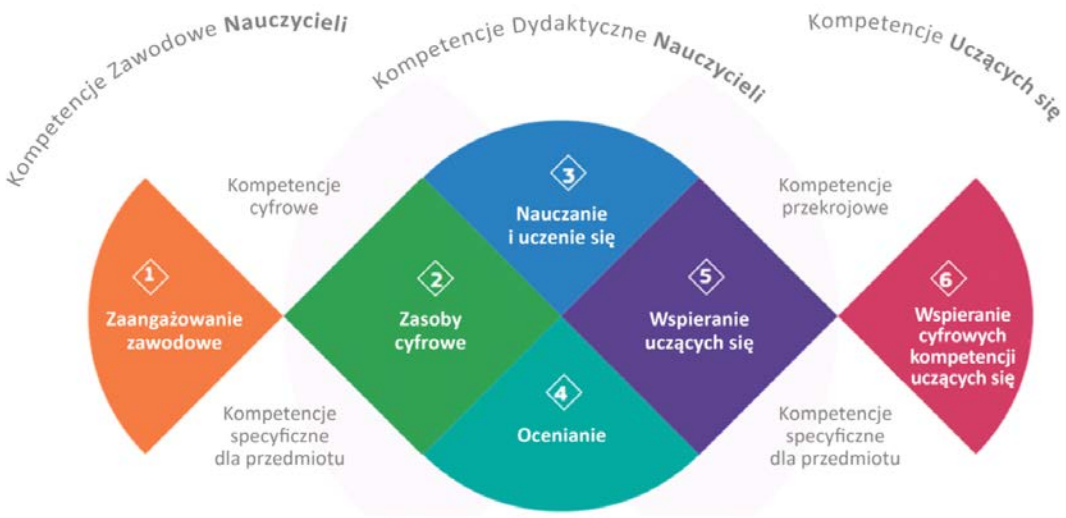
Autorzy przywołanego raportu zaznaczają, że w większości krajów nie obowiązują regulacje prawne dotyczące oceny kompetencji cyfrowych wymagane od nauczycieli przed podjęciem przez nich pracy w zawodzie, nie ma żadnych wymagań wobec certyfikatów potwierdzających posiadanie takich kompetencji, uczelnie są autonomiczne w określaniu kryteriów i obszarów oceny umiejętności studentów, a ich opis znajduje się w programach kształcenia.

> **Nauczyciele powinni podjąć rolę aktora w procesie reformowania instytucji oświatowych, ale także w szerszej perspektywie stymulować rozwój całej przestrzeni społecznej**

Standardy kompetencji cyfrowych nauczycieli

Zapewnienie odpowiedniej jakości kształcenia wymaga opracowania standardów oceny kompetencji cyfrowych osób zatrudnionych w sektorze edukacji. W związku z tym na poziomie międzynarodowym podejmowano różne inicjatywy. Opracowano wiele ram kompetencji, a także narzędzi do samooceny i programów szkoleniowych. Efektem podjętych działań było m.in. przygotowanie i opublikowanie w 2017 roku przez Wspólnotowe Centrum Badawcze (JRC – Joint Research Centre) raportu Digital Competence Framework for Educators (DigCompEdu), który zawiera europejskie ramy kompetencji cyfrowych dla osób zajmujących się edukacją. Raport jest efektem szeroko zakrojonych badań wśród ekspertów. Jego wynikiem jest opracowanie jednego kompleksowego modelu, który ma stanowić wsparcie i ogólne ramy odniesienia dla twórców modeli kompetencji cyfrowych państw członkowskich. Struktura DigCompEdu obejmuje kompetencje cyfrowe charakterystyczne dla zawodu nauczyciela zatrudnionego na wszystkich etapach edukacji (od przedszkola aż do szkolnictwa wyższego), a także w placówkach kształcenia specjalnego oraz w edukacji pozaformalnej.

RYS. 1. Digital Competence Framework for Educators (DigCompEdu)



Źródło: https://joint-research-centre.ec.europa.eu/digcompedu_en

DigCompEdu określa 22 kompetencje cyfrowe zgrupowane w sześciu obszarach.

1. **Rozwój zawodowy** (ang. Professional Engagement). Obejmuje on rozwój zawodowy nauczyciela i korzystanie z różnych kanałów komunikacji cyfrowej, wykorzystanie technologii cyfrowych do współpracy, rozwijanie umiejętności nauczania cyfrowego, wspieranie rozwoju przy wykorzystaniu technologii cyfrowych (np. przez udział w kursach online, MOOC, webinariach, wirtualnych konferencjach).

2. **Tworzenie i wymiana zasobów cyfrowych** (ang. Digital Resources): obejmuje kompetencje potrzebne do skutecznego i odpowiedzialnego wykorzystywania, tworzenia i udostępniania zasobów cyfrowych.

3. **Zarządzanie korzystaniem z technologii cyfrowych w procesie nauczania – uczenia się** (ang. Teaching and Learning): jest ukierunkowany na wykorzystanie cyfrowych technologii w organizacji procesu nauczania i uczenia się, obejmuje projektowanie, planowanie i wdrażanie technologii cyfrowych na różnych etapach edukacyjnych i zmierza do poprawy efektywności uczenia się, rozwijania zaangażowanego, refleksyjnego i wspólnotowego uczenia się.

4. **Ocena** (ang. Assessment): umiejętności korzystania z narzędzi cyfrowych wspierających praktyki oceniania formatywnego i sumatywnego. Odnosi się do wykorzystania technologii w procesie oceny i oceniania kształtującego, uwzględnia monitorowanie postępów pracy uczniów oraz ukierunkowane informacje zwrotne i zindywidualizowane wsparcie przy wykorzystaniu cyfrowych technologii.

5. **Wspieranie uczniów** (ang. Empowering Learners): obszar ten dotyczy umiejętności niezbędnych do wspierania rozwoju osobistego każdego ucznia z dbałością o włączanie i wzmacnianie osobistych talentów. Skupia się na wykorzystaniu potencjału technologii cyfrowych w urzeczywistnianiu strategii nauczania i uczenia się skoncentrowanych na uczniu, jego możliwościach, potrzebach, tempie pracy, zainteresowaniach, zwiększeniu zaangażowania uczniów w proces uczenia się, a także podejmowaniu uczenia się w szkole i poza nią.

6. **Umożliwianie uczniom nabywania kompetencji cyfrowych** (ang. Facilitating Learners' Digital Competence). Obszar ten dotyczy działań nauczyciela, które pośrednio sprzyjają rozwijaniu u uczniów kompetencji cyfrowych (projektowanie zadań wymagających używania narzędzi cyfrowych do komunikowania się i współpracy bądź wymagających tworzenia treści cyfrowych, kreatywnego wykorzystywania technologii cyfrowych do rozwiązywania konkretnych problemów).

Posiadanie kompetencji cyfrowych to nie tylko nieodzowny element codziennej pracy nauczyciela, lecz także warunek uzyskania kwalifikacji do wykonywania tego zawodu

Niezależnie od powyższego dokumentu w naszym kraju na zlecenie Departamentu Społeczeństwa Informacyjnego Kancelarii Prezesa Rady Ministrów w 2021 r. wykonano ekspertyzę specyficznych kompetencji cyfrowych wskazanych grup społecznych, wśród których znaleźli się m.in. nauczyciele.

Na potrzeby przeprowadzonych badań, zgodnie z Ramowym Katalogiem Kompetencji Cyfrowych opracowanym w 2018 na zlecenie Ministerstwa Cyfryzacji, kompetencje cyfrowe zdefiniowano jako „harmonijną kompozycję wiedzy, umiejętności i postaw umożliwiających życie, uczenie się i pracę w społeczeństwie cyfrowym (wykorzystującym technologie cyfrowe):

- **kompetencje informatyczne**,
- **kompetencje informacyjne,**
- **kompetencje funkcjonalne** – które są „oparte na kompetencjach informatycznych i informacyjnych i stanowią podłoże do realizacji konkretnych działań i osiągania konkretnych korzyści dzięki stosowaniu technologii cyfrowych" (Ramowy Katalog Kompetencji Cyfrowych (Jasiewicz i inni, 2018). **Obejmują one obok kompetencji powszechnych również kompetencje specyficzne związane z określoną rolą społeczną.**

W roli aktora

Myślę, że warto tutaj przytoczyć słowa prof. Bogusława Śliwerskiego, który stwierdził, że „W procesie kształcenia i doskonalenia zawodowego nauczycieli uświadamia się im, że są oni włączani w dynamikę rozwoju społecznego, zarówno swoich instytucji oświatowych, jak i pozaedukacyjną przestrzeń społeczną. Zatem **nauczyciele powinni podjąć rolę aktora w procesie reformowania instytucji oświatowych, ale także w szerszej perspektywie stymulować rozwój całej przestrzeni społecznej**". (Śliwerski, 2006).

Stąd też na szczególną uwagę zasługuje **rola nauczyciela w obszarze zmiany kompetencji cyfrowych jako podstawowy paradygmat rozwoju społeczeństwa informacyjnego**.

PARP
Grupa PFR

Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo

www.srtcb.radasektorowa.pl

Lider projektu:

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Partner projektu:

PIIT

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny