POLSKIE TOWARZYSTWO INFORMATYCZNE

NUMER 2/2026

PRZYSZŁOŚĆ ZACZYNA SIĘ DZISIAJ

Domena

ISSN 2720-6513

Numer specjalny towarzyszący

Konferencji z okazji 45-lecia PTI i ŚDTiSI

INFORMATYKA 2026 OCZAMI PTI

■ dokonania ■ perspektywy ■ wyzwania



PRZEGLĄD TEMATYKI WYSTĄPIEŃ KONFERENCYJNYCH

Spis treści

4 **Informatyka 2026 oczami PTI**
Jarosław Deminet

1 NOWOCZESNA INFORMATYKA W PRAKTYCE

11 **Cyfrowe bliźniaki w ważnych praktycznych zastosowaniach (medycyna, nauki o życiu)**
Maciej Malawski, Magdalena Otta

15 **Obliczenia dużej skali dla nauki, humanistyki, przemysłu**
Marek Magryś, Marian Bubak, Patryk Lasoń, Robert Pająk, Mariusz Sterzel

20 **Nowoczesna informatyka w Wielkiej Nauce: wyzwania, strategia, szanse**
Jakub T. Mościcki

24 **Obliczenia kwantowe w Polsce: stan i perspektywy**
Katarzyna Rycerz, Mariusz Sterzel, Justyna Zawalska, Marian Bubak

28 **Cyberbezpieczeństwo: ufaj, ale sprawdzaj**
Mirosław Kutyłowski

32 **Dostawcy wysokiego ryzyka**
Jarosław Deminet

2 SZTUCZNA INTELIGENCJA: NOWE MOŻLIWOŚCI I ZAGROŻENIA

37 **AI jako nowa Rewolucja Przemysłowa**
Janusz Kacprzyk

40 **Gaia AI Factory. Infrastruktura dla rozwoju sztucznej inteligencji i budowy suwerenności technologicznej**
Marek Kasztelnik, Paula Al-Hmiedat, Marek Magryś

44 **Robot społeczny w prawie nowych technologii**
Aneta Sieradzka

47 **Metoda naukowa w erze AI. Od asystenta do autonomicznego badacza**
Tomasz Kajdanowicz

50 **Inżynieria AI w erze Wielkiej Niewiadomej**
Borys Stokalski

3 ROZWÓJ SPECJALISTYCZNYCH KOMPETENCJI CYFROWYCH

56 **European Union and Support of AI Competences Education: A Subjective Overview**
Jakub Christoph

59 **Certyfikacja kompetencji cyfrowych. Od ICDL do Zintegrowanego Systemu Kwalifikacji**
Bogusław Dębski

62 **Sztuczna inteligencja w edukacji wyższej**
Tomasz Kulisiewicz

Sektorowa Rada ds. Kompetencji
IT, Telekomunikacja i Cyberbezpieczeństwo

66 **Pora na wdrażanie wypracowanych rozwiązań**
Dyskusja na temat zmian na rynku pracy i zapotrzebowania na nowe kwalifikacje.



Szanowni Państwo,

45 lat w rozwoju informatyki to więcej niż epoka. Młodym ludziom uświadamiam, że gdy 45 lat temu powstawało Polskie Towarzystwo Informatyczne w Polsce nie mieliśmy komputerów osobistych, telefonów komórkowych, a podstawą dla przetwarzania danych były Zakłady Elektronicznej Techniki Obliczeniowej (ZETO) oraz polskie komputery ODRA i MERA. Obowiązywało embargo amerykańskie na dostawy zaawansowanych komputerów i technologii, ale jednocześnie wtedy powstał działający do dzisiaj system PESEL.

Mieliśmy świetne uczelnie, świetnych wykładowców, szkoliliśmy dobrze przygotowanych do zawodu informatyka studentów. Absolwenci informatyki zostawali na uczelniach i tworzyli wysoko kwalifikowane zespoły pracowników naukowych na uniwersytetach i politechnikach. Wielu z nich kontynuowało potem rozwój zawodowy w Stanach Zjednoczonych, wnosząc swój wkład w rozwój zaawansowanych technologii także w największych amerykańskich korporacjach. Ci co zostali w Polsce zbudowali po 1990 r. polskie firmy informatyczne, informatyzowali przemysł i administrację, pracowali w polskich oddziałach zagranicznych korporacji.

W ten sposób Polska nadganiała okresy embarga. Straciliśmy jednak dystans w produkcji komputerów i półprzewodników. Ale wygrywamy światowe konkursy w programowaniu zespołowym i olimpiady Informatyczne. Ich laureaci uczestniczą w tworzeniu nowych technologii i rozwoju modeli generatywnej sztucznej inteligencji, ale nie w Polsce.

O tym wszystkim pisaliśmy w naszych wydawnictwach związanych z 40-leciem PTI. Gdy zbliżał się jubileusz 45-lecia postanowiliśmy spojrzeć na naszą organizację inaczej. Uznaliśmy, że celem PTI powinno być myślenie o przyszłości. Przyszłości informatyki, informatyków i rozwoju technik informacyjnych. Ostatnimi laty mówiliśmy na naszych konferencjach o przełomowych technologiach. Staraliśmy się rozbrajać marketingowy slang i przedstawiać prawdę o szansach zastosowania kolejnych technologii w rozwoju przemysłu, gospodarki i nauki.

Szansą dla realizacji misji PTI jest udział w jej aktywnościach informatyków z kolejnych pokoleń. Musimy się zmieniać, zmieniać metody naszego działania, aby odpowiedzieć na oczekiwania kolejnych roczników wchodzących w pełnoprawne życie zawodowe. Informatyków ze środowisk naukowych, biznesowych edukacyjnych. Tylko budując wzajemne relacje służące wymianie wiedzy i doświadczeń możemy tworzyć wpływowe środowisko wspierające promocję i rozsądne wdrażanie przełomowych technologii.

Rozwój informatyki zarówno w obszarze sprzętu, jak i oprogramowania stwarza szansę na istotne zmiany w gospodarce, strukturze zatrudnienia, rozwoju społecznym. Ale ma też podwójne zastosowanie. Wojny toczące się już wokół nas pokazują jak przełomowe technologie zmieniają pole walki, pojawiają się zagrożenia hybrydowe. Bezmyślne zastosowanie AI bez kontroli człowieka prowadzi do nieszczęść i brutalnych mordów.

Dzisiaj ma to i pozytywny, i negatywny wpływ na nasze życie, kulturę, naukę, edukację, procesy społeczne. Musimy tworzyć nowe kompetencje, budować systemy nabywania potrzebnej wiedzy i umiejętności. Nie możemy jednak zapominać o kluczowej roli człowieka w tym dążeniu do tworzenia nowego świata. Dotychczas widzieliśmy problemy etyczne w rozwoju i zastosowaniu broni atomowej. Dziś kwestia odpowiedzialności informatyków za efekty ich pracy zaczyna przypominać tamte dylematy.

Zapraszam więc na Konferencję „Informatyka 2026 oczami PTI: dokonania, perspektywy, wyzwania".

Cześć naszych Gości Wykładowców zdecydowała się zamieścić na łamach specjalnego numeru „Domeny" artykuły obejmujące tematykę ich wystąpień na konferencji.

Zachęcam do przeczytania obu numerów pisma.

Wiesław Paluszyński, prezes PTI

Informatyka 2026 oczami PTI

Jarosław Deminet

45 lat temu (23 maja 1981 r.) odbył się Zjazd Założycielski PTI. Termin wynikał ze względów ściśle politycznych. Okres solidarnościowego „karnawału" przyniósł pewną liberalizację – wprawdzie nie przepisów dotyczących stowarzyszeń, ale zasad ich stosowania. W Zjeździe uczestniczyło 142 członków-założycieli (w tym 10 kobiet). Ten tekst jest moim subiektywnym wspomnieniem tamtych czasów i próbą spojrzenia na nie z odległej już perspektywy. Nie gwarantuję dokładności ani kompletności – każdy czytelnik czyta go na własną odpowiedzialność.



Jarosław Deminet

informatyk od 1979 r., bywał nauczycielem akademickim, urzędnikiem, szefem działów produkujących oprogramowanie w korporacji, konsultantem biznesowym, publicystą.
Członek założyciel PTI.

Na przełomie lat 70. i 80. XX w. na świecie dużo się działo. Mijało dopiero 20 lat od pojawienia się informatyki jako samodzielnej dziedziny nauki i gospodarki (choć często ta data jest przesuwana wstecz, bo już wcześniej korzystano z maszyn cyfrowych).

Infopejzaż

Kończyła się bezwzględna dominacja nielicznych a kosztownych komputerów klasy *mainframe*, rosła baza minikomputerów (sama firma DEC w latach 70. XX w. wyprodukowała kilkaset tysięcy egzemplarzy PDP-11 i właśnie zaczynała produkcję superminikomputera VAX-11 z oszałamiającym 1 MB pamięci RAM). W USA od kilkunastu lat działała sieć Arpanet, od kilku lat instalowano szybkie sieci lokalne w standardzie Ethernet o przepustowości 1 Mb/s – z ich połączenia w ciągu kilku lat miał powstać Internet. Ci z nas, którzy mieli wówczas okazję odwiedzić zagraniczne ośrodki, poznali zalety poczty elektronicznej i komputerowej poligrafii (*desktop publishing*).

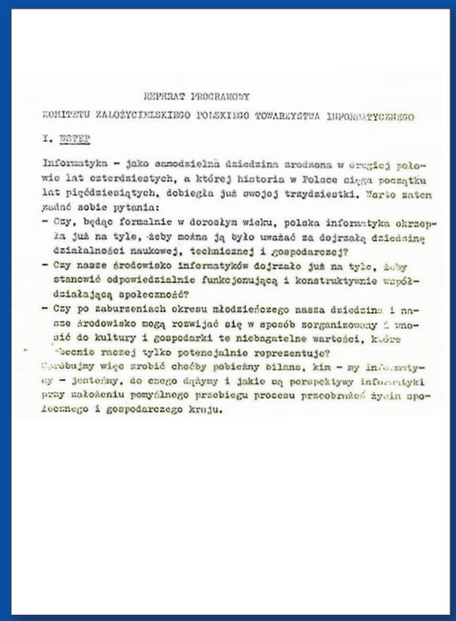
Komputery były powszechnie stosowane w gospodarce, w szczególności w bankowości (funkcjonowały np. bankomaty, choć tylko w okolicy macierzystych banków). Tradycyjny skład drukarski w dużej mierze został zastąpiony przez skład komputerowy (zecerzy byli pierwszą grupą zawodową wyeliminowaną wskutek informatyzacji). W biurach tu i ówdzie pojawiały się edytory tekstów oraz większe i mniejsze drukarki. Pracę ułatwiały pierwsze stacje robocze z ekranami graficznymi what-you-see-is-what-you-get i myszkami.

Szykowała się rewolucja mikrokomputerowa. Na rynku było kilka procesorów ośmiobitowych, rozpoczęła się produkcja Intela 8086, czyli protoplasty wszystkich pecetów (mam egzemplarz opisu technicznego z 1980 r. z nadrukiem „preliminary"). W sklepach z elektroniką były zarówno gotowe mikrokomputery do użytku domowego, jak i zestawy do samodzielnego składania (elementy były na tyle duże, że można było się do nich zabierać ze śrubokrętem i lutownicą, teraz już bym nikomu tego nie polecał). Czuć było, że informatyka nie będzie już zamknięta w ścianach korporacji i uniwersytetów, ale że niebawem stanie się powszechna, a informatycy przestaną być egzotyczną profesją.

Polscy informatycy byli świadomi dystansu do krajów rozwiniętych, zwłaszcza do USA.

Istniało kilka silnych ośrodków związanych z informatyką: wrocławskie ELWRO (duże komputery Odra i Riad, choć na 1981 r. plan przewidywał produkcję tylko trzech (!) sztuk), warszawska ERA (minikomputery Mera-300 i Mera-400, potem SM-3 i SM-4), Instytut Maszyn Matematycznych i Instytut Podstaw Informatyki PAN, sieć Zakładów Elektronicznej Techniki Obliczeniowej, ośrodki branżowe, kilka uczelni.

Pierwszy nabór na kierunek „informatyka" na Uniwersytecie Warszawskim nastąpił w 1973 r., przyjęto 120 osób, z czego po dwóch latach została połowa. W 1980 r.



REFERAT PROGRAMOWY
KOMITETU ZAŁOŻYCIELSKIEGO POLSKIEGO TOWARZYSTWA INFORMATYCZNEGO

I. WSTĘP

Informatyka – jako samodzielna dziedzina zrodzona w drugiej połowie lat czterdziestych, a której historia w Polsce sięga początku lat pięćdziesiątych, dobiegła już swojej trzydziestki. Warto więc zadać sobie pytania:
- Czy, będąc formalnie w dorosłym wieku, polska informatyka okrzepła już na tyle, żeby można ją było uważać za dojrzałą dziedzinę działalności naukowej, technicznej i gospodarczej?
- Czy nasze środowisko informatyków dojrzało już na tyle, żeby stanowić odpowiedzialnie funkcjonującą i konstruktywnie współdziałającą społeczność?
- Czy po zaburzeniach okresu młodzieńczego nasza dziedzina i nasze środowisko mogą rozwijać się w sposób zorganizowany i wnosić do kultury i gospodarki te niebagatelne wartości, które obecnie raczej tylko potencjalnie reprezentuje?

Spróbujmy więc zrobić choćby pobieżny bilans, kim – my informatycy – jesteśmy, do czego dążymy i jakie są perspektywy informatyki przy założeniu pomyślnego przebiegu procesu przeobrażeń życia społecznego i gospodarczego kraju.

Odbiciem ówczesnych nastrojów i postulatów był referat programowy Komitetu Założycielskiego PTI. Ma on 17 stron, z czego 11 zajmuje opis stanu polskiej informatyki i sytuacji polskich informatyków, a także celów i zadań powstającego Towarzystwa.

Na wstępie Ojcowie Założyciele pisali:

„Informatyka – jako samodzielna dziedzina zrodzona w drugiej połowie lat czterdziestych, a której historia w Polsce sięga początku lat pięćdziesiątych, dobiegła już swojej trzydziestki. Warto więc zadać sobie pytania:

- **Czy, będąc formalnie w dorosłym wieku, polska informatyka okrzepła już na tyle, żeby można ją było uważać za dojrzałą dziedzinę działalności naukowej, technicznej i gospodarczej?**
- **Czy nasze środowisko informatyków dojrzało już na tyle, żeby stanowić odpowiedzialnie funkcjonującą i konstruktywnie współdziałającą społeczność?**
- **Czy po zaburzeniach okresu młodzieńczego nasza dziedzina i nasze środowisko mogą rozwijać się w sposób zorganizowany i wnosić do kultury i gospodarki te niebagatelne wartości, które obecnie raczej tylko potencjalnie reprezentuje?"**

Po czym dodawali:
„Powszechne jest w środowisku poczucie kryzysu polskiej informatyki, będącego wynikiem konfrontacji nadmiernie rozbudzonych aspiracji i nikłych możliwości ich realizacji".

uczelnie opuściło ok. 500 absolwentów kierunków informatycznych (szeroko pojętych). Wychodził branżowy miesięcznik „Informatyka", adresowany przede wszystkim do praktyków (były w nim np. artykuły, jak zainstalować jakiś pakiet oprogramowania na Odrze czy Riadzie albo jak sobie poradzić z problemami z tymi maszynami). Użytkowany sprzęt był niestety zawodny i słabo skonfigurowany (np. większość systemów nie miała dysków). Według GUS w sumie istniało 1300 ośrodków obliczeniowych wyposażonych w 2300 komputerów różnej wielkości i zatrudniających ponad 50 tys. osób (z których tylko część była faktycznie informatykami). Środowiska przemysłowe i naukowe przenikały się (np. informatycy z Uniwersytetu Warszawskiego tworzyli oprogramowanie dla jednej z wielkich firm chemicznych).

Okienko wolności

W takiej atmosferze krążyła w środowisku idea powołania stowarzyszenia informatyków, ale na przeszkodzie stały ograniczenia polityczne. Trzeba było wykazać, że planowanych celów nie można osiągnąć w ramach już istniejących stowarzyszeń, poza tym stowarzyszenia branżowe musiały należeć do ściśle nadzorowanej przez władze Naczelnej Organizacji Technicznej. Naszym Ojcom Założycielom jakoś z NOT nie było po drodze. Na szczęście w atmosferze kilkunastomiesięcznego „karnawału" urzędnicy mieli większe problemy niż niewielka grupa zawodowa informatyków i byli gotowi nieco poluzować przepisy.

Aspiracje faktycznie były duże – minikomputer K-202 miał podbić europejski rynek, a Polska miała produkować własne mikroprocesory (w rzeczywistości mikroskopijna produkcja polskich klonów 8080 ruszyła, gdy na świecie masowo produkowano już mikroprocesory 32-bitowe). Powstawały teoretyczne koncepcje i diagramy usieciowionych i nowatorskich w skali światowej systemów do zarządzania gospodarką, planowania inwestycji, rozdziału cementu, opon czy stali zbrojeniowej. Informatyka miała być kluczem do dobrobytu.

A owe „nikłe możliwości realizacji" były nieodłączną cechą socjalistycznej gospodarki. Brak wolnorynkowej konkurencji i sztywny gorset gospodarki planowej we wszystkich krajach RWPG bardzo utrudniał postęp techniczny i szybkie dostosowanie się do potrzeb. Jeszcze 10 lat później problemem było zamówienie obudów do pecetów, wykonanych z odpowiednią dokładnością z odpowiedniej blachy. Polski papier był za gruby i strasznie pylił, co powodowało konieczność stałego serwisowania drukarek. Pęd do ilościowego wykonania planu owocował produkcją bezdyskowych komputerów, a beznadziejny stan sieci telekomunikacyjnej wykluczał możliwość budowy jakichkolwiek sieci komputerowych. Największym osiągnięciem w skali kraju było połączenie kilkunastu słabiutkich minikomputerów z komputerem centralnym siecią teleksową pracującą z prędkością 50 (!) bitów na sekundę, czyli 1000 razy wolniejszą niż pierwsze połączenia Arpanetu w 1969 r. W Warszawie i Krakowie po wielu miesiącach prac z wielkim trudem udało się połączyć podmiejskie ośrodki dysponujące w miarę szybkimi komputerami CDC z kilkunastoma końcówkami na terenie miasta siecią 4 kb/s. Jeszcze w drugiej połowie lat 80. XX w. do celów profesjonalnych używano zabawkowych mikrokomputerów typu ZX Spectrum, bo były one bardziej niezawodne od sprzętu wyprodukowanego w RWPG.

> ***Jeden z największych komputerów w Polsce, nowy radziecki R60, zainstalowany na początku lat 80. XX w. w Centrum Informatycznym Uniwersytetu Warszawskiego, wzorowany z grubsza na komputerach IBM z końca lat 60., miał średni czas między awariami liczony w pojedynczych godzinach.***

Dostęp do nowoczesnych komputerów z krajów kapitalistycznych był ograniczony zarówno ze względów ekonomicznych, jak i z powodu istniejącego embarga COCOM – w końcu nikt nie chce, aby jego komputer obliczał trajektorię rakiety, która ma mu spaść na głowę.

Zderzenie aspiracji i możliwości było więc faktem, ale rok 1981 wydawał się rokiem zmian, także w gospodarce, choć niedaleka przyszłość przekreśliła te nadzieje.

Propozycje sanacyjne PTI

W referacie programowym postulowano częściowe odejście od odgórnego sterowania wszystkim. Proponowano centralne wsparcie dla informatyzacji bankowości oraz systemów informacji naukowo-technicznej i ekonomicznej, pozostawiając innym przedsiębiorstwom informatyzację w ramach rachunku ekonomicznego. Uznano, że po załamaniu „informatycznych systemów rządowych" (faktycznie z wielu takich systemów budowanych w latach 70. ostał się jeno PESEL) należy rozważyć przejściowe ograniczenie inwestowania w rozwój takich systemów. W związku z kierunkami realizacji reformy gospodarczej większe środki byłyby przeznaczone na doskonalenie i rozwój systemów na szczeblu przedsiębiorstw, a zwłaszcza banków. Niestety, słowa o reformie gospodarczej okazały się nieco naiwne.

W socjalistycznej gospodarce, w której rozwój mierzono ilością wyprodukowanego węgla i stali, wytwarzanie oprogramowania nie mieściło się w tabelkach planistów. Nikomu nie przychodziło do głowy, że może to być działalność dochodowa, choć niektóre ośrodki sieci ZETO (Zakłady Elektronicznej Techniki Obliczeniowej) produkowały profesjonalne oprogramowanie (np. system zarządzania sieciową bazą danych RODAN). Jak pisano w referacie programowym, typowe rozwiązania informatyczne w PRL powstawały w odosobnionych ośrodkach informatycznych i nie podejmowano żadnych kroków, żeby je szerzej popularyzować. W referacie programowym kilkukrotnie wspomina się tę bolączkę, postulując, aby to PTI popularyzowało współczesne techniki produkcji oprogramowania oraz współdziałania przy ich opracowywaniu.

Do dziś słuszny pozostaje ówczesny postulat, aby to informacja stała się towarem wartościowym i atrakcyjnym, którego cena zależeć będzie zarówno od jej wiarygodności, jak i czasu udostępniania.

Postulowano także, aby PTI, jako instytucjonalny przedstawiciel środowiska, dostarczało ocen jednoznacznie wartościujących ważniejsze przedsięwzięcia informatyczne, zrealizowane i zamierzone.

Opiniotwórcza rola PTI miała objąć m.in. opracowanie *Raportu o stanie informatyki*, oceniającego stan środków informatyki i kadry profesjonalistów, kwalifikacji zawodowych i sposobów ich podniesienia, istniejących zastosowań i możliwości ich szerszego wykorzystania oraz istniejących struktur organizacyjnych. Powołano komitet redakcyjny, ale – jak Zarząd Główny przyznał w sprawozdaniu na kolejny Zjazd – nic z tego nie wyszło, zadanie przerosło siły społecznej organizacji.

Środowisko informatyków (czy raczej osób powiązanych z informatyką – mamy przecież Polskie Towarzystwo Informatyczne, a nie Polskie Towarzystwo Informatyków) było bardzo zróżnicowane. Informatyków „dyplomowanych" była garstka – kierunki informatyczne po kilku latach ich funkcjonowania opuściło dopiero kilka tysięcy absolwentów. W referacie wspomina się o m.in. sporach między teoretykami a praktykami, programistami a sprzętowcami, producentami a użytkownikami, konkludując jednak, że wszyscy oni są przekonani o wartości informatyki nie tylko jako składnika kulturotwórczego, lecz przede wszystkim jako jednego z potencjalnie najpoważniejszych czynników rozwoju gospodarki. PTI miało więc pełnić funkcję integrującą środowisko.

Zadaniem PTI było wypracowanie wzorców etyki zawodowej oraz czuwanie nad ich przestrzeganiem, w szczególności popieranie działań na rzecz ochrony prywatności wobec „wielkich systemów informacji personalnej". Ojcowie Założyciele postulowali wprowadzenie systemu oceny kwalifikacji zawodowych i stopni specjalizacyjnych.

PTI miało ambicje prowadzenia działalności szkoleniowej i publikacyjnej, z własnymi czasopismami i książkami, także naukowymi. W planach była organizacja konferencji naukowych, w tym dorocznej krajowej konferencji PTI. Przygotowywany co roku wykład PTI miał być prezentowany we wszystkich oddziałach. Przewidywano powołanie izby rzeczoznawców.

Bolesna weryfikacja

Młodzieńcze wizje i oceny stopniowo weryfikował czas. Już po trzech latach ustępujący Zarząd Główny I kadencji potwierdził, że problemy informatyki w gospodarce pozostały, w stosunku władz do niej panuje chaos, a zaniedbania zagrażają utrzymaniu kraju w gronie państw cywilizowanych. Postulowano powołanie fachowej rządowej agencji informatyki, która odpowiadałaby za formułowanie i realizowanie polityki państwa w tym obszarze. Podobny ton miały sprawozdania, referaty programowe i dyskusje na kolejnych zjazdach.

Największe zmiany nastąpiły oczywiście na przełomie lat 80. i 90. XX w. wraz z wprowadzeniem gospodarki wolnorynkowej i stopniowym znoszeniem embarga COCOM. Zniknęły pozafinansowe bariery w dostępie do nowoczesnego światowego sprzętu czy oprogramowania (próby ograniczenia dostępu do modułów niezbędnych dla sztucznej inteligencji uznaję za patologiczny wypadek przy pracy). Prywatne firmy same odpowiadają za informatyzację swojej działalności, organizacje społeczne nie muszą ich wspomagać ani sugerować producentom kierunków rozwoju. Pojawiły się izby gospodarcze, które są platformą współpracy producentów sprzętu i oprogramowania.

Państwowe przedsiębiorstwa produkujące sprzęt komputerowy ze swoją przestarzałą bazą produkcyjną i zawodnymi produktami nie utrzymały się na konkurencyjnym rynku. To samo spotkało zresztą inne kraje europejskie: brytyjski ICL, francuski Bull, włoski Olivetti czy niemiecki Siemens nie produkują już samodzielnie serwerów czy laptopów. Niewielu więc mamy w PTI „sprzętowców". Natomiast rozkwitły firmy wytwarzające i wdrażające oprogramowanie. W latach 80. XX w. powstało wiele małych firm, produkujących oprogramowanie na taki sprzęt, jaki był dostępny, głównie na komputery osobiste. Chyba nikt nie pokusił się dotąd o analizę, czy i w jakim stopniu przyczyniło się do tego PTI, ułatwiając kontakty środowiskowe i oferując parasol instytucjonalny firmom i osobom prywatnym, oferującym swoje produkty państwowym przedsiębiorstwom, niechętnym do kontaktów

z „prywaciarzami". Tak czy owak np. w 1987 r. w gdańskiej Hali Olivia zorganizowano duże targi prywatnych producentów oprogramowania. Takie firmy po konsolidacjach i przekształceniach stanowią do dziś rdzeń rynku oprogramowania i wdrożeń. Polska jest europejskim ewenementem pod względem udziału lokalnych firm, co zresztą przez lata było solą w oku światowych potentatów.

Informatyk niezwymiarowany

W 2024 r. liczba osób zatrudnionych w dziale gospodarki bezpośrednio związanym z IT wynosiła ok. 365 tys., inne źródła podają liczby dochodzące do 600 tys., co nie znaczy, że wszyscy oni są informatykami – a też informatycy nie zawsze pracują bezpośrednio w IT (znam to z autopsji). Nie ma zresztą zgody co do tego, kto jest informatykiem (choć raczej nie budzi wątpliwości to, kto jest inżynierem, prawnikiem, architektem lub lekarzem). W ciągu 45 lat w PTI regularnie wracano do koncepcji sformalizowania kwalifikacji zawodowych i stopni specjalizacyjnych. Nie udało się to w okresie PRL-u, gdy były sztywne siatki płac i stopnie specjalizacyjne mogłyby być podstawą do rozmaitych dodatków. Tym bardziej nie udało się potem, gdy w warunkach gospodarki rynkowej każdy przedsiębiorca zaczął sam decydować o tym, kogo i na jakim stanowisku chce zatrudnić. W latach 90. XX w. PTI podjęło próbę wdrożenia w Polsce brytyjskiego systemu rozwoju zawodowego. Podpisano nawet umowę z rządem, który miał to przedsięwzięcie częściowo sfinansować, ale rząd o umowie szybko zapomniał, a samo PTI nie było w stanie tego ambitnego zadania udźwignąć. Poszliśmy w nieco inną stronę – pomagając kształcić i certyfikować innych, najpierw wykorzystując ECDL (Europejski Certyfikat Umiejętności Komputerowych), a potem EUCIP (Europejski Certyfikat Zawodu Informatyka) i Sektorowe Rady ds. Kompetencji.

> ***Rola administracji publicznej w kształtowaniu rozwoju informatyki jest teraz mocno ograniczona, ale kolejne rządowe plany informatyzacji państwa czy strategie informatyzacji mają podobny związek z rzeczywistością jak Narodowy Plan Społeczno-Gospodarczy z roku 1981.***

W 1991 r. PTI opracowało 50-stronicową „Propozycję strategii rozwoju informatyki i jej zastosowań w Rzeczypospolitej Polskiej". Postulowano tam m.in. prawne uregulowanie ochrony danych osobowych i ochronę praw autorskich producentów oprogramowania, co faktycznie nastąpiło po kilku latach – niestety bardziej wskutek wymagań procesu akcesji do UE niż wskutek nacisków środowiska. Obecnie PTI coraz sprawniej, szczególnie w ostatnich latach, stara się wpływać na decyzje rządowe przez udział w konsultacjach społecznych, ale nasz głos nie jest jakoś szczególnie brany pod uwagę.

Nie powołano agencji informatyki postulowanej 40 lat temu, rozumianej jako podmiot kształtujący i wspierający zastosowania informatyki, zamiast tego powstał molochowaty Centralny Ośrodek Informatyki – państwowe przedsiębiorstwo produkujące oprogramowanie i eksploatujące systemy informatyczne administracji centralnej.

Wśród Ojców Założycieli PTI byli koryfeusze polskiej nauki. Ich intencją było, aby PTI stało się silnym i rozpoznawalnym stowarzyszeniem naukowym na wzór Polskiego Towarzystwa Matematycznego czy Polskiego Towarzystwa Fizycznego. Stąd pomysły m.in. wydawnictw i konferencji naukowych. Te plany zostały zrealizowane tylko częściowo. PTI jest współorganizatorem kilku konferencji stricte naukowych (przede wszystkim FedCSIS), istnieje Rada Naukowa, ale w powszechnym odczuciu akademickim PTI nie kojarzy się z działalnością naukową, a wielu wybitnych naukowców informatyków do PTI nie należy albo nie jest w nim aktywnych. Postulat powołania pisma naukowego PTI został porzucony po kilku latach, ponieważ sami naukowcy przyznali, że dla nich podstawowym miejscem publikacji były i pozostaną renomowane recenzowane branżowe czasopisma angielskojęzyczne. Nie udało się także stworzyć czasopisma integrującego różne dziedziny badawcze na wzór amerykańskiego „Communications of the ACM".

W 1981 r. nikt nie mógł przewidzieć wszystkich kierunków rozwoju informatyki jako dziedziny nauki czy gospodarki. Wyobraźnia podpowiadała może komputery osobiste i pakietową transmisję danych, ale nie smartfony i internet rzeczy. Liczono na (choćby ograniczoną) reformę gospodarczą, ale mało kto przewidział całkowite otwarcie gospodarki i tak masowy rozwój zastosowań, a więc i wzrost liczby zaangażowanych w to specjalistów. Po 1989 r. w łonie PTI powstawały nawet wątpliwości, czy dalsze istnienie stowarzyszenia w nowych warunkach społeczno-gospodarczych ma sens. Najważniejsza impreza integracyjna (Jesienne Spotkania PTI) musiała całkowicie zmienić formułę, a po kilku latach upadła. Liczba członków spadła w stosunku do lat 80., gdy PTI w dużym stopniu było podmiotem gospodarczym, świadczącym usługi na rzecz państwowych przedsiębiorstw. Jednocześnie PTI przejęło wielką rolę w edukacji informatycznej.Członkowie Towarzystwa ciągle uważają, że warto do niego należeć. I – na szczęście – ciągle napływają nowi.



Światowy Dzień Telekomunikacji i Społeczeństwa Informacyjnego 2026 oraz 45-lecie PTI

INFORMATYKA 2026

oczami Polskiego Towarzystwa Informatycznego

DOKONANIA, PERSPEKTYWY, WYZWANIA

14 maja, Warszawa

45 PTI POLSKIE TOWARZYSTWO INFORMATYCZNE

Na Konferencję **Informatyka 2026 oczami PTI: dokonania, perspektywy, wyzwania** zaprosiliśmy uznanych naukowców, przedstawicieli biznesu oraz administracji państwowej i samorządowej. Goście-wykładowcy zarysują m.in. perspektywy rozwoju technologii informatycznych oraz przychodzących z nimi nowych korzyści, wyzwań i zagrożeń dla społeczeństwa oraz dla rozwoju gospodarczego.

Konferencja składa się z trzech sesji tematycznych:

- „Nowoczesna informatyka w praktyce"
- „Sztuczna inteligencja: nowe możliwości i zagrożenia"
- „Rozwój specjalistycznych kompetencji cyfrowych".

Po każdej sesji prowadzący ją przedstawiciel PTI będzie inicjował i moderował dyskusję. Konferencję zakończy dyskusja panelowa podsumowująca obrady, prowadzona przez Wiesława Paluszyńskiego, prezesa PTI. Wnioski z tej dyskusji będą pomocne przy formułowaniu planu działania PTI na rzecz rozwoju polskiej informatyki.

Na następnych stronach tego konferencyjnego numeru „Domeny" znajdą Państwo artykuły ściśle związane z wystąpieniami konferencyjnymi. Niektóre z nich mają współautorów zaproszonych przez Wykładowców. Publikujemy je chronologicznie, zgodnie z programem każdej sesji. Mamy nadzieję, że w ten sposób utrwalimy ustalenia merytoryczne konferencji i łatwiej będzie wracać do jej tez i przewidywań. A po latach będziemy mogli z rozrzewnieniem wspominać obraz informatyki AD 2026.

Redakcja

SESJA 1

NOWOCZESNA INFORMATYKA W PRAKTYCE

Prowadzący:



Marek Bolanowski

absolwent Wydziału Elektrotechniki i Informatyki Politechniki Rzeszowskiej, doktor nauk technicznych (2009 r., Politechnika Łódzka). Pracownik naukowy Zakładu Systemów Złożonych Politechniki Rzeszowskiej. Główne zainteresowania badawcze: projektowanie i eksploatacja systemów rozproszonych, w tym sieci kognitywnych; wykrywanie i predykcja anomalii; cyberbezpieczeństwo; analiza wydajności; automatyzacja procesów zarządzania systemami informatycznymi. Lista publikacji, projektów i osiągnięć dostępna na stronie https://bolanowski.v.prz.edu.pl/.

Program sesji:

- **Cyfrowe bliźniaki w ważnych praktycznych zastosowaniach (medycyna, nauki o życiu)**
  Maciej Malawski – Dyrektor Sano Centre for Computational Medicine, Kraków
- **Obliczenia dużej skali dla nauki, humanistyki, przemysłu**
  Marek Magryś – Dyrektor ACK Cyfronet AGH
- **Nowoczesna informatyka w Wielkiej Nauce: wyzwania, strategia, szanse**
  Jakub T. Mościcki – Head of Storage and Data Management Group, CERN IT
- **Obliczenia kwantowe w Polsce: stan i perspektywy**
  Katarzyna Rycerz – Wydział Informatyki i ACK Cyfronet AGH
- **Cyberbezpieczeństwo: ufaj ale sprawdzaj**
  Mirosław Kutyłowski – Kierownik Zakładu Kryptologii, NASK
- **Cyberbezpieczeństwo: z czym do ludzi?**
  Maria Magdoń – z-ca dyrektora Departamentu Gospodarki Cyfrowej, Ministerstwo Rozwoju i Technologii
- **Dostawcy wysokiego ryzyka**
  Jarosław Deminet – Polskie Towarzystwo Informatyczne

Cyfrowe bliźniaki w ważnych praktycznych zastosowaniach (medycyna, nauki o życiu)

Maciej Malawski, Magdalena Otta

Jedno z pierwszych miejsc w Polsce, w którym dyskutowano o wykorzystaniu matematyki, fizyki i informatyki w biologii i medycynie, to konferencja MCSB[1] zainicjowana przez profesorów Jana Trąbkę i Ryszarda Tadeusiewicza, organizowana od 1978 r. w Krakowie na długo przed pojawieniem się terminu *digital twin*. Można powiedzieć, że to właśnie w takich środowiskach – dzięki współpracy lekarzy i inżynierów informatyków – powstawały fundamenty pod dzisiejsze cyfrowe bliźniaki.



Maciej Malawski

dyrektor Sano Centre for Computational Medicine oraz profesor na Akademii Górniczo-Hutniczej w Krakowie. Posiada stopień doktora i magistra informatyki oraz fizyki teoretycznej, a także doświadczenie zdobyte na Uniwersytecie Emory i Uniwersytecie Notre Dame. Jego badania obejmują obliczenia równoległe i rozproszone, analizę wielkoskalowych danych, technologie chmurowe, federacyjne uczenie maszynowe oraz ich zastosowania w medycynie obliczeniowej. Od 2002 r. uczestniczy w projektach biomedycznych finansowanych przez UE (CrossGrid, ViroLab, VPH-Share i EurValve), odegrał również kluczową rolę w powstaniu Sano.

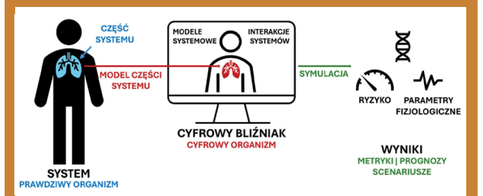
Magdalena Otta

badaczka zajmująca się modelowaniem i symulacją procesów biomedycznych, ze szczególnym uwzględnieniem przepływu krwi w zakrzepicy żył głębokich. Absolwentka University of Edinburgh, stopień doktora uzyskała na University of Sheffield. Łączy metody matematyczne, obliczeniowe i obrazowanie medyczne w badaniach o potencjale translacyjnym. Pracuje w Sano Centre for Computational Medicine w Krakowie.

1 https://mcsb.cm-uj.krakow.pl/ (Modelowanie Cybernetyczne Systemów Biologicznych).

Idea tworzenia bliźniaków istniała jeszcze przed erą komputerów – w postaci fizycznych modeli samolotów, turbin czy fantomów medycznych, które pozwalały testować zachowanie systemów w kontrolowanych warunkach. Można je uznać za „niecyfrowych przodków" współczesnych cyfrowych bliźniaków. Równolegle, od połowy XX w. rozwijało się modelowanie matematyczne w biomedycynie. Powstawały pierwsze równania opisujące elektrofizjologię serca, przepływ krwi czy procesy metaboliczne. Te wczesne modele stanowiły fundament dzisiejszych narzędzi obliczeniowych – w tym cyfrowych bliźniaków tworzonych na potrzeby medycyny[2].

Cyfrowy bliźniak to spersonalizowany model danego systemu, który potrafi przewidywać jego zachowanie w różnych warunkach. W medycynie oznacza to odwzorowanie wymiarów anatomicznych i właściwości fizjologicznych konkretnego pacjenta; sam model jest uproszczoną matematyczną reprezentacją tego systemu.



Taki bliźniak może być konstruowany na różne sposoby. George Box, brytyjski statystyk, mawiał: „wszystkie modele są błędne, ale niektóre są użyteczne". Kluczem jest dobranie właściwego rodzaju modelu do konkretnego problemu i umiejętność łączenia podejść bazujących na danych z podejściami wykorzystującymi prawa natury.

Najważniejsze podejścia do konstrukcji modeli

Modele bazujące na zasadach fizyki i biologii (*first-principles*)

U podstaw wielu cyfrowych bliźniaków leżą modele, które podążają za prawami natury. Opisują fizjologię równaniami różniczkowymi – zwyczajnymi (ODE) i cząstkowymi (PDE) – oraz ujęciami wieloskalowymi, łączącymi poziom komórki, tkanki i całego narządu. Dzięki nim przepływ krwi[3] można ująć w równaniach Naviera–Stokesa, a czynność bioelektryczną serca – w systemach równań elektrofizjologii. Tego rodzaju konstrukcje zachowują interpretowalność i wierność biologii, a co ważne, potrafią działać nawet wtedy, gdy danych pacjenta jest niewiele. Cena za tę przejrzystość bywa jednak natury obliczeniowej: zwłaszcza modele przestrzenne (np. 3D CFD) wymagają znacznych zasobów. Analityczne rozwiązania zdarzają się w medycynie rzadko – najczęściej sięgamy po metody numeryczne. Ich wyniki są przybliżeniem, ale przybliżeniem użytecznym, osiągalnym i wystarczająco precyzyjnym, by prowadzić nas przez złożoność biologii.

Modele bazujące na danych (*data-driven*)

W tym przypadku model uczy się zachowania systemu wyłącznie na podstawie obserwacji – np. danych z obrazowania lub sygnałów biologicznych. Te modele sprawdzają się, gdy istnieją duże zbiory danych. Działają szybko po wytrenowaniu, ale nie potrafią przewidywać tego, czego nie było w danych. To podejście obejmuje statystykę, klasyczne uczenie maszynowe, a współcześnie również bardziej złożone metody AI.

AI/ML (sztuczna inteligencja) jako podzbiór *data-driven*

Sztuczna inteligencja i uczenie maszynowe dynamicznie rozwijają się w prawie wszystkich dziedzinach życia – również w medycynie. Można tu segmentować obrazy i wyciągać geometryczne informacje dla modelu, przyspieszyć symulacje poprzez tzw. *surrogate models* (np. *PINNs*), uzupełniać brakujące fragmenty modeli tam, gdzie brakuje kompletnej wiedzy fizycznej, estymować parametry modeli na podstawie sygnałów pacjenta. Model nie jest jednak w stanie w pełni zastąpić fizyki i biologii – najlepiej działa, gdy stanowi element większego systemu modelowania. Wszystkie modele AI/ML należą do modeli *data-driven*, ale nie wszystkie modele *data-driven* to AI.

Modele hybrydowe (fizyka + dane)

Największą skuteczność osiąga się dziś, łącząc podejścia: fizyka/biologia zapewnia interpretowalność, dane – personalizację i szybkość, AI – automatyzację i optymalizację. Kluczowe jest jednak to, aby model był tak prosty, jak to możliwe, a jednocześnie wystarczająco złożony, by poprawnie opisywać zjawisko.

2 Peter Coveney P., Roger Highfield R.: Virtual You. How Building Your Digital Twin will Revolutionize Medicine and Change Your Life, Princeton University Press, 2023

3 Otta, Magdalena & Zając, Karol & Malawski, Maciej & Halliday, Ian & Lim, Chung & Tsui, Janice & Narracott, Andrew. (2025). Towards Sensitivity Analysis: 3D Venous Modelling in the Lower Limb. Computational Science – ICCS 2025 Workshops. ICCS 2025. Lecture Notes in Computer Science, vol 15908. Springer, Cham. https://doi.org/10.1007/978-3-031-97557-8_8

W praktyce oznacza to, że trzeba z góry wiedzieć, na jakie pytanie model ma odpowiedzieć i dobrać metodę do celu.

Personalizacja, VVUQ i obliczenia dużej skali

Aby model mógł stać się pełnoprawnym cyfrowym bliźniakiem, musi najpierw zostać „osadzony" w konkretnej osobie – dopasowany do jej anatomii, parametrów fizjologicznych i dostępnych danych klinicznych. Dopiero taki spersonalizowany bliźniak może być poddany kolejnym etapom: weryfikacji, walidacji i ocenie niepewności, czyli procesowi VVUQ, który decyduje o tym, czy można mu zaufać. Weryfikacja (*Verification*) sprawdza, czy bliźniak został zbudowany poprawnie – czy równania zapisano tak, jak trzeba i czy numeryka działa zgodnie z założeniami. Walidacja (*Validation*) odpowiada na inne pytanie: na ile zachowanie cyfrowego bliźniaka pokrywa się z obserwacjami świata rzeczywistego? Ocena niepewności (*Uncertainty Quantification*) pozwala zobaczyć, jak błędy i zmienność w danych wejściowych, parametrach czy algorytmach wpływają na wyniki. Analiza wrażliwości[4] dodatkowo wskazuje te elementy, które najmocniej przesuwają wynik w jedną lub drugą stronę, co staje się bezcenne przy dalszej personalizacji.

> ***W medycynie niepewność jest nieodłączna: dane są różnej jakości, obarczone błędami ludzkimi, systemowymi i pomiarowymi. Dlatego to właśnie VVUQ staje się bramą, przez którą cyfrowy bliźniak musi przejść, zanim zacznie wspierać decyzje medyczne.***

Proces ten wymaga ogromnej liczby symulacji – czasem tysięcy, czasem dziesiątek tysięcy – co w praktyce oznacza konieczność korzystania z komputerów dużej mocy (HPC) i zasobów chmurowych[5]. Personalizacja jest więc nie tylko cechą, lecz wręcz warunkiem istnienia cyfrowego bliźniaka. Dopiero bliźniak dopasowany, sprawdzony i „policzony" w wielu wariantach może być uznany za wiarygodny, a jego prognozy – za użyteczne w kontekście decyzji klinicznych.

Cyfrowe bliźniaki w medycynie

Można wyróżnić trzy główne obszary potencjalnego zastosowania medycznych bliźniaków cyfrowych. Po pierwsze, mogą wspierać prewencję, pomagając utrzymać zdrowie pacjentów poprzez monitorowanie czynników ryzyka, choć w praktyce jest to trudne ze względu na dużą zmienność biologiczną i brak jednoznacznej definicji „stanu zdrowia". Po drugie, mogą wspierać leczenie, czego przykładem jest istniejący już system automatycznej podaży insuliny u pacjentów z cukrzycą typu I, bazujący na modelu różniczkowym kalibrowanym na podstawie danych konkretnej osoby. Po trzecie, bliźniaki cyfrowe mogłyby w przyszłości służyć do rozwoju nowych terapii, np. w ramach wirtualnych badań klinicznych, które wymagałyby stworzenia cyfrowej populacji pacjentów. Bliźniaki cyfrowe mogą także wspomagać wczesne wykrywanie chorób, stratyfikację ryzyka i diagnostykę różnicową, uzupełniając tradycyjne badania obrazowe i laboratoryjne.

> ***Rozwój tej technologii wiąże się jednak z wyzwaniami: brakami regulacji, kwestiami prywatności, etyki oraz standaryzacji danych i modeli.***

Mimo to prace nad rozwojem medycznych bliźniaków cyfrowych postępują dynamicznie dzięki inicjatywom takim jak: Virtual Physiological Human (VPH) Society, Swedish Digital Twin Consortium czy ośrodkom takim jak Sano Centre for Computational Medicine.

VPH Society[6] to międzynarodowa organizacja skupiająca badaczy zajmujących się wieloskalowym modelowaniem człowieka. Jej celem jest tworzenie standardów, metod personalizacji, walidacji oraz infrastruktury dla cyfrowych bliźniaków. Społeczność VPH odegrała kluczową rolę w przeniesieniu modelowania obliczeniowego do medycyny. Towarzystwo to organizuje co dwa lata konferencję; tematem przewodnim najbliższej[7] jest „*Towards the adoption of digital twins in healthcare*" („W kierunku wdrożenia cyfrowych bliźniaków w opiece zdrowotnej"). Obecnie Komisja Europejska podjęła ini-

4 Sensitivity analysis of closed-loop one-chamber and four-chamber models with baroreflex K Tlałka, H Saxton, I Halliday, X Xu, A Narracott, D Taylor, M Malawski PLoS computational biology 20 (12), e1012377 https://doi.org/10.1371/journal.pcbi.1012377

5 Digital twin simulation development and execution on HPC infrastructures M Kasztelnik, P Nowakowski, J Meizner, M Malawski, A Nowak, K Gadek, K Zajac, A La Mattina, M Bubak International Conference on Computational Science, 18-32, https://doi.org/10.1007/978-3-031-36021-3_2

6 https://vph-society.org/

7 9th International Conference on the Virtual Physiological Human https://vph-conference.org/)

cjatywę budowy platformy informatycznej wspierającej badania nad tworzeniem modeli obliczeniowych dla cyfrowych bliźniaków[8].

Sano Centre for Computational Medicine[9] jest międzynarodową fundacją badawczą powstałą w 2019 r. w Krakowie, której celem jest prowadzenie prac badawczych i rozwojowych w dziedzinie zastosowań metod obliczeniowych i sztucznej inteligencji w medycynie oraz wprowadzanie ich do praktyki klinicznej. Obecnie agenda badawcza Sano[10] koncentruje się na rozwoju technologii cyfrowych bliźniaków, od poziomu infrastruktur obliczeniowych, poprzez tworzenie narzędzi informatycznych, modeli obliczeniowych po warstwę interfejsów dla użytkowników – badaczy, lekarzy i pacjentów. Zespół Sano łączy badaczy z różnych dziedzin, w tym informatyków, fizyków, inżynierów, biologów, którzy przy wsparciu programistów naukowych tworzą nowe rozwiązania we współpracy z lekarzami.

Pierwszym komercyjnie dostępnym rozwiązaniem dla lekarzy jest HeartFlow[11] – to przykład cyfrowego bliźniaka tętnic wieńcowych, który – na podstawie angio-TK – rekonstruuje geometrię naczyń i oblicza wirtualną frakcję przepływu (FFR-CT). Narzędzie jest dopuszczone klinicznie i pokazuje, że cyfrowe bliźniaki mogą realnie wspierać diagnostykę i planowanie terapii, redukując potrzebę inwazyjnych badań.

Wizja przyszłości

Cyfrowe bliźniaki będą zapewne wchodzić do medycyny stopniowo, nie jako pojedyncze narzędzia, lecz jako elementy większego ekosystemu, który wspiera diagnozowanie, monitorowanie i planowanie terapii. Można wyobrazić sobie niedaleką przyszłość, w której każdy pacjent ma swojego wirtualnego odpowiednika, stale aktualizowanego danymi z badań obrazowych i fizjologicznych, a także sensorów codziennego użytku. Decyzje kliniczne mogłyby być wtedy wspierane symulacjami różnych scenariuszy leczenia, a nowe interwencje najpierw testowane na populacjach cyfrowych, zanim trafią do tradycyjnych badań klinicznych. Wymaga to jednak uporządkowanej drogi: wspólnych standardów, rygorystycznej walidacji, jasnych regulacji prawnych oraz infrastruktury umożliwiającej pracę z dużą skalą danych i obliczeń. Mimo tych wyzwań kierunek rozwoju jest wyraźny – medycyna staje się coraz bardziej spersonalizowana, przewidywalna i bazująca na zrozumieniu indywidualnej fizjologii, a nie wyłącznie na uśrednionych wzorcach populacyjnych.

Idea cyfrowego bliźniaka dla opieki zdrowotnej wyszła już poza ośrodki badawcze: w marcu 2026 r. zakończyły się konsultacje publiczne opracowanej przez Klaster Lifescience[12] z udziałem Sano na zlecenie Małopolskiego Urzędu Marszałkowskiego, Mapy Drogowej Współpracy „Cyfrowy Pacjent", będącej częścią małopolskiej platformy „Zdrowe Społeczeństwo"[13].

8 https://www.virtualhumantwins.eu/

9 https://sano.science/

10 Sano Research Agenda 2025–2028, https://sano.science/sano-e-books/

11 https://www.heartflow.com/

12 https://lifescience.pl/

13 Małopolska Innowacyjna – Platforma „Zdrowe Społeczeństwo" https://innowacyjna.malopolska.pl/pl/wiedza/platformy-specjalizacyjne/platforma-zdrowe-spoleczenstwo

Obliczenia dużej skali dla nauki, humanistyki, przemysłu

Marek Magryś, Marian Bubak, Patryk Lasoń, Robert Pająk, Mariusz Sterzel



Marek Magryś
p.o. dyrektora Akademickiego Centrum Komputerowego Cyfronet AGH, kierownik Narodowego Centrum Kompetencji Obliczeniowych w ramach EuroHPC, specjalista w zakresie projektowania, wdrażania, testowania i eksploatacji systemów obliczeniowych dla zastosowań HPC (High Performance Computing) oraz AI (sztucznej inteligencji). Główny architekt najszybszych polskich superkomputerów ostatnich lat Heliosa, Atheny i Prometheusa. Ekspert Komisji Europejskiej, członek grupy doradczej INFRAG dla EuroHPC i komitetu doradczego HPC-AI Leadership Organization EMEA.

Marian Bubak
tytuły mgr. inż. fizyki technicznej i dr. informatyki uzyskał w AGH w Krakowie, gdzie przez wiele lat był adiunktem w Instytucie Informatyki. Nadal współpracuje z AGH, prowadząc wykłady z algorytmów równoległych, informatyki kwantowej i seminarium z informatyki kwantowej KQIS. W latach 2000–2004 dziekan i organizator Wydziału Informatyki WSZiB w Krakowie, zaś w latach 2006–2016 Professor of Distributed Systems Engineering w Informatics Institute, University of Amsterdam. Od 1997 r. pracownik ACK Cyfronet AGH. Obecnie jest dyrektorem ds. naukowych Sano Centre for Computational Personalised Medicine w Krakowie. Wiceprezes PTI ds. naukowych, https://pti.org.pl/zarzad-glowny/marian-bubak/

Patryk Lasoń
pracuje w ACK Cyfronet AGH od 2004 r., obecnie kierownik Działu Komputerów Dużej Mocy. Ma wieloletnie doświadczenie w projektowaniu, wdrażaniu, testowaniu i eksploatacji systemów obliczeniowych typu HPC (High Performance Computing). Administrator superkomputerów Prometheus, Ares, Athena, Helios. Uczestniczył w realizacji wielu projektów infrastrukturalnych, m.in.: EGEE, Crossgrid, POWIEW, Platon, PL-Grid, PLGrid Plus, PLGrid CORE, PRACE, PRACE-Lab.

Robert Pająk
tytuł mgr. inż. informatyki uzyskał w Akademii Górniczo-Hutniczej w Krakowie. Od 2002 r. pracuje w ACK Cyfronet AGH. Zajmował się promocją wielu międzynarodowych i krajowych projektów oraz organizacją dużych konferencji naukowych. Obecnie, na stanowisku kierownika Działu Użytkowników, zajmuje się m.in. opracowywaniem informacji oraz materiałów promujących działalność Cyfronetu.

Mariusz Sterzel
doktor nauk chemicznych, specjalista HPC, jest przedstawicielem Polski w Radzie EuroHPC JU. Kierownik aktywności ACK Cyfronet AGH w projektach AARC2, Sat4Envi, EuroHPC PL. Członek Rady TCS Anthropogenic Hazard w EPOS ERIC. Koordynator aktywności Polskiego Centrum Kompetencji EuroHPC w projekcie EuroCC. Po odbyciu staży zagranicznych w Wielkiej Brytanii i Stanach Zjednoczonych rozpoczął pracę w Cyfronecie przy serii projektów Enabling Grids for E-SciencE, w których koordynował Klaster Chemii Obliczeniowej w projektach EGEE II i EGEE III. Brał udział w tworzeniu infrastruktury PLGrid i koordynował tam prace polegające na ujednoliceniu dostępu do oprogramowania naukowego. Pracuje w ACK Cyfronet AGH na stanowisku kierownika działu Laboratorium Obliczeń Kwantowych. Główne kierunki aktywności Laboratorium to rozwiązywanie problemów optymalizacyjnych i obliczenia kwantowe struktury elektronowej molekuł.

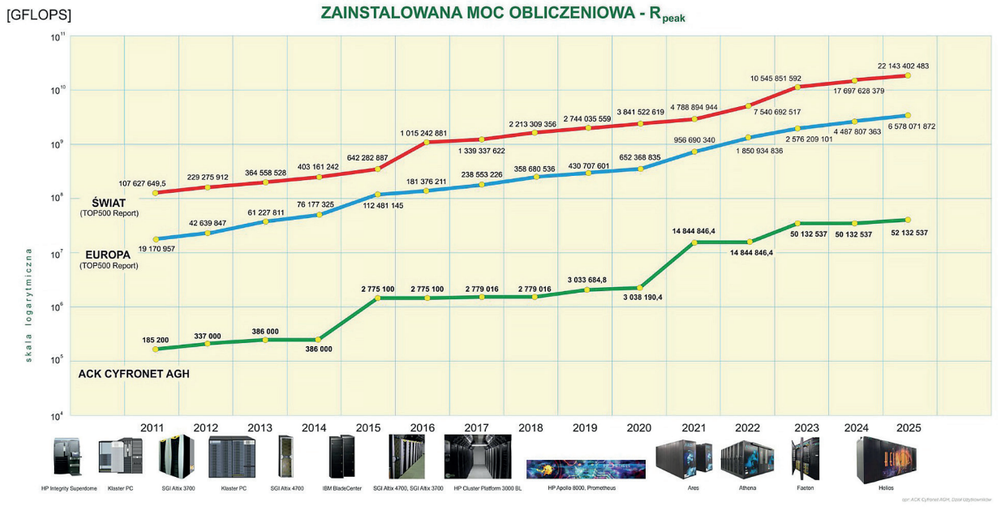
W Polsce działa obecnie sześć centrów Komputerów Dużej Mocy (KDM). Centra te współpracują i konkurują ze sobą, wykorzystując swego rodzaju komplementarność, wynikającą z różnych dróg powstawania i rozwoju. Uczestniczą w różnych przedsięwzięciach krajowych i międzynarodowych, wymieniają doświadczenia w zakresie usług obliczeniowych, przechowywania danych i rozwoju sieci komputerowych. Seniorem w tym gronie jest Akademickie Centrum Komputerowe Cyfronet AGH, starsze o 10 lat od PTI.

O historii tego centrum pięknie opowiada wydawnictwo, opublikowane w 2023 r. z okazji 50-lecia Cyfronetu[1].

Na początku było Środowiskowe Centrum Obliczeniowe Cyfronet

W 1971 r. Kolegium Rektorów uczelni krakowskich wystąpiło z ideą utworzenia centrum obliczeniowego na potrzeby akademickiego środowiska Krakowa. Decyzją rządową 23 marca 1973 r. zostało powołane Środowiskowe Centrum Obliczeniowe Cyfronet jako samodzielna jednostka podległa administracyjnie odpowiedniemu ministerstwu, a merytorycznie – Radzie Naukowej (Radzie Użytkowników). Warto wspomnieć, że w 1999 r. – w trosce o niezaburzanie struktury organizacyjnej jednostek naukowych w Polsce – Cyfronet stał się wyodrębnioną organizacyjnie i finansowo jednostką AGH.

Po decyzji rządowej w 1973 r. rozpoczęła się procedura zakupowa – co w owych czasach było niezwykle trudnym przedsięwzięciem (COCOM – patrz: Wikipedia) – w jej wyniku 27 czerwca1975 r. został oddany do użytku komputer CDC CYBER 72-16 ze swego rodzaju otoczeniem sieciowym, obejmującym 20 terminali ulokowanych w jednostkach naukowych Krakowa. W 1991 r. CYBER został odesłany na bardzo zasłużoną emeryturę, a na jego miejsce udało się zakupić maszynę wektorową CONVEX, określaną wtedy jako minisuperkomputer. W latach 90. ub. w. rozpoczęła się era obliczeń równoległych. W 1996 r. w Cyfronecie został zainstalowany komputer równoległy firmy CONVEX – EXEMPLAR SPP1600 i od tej pory cyfronetowe komputery trafiały na prestiżową listę TOP 500 (https://top500.org/).



Wzrost mocy obliczeniowej na świecie, w Europie i w Cyfronecie
Źródło: Cyfronet AGH, autor: Robert Pająk

[1] K. Wiatr et al. (red.), *Cyfronet: moc dla polskiej nauki, 50 lat Cyfronet: 1973/2023*, Kraków, ACK Cyfronet AGH, 2023

Zasoby sprzętowe Cyfronetu

Komputery Cyfronetu opisuje strona https://www.cyfronet.pl/pl/supercomputers/our-supercomputers. Poniżej tylko ich główne charakterystyki:

- Helios: 37 PFlops teoretycznej mocy obliczeniowej, ponad 131 tysięcy rdzeni obliczeniowych, 393 TB pamięci operacyjnej i 17,5 PB pojemności systemów dyskowych, wydajność 2 TB/s.
- Athena: 7,7 PFlops teoretycznej mocy obliczeniowej, 48 serwerów z procesorami AMD EPYC i 1 TB pamięci RAM (w sumie 6144 rdzenie obliczeniowe CPU) oraz 384 karty GPGPU NVIDIA A100.
- Ares: teoretyczna wydajność części CPU to ponad 3,5 PFlops, a części GPU to ponad 0,5 PFlops.
- Prometheus: moc obliczeniowa 2,65 PFlops, od uruchomienia w 2015 r. był 15 razy z rzędu notowany na liście TOP500, najwyżej na 38. pozycji.
- Faeton: teoretyczna moc obliczeniowa 288 Tflops, zbudowany z 64 serwerów obliczeniowych, a każdy z nich ma dwa procesory Intel Xeon Platinum, 1 TB pamięci operacyjnej oraz adaptery sieci 100 Gb/s Ethernet; cztery serwery mają dodatkowe 8 TB pamięci SCM Intel Optane.

Cyfronet dysponuje zaawansowanym systemem składowania danych połączonym z superkomputerami, a rozproszenie na trzy centra danych umożliwia automatyczne tworzenie kopii zapasowych w wielu fizycznych lokalizacjach, co zwiększa bezpieczeństwo danych (https://www.cyfronet.pl/pl/offer/data-storage).

Od 1990 r. Cyfronet rozwija Miejską Sieć Komputerową (MAN) jako oryginalne, autorskie rozwiązanie zespołu centrum. Obecnie ma ona ponad 200 km długości, korzysta z niej ok. 22 tys. pracowników naukowych i 160 tys. studentów. Cyfronet jest węzłem ogólnopolskiej sieci PIONIER.

Usługi obliczeniowe

Optymalne wykorzystanie infrastruktury sprzętowej wymaga zaawansowanego oprogramowania. Pracownicy Cyfronetu i współpracujących instytucji naukowych opracowali wiele narzędzi i platform obliczeniowych by zaspokoić potrzeby użytkowników. Oto kilka przykładów:

- Platforma Model Execution Environment (MEE), opracowana w Laboratorium Metod Informatycznych w Medycynie i w Sano Centre for Computational Personalised Medicine, to narzędzie do realizacji złożonych symulacji komputerowych, w tym wykonywanych przez kilka współpracujących ze sobą zespołów. Platforma MEE jest zintegrowana z mechanizmami uwierzytelniania i bezpieczeństwa infrastruktury PLGrid.
- Onedata, system opracowany i rozwijany w Laboratorium Technologii Chmurowych, to globalnie skalowalne narzędzie do zarządzania danymi, ujednolicające dostęp do danych przechowywanych w systemach rozproszonych.

Jedną z metod zwiększania kompetencji pracowników i nawiązywania współpracy są organizowane przez Cyfronet konferencje. Pierwszą międzynarodową konferencją Cyfronetu była Convex Users' Group w 1994 r., a po niej przyszły konferencje użytkowników PVM/MPI, IBM, SGI. Niektóre z nich były poważnym wyzwaniem logistycznym ze względu na liczbę uczestników i sesji równoległych: ICCS – International Conference on Computational Science w 2004 r. (ok. 650 uczestników) i w 2008 r. (ok. 450 uczestników), EuroHPC Summit w marcu 2025 r. (ok. 1500 uczestników). Z kolei cykl 18 konferencji CGW (Cracow Grid Workshop) w latach 2001–2018 był ukierunkowany na propagowanie technologii gridowych i chmurowych, zapraszano więc na CGW licznych ekspertów w tych dziedzinach.

Organizowana co roku wiosną (od 2008 r.) „KU KDM – Konferencja Użytkowników Komputerów Dużej Mocy" jest okazją do prezentacji wyników realizowanych symulacji komputerowych, wymiany doświadczeń, spotkań i dyskusji użytkowników z pracownikami Cyfronetu, licznych szkoleń i warsztatów. Tegoroczna zgromadziła ponad 220 uczestników (https://www.cyfronet.pl/pl/events/our-conferences/kukdm-2026).

Co roku w listopadzie (od 2004 r.) ma miejsce coroczna, otwarta, jednodniowa Konferencja „Dzień Otwarty Cyfronetu", prezentująca działalność Cyfronetu, jego zasoby sprzętowe, oprogramowanie i prowadzone projekty badawcze. Konferencja jest też okazją do ogłoszenia wyników konkursu na najlepszą rozprawę doktorską opracowaną z pomocą badań zrealizowanych z wykorzystaniem zasobów Cyfronetu (https://www.cyfronet.pl/pl/events/our-conferences/open-day-2025).

- Narzędzie pro-viz pozwala użytkownikom klastrów obliczeniowych na korzystanie z aplikacji w trybie graficznym (GUI) opartym o środowisko XFCE bezpośrednio na węzłach obliczeniowych klastra, również z możliwością akceleracji GPU.

- Platforma LLM Lab umożliwia korzystanie z dużych modeli językowych, dostosowanych do różnorodnych potrzeb, takich jak analiza danych, modelowanie oraz automatyzacji procesów badawczych. Jednym z modeli dostępnych na platformie jest Bielik, zoptymalizowany pod kątem polskiej morfologii i składni.

Cyfronet jako centrum kompetencji

Od początku istnienia Cyfronetu wielką wagę przywiązywano do szkoleń i rozwoju kadr; bez właściwie przygotowanych pracowników nie byłoby możliwe ani wykorzystanie zasobów sprzętowych, ani dostarczanie użytkownikom usług na wysokim poziomie. Kierownictwo Cyfronetu zawsze dbało o bardzo dobrą współpracę z uczelniami Krakowa, a współpraca z Instytutem Informatyki AGH była stała i bezpośrednia.

Oprócz działów realizujących zadania związane z utrzymaniem i rozwojem infrastruktury sprzętowej, administracją, finansami, obsługą projektów, w strukturze Cyfronetu działa pięć laboratoriów realizujących prace badawczo-rozwojowe. Są to laboratoria: Technologii Chmurowych, Przetwarzania Danych, Interdyscyplinarnych Obliczeń Naukowych, Obliczeń Kwantowych, Metod Informatycznych w Medycynie.

PLGrid

W 2007 r. pięć polskich centrów komputerowych (Cyfronet, PCSS, ICM, TASK i WCSS) utworzyło konsorcjum PLGrid (https://plgrid.pl/), które pozyskało trzy polskie granty na budowę i utrzymanie infrastruktury obliczeniowej dla polskiej nauki, a następnie na rozwój oprogramowania specyficznego dla wybranych dziedzin nauki. PLGrid oferuje dostęp do superkomputerów, komputerów kwantowych, specjalizowanych akceleratorów dla sztucznej inteligencji, chmury obliczeniowej, pamięci dyskowych, zoptymalizowanego oprogramowania obliczeniowego oraz wsparcia ekspertów z całej Polski. Wypracowane w tworzeniu PLGrid rozwiązania miały wartość naukową i zostały opublikowane w ramach serii *Springer Lecture Notes on Computer Science* zarówno w odniesieniu do infrastruktury[2], jak i oprogramowania i uzyskanych pierwszych wyników[3]. PLGrid pokazuje dobitnie, jak wartościowa dla polskiej nauki jest kooperacja polskich centrów komputerowych.

Polskie centra KDM:

1. **Akademickie Centrum Komputerowe Cyfronet AGH w Krakowie (https://www.cyfronet.pl/),**
2. **Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS) afiliowane przy Instytucie Chemii Bioorganicznej PAN (ICHB PAN) (https://www.pcss.pl/),**
3. **Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego (ICM) Uniwersytetu Warszawskiego (https://icm.edu.pl/),**
4. **TASK – Centrum Informatyczne Trójmiejskiej Akademickiej Sieci Komputerowej – Politechnika Gdańska (https://task.gda.pl/pl),**
5. **Wrocławskie Centrum Sieciowo-Superkomputerowe – Politechnika Wrocławska (https://wcss.pl/),**
6. **Centrum Informatyczne Świerk – Narodowe Centrum Badań Jądrowych, https://www.cis.gov.pl/.**

Współpraca międzynarodowa

Od początku rozwoju Cyfronetu stawiano na różne formy współpracy międzynarodowej. Były one związane ze szkoleniami pracowników w firmach CDC, CONVEX, HP, nawiązano też okazjonalną współpracę z Jülich Supercomputing Centre. Współpraca międzynarodowa naprawdę jednak rozwinęła się dopiero wtedy, gdy pojawiła się możliwość udziału w projektach badawczych Unii Europejskiej. Było to w roku 2002, na dwa lata przed przyjęciem Polski do UE.

Pierwszy projekt, realizowany w latach 2002–2005 i koordynowany przez Cyfronet (koordynator – prof. Michał Turała), to „CrossGrid – Development of GRID Environment for Interactive Applications" (https://cordis.europa.eu/article/id/84198-testing-computer-grid-infrastructure). Projekt zakończył się sukcesem i otworzył drogę do wielu innych działań. Kolejne etapy to uzyskanie grantu EU Widening Teaming na utworzenie Sano Centre for Computational Personalised Medicine (https://sano.science/), udział w EuroHPC JU (*The European High Performance Computing Joint Undertaking*) i LUMI (*The Large Unified Modern Infrastructure* – jeden z najszybszych superkomputerów w Europie). Cyfronet jest również krajowym koordynatorem aktywności Wspólnego Przedsięwzięcia EuroHPC. Dzięki tym projektom Cyfronet współpracuje na co dzień ze wszystkimi ważnymi centrami komputerowymi Unii Europejskiej, jest obecny, rozpoznawany i doceniany na ważnych w tym środowisku konferencjach: *International Supercomputing Conference* w Europie i *Supercomputing* w USA.

Nowe obszary działania

ACK Cyfronet AGH systematycznie rozszerza swoje pole aktywności nie zaniedbując tego, do czego przed 53 laty został powołany przez środowisko naukowe Krakowa: dostarczanie mocy dla polskiej nauki, mocy rozumianej szeroko, mierzonej nie tylko cyklami i liczbą procesorów, ale przede wszystkim wysokimi kompetencjami pracowników.

Nowymi obszarami działania Cyfronetu są:

- Obliczenia kwantowe, szerzej przedstawione w opublikowanym w tym numerze „Domeny" artykule „Obliczenia kwantowe w Polsce: stan i perspektywy",
- Metody i narzędzia sztucznej inteligencji, opisane w opublikowanym w tym numerze „Domeny" artykule „Gaia AI Factory: infrastruktura dla rozwoju sztucznej inteligencji i budowy suwerenności technologicznej".

- Oferta innowacyjnego, komercyjnego wdrażania obliczeń dużej skali i AI dla firm działających w logistyce, medycynie, przetwarzaniu obrazów satelitarnych, w badaniach nad lekami, w przemyśle motoryzacyjnym.

- Zastosowanie metod obliczeniowych, analizy danych i sztucznej inteligencji w badaniach z dziedziny sztuki i humanistyki oraz w udostępnianiu wyników tych prac; pierwsze wyniki pracownicy Cyfronetu pokazali na współorganizowanej przez Cyfronet konferencji „Informatyka w sztuce i w humanistyce" 19 maja 2025 r. (https://pti.org.pl/konferencja-informatyka-w-sztuce-i-humanistyce/).

- Cyberbezpieczeństwo, bezpieczeństwo przetwarzania danych.

Znakomita kadra, rozwinięta współpraca krajowa i międzynarodowa, krytyczni, ale rozumni użytkownicy, przyjazne i chętne do współdziałania środowisko oraz 53 lata doświadczeń są dobrą rękojmią powodzenia w realizacji przedstawionych zamierzeń i sprostania jeszcze nieznanym wyzwaniom. Cyfronet nadal będzie tym miejscem, gdzie – jak do tej pory – nowe idee i technologie informatyczne są implementowane z pożytkiem dla użytkowników.

2 M. Bubak, T. Szepieniec, K. Wiatr (eds), *Building a National Distributed e-Infrastructure - PL-Grid*, LNCS 7136, Springer, 2012.

3 M. Bubak, J. Kitowski, K. Wiatr (eds), *eScience on Distributed Computing Infrastructure. Achievements of PLGrid Plus Domain-Specific Services and Tools*, LNCS 8500, Springer, 2014.

Nowoczesna informatyka w Wielkiej Nauce: wyzwania, strategia, szanse

Jakub T. Mościcki

Jednym z głównych wyzwań stojących przed infrastrukturą informatyczną w projektach typu Big Science, takich jak *Large Hadron Collider* (LHC) lub *Square Kilometre Array* (SKA), jest zapewnienie wydajnego funkcjonowania tej infrastruktury podczas całego czasu eksploatacji kompleksu badawczego liczonego w dekadach. Duże i stale rosnące potrzeby w zakresie przechowywania i przetwarzania danych w eksperymentach LHC wymagają wieloletniej strategii bazującej na odpowiednim zestawie usług i technologii.



Jakub T. Mościcki

Head of Storage and Data Management Group, CERN

Strategia CERN IT bazuje na budowie rozwiązań z wykorzystaniem otwartego oprogramowania (Open Source) w ścisłej współpracy ze społecznością naukową i dostawcami infrastruktury. Istotną jej częścią są też projekty badawczo-rozwojowe prowadzone z przemysłem oraz współpraca z innymi organizacjami międzynarodowymi i badawczymi w ramach szerszego europejskiego ekosystemu innowacji i otwartej nauki (*Open Science*).

Rozwiązania zaprojektowane i wdrożone dla fizyki wysokich energii znalazły już swoje zastosowania przy budowie infrastruktury dla innych dziedzin nauki i – z perspektywy CERN IT – stanowią swoistą platformę innowacji technicznej na przyszłość. Stwarza to dodatkową przestrzeń dla instytucji z państw członkowskich CERN, takich jak Polska, do rozwijania współpracy, projektów technologicznych i wdrożeniowych, w ramach krajowych infrastruktur badawczych oraz szerszej strategii innowacji cyfrowej na poziomie europejskim.

Strategia przechowywania danych – przypadek LHC

Akceleratory, eksperymenty i informatyka to trzy filary infrastruktury badawczej CERN. Model obliczeniowy i infrastruktura informatyczna dla LHC została opracowana w trakcie budowy akceleratora i kompleksu eksperymentalnego w latach 1998–2009.

W ciągu pierwszych trzech lat działania LHC eksperymenty CERN – ATLAS, ALICE, CMS i LHCb – wytworzyły łącznie 60 PB danych surowych (RAW), co przyczyniło się do odkrycia bozonu Higgsa w 2012 r. Czternaście lat później, w roku 2026, eksperymenty LHC wytwarzają do 60 PB danych RAW **w ciągu jednego miesiąca**, a całkowita ilość zebranych danych eksperymentalnych przekroczyła 1 EB i podwoiła się w ciągu ostatnich trzech lat. Po najnowszym etapie modernizacji eksperymenty High Luminosity LHC mają, do początku lat 40. XXI wieku, wytworzyć dziesięciokrotnie więcej danych niż dotychczas. Dla porównania, całość danych z LEP – wcześniejszego eksperymentu CERN z lat 80. XX wieku – stanowi mniej niż 0,1 promila danych wygenerowanych przez LHC do tej pory.

> *Infrastruktura obliczeniowa i przechowywania danych dla LHC musi więc być utrzymywana i odpowiednio skalowana przez ponad 40 lat przy niezmiennym, ustalonym na tym samym poziomie rocznym budżecie (flat budget), w warunkach nieustannej ewolucji architektur sprzętowych i software'owych oraz branży IT jako całości.*

Strategia CERN IT zarządzania ryzykiem technologicznym i rynkowym przy jednoczesnym utrzymaniu możliwie niskich kosztów opiera się rozwoju definiowanych software'owo, wielowarstwowych usług przechowywania danych (*software-defined tiered-storage*), działających na bazie standardowej infrastruktury sprzętowej (*storage* i *compute*) wdrożonej lokalnie w CERN oraz w powiązanych centrach danych Worldwide LHC Computing Grid (WLCG). Rozwój tych technologii bazuje na modelu Open Source w ramach szerszej społeczności instytucji powiązanych z CERN (techweekstorage.web.cern.ch).

System EOS – opracowany w CERN do szybkiego dostępu oraz przetwarzania i analizy danych fizycznych – został zaprojektowany do zarządzania dużymi pulami danych (replikacja oraz *Erasure Coding*) z wykorzystaniem tanich systemów dysków JBOD i SSD. System CTA (CERN *Tape Archive*) efektywnie zarządza i optymalizuje dostęp do archiwalnej pamięci taśmowej z częstymi odwołaniami (*active archive*), wykorzystując niejednorodną infrastrukturę taśmową i dwie główne technologie nośników (*LTO* i *Enterprise*).

Obecnie w samym CERN oba systemy zapewniają łącznie ponad 2 EB pojemności: EOS zarządza 150 tys. dysków w 1500 węzłach pamięci masowej, a CTA zarządza 80 tys. kaset taśmowych w 6 bibliotekach taśmowych. Zarówno EOS, jak i CTA są wdrażane w wielu innych centrach danych WLCG. W rezultacie jednostkowy koszt przechowywania danych jest o jeden rząd wielkości niższy niż w chmurach publicznych lub komercyjnie dostępnych systemach storage. Taka strategia umożliwia także całościowe optymalizowanie systemu obejmującego aplikacje, protokoły dostępu do danych i warstwę storage.

Wyzwania technologiczne przechowywania danych w dużej skali

Otwarta architektura software'owego zarządzania przechowywaniem danych (*software-defined storage*) umożliwia stosunkowo łatwe dostosowanie usług do ewoluujących technologii pamięci masowych. Obecnie jest to szczególnie istotne, ponieważ tempo spadku kosztów pamięci masowej malej, a dostępna przepustowość (*bandwidth*) rośnie wolniej, niż rośnie pojemność dysków (*capacity*). Oznacza to, że mniejsza część danych przechowywanych na urządzeniach pamięci dyskowej może być efektywnie udostępniana w jednostce czasu, co powoduje, że większa część danych staje się „zimna" (*cold storage*). Zwiększa to też tzw. domeny awarii (*failure domains*) – awaria pojedynczego węzła storage może oznaczać utratę pojemności rzędu petabajtów – oraz wydłuża związany z nią czas odbudowy danych.

Pod wpływem komercyjnego rynku usług hiperskali (*hyperscalers*) również infrastruktura i technologie taśmowe ewoluują w kierunku zastosowań typu *cold storage*, gdzie dane są prawie nigdy nieodczytywane (czyli przeciwnie do wymagań dla systemów danych LHC). Nowo komercjalizowane biblioteki taśmowe w formacie rack, takie jak IBM *Diamondback*, wprowadzają mniejszy i stały stosunek liczby napędów taśmowych do liczby kaset niż w tradycyjnych bibliotekach taśmowych, co wprowadza dodatkowe ograniczenia operacyjne dla aktywnych archiwów danych.

Dotychczas skalowanie infrastruktury IT w CERN przy stałym budżecie było gwarantowane przez prawo Moore'a – wystarczyło poczekać, aby pojemność i przepustowość systemu się podwoiła przy tych samych kosztach. Jednak w ostatnich latach tempo skalowania infrastruktury spada przy jednoczesnym gwałtownym wzroście wolumenu danych zarówno w przypadku Big Science, jak i w skali globalnej. W konsekwencji zaawansowane optymalizacje wykorzystujące właściwości fizyczne nośników danych stają się kluczowe i są obecnie intensywnie rozwijane przez producentów sprzętu.

Na przykład zewnętrzne ścieżki dysków twardych oferują większą przepustowość danych niż wewnętrzne, co efektywnie tworzy regiony o odmiennych charakterystykach dostępu w obrębie jednego dysku, a technologia częściowego nadpisywania ścieżek magnetycznych (SMR) pozwala dalej zwiększać pojemność pojedynczych urządzeń (aczkolwiek kosztem wydajności zapisu). Warstwa zarządzania blokami pamięci dysków SSD (Flash Translation Layer) zapewnia nie-

zbędną redundancję w obrębie pojedynczego urządzenia, aczkolwiek tego typu optymalizacje mogą być bardziej efektywne, jeśli są koordynowane na poziomie oprogramowania obejmującego wiele urządzeń jednocześnie (np. w komercyjnych rozwiązaniach typu Filer). Nowym trendem jest też przetwarzanie bazujące na AI bezpośrednio w urządzeniach storage w celu optymalizacji systemu lub wykrywania zagrożeń związanych z cyberbezpieczeństwem.

Tym istotniejsze jest efektywne wykorzystanie tego typu optymalizacji przez warstwę software'ową w dużej skali, w systemach takich jak EOS i CTA. To przedmiot testów i badań prowadzonych wraz z producentami sprzętu w ramach CERN openlab.

Rozproszone zarządzanie danymi

Współczesna nauka w coraz większym stopniu bazuje na transgranicznej współpracy grup badawczych przy użyciu globalnej sieci zasobów informatycznych i rozproszonego udostępniania, zarządzania i archiwizacji danych. W przypadku fizyki wysokich energii społeczność użytkowników (ok. 30 tys. fizyków i inżynierów) znajduje się w większości poza CERN i – w ramach federacji WLCG – korzysta ze swoich zasobów instytucjonalnych lub krajowych do analizy danych LHC.

Model federacyjny wymaga globalnej dystrybucji danych, efektywnego zarządzania dostępnością zbiorów danych do przetwarzania w rozproszonych centrach obliczeniowych oraz spójnego dostępu do innych zasobów, takich jak oprogramowanie do analizy danych. Usługa *File Transfer Service* (FTS), rozwijana w CERN, zapewnia transport danych LHC i interoperacyjność w sieci około 100 ośrodków WLCG na całym świecie (w skali kilku eksabajtów danych przesłanych rocznie i 60 tys. równoległych transferów plików). Podobnie usługa CVMFS umożliwia globalną dystrybucję rozbudowanych pakietów oprogramowania do analizy i przetwarzania danych, zapewniając ich spójne wersjonowanie i udostępnianie na setkach tysięcy węzłów obliczeniowych w WLCG. Bazując na agresywnej deduplikacji bloków danych i wielopoziomowym buforowaniu, usługa CVMFS zapewnia efektywny dostęp do 90 repozytoriów oprogramowania eksperymentalnego zawierających w sumie 5 mld plików. Systemy zarządzania danymi wyższego poziomu, takie jak Rucio, zarządzają regułami dostępu i replikacji danych i są łatwe do dostosowania do szczególnych wymagań grup badawczych.

Model Open Source rozwoju serwisów m.in. FTS, CVMFS i Rucio umożliwia ich wykorzystanie do zarządzania danymi w różnych infrastrukturach, takich jak Grid Computing, centra HPC, Fabryki AI oraz szerzej – w ramach europejskich infrastruktur federacyjnych.

Europejskie infrastruktury federacyjne dla otwartej nauki

Infrastruktury federacyjne odpowiadają na jedno z największych strukturalnych wyzwań Europy: fragmentację między krajami, systemami i instytucjami. Europejskie inicjatywy federacji cyfrowej mają na celu stworzenie transgranicznych usług i jednolitego rynku cyfrowego w obrębie sektorowych przestrzeni danych (zdrowie, energia, mobilność) oraz instytucji publicznych, w szczególności w sektorze edukacji i badań.

> *Jednolity rynek cyfrowy, czyli unia danych, jest głównym celem strategicznym Europy w celu zmniejszenia zależności od pozaeuropejskich dostawców technologii oraz wspierania strategii innowacji cyfrowych. Otwarta nauka jest częścią tej strategii, a European Open Science Cloud (EOSC) to główna inicjatywa wdrożeniowa.*

Celem inicjatywy federacyjnej EOSC jest przekształcenie rozproszonych zasobów badawczych w jednolitą, otwartą i współpracującą przestrzeń cyfrową dla nauki oraz zapewnienie dostępu do danych zgodnie z zasadami FAIR (*Findable*, *Accessible*, *Reusable*, *Reproducible*). Interoperacyjność FAIR systemów przechowywania danych pozwala na lepszą integrację z systemami przetwarzania danych w fabrykach AI.

Jednym z typów usług dostępnych w ekosystemie EOSC są systemy *file sync & share* (EFSS – *Enterprise File Sync&Share*), które umożliwiają łatwe współdzielenie danych i współpracę pomiędzy użytkownikami. CERN IT było pionierem integracji tego typu usług ze środowiskami analizy i przetwarzania naukowego, wyprzedzając podobne rozwiązania rozwijane później przez przemysł (np. gDrive/GoogleCollab).

W przeciwieństwie do systemów komercyjnych, CERNBox zapewnia pełną integrację funkcji sync & share z dostępem online i offline do całego repozytorium danych naukowych na poziomie instytucjonalnym. CERNBox integruje się z narzędziami takimi jak *Jupyter Notebook* oraz lokalnymi platformami analitycznymi i zapewnia ciągłość przestrzeni pracy i analizy danych pomiędzy usługami centrum danych a urządzeniami końcowymi użytkowników. Umożliwia to zupełnie nowe sposoby gromadzenia, dostępu i pracy z danymi, takie jak: transparentne współdzielenie przestrzeni do analizy danych między urządzeniami końcowymi typu laptop, centralnymi usługami obliczeniowymi i przetwarzaniem Grid oraz zautomatyzowane pozyskiwanie i przetwarzanie danych z rozproszonych urządzeń laboratoryjnych (np. oscyloskopów).

Obecnie system CERNBox zarządza 4 mld plików i stanowi środowisko pracy dla tysięcy użytkowników CERN.

CERN IT odegrało również kluczową rolę w utworzeniu społeczności CS3 (cs3community.org) https://www.cs3community.org – użytkowników, deweloperów i operatorów usług *sync & share* w całej Europie. CS3 stworzyło forum umożliwiające skuteczne ustanowienie interoperacyjności technicznej pomiędzy platformami *sync & share*, rozwijanymi niezależnie przez europejskich dostawców oprogramowania. Standaryzacja protokołu interoperacyjności OCM (*Open Cloud Mesh*), obecnie w ramach IETF (*Internet Engineering Task Force*), umożliwia wykorzystanie usług *file sync & share* jako kluczowej zdolności federacyjnej dla EOSC. OCM umożliwia również integrację platform wykraczających poza usługi *sync & share* i źródeł danych dla platform obliczeniowych.

Perspektywa polska i szanse na przyszłość

Polska jest państwem członkowskim CERN od 1991 r. CERN zobowiązany jest do współpracy przynoszącej zwrot z inwestycji oraz zwiększającej wartość społeczną i ekonomiczną dla państw członkowskich. Jako państwo członkowskie Polska ma możliwość korzystania ze współpracy z CERN w obszarach wykraczających poza współpracę ściśle naukową i udział w eksperymentach: edukacji, zwrotu przemysłowego oraz współpracy technologicznej. Setki polskich studentów i młodych specjalistów IT uczestniczyły do tej pory w programach szkoleniowych CERN, a polskie firmy dostarczają znaczące ilości sprzętu pamięci masowej i obliczeniowego do centrum danych CERN. CERN będzie nadal rozwijał technologie informatyczne co najmniej do lat 40. XXI w. w ramach programu HL-LHC. Dalsze wykorzystanie możliwości współpracy technologicznej i rozwoju kapitału ludzkiego we współpracy z CERN powinno być częścią szerszej strategii wykorzystania rosnącej międzynarodowej pozycji Polski.

Przedstawiony przypadek przechowywania i zarządzania danymi w Big Science jest przykładem wyspecjalizowanym, ale istotnym. Jest to jeden z obszarów IT, w którym społeczność badawcza może nadal odgrywać wiodącą rolę w krajobrazie zdominowanym przez duży przemysł informatyczny. Polskie instytucje są aktywnie zaangażowane w ten obszar: Centrum Informatyczne Świerk (CIŚ) w Narodowym Centrum Badań Jądrowych (NCBJ) uzyskało oficjalny status Tier 1 w WLCG, a polskie instytucje akademickie, takie jak ACK Cyfronet AGH i PCSS, są aktywnymi uczestnikami i współorganizatorami działań CS3. Obecnie prowadzone są dyskusje mające na celu zademonstrowanie interoperacyjności innych typów usług, w tym Polskiego Węzła EOSC oraz platform programowych rozwijanych w polskim środowisku akademickim. Jest to osadzone w szerszym kontekście działalności tych instytucji, które realizują programy krajowe, a jednocześnie są częścią europejskich inicjatyw w zakresie HPC, takich jak Fabryki AI, oraz otwartej nauki, takich jak EOSC.

Zaproponowana przez Polskie Towarzystwo Informatyczne dyskusja o przyszłości tej dziedziny powinna uwzględniać fakt, że rola, widoczność i pozycja Polski w Europie w ostatnich latach szybko rosną, także w organizacjach międzynarodowych takich jak CERN.

Od początku lat dwutysięcznych wielu polskich specjalistów rozwinęło kariery w cenionych instytucjach poza granicami kraju, często na ważnych stanowiskach specjalistycznych, menedżerskich lub doradczych na styku przemysłu, nauki, badań rozwojowych, biznesu i polityki. Są to osoby doskonale znające realia i uwarunkowania obecnej przestrzeni działań międzynarodowych, w której funkcjonują polskie instytucje publiczne i firmy prywatne. Połączenie tego doświadczenia stwarza szansę na zdefiniowanie świeżej i obiektywnej perspektywy możliwości rozwojowych dla Polski w kontekście czwartej rewolucji przemysłowej, a także identyfikację przeszkód i barier zarówno w kraju, jak i w przestrzeni międzynarodowej.

> *Polskie Towarzystwo Informatyczne mogłoby odegrać rolę katalizatora poprzez stworzenie grupy konsultingowej lub think tanku w celu identyfikacji szans i zagrożeń oraz obiektywnej ewaluacji istniejących barier rozwojowych w Polsce w obszarze informatyki i nowych technologii, a także uzyskania realnego wpływu na ich usuwanie i tworzenie nowych możliwości rozwojowych dla kraju.*

Trudno nie zgodzić się z publicznymi deklaracjami Ministerstwa Funduszy i Polityki Regionalnej, które twierdzi, że największym mankamentem w Polsce pozostaje ciągle niedoinwestowany obszar badań i rozwoju oraz skuteczne przekuwanie badań naukowych w gotowe, innowacyjne rozwiązania i produkty.

Czy niezbędne do tego jest zrealizowanie w Polsce projektu typu Big Science? A może powinniśmy zacząć od pełnego wykorzystania szans w ramach istniejących powiązań polskich instytucji naukowych z organizacjami tworzącymi technologie (takimi jak CERN) oraz potencjału kapitału ludzkiego, rozproszonego w europejskich organizacjach?

Obliczenia kwantowe w Polsce: stan i perspektywy

Katarzyna Rycerz, Mariusz Sterzel, Justyna Zawalska, Marian Bubak

Polska informatyka wchodzi w obecną fazę kwantowej rewolucji pełną parą – bierzemy udział w uruchamianiu urządzeń kwantowych w ramach europejskich projektów, a w polskich uczelniach działają grupy badawcze w dziedzinie informatyki kwantowej.



Katarzyna Rycerz

stopień doktora informatyki uzyskała na Uniwersytecie UVA w Amsterdamie w 2006 r. Obecnie pracuje jako adiunkt w Instytucie Informatyki oraz w ACK Cyfronet AGH w Krakowie. Jest współautorką ponad 50 międzynarodowych publikacji z zakresu obliczeń rozproszonych, środowisk do symulacji wieloskalowych, symulacji obliczeń kwantowych i wsparcia aplikacji naukowych. Brała udział w unijnych projektach ICT: CrossGrid (jako członek Zespołu Architektury), CoreGRID i MAPPER (jako lider WP) oraz projekcie EuroHPC PL pod patronatem EuroHPC JU (jako lider zadania). Do jej zainteresowań należy wykorzystanie algorytmów kwantowych do rozwiązywania problemów optymalizacyjnych pojawiających się w HPC i chmurach. Interesuje się także grami kwantowymi.

Mariusz Sterzel

doktor nauk chemicznych, specjalista HPC, jest przedstawicielem Polski w Radzie EuroHPC JU. Kierownik aktywności ACK Cyfronet AGH w projektach AARC2, Sat4Envi, EuroHPC PL. Członek Rady TCS Anthropogenic Hazard w EPOS ERIC. Koordynator aktywności Polskiego Centrum Kompetencji EuroHPC w projekcie EuroCC. Po odbyciu staży zagranicznych w Wielkiej Brytanii i Stanach Zjednoczonych rozpoczął pracę w Cyfronecie przy serii projektów Enabling Grids for E-SciencE, w których koordynował Klaster Chemii Obliczeniowej w projektach EGEE II i EGEE III. Brał udział w tworzeniu infrastruktury PLGrid i koordynował tam prace polegające na ujednoliceniu dostępu do oprogramowania naukowego. Pracuje w ACK Cyfronet AGH na stanowisku kierownika Działu Laboratorium Obliczeń Kwantowych. Główne kierunki aktywności Laboratorium to rozwiązywanie problemów optymalizacyjnych i obliczenia kwantowe struktury elektronowej molekuł.

Justyna Zawalska

tytuł mgr informatyki uzyskała w Akademii Górniczo-Hutniczej w Krakowie. Obecnie pracuje w ACK Cyfronet AGH i jest doktorantką na Akademii Górniczo-Hutniczej. W 2023 r. odbyła staż badawczy na Uniwersytecie Ludwika i Maksymiliana w Monachium (LMU). Specjalizuje się w rozwiązywaniu problemów optymalizacji kombinatorycznej za pomocą hybrydowych algorytmów kwantowo-klasycznych. Jej zainteresowania obejmują zastosowanie tych algorytmów w obszarze obliczeń wysokiej wydajności, zwłaszcza w problemach szeregowania zadań i równoważenia obciążenia, w celu zwiększenia wydajności obliczeniowej i poprawy efektywności energetycznej.

Marian Bubak

tytuł mgr inż. z fizyki technicznej i doktorat w dziedzinie informatyki uzyskał w AGH w Krakowie, gdzie przez wiele lat był adiunktem w Instytucie Informatyki. Nadal współpracuje z AGH, prowadząc wykłady z algorytmów równoległych, informatyki kwantowej i seminarium informatyki kwantowej KQIS. W latach 2000–2004 dziekan i organizator Wydziału Informatyki WSZiB w Krakowie, zaś w latach 2006-2016 *Professor of Distributed Systems Engineering* w *Informatics Institute, University of Amsterdam*. Od 1997 r. pracownik ACK Cyfronet AGH. Obecnie jest dyrektorem ds. naukowych Sano Centre for Computational Medicine w Krakowie. Wiceprezes PTI ds. naukowych, https://pti.org.pl/zarzad-glowny/marian-bubak/

Idea obliczeń kwantowych została po raz pierwszy przedstawiona przez Richarda Feynmana na konferencji „Physics and Computation" w MIT w 1981 r. jako odpowiedź na problem, że występujące w naturze i tworzone przez człowieka systemy kwantowe nie mogą być w pełni badane za pomocą symulacji na komputerach cyfrowych. W 1985 r. David Deutsch przedstawił pierwszy algorytm kwantowy i pokazał, że będzie on wykonywany szybciej niż jego odpowiednik klasyczny, zaś 9 lat później Peter Shor opublikował algorytm faktoryzacji liczb w czasie wielomianowym, co spowodowało znaczący wzrost zainteresowania obliczeniami kwantowymi.

Dlaczego obliczenia kwantowe?

Trzy główne własności, z których wynika przekonanie o sile obliczeń kwantowych[1]:

- równoległość kwantowa: nie operujemy na pojedynczych bitach, lecz na superpozycji kubitów dzięki czemu wszystkie możliwe dane są przetwarzane równocześnie;
- kubity są elementami przestrzeni Hilberta, której wymiar jest znacznie (eksponencjalnie) większy niż przestrzeni używanej do opisania bitów, a to daje możliwość przetwarzania dużo większej liczby danych;
- kubity mogą być splątane, wykazując korelacje niespotykane w świecie klasycznym.

Warto zauważyć, że systemy fizyczne, na których wykonywane są obliczenia kwantowe, są urządzeniami analogowymi, a zachodzące w nich procesy są złożone i stąd można spotkać się z oporem wielu osób przed nazywaniem ich komputerami.

Kubity są niemożliwymi do podejrzenia obiektami kwantowymi, a to oznacza, że uzyskanie wyniku przetwarzania przez pomiar daje nam tylko część informacji; nie możemy podejrzeć wszystkich odpowiedzi równocześnie, pomimo, że zostały już obliczone wewnątrz urządzenia kwantowego. Z tego też powodu projektowanie i implementowanie algorytmów kwantowych to nie lada sztuka!

Kolejne ograniczenia wynikają z samej budowy urządzeń kwantowych. Na przykład algorytm Shora, choć teoretycznie poprawny, w obecnych warunkach nie może zostać uruchomiony na istniejących urządzeniach dla rzeczywistych zastosowań ze względu na wymóg użycia kilkukrotnie większej liczby kubitów niż faktyczna liczba bitów potrzebna do kodowania kluczy RSA. Ograniczeniem jest również głębokość samego obwodu kwantowego, w teorii wielomianowa, w praktyce wciąż zbyt duża dla realnych rozwiązań sprzętowych.

Jednym z istotnych problemów w budowie urządzeń kwantowych jest utrzymanie tzw. koherencji. Kubity działają poprawnie jeśli są izolowane od otoczenia, zaś interakcja z otoczeniem prowadzi do dekoherencji: właściwa odpowiedź zostaje zaszumiona i ginie wśród błędnych wyników. Izolacja kubitu jest trudna do uzyskania, gdyż obliczenie wymaga działania na nim. Im więcej operacji, tym większy szum. Dostępne obecnie urządzenia są nazywane „kwantowymi urządzeniami średniej skali z szumem" (*Noisy Intermediate-Scale Quantum – NISQ*).

Obecnie trwa dyskusja, do jakich zastosowań urządzenia kwantowe mogą okazać się najbardziej użyteczne. Ze względu na wspomniane wymagania sprzętowe, raczej nie będą to algorytmy typu algorytm Shora, pomimo że to właśnie on początkowo stanowił siłę napędową rozwoju tematyki obliczeń kwantowych. Wśród rokujących zastosowań wymienia się optymalizację w logistyce, finansach czy medycynie, kwantowe uczenie maszynowe (QML), badanie własności cząsteczek, symulacje złożonych układów fizycznych, zwłaszcza silnie skorelowanych. Tematy te przewijają się podczas licznych konferencji i warsztatów naukowych, takich jak Quantum Computing Workshop (QCW) w ramach International Conference on Computational Science (ICCS) (https://www.iccs-meeting.org/iccs2026/).

Główni gracze

Wśród licznych firm rozwijających sprzęt, oprogramowanie i aplikacje kwantowe istotne miejsca zajmują IBM (urządzenia działające w modelu bramkowym) oraz D-Wave Systems (wyżarzacze kwantowe). Firmy te bardzo wcześnie dały szerokiemu gronu użytkowników dostęp do swoich urządzeń, co wraz z udostępnieniem oprogramowania umożliwiło eksperymenty i przyniosło ogólne przeświadczenie, że temat nie jest czysto abstrakcyjny. Ten ruch pokazał praktyczną stronę technologii i – mimo początkowych niedoskonałości – sprzyjał samoorganizowaniu się społeczności. Inni ważni gracze, tacy jak Google, Rigetti Computing, IonQ, Quantinuum czy Xanadu również udostępniają publicznie symulatory i oprogramowanie, ale rezerwują sprzęt

1 Nielsen, M.A. and Chuang, I.L.: *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2001

dla wybranych partnerów. Firmy europejskie to przede wszystkim francuskie Pascal oraz Quandela, niemiecka attocube, austriacka Alpine Quantum Systems (AQT), fińska IQM Quantum Computers, hiszpańska Qilimanjaro Quantum Tech oraz brytyjska Orca Computing.

Polski udział

Polska informatyka uczestniczy zarówno w opracowywaniu algorytmów kwantowych, jak i w udostępnianiu urządzeń do obliczeń kwantowych. W większości znaczących polskich uczelni działają grupy badawcze w dziedzinie informatyki kwantowej, prowadzone są seminaria, wykłady i ćwiczenia laboratoryjne. Warto wspomnieć o pracach magisterskich z tej dziedziny nagradzanych w kilku edycjach Konkursu Prac Magisterskich PTI (https://kpm.pti.org.pl/).

Udostępnianie urządzeń kwantowych obejmuje udział w europejskich projektach zakupu i adaptacji systemów typu NISQ do istniejących infrastruktur superkomputerowych typu High Performance Computing (HPC), pozyskiwanie własnych urządzeń NISQ, tworzenie oprogramowania *quantum ready* oraz ambitne próby budowy własnych procesorów kwantowych od podstaw.

Zakup urządzeń kwantowych

W Europie do tej pory zakupiono – w ramach partnerstwa *European High Performance Computing Joint Undertaking* (EuroHPC JU) – sześć komputerów kwantowych (https://www.eurohpc-ju.europa.eu/index_en; https://www.eurohpc-ju.europa.eu/eurohpc-quantum-computers/our-quantum-computers_en). Polskie instytucje biorą udział w dwóch takich inicjatywach: LUMI-Q oraz EuroQCS-Poland.

Konsorcjum **LUMI-Q** jest koordynowane przez VSB – Uniwersytet Techniczny w Ostrawie oraz Narodowe Centrum Superkomputerowe IT4Innovations w Czechach. Obejmuje ono instytucje z dziewięciu krajów europejskich: Czech, Polski (ACK Cyfronet AGH), Finlandii, Belgii, Danii, Niemiec, Holandii, Norwegii i Szwecji. Działania konsorcjum doprowadziły do uruchomienia we wrześniu 2025 r. urządzenia kwantowego VLQ w Ostrawie. Jest to 24-kubitowy, bazujący na nadprzewodnikach system o topologii gwiazdy, wyprodukowany przez firmę IQM Quantum Computers (https://meetiqm.com/products/). VLQ został zintegrowany z superkomputerem Karolina. Planowane jest jego połączenie z superkomputerem LUMI oraz z innymi maszynami infrastruktury EuroHPC, w tym z polskim superkomputerem Helios w ACK Cyfronet AGH. Uruchamiane są na nim aplikacje kwantowe w obszarach: AI, chemii kwantowej, optymalizacji i bezpieczeństwa. Projekt finansują (7 mln euro) po połowie EuroHPC JU i kraje członkowskie.

Konsorcjum **EuroQCS-Poland** jest koordynowane przez Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS). W jego skład wchodzą także Centrum Fizyki Teoretycznej PAN i Creotech Instruments S.A. oraz Uniwersytet Łotewski. Działania konsorcjum doprowadziły do uruchomienia w czerwcu 2025 r. 20-kubitowego urządzenia kwantowego PIAST-Q w Poznaniu – systemu bazującego na pułapkach jonowych z obsługą łączności pomiędzy kubitami typu „wszystko-do-wszystkiego". Maszynę dostarczył **Alpine Quantum Systems (AQT)** (https://www.aqt.eu/) z Innsbrucku. Urządzenie zostanie zintegrowane z superkomputerem Altair i PIAST-AI. Projekt, finansowany kwotą 15,5 mln euro, wspiera aplikacje kwantowe w optymalizacji, chemii kwantowej, naukach o materiałach i uczeniu maszynowym.

W PCSS zainstalowano również urządzenie kwantowe wykorzystujące systemy fotoniczne. Służy ono do specjalistycznych zastosowań w optymalizacji i uczeniu maszynowym, wspierając hybrydowe algorytmy klasyczno-kwantowe. Stosuje model obliczeniowy bazujący na próbkowaniu bozonów. Maszynę dostarczyła brytyjska firma **ORCA Computing** (https://orcacomputing.com), instalacja zakończyła się w kwietniu 2024 r. Można więc uznać, że była to pierwsza pełna instalacja urządzenia kwantowego w Polsce, choć przeznaczonego do wąskich zastosowań specjalistycznych.

Wrocławskie Centrum Sieciowo-Superkomputerowe (WCSS) na Politechnice Wrocławskiej uruchomiło w maju 2025 r. komputer kwantowy Odra 5 – pierwszy w Polsce wykorzystujący nadprzewodzące kubity w niskiej temperaturze. Odra 5 to 5-kubitowy system IQM Spark, dostarczony – podobnie jak w LUMI-Q – przez IQM Quantum Computers.

Sprzęt od podstaw

W ramach projektu MIKOK, finansowanego ze środków Narodowego Centrum Badań i Rozwoju, powstała inicjatywa realizacji prototypu urządzenia kwantowego bazującego na pułapkach jonowych. W projekt zaangażowane są: Wojskowa Akademia Techniczna, Wojskowy Instytut Techniczny Uzbrojenia, Politechnika Śląska oraz firma SONOVERO R&D. Liderem przedsięwzięcia jest Politechnika Warszawska.

Quantum ready software

W ramach współpracy instytucji naukowych z firmami powstaje również oprogramowanie. Ze względu na niedoskonałość istniejących urządzeń kwantowych, rozwiązania te są budowane przy założeniu, że część ich funkcjonalności może zostać w przyszłości zastąpiona po pojawieniu się udoskonalonych wersji tych urządzeń. Naukowcy Instytutu Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk (IITiS PAN) w ramach startupu Quantumz.io wypuścili na rynek serię zaawansowanych solverów VeloxQ[2] do optymalizacji kombinatorycznej. Innym przykładem jest zestaw narzędzi opracowanych w ACK Cyfronet AGH w ramach projektu EuroHPC-PL. Narzędzie QHyper[3] oferuje ujednoliconą i niezależną od konkretnych solverów reprezentację problemów optymalizacji kombinatorycznej przy stosunkowo małym narzucie wydajnościowym. Modułowa architektura udostępnia ujednolicony interfejs dla solverów bazujących na bramkach, wyżarzaniu kwantowym oraz dla referencyjnych rozwiązań klasycznych. Przykłady zastosowań to rozwiązywanie problemu wykrywania społeczności z zakresu neuronauki we współpracy z Sano Centre for Computational Medicine czy też przydzielanie zasobów do zadań składających się na aplikacje naukowe we współpracy z Wydziałem Informatyki AGH.

Z kolei platforma AQMLator[4] wspiera kwantowe uczenie maszynowe. Automatycznie proponuje i trenuje warstwy kwantowe modeli ML przy minimalnym udziale użytkownika; pozwala naukowcom zajmującym się analizą danych ominąć barierę wejścia dla obliczeń kwantowych. Platforma wykorzystuje standardowe biblioteki, co ułatwia wprowadzenie do istniejących potoków ML.

Głównym celem tej strategii jest zapewnienie Europie do 2030 r. pozycji światowego lidera w dziedzinie technologii kwantowych. Strategia jest całościowa – koncentruje się na pięciu obszarach działania: badania i innowacje, infrastruktury kwantowe, wzmocnienie unijnego ekosystemu kwantowego, kosmiczne i kwantowe technologie podwójnego zastosowania (bezpieczeństwo i obrona), umiejętności kwantowe. Z całą pewnością pomocnymi w tej drodze będą służące wymianie doświadczeń między instytucjami otwarte seminaria Krakow Quantum Informatics Seminar i Fundacji Quantum AI (https://www.informatyka.agh.edu.pl/en/kqi-seminars/; https://www.qaif.org/). Istotna też będzie kontynuacja popularyzacji wiedzy o informatyce kwantowej prowadzona przez tę fundację ze wsparciem PTI.

Atmosferę tajemnic handlowych, swoistego „wyścigu kwantowych zbrojeń", niepewności „co zrobili inni" między dużymi graczami, zarówno geopolitycznymi, jak i biznesowymi, daje się oczywiście odczuć również w świecie naukowym.

Co dalej?

Tak naprawdę nikt nie wie, jak zakończy się obecna próba rewolucji kwantowej w obliczeniach. Z jednej strony fakt zaangażowania wielkich graczy i zainteresowanie grup naukowych na świecie daje nadzieję na postęp. Oprócz rozwoju algorytmów obliczeń kwantowych, oprogramowania i budowy sprzętu prowadzone są prace w kryptografii kwantowej nad rozwojem nowych kryptosystemów odpornych na komputery kwantowe.

> ***Swego rodzaju drogowskazem dla europejskiej i polskiej informatyki kwantowej jest strategia unijna „Quantum Europe Strategy" (https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy), przyjęta przez Komisję Europejską w lipcu 2025 r.***

Trzeba pamiętać, że nikt dotychczas nie odkrył fundamentalnych praw fizyki pokazujących, że budowa komputerów kwantowych jest niemożliwa. Niemniej jednak cała społeczność naukowa jest świadoma ograniczeń istniejących urządzeń typu NISQ i ich wrażliwości na sygnały z otoczenia. Dlatego nikt z całą pewnością nie jest w stanie odpowiedzieć na pytanie o przyszłość. Czy czeka nas zima kwantowa, podobnie jak w przeszłości zima sztucznej inteligencji? Czy wiele lat potem nadejdzie kolejna wiosna? A może przełom jest tuż za rogiem? Ten, który umiałby odpowiedzieć, zapewne znałby odpowiedzi na wiele innych pytań dręczących ludzkość. Jako naukowcy nie powinniśmy jednak ustawać w próbach odpowiedzi.

Podziękowania

Dziękujemy Karolowi Capale z Wydziału Informatyki i ACK Cyfronet AGH w Krakowie za liczne dyskusje.

2 Tuziemski, J., Tarasiuk, P., Przybysz, A., Adamski, R., Hendzel, K., Pawela, Ł. i in. (2025). *VeloxQ: A fast and efficient QUBO solver*, https://arxiv.org/abs/2501.19221

3 Lamża, T., Zawalska, J., Jurek, K., Sterzel, M., Rycerz, K.: *Facilitating usage of quantum–classical optimization software with QHyper library, Information and Software Technology,* Volume 188, 2025, 107861, ISSN 0950-5849, https://doi.org/10.1016/j.infsof.2025.107861.

4 Rybotycki, T.,Gawron, P.: *AQMLator – An Auto Quantum Machine Learning E-Platform*, 2024, https://arxiv.org/abs/2409.18338

Cyberbezpieczeństwo: ufaj, ale sprawdzaj

Mirosław Kutyłowski

Bezpieczeństwo systemów i urządzeń IT zależy nie tylko od wykorzystanych technologii ochrony – zasadniczą kwestią w budowie systemu uzasadnionego zaufania jest możliwość sprawdzenia realnego poziomu bezpieczeństwa. Z punktu widzenia użytkownika końcowego uzasadniony poziom zaufania jest tym wyższy, im głębiej on sam może je zweryfikować w posiadanym produkcie.



Mirosław Kutyłowski

kierownik Zakładu Kryptologii w NASK – Państwowym Instytucie Badawczym. Przez ponad 20 lat był związany z Politechniką Wrocławską, założyciel Katedry Podstaw Informatyki i badań z zakresu kryptografii na tej uczelni. Dwukrotnie członek Centralnej Komisji ds. Stopni i Tytułów, członek Komitetu Informatyki PAN. W latach 1980–2000 pracował na Uniwersytecie Wrocławskim (gdzie otrzymał wszystkie stopnie naukowe). Był stypendystą Humboldta na Uniwersytecie Technicznym w Darmstadt oraz docentem w Instytucie Heinza Nixdorfa na Uniwersytecie Paderborn. Profesor wizytujący na Uniwersytecie Xidian.

Zajmuje się głównie tematyką wrogiej kryptografii, obroną przed słabymi punktami technologii kryptograficznych oraz rozwiązaniami implementowanymi na elektronicznych dokumentach tożsamości.

Podczas wprowadzania produktów i systemów informatycznych powszechną tendencją jest koncentracja uwagi na jak najszerszych i jak najbardziej wygodnych funkcjonalnościach oraz na szybkości ich wprowadzenia na rynek lub uruchomienia. Zjawisko to występuje zarówno w obszarze rozwiązań oferowanych w obrocie prywatnym (minimalizacja okresu *time-to-market* i wykorzystanie niszy rynkowej przed konkurencją przy jak największej atrakcyjności dla klienta), jak i w obszarze administracji publicznej, gdzie wygoda dla wyborcy jest celem kluczowym. Jest to sytuacja krańcowo różna od sytuacji na rynku farmaceutycznym: wprowadzanie produktu poprzedzone jest tam wieloletnimi dogłębnymi badaniami określającymi poziom bezpieczeństwa i skutki uboczne. Mimo pewnych negatywnych skutków (większe koszty wprowadzania nowych specyfików na rynek) ma to głębokie uzasadnienie udokumentowane bolesnymi przykładami z przeszłości.

Na przeszkodzie zachowania ostrożności we wprowadzaniu nowych produktów i systemów teleinformatycznych stoi również samo podejście użytkowników końcowych – fascynacja nowymi możliwościami jest zwykle mocniejsza od obaw w zakresie bezpieczeństwa. Psychologicznie kuszące jest zbagatelizowanie zagrożeń i zaufanie dostawcy, szczególnie gdy brak jest wygodnych alternatyw.

Czarne skrzynki

Możliwości inspekcji rozwiązań informatycznych przez użytkownika końcowego są bardzo ograniczone, choć sytuacja w krajach Unii i tak jest istotnie lepsza niż poza Unią. Ograniczenia wynikają z ochrony praw własności intelektualnej i zabraniają, poza kilkoma przypadkami, inżynierii wstecznej produktu.

> ***W przypadku braku przesłanek związanych z zapewnieniem kompatybilności, usunięciem błędów lub zagwarantowaniem prawidłowego funkcjonowania programu zgodnie z jego uprawnionymi celami, inżynieria wsteczna jest nielegalna.***

Dopuszczone jest jedynie obserwowanie działania produktu w ramach normalnego użytkowania dopuszczonego umową licencyjną. W tak określonych ramach prawnych oznacza to, że o ile inspekcja nie jest *explicite* dopuszczona przez umowę licencyjną, a produkt działa poprawnie, to z punktu widzenia użytkownika ma on charakter czarnej skrzynki.

Model czarnej skrzynki, zwłaszcza gdy istnieją techniczne, a nie tylko prawne zabezpieczenia przed ingerencją w produkt, ma niewątpliwe zalety. Ogranicza możliwość dokonywania modyfikacji, a w szczególności ingerowania w jego zabezpieczenia. Jasne i rozgraniczone są zasady odpowiedzialności. Jest to jednak miecz obosieczny: brak możliwości inspekcji produktu stwarza pokusy dla dostawców nie tylko do wbudowywania nieudokumentowanych funkcji, ukrytych możliwości dostępu itp., lecz także do optymalizacji kosztów poprzez rezygnację z implementacji bardziej skomplikowanych lub kosztownych zabezpieczeń. Problem ten jest szczególnie istotny w przypadku produktów i dostawców o krótkim okresie obecności na rynku – przestają w tym momencie działać argumenty wskazujące na konieczność zachowania reputacji. Nie sposób też zignorować możliwość presji na producenta ze strony organów publicznych kraju pochodzenia podyktowanej względami „bezpieczeństwa publicznego". Bezpieczeństwo to może być rozumiane wąsko jako interes bezpieczeństwa kraju pochodzenia.

Trudność inspekcji

Klasycznym i dominującym podejściem wspierającym zaufanie do produktów informatycznych są procedury inspekcji produktu, często warunkujące dopuszczenie do obrotu lub uruchomienie systemu. W tym celu budowane są coraz bardziej zaawansowane automatyczne metody inspekcji wykrywające wrogie oprogramowanie i podatności na ataki. Bazują one na wykrywaniu wadliwych lub tylko podejrzanych elementów kodu, mogących być źródłem problemów bezpieczeństwa. Należy jednak mieć świadomość, że są to jedynie mechanizmy ograniczające skalę problemów, ale nie eliminujące je całkowicie. Nie tylko mechanizmy detekcji podlegają ciągłemu doskonaleniu – postęp dotyczy również metod ukrywania wrogiego oprogramowania w niewinnie wyglądającym kodzie. Trwa więc swoisty wyścig zbrojeń, w którym metody detekcji niekoniecznie są górą.

Wykrywanie podatności poprzez identyfikowanie określonych cech lub wzorców kodu ma swoje ograniczenia. Przykładowo metoda ta nie wykrywa zagrożeń w produktach, których podatności nie wynikają z obecności wrogiego lub szkodliwego oprogramowania, lecz są konsekwencją błędnego zaprojektowania całego systemu. Niebezpieczeństwo może również tkwić w niewłaściwym wykorzystaniu produktu: produkt X dla zastosowania A może być akceptowalny ze względu na znikome występujące tam ryzyka. Zmiana obszaru na zastosowanie B może jednak istotnie zmienić sytuację – ryzyka mogą stać się krytyczne.

Common Criteria – blaski i cienie

Trudności z oceną adekwatności zabezpieczeń określonego produktu dla konkretnego zastosowania są zasadniczym powodem powstania metodologii Common Criteria (CC). Klienci często nie mają odpowiednich specjalistycznych kompetencji do oceny bezpieczeństwa. Trudność porównania produktów wynika też z odmiennego sposobu prowadzenia dokumentacji bezpieczeństwa lub wręcz braku określonych istotnych informacji. Common Criteria – poprzez narzucenie metodologii skoncentrowanej wokół chronionych wartości, zagrożeń i odpowiadających im wymagań – pozwala nie tylko na zaadresowanie wszystkich istotnych zagrożeń, lecz także ułatwia odkrycie i rezygnację z nadmiarowych mechanizmów.

Niestety, proces certyfikacji według Common Criteria jest żmudny i kosztowny. O ile użycie tej metodologii sprawdza się w odniesieniu do odseparowanych i relatywnie niewielkich produktów, zastosowanie CC do systemów o dużym stopniu złożoności wydaje się zadaniem beznadziejnym. Stopień złożoności rośnie bowiem niezwykle szybko wraz ze wzrostem złożoności systemu. Należy zauważyć, że zakres stosowalności Common Criteria można rozszerzyć poprzez odpowiednią architekturę systemu i składanie go z komponentów.

Skuteczność certyfikacji Common Criteria zależy w krytyczny sposób od właściwego zidentyfikowania chronionych wartości oraz odpowiadających im zagrożeń. Błędy popełnione na tym etapie mają szczególnie poważne konsekwencje, ponieważ opinia klienta budowana na podstawie certyfikatu CC może dawać złudne poczucie bezpieczeństwa. W rezultacie certyfikat może uśpić czujność zarówno decydentów, jak i użytkowników.

Koncepcja E2E

Odmienna koncepcja powstała w trakcie budowy systemów *e-votingu*. W tym przypadku budowanie zaufania z wykorzystaniem instytucji certyfikujących jest niemożliwe. Powodem jest duży stopień zależności organów certyfikacyjnych od organów administracji państwowej, czyli pośrednio od osób ubiegających się o elekcję. Kolejnym problemem jest groźba współpracy dostawców produktów do *e-votingu* z laboratoriami certyfikującymi pod naciskiem grup usiłujących zdobyć w ten sposób władzę.

Wyjściem z tej sytuacji jest budowa systemów bazujących na koncepcji bezpieczeństwa E2E (*end-to-end*). W podejściu tym żaden aktor systemu (wliczając w to organy certyfikujące i samych użytkowników) nie jest uznawany za godnego zaufania. Kluczową rolę odgrywa weryfikowalność – niezależnie od tego, w jaki sposób zachowają się aktorzy i komponenty systemu (w tym odbiegający od wysokopoziomowej specyfikacji), możliwa jest weryfikacja, czy jakieś złośliwe zachowanie miało miejsce. Weryfikowalność może mieć charakter publiczny lub lokalny. W pierwszym przypadku weryfikacja bazuje na upublicznionych danych. W drugim – aktorzy systemu mają możliwość indywidualnej weryfikacji, posługując się szczególnymi prywatnymi danymi. W przypadku *e-votingu* dotyczyć to może sprawdzenia, „czy mój głos został poprawnie zaliczony".

Bezpieczeństwo kontra wykrywalność

Kluczową zmianą koncepcji zapewnienia bezpieczeństwa wynikającą z prac nad *e-votingiem* jest skoncentrowanie się na wykrywaniu nieprawidłowości zamiast na usiłowaniu budowy stuprocentowo bezpiecznych produktów. Okazuje się, że do pewnego stopnia możliwe jest zaprojektowanie wysokopoziomowych funkcjonalności odpowiadających za weryfikację zachowania systemu, skutecznych bez względu na sposób implementacji systemu na niższych warstwach.

Wykrywalność niepożądanych działań może okazać się wystarczająca. Jest to sytuacja analogiczna do zwalczania przestępczości poza cyberprzestrzenią: podczas gdy nie można zapewnić, by żaden członek społeczeństwa nie był skłonny do popełnienia przestępstwa (na przykład przez perswazje czy działania edukacyjne), pełna wykrywalność sprawców lub też sama groźba wykrycia jest wystarczająca do sprowadzenia przestępczości do zaniedbywalnego poziomu. Cyberprzestępczość w przeważającej liczbie przypadków ukierunkowana jest na osiągnięcie określonych korzyści, więc wykrywalność sprawców bywa wystarczająca dla wyeliminowania szeregu zjawisk. Na przykład, łamanie kluczy do weryfikacji podpisu elektronicznego w celu wydobycia klucza prywatnego nie ma sensu, o ile istnieją niezależne metody pozwalające na odsianie podpisów wygenerowanych za pomocą tak zdobytego klucza od podpisów wygenerowanych przez prawdziwego właściciela klucza.

Dane pod kontrolą

Jednym z obszarów, gdzie alternatywne podejście do budowy bezpiecznych systemów może pozwolić na realny postęp, jest kwestia „kontrolowalności" użycia danych.

Kwestia nieuprawnionego użycia danych jest centralnym zagadnieniem ochrony danych osobowych. Rozporządzenie RODO i wcześniejsze regulacje w tym względzie nakładają obowiązek przetwarzania danych osobowych wyłącznie w uprawnionych okolicznościach i w sposób zapewniający bezpieczeństwo techniczne. Nieprzestrzeganie tych zasad skutkuje sankcjami, jednak beneficjentem kar administracyjnych nie jest ofiara nieuprawnionego przetwarzania, tylko Skarb Państwa. Rozwiązanie to nie gwarantuje usuwania naruszeń, o ile dokonują je organy publiczne.

Inaczej do problemu podchodzi Rozporządzenie eIDAS w znowelizowanej wersji. Jednym z naczelnych zadań europejskiego portfela tożsamości jest zapewnienie kontroli nad użyciem danych. Bez względu na to, w jakim stopniu zostanie to zrealizowane (przynajmniej w początkowym okresie), jesteśmy świadkami zmiany podejścia. Podmiot danych osobowych ma otrzymać kontrolę nad tym, komu i jak są przekazywane jego dane. Tym samym ma się stać aktywnym aktorem nie tylko korzystającym z systemu, lecz także kontrolującym jego funkcjonowanie.

Plan B w zabezpieczeniach

Klasyczne mechanizmy ochrony, w szczególności techniki kryptograficzne, bazują na założeniu bezwzględnego bezpieczeństwa określonych elementów. Dotyczy to w szczególności ochrony kluczy prywatnych oraz generowania liczb losowych. Możliwości kontroli zabezpieczeń technicznych i jakości generatora w tym przypadku są ograniczone. Co więcej, nie dotyczy to tylko użytkownika końcowego. W tej sytuacji zaufanie do mechanizmów takich jak generowanie kluczy kryptograficznych czy kluczy efemerycznych powinno uwzględniać możliwość wadliwego działania tych mechanizmów. Rozwiązania takie istnieją, ale w niewystarczający sposób są wykorzystywane.

Niezbędne zaufanie *by design and default*

Prawo europejskie coraz powszechniej wprowadza wymagania dotyczące warunków bezpieczeństwa i ochrony danych oraz obowiązków dokumentowania działań w tym zakresie. Dotyczy to w szczególności najbardziej kluczowych obszarów dla bezpieczeństwa publicznego, ale wymagania stopniowo poszerzają swój zakres. Polityka ta ma głębokie uzasadnienie wobec istniejących zagrożeń zewnętrznych i wewnętrznych, jednak sukces w realizacji jest silnie uzależniony od końcowej praktyki. Po pierwsze, implementacja reguł może być powierzchowna i ograniczać się do realizacji procedur i tworzenia dokumentacji rzekomo adresującej wymagania, jednak luźno związanej ze stanem faktycznym lub, co gorsza, omijającej kluczowe luki bezpieczeństwa. Po drugie, powszechne podejście „najpierw zrealizuj produkt, potem zadbaj o bezpieczeństwo i zaufanie" może uniemożliwiać rzeczywiste zaadresowanie problemów. Decyzje projektowe mogą być nieodwracalne i realizacja wymagań wymagałaby wycofania określonego produktu. A należy zauważyć, że z przyczyn praktycznych wycofanie może nie być możliwe.

Regulacje europejskie wprowadzają paradygmaty *security by design and default* oraz *privacy by design and default* oraz obowiązek demonstrowalności praktyk w tym zakresie. Wydaje się jednak, że w wielu przypadkach niezbędne jest wprowadzenie paradygmatu *trust by design and default*, uwzględniającego możliwości weryfikacji przez wszystkich aktorów w systemie, tym samym ograniczając konieczność odwoływania się do zaufanych stron.

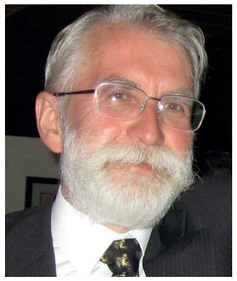
Realizowanie produktów i systemów w reżimie *trust by design and default* w końcowym rozrachunku prowadzi do oszczędności w kosztach audytu, certyfikacji i w kosztach operacyjnych. Czynności z zakresu cyberbezpieczeństwa przejmowane są częściowo przez użytkowników systemu i do pewnego stopnia niezależnie od ich kwalifikacji czy dbałości w tym obszarze.

Zaufanie może opierać się na nieuchronności wykrycia i udowodnienia nieuprawnionych działań czy luk w systemie. Najlepszym sposobem na powstrzymanie cyberprzestępczości nie jest budowanie systemów o najwyższym możliwie poziomie odporności (bo to po pierwsze się nie uda, a po drugie może być zbyt kosztowne), lecz odcięcie możliwości monetyzacji ataków.

Dostawcy wysokiego ryzyka

Jarosław Deminet

Wyobraźmy sobie bank, który zaprasza klientów do składania depozytów w swoim sejfie, ale z góry uprzedza, że właściwie nie bierze za nie odpowiedzialności, choć będzie się starał zapewnić bezpieczeństwo. Ale nigdy nie wiadomo, czy strażnicy nie są przekupieni, a zamek nie da się otworzyć agrafką. Więc depozytariusze powinni – na wszelki wypadek – dodatkowo zabezpieczać swoje skrytki łańcuchami i mikroładunkami wybuchowymi. I wyobraźmy sobie, że przechodząc przez most powinienem mieć ze sobą koło ratunkowe, bo projektant mógł być pijany, a huta mogła dostarczyć tandetną stal zbrojeniową.



Jarosław Deminet

informatyk od 1979 r., bywał nauczycielem akademickim, urzędnikiem, szefem działów produkujących oprogramowanie w korporacji, konsultantem biznesowym, publicystą. Członek założyciel PTI.

Co najmniej od 60 lat wiadomo, jak budować systemy informatyczne, żeby były bezpieczne. W każdym procesorze mamy nieprzenikalne przestrzenie adresowe poszczególnych procesów i różne poziomy bezpieczeństwa. Systemy operacyjne korzystają z tych mechanizmów, co powinno zapewnić pełne bezpieczeństwo pracy. Warstwowa budowa oprogramowania pozwala ograniczyć rozmiar najniższych, najbardziej krytycznych warstw, tak aby można było dokładnie sprawdzić ich kod i zabezpieczyć je przed ewentualną agresją ze strony innych, większych, ale mniej uprzywilejowanych programów. Kiedy 45 lat temu zajmowałem się oprogramowaniem systemów operacyjnych, wydawały mi się wyjątkowo bezpiecznymi produktami. Co więcej, powszechne było przekonanie, że bezpieczeństwo systemów bazuje na konkretnych rozwiązaniach technicznych, a nie na utrzymywaniu w tajemnicy ich kodu.

W nowoczesnej informatyce mamy trochę taką sytuację. Korzystamy z coraz potężniejszych komputerów i coraz szybszych sieci, budujemy systemy kwantowe, ale nie potrafimy zapewnić ich bezpieczeństwa. Trochę to dziwne.

Masowe pojawienie się wirusów w latach osiemdziesiątych XX w. zdawało się tymczasowym problemem wynikającym ze słabych możliwości ówczesnych procesorów i systemów operacyjnych w komputerach osobistych. Sytuacja zmieniła się na początku XXI w. i od tego czasu można było się spodziewać, że nasze systemy staną się bezpieczne. To, że tak nie jest, i że np. celowe i odpowiednio zaprojektowane przepełnienie stosu w jakimś programie potrafi doprowadzić do zablokowania komputera albo sformatowania dysku systemowego jest dla mnie wciąż niepojęte.

Złożoność kontra poprawność

Równocześnie rozmiar i złożoność oprogramowania rośnie w sposób trudny do wyobrażenia. Pięćdziesiąt lat temu złożoność systemu operacyjnego wynikała z algorytmów szeregowania procesów, zarządzania plikami czy stronicowania pamięci. Podejrzewam, że obecnie rozmiar tych algorytmów stanowi niewielki ułamek rozmiaru kodu potrzebnego do zarządzania okienkami na ekranie i generowania znaków o różnej wielkości na podstawie ich obwiedniowej definicji.

Oprogramowanie jest tworzone przez całe armie projektantów i programistów, którzy popełniają błędy, a czasem celowo zniekształcają działanie programów. Identyfikacja takich przypadków jest bardzo trudna. Czytanie i rozumienie cudzego kodu było i jest niesłychanie żmudne, niezależnie od stosowanych wzorców i dokumentacji. Każdy z nas potrafi opowiedzieć anegdoty o przypadkowym (lub celowym) użyciu tego samego słowa czy bitu do dwóch różnych celów, niezainicjowaniu zmiennej, zmianie działania wywoływanej procedury czy złych warunkach brzegowych („*off-by--one*"). Można stosować systematyczną inspekcję kodu, ale jest ona bardzo prachochłonna i nie wiem, czy występuje w praktyce. Pewnym zabezpieczeniem jest publiczne udostępnienie kodu (open source), szczególnie z wykorzystaniem sztucznej inteligencji do weryfikacji. To trochę jak z kontrolą biletów w autobusach: nie sprawdzimy wszystkich, ale ktoś celowo psujący kod musi liczyć się z tym, że ryzykuje ujawnienie i karę (co najmniej wizerunkową). Firmy informatyczne jednak niezbyt chętnie ujawniają swój kod. To samo niestety dotyczy podmiotów publicznych – vide wieloletnie przegrane boje o udostępnienie kodu systemu ZUS czy „sądolotka". A Ministerstwo Cyfryzacji konsekwentnie głosi tezę, że to właśnie ujawnienie kodu systemów publicznych zagrażałoby ich bezpieczeństwu.

> *Postulat public money – public code jakoś się nie przebija do urzędników.*

Od co najmniej 60 lat trwają prace nad dowodzeniem poprawności programów. Zbudowano wielkie teorie, ale nie słyszałem o ich zastosowaniu do kompletnego komercyjnego systemu operacyjnego czy programu do edycji dokumentów. Trudno zresztą sobie wyobrazić pełną formalną specyfikację takiego programu.

Pozostaje testowanie, ale – jak stwierdził Edsger W. Dijkstra: „Testowanie programu może służyć do wykazania obecności pluskiew [błędów], ale nigdy do wykazania ich braku!". Wyobraźmy sobie głosowanie elektronicznie i system, który po naciśnięciu przez operatora przez 3 sekundy jednocześnie prawego klawisza Shift i lewego klawisza Ctrl dodaje dwa głosy kandydatowi pierwszemu w kolejności alfabetycznej. Akurat taką manipulację łatwo byłoby wychwycić w kodzie, ale primo – ktoś musiałby ten kod przeczytać, secundo – bardziej złożona kombinacja byłaby już mniej widoczna.

Na tym tle jawi się kwestia naszego zaufania (czy jego braku) do systemów informatycznych. W praktyce zakup i instalacja każdego systemu wiąże się z pewnym ryzykiem. Pół biedy, jeśli chodzi o domowy laptop, na którym piszemy teksty i oglądamy filmy. Jeśli regularnie archiwizujemy dane, to przeżyjemy nawet poważne awarie, a nawet ataki wymuszeniowe (ransomware). Zdaję sobie sprawę, że komercyjny edytor, z którego korzystam, zapewne ma błędy, ale – skoro używają go miliony ludzi – pewnie są to błędy w mało używanych fragmentach kodu. Mogą być kłopotliwe, ale nie katastrofalne. Mogę także podejrzewać, że edytor może sporadycznie przekazywać jakieś informacje o moich tekstach do jakiegoś zewnętrznego podmiotu. Jakoś się z tym pogodziłem.

Gorzej jest, jeśli sprawa dotyczy systemów istotnych dla bezpieczeństwa państwa czy poszczególnych ludzi, takich jak serwery, komputery w instytucjach i ważnych urzędach, sterowniki w samolotach czy osprzęt sieciowy. Przez wiele lat przykładem największego zagrożenia były systemy sterujące elektrowniami atomowymi. Ich awaria (przypadkowa lub celowa), nie do skorygowania przez człowieka, prowadziłaby co najmniej do zniszczenia reaktora, a może i do większej katastrofy. Na szczęście na razie nigdy to się nie stało. Wszystko jednak wskazuje na to, że kilka katastrof lotniczych było skutkiem błędnego działania komputerów pokładowych. A szczególnie groźna byłaby sytuacja, w której ktoś z zewnątrz zaingerowałby w działanie systemu i na przykład zdalnie spowodował katastrofę samolotu. Przykłady są – wybuchające palestyńskie pagery i samouszkadzające się irańskie ultrawirówki.

Wprawdzie nie jesteśmy w stanie w 100% przetestować programu ani udowodnić jego poprawności, ale możemy próbować nadzorować proces wytwórczy – normy jakości, audyty itp. Niestety zawodzi to całkowicie, jeśli sam producent działa w złej wierze i celowo dostarcza produkt niezgodny ze specyfikacją (np. z modułami szpiegującymi użytkownika albo przyjmującymi nieautoryzowane polecenia z zewnątrz).

Dostawcy pod lupą

Jeśli trudno jest zweryfikować poprawność kupowanych towarów czy usług, to może więc weryfikować ich

dostawców. Nie kupimy komputerów w firmie, która zawaliła poprzednią dostawę, nie dotrzymała żadnych terminów, potem jej sprzęt się notorycznie psuł, a serwis nie reagował na zgłoszenia. Będziemy się także trzymać z dala od firmy, która w przeszłości nas szpiegowała (jeśli potrafimy się o tym dowiedzieć). To tylko proteza, ale czasami należy się nią posłużyć.

Z podobnego na pozór założenia wyszli unijni spece od bezpieczeństwa telekomunikacji, wprowadzając przepisy i rekomendacje produktów do budowy sieci 5G, uznanych za szczególnie krytyczne dla funkcjonowania społeczeństwa i gospodarki. Skoro nie potrafimy ocenić ryzyka związanego z korzystaniem z konkretnych urządzeń, to oceńmy ryzyko związane z ich dostawcami i stwórzmy czarną listę „dostawców wysokiego ryzyka" (dalej DWR), od których nie będziemy kupować. Istotnym czynnikiem było to, czy państwo, z którego pochodzi dostawca, może ingerować w swobodę działalności gospodarczej. Inaczej mówiąc, czy przedstawiciel administracji kraju X może postawić prezesowi firmy Y pochodzącej z tego kraju propozycję nie do odrzucenia: albo sprzęt będzie szpiegował na rzecz służb kraju X (lub np. nieprawidłowo przesyłał informację w sieci), albo firma Y będzie miała poważne kłopoty, a prezes wyląduje w więzieniu (pretekst zawsze się znajdzie).

W przypadku zakupów przez podmioty publiczne zawsze można byłoby po prostu wykluczyć dostawców z określonych krajów. Tu jednak chodziło o nałożenie ograniczeń na podmioty prywatne – operatorów sieci, czyli o mocną ingerencję w zasadę wolności gospodarczej.

Tajemnicą poliszynela było, że wówczas na rynku istniały dwa dojrzałe rozwiązania 5G – chińskie (tańsze) i europejskie, z udziałem amerykańskim (droższe). Nie ma wątpliwości, że Chiny są krajem niepraworządnym i opresyjnym, w którym prezesa każdej firmy można wsadzić do więzienia, a każdej firmie uniemożliwić działalność. Na dyskusję o cyberbezpieczeństwie nałożył się więc lobbing dostawców oraz operatorów i oskarżenia o próbę eliminacji dostawcy z rynku jedynie na podstawie przypuszczenia o możliwości popełnienia przestępstwa w przyszłości.

Nawiasem mówiąc dyrektor finansowa chińskiej firmy od 5G przesiedziała 2 tygodnie w kanadyjskim areszcie i 3 lata w areszcie domowym na podstawie oskarżenia przez USA o pośrednie łamanie amerykańskich sankcji nałożonych na Iran. Po trzech latach zarzuty praktycznie wycofano, a areszt zniesiono.

DWR po polsku

Polscy urzędnicy od cyberbezpieczeństwa postanowili koncepcję DWR twórczo rozciągnąć także na inne produkty teleinformatyczne. Zgodnie z niedawną nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa Minister Cyfryzacji będzie mógł uznać jakąś firmę za DWR i wówczas tzw. podmioty kluczowe (niezbędne dla funkcjonowania społeczeństwa, m.in. energetyka, transport, bankowość, administracja publiczna) i podmioty ważne (m.in. usługi pocztowe, produkcja żywności, motoryzacja) nie będą mogły korzystać ze wskazanych przez ministra rodzajów produktów, usług lub procesów pochodzących z tej firmy (nazwa stała się nieadekwatna do treści, ale zapewne dla wygody ją pozostawiono). Nie chodzi już tylko o 5G czy w ogóle sieci, ale także np. o serwery, laptopy czy telefony. Jeśli takie produkty są już używane, to należy się ich pozbyć w ciągu 7 lat (a w przypadku sieci telekomunikacyjnych – w ciągu 4 lat).

Decyzja ministra będzie w zasadzie arbitralna, w ustawie nie ma kompletnej listy przesłanek do uznania firmy za DWR. Opisano tylko procedurę – minister musi przede wszystkim zasięgnąć opinii Kolegium ds. Cyberbezpieczeństwa (ale to tylko opinia). Opinia ta obejmuje informacje techniczne (wcześniej wykryte podatności lub incydenty) i organizacyjne (proces wytwarzania i dostarczania produktów), ale przede wszystkim polityczne, opisane powyżej. Skądinąd wiemy, że problem dotyczy nie tylko azjatyckich despotii – np. w USA firmy muszą deklarować udostępnienie rządowi wszelkich posiadanych danych o zagranicznych osobach i firmach (dane podmiotów amerykańskich podlegają konstytucyjnej ochronie). Odmowa wiąże się z odpowiedzialnością karną zarządu (m.in. Cloud Act). Nie można także wykluczyć np. „przyjacielskiej prośby" prezydenta USA do właściciela sieci Starlink o jej wyłączenie tu czy tam. Na wszelki wypadek MC wyłączyło z analizy ryzyka politycznego firmy z krajów UE i NATO, uznając że podsłuchiwanie lub wyłączanie sieci przez sojusznika nie zagraża bezpieczeństwu kraju ani jego obywateli.

Zastrzeżenia wielu środowisk

Każdy zdaje sobie sprawę z zagrożenia, jakie stanowi system zawodny albo celowo wyposażony w mechanizmy dywersji, ale mechanizm DWR budzi poważne wątpliwości, na które wskazali uczestnicy konsultacji, a potem posłowie i eksperci w czasie obrad komisji sejmowej. Federacja Konsumentów zwracała uwagę na wyjątkowo szeroki zakres regulacji i koszty dla konsumentów. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji zarzucała naruszenie zasady proporcjonalności i adekwatności, postulując podejmowanie decyzji tylko na podstawie przesłanek technicznych, a nie politycznych. Członkowie Izby twierdzili zresztą, że chińskie firmy szybciej i sprawniej reagowały na zgłaszane problemy (także te związane z bezpieczeństwem) niż europejskie i amerykańskie. Polska Izba Informatyki i Telekomunikacji krytykowała 4-letni czas na wymianę dostawcy przez operatorów telekomunikacyjnych, co praktycznie wymusi demontaż jeszcze sprawnych urządzeń. Zarzucano, że w wielu dziedzinach wykluczenie dostawców chińskich będzie oznaczać uzależnienie od USA. Niestety przedstawiciel MC na posiedzeniu komisji sejmowej nie przedstawiał żadnych argumentów, dość arogancko pouczał posłów, że sprawa już została przesądzona i MC żąda uchwalenia przepisów w brzmieniu przedstawionym przez rząd. Tak się też stało.

Warto opisać, jakie konsekwencje miałoby np. w Polsce wpisanie chińskiego dostawcy sieci 5G na listę DWR. Część operatorów komórkowych musiałaby w ciągu 4 lat całkowicie przebudować swoje sieci, a koszty z tym związane pogorszyłyby ich pozycję konkurencyjną względem tych operatorów, którzy korzystają z innych rozwiązań. Nic dziwnego, że i u nas trwał i trwa intensywny lobbing zwolenników i przeciwników takiego rozwiązania (niestety także PTI nie uniknęło uwikłania w ten proces, o czym pisałem w „Domenie" kilka lat temu).

Nawiasem mówiąc Minister Obrony Narodowej bez ustawy wprowadził zakaz wjazdu samochodów wyprodukowanych w Chinach (w tym np. Tesli) na teren obiektów wojskowych ze względu na możliwość nieautoryzowanego użycia kamer. Podobny zakaz już wcześniej wprowadzono w Austrii w basenach w saunowych częściach kąpielisk. Zabroniono noszenia okularów do pływania, żeby uniknąć nagrywania współkąpiących się nagusów.

> ***W tej całej politycznej dyskusji zbyt mało koncentrowano się jednak na tym, czy wprowadzenie DWR faktycznie przynajmniej częściowo rozwiąże problem cyberbezpieczeństwa.***

Procedura uznania firmy i jej produktów za DWR jest bardzo długa, podlega KPA, na samą opinię Kolegium ds. Cyberbezpieczeństwa ma 3 miesiące, potem na decyzję przysługuje skarga do sądu. Praktyczne znaczenie będą miały czynniki polityczne, bo techniczne każdy użytkownik będzie stosował i bez tego narzędzia. Nikt przecież nie kupi systemu, za którym ciągnie się historia awarii i cyberincydentów. A jeśli już zostanie wydana decyzja, to potencjalnie cyberniebezpieczne komputery, telefony, kamery czy rutery będą jeszcze przez 7 lat szpiegować i siać dywersję. W przypadku dużych sieci telekomunikacyjnych będą to 4 lata – też sporo. Z drugiej strony bez wyraźnych dowodów winy trudno wykluczać firmy z rynku i zmuszać operatorów do wydawania dużych pieniędzy na natychmiastową wymianę sprzętu.

Pewnym rozwiązaniem jest przewidziana w ustawie możliwość wydania przez ministra polecenia zabezpieczającego. Zobowiązuje ono użytkownika systemu, uznanego za niebezpieczny, do niezwłocznego podjęcia działań zabezpieczających (zmiana konfiguracji posiadanego sprzętu, wprowadzenie dodatkowych procedur nadzoru itp.). Wydaje się, że to właśnie takie polecenia byłyby skuteczniejszym narzędziem poprawy cyberbezpieczeństwa i na nich właśnie należałoby się skupić.

Nowelizacja wprowadziła obowiązek prowadzenia regularnych audytów bezpieczeństwa użytkowanych systemów, zgodnie zresztą z postulatami specjalistów od takich audytów. Radykalnym środkiem byłoby nałożenie na dostawców np. obowiązku szerokiego udostępniania kodu źródłowego swoich produktów (konkurencja dokładnie by je sprawdziła), ale to zapewne wymagałoby dodatkowych rozwiązań dotyczących możliwości patentowania oprogramowania (udostępniam swój kod, konkurenci mogą sprawdzić, czy nie ma w nim błędów czy pułapek, ale nie mogą go przenieść do swoich produktów).

Nowelizacja weszła w życie 2 kwietnia 2026 r. Bardzo jestem ciekaw, czy i kiedy Minister Cyfryzacji rzeczywiście wyda decyzje o uznaniu jakiejś firmy za DWR i jakich produktów taka decyzja będzie dotyczyć.

Podsumowując: nowoczesna informatyka w praktyce coraz bardziej brnie w kłopoty z wiarygodnością i niezawodnością. Złożoność sprzętu i oprogramowania jest tak duża, że dostawcy nie są w stanie wykazać poprawności rozwiązań. Jest to szczególnie groźne w przypadku zastosowań krytycznych, co prowokuje klientów do stosowania topornych rozwiązań o wątpliwej skuteczności, takich jak „dostawcy wysokiego ryzyka". A przecież to nie sam dostawca stanowi ryzyko, ale oprogramowanie i zawierające je produkty. Niebezpieczne są nie tylko mechanizmy wprowadzone celowo do programu, ale także zwykłe błędy, a także niedopracowany czy źle zaprojektowany sprzęt. Budowa i rozwój metod praktycznej weryfikacji oprogramowania nie jest tak spektakularna, jak informatyka kwantowa, ale może bardzo ułatwić nam życie i uczynić je bezpieczniejszym. Może to jest pole do zastosowań sztucznej inteligencji w połączeniu z obowiązkiem powszechnego udostępniania kodów programów.

SESJA 2

SZTUCZNA INTELIGENCJA: NOWE MOŻLIWOŚCI I ZAGROŻENIA

Prowadzący:



Maria Ganzha

profesor Politechniki Warszawskiej, dr hab. nauk matematycznych (PAN). Jej badania skupiają się na systemach rozproszonych (ze szczególnym uwzględnieniem technologii agentowych i Internetu Rzeczy), technologiach semantycznych oraz uczeniu maszynowym. Koordynator Techniczny w projekcie unijnym ASSIST-IoT i koordynator zespołu IBSPAN w projekcie unijnym aerOS. Prezes Oddziału Mazowieckiego PTI. Członek Zarządu Sekcji PTI: „Aktualne Wyzwania Sztucznej Inteligencji".

Program sesji:

- **AI jako nowa Rewolucja Przemysłowa**
  Janusz Kacprzyk – Instytut Badań Systemowych PAN, przewodniczący RN PTI
- **Gaia AI Factory. Infrastruktura dla rozwoju sztucznej inteligencji i budowy suwerenności technologicznej**
  Marek Kasztelnik – koordynator projektu Gaia AI Factory, ACK Cyfronet AGH
- **Robot społeczny w prawie nowych technologii**
  Aneta Sieradzka – Prezeska Fundacji AI One Health, CEO Sieradzka&Partners
- **Metoda naukowa w erze AI. Od asystenta do autonomicznego badacza**
  Tomasz Kajdanowicz – Katedra Sztucznej Inteligencji, Politechnika Wrocławska
- **Inżynieria oprogramowania w świecie AI**
  Radosław Kita, AI Director at TVN Warner Bros. Discovery
- **Inżynieria AI w erze Wielkiej Niewiadomej**
  Borys Stokalski – doradca technologiczny, ekspert GPAI/OECD, członek Rady PIIT

AI jako nowa Rewolucja Przemysłowa

Janusz Kacprzyk

Sztuczna inteligencja oznacza tak istotną zmianę technologiczną, że w jej przypadku możemy mówić o rewolucji przemysłowej. Przeanalizujmy więc kilka istotnych, charakterystycznych cech związanych z tą perspektywą. Skoncentruję się przede wszystkim na implikacjach związanych z edukacją i innymi obszarami społeczno-ekonomicznymi. Przykładowo, omówię kilka istotnych aspektów niedoboru wysoko wykwalifikowanych specjalistów AI, którzy byliby w stanie obsługiwać różnorodne urządzenia i systemy bazujące na AI lub je rozwijać, projektować i wdrażać. Jest to *explicite* związane z misją i bardzo ważnymi obszarami działalności PTI, a także z wyzwaniami stojącymi przed polską gospodarką i społeczeństwem.



Janusz Kacprzyk

Fellow of IEEE (Life), IET, IFSA, EurAI, IFIP, AAIA, AIIA, I2CICC, CoreAcad, SMIA Instytut Badań Systemowych Polskiej Akademii Nauk, Wydział Informatyki, Elektroniki i Telekomunikacji Akademia Gorniczo-Hutnicza im. Stanisława Staszica, Sieć Badawcza Łukasiewicz – Przemysłowy Instytut Automatyki i Pomiarow PIAP

Informatyka, czy szerzej technologie cyfrowe, od dawna mają wpływ nie tylko na naukę czy technikę, ale na losy nas wszystkich – głębokie zmiany technologiczne doprowadziły do prawdziwej rewolucji technicznej, która zmieniła obraz świata, prowadząc do burzliwego rozwoju tych firm, państw, a nawet kontynentów, które za tą rewolucją podążyły, a do zacofania i zbiednienia tych, którzy ją „przespali".

> *Na AI, tak jak na wszystkie nowe technologie o doniosłym znaczeniu, można więc patrzeć z różnych perspektyw: nauk ścisłych i technicznych (zwłaszcza analiz formalnych), algorytmiki, implementacji informatycznej, ale też nauk kognitywnych, psychologii, prawa, nauk społecznych, nauk humanistycznych czy ekonomii.*

Zmiany technologiczne zawsze wywoływały tak istotne transformacje, że prowadziły do rewolucji. Zdobycie przewagi technologicznej zapewniało konkurencyjność i utrzymanie tempa wzrostu gospodarczego i społecznego. Tak było już w przypadku rolnej rewo-

lucji neolitycznej (ok. 10 tys. lat p.n.e.), polegającej na przejściu od łowiectwa i zbieractwa do osiadłego trybu życia rolniczego; arabskiej rewolucji rolnej (VIII–XIII w.) związanej z rozprzestrzenianiem się nowych upraw i technik uprawy, głównie w świecie muzułmańskim; rewolucjami brytyjską i szkocką (XVII–XIX w.), charakteryzującymi się ogromnym wzrostem produkcji rolnej, zwłaszcza zbóż i wreszcie trzecią rewolucją rolną (1930-1960), która przyniosła ogromny wzrost produkcji rolnej, głównie upraw, szczególnie w krajach Trzeciego Świata.

Obecnie pojawiła się bardziej zaawansowana koncepcja związana z rolnictwem i produkcją rolną – Rolnictwo 4.0. Chodzi o wykorzystanie zaawansowanych maszyn i urządzeń, nowe techniki (np. rolnictwo precyzyjne), optymalizację produkcji roślinnej i zwierzęcej za pomocą sensorów, IoT (Internetu Rzeczy), bazowanie na analizach danych i uczeniu maszynowym, świadome i precyzyjne wykorzystanie chemikaliów, zwłaszcza nawozów i herbicydów, korzystanie z nowych osiągnięć w biotechnologii i biochemii, optymalizację nawadniania. Zaleca się ukierunkowaną i wyspecjalizowaną produkcję roślinną i zwierzęcą, aktywniejsze zaangażowanie w globalne łańcuchy dostaw, szersze uwzględnienie aspektów środowiskowych i zrównoważonego rozwoju itp. Nowe technologie rolnicze korzystają w coraz większym stopniu z osiągnięć AI.

Jaką rewolucję przyniesie AI?

Wpływ informatyki na rozwój świata wpisuje się w historię rewolucji przemysłowych.

Nie ma zgody, czy AI jest immanentną częścią Czwartej Rewolucji Przemysłowej, czy już zapoczątkowała Piątą Rewolucję Przemysłową, która charakteryzuje się przede wszystkim powszechnym wykorzystaniem sztucznej inteligencji, komputerów kwantowych, technologii semantycznych itp. Jedną z głównych cech Piątej Rewolucji jest współpraca ludzi i maszyn we wszystkich działaniach.

Wraz z każdym potężniejszym modelem pojawiają się nowe potencjalne zastosowania AI. Już nie frapuje nas automatyzacja wszelkich czynności zarezerwowanych dotąd dla ludzi, analiza danych, wizualizacja i werbalizacja, profilowanie użytkowników i/lub interesariuszy. Widzimy jak systemy wspomagania decyzji zmieniają biznes i pole walki, jak za chwilę będą siać spustoszenie w systemach cyberbezpieczeństwa. Czujemy, że zmieni się wszystko, jesteśmy podekscytowani, że zastosowanie technologii AI staje się warunkiem *sine qua non* sukcesu. Dyskutujemy nie tylko o narzędziach formalnych, algorytmicznych i inżynieryjnych, brane pod uwagę są także aspekty poznawcze, psychologiczne, etyczne, prawne itp. Dużą wagę przywiązuje się też do ludzkiego zaufania do tych nowych technologii i ich wiarygodności.

Jednak między potencjałem technologii a jej praktycznym wykorzystaniem w celu uzyskania wartości dodanej towarów i usług jest ogromna różnica.

Jedna z popularnych klasyfikacji rewolucji przemysłowych wyróżnia:

- **Pierwszą Rewolucję Przemysłową: od końca XIX w. do początku XX w. – przejście z gospodarki rolniczej do przemysłowej, bazujące głównie na parze oraz produkcji żelaza i stali,**
- **Drugą Rewolucję Przemysłową: od końca lat 1900 do początku XXI w. – wykorzystanie elektryczności, kolei, silników spalinowych, produkcji masowej itd.,**
- **Trzecią Rewolucję Przemysłową: od końca lat 2000. do chwili obecnej („rewolucję cyfrową" lub „epokę informacji") – powszechne wykorzystanie komputerów, Internetu i technologii cyfrowych, urządzeń mobilnych, zaawansowanej telekomunikacji itp.**
- **Czwartą Rewolucję Przemysłową, trwającą od przełomu wieków XX i XXI – masowe wykorzystanie technologii cyfrowych, przetwarzania w chmurze, robotyki mobilnej i autonomicznej, Internetu rzeczy (IoT), rzeczywistości wirtualnej i rozszerzonej (VR, ER), blockchainu itp.**

Bariera kadrowa

Otóż wykorzystanie nowych technologii, głównie AI i pokrewnych, napotyka praktycznie na całym świecie na olbrzymie trudności z uwagi na chroniczny i pogłębiający się brak wykwalifikowanej kadry, która byłaby w stanie – po pierwsze – stosować zaawansowane rozwiązania bazujące na AI, a po drugie – tworzyć oryginalne rozwiązania. Te braki kadrowe występują szczególnie w USA, Chinach, Kanadzie, Australii i Wielkiej Brytanii, ale także w UE i Japonii. Sytuacja pogarsza się w coraz większej liczbie krajów i należy się spodziewać, że Polska nie będzie, niestety, wyjątkiem.

Te niedobory – będące bezpośrednią implikacją lawinowo rosnącej skali zastosowań zaawansowanych zastosowań AI w praktycznie wszystkich obszarach biznesu i branżach – wymagają pilnego uruchomienia większej liczby programów studiów licencjackich i magisterskich związanych z AI, a także różnych form szkoleń oraz uaktualniania umiejętności i kwalifikacji dla wszystkich rodzajów pracowników.

> ***PTI ma do odegrania kluczowa rolę przy opracowaniu koncepcji i sposobu efektywnej realizacji właściwego przygotowania niezbędnych kadr.***

Ostatnio wyróżniono dwie główne kategorie niedoborów kadrowych związanych ze sztuczną inteligencją, które są kluczowe dla różnych rodzajów działań w projektach z nią związanych:

- Luka w umiejętnościach (*AI Skills Gap*)
- Luka w talentach (*AI Talent Gap*).

Dotyczą one dwóch aspektów rozwoju, projektowania, wdrażania i wreszcie praktycznego wykorzystania systemów wykorzystujących AI. Luka w umiejętnościach w zakresie AI oznacza zwykle rozbieżność między tym, czego potrzebują użytkownicy nowoczesnych systemów i urządzeń opartych na AI, aby zapewnić skuteczne i wydajne ich użycie, a dostępnością odpowiednio wykwalifikowanego personelu na rynku.

Luka w talentach oznacza natomiast rozbieżność w zapotrzebowaniu na wysoko wykwalifikowanych specjalistów w dziedzinie AI, takich jak badacze i inżynierowie zajmujący się nauką o danych, uczeniem maszynowym itp., którzy potrafią opracowywać, testować i wdrażać nowoczesne rozwiązania oparte na AI, a dostępnością takich specjalistów na rynku.

Te niedobory kadrowe powodują wiele negatywnych konsekwencji dla wszystkich graczy na rynku (biznesu, przemysłu, edukacji, sektora publicznego itd.). Całkowite ich rozwiązanie w przewidywalnej perspektywie jest praktycznie niemożliwe, pozostaje więc jedynie ich bieżące łagodzenie. Sprawa niedoboru umiejętności i kwalifikacji w zakresie AI była przedmiotem analiz wielu interdyscyplinarnych zespołów, skupiających zarówno informatyków, jak i ekonomistów, polityków, humanistów, przedstawicieli nauk społecznych itp. Nie stracił aktualności tzw. Raport Gagne'a (https://jfgagne.ai/blog/ai-talent-2019/), badający lukę w zakresie talentów w dziedzinie AI, co jest dla nas ważne. Dotyczy on głównie aktywnych badaczy, „czołowych talentów", uczestniczących w renomowanych konferencjach i publikujących w prestiżowych czasopismach. Przebadano ok. 22 400 badaczy, z czego 4000 ma wysoką liczbę cytowań, a także ok. 36 000 czołowych specjalistów od AI z serwisu LinkedIn.

Raport wskazuje 5 krajów o największym potencjale w dziedzinie sztucznej inteligencji: Stany Zjednoczone, Chiny, Wielką Brytanię, Kanadę i Niemcy.

Wnioski podsumowujące tego obszernego raportu:

- **Ok. 1/3 badaczy pracuje w kraju innym niż kraj ich pochodzenia, czyli ten, w którym uzyskali stopień doktora,**
- **Firmy amerykańskie przyciągnęły większość badaczy z innych krajów,**
- **Tajwan, Szwecja, Korea, Hiszpania, USA, Szwajcaria, Chiny, Japonia, Wielka Brytania i Australia mają większy „napływ" talentów w dziedzinie sztucznej inteligencji niż „odpływ",**
- **W Szwajcarii i Szwecji ok. połowa zatrudnionych talentów pochodzi z innych krajów, a w Wielkiej Brytanii ponad proc.,**
- **Francja i Izrael odnotowują większy „odpływ" talentów niż ich „napływ",**
- **Kanada, Holandia, Singapur, Szwajcaria i Wielka Brytania mają wyższe niż przeciętne napływy i odpływy kadr.**

Wiele krajów z bardzo dobrymi systemami edukacji, wysokim poziomem kształcenia, zwłaszcza w dziedzinie nauk ścisłych, technologii, inżynierii i matematyki (STEM), kształci wielu wysoko wykwalifikowanych absolwentów. Jednocześnie kraje te nie są w stanie lokalnie wchłonąć tych kadr i zaoferować im odpowiednich miejsc pracy i konkurencyjnych warunków. Dlatego część specjalistów decyduje się na wyjazd, czekają na nich renomowane uniwersytety i firmy z branży AI na całym świecie. Dla kraju kształcącego oznacza to straty, zarówno finansowe, jak i kadrowe. Do takich krajów można też zaliczyć Polskę, znaną w świecie z dużej podaży znakomitych matematyków, informatyków i inżynierów, także specjalistów AI.

Podejmowane są też doraźne próby łatania luk kompetencyjnych w postaci systemów imigracyjnych i wiz specjalnych dla specjalistów o wysokich kwalifikacjach, takie rozwiązania stosują m.in. Wielka Brytania, Kanada czy Japonia. Możemy skorzystać z tych doświadczeń przy opracowywaniu systemu pozyskiwania talentów AI dla Polski.

Gaia AI Factory
Infrastruktura dla rozwoju AI i budowy suwerenności technologicznej

Marek Kasztelnik, Paula Al-Hmiedat, Marek Magryś

Rozwój współczesnych modeli sztucznej inteligencji w coraz większym stopniu zależy od dostępu do ogromnych zasobów obliczeniowych, w szczególności do akceleratorów graficznych wykorzystywanych w procesach trenowania tych modeli. Największe systemy tego typu znajdują się obecnie w centrach danych globalnych dostawców usług chmurowych, bardzo często zlokalizowanych poza Europą. Oznacza to, że zarówno środowisko naukowe, jak i przedsiębiorstwa w Europie uzależnione są od infrastruktury znajdującej się poza ich bezpośrednią kontrolą.



Marek Kasztelnik

Principal Software Engineer, architekt oraz team leader w ACK Cyfronet AGH. Specjalizuje się w tworzeniu rozwiązań umożliwiających uruchamianie aplikacji naukowych na rozproszonych zasobach HPC oraz w infrastrukturach chmurowych. Kierownik z ramienia Cyfronetu w projektach badawczo-wdrożeniowych z obszaru medycyny obliczeniowej (m.in. Gemini) oraz sztucznej inteligencji (Meetween, DVPS). Koordynator Gaia AI Factory. Twórca Model Execution Environment – systemu potokowego przetwarzania danych do symulacji pacjentów, zintegrowanego z superkomputerami Helios, Ares i Athena. Architekt i główny deweloper pierwszej wersji EOSC Marketplace oraz systemu grantowego PLGrid. Autor ponad 50 publikacji i prezentacji z zakresu e-science, medycyny spersonalizowanej, HPC i AI.

Paula Al-Hmiedat

trenerka, facylitatorka, instructional designerka i project managerka z wieloletnim doświadczeniem w projektach krajowych i europejskich realizowanych na styku technologii, sztucznej inteligencji, rozwoju kompetencji oraz polityk publicznych. Specjalizuje się w przygotowywaniu i koordynacji projektów związanych z infrastrukturą cyfrową, obliczeniami wysokiej wydajności (HPC) oraz sztuczną inteligencją, w szczególności w zakresie budowania ekosystemów współpracy między nauką, przemysłem a sektorem publicznym.

Marek Magryś

p.o. dyrektora ACK Cyfronet AGH, kierownik Narodowego Centrum Kompetencji Obliczeniowych w ramach EuroHPC, specjalista w zakresie projektowania, wdrażania, testowania i eksploatacji systemów obliczeniowych dla zastosowań HPC (High Performance Computing) oraz AI (sztucznej inteligencji). Główny architekt najszybszych polskich superkomputerów ostatnich lat, Heliosa, Atheny i Prometheusa. Ekspert Komisji Europejskiej.

Ostatnio coraz częściej podkreśla się, że rozwój technologii AI wymaga nie tylko kompetencji badawczych, lecz także własnej, suwerennej infrastruktury obliczeniowej pozwalającej trenować i testować modele na dużą skalę. Dlatego w ramach programu EuroHPC JU[1] pojawiła się inicjatywa budowy tzw. Fabryk Sztucznej Inteligencji. Jej celem jest stworzenie w Europie sieci ośrodków zapewniających dostęp do infrastruktury obliczeniowej przeznaczonej do rozwoju systemów AI. W ramach tego programu powstają wyspecjalizowane centra integrujące zasoby obliczeniowe, środowiska programistyczne oraz kompetencje badawcze potrzebne do trenowania i wdrażania modeli AI.

Polską częścią tej inicjatywy jest projekt Gaia AI Factory (Gaia AIF)[2]. Jego celem jest budowa infrastruktury umożliwiającej prowadzenie badań nad sztuczną inteligencją oraz rozwijanie jej zastosowań w gospodarce i administracji publicznej. Jednocześnie projekt ma znaczenie dla wzmacniania europejskiej i krajowej suwerenności technologicznej. Posiadanie własnej infrastruktury obliczeniowej pozwala prowadzić prace nad modelami sztucznej inteligencji w środowisku kontrolowanym przez instytucje publiczne i ośrodki naukowe, bez konieczności przenoszenia danych i procesów obliczeniowych do zewnętrznych platform komercyjnych.

Struktura konsorcjum projektowego

Projekt Gaia AI Factory realizowany jest przez konsorcjum instytucji posiadających doświadczenie w rozwijaniu infrastruktury obliczeniowej oraz prowadzeniu badań związanych ze sztuczną inteligencją. Koordynatorem projektu jest Akademickie Centrum Komputerowe Cyfronet AGH[5]. Partnerami przedsięwzięcia są: Wydział Technologii Kosmicznych AGH[6], Wrocławskie Centrum Sieciowo-Superkomputerowe[7], Centrum Informatyczne TASK Politechniki Gdańskiej[8], Narodowe Centrum Badań Jądrowych, Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego Uniwersytetu Warszawskiego[9], NASK – Państwowy Instytut Badawczy[10], Ośrodek Przetwarzania Informacji – Państwowy Instytut Badawczy[11], Sano Centre for Computational Medicine[12], Małopolskie Centrum Biotechnologii Uniwersytetu Jagiellońskiego[13], Instytut Matki i Dziecka[14] oraz Krakowski Park Technologiczny[15]. Budżet projektu wynosi 70 mln euro i jest współfinansowany ze środków krajowych oraz programu EuroHPC JU.

Architektura i potencjał obliczeniowy Gaia AI Factory

Centralnym elementem Gaia AI Factory będzie klaster obliczeniowy przeznaczony do realizacji zadań związanych z trenowaniem i uruchamianiem modeli AI. System ten zostanie wyposażony w około tysiąc akceleratorów GPU zoptymalizowanych pod kątem obliczeń tensorowych[3]. Stworzona infrastruktura pozwoli prowadzić zarówno eksperymenty badawczo-rozwojowe, jak i projekty wymagające intensywnych obliczeń na dużych zbiorach danych.

Architektura systemu została zaprojektowana z myślą o obsłudze dwóch głównych typów obliczeń związanych z rozwojem AI. Pierwsza część infrastruktury będzie przeznaczona do trenowania modeli wymagających równoległego wykorzystania wielu akceleratorów GPU. Druga będzie służyć zadaniom związanym z uruchamianiem wytrenowanych modeli, ich testowaniem oraz wykorzystaniem w praktycznych zastosowaniach.

Całość infrastruktury zostanie zintegrowana z ekosystemem PLGrid[4], który od wielu lat zapewnia dostęp do zasobów wysokowydajnych systemów obliczeniowych w Polsce. Integracja ta oznacza, że użytkownicy będą korzystać ze znanych mechanizmów uwierzytelniania, systemów kolejkowych do zarządzania zadaniami obliczeniowymi oraz narzędzi umożliwiających monitorowanie i analizę wykonywanych obliczeń. Dzięki temu infrastruktura Gaia AI Factory stanie się kolejnym elementem krajowego środowiska HPC (High Performance Computing) wykorzystywanego przez środowisko naukowe i przemysłowe.

1 EuroHPC Joined Undertaken, https://www.eurohpc-ju.europa.eu
2 Gaia AI Factory, https://gaia.plgrid.pl
3 Obliczenia tensorowe to operacje matematyczne wykonywane na wielowymiarowych tablicach danych – tensorach – stanowiące podstawę działania współczesnych modeli uczenia maszynowego i sieci neuronowych.
4 https://plgrid.pl
5 https://www.cyfronet.pl
6 https://spacetech.agh.edu.pl
7 https://wcss.pl
8 https://task.gda.pl
9 https://icm.edu.pl
10 https://www.nask.pl
11 https://opi.org.pl
12 https://sano.science
13 https://mcb.uj.edu.pl
14 https://imid.med.pl
15 https://www.kpt.krakow.pl

Udostępnianie infrastruktury i harmonogram prac

Realizacja projektu Gaia AIF została zaplanowana jako proces obejmujący kilka równoległych etapów związanych z przygotowaniem infrastruktury technicznej oraz budową środowiska usług dostępnych dla użytkowników. Jednym z pierwszych kroków jest modernizacja i przygotowanie infrastruktury mającej na celu instalację maszyny Gaia.

Równolegle prowadzone są działania związane z przygotowaniem dedykowanych usług Gaia AIF oraz ich integracją z ekosystemem PLGrid. Istotnym założeniem projektu jest udostępnienie części tych usług jeszcze przed instalacją docelowego systemu obliczeniowego. Dzięki temu użytkownicy będą mogli rozpocząć pracę z narzędziami przygotowanymi w ramach projektu, korzystając z istniejących zasobów infrastruktury HPC dostępnych w Polsce. Pozwoli to testować środowiska programistyczne, przygotowywać dane oraz rozwijać modele sztucznej inteligencji jeszcze przed uruchomieniem nowego systemu GPU.

W tym samym czasie przygotowywany jest program wsparcia użytkowników, obejmujący szkolenia i warsztaty dotyczące wykorzystania infrastruktury HPC w projektach sztucznej inteligencji oraz korzystania z usług udostępnianych w ramach Gaia AIF. Działania te mają umożliwić przyszłym użytkownikom przygotowanie projektów i zespołów do pracy z nową infrastrukturą.

Kluczowym etapem projektu będzie zakup i wdrożenie systemu obliczeniowego Gaia. Po jego instalacji planowane jest stopniowe udostępnianie zasobów użytkownikom, początkowo w ramach projektów pilotażowych realizowanych we współpracy z partnerami projektu. Pozwoli to na przetestowanie działania infrastruktury w praktyce oraz dostosowanie modelu udostępniania zasobów do potrzeb użytkowników.

Dostęp do infrastruktury dla nauki i gospodarki

Jednym z głównych celów Gaia AI Factory jest udostępnienie infrastruktury obliczeniowej oraz ekspertyzy podmiotom, które nie dysponują własnymi zasobami GPU w skali potrzebnej do trenowania współczesnych modeli sztucznej inteligencji. Dotyczy to zarówno zespołów badawczych rozwijających nowe metody uczenia maszynowego, jak i przedsiębiorstw wykorzystujących AI w swoich produktach.

W praktyce oznacza to możliwość prowadzenia eksperymentów z modelami wymagającymi znacznych zasobów obliczeniowych bez konieczności inwestowania we własną infrastrukturę sprzętową. Dla wielu małych i średnich przedsiębiorstw koszt zakupu i utrzymania dużych systemów GPU stanowi istotną barierę wejścia w obszar zaawansowanej analizy danych i sztucznej inteligencji. Udostępnienie infrastruktury w ramach krajowego systemu HPC pozwala tę barierę częściowo ograniczyć i zwiększyć liczbę projektów wykorzystujących technologie AI.

Istotnym elementem projektu jest również system wsparcia dla użytkowników. Obejmuje on pomoc techniczną w zakresie konfiguracji środowisk obliczeniowych, optymalizacji zadań treningowych oraz wykorzystania narzędzi dostępnych w środowisku HPC. Tego typu wsparcie jest szczególnie ważne dla zespołów, które rozpoczynają pracę z infrastrukturą wysokowydajnych systemów obliczeniowych.

Równolegle prowadzone będą działania związane z rozwijaniem kompetencji w zakresie wykorzystania infrastruktury obliczeniowej w projektach AI. Obejmą one organizację warsztatów, wydarzeń edukacyjnych oraz programów stażowych, które umożliwią studentom, badaczom, przedstawicielom MŚP oraz startupom zdobycie doświadczenia w pracy z dużymi systemami obliczeniowymi, wykorzystywanymi przy rozwijaniu i wdrażaniu rozwiązań sztucznej inteligencji.

Obszary zastosowań

Infrastruktura Gaia AI Factory będzie wykorzystywana w projektach badawczych i wdrożeniowych z różnych dziedzin, w których analiza dużych zbiorów danych i trenowanie złożonych modeli sztucznej inteligencji stanowią kluczowe elementy. Jednym z takich obszarów jest medycyna i biotechnologia, gdzie metody uczenia maszynowego wykorzystywane są m.in. do analizy obrazów medycznych, modelowania struktur białek oraz wspomagania projektowania nowych leków.

Istotną rolę będą odgrywać również projekty związane z analizą danych satelitarnych i teledetekcyjnych. Systemy sztucznej inteligencji są coraz częściej stosowane do przetwarzania obrazów satelitarnych, monitorowania zmian środowiskowych oraz analizy dużych zbiorów danych geograficznych. Infrastruktura obliczeniowa umożliwiająca przetwarzanie takich danych w dużej skali jest w tym kontekście jednym z kluczowych elementów.

Kolejnym obszarem są zastosowania w sektorze publicznym, gdzie sztuczna inteligencja będzie wspierać analizę dużych zbiorów danych administracyjnych, automatyzować przetwarzanie dokumentów oraz wspomagać procesy decyzyjne oparte na analizie danych.

Etyka, transparentność i regulacje

Rozwój infrastruktury przeznaczonej do trenowania modeli sztucznej inteligencji wiąże się również z koniecznością uwzględnienia kwestii regulacyjnych i etycznych. W Europie szczególne znaczenie ma w tym kontekście rozporządzenie AI Act[16], które wprowadza ramy prawne dla projektowania i wykorzystywania systemów sztucznej inteligencji.

Gaia AI Factory umożliwi prowadzenie badań i projektów w sposób zgodny z obowiązującymi regulacjami. W praktyce oznacza to możliwość dokumentowania procesu trenowania modeli, kontrolowania jakości i pochodzenia danych treningowych oraz analizowania ich wpływu na działanie modeli. Infrastruktura będzie umożliwiać identyfikowanie stronniczości w danych treningowych, jak również w wynikach generowanych przez modele sztucznej inteligencji. Takie podejście jest szczególnie istotne w przypadku zastosowań AI w obszarach o dużym znaczeniu społecznym, takich jak administracja publiczna czy medycyna.

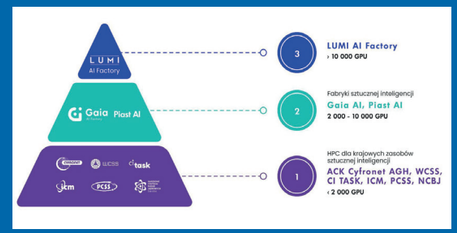
wisk danych umożliwiających trenowanie coraz bardziej złożonych modeli sztucznej inteligencji. Wraz ze wzrostem zapotrzebowania na obliczenia związane z AI rośnie także znaczenie współpracy między ośrodkami badawczymi, administracją publiczną oraz sektorem prywatnym.

> ***W dłuższej perspektywie Gaia AI Factory stanie się fundamentem europejskiego ekosystemu technologicznego w obszarze sztucznej inteligencji, umożliwiając rozwój i wdrażanie nowych rozwiązań w sposób niezależny od infrastruktury dostarczanej przez globalne platformy technologiczne, a tym samym wzmacniając suwerenność technologiczną w obszarze przetwarzania danych i obliczeń wysokiej wydajności.***

Integracja w europejskim ekosystemie AI

Gaia AI Factory jest częścią szerszej europejskiej inicjatywy rozwoju infrastruktury dla sztucznej inteligencji rozwijanej w ramach programu EuroHPC JU. W jej ramach powstaje sieć fabryk AI oraz systemów superkomputerowych, które wspólnie tworzą europejski ekosystem wspierający rozwój i wdrażanie rozwiązań opartych na sztucznej inteligencji.

Projekt zakłada współpracę z innymi ośrodkami powstającymi w ramach programu EuroHPC, w tym z rozwijanymi w Polsce LAIF[17] oraz PIAST[18] AI Factory. Integracja tych ośrodków z europejskimi systemami superkomputerowymi umożliwia skalowanie projektów badawczych od infrastruktury krajowej do zasobów dostępnych w skali całej Europy.



Ekosystem infrastruktury wspierającej rozwój sztucznej inteligencji – od krajowych centrów HPC do europejskich fabryk AI

Znaczenie dla rozwoju technologicznego

Budowa Gaia AI Factory jest pierwszym krokiem w kierunku stworzenia w Polsce trwałej infrastruktury wspierającej rozwój sztucznej inteligencji. W perspektywie kolejnych lat można oczekiwać dalszego zwiększania skali dostępnych zasobów obliczeniowych oraz integracji z kolejnymi systemami HPC rozwijanymi w Europie.

Istotnym kierunkiem rozwoju będzie również rozszerzanie ekosystemu narzędzi programistycznych oraz środowisk danych umożliwiających trenowanie coraz bardziej złożonych modeli sztucznej inteligencji. Wraz ze wzrostem zapotrzebowania na obliczenia związane z AI rośnie także znaczenie współpracy między ośrodkami badawczymi, administracją publiczną oraz sektorem prywatnym.

Jednocześnie funkcjonowanie Gaia AI Factory będzie generować doświadczenia wynikające z realizacji konkretnych zastosowań AI, modeli dostępu do infrastruktury obliczeniowej oraz sposobów współpracy między nauką, biznesem i administracją publiczną. Zgromadzona w ten sposób wiedza będzie stanowić ważne źródło empirycznych przesłanek dla dalszego rozwoju polityk i strategii w obszarze sztucznej inteligencji, danych i cyfryzacji, zarówno na poziomie krajowym, jak i w szerszym ekosystemie europejskim.

16 EU Artificial Intelligence Act, https://artificialintelligenceact.eu

17 https://lumi-ai-factory.eu

18 https://www.pcss.pl/piast-ai

Robot społeczny w prawie nowych technologii

Aneta Sieradzka

Dynamiczny rozwój technologii bazujących na sztucznej inteligencji prowadzi do powstawania coraz bardziej zaawansowanych systemów interakcyjnych, wchodzących w bezpośrednie relacje z człowiekiem. Wśród nich szczególne miejsce zajmują tzw. roboty społeczne – systemy projektowane nie tylko do wykonywania zadań technicznych, lecz przede wszystkim do nawiązywania i podtrzymywania interakcji społecznych. Pojęcie to, choć szeroko wykorzystywane w naukach technicznych, psychologii czy socjologii, nie ma jednoznacznego umocowania w obowiązującym porządku prawnym.



Aneta Sieradzka

prezeska Fundacji AI One Health, członkini Społecznego Zespołu Ekspertów przy Prezesie UODO i Zespołu ds. rozwoju zastosowań Big Data i uwarunkowań regulacyjnych przy Prezesie GUS.

Rodzi to wiele wątpliwości: czy „robot społeczny" jest kategorią prawną, gdzie przebiegają granice między nim a innymi systemami cyfrowymi oraz czy istnieje potrzeba jego odrębnej regulacji? Przeanalizujmy prawny status robotów społecznych ze szczególnym uwzględnieniem problemu ich definicji, granic regulacyjnych, odpowiedzialności za ich działanie oraz przyszłych kierunków legislacyjnych.

Robot społeczny jako kategoria pozaprawna

Pojęcie „robota społecznego" funkcjonuje przede wszystkim jako konstrukcja opisowa, wypracowana na gruncie badań interdyscyplinarnych. Najczęściej definiuje się go jako system wyposażony w elementy sztucznej inteligencji oraz fizyczny interfejs – nierzadko humanoidalny lub zoomorficzny – którego głównym celem jest interakcja społeczna z człowiekiem. Może ona obejmować komunikację werbalną, rozpoznawanie emocji, reagowanie na zachowania użytkownika czy budowanie długotrwałych relacji.

> ***Z perspektywy prawa istotne jest jednak to, że „robot społeczny" nie stanowi obecnie kategorii normatywnej. Ani ustawodawstwa krajowe, ani regulacje ponadnarodowe nie wyróżniają tej klasy systemów jako odrębnego przedmiotu regulacji.***

Zamiast tego prawo operuje kategoriami funkcjonalnymi i ryzykownymi, koncentrując się na tym, co dana technologia robi, a nie jak wygląda. Oznacza to, że robot społeczny może być jednocześnie: systemem sztucznej inteligencji, produktem w rozumieniu przepisów o bezpieczeństwie produktów, narzędziem przetwarzającym dane osobowe, a w określonych kontekstach – nawet wyrobem medycznym. Brak jednoznacznej definicji prawnej nie jest przypadkowy. Wynika on z dominującego w nowoczesnych regulacjach podejścia bazującego na analizie ryzyka, które zakłada neutralność technologiczną prawa.

Jednym z kluczowych problemów jest ustalenie granicy między robotem społecznym a innymi systemami technologicznymi. W praktyce granica ta ma charakter funkcjonalny, a nie ontologiczny. System może przyjmować różne formy: aplikacji mobilnej, asystenta głosowego, urządzenia fizycznego (np. robota humanoidalnego). Z prawnego punktu widzenia forma ma znaczenie drugorzędne. Kluczowe są natomiast takie elementy jak: zdolność do przetwarzania danych (w tym danych osobowych), autonomia decyzyjna, wpływ na zachowanie użytkownika, kontekst zastosowania (np. opieka zdrowotna, edukacja, rozrywka). W konsekwencji robot społeczny nie jest wyraźnie odróżnialny od „systemu AI w fizycznej obudowie". Jeśli dwa systemy realizują tę samą funkcję – np. prowadzą rozmowę terapeutyczną – to będą podlegały podobnym regulacjom, niezależnie od tego, czy jeden z nich ma postać aplikacji, a drugi robota.

Takie podejście odzwierciedla szerszy trend w prawie nowych technologii: odejście od klasyfikacji urządzeń na rzecz analizy ich funkcji i skutków.

Projektowanie relacji a problem manipulacji emocjonalnej

Roboty społeczne wyróżnia cecha szczególna: są projektowane w celu budowania relacji z człowiekiem. Wykorzystują mechanizmy psychologiczne, takie jak antropomorfizacja, przypisywanie intencji czy empatia. Człowiek ma naturalną tendencję do traktowania takich systemów jak podmiotów społecznych, nawet jeśli jest świadomy ich sztucznego charakteru. Z perspektywy prawa rodzi to problem tzw. projektowania perswazyjnego. Technologia może być zaprojektowana w sposób celowy, aby wpływać na decyzje użytkownika, wzbudzać określone emocje, budować zaufanie, a nawet uzależniać od interakcji.

Nie zawsze jest to zjawisko negatywne. W wielu przypadkach – takich jak terapia, rehabilitacja czy edukacja – wpływ na zachowanie użytkownika jest pożądany. Problem pojawia się jednak wtedy, gdy użytkownik nie jest świadomy natury systemu, wykorzystywana jest jego podatność psychologiczna i dochodzi do manipulacji emocjonalnej. Dzieci, osoby starsze czy pacjenci są grupami szczególnie wrażliwymi. W ich przypadku relacja z robotem społecznym może realnie wpływać na autonomię decyzyjną. W odpowiedzi na te wyzwania pojawia się postulat rozszerzenia regulacji na sam proces projektowania systemów. Oznacza to przesunięcie akcentu z pytania „co system robi" na „w jaki sposób oddziałuje na użytkownika". W praktyce może to prowadzić do obowiązku transparentności (np. informowania, że użytkownik ma do czynienia z systemem AI), ograniczeń w zakresie projektowania interfejsów manipulacyjnych, szczególnych zasad ochrony użytkowników podatnych na wpływ.

Jakie obszary wymagają dookreślenia?

Jednym z kluczowych, a jednocześnie niedostatecznie rozstrzygniętych obszarów związanych z wykorzystaniem robotów społecznych są zagadnienia prywatności, cyberbezpieczeństwa oraz etyki projektowania i użytkowania tych systemów. Wynika to przede wszystkim z ich specyfiki – roboty społeczne nie tylko przetwarzają dane, lecz także czynią to w kontekście bezpośredniej, często długotrwałej relacji z użytkownikiem.

W zakresie ochrony prywatności szczególne znaczenie ma fakt, że roboty społeczne operują na danych o wysokiej wrażliwości. Oprócz klasycznych danych osobowych mogą one przetwarzać: dane biometryczne (np. rozpoznawanie twarzy, głosu), dane behawioralne (sposób poruszania się, reakcje użytkownika), dane emocjonalne (analiza mimiki, tonu głosu), informacje dotyczące zdrowia psychicznego lub fizycznego. Zakres i głębokość tej analizy powodują, że robot społeczny staje się nie tylko narzędziem, lecz także swoistym „sensorem życia prywatnego". Z perspektywy prawa rodzi to konieczność stosowania zaawansowanych mechanizmów ochrony danych, takich jak minimalizacja danych, ograniczenie celu przetwarzania czy zapewnienie przejrzystości działania systemu. Szczególne znaczenie ma również świadoma zgoda użytkownika, która w kontekście relacyjnego charakteru interakcji może być trudna do jednoznacznego ustalenia.

Równolegle pojawia się problem cyberbezpieczeństwa. Roboty społeczne, jako urządzenia fizyczne połączone z systemami informatycznymi, stanowią potencjalny wektor ataków. Naruszenie ich bezpieczeństwa może prowadzić nie tylko do wycieku danych, ale również do bezpośredniego wpływu na zachowanie użytkownika. W skrajnych przypadkach możliwe jest przejęcie kontroli nad urządzeniem, manipulowanie jego komunikatami czy wykorzystanie go do działań szkodliwych. Z tego względu bezpieczeństwo robotów społecznych powinno być analizowane w sposób ho-

listyczny – obejmujący zarówno warstwę techniczną (np. zabezpieczenia systemów, aktualizacje oprogramowania), jak i warstwę interakcyjną (np. odporność na manipulację społeczną czy nadużycia relacyjne). Coraz częściej podkreśla się potrzebę wdrażania koncepcji *security by design* oraz *privacy by design*, czyli uwzględniania wymogów bezpieczeństwa i prywatności już na etapie projektowania systemu.

Nie mniej istotny jest wymiar etyczny, chodzi o granice dopuszczalnego oddziaływania robotów społecznych. Kluczowe dylematy etyczne obejmują m.in.: dopuszczalność „symulowania" emocji i relacji przez systemy nieludzkie i ryzyko wprowadzania użytkownika w błąd co do natury interakcji, wpływ na autonomię i sprawczość człowieka, potencjalne uzależnienie od relacji z technologią, zastępowanie relacji międzyludzkich relacjami z systemami sztucznymi. W odpowiedzi na te wyzwania rozwijane są różnego rodzaju wytyczne etyczne oraz standardy projektowe, które mają na celu zapewnienie, że technologia pozostaje podporządkowana interesowi człowieka. Coraz częściej wskazuje się również na potrzebę wprowadzenia mechanizmów etyki wbudowanej (*ethics by design*), które integrowałyby normy etyczne bezpośrednio w architekturze systemów.

Zagadnienia prywatności, cyberbezpieczeństwa i etyki stanowią integralny element dyskusji o robotach społecznych. Nie są one jedynie dodatkiem do problematyki prawnej, lecz jednym z jej centralnych wymiarów. To właśnie w tych obszarach najpełniej ujawniają się napięcia między innowacyjnością technologii a koniecznością ochrony podstawowych wartości, takich jak autonomia, godność i bezpieczeństwo człowieka.

Kto odpowiada za działanie robotów społecznych

Kolejnym istotnym zagadnieniem jest przypisanie odpowiedzialności za skutki działania robotów społecznych. Ze względu na ich złożoność odpowiedzialność ta ma charakter rozproszony. Producent odpowiada za bezpieczeństwo produktu oraz jego zgodność z deklarowanymi funkcjami. W przypadku wad konstrukcyjnych lub projektowych może ponosić odpowiedzialność na zasadzie odpowiedzialności za produkt niebezpieczny. Dostawca oprogramowania odpowiada za działanie algorytmów i modele decyzyjne. Jeśli określone zachowania systemu wynikają z błędów w oprogramowaniu lub danych treningowych, odpowiedzialność może być przypisana właśnie temu podmiotowi. Operator lub instytucja wdrażająca (np. szpital, dom opieki) ponosi odpowiedzialność za sposób użycia technologii. Nawet bezpieczny system może stać się źródłem ryzyka, jeśli zostanie niewłaściwie zastosowany. Projektanci systemu odgrywają coraz większą rolę w kontekście odpowiedzialności za decyzje projektowe, zwłaszcza te związane z interakcją społeczną i wpływem na użytkownika.

> ***W efekcie odpowiedzialność ma charakter systemowy. Prawo stopniowo odchodzi od modelu przypisywania winy jednemu podmiotowi na rzecz rozłożenia jej wzdłuż całego łańcucha technologicznego – zgodnie z zakresem kontroli nad ryzykiem.***

Pora na pytanie natury zasadniczej: czy niezbędne jest stworzenie odrębnej kategorii regulacyjnej dla robotów społecznych? Obecne tendencje wskazują, że jest to mało prawdopodobne. Nowoczesne regulacje technologiczne bazują na kilku kluczowych zasadach: neutralności technologicznej, podejściu opartym na ryzyku, elastyczności regulacyjnej. Zgodnie z tym podejściem nie ma potrzeby tworzenia osobnych przepisów dla każdej nowej kategorii technologii. Wystarczające jest stosowanie istniejących ram prawnych do nowych kontekstów. Jednocześnie roboty społeczne ujawniają nowe wyzwania, które mogą wymagać doprecyzowania prawa, w szczególności w zakresie: relacji człowiek – technologia, ochrony autonomii użytkownika, regulacji wpływu emocjonalnego, standardów projektowania interfejsów. Dlatego bardziej prawdopodobny jest rozwój szczegółowych zasad dotyczących systemów AI i interakcji z użytkownikiem niż powstanie odrębnej gałęzi prawa „robotów społecznych".

Robot społeczny jest dziś przede wszystkim kategorią opisową, a nie prawną. Jego znaczenie wynika nie z formalnej definicji, lecz z funkcji, jaką pełni. Prawo nie koncentruje się na samej formie technologii, lecz na ryzykach, jakie generuje. W tym sensie granica między robotem społecznym a innymi systemami AI jest płynna i zależy od kontekstu zastosowania. Największym wyzwaniem nie jest więc klasyfikacja robotów społecznych, lecz zrozumienie i regulacja relacji, jakie tworzą one z użytkownikami. To właśnie w tej relacji – a nie w samej technologii – ujawniają się kluczowe problemy prawne przyszłości.

Metoda naukowa w erze AI
Od asystenta do autonomicznego badacza

Tomasz Kajdanowicz

Przez stulecia metoda naukowa pozostawała niezmieniona – obserwacja, hipoteza, eksperyment, wnioski. Dziś sztuczna inteligencja wkracza w każdy etap procesu badawczego, nie tylko przyspieszając pracę naukowca, lecz także stawiając pytanie, które brzmi coraz mniej abstrakcyjnie: czy nauka może się obejść bez naukowca?



Tomasz Kajdanowicz
profesor uczelni, kierownik Katedry Sztucznej Inteligencji
na Wydziale Informatyki i Telekomunikacji
Politechniki Wrocławskiej

Sztuczna inteligencja stała się wszechobecna w ludzkich aktywnościach – od sztuk kreatywnych po badania naukowe. Potężne systemy generatywnej AI, takie jak duże modele językowe (np. GPT-5), potrafią dziś realizować zadania, które do niedawna wymagały ludzkiej inteligencji: przeszukiwać literaturę, analizować dane, generować kod czy pisać fragmenty artykułów naukowych. Wizja dostępu do technologii autonomicznego naukowca AI nie jest już odległa.

Przyjrzyjmy się więc, jak AI przekształca każdy z klasycznych kroków metody naukowej – od definiowania problemu badawczego po interpretację wyników i publikację. To zarazem dobra okazja do zastanowienia się, gdzie leżą granice tej transformacji i co w procesie badawczym musi pozostać domeną człowieka.

Jak AI zmienia każdy krok metody naukowej

Klasyczna metoda naukowa to iteracyjny i nieliniowy cykl sześciu kroków: (1) zdefiniowanie problemu badawczego, (2) przegląd istniejącej wiedzy, (3) sformułowanie hipotez, (4) zaprojektowanie eksperymentu, (5) zbieranie i analiza danych, (6) interpretacja wyników i wyciąganie wniosków. Każdy z tych kroków wymaga kreatywności, wiedzy dziedzinowej, umiejętności analitycznych i osądu. Dziś AI wkracza w każdy z tych etapów z różną intensywnością i z różnymi konsekwencjami.

Krok 1: Definiowanie problemu badawczego

Tradycyjnie wybór problemu badawczego to akt twórczy i wartościujący. Naukowiec identyfikuje luki w wiedzy i decyduje, które pytania warto zadać. Dziś duże modele językowe i narzędzia analizujące grafy wiedzy pomagają w skanowaniu literatury, identyfikowaniu niezbadanych obszarów i generowaniu kandydac-

kich pytań badawczych. AI może zaproponować listę otwartych problemów w danym polu, podpowiedzieć, gdzie istnieją sprzeczne wyniki między badaniami, a nawet wskazać interdyscyplinarne połączenia, których ludzki badacz mógłby nie dostrzec. W perspektywie przyszłej mówi się wręcz o „eksploracji bez hipotezy", zanurzeniu w dane bez prekoncepcji, by zobaczyć, jakie wzorce się wyłonią.

Krok 2: Przegląd literatury

AI jest niezwykle skuteczna w przetwarzaniu tekstu, co czyni ją naturalnym wsparciem dla przeglądu literatury. Narzędzia takie jak *Elicit*, *Semantic Scholar* czy *Consensus* potrafią przeszukać tysiące artykułów, wygenerować zwięzłe podsumowania i zsyntetyzować stan wiedzy w danym temacie. Zamiast tygodni ręcznego przeglądania baz danych badacz może w kilka godzin uzyskać mapę kluczowych prac z wyodrębnionymi wnioskami. Trzeba jednak pamiętać o ograniczeniach: AI potrafi streszczać, co mówią prace, ale nie rozumie jeszcze głęboko koncepcji ani jakości dowodów. Modele językowe bywają też skłonne do generowania fałszywych cytatów; badacz musi traktować wyniki AI jako punkt wyjścia, a nie ostateczne słowo.

Krok 3: Formułowanie hipotez

Generowanie hipotez to tradycyjnie domena ludzkiej kreatywności i rozumowania abdukcyjnego. AI może tu wnieść istotny wkład, analizując duże zbiory danych i wskazując nieoczywiste korelacje do testowania. W odkrywaniu leków modele generatywne proponują nowe struktury molekularne, w istocie generując hipotezy o aktywności chemicznej. Ograniczeniem pozostaje to, że AI nie ma prawdziwego rozumienia znaczenia ani kontekstu i może generować hipotezy, które na papierze wyglądają logicznie, ale w praktyce są trywialne, nieetyczne lub nierealizowalne.

Krok 4: Projektowanie eksperymentów

AI zaczyna wspomagać projektowanie metodologii. Algorytmy optymalizacji mogą zaproponować najefektywniejsze parametry eksperymentu, dobór próby czy wybór metod statystycznych. Perspektywą przyszłości są samooptymalizujące się protokoły badawcze, w których AI na bieżąco analizuje wyniki i autonomicznie decyduje o następnym kroku, coś w rodzaju agenta wspomagającego projektowanie kolejnych kroków badań. Jednak AI nie rozumie „ducha" eksperymentu, może zaproponować plan statystycznie poprawny, ale ignorujący praktyczne realia laboratorium.

Krok 5: Zbieranie i analiza danych

To etap, na którym AI przynosi największe przyspieszenie. Uczenie maszynowe i głębokie sieci neuronowe potrafią przetwarzać ogromne zbiory danych, wykrywać wzorce, klastry i anomalie na skalę daleko przekraczającą ludzkie możliwości. Narzędzia takie jak *Code Interpreter* czy *GitHub Copilot* umożliwiają badaczom interakcję z danymi w trybie konwersacyjnym, demokratyzując zaawansowaną analizę. Krytycznym ograniczeniem jest to, że modele AI nie poszukują prawdy, a optymalizują trafność predykcji. Znajdą wzorce niezależnie od tego, czy są one przyczynowe czy przypadkowe.

Krok 6: Interpretacja wyników i publikacja

Modele językowe mogą pisać szkice sekcji artykułów, sugerować odpowiedni język naukowy, a nawet służyć jako „wirtualny recenzent" sprawdzający logiczną spójność wniosków. AI pomaga również w procesie publikacyjnym: wyszukiwaniu referencji, formatowaniu, tłumaczeniu na angielski naukowy. Perspektywą są systemy wykonujące metaanalizy całych pól badawczych w trybie ciągłym, automatycznie identyfikujące, kiedy zebrano wystarczające dowody, by uznać daną hipotezę za potwierdzoną lub obaloną.

Narzędzia AI w warsztacie naukowca

Przegląd literatury: *Elicit* – automatyczna ekstrakcja wniosków z artykułów; *Semantic Scholar* – inteligentne wyszukiwanie z grafem cytowań; *Research Rabbit* – wizualizacja powiązań między pracami; *Consensus* – syntetyczne odpowiedzi na pytania badawcze.

Generowanie hipotez: *AlphaFold* (*DeepMind*) – przewidywanie struktury białek; *AI Scientist* (*Castelvecchi, D., 2024*) – prototyp systemu prowadzącego badania end-to-end.

Analiza danych: *GitHub Copilot* i *Code Interpreter* – generowanie kodu analitycznego w trybie konwersacyjnym; *AutoML* – automatyczny dobór i optymalizacja modeli.

Pisanie i publikowanie: *Scite* – weryfikacja cytatów i kontekstu cytowań; *DeepL Write* – poprawa języka naukowego; *Jenni.ai* – asystent pisania akademickiego.

Autonomiczny naukowiec – wizja czy bliska rzeczywistość?

Naturalnym pytaniem jest, czy wszystkie kroki metody naukowej mogą zostać zautomatyzowane od początku do końca? Niektórzy badacze już próbują odpowiedzieć na to pytanie eksperymentalnie.

W 2024 r. zespół Sakana AI zbudował prototyp *AI Scientist*, systemu bazującego na GPT-4, który autonomicznie przeszukiwał literaturę, generował hipotezy, projektował i wykonywał eksperymenty obliczeniowe, a następnie pisał i recenzował własne szkice artykułów naukowych. System wciąż miał poważne ograniczenia, ale sam fakt stworzenia takiego prototypu był przełomowy. Podobnie w chemii i naukach o materiałach działają „laboratoria robotyczne", w których AI decyduje, jaki eksperyment przeprowadzić następnie, a ramiona robotyczne go wykonują.

Optymistyczna wizja zakłada, że armie agentów AI mogłyby prowadzić dziesiątki równoległych linii badawczych, dramatycznie przyspieszając tempo odkryć. Pesymistyczna, że nauka prowadzona wyłącznie przez AI utraci wymiar ludzki: poczucie sensu, etyczny kompas i zdolność do rozróżniania, które pytania naprawdę warto zadać.

Dług poznawczy – ukryty koszt asystenta AI

Badacze z MIT Media Lab przeprowadzili w 2025 r. eksperyment, w którym uczestnicy pisali eseje w trzech wariantach: samodzielnie, z pomocą wyszukiwarki internetowej i z pomocą dużego modelu językowego. Monitorowano aktywność mózgu za pomocą EEG.

Wyniki były uderzające: osoby korzystające z AI wykazywały najsłabszą aktywność neuronalną, ich mózg pracował jak na „jałowym biegu". Po kilku sesjach grupy intensywnie korzystające z AI gorzej radziły sobie także bez niego, ich „mięśnie poznawcze" zanikały z braku ćwiczenia. Dla naukowców to ostrzeżenie: AI może przyspieszyć pracę, ale nadmierne poleganie na niej grozi utratą umiejętności głębokiego myślenia i twórczego rozumowania.

Co to oznacza dla nas, naukowców?

Analiza wpływu AI na poszczególne etapy metody naukowej prowadzi do wniosku formułowanego coraz wyraźniej: pewne elementy procesu badawczego powinny pozostać w rękach człowieka.

Przede wszystkim jest to definiowanie problemu badawczego. To akt twórczy i wartościujący, osadzony w kontekście społecznym, etycznym i kulturowym. AI może sugerować tematy, ale nie ma poczucia sensu, nie wie, dlaczego pewne pytania mają większe znaczenie od innych. Trafnie ujęto to w debacie naukowej: nauka potrafi powiedzieć nam, jak sklonować gen, ale nie powie, czy powinniśmy to robić.

Drugim elementem jest interpretacja wyników. To wymaga mądrości, umiejętności osadzenia ustaleń w szerszym kontekście, rozpoznania ich implikacji, dostrzeżenia ograniczeń. AI może stwierdzić, że „X koreluje z Y", ale skok do zrozumienia, dlaczego tak jest i co to oznacza, pozostaje domeną ludzkiego rozumowania. Istnieje też ryzyko pozornej obiektywności – przeświadczenia, że „komputer to policzył, więc musi być prawda".

> ***Rewolucja AI w nauce już trwa. Pytanie nie brzmi, czy narzędzia sztucznej inteligencji zmienią sposób prowadzenia badań, bo przecież one już go zmieniają. Kluczowe jest, jak ta zmiana przebiegnie.***

Najbardziej prawdopodobny scenariusz to „nauka przyspieszona przez AI", model, w którym każdy etap procesu badawczego jest wspomagany przez inteligentne narzędzia, ale człowiek pozostaje u steru: wyznacza cele, ocenia wyniki, podejmuje decyzje wartościujące.

Bardziej radykalna wizja „nauki zautomatyzowanej" wymaga ostrożności. I to nie dlatego, że jest technicznie niemożliwa, lecz dlatego, że może prowadzić do utraty tych jakości, które czynią naukę ludzkim przedsięwzięciem dążenia do prawdy, poczucia odpowiedzialności i etycznego kompasu.

Dla polskiej społeczności informatyków i naukowców płynie z tego wyraźny przekaz: nie unikajmy tych narzędzi, ale włączajmy je w nasz warsztat badawczy z pełną świadomością ich możliwości i ograniczeń. Przygotowujmy studentów i młodych badaczy do pracy w świecie, w którym AI jest partnerem, ale partnerem, którego wyniki trzeba umieć krytycznie oceniać.

Referencje

Castelvecchi, D. (2024). Researchers built an 'AI Scientist'– what can it do. *Nature*, 633(8029), 266–266.

Gstrein, O.J., Haleem, N., Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. *Internet Policy Review*, 13(3), 1–26.

Kosmyna, N. et al. (2025). Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task. arXiv:2506.08872 (MIT Media Lab).

Wang, H. et al. (2023). Scientific discovery in the age of artificial intelligence. *Nature*, 620, 47–60.

Zhou, E., Lee, D. (2024). Generative artificial intelligence, human creativity, and art. *PNAS Nexus*, 3(3), 52.

Inżynieria AI w erze Wielkiej Niewiadomej

Borys Stokalski

Gdy w 2023 r. ChatGPT stał się usługą masową, okazało się oczywiste, że nasza branża, która od dekad nie rozwiązała podstawowych problemów z jakością i niezawodnością oprogramowania, właśnie dostała do ręki kerning o ogromnej „sile rażenia".



Borys Stokalski

praktyk i doradca technologiczny,
ekspert GPAI/OECD, twórca frameworku CAST.
Autor książki *Do AI Right. Building Responsible AI Engineering Practice Using CAST Framework*
(Oficyna Wydawnicza SGH,
Warszawa 2025, ISBN 978-83-8030-772-8).
Framework CAST jest dostępny pod adresem
www.doairight.org oraz w katalogu narzędzi OECD AI Policy Observatory.

Standish Group od dekad dokumentuje tę samą ponurą statystykę: tylko ok. 31% projektów IT kończy się sukcesem w klasycznym sensie: na czas, w budżecie, z wymaganymi funkcjami. Połowa ma drastyczne opóźnienia i/lub przekraczane budżety. Taka jest cena wykładniczego rozwoju technologii i złożoności rozwiązań. Teraz dołożyliśmy do tego zestawu modele z bilionami parametrów.

Potrafimy sprawnie generować kod – ale czy potrafimy tak zorganizować pracę, że ten kod będzie robił to, co trzeba i tak, jak trzeba? To banalne pytanie staje się dzisiaj jednym z centralnych dylematów rozwojowych. W mojej opinii – ważniejszym niż pytanie o to, czy starczy nam energii i mocy obliczeniowych. Odpowiedź na nie określi, czy monstrualne inwestycje w AI wygenerują zwrot, czy okażą się paleniem w piecu postępu pieniędzmi, które – coraz częściej – należą do podatników, a nie tylko do prywatnych inwestorów technologicznych.

Dlaczego IT nie ma odpowiedzialnej inżynierii?

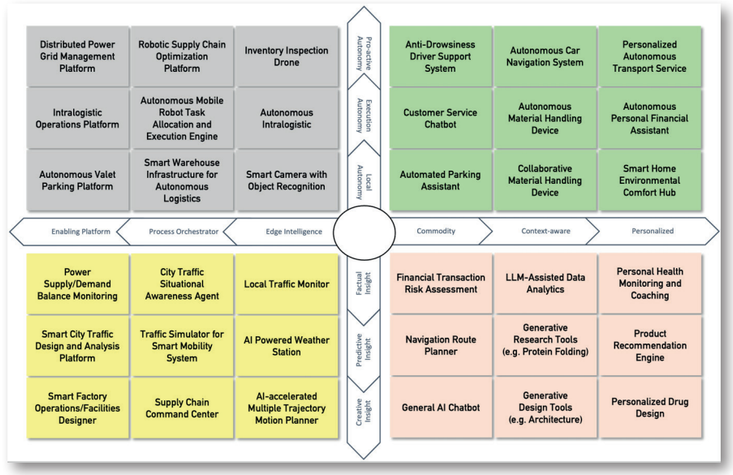
W budownictwie i lotnictwie odpowiedzialna inżynieria nie jest filozoficzną deklaracją. Jest systemem: standardy, certyfikacje, autonomia specjalistów, niezależne badania wypadków, zawodowe kodeksy etyczne. Kanadyjski Żelazny Pierścień – noszony na palcu przez inżynierów od 1925 r. – to symbol czegoś bardzo konkretnego: zobowiązania wobec społeczeństwa, które ma instytucjonalne zakotwiczenie.

IT takiego systemu nie zbudowało. Nawet, gdy oprogramowanie zaczęło sterować samolotami, dawkować promieniowanie RTG albo liczyć wyniki wyborów, rozwiązania IT miały charakter punktowy, nie systemowy.

> ***Doskonaliliśmy metody formalne, narzędzia, ale nie zmieniliśmy systemu kształtującego odpowiedzialność twórców oprogramowania – firm i ludzi.***

Oczywiście, most, który się wali, zabija ludzi natychmiast i publicznie, co kształtuje zupełnie inną kulturę odpowiedzialności. Jednak holenderski system świadczeń społecznych – algorytm decyzyjny, który przez lata dyskryminował tysiące rodzin, rujnując im życie poprzez fałszywe oskarżenia o wyłudzenia – to nie jest metafora. To realne konsekwencje złego oprogramowania. Autonomiczny pojazd GM, któremu cofnięto licencję w San Francisco po serii wypadków – to realne konsekwencje niewystarczającego testowania.

W 2019 r. OECD sformułowało Pryncypia Odpowiedzialnej AI – transparentność, sprawiedliwość, rozliczalność, bezpieczeństwo. W tym samym roku grupa ekspertów Komisji Europejskiej opublikowała wytyczne dla godnej zaufania AI (Trustworthy AI). Jednak między zasadami a praktyką jest przepaść, której nie zasypie AI Act. Odpowiedzialność za wartości produktu AI jest rozmyta między inwestorami, product ownerami, data scientists a prawnikami. Wartości, które nie mają właściciela, nie stają się elementem kultury pracy – postaw i zachowań – w procesie projektowania i budowy produktu.



„Siatka" pokazująca mapę klas rozwiązań AI wraz z przykładami.

Jak działa CAST

Zamiast kategoryzować AI według technik (modele klasyfikacyjne, sieci neuronowe, algorytmy reinforcement learning), CAST kategoryzuje rozwiązania według ich profilu biznesowego i roli w relacji z człowiekiem. Wyróżniam cztery główne klasy Smart Solutions: Servant Proxies – asystenci poznawczy, augmentujący ludzką pracę; Digital Coworkers – systemy współpracujące z ludźmi w ramach wspólnych procesów; Autonomous Operations Platforms – systemy działające w dużym stopniu samodzielnie; oraz systemy wirtualizacji i zarządzania aktywami i procesami. Każda klasa ma swój profil ryzyka, charakterystyczne dylematy projektowe i inne wymagania nadzoru.

Zauważenie tej luki było punktem wyjścia dla projektu CAST (Constructive Approach to Smart Technologies). Zacząłem go budować wraz z grupą wspierających mnie znawców AI (prof. Bogumił Kamiński, Daniel Kaszyński, Robert Kroplewski i prof. Przemysław Biecek) w ramach Global Partnership on Artificial Intelligence – sieciowego ciała ekspertów wspierającego OECD. Problem rysował się wyraźnie: jak pogodzić codzienną pracę inżynierów, architektów i właścicieli produktu z ekosystemem zasad i wytycznych. Jak przełożyć „transparentność AI" na decyzję architektoniczną? Jak uczynić ze „sprawiedliwości" wymaganie funkcjonalne?

CAST nie jest kolejnym zestawem zasad. To zbiór praktyk wpisujących się w cykl życia systemu i inżynierskie procesy z nim związane.

Centralnym artefaktem każdego projektu w CAST jest „mandat" rozwiązania (Solution Charter) – zapis intencji, który poprzedza jakikolwiek kod, model czy specyfikację. Mandat definiuje cel rozwiązania, wartości produktu, ograniczenia etyczne i kryteria sukcesu. To żywy dokument, w którym pytania, takie jak „kto jest odpowiedzialny za uczciwość (fairness) modelu?" lub „jaką wartość wnosi wyjaśnialność dla użytkownika i jak uczynić z niej czynnik przewagi konkurencyjnej tworzonego produktu", stają się pytaniami projektowymi, a nie filozoficznymi.

Dla systemów agentowych – które stają się dominującą architekturą w AI produkcyjnym – równie kluczowy jest „mandat agenta" (Agent Charter). Definiuje zakres autonomii agenta, jego pętle decyzyjne (OODA: Observe-Orient-Decide-Act), mechanizmy

eskalacji i logikę radzenia sobie z sytuacjami, których nie uwzględniliśmy, projektując agenta (fallback). W czasach, gdy agenci AI zarządzają zadaniami i inicjują działania o realnych konsekwencjach, precyzyjne zdefiniowanie granic autonomii jest tak samo krytycznym wymaganiem, jak specyfikacja funkcjonalna.

Odpowiedzialne projektowanie

Kompromisy projektowe to sedno odpowiedzialnej inżynierii. Właśnie w nich przejawia się prawdziwa odpowiedzialność, nie w deklaracjach. Przykłady z codziennej praktyki:

- Dokładność kontra wyjaśnialność. Głębokie modele sieci neuronowych często są dokładniejsze – ale ich decyzje są nieprzejrzyste nawet dla twórców. W systemach ochrony zdrowia czy edukacji to nie jest kwestia preferencji – to wymaganie prawne i etyczne. Nikt nie powinien stracić dostępu do leczenia z powodu decyzji, której nie można wytłumaczyć. CAST nie rozstrzyga tego dylematu za projektanta, ale wymaga, żeby był on świadomie podjęty, udokumentowany i przypisany do właściciela.
- Prywatność kontra użyteczność, automatyzacja kontra nadzór ludzki i wiele innych kompromisów – do rozwiązywania tego typu dylematów CAST dostarcza język i strukturę.

Platforma, dostępna pod adresem www.doairight.org, zawiera interaktywny nawigator taksonomii, wzorce projektowe, heurystyki inżynierskie i narzędzia generatywne wspierające pracę z frameworkiem. Jest projektem społecznościowym – zarejestrowanym w katalogu narzędzi OECD AI Policy Observatory.

Rozwijam ją z przekonaniem, że odpowiedzialna inżynieria AI potrzebuje wspólnego języka praktyki, nie kolejnych deklaracji wartości. Korzystam z doświadczeń pracy z zespołami tworzącymi produkty AI w programie mentoringowym Scaling Responsible AI Solutions uruchomionym przez GPAI. Taka praca bardzo dobitnie pokazuje, że tworzenie odpowiedzialnych rozwiązań to nie jest przede wszystkim kwestia zarządzania zgodnością regulacyjną przez działy compliance. Kluczowe jest mapowanie pryncypiów odpowiedzialnej AI na założenia architektury produktu tak wcześnie w cyklu życia, jak to tylko możliwe.

Wielka Niewiadoma

Budujemy systemy, których do końca nie rozumiemy. I robimy to w pośpiechu, bo kapitał płynie, rynek czeka, a konkurencja nie zwalnia. Brytyjski alpinista George Mallory pytany, dlaczego wspina się na Mount Everest, odpowiedział „bo tam jest". W świecie technologii bywa podobnie – dzisiejsza pogoń za skalowaniem modeli jest de facto napędzana ciekawością, jak daleko ta ścieżka doprowadzi, jakie emergentne cechy modeli pojawią się, kiedy powiększymy ich złożoność o kolejne rzędy wielkości. Taka motywacja jest zrozumiała, ale niewystarczająca w przypadku narzędzi o tak dużym wpływie.

Kiedy w 2016 r. program AlphaGo firmy Google DeepMind wygrał w go z Lee Sedolem 4:1, świat był zaskoczony. Eksperci byli zgodni, że maszyna nie pokona człowieka w go przez co najmniej dekadę – gra jest zbyt złożona, zbyt intuicyjna, zbyt „ludzka". Myliliśmy się. Również w przypadku AI przełomy przychodzą wcześniej, niż przewidujemy i w zaskakujących formach.

To samo dotyczy zachowania systemów w produkcji. Duże modele językowe „rozwijają" zdolności, których nikt nie projektował. Systemy wieloagentowe tworzą dynamiki, których nie da się wydedukować z analizy poszczególnych agentów. Systemy uczą się w środowiskach, które same ewoluują. Ryzyko „dryfu kontekstu" – stopniowego oddalania się zachowania systemu od pierwotnych założeń – jest realne, trudno mierzalne i łatwe do przeoczenia w codziennym natłoku zadań.

Klasyczna logika inżynieryjna: specyfikacja, implementacja, testy, wdrożenie – coraz rzadziej wystarcza. Nie dlatego, że jest zła. Dlatego, że zakłada, iż wiemy, czego chcemy zanim zaczniemy budować. W systemach AI z prawdziwą adaptacją i emergencją to założenie często się nie sprawdza.

Jest jeszcze jeden wymiar, o którym mówi się zbyt rzadko: fundamentalne ograniczenia kognitywne ludzi projektujących złożone systemy AI. Psychologia kognitywna pokazuje, że jesteśmy w stanie równolegle aktywnie przetwarzać około 7±2 elementów. Architektura systemu AI w produkcji ma ich nieporównanie więcej. Każdy specjalista widzi swój kawałek — architekt widzi architekturę, data scientist widzi model, prawnik widzi compliance, etyk widzi wartości. Nikt nie widzi całości.

I to jest sytuacja strukturalna, nie wynik niedostatecznego talentu czy zaangażowania. Nie da się tego naprawić, zatrudniając mądrzejszych ludzi. Można to naprawić, budując lepszą infrastrukturę – narzędzia, procesy i struktury, które sprawiają, że złożoność jest zarządzana systemowo, a nie pozostawiana wyłącznie ludzkim ekspertom.

Czy odpowiedzialna inżynieria AI jest w ogóle możliwa?

Tak, jeśli zamiast „czy możemy zagwarantować pełne bezpieczeństwo?" zapytamy: „jak zaprojektować system i procesy wokół niego tak, by ryzyko było identyfikowalne, zarządzalne i możliwe do ograniczenia?"

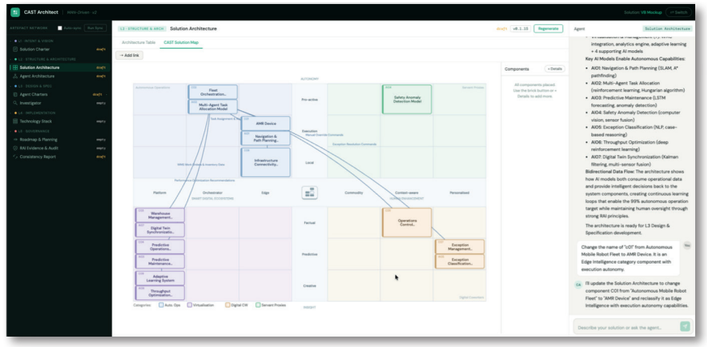
To zmiana paradygmatu – z inżynierii gwarancji na inżynierię odporności. Akceptujemy, że systemy AI będą się mylić, i projektujemy mechanizmy wykrywania, eskalacji i korekcji. Akceptujemy, że wartości będą wchodzić w konflikt – i projektujemy jawne procedury rozstrzygania tych konfliktów z udokumentowaną odpowiedzialnością. Akceptujemy, że nasze rozumienie systemu jest niepełne, i budujemy observability i nadzór ludzki jako pierwszoklasowe wymagania architektoniczne, nie jako opcjonalne dodatki.

CAST wpisuje się w ten paradygmat. Nie gwarantuje doskonałości tylko strukturę, w której odpowiedzialność jest wbudowana w procesy i artefakty, a niedoskonałość jest zarządzana, a nie ignorowana.

W pewnym momencie prac nad CAST zrozumiałem, że framework odpowiada na pytanie: „jak projektować odpowiedzialne systemy AI", ale nie odpowiada w wystarczający sposób na pytanie głębsze: „jak utrzymać spójność rozumienia w zespole, który działa w środowisku generatywnej AI?". Jak to zrobić w świecie galopującego rozwoju narzędzi generatywnych, bez których nie zdołamy już budować systemów AI, ale które nie mogą stać się czarnymi skrzynkami.

MAN Driven Development

To pytanie stało się punktem wyjścia kolejnej koncepcji związanej z CAST – MAN Driven Development, gdzie MAN to Multi-level Artefact Network, czyli wielopoziomowa sieć artefaktów definiujących system i jego funkcjonalność z wykorzystaniem narzędzi generatywnych. MAN w tym określeniu oznacza również intencję postawienia człowieka w centrum procesu, mimo kognitywnej przewagi, jaką na wielu polach mają maszyny. Bo w tym ekosystemie człowiek jest jedynym elementem, który rozumie istotę wartości i działa intencjonalnie.



Wielopoziomowa sieć artefaktów w środowisku systemu CAST Architect (eksperymentalna platforma projektowania systemów AI zgodnie z paradygmatem MANDD).

Generatywna AI zmieniła ekonomikę i dynamikę wytwarzania oprogramowania w sposób, który jest głębszy niż się wydaje na pierwszy rzut oka. Kod generuje się w sekundy. Specyfikacje powstają w minuty. Całe szkice architektur można uzyskać z kilku promptów. To brzmi jak odpowiedź na nasze problemy. Ale w rzeczywistości stworzyło nowe wąskie gardło – i to poważniejsze niż szybkość produkcji.

> ***To nie szybkość produkcji artefaktów jest dziś wąskim gardłem procesu wytwórczego. Staje się nim spójność koncepcji opisywanej z różnych perspektyw i nasza zdolność do jej rozumienia i krytycznej oceny.***

Im szybciej generujemy, tym szybciej narastają niespójności – między intencją a projektem, między projektem a implementacją, między implementacją a wdrożonym zachowaniem systemu. Istniejące paradygmaty nie były projektowane dla tego świata. Spec-Driven Development zakłada liniowy pipeline: człowiek pisze specyfikację, maszyna implementuje. Agile zarządza backlogiem jako płaską listą tasków. Model-Driven Architecture definiuje formalne transformacje między stałymi poziomami. Żaden nie był projektowany z myślą o tym, że AI-agenci i ludzcy współtwórcy jednocześnie produkują artefakty na każdym poziomie abstrakcji – i że spójność całości jest centralnym wyzwaniem inżynierskim.

MAN definiuje pięć poziomów abstrakcji, na których istnieją artefakty inżynierskie. L1 to Intencja i Wizja: cele, ograniczenia etyczne, wartości produktu – tu za-

korzenione są wymagania z Solution Charter CAST. L2 to Struktura i Architektura: mapa komponentów, hierarchia agentów, kluczowe decyzje architektoniczne. L3 to Projekt i Specyfikacja: Agent Charters, specyfikacje modeli, kryteria akceptacji. L4 to Implementacja: kod, wytrenowane modele, konfiguracja, testy. L5 to Weryfikacja i Governance: wyniki testów, dashboardy monitoringu, ścieżki audytu, dowody spełnienia wymagań RAI.

Kluczowe jest to, co dzieje się między poziomami. MAN traktuje każde przejście jako jawną, rządzoną transformację: z wyraźnie określonym agentem (człowiek lub AI), kierunkiem i zobowiązaniem spójności. Nie ma „niejawnego rozumienia". Artefakt generowany przez AI bez powiązania z siecią artefaktów nie jest wkładem inżynierskim – jest szumem. I to właśnie szum akumuluje się najszybciej, gdy generujemy z prędkością, na jaką pozwala generatywna AI.

Kolaps poziomu abstrakcji

Jeden z siedmiu princypiów MAN, który uważam za szczególnie ważny, to zakaz kolapsu poziomu abstrakcji. Każdy poziom ma swój charakterystyczny język i poziom szczegółowości. Artefakt implementacyjny, który importuje rozumowanie architektoniczne, lub artefakt architektoniczny, który przepisuje wybory implementacyjne – to najczęstsze źródło niespójności w złożonych systemach. MAN czyni z poziomu abstrakcji wymaganie inżynierskie, nie preferencję stylistyczną.

CAST i MAN wzajemnie się wzmacniają i zamierzam rozwijać je razem. CAST dostarcza taksonomii rozwiązań, wzorców projektowych i heurystyk dla konkretnych kategorii systemów AI. MAN dostarcza metaframeworku zarządzania artefaktami, który sprawia, że decyzje projektowe CAST są możliwe do śledzenia, spójne i propagowane przez cały cykl życia. Razem adresują pytanie, które dla mnie jest centralnym wyzwaniem odpowiedzialnej inżynierii AI w erze generatywnej: jak utrzymać integralność intencji w procesie, który jest z natury wielopoziomowy, iteracyjny i coraz częściej współtworzony przez narzędzia, które produkują szybciej, niż my jesteśmy w stanie weryfikować.

To ma bezpośrednie przełożenie na odpowiedzialność. Siódma zasada MAN brzmi: odpowiedzialne wymagania – ograniczenia etyczne, granice bezpieczeństwa, zobowiązania regulacyjne – są pełnoprawnym źródłem wymagań projektowych i propagują się w dół przez sieć transformacji, tak jak każde inne wymaganie. Odpowiedzialny system AI to taki, którego MAN zawiera pełny, nieprzerwany łańcuch śledzenia od odpowiedzialnej intencji na L1 do zweryfikowanego zachowania na L5. Odpowiedzialność AI nie jest checklistą nakładaną po fakcie. Jest właściwością dobrze skonstruowanej sieci artefaktów.

Do AI Right nie jest manifestem idealisty. Napisałem ją jako praktyk, który przez lata widział, jak dobre intencje rozbijają się o brak struktury, a to dobra struktura pozwala dobrym intencjom przetrwać zderzenie z rzeczywistością projektów, presją czasu i rynkową konkurencją.

Technologia AI nie jest ani dobra, ani zła sama w sobie. Jej wartość – i jej ryzyko – zależy od tego, jak jest zaprojektowana, zbudowana i nadzorowana. Zbyt długo branża IT traktowała etykę jako warstwę dekoracyjną nakładaną na gotowy produkt. W erze AI, gdy systemy działają autonomicznie, uczą się i podejmują decyzje o realnych konsekwencjach, to podejście jest nie tylko niewystarczające. Staje się niebezpieczne.

CAST i MAN to propozycja infrastruktury, która sprawia, że odpowiedzialność jest wbudowana w codzienną pracę zespołów – w artefakty, procesy, role i decyzje projektowe – a nie zarezerwowana dla komitetów etycznych spotykających się raz na kwartał. To narzędzia, nie filozofia.

Jest jeszcze jeden wymiar, który chcę podkreślić: wspólnota. Odpowiedzialna inżynieria AI nie jest zadaniem dla jednostek ani nawet dla pojedynczych organizacji. Wymaga wspólnego języka, wspólnych standardów i środowiska, w którym doświadczenia – zarówno sukcesy, jak i porażki – są dzielone i stanowią podstawę do nauki. PTI jako środowisko skupiające praktyków kształtujących cyfrową przyszłość Polski ma tu wyjątkową rolę do odegrania. Nie tylko jako forum wymiany wiedzy, lecz także jako instytucja zdolna wspierać kształtowanie kultury odpowiedzialnej inżynierii AI – od edukacji, przez standardy, po dialog z regulatorami.

> ***Presje wywierane na ludzi „robiących AI" są ogromne. Mamy jednak wybór, jak na nie odpowiadamy, i warto go podjąć świadomie.***

SESJA 3

Rozwój specjalistycznych kompetencji cyfrowych

Sesja Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo

Prowadzący:

Tomasz Kulisiewicz

absolwent informatyki Budapeszteńskiego Uniwersytetu Technicznego (1974), doktorat z informatologii na Uniwersytecie Warszawskim (2015). Analityk i wykładowca, autor publikacji naukowych oraz analiz dla Komisji Europejskiej, instytucji krajowych i zagranicznych. Współzałożyciel i ekspert Ośrodka Studiów nad Cyfrowym Państwem. Sekretarz Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo.

Program sesji:

- **European Union and Support of AI Competences Education: A Subjective Overview**
  Jakub Christoph – Sekretarz Generalny CEPIS
- **Rady Sektorowe odpowiedzią na zmiany kompetencji poszukiwanych na rynku pracy**
  Bogdan Kościuch, Dyrektor Departamentu Rozwoju Kadr w PARP
- **Certyfikacja kompetencji cyfrowych. Od ICDL do Zintegrowanego Systemu Kwalifikacji**
  Bogusław Dębski – Dyrektor Centrum Certyfikacji Kompetencji i Potwierdzania Kwalifikacji PTI
- **Rola edukacji pozaformalnej w czasach AI**
  Beata Ostrowska – BROst Centrum Edukacji i Technologii Komputerowej, Wiceprzewodnicząca Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo
- **AI w kształceniu akademickim – nowe wyzwania**
  Danuta Morańska – Akademia Humanitas, ekspert Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo
- **Różne oblicza informatyki w zawodach szkolnictwa branżowego**
  Sławomir Smugowski – Centrum Kształcenia Zawodowego i Ustawicznego w Jaworznie / Uniwersytet Śląski, członek Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo
- **Kim będą w najbliższych latach specjaliści ITCB**
  Katarzyna Starosławska – Wiceprezes Zarządu Fundacji SpeakLeash, członkini Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo

European Union and Support of AI Competences Education

A Subjective Overview

Jakub Christoph

Across Europe, artificial intelligence (AI) has become a central pillar of digital transformation in education. Governments, European Union (EU) institutions, and transnational organizations are implementing policies to ensure that citizens gain the digital and AI related competences needed to thrive in an increasingly automated world.



Jakub Christoph

Christoph is the CEPIS and ITPE Secretary General since September 2021. He coordinates the work of both organisations to promote IT professionalism by fostering professional standards and experience sharing among IT professionals; community.

He previously held the position of Regional Development Manager for Europe and MENA in ICDL Foundation. His role involved coordinating activities of ECDL/ ICDL Operators, advocacy for digital literacy and its certification in Europe and MENA region.

He is a passionate advocate of user digital skills and professional competence development.

The shift is driven by rapid technological change, the rise of generative AI, and the recognition that AI literacy is now a prerequisite for meaningful participation in society and the labour market. Recent EU level legislation—especially the **AI Act**[1] —has further accelerated the adoption of structured AI competence frameworks and mandatory literacy requirements, influencing national strategies across all Member States. EU Level Frameworks Driving National Adoption

The EU's **Digital Education Action Plan**[2] **(DEAP)** remains the foundation for Member States' digital and AI education reforms. It calls for a high performing digital education ecosystem and stronger cooperation between countries to build digital and advanced skills, including AI and data literacy.

It also recognizes AI, high performance computing, and cybersecurity as key technologies essential for Europe's competitiveness. Member States are encouraged to integrate these into formal and informal education systems, from early schooling to tertiary levels. More specifically, the EU AI Act—the first comprehensive AI regulation globally—introduces mandatory AI literacy obligations. Under Article 4, both providers and deployers of AI systems must ensure that relevant staff possess adequate levels of AI literacy[3]. This requirement applies across sectors, including education, and influences national teacher training, curriculum design, and workforce development programs.

Importantly, the Act embeds human centric and ethical principles, requiring transparency, safety, and fairness in all AI systems used in schools.

The AI Act is a basis of **AI Literacy Framework**[4], jointly developed by the European Commission and OECD (review draft published May 2025), supports primary and secondary education systems in defining essential AI knowledge and skills. It aligns with DEAP, the Council Recommendations on digital education[5], the DigComp 3.0 framework[6], and the abovementioned EU AI Act. It aims to guide countries in updating curricula and teacher resources to ensure informed, ethical, and human centred use of AI.

The framework is designed to help schools understand *„what students should know, understand, and be able to do"* in a world where AI is ubiquitous. It ensures learners develop not only technical familiarity but also critical thinking, ethical understanding, and responsible digital citizenship. Although still in draft form, the framework defines literacy in ai as spanning knowledge, skills, and attitudes across several key dimensions: understanding what AI is (foundational concepts), recognizing ethical, social, and human rights implications, developing critical data literacy, applying AI tools responsibly and creatively as well as fostering lifelong learning and adaptability.

It is noteworthy that the framework is not meant to create a separate AI subject. Instead, it provides guidance on integrating AI concepts across: STEM subjects (e.g., computing, mathematics), humanities (e.g., ethics, social science), as well as media literacy and citizenship education. The final version of the framework is scheduled to be published later this year.Futile exercise?

It is, however, by no means a given that the EU AI Literacy framework will have any significant impact on the level of AI competences across Europe. In fact, a degree of scepticism is not out of place.

Under the Treaty on the Functioning of the European Union (TFEU), education is not an area in which the EU can legislate by harmonizing national systems. Instead, it is a supporting competence. This means the EU—and therefore the European Commission—may support, coordinate, or complement the actions of Member States, but cannot replace or override national authority on how education systems are organized or what they teach. In other words, it is the prerogative, for better or worse, of national governments to determine their educational curricula, systems and allocated resources.

Secondly, competence frameworks are widely misunderstood. Digital competence frameworks are supposed to define the digital skills people need to learn and work effectively, collaborate online, manage data, and use technology safely. They should act as reference points for understanding digital competence needs for particular job profiles, assessing individual and organisational skills gaps, or understanding scope of existing training and certification tools. In an ideal world, a recruiter using a framework would be able to check what level of digital skills (and their appropriateness for the offered position) can be expected from a candidate certified with six modules of ICDL or CompTIA.

Instead, the existing digital competence frameworks are confused with curricula. Many decision-makers treat them as a list of essential competences everyone should have in the digital era. As an example, at the time when DigComp 1.0 was published, in Poland the Ministry of Development Funds and Regional Policy, which at that time managed European Social Fund allocation, planned to require any digital skills training funded by the EU to cover the whole framework.. If such a policy were to be implemented, an over 50-year-old jobseeker in a small town attending a 50-hour course to improve their prospect for a basic office job would be required to obtain such competences as:

- *"I can solve conceptual problems taking advantage of technologies and digital tools, I can contribute to the knowledge creation through technological means, I can take part in innovative actions through the use of technologies. I proactively collaborate with others to produce creative and innovative outputs." 5.3C, DigComp 1.0 or*

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. Retrieved on 2 April 2026 from Regulation - EU - 2024/1689 - EN - EUR-Lex

2 Digital Education Action Plan 2021-2027 - European Education Area, retrieved on 2 April 2026.

3 Regulation - EU - 2024/1689 - EN - EUR-Lex, retrieved on 2 April 2026.

4 AI Literacy Framework, retrieved on 2 April 2026 from Home | AILit Framework.

5 Council Recommendation on the key enabling factors for successful digital education and training, 23 November 2023, retrieved on 2 April 2026 from Digital skills and competences and successful digital education and training: fit for the digital era - Consilium

6 DigComp 3.0: European Digital Competence Framework. Retrieved on 2 April 2026 from JRC Publications Repository - DigComp 3.0: European Digital Competence Framework

- *"I can interfere with (open) programmes, modify, change or write source code, I can code and programme in several languages, I understand the systems and functions that are behind programmes." 3.4C, DigComp 1.0*

Fortunately, the Ministry plans were altered. However, the problem of misunderstanding competence frameworks still exists and is not limited to the former Ministry in Poland.

The biggest reason for potential scepticism of the ability to evaluate the effectiveness of AI education support on a European scale is lack of data regarding the current level of AI, or, even more broadly, general digital skills. One might point to data sources such as the State of the Digital Decade Report[7] (formerly Digital Economy and Society Index (DESI)), which is published on annual basis and is widely used to compare digital readiness of European countries. However, this index has a fundamental flaw that significantly reduces its suitability for measuring digital competence levels. The DESI Methodological Note[8] identifies that DESI indicators relative to digital skills are sourced from EUROSTAT 'ICT Usage in Households and by Individuals' survey. Examination of the methodology of the said survey reveals that the data is based on self-reflection (not even self-assessment) of the respondents rather than any objective assessment. The participants in the survey are, for example, asked if they "*have carried out the following software related activities out in the last 3 months: a) Using word processing software b) Creating files (e.g. document, image, video) incorporating several elements, e.g. text, picture, table, chart, animation, sound c) Using spreadsheet software c1) Using advanced features of spreadsheet software (functions, formulas, macros, Visual Basic) to organise, analyse, structure or modify data d) Editing photos, video or audio files e) Writing code in a programming language*". In order to demonstrate their skills, respondents need to answer 'yes' to each question. Data obtained through self-assessment is arguably not sufficiently reliable to objectively evaluate digital skills levels of the population. However, it is widely used by many European stakeholders, who treat it with credibility that is not fully merited.

Conclusion

Despite the pessimistic outlook, it is worth acknowledging that European countries are demonstrating a strong, coordinated effort to support the integration of AI competences into education across all levels of society. Through EU wide legislative requirements, national digital strategies, teacher training frameworks, and international collaboration projects, Europe is building the foundations of an AI literate population. These education reforms—grounded in ethics, human rights, and innovation—ensure that European learners and workers are prepared not only to use AI tools but to understand, question, and shape the AI driven world around them.

The result may well be a dynamic and forward looking European AI education ecosystem, characterized by high level policy alignment, practical school level guidance, expansive teacher development programmes, and a strong commitment to digital inclusion and equality.

On the other hand, it may also become a bureaucratic EU-wide chaos, giving the Eurosceptics another reason to mock the European project. Much will depend on strong collaboration, sustained commitment from all stakeholders, clear definitions of core concepts, and willingness to adapt to the rapidly changing digital landscape of our times.

7 Digital Decade DESI visualisation tool, retrieved on 2 April 2026 from Digital Decade DESI visualisation tool - Digital Decade DESI visualisation tool.

8 Digital Decade 2025: DESI methodological note, retrieved on 2 April 2026 from Digital Decade 2025: DESI methodological note | Shaping Europe's digital future.

Certyfikacja kompetencji cyfrowych
Od ICDL do Zintegrowanego Systemu Kwalifikacji

Bogusław Dębski

W epoce gwałtownej cyfryzacji rozwój kompetencji cyfrowych stał się nie tylko szansą, lecz przede wszystkim koniecznością. Nawet te zawody, które jeszcze niedawno wydawały się od technologii odległe, dziś wymagają sprawnego poruszania się w cyfrowym środowisku. Dlatego nie zastanawiamy się już nad tym, czy warto rozwijać kompetencje cyfrowe, lecz nad tym, jak wiarygodnie potwierdzić ich posiadanie. Jak odróżnić deklaracje od rzeczywistych umiejętności? Jak zapewnić, by publiczne środki inwestowane w szkolenia przekładały się na faktyczny rozwój, a nie jedynie na listę obecności – często świadczącą głównie o tym, że uczestnik spędził kilka godzin na sali szkoleniowej, popijając kawę lub herbatę?



Bogusław Dębski

były zastępca dyrektora Departamentu Społeczeństwa Informacyjnego Ministerstwa Cyfryzacji, wiceprzewodniczący Sektorowej Rady ds. Kompetencji – Informatyka, obecnie dyrektor Centrum Certyfikacji Kompetencji i Potwierdzania Kwalifikacji w PTI.

Mamy obecnie do dyspozycji dwa narzędzia, które w uporządkowany i wiarygodny sposób pozwalają szukać odpowiedzi na pytania o prawdziwe, a nie deklarowane kompetencje cyfrowe. Z jednej strony jest International Certification of Digital Literacy (ICDL), z drugiej – Zintegrowany System Kwalifikacji (ZSK). Choć działają w dwóch różnych przestrzeniach – globalnej i krajowej – łączy je zasada kluczowa dla jakości procesu walidacji: umiejętności nie może oceniać ten, kto uczy. To właśnie ta niezależność egzaminowania stanowi wspólny fundament obu systemów.

Fundament, który – poza systemem edukacji formalnej – powinien w zdecydowanej większości stać się obowiązkowym standardem. Zgodnie z ideą ZSK: nie ma znaczenia, skąd i w jaki sposób zdobyłeś wiedzę czy umiejętności. Liczy się to, że potrafisz je wykazać,

a my potwierdzimy je w sposób wiarygodny, przejrzysty i niezależny. W tym tkwi siła ZSK: docenia nie ścieżkę, lecz efekt uczenia się. Takie też jest ICDL.

> *W praktyce oznacza to, że osoba czy instytucja ucząca nie ma prawa wystawiać certyfikatu. Egzamin odbywa się w sposób neutralny, niezależny i obiektywny, dzięki czemu jego wynik ma wartość, której nie podważają ani okoliczności, ani subiektywne oceny.*

Przemyślane podejście

ICDL Foundation – organizacja rozwijająca ICDL na całym świecie – od lat stawia na najwyższe standardy oceny kompetencji. Dlatego egzaminy ICDL są wykonywane według ściśle określonych procedur, z wykorzystaniem globalnych sylabusów i testów praktycznych, które sprawdzają realne umiejętności użytkownika: pracę z arkuszami kalkulacyjnymi, dokumentami, narzędziami chmurowymi czy bardziej zaawansowanymi elementami, takimi jak analiza danych, IoT czy AI. Siła ICDL polega na powtarzalności i transparentności – niezależnie od tego, czy egzamin odbywa się w Polsce, Irlandii czy Singapurze, wynik oznacza dokładnie to samo.

Podobną logiką kieruje się ZSK, który działa na mocy ustawy z 2016 r. Jednak w przeciwieństwie do ICDL, ZSK nie jest pojedynczym egzaminem ani zestawem testów. To ogólnokrajowa rama, która określa zasady tworzenia, opisywania i weryfikowania kwalifikacji funkcjonujących w Polsce. Każda kwalifikacja włączona do systemu zostaje przypisana do odpowiedniego poziomu Polskiej Ramy Kwalifikacji i opisana poprzez efekty uczenia się – jasno sformułowane, mierzalne i możliwe do obiektywnej weryfikacji.

Podobnie jak w ICDL, w ZSK kluczową rolę odgrywa zasada pełnej niezależności: instytucja, która uczy, nie może egzaminować. Rozdzielenie procesu kształcenia od procesu walidacji zapewnia przejrzystość i wiarygodność systemu, a jednocześnie buduje zaufanie. Skoro egzamin nie odbywa się „u siebie", certyfikat nabiera realnej wartości – zarówno dla ucznia, pracownika, jak i pracodawcy.

Możemy sobie wyobrazić scenariusz, w którym ICDL dostarcza narzędzia do praktycznego sprawdzania cyfrowych umiejętności. ZSK zapewnia zaś formalne ramy, które pozwalają te umiejętności wpisać w krajowy i europejski system kwalifikacji. Tam, gdzie ICDL daje obiektywny dowód opanowania cyfrowych kompetencji, ZSK oferuje możliwość ich oficjalnego uznania. To właśnie dzięki temu certyfikat ICDL może być traktowany jako wiarygodne potwierdzenie części efektów uczenia się potrzebnych do zdobycia kwalifikacji włączonej do ZSK. W praktyce oznacza to, że osoba rozpoczynająca proces walidacji w ZSK nie zaczyna od zera – jeśli ma certyfikat ICDL, część jej umiejętności jest już potwierdzona. To znacząco skraca i ułatwia proces zdobywania formalnych kwalifikacji.

Ten mechanizm staje się tym bardziej potrzebny, im większa jest luka kompetencyjna – a ta w Polsce wciąż jest poważna. Europejskie analizy, w tym Digital Economy and Society Index (DESI) – Indeks Gospodarki Cyfrowej i Społeczeństwa Cyfrowego – pokazują, że mniej niż połowa dorosłych Polaków ma choćby podstawowe kompetencje cyfrowe. To zaskakujące, zwłaszcza że większość z nas korzysta z internetu każdego dnia[1].

> *Choć ZSK i ICDL działają na różnych poziomach, ich współistnienie tworzy niespodziewanie spójny ekosystem.*

Na pierwszy rzut oka może się wydawać, że mamy tu jakąś sprzeczność. W rzeczywistości jednak żadnej sprzeczności nie ma. Trzyletnie dziecko bawiące się tabletem w parku nie jest symbolem cyfrowej dojrzałości społeczeństwa. Podobnie jak osoba starsza ze smartfonem nie jest dowodem pełnego włączenia cyfrowego.

Problem tkwi w tym, że samo korzystanie z urządzeń nie oznacza posiadania kompetencji potrzebnych w miejscu pracy. Przepaść między „używaniem" a „umiejętnością" jest realna – i z roku na rok coraz głębsza. Cyfrowa codzienność stała się powszechna, ale cyfrowa biegłość nadal jest rzadkością. To właśnie dlatego rzetelna certyfikacja kompetencji ma dziś tak ogromne znaczenie.

Mamy europejskie wzory

W krajach takich jak Włochy czy Francja lukę kompetencyjną próbuje się zamykać systemowo np. poprzez włączanie certyfikacji do edukacji formalnej lub tworzenie państwowych mechanizmów finansowania egzaminów. We Włoszech certyfikacja kompetencji cyfrowych, w tym ICDL, jest obecna w systemie edukacji od wielu lat i została oficjalnie uznana przez Ministerstwo Edukacji jako standard potwierdzania umiejętności cyfrowych[2]. Jest szeroko stosowana w szkołach i instytucjach edukacyjnych, choć stanowi jedno z wielu dostępnych narzędzi rozwijania i walidacji kompetencji cyfrowych. We Francji natomiast funkcjonują różne formy certyfikacji kompetencji cyfrowych, a pracownicy mogą korzystać z indywidualnych kont szkoleniowych (Compte Personnel de Formation – CPF) w celu finansowania rozwoju umiejętności[3]. Stąd m.in. ICDL jest wpisany do krajowego rejestru kwalifikacji, co umożliwia jego finansowanie w ramach CPF, jednak stanowi jedną z wielu dostępnych kwalifikacji, a nie dominujący standard.

W obu modelach kluczowe są trzy elementy: powszechność, realna dostępność i zaufanie społeczne do zewnętrznego, niezależnego procesu certyfikacji. To one decydują, że certyfikat nie jest papierkiem „do szuflady", ale narzędziem o realnej wartości rynkowej i edukacyjnej.

W Polsce podobne rozwiązania będą nie tylko potrzebne, lecz wręcz nieuniknione. Coraz więcej instytucji edukacyjnych włącza ICDL do swoich programów, a liczba kwalifikacji trafiających do ZSK systematycznie rośnie. Szczególnego znaczenia nabiera również koncepcja mikropoświadczeń. Mikropoświadczenia od lat stanowią immanentny element certyfikacji ICDL – każda zdana część egzaminu, każdy moduł to właśnie małe, precyzyjnie zdefiniowane potwierdzenie umiejętności. Ten sam kierunek jest dziś widoczny w ZSK, gdzie mikropoświadczenia mają swoje odzwierciedlenie dzięki systemowi Odznaka+[4], wdrożonemu przez Instytut Badań Edukacyjnych. To rozwiązanie pozwala dokumentować poszczególne osiągnięcia i umiejętności w sposób cyfrowy, transparentny i łatwy do weryfikacji. Daje też możliwość budowania własnego portfolio, na który składają się zarówno kwalifikacje ZSK i ICDL, jak i pojedyncze zestawy efektów uczenia się.

Istotnym impulsem rozwojowym jest również zmiana prawa oświatowego, która umożliwiła dyrektorom szkół – szczególnie techników – włączanie do programów nauczania przygotowania uczniów do certyfikacji kwalifikacji rynkowych funkcjonujących w ZSK. To krok milowy: szkoła nie tylko uczy, lecz także przygotowuje do zdobywania zewnętrznych kwalifikacji.

Równocześnie mikropoświadczenia przestają być traktowane w Polsce jako teoretyczny koncept czy modny slogan. Coraz częściej są postrzegane jako praktyczne narzędzie nowoczesnej polityki edukacyjnej: elastyczne, skalowalne i adekwatne do tempa zmian technologicznych. Na świecie boom na mikropoświadczenia trwa od ponad dekady. Według danych opublikowanych przez platformę Accredible[5], do 2024 r.wydano tylko za jej pośrednictwem ponad 125 mln cyfrowych poświadczeń, co czyni ją największym dostawcą tego typu rozwiązań na świecie.

Jeśli te wszystkie kierunki zostaną właściwie połączone – poprzez wsparcie finansowania egzaminów, upowszechnienie wartości certyfikacji oraz stałe monitorowanie efektów – możemy stworzyć w Polsce system, który pozwoli obywatelom zdobywać i potwierdzać umiejętności w sposób przejrzysty, elastyczny i wiarygodny. To podejście daje szansę na zbudowanie spójnego ekosystemu, wzmacniającego zarówno edukację, jak i rynek pracy. Najważniejsze jednak pozostaje zrozumienie, że ICDL i ZSK nie muszą być wobec siebie konkurencją ani alternatywami. Razem tworzą spójny model, który może realnie przyspieszyć rozwój kompetencji cyfrowych w Polsce.

1 https://digital-decade-desi.digital-strategy.ec.europa.eu/

2 https://digital-decade-desi.digital-strategy.ec.europa.eu/

3 https://icdl.org/references-and-endorsements/ecdl-is-on-the-national-register-of-professional-qualifications-cpf-in-france/

4 https://odznakaplus.ibe.edu.pl/

5 https://www.accredible.com/blog/accredibles-2024-year-in-review

Sztuczna inteligencja w edukacji wyższej

Tomasz Kulisiewicz

Eksplozja modeli i narzędzi sztucznej inteligencji, jaką rozpoczęło publiczne udostępnienie ChataGPT z rodziny GPT-3.5 przez OpenAI pod koniec 2022 r., nie mogła pozostać bez wpływu na szeroko rozumianą edukację formalną i pozaformalną. Co więcej: LLMy i coraz liczniejsze narzędzia AI wręcz na naszych oczach wysadzają w powietrze cały dotychczasowy model edukacji – zwłaszcza szkolnej i akademickiej.



Tomasz Kulisiewicz

Analityk i wykładowca, autor publikacji naukowych oraz analiz dla Komisji Europejskiej, instytucji krajowych i zagranicznych. Współzałożyciel i ekspert Ośrodka Studiów nad Cyfrowym Państwem. Sekretarz Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo.

Co to jest inteligencja? Na to pytanie OpenAI GPT-5.4 odpowiada prostą definicją: inteligencja to umiejętność myślenia, wyciągania wniosków i skutecznego działania w różnych sytuacjach. „Pociągnięty za język" dodaje, że w psychologii przez inteligencję często rozumiany jest zespół zdolności obejmujących logiczne myślenie, analizowanie i porównywanie, zapamiętywanie, planowanie, rozumienie relacji między zjawiskami oraz dostosowanie się do zmian. Natomiast w odniesieniu do samego siebie wspomniany serwis określa SI jako zdolność systemu do przetwarzania informacji, uczenia się, podejmowania decyzji i rozwiązywania problemów w sposób przypominający człowieka.

Porównując własne „rozumienie" SI z ugruntowanymi przez lata definicjami inteligencji ludzkiej można przytoczyć typologię inteligencji wielorakiej zaproponowaną w 1983 r. przez Howarda Gardnera, amerykańskiego psychologa i badacza edukacji związanego z Uniwersytetem Harvarda. W swojej pracy[1] sformułował tezę, że inteligencja nie jest jedną ogólną zdolnością, lecz składa się z kilku względnie odrębnych typów. Jego teoria jest co prawda krytykowana z uwagi na słabe potwierdzenie eksperymentalne i trudności w pomiarze, nakładanie się na siebie poszczególnych typów oraz za „mieszanie" do inteligencji innych pojęć – umiejętności, talentów a nawet cech osobowości. Natomiast zdaniem wielu praktyków typologia Gardnera jest „atrakcyjna pedagogicznie". Porównanie tych dwóch podejść wskazuje, że dzisiejszej sztucznej inteligencji jest jeszcze dość daleko do inteligencji wielorakiej według Gardnera.

Typ inteligencji	Umiejętność, aktywność
językowa (werbalna)	komunikowanie się za pomocą słów
logiczno-matematyczna	liczenie, myślenie logiczne i analityczne oraz wyciąganie wniosków
muzyczna (także rytmiczna)	łatwość odbioru oraz tworzenia muzyki, muzykalność, dostrzeganie i rozumienie struktury utworów muzycznych
wizualno-przestrzenna	orientacja przestrzenna, umiejętność czytania map, wykresów i schematów, zdolność do tworzenia w umyśle obrazów, relacji przestrzennych i wizualizacji
przyrodnicza	wrażliwość ekologiczna, zdolnością dostrzegania wzorców w naturze, rozpoznawanie i kategoryzowanie obiektów przyrody, zainteresowanie otoczeniem naturalnym
ruchowa (fizyczno-kinestetyczna)	zręczność, dobra koordynacja ruchów ciała, uzdolnienia manualne i sportowe
interpersonalna	umiejętność komunikowania się i rozumienie innych ludzi, chęć do współpracy, empatia, zdolność do wchodzenia w interakcje społeczne
intrapersonalna	związana z emocjami i intuicją, umiejętność poznawania własnych uczuć i samego siebie, wysoka samoświadomość, zdolnością do autorefleksji, oceny własnego zachowania i motywacji, postrzeganie świata przez pryzmat własnej osoby

Tabela 1. Inteligencja wieloraka według Howarda Gardnera

na podstawie: https://pedagogonline.pl/inteligencje-wielorakie/

Pojęcie sztucznej inteligencji po raz pierwszy pojawiło się we wniosku badawczym z 1955 r. dotyczącym organizacji w 1956 r. słynnej konferencji w Dartmouth. John McCarthy i współautorzy postawili tezę, że inteligencję da się opisać naukowo, maszyna może ją symulować i dlatego warto badać możliwość stworzenia sztucznej inteligencji[2].

AI a tradycyjny model edukacji

Warto przypomnieć naukową podstawę modelu edukacji zdefiniowaną przez Johanna Friedricha Herbarta (1776-1841), niemieckiego filozofa, psychologa i pedagoga, twórcę założeń pedagogiki naukowej. W modelu herbartowskim szkoła ma realizować zadanie wychowania ucznia, polegające na ukształtowaniu jego charakteru z wykorzystaniem etyki i psychologii. Etyka wyznacza cele wychowania, a psychologia uzasadnia stosowanie wszelkich środków do odpowiedniego ukształtowania charakteru. Głównym środkiem jest nauczanie wychowujące polegające na przekazywaniu przez nauczyciela *ex cathedra* gotowej wiedzy i narzucające karność. Uczniowie muszą podporządkować się nauczycielowi, mają słuchać, powtarzać i uczyć się na pamięć.

Model ten, dziś mocno krytykowany za nadmierny rygoryzm i pasywność uczniów, miał jednak pewne osiągnięcia: wprowadził do pedagogiki systemowe planowanie lekcji oraz wskazał na konieczność wykorzystywania psychologii w dydaktyce. Dla utrzymania karności model ten dopuszczał jednak stosowanie

1 Gardner H., *Frames of Mind: The Theory of Multiple Intelligences*, 1983, New York: Basic. Po polsku: Gardner H., *Inteligencje wielorakie. Teoria w praktyce*, 2002, Wydawnictwo Media Rodzina, Poznań

2 (*McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. August 31, 1955*).



„Lasset die Kindlein zu mir kommen" (Pozwólcie dzieciom przyjść do mnie) lub „Pierwszy dzień w szkole" obraz niemieckiego malarza Johanna Petera Hasenclevera z 1852 r.

Źródło: https://www.stiftung-volmer.de/art-work/725

kar cielesnych, co (w różnym tempie w różnych krajach) zostało na szczęście zakazane.

Szkoła w defensywie

Część instytucji edukacji formalnej usiłuje jeszcze „nie zauważać" wpływu SI na model ich działania i często broni się zakazami wykorzystywania rozwiązań sztucznej inteligencji. Zdajemy sobie jednak sprawę, że jest to nie tylko taktyka nieskuteczna, ale nawet kontrproduktywna. Wskazują na to również moje osobiste doświadczenia.

Należę do pokolenia, któremu w pierwszych klasach szkoły podstawowej nie wolno było używać piór wiecznych (nie mówiąc już o importowanych początkowo z dalekiego Zachodu długopisach!). Musieliśmy pisać obsadkami ze stalówkami, a na pulpitach szkolnych ławek w specjalnych otworach były kałamarze z atramentem uzupełnianym przez woźnych. Obronę (traconych) pozycji kontynuowały uczelnie – na niejednej politechnice (w tym na mojej Alma Mater) w końcu lat 60. i pierwszej połowie lat 70. XX w. na egzaminach i zaliczeniach nie wolno było korzystać z kalkulatorów, jeszcze wtedy tych zwykłych[3] – wszystko liczyliśmy na suwakach logarytmicznych. Taktyka wymuszania przez system edukacji używania narzędzi poprzedniej generacji załamała się, kiedy uczniowie zaczęli przynosić do szkoły smartfony. Szkoła nie mogła im przecież kazać przynosić na lekcje telefonów stacjonarnych…

Obecnie w niektórych szkołach i krajach można korzystać ze smartfonów na lekcjach, w innych – tylko na przerwach, w jeszcze innych trzeba je zostawiać w przegródkach w szatni. Nie ma jednak wątpliwości, że upowszechnienie smartfonów spowodowało, iż dziś uczniowie i studenci mają podręczne urządzenia dostępu do znajdujących się w Internecie rozwiązań AI i nie wahają się ich używać.

Akademia i algorytmy

– Powszechne stosowanie generatywnej sztucznej inteligencji powoduje utratę przez uczelnię dotychczasowego monopolu na wytwarzanie, przetwarzanie i weryfikację wiedzy – to jedna z najważniejszych tez opracowania dotyczącego problematyki zastosowań GenAI w szkolnictwie wyższym[4] (prace zespołu DELab UW i ich autorki kilkakrotnie gościły na łamach „Domeny").

Logika operacyjna dzisiejszych rozwiązań GenAI w zasadzie bazuje na statystycznym dopasowaniu, systemy te nie potrafią jeszcze tworzyć wiedzy, choć potrafią imitować działanie intelektu. Rozwiązania AI bazujące na statystycznej predykcji mogą wspierać procesy poznawcze, ale nie mają intencji, zdolności rozumowania ani relacyjności – cech opisujących zarówno uczących się, jak i twórców wiedzy. Autorki zauważają, że GenAI zmienia reguły gry w szkolnictwie wyższym, bowiem nie jest już tylko narzędziem a wdrażanie rozwiązań AI nie jest procesem technicznym, ale „nowym elementem infrastruktury poznawczej uczelni".

Uczelnia wyższa już nie jest dystrybutorem wiedzy – musi aktywnie filtrować i korygować efekty działania AI, zwłaszcza takie, które symulują wiedzę, ale nie ponoszą za nią odpowiedzialności poznawczej.

3 Pierwszy kieszonkowy kalkulator programowalny, HP-65, pojawił się na rynku w 1974 r. Wcześniej, w latach 60. kilka firm (m. in. HP, Olivetti, Monroe, Wang) produkowało programowalne elektroniczne kalkulatory biurkowe. W pewnym zakresie programowalne były też daleko wcześniejsze (koniec XIX w.) mechanograficzne urządzenia liczące – tabulatory systemów Holleritha i Powersa.

4 Śledziewska K., Włoch R., *GenAI w szkolnictwie wyższym: Rekomendacje dla polityki publicznej*, 2025, DELab UW, Warszawa

Jest to zadanie coraz ważniejsze, bo w miarę rozwoju GenAI granice między wiedzą a jej symulacją przez LLMy są coraz mniej wyraźne. Opracowanie przywołuje wyniki badań pokazujących, że studenci przeceniają trafność odpowiedzi generowanych przez AI, a nie doceniają ryzyk wynikających np. z nieobiektywności (wynikającej głównie z niewłaściwego doboru danych treningowych modeli). Uczelnia powinna być „strażnikiem znaczenia wiedzy", uczyć nie tylko korzystania z narzędzi AI, ale przede wszystkim umiejętności ich krytycznego stosowania.

Jako jedną z propozycji odpowiedzi na wyzwania autorki przytaczają strategię CRAFT zaproponowaną przez D. Liu i S. Batesa[5]. Zgodnie z nią uczelnie powinny budować swoje podejście do rozwiązań AI wokół pięciu osi: kultury (*Culture*), reguł (*Rules*), dostępu (*Access*), oswojenia (*Familiarity*) i zaufania (*Trust*).

Autorki prezentują cztery scenariusze działania i rozwoju uczelni wobec upowszechniania się GenAI:

1. **scenariusz transformacyjny – AI jest dla studentów partnerem i symulatorem myślenia, nie uczy ich, ale pomaga im się uczyć, zaś nauczyciel akademicki pełni rolę mentora;**

2. **scenariusz dialogiczny – uczelnia uznaje obecność AI, ale traktuje ją tylko jako pomoc w analizie treści, organizacji materiału czy komunikacji, wsparcie AI polega głównie na generowaniu przykładów (przez wykładowców), na porządkowaniu pojęć i pomocy w przygotowywaniu do egzaminów (przez studentów);**

3. **scenariusz przetrwania – uczelnia nie potrafi wykorzystać AI, pozornie nic się nie zmienia, ale studenci tworzą teksty nie oceniane jakościowo, bo nauczyciele nie potrafią rozpoznawać wkładu pracy studentów; autorki podkreślają, że jest to scenariusz grożący m.in. utratą zaufania studentów do procesu edukacyjnego, pogłębianiem nierówności poznawczych oraz spadkiem zaangażowania kadry dydaktycznej;**

4. **scenariusz obojętności – uczelnia nie reaguje na obecność GenAI, nie tworzy reguł, nie prowadzi rozmów, nie edukuje; studenci korzystają z AI nie tylko bez wsparcia, czy refleksji, ale nawet tego nie ujawniając; część kadry stosuje AI, część zakazuje jej stosowania, resztą ignoruje obecność i korzystanie z AI; jest to scenariusz najgorszy z punktu widzenia roli uczelni w edukacji.**

Nierozumienie głównych reguł stosowania narzędzi AI może sprawić, że dominujące dziś zastosowania GenAI w uczelniach – generowanie streszczeń tekstów, wersji roboczych oraz parafrazowania („opowiadania treści własnymi słowami") będą prowadzić do zastępowania myślenia produkcją tekstu. Przywoływane są też analizy pokazujące, że niewielka część studentów wykorzystuje GenAI do pogłębiania zrozumienia, natomiast większość korzysta z nich jako narzędzi do wypełniania wymagań uczelnianych „na zaliczenie".

We wnioskach końcowych autorki wyraźnie zaznaczają, że uczelnia jako instytucja ma przed sobą dwie drogi. Wobec upowszechniania się GenAI może przyjąć postawę obronną – zakazywać lub ignorować, ewentualnie ograniczyć się do reagowania na pojawiające się zjawiska czy problemy. Może też pójść drugą, trudniejszą drogą – jak piszą „wziąć odpowiedzialność za

5 https://www.apru.org/resources_report/whitepaper-generative-ai-in-higher-education-current-practices-and-ways-forward/

Pora na wdrażanie wypracowanych rozwiązań

Po raz kolejny Polska Agencja Rozwoju Przedsiębiorczości (PARP) powierzyła Polskiemu Towarzystwu Informatycznemu prowadzenie Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo (w poprzedniej perspektywie finansowej PTI prowadziło Sektorową Radę ds. Kompetencji Informatyka oraz Sektorową Radę ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo). Beata Ostrowska, wiceprzewodnicząca nowej Rady, Bogdan Kościuch, dyrektor Departamentu Rozwoju Kadr w Przedsiębiorstwach w PARP oraz Wiesław Paluszyński, prezes PTI i przewodniczący nowej Rady rozmawiają na temat zmian na rynku pracy i zapotrzebowania na nowe kwalifikacje.



Beata Ostrowska

wiceprzewodnicząca Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo



Bogdan Kościuch

dyrektor Departamentu Rozwoju Kadr w Przedsiębiorstwach w PARP



Wiesław Paluszyński

prezes PTI, Przewodniczący Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo

Beata Ostrowska: PTI ma już doświadczenie w realizacji projektów rad sektorowych. Porozmawiamy o tym, w jaki sposób wnioski wyniesione z poprzedniej edycji wpływają na obecne działania Rady?

Wiesław Paluszyński: Odpowiedź nie jest prosta, ponieważ poprzednie lata były absolutnie nietypowe. Spora część aktywności rad została zdominowana przez pandemię COVID-19, która drastycznie przyspieszyła cyfryzację i wymusiła nagły wzrost kompetencji pracowników w zakresie pracy zdalnej. Musimy jednak pamiętać, że nasza uwaga skupia się na małych i średnich przedsiębiorstwach (MŚP), a nie korporacjach.

Dziś sytuacja jest inna: rozwiązania, które wczoraj były nowinkami, obecnie są standardem. Przed radami stoi nowe wyzwanie – musimy zdefiniować obszary kompetencyjne w dobie sztucznej inteligencji (AI) i rygorystycznych regulacji cyberbezpieczeństwa. Naszą rolą jest wskazanie PARP-owi, gdzie należy ulokować strumienie pieniędzy, aby polscy przedsiębiorcy odnieśli maksymalne korzyści. Oprócz czysto technicznych umiejętności niezbędne są teraz kompetencje prawne, by MŚP nie

Sektorowa Rada
ds. Kompetencji
IT, Telekomunikacja
i Cyberbezpieczeństwo

wypadały z łańcuchów dostaw większych podmiotów z powodu braku zgodności z nowymi przepisami.

B.O.: A jak z perspektywy PARP wygląda rola rad sektorowych w całym systemie rozwoju kompetencji w Polsce?

Bogdan Kościuch: System Rad ds. Kompetencji został wprowadzony przez PARP w 2016 r. w celu wspierania rozwoju kompetencji na rynku pracy oraz integracji z biznesem. Rady, skupiając w swoim gronie przedstawicieli przedsiębiorców, instytucji edukacyjnych, badawczych oraz administracji publicznej, zajmują się na bieżąco analizą potrzeb kompetencyjnych w swoich sektorach, monitorują zmiany i ich wpływ na wymagane kompetencje czy kwalifikacje. Na tej podstawie przygotowują rekomendacje dotyczące kształcenia i szkolenia zawodowego. Mogą również inicjować zmiany legislacyjne mające na celu lepsze dostosowanie systemu edukacji przygotowującego przyszłych pracowników do zmian zachodzących w gospodarce. Innymi słowy, to rady – ściśle powiązane z poszczególnymi sektorami gospodarki – dysponują kluczowymi informacjami na temat wymaganych przez przedsiębiorców kompetencji i proponują na bieżąco rozwiązania mające przyczynić się do wypełnienia luk kompetencyjnych.

B.O.: W jaki sposób prace Rady przekładają się w praktyce na konkretne zmiany, np. w systemie edukacji, szkoleniach czy podejściu pracodawców do kompetencji?

W.P.: Widoczne są m.in. w dopasowaniu tematów szkoleń do realnych potrzeb rynku. Potwierdzają to dane od operatorów szkoleń – rekomendowane przez nas obszary cieszyły się dużym zainteresowaniem, a zaplanowane działania zostały w pełni zrealizowane, co potwierdza trafność diagnozy kompetencyjnej.

Jednocześnie widzimy wyzwania związane z rosnącą rolą kompetencji horyzontalnych, zwłaszcza w obszarze cyberbezpieczeństwa. Dotyczą one nie tylko firm z sektora IT, telekomunikacji czy cyberbezpieczeństwa, lecz także większości przedsiębiorstw. To oznacza, że w kolejnych latach konieczne będzie lepsze uwzględnienie tych potrzeb w systemie edukacji i szkoleń – także poza wąsko definiowanymi sektorami.

B.O.: W jakich obszarach zidentyfikowano największe niedopasowania kompetencyjne w obszarze IT, telekomunikacji i cyberbezpieczeństwa?

B.K.: Ostatnie badania Sektorowej Rady ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo identyfikują kilkadziesiąt luk kompetencyjnych, z którymi obecnie zmaga się sektor. Rada wskazuje, jak ma wyglądać usługa rozwojowa wspierająca uzyskanie tej kompetencji, do kogo ma być skierowana, jakie mają być efekty uczenia się i kryteria jej walidacji oraz cena tej usługi. Na tej podstawie będą organizowane szkolenia dla pracowników firm z sektora.

Luki kompetencyjne zidentyfikowane przez Sektorową Radę ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo:

- **tworzenie i rozwój rozwiązań z zakresu sztucznej inteligencji (szacowana skala niedoboru kompetencji dotyczy 6,5 tys. osób);**
- **wykorzystanie sztucznej inteligencji (AI): w programowaniu (6,5 tys.; w testowaniu oprogramowania – 1,5 tys.) ; w cyberbezpieczeństwie (5 tys.); w zarządzaniu sieciami teleinformatycznymi (1 tys.);**
- **zarządzanie cyberbezpieczeństwem (2 tys. w przypadku specjalisty do 2,5 tys. w przypadku eksperta i menedżera);**
- **administrowanie siecią lokalną LAN (500);**
- **programowanie na poziomie podstawowym i zaawansowanym (400);**
- **testowanie oprogramowania (1,5 tys.);**
- **instalowanie i konfigurowanie sieci i urządzeń telekomunikacyjnych (2,5 tys.);**
- **tworzenie i rozwój rozwiązań do analizy dużych zbiorów danych (3,5 tys.);**
- **projektowanie i tworzenie rozwiązań chmurowych (2,5 tys.).**

B.O.: Jak zatem identyfikować kompetencje przyszłości, by nadążać za tempem zmian technologicznych? Czy to w ogóle możliwe w dzisiejszym świecie?

W.P.: Najpierw analizujemy kierunki rozwoju technologii, a następnie przekładamy je na kompetencje. Konferencja związana z istotnym wydarzeniem branżo-

wym – obchodami Światowego Dnia Telekomunikacji i Społeczeństwa Informacyjnego (z tej okazji ukazuje się ten numer specjalny „Domeny") – dobrze pokazuje nasze podejście. Dwa pierwsze bloki poświęcone są właśnie rozwojowi nowych technologii i perspektywom ich zastosowania, a trzeci (organizowany przez Radę) wskazuje niezbędne kompetencje.

Jednym z kluczowych obszarów jest dziś sztuczna inteligencja. Nie chodzi już tylko o proste korzystanie z narzędzi, ale o umiejętność świadomego i odpowiedzialnego ich wykorzystywania, rozumienia ograniczeń, takich jak tzw. halucynacje, zadawanie właściwych pytań czy budowanie bardziej zaawansowanych zastosowań, np. bazujących na AI agentowej. To wyzwanie dotyczy także większych firm z sektora MŚP, w których skala i złożoność wdrożeń są znacznie większe. W efekcie rośnie zapotrzebowanie zarówno na kompetencje techniczne, jak i miękkie.

Drugim kluczowym obszarem jest, wspomniane wcześniej, cyberbezpieczeństwo. W tym przypadku ważne jest szybkie reagowanie na zmieniające się zagrożenia i korzystanie z aktualnych analiz rynku, np. opracowań publikowanych przez NASK. To pozwala lepiej identyfikować potrzeby kompetencyjne i dostosowywać działania szkoleniowe do realnych wyzwań.

Ostatnio zapytano mnie, czego powinna uczyć się młodzież na poziomie szkoły średniej, aby skutecznie korzystać z narzędzi AI. Kluczowe jest przede wszystkim rozwijanie podstawowych kompetencji, które później pozwolą świadomie korzystać z narzędzi bazujących na sztucznej inteligencji. To przede wszystkim matematyka, jako sposób formalnego opisu rzeczywistości, oraz język polski – pojmowany jako umiejętność czytania ze zrozumieniem, analizy treści i precyzyjnego formułowania myśli.

B.O.: Ze swojej strony dodałabym, że równie ważna jest umiejętność analizy i rozwiązywania problemów, która u młodzieży często wymaga wzmocnienia. Jak prezentuje się przestrzeń do dalszego rozwoju systemu rad sektorowych?

B.K.: Odwołam się do silnych stron rad. Po pierwsze – obejmują większość sektorów polskiej gospodarki. Po drugie – mają realny, aktywny wpływ na system edukacji poprzez oddziaływanie na program, sposób nauczania, zakres i poziom kwalifikacji absolwentów, a więc także potencjalnych przyszłych pracowników. Po trzecie – rady wzmacniają poczucie odpowiedzialności i zaangażowanie przedsiębiorców w rozwój edukacji – pracodawcy nie występują wyłącznie w charakterze zgłaszających wymagania klientów, lecz przejmują na siebie współodpowiedzialność za kształcenie kadr. Po czwarte – działalność rad wpływa pośrednio na obniżenie kosztów HR przedsiębiorstw, bo mogą łatwiej i szybciej zatrudniać specjalistów posiadających potrzebne umiejętności bez konieczności długotrwałego szkolenia osób nowoprzyjętych. Ogranicza to ryzyko wakatów na istotnych stanowiskach, a w efekcie – obniża ryzyko przestojów czy niedotrzymania terminów. Po piąte – rady mogą szybko reagować na zmieniające się warunki i wymagania, w jakich funkcjonuje dany sektor. Jestem przekonany, że system rad sektorowych będzie obejmował nowe sektory polskiej gospodarki, umacniał swoją eksperckość i rolę w rozwoju kompetencji niezbędnych na polskim rynku pracy.

B.O.: Na ile skutecznie udaje się dziś łączyć perspektywę biznesu, edukacji i administracji? Co jest największym wyzwaniem w tej współpracy? Ja widzę silosy, które nie współpracują lub współpracują za rzadko i w zbyt wąskim zakresie.

W.P.: W tej chwili kluczowym wyzwaniem jest aktywne włączenie się Rady w opiniowanie zmian w systemie edukacji formalnej zarówno na poziomie szkoły podstawowej, jak i średniej. To właśnie tam kształtują się podstawy, które później powinny być uzupełniane edukacją pozaformalną i szkoleniami.

Istotnym problemem pozostaje niespójność systemowa, szczególnie w obszarze ram kwalifikacji, które miały zapewniać interoperacyjność między różnymi sektorami i resortami. W praktyce obserwujemy tendencje do tworzenia równoległych, silosowych, jak powiedziałaś, rozwiązań, co osłabia spójność całego systemu potwierdzania kompetencji.

Dlatego ważnym zadaniem Rady jest wzmacnianie podejścia bazującego na wspólnych ramach oraz dbanie o to, aby wypracowane kompetencje były formalnie uznawane i mogły być realnie wykorzystywane przez pracodawców – np. w procesach rekrutacyjnych czy przy określaniu wymagań wobec pracowników.

B.O.: W pełni się zgadzam z potrzebą spójności systemu. Zintegrowany System Kwalifikacji jest dużym, dobrze zaprojektowanym przedsięwzięciem, w które zainwestowano istotne środki, także unijne. Jednak w praktyce jego wykorzystanie nadal pozostaje ograniczone. Brakuje dziś silnego „zakotwiczenia" ZSK zarówno w politykach publicznych, jak i w świadomości przedsiębiorców czy systemie edukacji. W efekcie narzędzie, które mogłoby odgrywać rolę wspólnego punktu odniesienia dla kompetencji od edukacji aż po rynek pracy, nie jest powszechnie rozpoznawalne ani wykorzystywane. A szkoda, bo ZSK mogłoby realnie pełnić funkcję praktycznego przewodnika: wskazywać, jakie kompetencje są potrzebne na konkretnych stanowiskach, jak je zdobywać oraz gdzie i w jaki sposób je potwierdzać. Wzmocnienie jego roli mogłoby znacząco poprawić przejrzystość rynku kompetencji i ułatwić zarówno pracownikom, jak i pracodawcom podejmowanie świadomych decyzji.

W.P.: Warto dodać, że jednym z realnych celów działania Rady w tej kadencji powinno być nie tylko rozwijanie dialogu między edukacją a biznesem, lecz przede wszystkim „operacjonalizacja" Zintegrowanego Systemu Kwalifikacji w praktyce rynkowej. Chodzi o to, aby – podobnie jak w poprzednich inicjatywach, np. podczas konferencji EduMixer – konsekwentnie pokazywać, że ZSK jest realnym narzędziem, z którego można i warto korzystać. Nie tylko w edukacji, lecz także w decyzjach biznesowych: rekrutacji, planowaniu kompetencji czy rozwoju organizacji.

W tym kontekście zasadne wydaje się także podjęcie bardziej systemowych działań – być może we współpracy z PARP – ukierunkowanych na wzmocnienie roli administracji publicznej, w tym ministerstwa odpowiedzialnego za rynek pracy i politykę zatrudnienia. Nie tylko w zakresie regulacji czy kontroli, lecz także w obszarze aktywnych rekomendacji dla pracodawców, wskazujących, gdzie i jak definiować wymagania kompetencyjne oraz jak korzystać z istniejących narzędzi systemowych.

Wydaje się, że to jest dziś ważniejsze niż ogólne postulaty współpracy biznesu z edukacją, bo na poziomie szkół i uczelni pewne mechanizmy już funkcjonują. Natomiast brakuje spójnego ekosystemu dla pracodawców, który pozwalałby im w praktyce korzystać z dostępnych narzędzi i odnosić je do realnych potrzeb rynku pracy. I właśnie w tym obszarze widziałbym jedno z kluczowych zadań Rady – nie tyle tworzenie kolejnych deklaracji, co realne domykanie systemu kompetencji w praktyce gospodarczej.

B.O.: Jak przedsiębiorcy mogą realnie korzystać z efektów prac rad sektorowych? Co powiedziałby PARP firmom, które jeszcze nie angażują się w ten system?

B.K.: Kompetencje pracowników muszą odpowiadać aktualnym wymaganiom przedsiębiorców. Nierzadko bowiem umiejętności i kompetencje pracowników w danej branży mają się nijak do oczekiwań przedsiębiorców. Każda z 29 działających rad sektorowych przygotowuje i corocznie aktualizuje rekomendacje, czyli kluczowe z punktu widzenia danego sektora dokumenty, które zawierają konkretne i aktualne informacje dotyczące tego, jakich kompetencji bądź kwalifikacji brakuje aktualnie w ramach danego sektora. Następnie te informacje trafiają do podmiotów zajmujących się organizacją szkoleń czy kursów, które rozwijają ofertę szkoleniową w tym zakresie. W rezultacie każdy podmiot prowadzący działalność gospodarczą (niezależnie od jego wielkości) może uzyskać dofinansowanie dla swoich pracowników lub pracownic, aby poprzez uczestnictwo w kursie czy szkoleniu mogli oni podnosić dotychczasowe kompetencje lub nabywać nowe. To są właśnie realne efekty działalności rad sektorowych. Warto dodać, że wkład własny przedsiębiorcy to co najmniej 20% kosztów usługi szkoleniowej, a można go wnieść zarówno w formie opłaty, jak i w postaci kosztów wynagrodzeń uczestników/uczestniczek szkoleń, gdy usługa szkoleniowa odbywa się w godzinach pracy. To wymierna korzyść dla przedsiębiorcy.

B.O.: Zastanówmy się, jak będzie wyglądał rynek kompetencji w obszarze IT, telekomunikacji i cyberbezpieczeństwa w perspektywie najbliższych 3–5 lat i jaką rolę w tym procesie powinny odegrać rady sektorowe?

B.K.: To bardzo trudne zadanie. Czy 5 lat temu można było przewidzieć tak daleko idącą ingerencję sztucznej inteligencji w nasze życie?

W mojej ocenie w perspektywie najbliższych 3–5 lat będziemy obserwować wzrastające zapotrzebowanie na specjalistów z zakresu cyberbezpieczeństwa, a co za tym idzie wszelkich kompetencji z tym związanych. Wraz z postępującą cyfryzacją wszystkich aspektów życia gospodarczego i społecznego rośnie zarówno liczba, jak i stopień zaawansowania cyberzagrożeń. Ataki hakerskie czy kradzieże danych dotykają już nie tylko przedsiębiorców i instytucji, coraz częściej uderzają również w osoby fizyczne. Poszukiwane kompetencje obejmą w tej sytuacji wiele dziedzin, m.in.: zaawansowane zarządzanie ryzykiem technologicznym i operacyjnym, zapewnienie zgodności z obowiązującymi normami i regulacjami, projektowanie i implementacja nowoczesnych architektur bezpieczeństwa, zabezpieczanie aplikacji webowych i mobilnych, ochrona infrastruktury chmurowej, a także szybkie i skuteczne reagowanie na incydenty bezpieczeństwa oraz prowadzenie dochodzeń cyfrowych. Warto dodać, że całkiem niedawno (26 marca b.r.) rozporządzeniem Ministra Edukacji Narodowej wprowadzono w Polsce nowy zawód – technik cyberbezpieczeństwa.

Niezwykle istotny będzie również rozwój kompetencji związanych ze sztuczną inteligencją. Sztuczna inteligencja wpływa na biznes niemal każdej branży i wielu przedsiębiorców upatruje w niej szansę m.in. na automatyzację procesów, możliwości wdrożenia nowych modeli bizneso-

wych czy zbudowanie przewagi konkurencyjnej. Sztuczna inteligencja i uczenie maszynowe stają się fundamentalnym elementem transformacji cyfrowej w niemal każdej branży, a wciąż niewielu pracowników ma niezbędne umiejętności do wdrażania i pracy z takimi systemami. Zaawansowane modele językowe, platformy do tworzenia treści multimedialnych czy inteligentni asystenci programowania rewolucjonizują metody pracy programistów, analityków danych, testerów oprogramowania, a nawet specjalistów od marketingu. W tym kontekście kluczowe będą kompetencje związane nie tylko z prostym użytkowaniem tych wymienionych narzędzi, lecz także z głębszym rozumieniem zasad ich działania.

Kolejny niezwykle istotny obszar to big data i zaawansowana analityka danych. W epoce informacyjnej dane stały się jednym z najcenniejszych aktywów każdej organizacji, a umiejętność ich efektywnego zbierania, bezpiecznego przechowywania, inteligentnego przetwarzania, dogłębnej analizy i klarownej wizualizacji jest absolutnie kluczowa dla podejmowania trafnych decyzji strategicznych i operacyjnych. W tej sytuacji niezbędne będą kompetencje związane z obsługą narzędzi ETL (*Extract, Transform, Load*), znajomością różnorodnych systemów bazodanowych, w tym relacyjnych i NoSQL, a także praktyczną umiejętnością programowania w językach takich jak Python.

No i na koniec nie należy zapominać o rozwoju chmur obliczeniowych i rozwiązań w modelu *cloud-native*. Kluczowe kompetencje będą dotyczyć obsługi platform chmurowych, a także technologii wspierających, jak konteneryzacja i projektowanie architektury opartej na mikroserwisach.

Rady sektorowe muszą zatem wnikliwie przyglądać się zachodzącym zmianom w sektorze IT, telekomunikacji i cyberbezpieczeństwa, reagować i na nie, i na sygnały pochodzące od przedsiębiorców.

W.P.: Zgadzam się, że rozwój kompetencji będzie koncentrował się przede wszystkim wokół dwóch głównych obszarów: powszechnego wykorzystania narzędzi sztucznej inteligencji oraz cyberbezpieczeństwa.

Z perspektywy przedsiębiorców kluczowe będzie nie tylko wdrażanie nowych technologii, lecz także budowanie przewagi konkurencyjnej na rynku europejskim poprzez rozwój kompetencji pracowników, zarówno w zakresie bezpiecznego korzystania z AI, jak i świadczenia usług cyberbezpieczeństwa.

Szczególnie istotna stanie się umiejętność pracy z danymi – ich analiza i zapewnienie jakości, ponieważ to od jakości danych w dużej mierze zależy skuteczność systemów sztucznej inteligencji. W tym obszarze już dziś widoczny jest deficyt specjalistów.

Równolegle rosnąć będzie znaczenie kompetencji krytycznego myślenia i zdrowego rozsądku – zdolności oceny wyników generowanych przez AI i ich adekwatności do realnych potrzeb biznesowych.

B.O.: Podsumowując, mamy obecnie do dyspozycji dobrze zdiagnozowane potrzeby rynku, rozwinięte narzędzia systemowe oraz rosnącą świadomość zmian technologicznych. Wydaje się więc, że kolejnym krokiem nie jest już tylko analiza, lecz konsekwentne wdrażanie wypracowanych rozwiązań. W dużej mierze mamy już gotowy „plan działania" dla sektora – teraz kluczowe jest jego skuteczne wykorzystanie: w edukacji, szkoleniach i praktyce rynkowej. I to właśnie tutaj upatruję szczególnej roli Sektorowej Rady ds. Kompetencji IT, Telekomunikacji i Cyberbezpieczeństwa w najbliższych latach.



Michał Kanownik

prezes Związku Cyfrowa Polska, wiceprzewodniczący
Sektorowej Rady ds. Kompetencji IT,
Telekomunikacja i Cyberbezpieczeństwo

Sektorowa Rada ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo odgrywa ważną rolę w budowaniu cyfrowych kompetencji w Polsce – skutecznie łączy ze sobą świat biznesu, edukacji i administracji. Jako wiceprzewodniczący Rady mogę powiedzieć wprost: jej największa wartość tkwi w tym, że potrafi trafnie rozpoznać, czego rynek pracy naprawdę potrzebuje, i przełożyć to na konkretne wskazówki dla szkół, uczelni i decydentów.

Fundamentem naszej pracy jest bezpośredni kontakt z przedsiębiorcami. Dzięki temu wiemy na bieżąco,

Fundusze Europejskie dla Rozwoju Społecznego | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską

Projekt Sektorowa Rada ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo jest współfinansowany w ramach programu Europejskiego Funduszu dla Rozwoju Społecznego na lata 2021–2027 współfinansowanego ze środków Europejskiego Fundusz Społecznego Plus.

jakich kompetencji brakuje dziś i jakie będą potrzebne jutro w IT, telekomunikacji i cyberbezpieczeństwie. To pozwala nam nie tylko reagować na już istniejące luki kadrowe, lecz także wyprzedzać zmiany wynikające z postępu technologicznego czy rosnącej roli cyberbezpieczeństwa. Rada jest więc pomostem między dynamicznym rynkiem a systemem edukacji, który z natury zmienia się wolniej. Szczególnie zależy nam na tym, żeby firmy i uczelnie faktycznie ze sobą rozmawiały i współpracowały. Efekty są wymierne: programy nauczania lepiej odpowiadają realiom rynku, rośnie rola kształcenia praktycznego, a nauka w miejscu pracy staje się czymś normalnym. Współpraca z Branżowym Centrum Umiejętności daje nam dodatkową przestrzeń do testowania nowych podejść i szybkiego wdrażania tego, co działa.

Ze strony Związku Cyfrowa Polska szczególnie doceniamy to, że Rada regularnie aktualizuje rekomendacje dotyczące rozwoju kadr. To realne wsparcie zarówno dla firm planujących szkolenia pracowników, jak i dla urzędników projektujących programy pomocowe. Ważne są też działania promujące ciągłe uczenie się i podnoszenie kwalifikacji, bo w branży technologicznej stanie w miejscu oznacza cofanie się.

Wpływ Rady na cyfrowe kompetencje Polaków jest realny i widoczny. Budujemy ekosystem, w którym edukacja i gospodarka wzajemnie na siebie reagują. A to dobra wiadomość zarówno dla pracowników, firm, jak i dla konkurencyjności całej polskiej gospodarki.



prof. dr hab. Grażyna Szpor

kierownik Katedry Prawa Informatycznego Wydziału
Prawa i Administracji UKSW wiceprzewodnicząca
Sektorowej Rady ds. Kompetencji IT,
Telekomunikacja i Cyberbezpieczeństwo

Wpływ Rady na rozwój kompetencji obejmuje diagnozowanie potrzeb i działania redukujące deficyty. Członkowie i eksperci Rady brali aktywny udział w kształtowaniu modelu regulacyjnego transformacji cyfrowej. Sporządzano opinie i rekomendacje do projektów wielu aktów prawnych, m.in. ustawy z 12 lipca 2024 r. – Prawo komunikacji elektronicznej, uchylającej ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz gruntownie nowelizowanej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwracając uwagę na nowe wyzwania i uwarunkowania skuteczności regulacji. Do podnoszenia poziomu kompetencji mobilizuje obecnie m.in. ustawowy wymóg corocznego udziału kierowników podmiotów kluczowych i ważnych w szkoleniach z zakresu cyberbezpieczeństwa, którego niedopełnienie może skutkować nałożeniem na nich kary pieniężnej (art. 8e i art. 73a ustawy o ksc), a także szereg innych instrumentów prawnych.

Rada przyczynia się do intensyfikacji współpracy między biznesem, edukacją i administracją m.in. w ramach rozwijania Zintegrowanego Systemu Kwalifikacji w Polsce. Z udziałem interesariuszy opracowywane i popularyzowane były trzy sektorowe ramy kwalifikacji: dla informatyki, telekomunikacji i cyberbezpieczeństwa, obejmujące specyficzne aspekty wiedzy, umiejętności i kompetencji społecznych. Z perspektywy środowiska naukowego istotne są wspólne projekty badawczo-wdrożeniowe, aktualizowanie programów studiów oraz uruchamianie nowych kierunków i form kształcenia, uwzględniających zarówno aktualne potrzeby rynku pracy, jak i trendy rozwoju, zwłaszcza związane z systemami sztucznej inteligencji.

Szczególnie istotne dla przyszłości są działania Rady zmierzające do rozpoznania oraz uwzględnienia w systemie edukacji formalnej i pozaformalnej potrzeb rynku pracy wynikających z nowych obowiązków prawnych nałożonych na podmioty gospodarcze. Dotyczą one m.in. usług cyfrowych, systemów sztucznej inteligencji, cyberbezpieczeństwa, infrastruktury krytycznej czy cyberodporności produktów z elementami cyfrowymi. Nowe wyzwania wiążą się przy tym z horyzontalnym charakterem unijnych regulacji, znacznie wykraczającym poza grupy przedsiębiorców prowadzących działalność w określonych 8 kodami sekcjach PKD 2007, które zostały zaliczone do sektora IT, telekomunikacji i cyberbezpieczeństwa (ITCB) w projekcie realizowanym przez Polskie Towarzystwo Informatyczne na podstawie umowy z PARP (nr FERS.01.10-IP.09-0010/25). Rozważenia zatem wymaga poszerzenie zakresu planowanego na lata 2025–2029 działania Rady ds. Kompetencji Sektora IT, Telekomunikacja i Cyberbezpieczeństwo.



Światowy Dzień Telekomunikacji i Społeczeństwa Informacyjnego 2026 oraz 45-lecie PTI

INFORMATYKA 2026

oczami Polskiego Towarzystwa Informatycznego

DOKONANIA, PERSPEKTYWY, WYZWANIA

14 maja, Warszawa

45 PTI POLSKIE TOWARZYSTWO INFORMATYCZNE

Organizatorzy i partnerzy

45 PTI POLSKIE TOWARZYSTWO INFORMATYCZNE

CYFROWY BIZNES

Sektorowa Rada ds. Kompetencji IT, Telekomunikacja i Cyberbezpieczeństwo

NOT

SEP

Patronat Honorowy

Ministerstwo Cyfryzacji

Minister Edukacji

Marcin Kulasek Minister Nauki i Szkolnictwa Wyższego

Ministerstwo Rozwoju i Technologii

Ministerstwo Funduszy i Polityki Regionalnej

Polska Agencja Rozwoju Przedsiębiorczości

ITU

Sponsorzy

IBM

kyndryl

AZ frame

Patronat medialny

NAUKA W POLSCE

Teleinfo24 NOWE TECHNOLOGIE DLA BIZNESU

PTI Domena
nr 2/2026

Wydawca:
Polskie Towarzystwo Informatyczne

Zarząd Główny:
ul. Solec 38 lok.103
00-394 Warszawa
NIP: 522-000-20-38
tel.: +49 22 838 47 05
e-mail: pti@pti.org.pl

Redaktor naczelna:
Anna Kniaź
(anna.kniaz@pti.org.pl)

Rada Programowa „Domeny":
Wiesław Paluszyński
– przewodniczący Rady

Marek Bolanowski
Marian Bubak
Beata Chodacka
Bogusław Dębski
Wojciech Kiedrowski

Współpraca redakcyjna:
Tomasz Kulisiewicz

Korekta:
Jolanta Jamiołkowska

Skład i opracowanie graficzne:
Agencja HEADOUT
Headout

Wszystkie teksty udostępniamy na licencji Creative Commons
Uznanie autorstwa
-Użycie niekomercyjne
-Na tych samych warunkach 4.0