NUMER 4/2021

BIULETYN PTI

POLSKIEGO TOWARZYSTWA INFORMATYCZNEGO

ISSN 2719-8472

HUAWEI A SPRAWA POLSKA

OD POLICYJNYCH RADIOTELEFONÓW PO 6G

Roboty nie tylko spawają

O ALGORYTMACH INACZEJ

O nowej Sekcji Informatyki Szkolnej pisze Beata Chodacka

Spis treści

Biuletyn PTI
nr 4/2021

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 Biuletynu PTI:
Wojciech Kiedrowski
– przewodniczący Rady
Tomasz Klasa
Jarosław Kowalski
Beata Ostrowska
Marcin Paprzycki

Współpraca redakcyjna:
Tomasz Kulisiewicz

Korekta:
Jolanta Jamiołkowska

Skład i opracowanie graficzne:
Agencja HEADOUT

W 2021 r. próbowaliśmy spojrzeć na informatykę oczami Stanisława Lema. Będziemy zapewne powracali do jego filozoficznych wizji w kolejnych latach, bo w zadziwiający sposób pozostają wciąż aktualne – polecam najnowszą książkę „Głos Pana Lema" autorstwa Pawła Okołowskiego.

Nadal współdzielimy z Lemem nasze obawy, w tym związane z rozwojem sztucznej inteligencji w powiązaniu z problematyką otwartych danych, niezbędnych dla jej „nauczania". Każda nowa koncepcja zastosowania SI budzi stare wątpliwości, a dyskusja o konsekwencjach jej wdrożenia jak w soczewce pokazuje wiele dylematów związanych z tymi implementacjami. Aktualne wciąż pozostaje pytanie, czy my naprawdę jesteśmy na etapie wdrażania sztucznej inteligencji? Gdzie skończy się uczenie maszynowe, a zacznie prawdziwa sztuczna inteligencja i ile „człowieczeństwa" wówczas zdołamy ocalić. Pośrednio próbowaliśmy odpowiedzieć na to pytanie, wybierając transhumanizm na wiodący temat naszej Gali 40-lecia PTI.

Już w latach 60. XX w. w swojej „Summa technologiae" Lem przepowiedział pojawienie się sztucznej inteligencji, którą nazwał fantomatyką. Za fantomatykę uważał głównie rozwój biotechnologii z przewagą inżynierii genowej. Dostrzeżone przez Lema zagrożenia brzmią zadziwiająco znajomo: „(...) Świat fantomatyczny jest światem całkowitego osamotnienia (...) Żadna cywilizacja nie może się «w pełni sfantomatyzować». Gdyby bowiem wszyscy jej członkowie jęli przeżywać od pewnego momentu wizje fantomatyczne, świat realny tej cywilizacji zatrzymałby się i zamarł (...)". Popatrzmy na otaczającą nas rzeczywistość i już widoczne zmiany społeczne, jakie przyniosła praca zdalna…

Krzątając się wokół spraw niewątpliwie ważnych: tworzenia środowiska wymiany doświadczeń dla nauczycieli informatyki, uruchamiania nowych obszarów certyfikacji kwalifikacji i kompetencji w zakresie cyberbezpieczeństwa oraz licznych konkursów, konferencji i webinariów, musimy jednak mieć na uwadze pytanie nadrzędne: dokąd – jako informatycy – prowadzimy naszą cywilizację?

Nowym forum do wymiany opinii na ten temat będzie pismo problemowe Polskiego Towarzystwa Informatycznego „Domena", które zastąpi dotychczasowy „Biuletyn PTI". Zamierzamy przeznaczyć w nim więcej miejsca na treści związane ze społecznymi implikacjami rozwoju technologii.

Kolejne spotkanie czeka nas więc w pierwszym kwartale 2022 r. na łamach „Domeny". Zapraszam i życzę w nadchodzące dni Świąt Bożego Narodzenia i Nowego Roku wiele radości w gronie Rodziny oraz okazji do pozytywnych przemyśleń

Wiesław Paluszyński
prezes PTI

Huawei a sprawa polska

„Zagrożenia dla cyberbezpieczeństwa sieci telekomunikacyjnych w Polsce ze strony potencjalnych dostawców wysokiego ryzyka" to najnowsza ekspertyza Polskiego Towarzystwa Informatycznego. Z jej autorami: Wiesławem Paluszyńskim i Jarosławem Mojsiejukiem rozmawia Anna Kniaź.

Wiesław Paluszyński

Prezes Polskiego Towarzystwa Informatycznego, wiceprezes Polskiej Izby Informatyki i Telekomunikacji. Członek Rady Cyfryzacji poprzedniej kadencji i ekspert Rady w obecnej kadencji. Prezes firmy Trusted Information Consulting. Były Dyrektor Departamentu Analizy Zagrożeń w Biurze Bezpieczeństwa Narodowego.

Jarosław Mojsiejuk

Prawnik i manager IT z ponad dwudziestoletnim stażem w zakresie bezpieczeństwa i cyberbezpieczeństwa. Były Wiceprzewodniczący Komitetu Administracji Cyfrowej i Koordynator Zespołu Cyberbezpieczeństwa Polskiej Izby Informatyki i Telekomunikacji, wieloletni członek władz tej Izby. Ekspert Rady ds. Cyfryzacji ubiegłej i obecnej kadencji, członek Komitetu Cyberbezpieczeństwa ZCP (ZIPSEE).

Kontrolę nad bardzo dużą częścią polskiej infrastruktury telekomunikacyjnej – sieciami szerokopasmowymi i lokalnymi – mają w Polsce firmy chińskie. Dlaczego więc ocena wiarygodności dostawcy stała się tak gorącym tematem dopiero przy budowie sieci 5G?

Wiesław Paluszyński: Sieć nowej generacji 5G to podstawa do budowy znacznie większego spektrum usług. Moduły telekomunikacyjne będą warunkować rozwój przemysłu 4.0, technologii bazujących na Internecie Rzeczy czy sztucznej inteligencji. Niestety, kolejne generacje sieci radiowych wraz z nowymi możliwościami niosą także i nowe zagrożenia. Technika segmentowania (network slicing) pozwala na budowę wielu równoległych, odizolowanych – fizycznie lub logicznie – sieci. Oferowały to już sieci VPN, ale technologia 5G oferuje możliwość wykreowania podsieci o odpowiednich parametrach technicznych niezbędnych do obsługi konkretnej klasy aplikacji sieciowych 5G. Mogą one wywierać szkodliwy wpływ na wiele rzeczywistych procesów (samochody autonomiczne, procedury i sprzęt medyczny, urządzenia Internetu Rzeczy), a nawet na krytyczną infrastrukturę krajową.

W przypadku technologii 5G dostawcy rozwiązań uzyskają dostęp nie tylko do informacji związanych z zarządzaniem siecią, ale także do wielu innych, w tym o charakterze strategicznym dla bezpieczeństwa państwa. Zapewnienie cyberbezpieczeństwa sieci 5G wymaga więc całościowej oceny

ryzyk związanych z: budową sieci, dostawcami urządzeń i technologii oraz warunkami eksploatacji sieci.

Niezwykle ważne są uwarunkowania związane z wiarygodnością dostawcy, w tym ocena wpływu czynników zewnętrznych na jego działanie. Dlatego zagrożenia ze strony organów państw mających interes w przejmowaniu jak największych ilości danych w celach wywiadowczych czy ekspansji gospodarczej bezwzględnie należy uwzględniać przy analizie bezpieczeństwa budowy sieci nowej generacji.

Jarosław Mojsiejuk: Dyskusję na temat pojęcia i zakresu uznawania za dostawcę wysokiego ryzyka (DWR) zapoczątkowały w Polsce kolejne akty i decyzje organów UE, a rozgorzała ona na dobre w chwili pojawienia się projektów nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Tej dyskusji dodatkowych kolorów niewątpliwie przydała sytuacja międzynarodowa, w tym rosnące ryzyko konfliktów dotyczących Polski. Pomału dociera do nas, że na sieci telekomunikacyjne trzeba patrzeć jak na zasób strategiczny i zdawać sobie sprawę, że najnowsza generacja technologii ma dla rozwoju i bezpieczeństwa Polski takie samo znaczenie, jak dostęp do podstawowych surowców energetycznych. Uzależnienie się od dostawców ropy i gazu jest tak samo groźne, jak uzależnienie się od dostawców komponentów do budowy sieci telekomunikacyjnych nowej generacji. Dla całej Europy zresztą wybór orientacji technologicznej jest wyborem o charakterze geopolitycznym.

Jaki cel ma ekspertyza powstała pod Panów kierunkiem?

Wiesław Paluszyński: Od jakiegoś czasu trwa ożywiona dyskusja w gronie polityków, organizacji branżowych i ekspertów nad kwestią dopuszczalności wprowadzenia ograniczeń dla niektórych dostawców komponentów do budowy sieci nowej generacji w Polsce. Pojawia się w niej sporo argumentów merytorycznych, ale nie brakuje dezinformacji. Chcieliśmy uporządkować przede wszystkim wiedzę techniczną, lecz także prawną na ten gorący temat. Sporo miejsca poświęciliśmy perspektywie geopolitycznej, nadrzędnej dla omawianej kwestii. Osobny rozdział traktuje o nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, w której pojawiły się stosowne propozycje zapisów w celu umożliwienia eliminowania z rynku dostawców wysokiego ryzyka (DWR).

Jak dużym zagrożeniem dla globalnego cyberbezpieczeństwa mogą być Chiny?

Jarosław Mojsiejuk: Ogromnym, czego od dawna świadome są zarówno Stany Zjednoczone, jak i kraje europejskie. Nie chodzi o doniesienia o licznych incydentach z udziałem chińskich firm, które również omawiamy w naszej ekspertyzie, tylko o zdiagnozowane i wielokrotnie potwierdzone bezpośrednie związki chińskich firm nie tylko z Komunistyczną Partią Chin, lecz także z sektorem militarnym i służbami specjalnymi, odpowiedzialnymi za ataki na naszych sojuszników w NATO i UE.

Wiesław Paluszyński: Musimy sobie zdawać sprawę, że w Chinach, państwie monopartyjnym i autorytarnym, wszelka aktywność pozostaje pod kontrolą władz. Chiny mają potężne aspiracje i zgodnie m.in. z przyjętym planem „Made in China 2025" zamierzają przodować technologicznie w strategicznych gałęziach przemysłu, takich jak: robotyka, urządzenia energetyczne, IT nowej generacji, elektromobilność, lotnictwo, zaawansowane materiały czy transport. To ma być recepta na uniezależnienie się od USA, dlatego także prywatne chińskie przedsiębiorstwa będą musiały się dostosować do tego rządowego imaginarium.

Zgodnie z chińskim prawem, państwo może domagać się dostępu do danych przepływających przez systemy należące do chińskiego sektora prywatnego. Formalnie Huawei jest oczywiście firmą prywatną, należącą do ok. 100 tys. pracowników. Nie mają oni jednak ani wpływu, ani kontroli nad swoją własnością. Sprawuje ją kontrolowany przez państwo „komitet związków zawodowych". Trzeba mieć na uwadze, że zarówno wojskowi, jak i cywilni pracownicy etatowi oraz specjaliści na kontraktach w chińskich firmach działają na rzecz i pod nadzorem władz centralnych. Chiny oczywiście zaprzeczają, że firmy: Huawei, ZTE, Hytera czy Hikvisioni Dahua to organizacje państwowe i składają publicznie obietnice ukrócenia wszelkich nagannych praktyk. Na szczęście i w Europie, i w Polsce jesteśmy w pełni świadomi reguł tej gry pozorów.

Nie jest tajemnicą, że Chiny wręcz wyspecjalizowały się w wykorzystywaniu zespołów zajmujących się włamaniami, tworzeniem złośliwego oprogramowania i poszukiwaniem tzw. 0-day. Chińskie ofensywne działania w cyberprzestrzeni to w dużej mierze szpiegostwo przemysłowe nastawione na kradzież technologii, które mają wspomóc modernizację chińskich sił zbrojnych czy przemysłu.

Jarosław Mojsiejuk: Ofiarami chińskich ataków cybernetycznych padają w zdecydowanej większości podmioty amerykańskie, więc Stany Zjednoczone – po przeprowadzeniu analiz – podjęły działania eliminujące chińskich operatorów telekomunikacyjnych ze swojego rynku. W amerykańskim prawie zamówień publicznych wprowadzono ograniczenia dotyczące chińskich dostawców, ale pozostała furtka – ten sam sprzęt mógł być nadal używany, jeśli został zakupiony za prywatne lub inne niż federalne publiczne środki. Tę lukę prawną ostatecznie zlikwidował Secure Equipment Act of 2021, podpisany w listopadzie 2021 r. przez prezydenta Joe Bidena, zgodnie z którym Federal Communications Commission nie będzie mogła nawet rozważać wydania nowych licencji na sprzęt telekomunikacyjny firmom uznanym za zagrażające bezpieczeństwu.

Jakie są zalecenia UE dotyczące walki z chińską ekspozyturą technologiczną?

Jarosław Mojsiejuk: We wrześniu 2021 r. pojawiła się Rezolucja Parlamentu Europejskiego w sprawie nowej strategii UE–Chiny, postulująca zapewnienie narzędzi i danych niezbędnych do przeciwdziałania zagrożeniom politycznym, gospodarczym, społecznym i technologicznym wywołanym przez Chiny. Dokument, wzywający do współpracy na tym polu, zakłada także monitorowanie kluczowych umów dotyczących infrastruktury w państwach członkowskich i krajach przystępujących w celu zapewnienia ich zgodności z prawodawstwem UE, a także ich zgodności ze strategicznymi interesami UE określonymi w strategii UE–Chiny, ochronę infrastruktury krytycznej przed wpływem państw trzecich, który mógłby być szkodliwy dla interesów gospodarczych i w zakresie bezpieczeństwa UE i jej państw członkowskich. Stosunek do Chin poszczególnych krajów UE, będących także stronami umów o wolnym handlu, jest jednak bardzo zróżnicowany i niektóre z nich nie chcą nawet rozmawiać o ewentualnych wspólnych sankcjach.

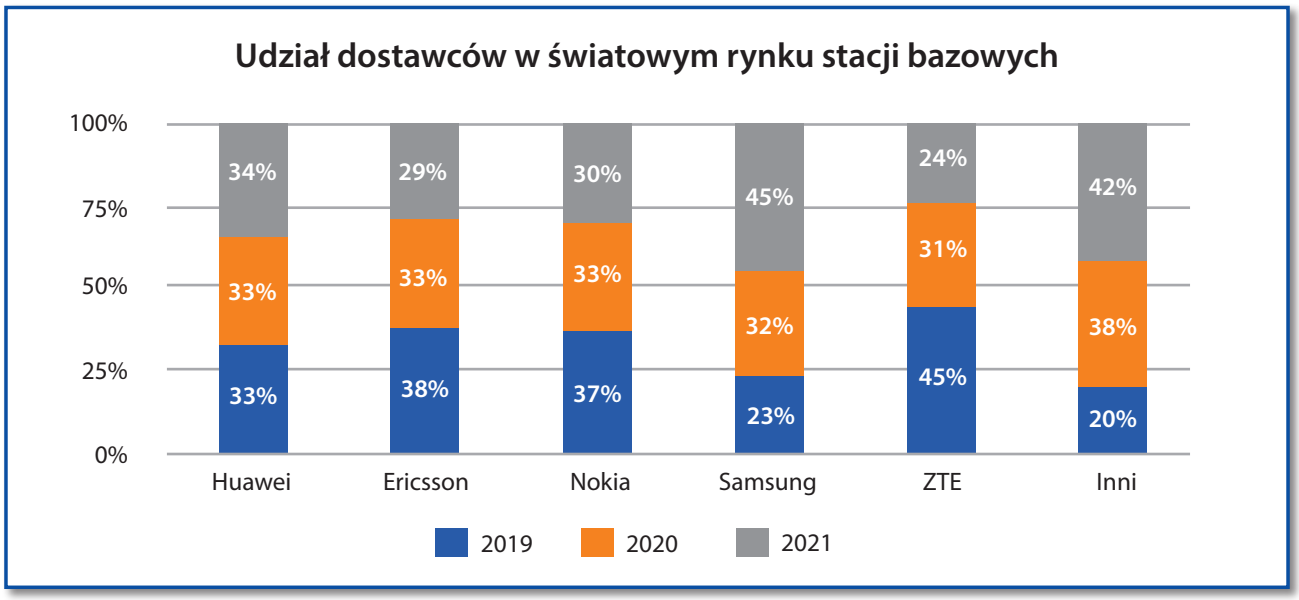
W kontekście Unii Europejskiej należy też wymienić inne drogowskazy prawne, które omawiamy w naszej ekspertyzie: „Strategię UE w zakresie cyberbezpieczeństwa na cyfrową dekadę", dyrektywę NIS z 2016, Electronic Communications Code z 2018 r., rekomendacje dotyczące cyberbezpieczeństwa sieci 5G z 2019 r., raport Grupy Współpracy NIS Nr 01/2020 „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures" (zwany popularnie „5G Toolbox") czy konkluzje ze spotkania „Shaping Europe's Digital Future" z 2020 r. Posiłkując się wnioskami m.in. z tych dokumentów, minister cyfryzacji wydał w połowie 2020 r. rozporządzenie do art. 175 d „Prawa Telekomunikacyjnego" dotyczące usług cyfrowych i integralności sieci.

Wiesław Paluszyński: System norm prawnych uzupełniają standardy techniczne dotyczące sieci 5G, które także omawiamy w naszej ekspertyzie. Załączamy do niej dokument najświeższy, przygotowany przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa ENISA (skrót pochodzi od dawnej nazwy European Network and Information Security Agency), która w listopadzie 2021 r. opublikowała niezwykle ważny dokument: „5G CYBERSECURITY STANDARDS Analysis of standardisation requirements in support of cy-bersecurity policy v.11.9 – final draft for circulation". Ta długa lista standardów i norm, które powinny mieć zastosowanie w sieciach 5G, pokazuje złożoność systemu zapewnienia bezpieczeństwa.

Jarosław Mojsiejuki: Warto zauważyć, że poszczególne państwa, zarówno w UE, jak i poza nią (USA, Australia, Kanada, Nowa Zelandia) mają różne strategie dotyczące DWR, w tym zakazujące lub ograniczające stosowanie urządzeń Huawei i ZTE w sieciach telekomunikacyjnych. Przykładowo Brytyjczycy w swoich regulacjach określili, że dopuszczany jest tylko jeden DWR, nie może on dostarczać sieci core'owej, a jego udział w sieci nie może przekraczać 35%. W Szwecji wprowadzono na etapie aukcji na częstotliwości sądowy zakaz stosowania urządzeń firm Huawei i ZTE. Finlandia, Austria i Niemcy wyspecyfikowały te elementy sieci, w których nie mogą być stosowane urządzenia DWR, trwają dyskusje co do zakresu tak zwanych funkcji krytycznych.

Jakie rozwiązania w stosunku do DRW proponuje nowelizacja ustawy o KSC?

Jarosław Mojsiejuk: Projekt ustawy przewiduje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania – dla szczególnego rodzaju podmiotów gospodarczych i społecznych – za DWR. Minister właściwy ds. informatyzacji uzyskuje



Źródło: Mobile base station vendor market share worldwide 2019-2021, Statista

kompetencję do przeprowadzenia stosownego postępowania o charakterze administracyjnym. Projekt nowelizacji ustawy nie przewiduje generalnych zakazów wprowadzenia produktów określonego dostawcy, ale może dotyczyć setek firm: producentów, importerów, dystrybutorów.

Wiesław Paluszyński: Warto pochylić się nad zapisami tej nowelizacji, bo już na wczesnym etapie, po przyjęciu ustawy przez Komitet Stały Rady Ministrów, ma ona stanowić podstawę do wszczęcia aukcji częstotliwości. Ten pospiech jest podyktowany opóźnieniami, jakie mamy w harmonogramie przeprowadzania aukcji w stosunku do terminów przyjętych przez KE. W naszej ekspertyzie oceniamy, na ile proponowane zapisy ustawy wpisują się w poprawny model ochrony polskiej cyberprzestrzeni w całym obszarze gospodarki i życia społecznego, ze szczególnym uwzględnieniem infrastruktury krytycznej.

Ekspertyza identyfikuje wiele ryzyk związanych z wdrożeniem sieci 5G w Polsce…

Wiesław Paluszyński: Istotnym ryzykiem jest znaczne uzależnienie polskich operatorów telekomunikacyjnych od dostaw technologii jednej firmy. Tylko w latach 2019–2020 Huawei uzyskała w Polsce pozwolenia na uruchomienie swojej technologii na ponad 20 tys. masztów radiowych! W efekcie polityki protekcjonistycznej Chin ten sprzęt jest relatywnie tani i z punktu widzenia operatorów sieci komórkowych najłatwiej byłoby nadal się go trzymać, zwłaszcza że integracja np. anten z urządzeniami innych dostawców jest nie tylko kosztowna, lecz może także istotnie opóźniać proces wdrażania 5G. To prosta droga do monopolu jednego dostawcy ze wszystkimi negatywnymi tego konsekwencjami, nie tylko gospodarczymi. Tymczasem w interesie Polski leży dywersyfikacja dostawców, bazująca na rozwiązaniach ustawowych. Musimy wyraźnie rozróżnić DWR od dostawców pochodzących z UE oraz państw NATO. Zdaniem autorów ekspertyzy, stosowane przez Huawei i ZTE praktyki ograniczające konkurencję metodą Vendor lock powinny spowodować wdrożenie procedur antymonopolowych nie tylko w Polsce, lecz w całej UE, a nawet WTO.

Istotne są też ryzyka związane z istnieniem nieautoryzowanych kanałów transmisji i przekazywania danych. Prowadzone w Wlk. Brytanii badania rozwiązań i urządzeń Huawei – pod kontrolą organizacji rządowych – nie napawają optymizmem, bo dowodzą niskiej jakości oprogramowania, co rodzi poważne obawy dotyczące zarządzania podatnością na zagrożenia w perspektywie długoterminowej. Tymczasem żaden kraj nie dysponuje możliwościami zbadania całego oprogramowania dostarczanego przez Huawei. Rząd RP wysłał w czerwcu 2021 r. obszerną analizę ryzyk do Komisji Europejskiej. Własną analizę przygotowała także Rada ds. Cyfryzacji przy Ministrze Cyfryzacji.

Jarosław Mojsiejuk: Kształt nowelizacji ustawy o KSC jest przedmiotem ożywionych działań lobbingowych. Pojawiają się zaowalowane groźby wyłączenia wsparcia dla już dostarczonych rozwiązań sieci 2–4G w przypadku zablokowania dostaw produktów Huawei/ZTE dla nowo budowanych sieci 5G, mimo że na podstawie ważnych umów Huawei jest prawnie zobowiązana do świadczenia usług w zakresie 2–4G. Próbuje się także używać argumentów o rzekomej dominacji rozwiązań z Chin w obszarze uzyskanych patentów oraz standardów, a także straszyć niebotycznymi kosztami ewentualnej wymiany całej infrastruktury telekomunikacyjnej w Polsce. W ekspertyzie weryfikujemy te mocno przesadzone szacunki.

Wiesław Paluszyński: Ekspertyza PTI jasno wskazuje priorytety przy wdrażaniu sieci 5G. Nie ulega wątpliwości, że bezpieczeństwo narodowe jest dobrem nadrzędnym, a telekomunikacja jest krwiobiegiem współczesnego państwa. Nie jesteśmy skazani na DWR; kilku światowych liderów telekomunikacji, działających również w Polsce, z powodzeniem wdraża technologie 5G na świecie. Mamy także własne, sprawdzone zasoby.

Nasi decydenci powinni sobie zdawać sprawę, że budowa sieci 5G łatwo może przerodzić się w technologiczny Nord Stream 2. Tę inwestycję Polska od początku uważała za instrument polityczny, służący realizacji imperialnej polityki Rosji i historia, niestety, przyznała nam rację. Budowa sieci 5G zdecydowanie nie ma wyłącznie biznesowego charakteru. Musimy z całą bezwzględnością eliminować niebezpieczne produkty z rynku publicznego i z kluczowych elementów infrastruktury. Apelujemy do polskiego rządu, żeby w sprawie budowy sieci 5G zajął równie twarde stanowisko jak w kwestii Nord Stream 2.

Ekspertyza dostępna jest pod adresem:
https://portal.pti.org.pl/dostawcy-wysokiego-ryzyka/

Impresja pozjazdowa

Wojciech Kiedrowski

wiceprezes PTI ds. programu i działań statutowych

Poranek po krótkiej nocy. Nasze myśli wciąż krążą wokół tematów dnia poprzedniego, pozostając w meandrach lemowskich wizji przyszłości, które przecież się jeszcze nie ziściły w pełni, ale już jesteśmy niemal przekonani, że nadejdą. Owa mieszanka myśli i odczuć wprowadza nas w atmosferę o tyle wzniosłą, co też pełną niepewności i obaw. W tym wszystkim ingrediencja transhumanizmu, niejako nowa–stara idea budząca ekscytację. Jak daleka przestrzeń dzieli człowieka od maszyny? Czy nasze telluryczne postrzeganie świata pozwoli kiedykolwiek znaleźć odpowiedź na to pytanie? A jeśli tak, to czy maszyna posiądzie władzę nad ludzkością i urządzi jej świat po swojemu, czy też człowiek wciąż będzie trzymał stery w swoich rękach. Czy nasza ludzka świadomość (świadomość wiadomo, że zawsze jest ludzka, ale tym razem na wszelki wypadek wolałem to podkreślić) wciąż będzie wolna lub przynajmniej będzie czuła się wolna? Czy też świadomie będziemy się wspomagać technologią w celu osiągnięcia doskonałości intelektualnej i fizycznej?

Istnienie świadomości, co pozostaje wciąż w sferze naszej wiary lub niewiary, budzi niesłabnące od wieków imaginacje. Czy jest wytworem jedynie naszej fizyczności i rodzi się w mózgu, utwierdzając w przekonaniu, że ciało ludzkie jest jedynie najdoskonalszą maszyną? Czy też świadomość jest niezależna od ciała ludzkiego, które stanowi niedoskonałą strukturę, w której ta przebywa, i to jedynie przez krótką chwilę? Nie idźmy dalej w tych rozważaniach, nie czas i miejsce teraz na to.

Muzyka Wojciecha Kilara, dodająca temu wieczorowi magii, jeszcze pobrzmiewa w uszach, łagodząc niejako rozterki ducha, przywołując znane nam dobrze obrazy i emocje, uspokaja i dobrze nastraja do wyzwań dnia, który przed nami. Za oknami jednostajnie szumi ulica, Warszawa budzi się weekendowo do życia, a my, przekraczając próg hotelowej sali śniadaniowej, wkraczamy w rzeczywistość Nadzwyczajnego Zjazdu Delegatów PTI.

Zjazd otworzył i delegatów powitał Prezes Polskiego Towarzystwa Informatycznego – Wiesław Paluszyński. Po ukonstytuowaniu się władz zjazdu, powołaniu niezbędnych do jego przeprowadzenia komisji i zespołów, przystąpiliśmy do obrad.

Na początku przeżyliśmy miłe chwile, związane z nadaniem tytułów Członków Honorowych naszym najbardziej zasłużonym i szeroko znanym w środowisku informatyków z osiągnięć naukowych i zawodowych Kolegom:

Januszowi Dorożyńskiemu,
Januszowi Kacprzykowi,
Włodzimierzowi Marcińskiemu,
Tadeuszowi Syryjczykowi.

Miło było ogrzać się w blasku wyróżnionych.

Następnie rozgorzała dyskusja nad tym, co dobre, a co nie, co zmienić, a czego nie warto zmieniać. Świat wokół nas się zmienia, a my postanowiliśmy podążać za zmieniającym się światem. Okazało się to trudniejsze, niż się spodziewaliśmy. Przy wygłaszaniu tez na temat przyszłości Polskiego Towarzystwa Informatycznego, potrzebnych zmian i otwieraniu się na rzeczywistość przyszłości, odwaga ścierała się z rozwagą. Zmiany, które jednocześnie są naszym wyzwaniem, to między innymi otwarcie się Towarzystwa na młodsze pokolenia.

Ta przełomowa decyzja wiele zmienia. W moim odczuciu skraca dystans pomiędzy „starą gwardią" informatyków a adeptami stawiającymi pierwsze kroki na polu edukacji informatycznej czy zawodowym. Zbliża nas do szkół, którym mamy sporo do zaoferowania, nie tylko w obszarze certyfikacji ICDL. Z dużym zainteresowaniem spotkał się nasz konkurs gier edukacyjnych GEEK. Pierwsza jego edycja pokazała ogromny potencjał do zagospodarowania

> *Po raz pierwszy w historii PTI zaprosiliśmy do pełnego członkostwa uczniów szkół średnich i studentów studiów I stopnia, począwszy od pierwszych roczników.*

w tym obszarze. Powołaliśmy nową Sekcję Gier Edukacyjnych Komputerowych, której celem jest wymiana doświadczeń i informacji dotyczących gier edukacyjnych i konkursu GEEK oraz wspieranie uczestników i organizatorów konkursów gier, w tym pomoc merytoryczna.

Nową ofertę skierowaną do szkół przygotowuje Sekcja Informatyki Szkolnej. Jej aktywność skupia się na różnorodnym wsparciu nauczycieli informatyki, zarówno w sferze rozwoju kompetencji, podnoszenia kwalifikacji, w obszarze metodycznym, jak i organizacyjnym w pracy z uczniami. Dobra energia zatem, jaka udzieliła się nam wszystkim po zjeździe, zaowocowała już pierwszymi inicjatywami.

Świat pędzi coraz szybciej, a wraz z nim podąża rozwój informatyki. A może jest odwrotnie, może to informatyka pociąga za sobą zmiany rozwojowe społeczeństw i gospodarek? Nasze deklaracje na Zjeździe świadczą o tym, że nie zamierzamy się temu zjawisku bezczynnie przyglądać. W procesach zachodzących w świecie chcielibyśmy zawsze widzieć człowieka, wraz z jego potrzebą bezpieczeństwa, rozwoju, koniecznością zapewnienia mu otwartego dostępu do edukacji, możliwością korzystania z dobrodziejstw technologii i poczuciem przynależności do wspólnoty.

Przesłanki te skłoniły nas do ogłoszenia Manifestu Programowego Polskiego Towarzystwa Informatycznego, definiującego pięć filarów działań:

- INFORMATYCZNA EDUKACJA SPOŁECZEŃSTWA,
- CERTYFIKACJA WIEDZY EKSPERCKIEJ,
- WSPARCIE LEGISLACJI W OBSZARZE INFORMATYKI,
- WIEDZA EKSPERCKA,
- ROZWÓJ ZAWODOWY CZŁONKÓW STOWARZYSZENIA.

Staraliśmy się również objąć troską prawidłowy rozwój oraz podkreślić misyjny charakter nauki polskiej, wyrażając nasze obawy i definiując kierunki działań w przyjętej Uchwale Nadzwyczajnego Zjazdu w Sprawie Nauki. Poszczególne akapity traktują o: potrzebie tworzenia potencjału naukowego w odpowiedzi na wyzwania zmieniającego się świata, potrzebie zapewnienia i wzmacniania kadr naukowych, misji kształcenia społeczeństwa i zapewnienia wyznaczników etycznych i reguł prawnych przy komercjalizacji osiągnięć naukowych. Rozwój zaawansowanej technologii, w szczególności w takich obszarach, jak: telekomunikacja, sztuczna inteligencja, Internet rzeczy, optymalizacja procesów, rzeczywistość rozszerzona i wirtualna, robotyka, stawia świat przed nowymi wyzwaniami. Jednym z istotniejszych problemów jest cyberbezpieczeństwo, które wymaga ciągłego doskonalenia i pochłania coraz więcej zasobów intelektualnych, organizacyjnych i finansowych.

Czy to wystarczy? Czy sprawi, że Towarzystwo będzie dostrzegane przez społeczność informatyków w Polsce i czy ta społeczność uzna, że Towarzystwo jest im potrzebne do działania, pracy, życia? Na to pytanie odpowie najbliższa przyszłość. Stanisław Lem tworzył nowe światy przyszłości, my również chcielibyśmy mieć skromny udział w kreowaniu nowej, lepszej rzeczywistości, w której powszechne zastosowanie technologii będzie służyło dobru, a nie będzie skierowane przeciwko człowiekowi. W dobie ekspansji nowych technologii informacji i komunikacji, automatyzacji pozyskiwania wiedzy, ludzkość wchodzi w posiadanie niezbadanych możliwości. W obliczu tych cybermożliwości warto przejrzeć się – niczym w magicznym zwierciadle – w wizji lemowskich światów. Lem w swojej twórczości zwerbalizował bowiem cały szereg problemów cywilizacyjnych i etycznych, których obecnie doświadczamy.

Nie ulega wątpliwości, że po długim czasie współpracy bazującej na kontaktach wirtualnych, niezwykle miło było się spotkać w świecie rzeczywistym, tak zwyczajnie porozmawiać przy kawie lub kieliszku wina. Trudno bezpośredni kontakt zastąpić substytutem, jakim są obrazy wyświetlane na monitorze i telefon przyłożony do ucha. Odwzajemnianie czyjegoś uśmiechu czy usłyszenie kilku ciepłych słów nadal sprawia przyjemność. Po tak długim czasie smakuje wybornie i chyba wciąż trwająca pandemia sprawiła, że obecnie te proste, drobne ludzkie gesty doceniamy jeszcze bardziej.

A swoją drogą ciekawe, czy Stanisław Lem pochwaliłby nasze aspiracje i metody działania?

POLSKIE TOWARZYSTWO INFORMATYCZNE

Uchwała nr 4

Nadzwyczajnego Zjazdu PTI odbytego 11 września 2021

Przyspieszający postęp naukowy i technologiczny, powszechne wkraczanie technologii informacyjnych w działalność naukową, społeczną i związane z tym interakcje **skutkują wyzwaniami dla nauki** w zakresie informatyki:

Tworzenie potencjału do odpowiedzi na wyzwania zmieniającego się świata – Nieustanne powstawanie nowych wyzwań w dziedzinie nauk informatycznych uniemożliwia uprzednie przygotowanie się na zmiany, które nadejdą w przyszłości. Wpływ informatyki na wszelkie sfery życia powoduje, że będą miały miejsce coraz intensywniejsze oddziaływania informatyki z innymi dziedzinami nauki badającymi te sfery. Dlatego konieczna jest ochrona wolności badań naukowych, różnorodności podejmowanych zagadnień badawczych, oraz wspierających je regulacji i instytucji.

Kadry – Dysproporcja warunków pracy w przemyśle i w instytucjach naukowych, badawczych i edukacyjnych powoduje odchodzenie nauczycieli i naukowców do przemysłu. Dotyczy to nawet osób na zaawansowanych szczeblach kariery. Dlatego należy wspierać rozwój i utrzymanie kadr na wszystkich etapach kariery. Należy również dodatkowo dofinansować nauczycieli i naukowców w zakresie informatyki i dziedzin pokrewnych.

Edukacja społeczeństwa – Widoczny w ostatnich latach kryzys społecznego zaufania do nauki, wykorzystywanie narzędzi informatycznych do promowania ignorancji i obskurantyzmu, niezrozumienie czym jest i jak działa nauka, są wyzwaniami dla naukowców w ogólności. Dlatego należy upowszechniać wiedzę o zasadach uprawiania nauki, jej osiągnięciach, o technologiach informacyjnych, ich naukowych podstawach i ograniczeniach.

Społeczna odpowiedzialność informatyków – Informatyka wkroczyła w istotne obszary życia osobistego i społecznego. Podejmowane badania i tworzone technologie często nie są neutralne etycznie. Dlatego niezwykle istotne jest rozumienie i stosowanie właściwych rozwiązań etycznych i prawnych.

Najbliższe lata – Szerokie rozpowszechnienie technologii takich jak telekomunikacja, sztuczna inteligencja, Internet rzeczy, optymalizacja procesów, rzeczywistość rozszerzona i wirtualna, robotyka, oraz związane z nimi nowe formy przemysłu, stwarzają szereg wyzwań badawczych, edukacyjnych i społecznych. Szczególnie istotne jest zapewnienie cyberbezpieczeństwa wszystkich elementów infrastruktury teleinformatycznej. Dlatego należy finansować i na inne sposoby wspierać badania nad nowymi technologiami i kierunkami w informatyce, aby społeczeństwo polskie mogło nadążać za zachodzącymi zmianami i aby mądrze i bezpiecznie z nich korzystać.

Wzywamy Członków PTI, Organy Statutowe, Polityków i Decydentów o wparcie działań na rzecz rozwiązywania powyższych i przyszłych problemów nauki w zakresie informatyki.

Sekretarz Zjazdu

Kajetan Wojsyk

Przewodniczący Zjazdu

Marian Bubak

POLSKIE TOWARZYSTWO INFORMATYCZNE

Uchwała nr 5

Nadzwyczajnego Zjazdu PTI odbytego 11 września 2021

MANIFEST PROGRAMOWY POLSKIEGO TOWARZYSTWA INFORMATYCZNEGO

Dynamiczny rozwój informatyki, zarówno teoretycznej jak i stosowanej, niemający precedensu w odniesieniu do innych dziedzin w historii świata, wywierający ogromny wpływ na codzienne życie całej światowej społeczności, nie może pozostać bez zajęcia stanowiska naszego Stowarzyszenia.

Polskie Towarzystwo Informatyczne od początku swojego istnienia skupiało osoby żywotnie zainteresowane dalszym rozwojem informatyki, a w szczególności wykorzystania jej dla dobra całego społeczeństwa, dziś określanego mianem społeczeństwa informacyjnego.

Szanując tradycję i ogromny wkład w rozwój informatyki naszych prekursorów, z których wielu odeszło już od nas na zawsze, widzimy potrzebę dalekiego spojrzenia w przyszłość i nakreślenia kierunków działania, w których nasze Stowarzyszenie zamierza uczestniczyć, traktując to działanie jako swoją misję.

Poniżej przedstawiamy pięć FILARÓW, które zamierzamy traktować jako fundamentalne wyznaczniki naszej działalności.

FILAR I – INFORMATYCZNA EDUKACJA SPOŁECZEŃSTWA

Dynamiczny rozwój narzędzi i zastosowań informatycznych oraz radykalne obniżenie kosztów jednostkowych takich urządzeń jak komputer, smartfon, tablet, czy innych tego typu urządzeń wbudowanych w sprzęt powszechnego użytku spowodował, że życie bez umiejętności poprawnego i co równie ważne, bezpiecznego posługiwania się nimi stało się bardzo trudne. Brak tych umiejętności powoduje wykluczenie części społeczeństwa z dostępu do wielu usług, także tych najbardziej podstawowych.

Zamierzamy kontynuować i rozwijać szeroką akcję edukacyjną skierowaną do osób w różnym wieku i o różnym poziomie wykształcenia. Służyć temu ma kontynuowanie organizacji certyfikacji ECDL/ICDL na wszystkich poziomach zaawansowania, a także nowe inicjatywy (np. konkursy) skierowane do młodzieży szkolnej, umożliwiające im jak najwcześniejsze zdobycie wiedzy i umiejętności w różnych specjalnościach informatyki.

Stowarzyszenie zamierza również skierować swoje działania w stronę seniorów, którym niejednokrotnie brak podstawowych umiejętności IT utrudnia życie. Skutkiem tego może być np. brak dostępu do usług bankowych lub kontaktów z administracją w celu sprawnego załatwiania spraw.

FILAR II – CERTYFIKACJA WIEDZY EKSPERCKIEJ

Dynamiczny i żywiołowy rozwój narzędzi informatycznych i poziom ich złożoności spowodował, że na rynku pracy od dawna brakuje specjalistów o zweryfikowanych umiejętnościach i wiedzy. Zjawisko to, widoczne w skali świata, spowodowało, że pracodawcy w swoich wyborach kierują się certyfikatami wydanymi przez uznane organizacje międzynarodowe lub wręcz przez producentów sprzętu bądź oprogramowania. Dla wielu osób w krajach, dla których język angielski nie jest językiem natywnym stanowi to trudną do pokonania barierę. Mimo posiadania wystarczającej wiedzy merytorycznej osoby te nie są w stanie zdać egzaminów prowadzonych w formie pisemnej.

Zamierzamy, wychodząc naprzeciw ogromnym potrzebom podmiotów publicznych i prywatnych, prowadzić proces certyfikacji wiedzy tych osób w języku polskim, po spełnieniu wszelkich wymagań formalnych przewidzianych przepisami prawa. W pierwszej kolejności, biorąc pod uwagę potrzeby zapewnienia cyberbezpieczeństwa, zamierzamy wprowadzić certyfikację specjalistów z tego obszaru.

Kontynuacja certyfikacji w obszarze ECDL/ICDL, o której była mowa w I FILARZE również jest istotną częścią tu przedstawionego II FILARU.

FILAR III – WSPARCIE LEGISLACJI W OBSZARZE INFORMATYKI

Stojąc na stanowisku, że gwarantem pomyślności i bezpieczeństwa obywateli jest państwo działające na podstawie i w granicach dobrze stanowionego prawa, zamierzamy aktywnie uczestniczyć w tym procesie poprzez opiniowanie projektów aktów legislacyjnych przez naszych ekspertów, wspartych przez szerokie grono członków Stowarzyszenia.

Zamierzamy aktywnie uczestniczyć jako ciało społeczne w pracach Komisji Sejmowych, pracujących nad aktami prawnymi regulującymi obszar szeroko rozumianej teleinformatyki.

FILAR IV – WIEDZA EKSPERCKA

Mając w swoich szeregach wysokiej klasy ekspertów, działających w Izbie Rzeczoznawców PTI zamierzamy kontynuować i rozwijać tą działalność, umożliwiając podmiotom publicznym i prywatnym pozyskanie wsparcia ze strony osób dysponujących wiedzą o najwyższej próbie, zweryfikowanych w praktycznym działaniu.

FILAR V – ROZWÓJ ZAWODOWY CZŁONKÓW STOWARZYSZENIA

Zamierzamy kontynuować działania w obszarze rozwoju zawodowego naszych członków, z uwzględnieniem nowych form ich prowadzenia takich jak telekonferencje i webinaria. W miarę potrzeb i możliwości wynikających z trudnych wyzwań, jakich jesteśmy świadkami w ostatnich czasach zamierzamy kontynuować spotkania i organizować konferencje merytoryczne, zarówno poprzez wsparcie udzielane jednostkom terenowym PTI jak i poprzez organizację imprez centralnych.

Mamy również na uwadze potrzebę podtrzymania nieformalnych kontaktów koleżeńskich członków Stowarzyszenia i jego Sympatyków poprzez organizację imprez o charakterze rekreacyjnym, mających wieloletnią tradycję w PTI.

Sekretarz Zjazdu

Kajetan Wojsyk

Przewodniczący Zjazdu

Marian Bubak

Sekcja Informatyki Szkolnej – wsparcie dla nauczycieli

Ze sprzętem komputerowym, mimo braku jakichkolwiek standardów, szkoły jakoś sobie radzą, ale tysiące nauczycieli szuka inspiracji, jak zaszczepić w uczniach pasję do pozyskiwania umiejętności cyfrowych, które są przepustką do cywilizowanego świata. Polskie Towarzystwo Informatyczne – tworząc przestrzeń do wymiany edukacyjnych doświadczeń – zamierza pomóc zapełnić tę lukę.

Ta przestrzeń to nowo powołana Sekcja Informatyki Szkolnej (SIS), na jej stronach (https://sis.pti.org.pl/ i https://www.facebook.com/sispti sis.pti.org.pl) nauczyciele, którzy zgłosili swój akces do SIS, znajdą ciekawe informacje, rekomendowane wydarzenia, szkolenia oraz spójny spis konkursów informatycznych.

Upowszechnianie doświadczeń

Sekcja powstała z myślą o skupieniu przy Polskim Towarzystwie Informatycznym praktykujących nauczycieli informatyki, pracujących zawodowo w szkołach wszelkiego typu. Z uwagi na szerokie zastosowanie narzędzi informatycznych na wielu przedmiotach oraz przygotowywanie zadań i ćwiczeń wymagających rozwiązywania algorytmicznych problemów, do Sekcji dołączają również nauczyciele innych przedmiotów aktywnie wykorzystujący technologię informacyjno-komunikacyjną w dydaktyce.

Sekcję prowadzimy wyłącznie wirtualnie, a poza członkami PTI udział w SIS mogą deklarować nauczyciele aktywni zawodowo, którzy po dołączeniu do sekcji stają się Sympatykami PTI. Już w pierwszych dniach po uruchomieniu zapisów do sekcji dołączyło 30 osób, głównie znakomitych nauczycieli informatyki szeroko znanych w tym środowisku (m.in. Jacek Ścibor – założyciel grupy SuperBelfrzy RP, Barbara Halska – promotorka prac i projektów informatycznych, które zdobywają międzynarodowe sukcesy w Paryżu, Brukseli, Seulu i Moskwie, Karolina Szulc – redaktor naczelna czasopisma „TIK w Edukacji", Adam Jurkiewicz.). Naszą inicjatywą zainteresowali się także nauczycieli aktywnie korzystający z technologii informacyjno-komunikacyjnych. Czujemy się zaszczyceni, witając w tym gronie m.in. Jolantę Okuniewską – finalistkę światowego konkursu The Global Teacher Prize (2016) i autorkę bloga „Tableszyt w okładce w motyle" (http://tableciaki.blogspot.com/) oraz Aleksandrę Schoen-Kamińską – autorkę bloga „Klikankowo"

Beata Chodacka
nauczyciel informatyki w V LO i SP 33 w Krakowie, wiceprezes Oddziału Małopolskiego PTI, animatorka działań na rzecz edukacji informatycznej, współtwórca zbioru zadań z informatyki exeBOOK. Współtwórca i współorganizator projektu „Klasa z ECDL". Koordynator merytoryczny w Centrum Mistrzostwa Informatycznego przy AGH, członek grupy SuperBelfrzy RP, inicjatorka i przewodnicząca Sekcji Informatyki Szkolnej przy PTI.

(https://klikankowo.jimdofree.com/), który podczas zdalnego nauczania osiągnął 2 miliony wyświetleń!. Cieszymy się także z obecności Alicji Podstolec, programującej na języku polskim, Agnieszki Halickiej – prekursorki wielu pomocnych TIKów dla nauczycieli. Gdy piszę ten tekst, sekcja liczy już 81 członków. Wielu z nich deklaruje chęć przystąpienia do PTI.

Na stronie SIS proponujemy także krótkie i ciekawe wpisy z rozwiązaniami dydaktycznymi, zadaniami lub aplikacjami do wykorzystania nie tylko na lekcjach informatyki, lecz również na innych przedmiotach. Wiele z tych wpisów zawiera metodyczne wskazówki i warianty rozwiązań dla różnych poziomów nauczania.

Dostępny i na bieżąco prowadzony jest dział wydarzenia wraz z kalendarzem (https://calendar.google.com/calendar/u/0?cid=Y2JlNGIwOTZkMzhzazlqMG9hcWZrMjR0cmdAZ3JvdXAuY2FsZW5kYXIuZ29vZ2xlLmNvbQ), który można

zasubskrybować. Znajdują się tam rekomendowane przez członków SIS (lub przez nich prowadzone) konferencje dla nauczycieli, webinary, szkolenia, konkursy itd. Członkowie Sekcji przy okazji przygotowują aktywności związane z kalendarzem. Już w październiku na CodeWeek powstała interaktywna tablica (https://sis.pti.org.pl/zadania-na-codeweek/) z zadaniami od SIS, które wykonało ponad 1000 osób. W grudniu 2021 r. przez tydzień w ramach Godziny Kodowania (https://sis.pti.org.pl/godzina-kodowania-zadania-od-sis/) powstały ciekawe, autorskie zadania publikowane codziennie na witrynie SIS.

W ciągu niespełna dwóch miesięcy działania Sekcji, jej profil na FB obserwuje niemal 400 osób, wiele publikowanych postów miało znacznie większą liczbę odbiorców (nawet do 20 tys. wyświetleń). Otrzymaliśmy wiele zwrotnych informacji, że nasze działania są ciekawe, potrzebne i wypełniają lukę w przestrzeni edukacyjnej. Dzięki wsparciu partnerskiemu (https://sis.pti.org.pl/wspolpraca/), współdzieleniu informacji i podejmowaniu wspólnych inicjatyw dość szybko zyskaliśmy przychylność w kręgach edukacji informatycznej.

Konkursy aktywizują

Powstał również dział Konkursy (patrz także ramka), obecnie wpisanych jest tam 11 ogólnopolskich konkursów informatycznych wraz z terminami, wymaganiami i kryteriami. Nauczyciele uważają takie zestawienie za bardzo pomocne.

Inauguracja działań

SIS po raz pierwszy pokazała się publicznie podczas listopadowego Klubu Informatyka (https://mazowsze.pti.org.pl/13,aktualnosci/article:386), na spotkaniu dotyczącym prowadzenia informatyki w szkołach: **„Paint forever? O informatyce w szkole!"**. O tym, czego warto nauczyć osobę o specjalizacji technik informatyk, jak działać między pasją a obowiązkiem oraz o informatyce poza informatyką opowiedziała Karolina Antkowiak, nauczyciel matematyki, fizyki oraz przedmiotów zawodowych w technikum o profilu informatycznym. Ważny temat neutralności technologicznej w nauczaniu informatyki w szkołach poruszył Adam Jurkiewicz, członek zarządu SIS. Sylwetkę nauczyciela informatyki na podstawie danych zebranych z ponad 400 ankiet przedstawiła Beata Chodacka, przewodnicząca Sekcji. O tym „jak zmienia się uniwersum sprzętowe polskiej szkoły, jakie to wyzwanie i dla kogo" opowiedział, jak zawsze świetnie, Jacek Ścibor.

Beata Chodacka i Agnieszka Halicka opowiadały o SIS i jej konkursach podczas niedawnego XIV Zlotu Innowacyjnych Nauczycieli i Dyrektorów w Krakowie. Była to też okazja do osobistego spotkania z wieloma członkami Sekcji oraz pozyskania nowych niezwykłych nauczycieli do naszego zespołu.

Przedstawiciele różnych środowisk zarządzają SIS

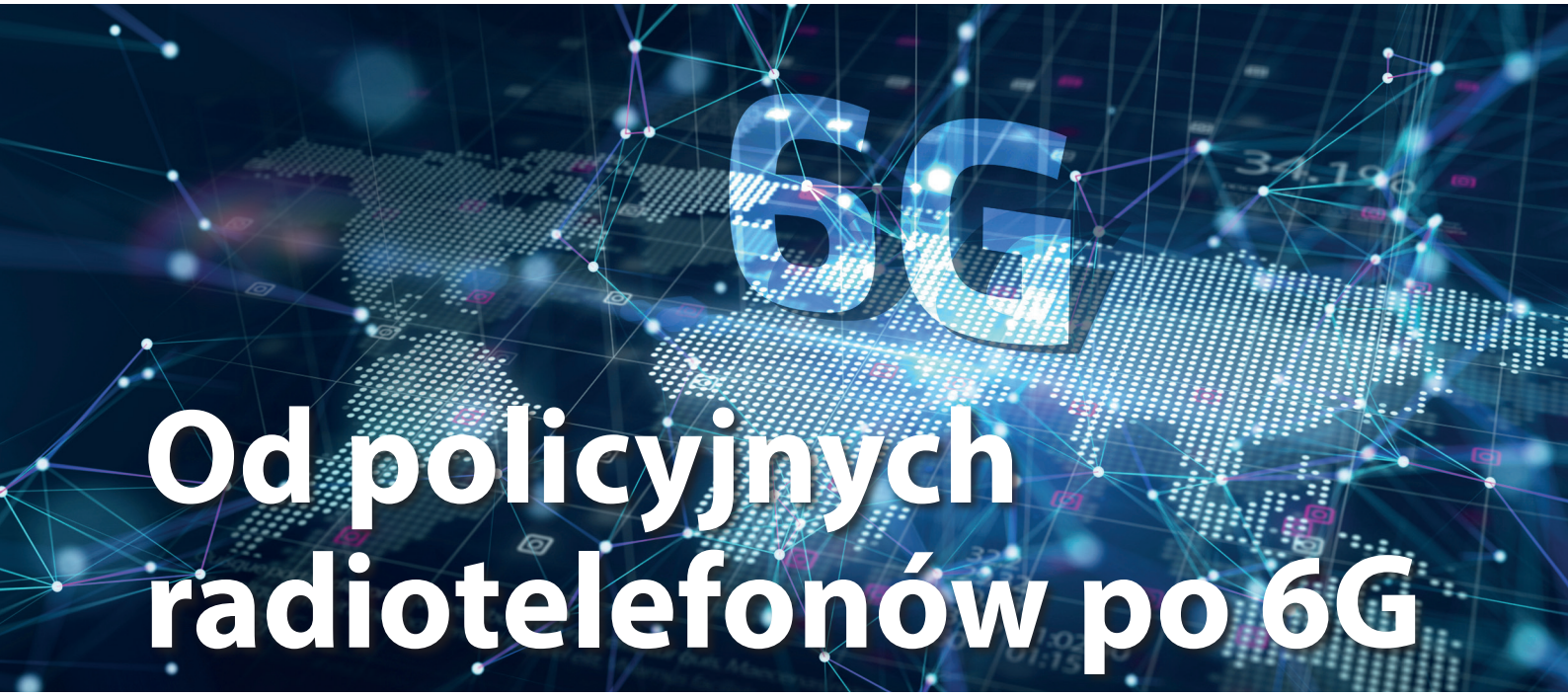
Przewodniczącą Sekcji została jej inicjatorka – Beata Chodacka z Oddziału Małopolskiego PTI. W skład zarządu SIS weszli: Grzegorz Szyjewski (Oddział Zachodniopomorski), który podjął się administrowania i zarządzania narzędziami informatycznymi wykorzystywanymi przez zespół, Elżbieta Bowdur (Oddział Śląski) jako wiceprzewodnicząca oraz Anna Wrzeciono (Oddział Małopolski).

Zarząd Sekcji został rozszerzony o dwóch sympatyków PTI: Adama Jurkiewicza, nauczyciela informatyki, autora podręczników do programowania w Pythonie oraz platformy do programowania w Pythonie dla szkół (https://python.szkola.pl) oraz Agnieszkę Halicką – nauczycielkę bibliotekarkę, animatorkę, prowadzącą blog https://www.edutriki.pl, na którym dzieli się niezwykłymi pomysłami na wykorzystanie różnych aplikacji.

Sekcja uruchomiła ogólnopolski konkurs „Geniallne Miejsca"

(https://sis.pti.org.pl/konkursy/konkurs-geniallne-miejsca/), polegający na przygotowaniu prezentacji w postaci gry lub escape-roomu (np. w aplikacji genially) na temat miejscowości lub okolicy, gdzie znajduje się szkoła. W ramach pracy można opracować zadania dotyczące np. ciekawej postaci związanej z regionem, interesującego miejsca historycznego lub przyrodniczego, opowiedzieć legendę, poznać miejsce kultu. **Dodatkowo jednym z założeń konkursu jest możliwość wysłania pracy (o ile spełnia wymogi regulaminu) również do konkursu GEEK (Gry Eksperymentalne Edukacyjne Komputerowe), którego drugą edycję uruchomiło właśnie PTI i który SIS chce aktywnie promować.** Jednym z celów Sekcji jest współpraca przy organizacji konkursów, zawodów i olimpiad informatycznych organizowanych przez PTI.

W każdym województwie powołani zostali koordynatorzy, którzy wyrazili chęć pomocy. SIS zorganizowała już dwa webinary dla nauczycieli i uczniów, zachęcające do udziału w tych wydarzeniach oraz pokazujące, jak przygotować ciekawe prace. W spotkaniach online wzięło udział każdorazowo ponad 120 osób, a nagrania obejrzało blisko 3 tys. osób.



Od policyjnych radiotelefonów po 6G

Po ubiegłorocznym, dyskusyjnym – według obserwatorów naszego rynku komunikacji elektronicznej – przerwaniu i anulowaniu aukcji na bardzo istotne dla 5G pasmo C (3,4-3,8 GHz) „wielka czwórka" operatorów na razie oferuje usługi mobilne i stacjonarne w tej technologii w posiadanych pasmach 2100 MHz i 2600 MHz.

Pasma te są jednak wykorzystywane przez operatorów do świadczenia usług LTE – usługi 5G zostały przez nich uruchomione w trybie 5G NSA (*Non-Stand Alone*). Na razie mają więc dylemat: na ile intensywnie oferować 5G, skoro trzeba to robić kosztem zmniejszania przepustowości pasm LTE. W dodatku pomiary prędkości pobierania i wysyłania plików potwierdzają, że w praktyce prędkości transmisji 5G uruchamianych w sieciach współdzielących zasoby częstotliwości bywają niższe niż uzyskiwane w „czystych" sieciach 4G/LTE. W sieci LTE dostępna jest bowiem tzw. agregacja pasm, co przy transmisji poprzez stacje obsługujące taką możliwość (i oczywiście telefony oraz modemy potrafiące działać w taki sposób) teoretycznie umożliwia osiąganie prędkości transmisji 4G nawet do 600 Mb/s.

Tomasz Kulisiewicz
sekretarz Sektorowej Rady ds. Kompetencji – Informatyka

Trochę o historii łączności mobilnej

Początki cywilnej i „konsumenckiej" łączności ruchomej sięgają końca lat 40. XX w. Zarówno zastosowane technologie radiowe, jak i urządzenia wywodziły się z radiowej łączności profesjonalnej oraz wojskowej. W latach 1946–1948 amerykański operator Bell Systems uruchomił w kilku stanach sieć nazywaną MTS (Mobile Telephone Service), korzystającą z przystosowanych radiotelefonów policyjnych produkcji Western Electric. Były to telefony samochodowe (masa zestawu ok. 40 kg – patrz fotografia), zajmujące sporą część bagażnika, wcale nie małego w obszernych amerykańskich samochodach osobowych tamtych czasów.

Źródło: http://www.wb6nvh.com/MTSfiles/Carphone1.htm

Sieć działała w dwóch wariantach: Highway i Urban. Urban w 1948 r. miał 4 tys. abonentów w 60 miastach północnych i wschodnich stanów USA oraz w Kanadzie, autostradowy Highway – 1900 abonentów (głównie transportowców). Według ironicznego powiedzonka bogaci biznesmeni (w przeliczeniu na dzisiejszą siłę nabywczą abonament wynosił ponad 210 dolarów miesięcznie, minuta rozmowy od 4,20 do niemal 6 dolarów) mogli z samochodu wykonać dwa połączenia: jedno do żony, że spóźnią się na obiad, a drugie do elektryka samochodowego, że jadą do niego doładować akumulator. Telefony nie miały funkcji wybierania numerów – trzeba się było połączyć z centralą, która łączyła abonentów ręcznie, zupełnie jak pół wieku wcześniej w sieciach stacjonarnych. Dostępnych kanałów radiowych było tak mało, że jednocześnie w sieci mogło wykonywać połączenia tylko 3 abonentów. Jeszcze w 1965 r. w unowocześnionej sieci IMTS (ok. 40 tys. abonentów) abonenci w Nowym Jorku, których było ok. 2 tysięcy, mieli do dyspozycji tylko 12 kanałów radiowych, a na wykonanie połączenia musieli czekać do 30 minut, choć już mogli sami wybierać numer tarczą.

Sieci 1G (analogowe) i 2G (cyfrowe GSM) w zasadzie służyły do wykonywania połączeń głosowych, choć obsługiwały także transmisję danych z maksymalną prędkością 2,4 kbps (1G) i 9,6 kbps (2G, protokół CSD[1]). O prawdziwym Internecie mobilnym możemy mówić dopiero od uruchomienia w sieciach 2G pakietowej transmisji GPRS. Już w 1992 r. ruszyły prace nad 3G, w 1999 r. ITU zatwierdził 5 technologii transmisji w ramach specyfikacji IMT-2000. W 2001 r. uruchomiono pierwsze komercyjne sieci 3G/UMTS w standardzie W-CDMA w Japonii (NTT DoCOMo) i w Norwegii (Telenor) oraz w standardzie CDMA2000 1x EV-DO w Korei Płd. (KT) i USA (Monet) – choć z trudnościami, bo na rynku niewiele było telefonów i modemów 3G.

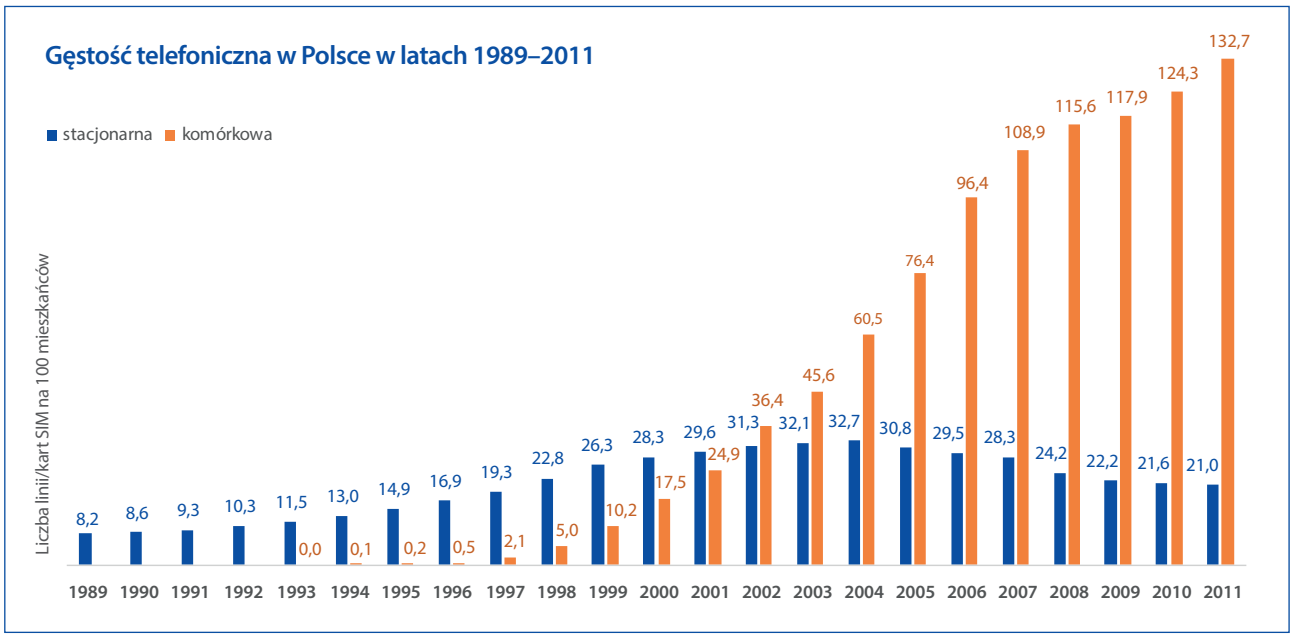
Aukcje i konkursy piękności

Uruchomienie 3G/UMTS w Europie (w tym także w Polsce) poprzedziła „gorączka aukcyjna". Operatorzy – zwłaszcza nowi, którzy dopiero chcieli wejść na rynek zajęty od dekady przez operatorów GSM – byli tak zdeterminowani, że w pierwszych wielkich aukcjach częstotliwości UMTS w kilku krajach europejskich niemal zalicytowali się na śmierć. W 2000 r. w Wielkiej Brytanii 5 operatorów wylicytowało łącznie równowartość 36,9 mld EUR, w Niemczech aukcja doszła do równowartości 50,8 mld EUR, we Włoszech – do 12,6 mld EUR. Kiedy w Holandii licytacja zatrzymała się na poziomie równowartości 2,7 mld EUR, bo spasował jeden z 5 konkurentów do 5 oferowanych licencji, policja – podejrzewając zmowę – zaczęła przeszukiwać biura operatorów. Zupełnie inną drogą poszli regulatorzy rynku np. w Finlandii, Hiszpanii, Irlandii i Szwecji, przydzielając częstotliwości w „konkursach piękności", polegających na ocenie deklaracji dotyczących tempa budowy sieci i osiągania pokrycia obszaru kraju. Za częstotliwości pobierano tylko stosunkowo umiarkowaną opłatę administracyjną.

W Polsce przydział częstotliwości UMTS w 2000 r. także miał dość dramatyczny przebieg. Minister Łączności we wrześniu 2000 r. planował przetarg na 5 licencji po 700-800 mln EUR za każdą z nich. TP SA miała dostać licencję „z urzędu", preferowani mieli być już działający operatorzy. Jednak w ostatniej chwili wycofali się tacy poważni zagraniczni partnerzy krajowych oferentów, jak hiszpańska Telefonica i Hutchison, właściciel operatora „3" na rynkach Europy Zachodniej (warunki określały, że podmiot, którzy otrzyma licencję musi mieć 51% polskiego udziału) i zostało tylko trzech ówczesnych operatorów GSM. Przetarg został unieważniony, resort zdecydował, że zamiast tego rozszerzy 3 wydane im licencje GSM o przedział dla UMTS – za 650 mln EUR za sztukę. Operatorzy zgodzili się na to, choć dla analityków rynku było jasne, że nie było szans odzyskać takich kwot od abonentów w rozsądnym czasie. Operatorzy w kilku innych krajach (np. na Słowacji, na Węgrzech, w Portugalii i Słowenii) zdecydowali się poczekać na rozsądniejsze warunki. Żartowano, że skrót UMTS oznacza *Unlimited Money To Spend*.

U nas trójka operatorów zapłaciła po 10 mln EUR po otrzymaniu koncesji, potem jeszcze po 250 mln w 3 ratach, a pozostałe 390 mln w latach 2005–2022. Do 2011 r., kiedy operatorom zostało do zapłacenia jeszcze ponad 1 mld EUR, trwały batalie o możliwość zamiany tych zobowiązań finansowych na inwestycyjne, podobnie jak to się stało ze zmienionymi wcześniej ustawą wygórowanymi opłatami za koncesje międzymiastowe i międzynarodowe od operatorów sieci stacjonarnych. Mowa była nawet o zamianie zobowiązania na zakupy przez operatorów GSM/UMTS laptopów dla uczniów, ale budżet nie odpuścił. Dopiero w 2005 r. wpuszczono na rynek czwartego operatora, międzynarodową grupę P4. P4 koncesję dostała jeszcze jako Netia Mobile, ale zaraz zmieniła nazwę na Play. Bardzo odważnym krokiem była decyzja Playa o działaniu tylko w telefonii 3G – w łączności 2G udało się namówić regulatora do zezwolenia na skorzystanie z roamingu krajowego w sieci Plus Polkomtela (do 2019 r., obecnie głównie w sieci Orange). Mimo początkowej „drogi przez mękę" w pozyskiwaniu

[1] Do 115 kbps w technologii HSCSD, jeśli sieć obsługiwała łączenie 8 slotów czasowych



Źródło: na podstawie danych GUS

zezwoleń na stawianie własnych stacji bazowych (w sieciach 3G nazywanych Node B), co opóźniło start Playa o ponad pół roku, od marca 2007 r. sieć rozwijała się tak szybko, że według corocznych raportów UKE w latach 2017–2020 r. zajmowała już pierwsze miejsce w udziale w rynku pod względem liczby użytkowników (28–29%).

Liczba aktywnych kart SIM na koniec I kwartału 2021 r.	
Sieć	**mln**
Orange	15,8
Play	15,4
Plus	12,8
T-Mobile	11,2
pozostałe	2,1

Na podstawie https://www.my-mobile.pl

Po co nam sieć 5G

I w Polsce, i na całym świecie zarówno operatorzy, jak i użytkownicy wiążą spore nadzieje z sieciami 5G – ale nie tylko z powodu osiąganych w nich wysokich prędkości transmisji. Z wysokich prędkości i niskich opóźnień zgodnych ze specyfikacjami ITU-R (patrz tabela) mogą się cieszyć miłośnicy oglądania filmów i seriali oraz transmisji sportowych na komórkach czy uczestnicy gier online. Ważniejsze są jednak inne charakterystyki 5G, dzięki którym można je wykorzystywać w trzech różnych obszarach zastosowań.

Podstawowe parametry sieci 3G, 4G i 5G			
Sieć	Prędkość transmisji (Mb/s)		Opóźnienia
	DL (downlink)	UL (uplink)	
3G/UMTS	14,4	5,5	100–500
4G/LTE/LTE-Advanced	100–300	50–75	10–200
5G	400–3000	500–1500	1–20

Na podstawie publikacji ITU i innych

Niezwykle istotną z punktu widzenia zastosowań cechą architektury sieci 5G jest możliwość jej segmentowania (*network slicing*). Poszczególne segmenty (zwane też plastrami) mogą działać z różnymi parametrami, w zależności od warunków i potrzeb. Dzięki temu można tworzyć w tej samej infrastrukturze fizycznej wirtualne niezależne sieci logiczne, każdy segment (plaster) jest odizolowaną siecią o parametrach dostosowanych do sposobu wykorzystania. W dodatku dzięki wysokiej wydajności widmowej (do 30 bitów/sek/Hz – dla porównania wydajność widmowa sieci 4G sięga 2 bitów/sek/Hz)[2], osiąganej dzięki zaawansowanym technikom kodowania sygnału w sieciach 5G można jednocześnie ob-

2 Wydajność widmowa określa efektywność wykorzystania pasma radiowego. W sieciach komórkowych używa się także wskaźnika wydajności w bit/s/Hz na jednostkę obszaru lub na stanowisko, który pokazuje, jak wielu użytkowników lub usług można jednocześnie obsłużyć/dostarczyć przez pasmo o danej częstotliwości radiowej na zdefiniowanym obszarze.

służyć do 1 mln urządzeń na km² (w sieciach LTE 1 mln urządzeń, ale rozproszonych na obszarze 500 km²).

Wspomniane trzy główne obszary zastosowań 5G, które można realizować jako trzy „plastry" to:

- eMBB (*enhanced Mobile Broadband*) – dostęp wysokich prędkości;
- URLLC (*Ultra Reliable Low Latency Communications*) – zastosowania wymagające bardzo niskich opóźnień (poniżej 1 ms) i/lub wysokiej niezawodności (stopy błędów);
- mMTC (*massive Machine Type Communications*) – masowa obsługa urządzeń Internetu Rzeczy (IoT).

Zastosowania eMBB to nie tylko szerokopasmowy dostęp w ruchu (np. w samochodzie czy w pociągu), lecz także FWA (*Fixed Wireless Access*) – bezprzewodowy dostęp stacjonarny stanowiący alternatywę dla sieci przewodowych, ze zbliżoną do takich sieci gigabitową prędkością i opóźnieniami rzędu 4–5 ms.

Segment URLLC z uwagi na czasy opóźnień nawet poniżej 1 ms oraz stopę błędów na poziomie 10^{-5} to zastosowania w transporcie, w tym transporcie autonomicznym, w energetyce, a także w rozwiązaniach rzeczywistości rozszerzonej i wirtualnej (AR/VR), przydatnych w bardzo wielu dziedzinach.

W segmencie mMTC wykorzystuje się przede wszystkim wynikającą z wysokiej wydajności możliwość obsługi do 1 mln urządzeń (np. urządzeń IoT) na km², a więc parametr potrzebny w takich dziedzinach, jak: przemysł 4.0, miasta inteligentne czy osobiste czujniki stosowane w ochronie zdrowia.

Cała sieć 5G realizowana jest w zunifikowanej architekturze All-IP z zastosowaniem protokołu IPv6, obsługującego wielokrotnie rozszerzoną przestrzeń adresową. Poszczególne „plastry" sieci mogą być zarządzane niezależnie od siebie i dynamicznie rekonfigurowane w zależności od warunków i potrzeb.

Według danych GSA, światowego stowarzyszenia producentów sprzętu dla sieci mobilnych, w końcu września 2021 r. 796 operatorów w 240 krajach i regionach dostarczało komercyjne usługi LTE mobile i/lub FWA, zaś 180 operatorów w 72 krajach i regionach usługi mobilne i/lub stacjonarne 5G. Zaczyna się już wyłączanie usług poprzednich generacji (2G/3G), przy czym ze względów praktycznych wcześniej zaczęto wyłączać sieci 3G. W Europie większość operatorów ma zamiar rozpocząć wyłączanie 3G już w ciągu najbliższych dwóch lat, a wyłączanie sieci 2G (zapewniającej łączność głosową z wykorzystaniem starszych telefonów i w obszarach o niskiej gęstości sieci) odkłada na lata po 2025 r.[3]. Na przykład w Czechach, Grecji, Holandii, Niemczech i Norwegii niektórzy operatorzy już wyłączyli 3G – albo całkowicie, albo tylko w wyższych pasmach, przeznaczając zwolnione częstotliwości na 4G i 5G[4].

Według prognoz zaprezentowanych w czerwcowym wydaniu corocznego raportu „Ericsson Mobility Report"[5] w 2026 r. na świecie ma już być 3,5 mld użytkowników 5G (licząc terminale mobilne oraz FWA, bez uwzględniania urządzeń IoT), a więc udział 5G w ogólnej liczbie użytkowników/abonamentów, która w 2026 r. ma sięgnąć 8,8 mld, będzie już istotny.

Na razie w Europie do wykorzystania komercyjnego – obok częstotliwości współdzielonych z 4G – przewidziano trzy główne pasma:

- pasmo 700 MHz – dające zasięgi rzędu kilku kilometrów, dobre przenikanie do wewnątrz budynków, prędkości do 50–250 Mb/s i wydajność widmową przybliżoną do 4G (2 b/s/Hz);
- pasmo 3,4–3,8 GHz – charakteryzujące się zasięgiem kilkuset metrów, wysokimi prędkościami (głównie dla segmentu eMBB) i dobrą wydajnością (4–8 b/s/Hz);
- pasma wysokich częstotliwości (26/39/42 GHz) – z zasięgiem rzędu 200–500 m, gigabitowymi prędkościami i wydajnością widmową sięgającą 30 b/s/Hz.

Pewnym problemem wykorzystania pasm wysokich częstotliwości jest słabe przenikanie fal radiowych tych częstotliwości do wewnątrz budynków. W nowoczesnych biurowcach stosuje się coraz więcej szkła termicznego, w tym także fotowoltaicznego, które stanowi skuteczną zaporę dla

3 Użytkownicy nowszych telefonów (i operatorzy, którzy umożliwiają taką usługę) mogą korzystać z łączności głosowej w trybie VoLTE (Voice-over-LTE).

4 W Polsce T-Mobile w październiku br. wyłączył 3G w paśmie 2100 MHz, zostawiając 3G w paśmie 900 MHz.

5 https://www.ericsson.com/4a03c2/assets/local/reports-papers/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf

łączności w pasmach gigahercowych. Problem ten trzeba będzie rozwiązywać poprzez odpowiednią architekturę sieci – rozmieszczenie stacji bazowych wewnątrz pomieszczeń.

Regulatorzy przydzielający pasma częstotliwości mają dwa istotne dylematy:

- w jaki sposób przydzielać pasma operatorom: za wylicytowane w aukcjach wielkie kwoty (zasypujące dziury budżetowe, oczywiście płacone przez operatorów za pieniądze użytkowników ich sieci), czy za stosunkowo umiarkowaną opłatę administracyjną w „konkursach piękności" (co jednak wymaga bardzo starannego przygotowania warunków oceny ofert, bywa też dużo bardziej podatne na protesty uczestników konkursów);

- jak szerokie fragmenty pasma przydzielać poszczególnym operatorom.

Z nieubłaganych praw fizyki i informacji (twierdzenie o przepustowości Shannona-Hartleya) wynika, że przepustowość transmisji można zwiększyć albo przez podwyższenie mocy, albo przez zmniejszenie szumów (polepszenie stosunku sygnału do szumu), albo przez zwiększenie szerokości pasma. Te możliwości są ograniczone z różnych powodów.

Moc sygnału można podwyższać, ale pociąga to za sobą zwiększenie zużycia energii, a górnym pułapem są ustalone normy wielkości emisji. Kwestia jest drażliwa społecznie – pamiętamy obawy, protesty, a nawet próby podpalania masztów stacji bazowych.

Można polepszyć stosunek sygnału do szumu, wprowadzając coraz bardziej zaawansowane metody kodowania sygnału. Stosowane są różne adaptacyjne techniki modulacji, wielodrogowości sygnału, zwielokrotniania przestrzennego. Wszystko to jednak komplikuje systemy, wymagając odpowiednich rozwiązań sprzętowych (w tym złożonych systemów antenowych) i software'owych, podwyższając też „narzut administracyjny" elementów kodujących na sygnale użytkowym. W systemach wielodrogowych pojawiają się też – wynikające z istoty tych technik – problemy m.in. z kilkoma przesuniętymi w czasie kopiami tego samego sygnału radiowego czy z interferencjami międzysymbolowymi.

Z szerokością przydzielanego pasma pewien problem mają regulatorzy. Ze wspomnianego twierdzenia Shannona-Hartleya wynika, że im szersze jest pasmo, w jakim prowadzona jest transmisja, tym większa jest prędkość i wydajność. Obecnie operatorzy działający w Polsce dysponują na różnych częstotliwościach różnymi segmentami – od 2 x 4,4 MHz do 2 x 15 MHz w architekturze FDD[6] (grupa Cyfrowego Polsatu/Polkomtela ma też blok 50 MHz w architekturze TDD[7] w pasmie 2600 MHz). Tymczasem do osiągania wysokiej przepustowości 5G potrzebne są pasma dużo szersze. Na przykład w anulowanej polskiej aukcji w marcu 2020 r. UKE zamierzało w paśmie 3,6 GHz przydzielać bloki po 80 MHz, we wrześniowej aukcji w Norwegii w paśmie 2600 MHz przydzielono pasma 2 x 30 i 2 x 40 MHz (FDD), zaś w paśmie 3,6 GHz – bloki od 80 do 120 MHz każdy. W pionierskiej pod tym względem Finlandii w 2018 r. w paśmie 3,4–3,8 GHz przydzielano bloki po 130 MHz, zaś w ubiegłorocznej aukcji na pasmo 26 GHz – bloki po 800 MHz. Im wyższe częstotliwości, tym większe „kawałki" pasma można na nich udostępniać, natomiast w wykorzystywanych do tej pory przez 3G pasmach ok. 2 GHz regulator – zwłaszcza taki bliżej współpracujący z ministrem finansów – ma dylemat: sprzedać mniej bloków szerszych (ale miliardów już się za nie i tak nie weźmie), czy więcej węższych...

Co dalej – 6G, ...?

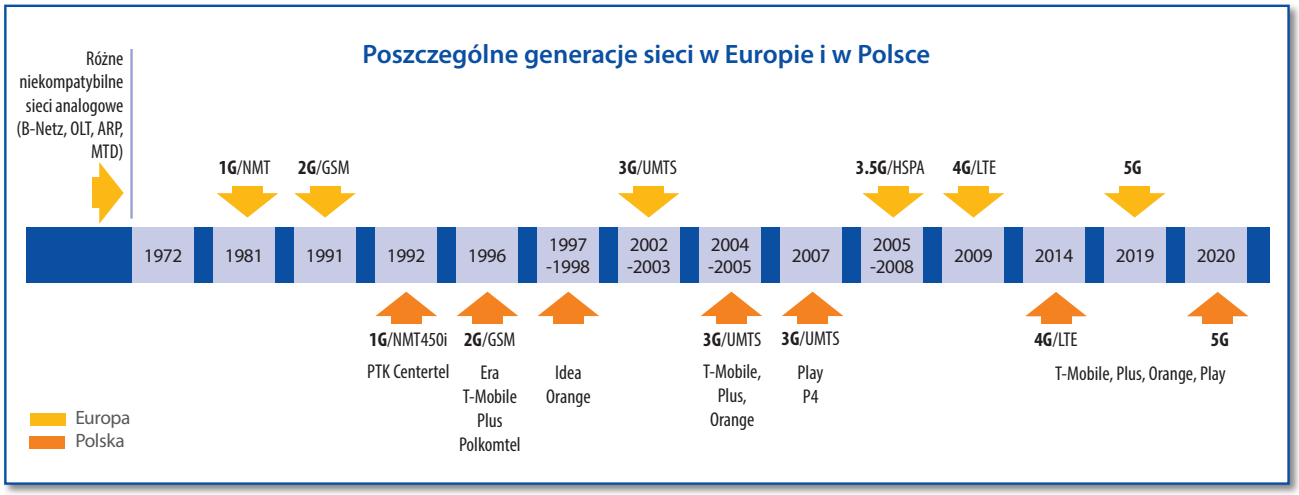
Sieci 5G i planowane dalsze generacje to już sieci w pełni o charakterze SDN/SDR (*Software Defined Networks/Software Defined Radio* – sieci definiowane programowo[8]). Rozwiązania w takich sieciach charakteryzują się stosowaniem uniwersalnych sprzętowych układów „generycznych". Parametry transmisji i ogólnie: działanie urządzeń i sieci uzyskuje się poprzez odpowiednią pracę oprogramowania sterującego. Pozwala to na dynamiczne rekonfigurowanie nie tylko sposobu działania danego urządzenia, lecz także całej sieci lub jej fragmentów, w tym wspomnianych „plastrów", odpowiednio do potrzeb i warunków otoczenia (chwilowe obciążenie, warunki propagacji fal radiowych, oddziaływanie innych sieci, prędkość ruchu terminala itp.).

Zaprojektować taką sieć potrafią ludzie wspierani rozlicznymi specjalistycznymi programami do projektowania jej topologii, parametrów, urządzeń itp., bo tak się to robi już od dobrych kilku(nastu) lat. Kluczowym elementem bieżącego zarządzania siecią, w tym parametrami tysięcy i milionów działających w niej urządzeń, będzie jednak oprogramowanie potrafiące w czasie rzeczywistym reagować na zmieniające się warunki i potrzeby, odpowiednio zmieniając działanie sieci i jej elementów. Dać sobie z tym radę potrafią tylko

6 Frequency Division Duplex – transmisja z podziałem częstotliwości, odbywająca się jednocześnie w dwóch różnych przedziałach częstotliwości.

7 Time Division Duplex – transmisja z podziałem czasu, odbywająca się w tym samym paśmie w naprzemiennie przydzielanych szczelinach czasowych.

8 W zasadzie takimi sieciami są już sieci 4G.



Źródło: opracowanie własne autora

systemy korzystające z metod sztucznej inteligencji, uczące się działania na zebranych w praktyce danych rzeczywistych, używanych najpierw do trenowania algorytmów, a później do ich doskonalenia i modyfikowania na podstawie doświadczeń z eksploatacji sieci.

Na horyzoncie badawczym i planistycznym są już sieci 6G, w których osiągane mają być prędkości do 3 Tb/s i opóźnienia rzędu 0,1 do 1 ms. Działać mają w kolejnych wersjach protokołów IPv6+, umożliwiających działanie sieci jako *App-Aware*, automatycznie dostosowującej swoje parametry do charakteru i potrzeb obsługiwanych aplikacji sieciowych. Nazywa się je także sieciami *Cloud Native* – przeniesienie większości infrastruktury software'owej tych sieci do chmury ma umożliwić adaptacyjne, dynamiczne dostosowywanie nie tylko parametrów sieci, lecz także jej architektury i topologii. Sieci 6G działać będą w pasmach bardzo wysokich częstotliwości: od 100 GHz aż do 3 THz. Mają znaleźć zastosowanie w połączeniu świata realnego, w tym biologicznego, z jego cyfrową reprezentacją, mają obejmować także łączność satelitarną. Oczekuje się, że pierwsze sieci 6G uruchomione zostaną ok. 2030 r.

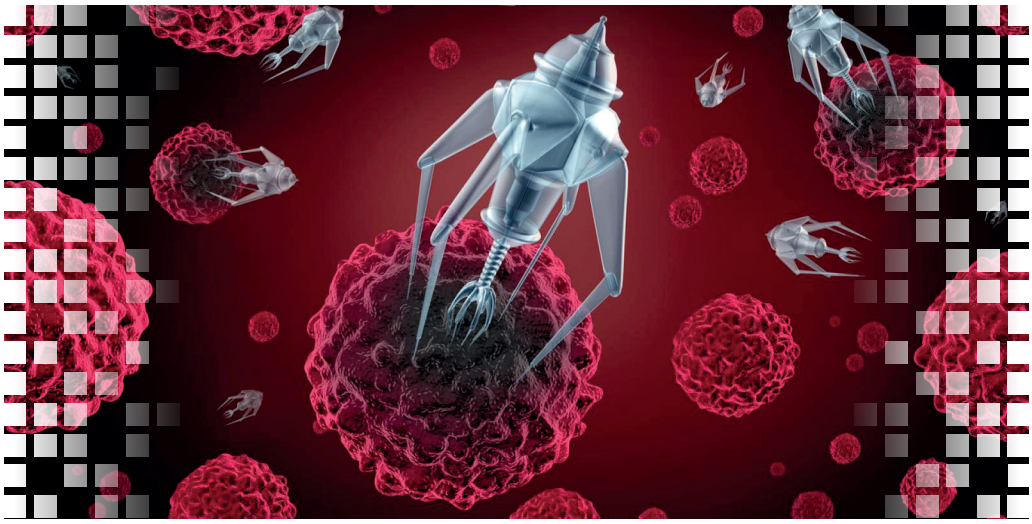
5G w paśmie 700 MHz a KSC

W kolejnych wersjach projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa pojawił się pomysł utworzenia państwowego podmiotu – Operatora Strategicznej Sieci Bezpieczeństwa (OSSB). Może nim być jednoosobowa spółka Skarbu Państwa, będąca jednocześnie operatorem telekomunikacyjnym. Podmiot ten ma powołać spółkę kapitałową o nazwie „Polskie 5G", która będzie hurtowym operatorem sieci 5G w pasmach 713–733 MHz i 768–788 MHz.

„Polskie 5G" będzie zobowiązane do zapewnienia infrastruktury dostępowej na terenie całego kraju. Ma oferować usługi hurtowe z priorytetyzacją ruchu w sytuacjach zagrożenia bezpieczeństwa publicznego. Finansowanie łączności strategicznej ma się odbywać przez rządowy fundusz (ok. 1 mld zł), zasilany opłatami za częstotliwości w pasmach 700 MHz i 3,6 GHz. Na razie trwa tzw. refarming pasma 700 MHz, do tej pory zajmowanego przez naziemną telewizję cyfrową.

Zasady wykorzystywania częstotliwości radiowych określane są przez ITU-R, Sektor Radiokomunikacji Międzynarodowego Związku Telekomunikacyjnego, specjalistycznej agendy ONZ. Polska jest członkiem ITU od 1921 r. Przeglądy, ustalenia i korekty przydziałów pasm dokonywane są na Światowych Konferencjach Radiokomunikacyjnych (WRC) odbywających się co kilka lat. Pierwsza odbyła się w 1903 r.; konferencja w 1912 r. miała miejsce kilka miesięcy po katastrofie Titanica i jednym z jej rezultatów było ustalenie zasad łączności ratunkowej w żegludze morskiej.

Na WRC-15 w 2015 r. przeznaczono dla 5G pasmo 700 MHz w Regionie 1 (Europa, Afryka, teren b. ZSRR, Mongolia, Bliski Wschód) oraz w kilku krajach Regionu 3 (Azja i Oceania), a także pasmo 3,4–3,8 GHz dla Regionu 1, Regionu 2 (obie Ameryki) oraz niektórych krajów Regionu 3. Na WRC-19 określono wykorzystanie pasm wysokich (24,25–27,5 GHz, 37–43,5 GHz, 45,5–47 GHz, 47,2–48,2 GHz oraz 66–71 GHz) oraz „koegzystencji" z pasmami badawczymi i łączności satelitarnej (23,6–24 GHz i 24,25–27,5 GHZ). W programie WRC-23 zapowiedziano uporządkowanie pasm 3300–3400 MHz, 3600–3800 MHz, 4800–4990 MHz, 6425–7025 MHz, 7025–7125 MHz oraz 10–10,5 GHz.



Źródło: https://www.futuresplatform.com/blog/can-we-use-nanobots-cure-cancer

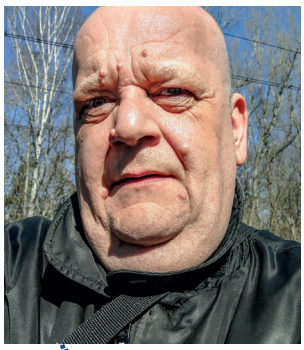
Cyfrowe ingerencje w tożsamość człowieka

Pandemia spowodowana przez wirusa SARS-Cov2 odbiła się w świecie szerokim echem lockdownów, zablokowanych szpitali i nadmiarowych zgonów. Jednak ma ona też swoje drugie dno – stała się katalizatorem przemian zachodzących zarówno w technice, jak i w świadomości przeciętnego człowieka.

Profesor Klaus Schwab, założyciel i prezes Światowego Forum Ekonomicznego (WEF) organizującego m.in. znane konferencje finansjery i polityków w Davos, napisał w swojej niedawno wydanej książce „Covid-19. The great reset": *Wielu z nas zastanawia się, kiedy sytuacja wróci do normy. Krótka odpowiedź brzmi: nigdy (…) ponieważ pandemia koronawirusa stanowi fundamentalny punkt zwrotny (…) Nadchodzą radykalne zmiany o takich skutkach, że niektórzy eksperci odnoszą się do ery przed koronawirusem (BC) i po koronawirusie (AC).*

Cywilizacja na rozstaju dróg

Schwab nie ukrywa, że obecnie coraz częściej większą przeszkodą w dalszym postępie stają się problemy etyczne i opory ludzi przed wprowadzaniem nowych technologii, a nie bariera technologiczna jako taka. Dlatego pandemia ma być punktem zwrotnym w nadchodzącym przewrocie technologicznym, określonym wcześniej przez Schwaba mianem „czwartej rewolucji przemysłowej". Na dowód swojej tezy przytacza on różne przykłady – m.in. pisze o firmie, która z powodu pandemii w ciągu dwóch tygodni wdrożyła program



Jacek Grabowski

z wykształcenia specjalista gazownictwa i górnictwa naftowego, przygodę z informatyką rozpoczął w końcu lat 80. XX wieku od współpracy z wydawnictwem „Lupus", gdzie publikował teksty głównie w dwutygodniku „PCkurier" i miesięczniku „Enter". Współtwórca pierwszego w Polsce informatycznego czasopisma B2B „MRK" (1997). Były redaktor naczelny miesięcznika „Reset", współpracownik wielu innych tytułów (magazyn „WWW", „IT Reseller", „Komputer Świat"). Obecnie freelancer, współpracuje m.in. z warszawską komunikacją miejską.

cyfrowej platformy sprzedażowej wcześniej zaplanowany na 18 (!) miesięcy, ratując się w ten sposób przed bankructwem.

Lawinowy wzrost sprzedaży i kontaktów online spowodowany koronawirusem związał jeszcze silniej z Internetem zarówno pojedynczych ludzi, jak i firmy, powodując błyskawiczne poszerzenie zakresu cyfryzacji stosunków społecznych. Połączenie z globalną siecią stało się nagle koniecznością. Przykład ten pokazuje nam, że koronawirus wytworzył sytuację, w której technologie już istniejące i rozpowszechnione, ale wcześniej traktowane przez część ludzi nieufnie, czy też niespiesznie wdrażane, mogą nagle przyspieszyć i znaleźć się w centrum zainteresowania. Jest to szczególnie interesujące w kontekście takich dziedzin, wokół których pojawia się najwięcej etycznych znaków zapytania. Możemy tu np. wskazać robotykę, sztuczną inteligencję, genetykę czy bardziej ogólnie – medycynę.

Umysł z tożsamością cyfrową

Wiele wskazuje na to, że zbliżamy się nie tylko do momentu tzw. technologicznej osobliwości, w którym AI wyprzedzi mózg ludzki, lecz także do chwili, w której komputery i związana z nimi nasza tożsamość cyfrowa zostaną zintegrowane z naszymi ciałami, a może nawet z układem nerwowym. Wtedy komputerowa „dźwignia" dla umysłu będzie dyktować swoje mądrości bezpośrednio do naszych myśli… Sztuczna inteligencja wspomoże inteligencję naturalną. Niemożliwe? Fantastyczne? W raporcie „Deep Shift", opracowanym przez WEF w 2015 r. i obficie cytowanym przez Klausa Schwaba, wskazany jest rok 2025 jako moment pojawienia się wszczepianego telefonu komórkowego. Czytamy tam: *(...) wszczepiane urządzenia prawdopodobnie będą mogły przekazywać myśli wyrażane zwykle werbalnie za pomocą „wbudowanego" smartfona, oraz potencjalnie niewyrażone myśli lub nastroje poprzez odczytywanie fal mózgowych i innych sygnałów.*

Przygotowania do transformacji ciała człowieka przez wszczepianie elektroniki trwają już od jakiegoś czasu. Najprostszym przykładem jest rozrusznik serca. „Biohacking", „biohackerzy" – to terminy określające oddolne ruchy społeczne lub indywidualnych hobbistów/technologicznych freaków, których celem jest przeprowadzanie różnych eksperymentów mających w domyśle na celu „udoskonalenie" człowieka. Nie przypadkiem odwołują się one do hackingu, choć rozumianego w sposób szlachetny – jako prawo dostępu do informacji. W dawniejszych czasach biohacking opierał się raczej na naturalnych środkach i metodach, np. stymulowaniu mózgu poprzez odpowiednią kombinację diety, dyscypliny snu i ćwiczeń. Obecnie coraz częściej mamy do czynienia z tzw. hard biohackingiem, w którym rolę zaczynają grać wszczepiane implanty czy endoprotezy różnych typów.

W Polsce od niedawna mówi się o podskórnym wszczepianiu implantów RFID I NFC, ułatwiających np. płatności zbliżeniowe czy logowania do komputerów. Na razie takie

Implant
Źródło: https://medicalfuturist.com/rfid-implant-chip/

implanty są u nas relatywnie mało przydatne. Poza Polską jest to jednak technika znana znacznie dłużej i w niektórych krajach bardzo popularna, używana np. przez firmy do identyfikacji pracowników. Oczywiście nie są to implanty wchodzące w interakcję z naszym umysłem czy systemem nerwowym, tylko proste czujniki komunikacyjne z zapisanymi danymi, reagujące na inne urządzenia i współpracujące z nimi. Niemniej, jak wszystko wskazuje, jest to dopiero pierwszy, najniższy stopień integracji ciała człowieka z jego cyfrową tożsamością i otaczającymi urządzeniami.

Wszczepianie implantów to inwazyjna, niekoniecznie miła metoda, grożąca konsekwencjami w postaci zakażeń i chorób skóry. Dlatego w zaawansowanych badaniach znajdują się także inne techniki integracji ciała człowieka z elektroniką. Jednym z przykładów mogą być tzw. cyfrowe tatuaże (*smart tattoos*). Z rzeczywistymi tatuażami nie mają one zbyt wiele wspólnego, chodzi o rodzaj silikonowej membrany wszczepianej pod skórę i zawierającej elementy elektroniczne niepotrzebujące dodatkowego zasilania. Taki „tatuaż" miałby połączenie z układem nerwowym człowieka i mógłby być wykorzystywany do różnych celów, w tym np. do sterowania i współpracy z implantami elektronicznymi, choćby ze wspomnianym smartfonem. Opracowano nawet metodę, dzięki której nasz organizm nie odrzucałby takiego „tatuażu" jako ciała obcego i przeprowadzono z sukcesem eksperymenty na zwierzętach. Na razie największym problemem tej techniki jest trwałość „tatuażu", który zbyt szybko ulega zniszczeniu.

Tatuaż cyfrowy
Źródło: https://duoskin.media.mit.edu

Ratowanie życia – kto będzie przeciw?

Nieprzypadkowo właśnie zdarzenie medyczne, w którym pojawiło się realne i poważne zagrożenie życia ludzi – czyli pandemia – może stanowić dźwignię dla nowych, kontrowersyjnych technologii. Wiele rozwiązań można bowiem wytłumaczyć koniecznością ratowania zdrowia i życia człowieka. Zarówno implanty, jak i „cyfrowe tatuaże" miałyby przecież zastosowanie np. w diagnostyce medycznej. Zintegrowane z urządzeniem komunikacyjnym (wszczepionym smartfonem) czujniki połączone z systemem nerwowym mogłyby błyskawicznie informować lekarzy o zagrożeniu życia pacjenta, jednocześnie dostarczając im wystarczająco dużo informacji pozwalających na szybkie postawienie diagnozy. Oprogramowanie sztucznej inteligencji zainstalowane na domowym laptopie mogłoby też pobierać i analizować dane z czujników, a potem stawiać rozpoznania.

To wszystko jest już możliwe nie tylko w teorii. Istnieją zewnętrzne czujniki monitorujące ciśnienie krwi czy puls, mogą one też komunikować się z innymi urządzeniami, na których jest np. zainstalowane konsumenckie oprogramowanie zbierające i analizujące dane np. do treningów. Istnieje już także całkiem zaawansowane oprogramowanie medycznej sztucznej inteligencji. Na przykład lekarze z Uniwersytetu Nottingham zastosowali system AI do analizy rutynowych danych diagnostycznych kilkuset tysięcy pacjentów. System nie tylko osiągnął nieco lepszą dokładność diagnoz niż lekarze (o 2 proc.), ale dzięki niemu udało się zapobiec poważnym konsekwencjom zdrowotnym u ponad 300 osób. Kwestią czasu jest więc rozwiązanie kilku problemów technologicznych i zestawienie wszystkich elementów w całość, żeby uzyskać rewelacyjne medyczne narzędzie diagnostyczne.

Nanoprzejażdżka wewnątrz człowieka

Wszczepiane czujniki mogą jedynie dostarczać informacji służącej do postawienia diagnozy; w planach są już przełomowe technicznie narzędzia, które umożliwią także leczenie. Półżartem można powiedzieć, że inspiracją była „Fantastyczna podróż" Isaaca Asimova, w której zminiaturyzowana łódź podwodna wraz z załogą medyczną została wpuszczona do organizmu człowieka, a lekarze dokonali precyzyjnej operacji skrzepu mózgu, ratując życie pacjenta. Dziś mamy już mikroskopijne nanoroboty pracujące wewnątrz ciała pacjenta. Pojęcie „nanorobot" w kontekście medycznym jest przy tym bardzo szerokie: mogą to być zarówno mikroskopijne maszyny, jak i „roboty" biologiczne.

Najprostszym przykładem już stosowanego mikrourządzenia medycznego pracującego wewnątrz organizmu jest tzw. kapsułka endoskopowa. W środku kapsułki o wymiarach 26 lub 30x11 mm (podobnej do takich, w których przyjmujemy np. preparaty witaminowe) znajduje się specjalna kamera cyfrowa z obiektywem, lampa LED, antena i nadajnik. Istotną częścią zajmującą niemal połowę objętości urządzenia jest bateria, która musi zapewnić zasilanie przez cały czas badania trwającego kilka godzin. Do ciała pacjenta na czas badania przyklejane sa elektrody-anteny połączone z odbiornikiem gromadzącym zdjęcia robione przez kamerę.

Kapsułka to jeszcze nie robot

Kapsułka endoskopowa działa właściwie na ślepo. Ruch zapewniają jej naturalne właściwości organizmu człowieka, a urządzenie jest po jakimś czasie wydalane naturalną drogą. Lekarze podczas badania nie mają możliwości dokładnego zlokalizowania miejsca, w którym znajduje się kapsułka w danym momencie, nie mogą też stwierdzić, jakie jest jej położenie względem fotografowanych narządów, ani w jakim dokładnie miejscu badanego narządu znajdują się sfotografowane zmiany chorobowe. Kamera w kapsułce dostarcza masę fotografii (ok. 50 tys.), ale są to obrazy przypadkowe, przedstawiające to, co uchwyci obiektyw z odpowiednio szerokim kątem widzenia. Analiza takiej liczby obrazów o niezbyt wysokiej rozdzielczości jest oczywiście czasochłonna i bardzo trudna, dlatego pomocne są w niej m.in. odpowiednie programy komputerowe.

Kapsułka endoskopowa
Źródło: https://hamiltongi.com/capsule-endoscopy/

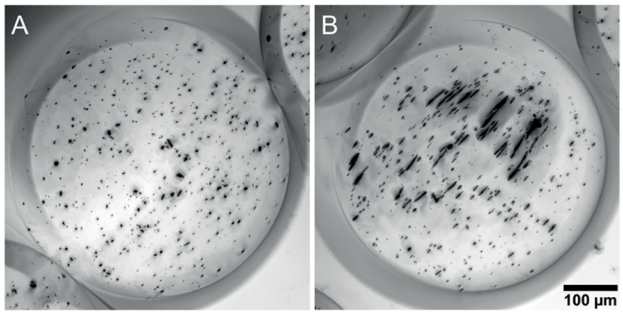
Przykład kapsułki pokazuje, że w obecnych badaniach naukowców nad nanorobotami medycznymi największą rolę grają dwie kwestie: sterowanie ruchem i napęd. Obie zresztą są trudne do rozwiązania, choć pojawiają się różne propozycje. Jednym z bardziej zaawansowanych i rokujących duże nadzieje rozwiązań jest projekt MANiAC (Magnetically Aligned Nanorods in Alginate Capsules). Zastosowano w nim pole magnetyczne do sterowania alginianowymi żelowymi kapsułkami, w których zostają zatopione specjalne nanopręciki. Dzięki nim kapsułka reaguje na zewnętrzne pole magnetyczne i może być prowadzona wewnątrz organizmu, np. precyzyjnie dostarczając lekarstwo lub robiąc zdjęcia. Badania wykazały, że kapsułka MANiAC jest zdolna do zawracania „pod prąd" w cieczy imitującej płyn mózgowo-rdzeniowy i może również – w pewnym zakresie – wspinać się pod górę.

Istnieją także inne propozycje magnetycznego napędu nanorobotów, wykorzystujące szczególny rodzaj nanostruktury ze stopu żelazowo-platynowego o właściwościach magnetycznych przewyższających najsilniejsze znane mikro-

magnesy (NdFeB), przy jednoczesnym zachowaniu stabilności chemicznej i biozgodności. Naukowcy z trzech ośrodków: Instytutu Nanotechnologii Russella Berriee, Instytutu Maksa Plancka i Uniwersytetu w Stuttgarcie opanowali proces technologiczny i wytworzyli na bazie tego materiału „nanośmigła" przypominające kształtem rozciągnięte wiertła. Takie „nanośmigło" jest wielkości bakterii, może być sterowane względnie słabym polem magnetycznym i ma zdolność poruszania się z prędkością rzędu 13 własnych długości na sekundę. Za jego pomocą można również aktywnie dostarczać np. geny do komórek, lekarstwa itd.

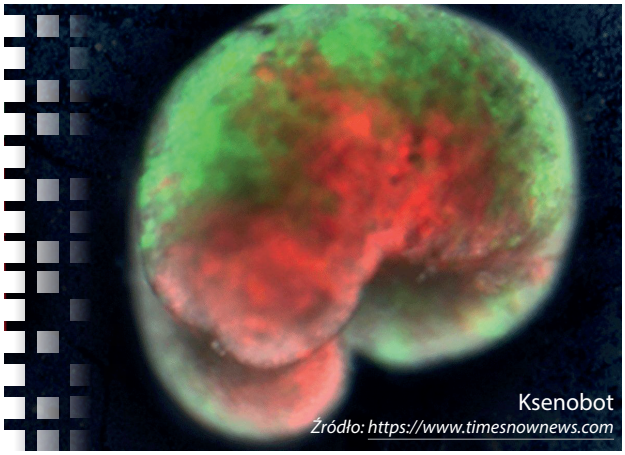
Roboty biologiczne

Jednym z trendów w medycynie, które szybko rozwinęły się zwłaszcza od czasu odkrycia przez Jennifer Doudna i Emmanuelle Charpentier (Nobel 2020) metody edycji genów znanej jako CRISPR-Cas9, jest modyfikowanie bakterii i wirusów w taki sposób, żeby mogły one – wniknąwszy do organizmu człowieka – reprogramować chore komórki w celu ich wyleczenia. Konstrukcja wirusów jest na tyle prosta, że dość łatwo je zmieniać i wykorzystać jako nośniki wybranych genów. Po wniknięciu w komórkę taki wirus „programuje" ją, przekazując inny zestaw instrukcji. Naukowcy z instytutu onkologicznego w São Paulo pod kierownictwem Bryana Erica Straussa na podstawie reprogramowanego wirusa przeprowadzili na myszach eksperymentalną terapię zwalczającą raka prostaty. Myszom wszczepiono ludzkie komórki rakowe i po utworzeniu się guzów wstrzykiwano bezpośrednio do nich zmodyfikowanego wirusa, który reprogramował komórki guza w taki sposób, aby obumarły. Wyniki badań były zachęcające, przy czym okazało się, że najlepsze efekty daje symultaniczne stosowanie terapii „wirusowej" i klasycznej chemioterapii.



MANiAC
Źródło: https://www.mdpi.com

Jeszcze bardziej szokującym i niekonwencjonalnym wynalazkiem są tzw. ksenoboty. Jest to zupełnie nowy organizm „wyhodowany" przez naukowców wspomaganych sztuczną inteligencją. Uzyskano w ten sposób biologiczne „urządzenie", zresztą sami twórcy mówią o swoich odkryciach, że to nowa forma produkcji urządzeń. Posłużono się tutaj komputerową symulacją ewolucji organizmu stworzonego z pluripotencjalnych komórek macierzystych pewnego gatunku żab, nazywanego po łacinie *Xenopus laevis* (stąd nazwa „ksenobot"). Na podstawie wyników działania symulacji ręcznie „zbudowano" prosty organizm, łącząc komórki żaby w struktury zaprojektowane komputerowo. Wyniki okazały się bardzo obiecujące, wstępne założenia zostały wypełnione, biologiczny „robot" był zdolny do poruszania się i samoregeneracji(!). Takie biourządzenie może „żyć" około tygodnia bez zewnętrznego źródła energii, potem po prostu obumiera jak każda inna komórka. Ksenobot nie może się rozmnożyć, nie myśli ani nie ma świadomości. Trudno powiedzieć, czy jest żywy, chociaż nie jest martwy. To pierwszy sztuczny – w pełni tego słowa – organizm stworzony z naturalnego materiału genetycznego.



Ksenobot
Źródło: https://www.timesnownews.com

Wyzwanie dla świata

Celowo skupiłem się w tym tekście na takich aspektach „wielkiego resetu" czy też „czwartej rewolucji przemysłowej", które wydają się najbardziej kontrowersyjne. Cyfryzacja handlu i przemysłu to zagadnienia, które toczą się w pewnym sensie mimo społeczeństwa, zwykle niedostrzegane i banalizowane przez masy. Czy słusznie – to inna sprawa, jednak łatwiej się nam z nimi pogodzić niż z technologiami głęboko wnikającymi w nasze ciała i umysły. Dlatego czekający nas szok technologiczny w postaci urządzeń integrujących się z naszym ciałem, a może i z psychiką, na pewno jest czymś, co niełatwo będzie zaakceptować.

To jasne, że choć nowe technologie mają wiele plusów, niosą także wiele potencjalnych zagrożeń dla naszej prywatności, intymności i wolności osobistej. Nawet przy założeniu, że „gentlemen's agreement" między społeczeństwem a władzą spowoduje, że urządzenia będą wykorzystywane tylko w „dobrych" zastosowaniach, trudno nie przewidzieć, że znajdą się tacy, którzy będą chcieli wykorzystać je w celach „złych". Współczesne Chiny są przykładem, jak technologie mogą negatywnie wpływać na życie prywatne obywateli. Tak czy owak czeka nas w najbliższych latach konieczność dostosowania się do nowego świata. Przeorientowaniu ulegnie wiele zagadnień etycznych. Będziemy musieli zupełnie inaczej spojrzeć na siebie i swoją rolę w świecie.

Trzecia linia obrony w cyberbezpieczeństwie

„Ważnym elementem zagwarantowania jakości i przejrzystości procesów oceny zgodności są przepisy dotyczące skarg. (...) skarga może być podstawą do podjęcia działań nadzorczych wobec danej jednostki, przeprowadzenia audytu czy kontroli w tej jednostce". To cytat z uzasadnienia nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (uksc)(https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html). Czas ponownie wyjaśnić, co to jest audyt i jaką odgrywa rolę w cyberbezpieczeństwie.

Jak zaznaczono w *Glosariuszu terminów dotyczących kontroli i audytu w administracji publicznej* (https://www.nik.gov.pl/plik/id,3364.pdf) wydanym wspólnie przez NIK, KPRM, MF i MSW:

- kontrola to przyjęty system zarządzania (procedury, instrukcje, zasady, mechanizmy) służący do uzyskania racjonalnej pewności, że cele zarządzania zostaną osiągnięte;
- audyt to badanie lub przegląd polegający na ustaleniu stanu faktycznego, porównaniu go ze stanem wymaganym (pożądanym) oraz dokonanie jego oceny.

Z kolei według ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, przeprowadzenie kontroli ma na celu ocenę działalności jednostki kontrolowanej dokonaną na podstawie ustalonego stanu faktycznego przy zastosowaniu przyjętych kryteriów kontroli. Czyli kontrola w administracji rządowej to de facto tradycyjny audyt.

Przytoczę jeszcze moją własną definicję audytu opracowaną na podstawie zapisów zawartych w różnych przepisach oraz dokumentach uznanych podmiotów zajmujących się audytem i zapewnieniem (ang. assurance):

Joanna Karczewska
audytor SI, ekspert ds. cyberbezpieczeństwa i ochrony danych osobowych

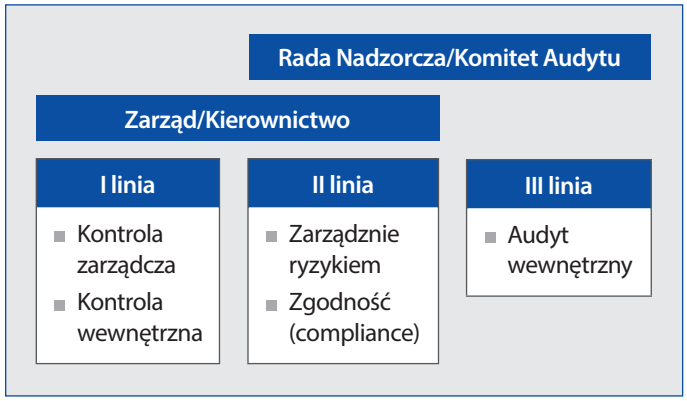
Audyt to:

- przeprowadzenie **niezależnego** badania/przeglądu stanu faktycznego,
- wydanie **obiektywnej i niezależnej** oceny,
- przedstawienie wniosków i rekomendacji,

zgodnie z przyjętymi standardami i kryteriami oceny.

KRI albo nie KRI

W 2013 r. The Institute of Internal Auditors opublikował tzw. position paper „The Three Lines Of Defense In Effective Risk Management And Control". W dokumencie zdefiniowano trzy linie obrony, które w każdej organizacji składają się na skuteczne zarządzanie ryzykiem i efektywną kontrolę, wdrożone w organizacji:



Tym samym podkreślono znaczenie audytu wewnętrznego w zarządzaniu także ryzykiem wynikającym z coraz większego stosowania systemów informatycznych w działalności wszelkich podmiotów – dużych i małych.

Toteż należy chwalić zapis zawarty w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (w skrócie KRI) o zapewnianiu przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Audytu, nie kontroli. Audytu, który wskaże słabości systemu zarządzania bezpieczeństwem informacji coraz częściej przetwarzanych w systemach informatycznych „online – zdalnie – przez internet". Audytu, który jednostka może zlecić audytorowi zewnętrznemu. Sama przeprowadziłam wiele audytów KRI i zawsze we współpracy z audytorem wewnętrznym, by mógł monitorować realizację zaleceń (standard audytu ISACA 1402 Follow-up Activities).

Zgodnie z RODO przeprowadzanie audytów, w tym audytów bezpieczeństwa przetwarzania, należy do inspektora ochrony danych (ang. DPO). W jego przypadku Grupa Robocza Art. 29 w Wytycznych nr 243 na pierwszym miejscu stawia wymóg odpowiedniej wiedzy z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak **również** dogłębnej znajomości RODO. I dodaje: „DPO powinien również posiadać odpowiednią wiedzę na temat operacji przetwarzania danych, systemów informatycznych oraz zabezpieczeń (ang. data security) stosowanych u administratora i jego potrzeb w zakresie ochrony danych". Trochę martwi słowo „również", bo deprecjonuje umiejętności umożliwiające fachowy audyt bezpieczeństwa przetwarzania. Sama jestem DPO i wiem, że to właśnie wiedza o zapewnianiu bezpieczeństwa teleinformatycznego jest kluczowa dla ochrony danych osobowych w dobie powszechnej cyfryzacji i zdalnego dostępu.

Ustawa o krajowym systemie cyberbezpieczeństwa także wprowadziła wymóg audytów (nie kontroli) bezpieczeństwa systemów informacyjnych w przypadku:

- operatora usługi kluczowej – co najmniej raz na 2 lata,
- dostawcy usługi cyfrowej – bez podania częstotliwości,
- podmiotów publicznych – obowiązuje zapis KRI (zaznaczono w uzasadnieniu do projektu ustawy).

Wykaz certyfikatów uprawniających do prowadzenia kontroli [audytu] systemów teleinformatycznych zawarty w Rozporządzeniu MSWiA z 2010 r.	Wykaz certyfikatów uprawniających do przeprowadzenia audytu u operatora usługi kluczowej zawarty w Rozporządzeniu MC z 2018 r.
■ Audytor SZBI według normy PN ISO/IEC 27001 ■ Audytor SZ usługami informatycznymi według normy PN ISO/IEC 20000 ■ Audytor systemu zarządzania jakością według normy PN ISO/IEC 9001 ■ CISA ■ CGEIT ■ CIA ■ CISSP ■ SSCP ■ EUCIP Professional, specjalizacja Audytor SI	■ Audytor wiodący SZBI według normy PN-EN ISO/IEC 27001 ■ Audytor wiodący SZ ciągłością działania PN-EN ISO 22301 ■ CISA ■ CISM ■ CRISC ■ CGEIT ■ CIA ■ CISSP ■ SSCP ■ Certified Reliability Professional ■ ISA/IEC 62443 Cybersecurity Expert

Kryteria oceny

A po co są kryteria oceny? By oceniać obiektywnie. Standardy, normy, metodyki, wytyczne i dobre praktyki stanowią zbiorową mądrość zawodową specjalistów z całego świata. Korzystanie z nich do oceny jest ze wszech miar rekomendowane, bowiem zarówno audytor, jak i audytowany będą wiedzieć, z czym porównywany zostanie stan faktyczny. W ten sposób wykluczona zostaje uznaniowość. Dlatego standard audytu ISACA 1004 UZASADNIONE OCZEKIWANIA (ang. Reasonable Expectation) zaleca audytorom, by podejmowali się wykonania audytu tylko wtedy, gdy jego przedmiotowy zakres można ocenić na podstawie stosownych kryteriów. Zaś standard audytu ISACA 1008 KRYTERIA wymaga od audytorów, by wybierali kryteria oceny przedmiotowego zakresu, które są obiektywne, kompletne, relewantne, wymierne, jasne, powszechnie uznane, miarodajne i zrozumiałe przez lub dostępne dla wszystkich czytelników i użytkowników raportu. Wymienione standardy audytu ISACA obowiązują audytorów z certyfikatami CISA, CISM, CRISC i CGEIT.

W KRI wskazano podstawowe kryteria oceny systemu zarządzania bezpieczeństwem informacji w postaci norm PN-ISO/IEC 27001, 27002, 27005 i 24762 (norma wycofana w 2016 r.). Wprawdzie w Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych wydanych przez Ministerstwo Cyfryzacji w 2015 r. zaznaczono, że KRI nie nakłada obowiązku stosowania wskazanych norm i że normy mogą być stosowane w dowolnym zakresie. Jednakże stanowią podstawę oceny wydanej przez audytorów.

W RODO nie określono żadnych kryteriów oceny dość enigmatycznych „odpowiednich środków technicznych i organizacyjnych" dotyczących bezpieczeństwa przetwarzania. W motywie 83 zaznaczono tylko, że „oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych".

Ustawa o krajowym systemie cyberbezpieczeństwa wymaga uwzględnienia norm polskich i międzynarodowych mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych. W rozporządzeniach do ustawy wymieniono tylko Polskie Normy PN-EN ISO/IEC 27001 i PN-EN ISO 22301 (zniknęła z nowszej wersji rozporządzenia wydanego na podstawie art. 14 ust. 4).

O krok dalej poszedł Urząd Dozoru Technicznego. Na potrzeby przeprowadzania audytu organizacji w obszarze cyberbezpieczeństwa opracował własną metodykę oceny *Framework UDTCyber* [https://udt.gov.pl/cyberbezpieczenstwo]. Do norm PN-ISO/IEC 27002 i PN-EN ISO 22301 jako kryterium oceny dodał NIST Cybersecurity Framework. Według autorów „Przygotowany Framework UDTCyber stanowi podstawę do wdrożenia strategii cyberbezpieczeństwa, która wraz z odpowiednimi mechanizmami współpracy z Operatorami Usług Kluczowych wspiera rozwój obszaru cyberbezpieczeństwa".

COBIT też

Szkoda, że Urząd nie dodał także metodyki COBIT opracowanej przez ISACA. Jako jedyna osoba z Polski, która była tzw. Expert Reviewer metodyk COBIT® 5 i COBIT® 2019, jestem jej ambasadorem. Gdy ISACA opublikowała pierwszy projekt COBIT® 5 Framework, zgłosiłam najwięcej uwag spośród wszystkich recenzentów z całego świata. Toteż jeden z autorów, będąc w Warszawie, zaprosił mnie na spotkanie i dwie godziny się tłumaczył z niedoróbek, które wyłapałam. Cieszę się, gdy kolejne podmioty korzystają z niej i polecają innym. Wzruszyłam się, gdy tak się stało w programie „Cyfrowa Gmina".

Zgodnie z Regulaminem Konkursu Grantowego, jego celem jest „wsparcie JST w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji instytucji samorządowych oraz jednostek im podległych i nadzorowanych, a także zwiększenie cyberbezpieczeństwa". W ramach przyznanego grantu obligatoryjne jest przeprowadzenie **diagnozy cyberbezpieczeństwa JST** – zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej – przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu MC z 2018 r. W formularzu określono kryteria oceny:

- art. 21, 22 i 23 uksc i par. 20 KRI (komentarz: są mapowania na PN-ISO/IEC 27001),
- lista zagadnień CERT-u (komentarz: brak źródła) oraz
- proces DSS05 – Managed Security Services COBIT® 2019 !!!

Moje wzruszenie było jednak przedwczesne, bowiem autorzy formularza **kompletnie** nie zrozumieli modelu poziomów potencjału dla procesów (ang. Capability Levels for Processes) metodyki COBIT® 2019. Ponadto przeinaczanie modelu narusza prawa autorskie ISACA. Arkusz DSS05 formularza jest **do wyrzucenia**.

Szablony

Podobny problem jest z szablonami sprawozdania z audytu zgodnego z uksc, opublikowanymi przez Ministra Cyfryzacji

(https://mc.bip.gov.pl/operatorzy-uslug-kluczowych/szablon-sprawozdania-z-audytu-zgodnego-z-ustawa-o-krajowym-systemie-cyberbezpieczenstwa.html). Jak zaznaczono na stronie BIP-u: „szablon należy interpretować jako wzór audytu oceny Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa". Szablony stały się bardzo popularne w przetargach na audyty zgodności z uksc. Oto przykłady zapisów SIWZ i umów:

- Przeprowadzenie audytu zgodnie z szablonem stanowiącym Załącznik nr 3 do RFI (Energa).
- Wykonawca zobowiązany jest przeprowadzić Audyt w zakresie określonym w Szablonie sprawozdania z Audytu, stanowiącym załącznik nr 1 do Umowy (Port Lotniczy Poznań-Ławica).
- Zakres Raportu powinien być zgodny z aktualną na czas realizowania badania wersją Szablonu sprawozdania z Audytu zgodną z ustawą o Krajowym Systemie Cyberbezpieczeństwa, zamieszczoną na stronie https://issa-polska.github.io/Audyt_KSC/ należącej do ISSA Polska Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych (Główny Inspektorat Transportu Drogowego).

Niestety, oprócz licznych błędów edycyjnych, składniowych i stylistycznych, szablony zawierają przede wszystkim **poważne błędy merytoryczne** i są niespójne. Przyjęta skala opinii audytorskiej o systemie bezpieczeństwa: pozytywna, pozytywna z zastrzeżeniami, negatywna może wprowadzać w błąd odbiorców sprawozdania z audytu i uśpić czujność zainteresowanych stron. Opinia pozytywna jest nierealna przy dzisiejszych zagrożeniach dla cyberbezpieczeństwa (który audytor odważy się wydać taką opinię, przyjmując podaną definicję?), zaś opinia pozytywna z zastrzeżeniami może zostać zinterpretowana jako prawie pozytywna i niewymagająca dalszych prac nad zapewnieniem cyberbezpieczeństwa. Autorzy ograniczyli się do norm PN-EN ISO/IEC 27001 i PN-EN ISO 22301. Na dodatek z niezrozumiałych przyczyn dokumenty tworzone na bazie szablonów są objęte licencją MIT (https://pl.wikipedia.org/wiki/Licencja_MIT).

Zgodnie ze standardem audytu ISACA 1401 SPRAWOZDAWCZOŚĆ (ang. Reporting), audytor powinien „przedyskutować z kierownictwem merytoryczną treść raportu wstępnego przed jego finalizacją i publikacją". W praktyce oznacza to, że audytor bierze pełną odpowiedzialność zawodową za każde słowo zawarte w sprawozdaniu i musi być w stanie odpowiedzieć na każde pytanie kierownictwa dotyczące jego treści. Standard audytu ISACA 1401 nie narzuca szablonu, tylko wylicza, które informacje muszą znaleźć się w sprawozdaniu z audytu.

> ***Nie wolno wymagać od certyfikowanego audytora, by korzystał z materiału, na którego opracowanie nie miał wpływu i który nie zawiera dostatecznych wyjaśnień co do jego treści.***

Pomimo zgłaszanych uwag szablony pozostają bez zmian od 28 kwietnia 2020 r. Nadszedł najwyższy czas na ich przegląd i decyzję, czy pozostają w użyciu.

Z ostatniej chwili: Centrum Projektów Polska Cyfrowa usunęło arkusz DSS05 z formularza diagnozy cyberbezpieczeństwa JST.

Na koniec ...

wracam do tematu, który poruszyłam w poprzednim artykule, czyli do nowelizacji Kodeksu pracy. Ministerstwo Rozwoju, Pracy i Technologii odniosło się do mojej uwagi zgłoszonej w ramach konsultacji publicznych:

Projekt	Art. 67^{18}. Praca może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i uzgodnionym z pracodawcą, w tym w miejscu zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (praca zdalna).
Moja opinia	Zapis powinien uwzględniać bezpieczeństwo komunikacji, czyli powinien być następujący: „z wykorzystaniem **bezpiecznych** środków bezpośredniego porozumiewania się na odległość (praca zdalna)".
Odniesienie się projektodawcy	Bezpieczeństwo ww. środków wynika z przepisów ogólnych; nie ma potrzeby takiego doprecyzowania.

https://legislacja.rcl.gov.pl/docs//2/12346911/12789144/12789148/dokument523282.docx

Czy jestem zaskoczona bagatelizowaniem kwestii bezpieczeństwa teleinformatycznego? Tak. Od 2018 r. zapisy dotyczące ochrony danych osobowych są wciskane na siłę do każdej możliwej ustawy – nie zawsze szczęśliwie, o czym pisałam w moich poprzednich artykułach. W tym przypadku uznano, że nie ma takiej potrzeby. Bo uwaga nie została zgłoszona przez UODO. Martwi mnie brak zrozumienia i świadomości, że o cyberbezpieczeństwo należy dbać na każdym kroku.

Wszystkie informacje zawarte w artykule są podane według stanu na 29 października 2021 r.

Nowelizacja ustawy o KSC

Kolejna wersja ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) realizuje wymagania zaprezentowane 16 grudnia 2020 r. przez Komisję Europejską jako nowy pakiet cyberbezpieczeństwa.

Częścią tego pakietu, poza Strategią Cyberbezpieczeństwa i Dyrektywą o odporności krytycznych podmiotów, jest propozycja Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. Uchyla ona poprzednią dyrektywę obowiązującą w tym zakresie od 2016 r. – Dyrektywę NIS (Network and Information Security) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

W Polsce 28 sierpnia 2018 r. weszła w życie ustawa z dnia 5 lipca 2018 r. o KSC, która ma szerszy zakres niż Dyrektywa NIS, ponieważ nie ogranicza się tylko do operatorów usług kluczowych, dostawców usług cyfrowych oraz siedmiu organów właściwych ds. cyberbezpieczeństwa czy Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT (Computer Security Incident Response Team), ale stanowi, że w skład systemu wchodzą również administracja publiczna, zarówno szczebla rządowego, jak i samorządowego, a także uczelnie i instytuty badawcze.

Grzegorz Cenkier
wieloletni pracownik Politechniki Warszawskiej, Instytutu Podstaw Informatyki PAN oraz instytucji finansowych i międzynarodowych systemu ONZ. Członek Zarządu ISSA Polska, Naczelnego Sądu Koleżeńskiego oraz Izby Rzeczoznawców Polskiego Towarzystwa Informatycznego. Ekspert grupy roboczej w zakresie normalizacji: ISO/TC307/AHG2–Guidance for Auditing DLT Systems, reprezentant w Komitecie Technicznym PKN 333 Blockchain i Technologii Rozproszonych Rejestrów.

NIS 2

Zrewidowana wersja Dyrektywy NIS została nazwana Dyrektywą NIS 2. Propozycja NIS 2 rozszerza zakres sektorów objętych dotychczasową dyrektywą m.in. o administrację pu-

bliczną, sektor żywności, telekomunikację, ścieki, przemysł, zarządzanie odpadami i przestrzeń kosmiczną oraz rozszerza zakres infrastruktury cyfrowej. Sektory te zostały uznane za podmioty kluczowe (*essential entities*). Lista ta została rozszerzona o podmioty ważne (*important entities*), do których zaliczono: usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcję wyrobów medycznych, produkty komputerowe, elektroniczne i optyczne, sprzęt elektryczny, maszyny i wyposażenie, pojazdy samochodowe, przyczepy i naczepy oraz produkcję i dystrybucję chemikaliów, a także przetwarzanie i dystrybucję żywności.

Podmioty objęte Dyrektywą NIS 2 będą musiały sprostać większym niż dotychczas wymaganiom w zakresie: zarządzania, obsługi i ujawniania luk w zabezpieczeniach, testowania poziomu cyberbezpieczeństwa oraz efektywnego wykorzystywania szyfrowania. Propozycja precyzuje w większym stopniu niż Dyrektywa NIS zapisy w zakresie raportowania incydentów. Nowością jest **wprowadzenie odpowiedzialności kierownictwa firmy za zarządzanie ryzykiem** w zakresie cyberbezpieczeństwa.

Zaproponowano ustanowienie Europejskiej sieci zarządzania kryzysowego w cyberprzestrzeni (*European Cyber Crises Liaison Organisation Network, EU-CyCLONe*), której zadaniem będzie koordynacja zarządzania incydentami na wielką skalę na poziomie Unii Europejskiej. NIS 2 wprowadza koordynację w zakresie ujawniania podatności (*volnerability disclosure*), a także wzmacnia rolę ENISA – Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, która po przyjęciu propozycji będzie odpowiedzialna za przygotowanie „Sprawozdania o stanie cyberbezpieczeństwa w Unii".

Jeden zespół więcej

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

W projekcie nowej ustawy o KSC zapisano, że przybędzie jeszcze jeden CSIRT INT podległy Agencji Wywiadu, który ma wspierać obsługę incydentów zgłaszanych przez jednostki podległe Ministrowi Spraw Zagranicznych (w tym placówki zagraniczne RP) oraz przez samą Agencję.

Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa, który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze. Obecnie organy właściwe, zgodnie z Dziennikiem Ustaw z 2020 r. poz. 1369 w wersji obowiązującej od 1 stycznia 2021 r. to dla:

- sektora energii – minister właściwy do spraw energii;
- sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu;
- podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej;
- sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;
- sektora ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw zdrowia;
- sektora ochrony zdrowia obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej;
- sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej;
- sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw informatyzacji;
- sektora infrastruktury cyfrowej obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej;
- dostawców usług cyfrowych z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw informatyzacji;
- dostawców usług cyfrowych obejmujących podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej.

Krajowy system cyberbezpieczeństwa składa się więc z: 9 Organów Właściwych (OW), 3 CSIRT-ów poziomu krajowego (będą 4), Pojedynczego Punktu Kontaktowego w Departamencie Cyfryzacji, Pełnomocnika Rządu ds. Cyberbezpieczeństwa, który odpowiada za koordynację polityki rządu RP w obszarze cyberbezpieczeństwa, oraz Kolegium ds. Cyberbezpieczeństwa (ciało doradcze przy Radzie Ministrów). Za koordynację obsługi incydentów w tym zdecentralizowanym systemie odpowiada CSIRT NASK, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Zgodnie z proponowaną ustawą, OW obligatoryjnie tworzą w ciągu 18 miesięcy od dnia wejścia w życie nowelizacji CSIRT-y sektorowe; do tej pory działał tylko jeden utwo-

rzony przez KNF. Nie będzie obowiązku utworzenia nowej lub przekształcenia istniejącej jednostki, ponieważ zadania w tym zakresie będzie można powierzyć jednemu z zespołów CSIRT poziomu krajowego.

Działania w zakresie cyberbezpieczeństwa będą wspierać ISAC (*Information Sharing and Analysis Center*) – centra wymiany i analiz informacji, tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, które mogą działać w formie partnerstwa publiczno-prywatnego (PPP). Ich zadaniem będzie analiza informacji o potencjalnych zagrożeniach i podatnościach oraz wymiana informacji, a także dzielenie się najlepszymi praktykami.

Propozycja ustawy wprowadza do Krajowego Systemu Cyberbezpieczeństwa pojęcie SOC (*Security Operations Center*) – operacyjnych centrów bezpieczeństwa, które będą zobowiązani posiadać operatorzy usług kluczowych. SOC realizować będą wszystkie funkcje związane z monitorowaniem i zarządzaniem bezpieczeństwem systemów informacyjnych zarówno na potrzeby wewnętrzne, jak i usług zewnętrznych, świadczonych na rzecz innych organizacji.

> *Minister właściwy do spraw informatyzacji będzie prowadził wykaz operacyjnych centrów bezpieczeństwa.*

Wprowadzono również dwa rodzaje incydentów wpływających na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne).

Do obowiązków operatorów usług kluczowych, które są określone w ustawie o KSC, należą:

- zarządzanie ryzykiem (w tym szacowanie ryzyka);
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, w tym zapewnienie bezpieczeństwa fizycznego i środowiskowego umożliwiającego utrzymanie i bezpieczną eksploatację systemu informacyjnego;
- bezpieczeństwo i ciągłość dostaw;
- wdrażanie, dokumentowanie i utrzymywanie planów działania;
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty;
- obsługa incydentów i współpraca w tym zakresie z właściwym CSIRT;
- wykorzystywania kryptografii i szyfrowania;
- wyznaczenie osoby kontaktowej na potrzeby KSC.

Aby zrealizować wymagane przepisami prawa obowiązki należy odpowiednio przygotować infrastrukturę operatora usługi kluczowej i ocenić – oszacować ryzyko, czy zapewnione jest właściwe bezpieczeństwo sytemu informacyjnego. Zgodnie z ustawą należy raz na dwa lata przeprowadzić audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

Upgrade audytu

Audyt informatyczny to proces zbierania i oceniania dowodów w celu określenia, czy system informatyczny i związane z nim zasoby właściwie chronią majątek, utrzymują integralność danych i dostarczają odpowiednich i rzetelnych informacji, osiągają efektywnie cele organizacji, oszczędnie wykorzystują zasoby i stosują mechanizmy kontroli wewnętrznej tak, aby dostarczyć rozsądnego zapewnienia, że osiągane są cele operacyjne i kontrolne oraz że chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane, a ich skutki na czas korygowane.

Audyt zgodny z ustawą KSC nakłada dodatkowe warunki. Zespół audytorski w składzie co najmniej dwuosobowym powinien posiadać odpowiednie kwalifikacje potwierdzone rozpoznawalnymi i uznanymi certyfikatami zawodowymi – pełna lista certyfikatów została opublikowana w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu 11 certyfikatów uprawniających do przeprowadzenia audytu KSC, a zawiera uprawnienia takie, jak: Certified Internal Auditor (CIA), Certified Information System Auditor (CISA), Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001, Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301, Certified in the Governance of Enterprise IT (CGEIT), Certified Information Systems Security Professional (CISSP) i wiele innych.

Ważne jest, aby audytor/rzy posiadał/li wieloletnie i szerokie doświadczenie, kompetencje i kwalifikacje techniczne dotyczące oceny architektury bezpieczeństwa oraz przeprowadzania testów technicznych – testów konfiguracji, podatności i testów penetracyjnych. Istotna jest również umiejętność poprawnej interpretacji uzyskanych wyników oraz raportowania. Chodzi o to, by poprzez zalecenia i rekomendacje dostarczyć wartość dodaną oraz wskazać rozwiązania ograniczające zidentyfikowane słabości w jednej, profesjonalnej, organizacyjno-technicznej usłudze audytowej. Zgodnie z ustawą o KSC, zespoły muszą być co najmniej dwuosobowe, jednak ze względu na zakres prac audytowych właściwsze wydają się zespoły liczące od dwóch do pięciu osób, z których przynajmniej jedna posiada kwalifikacje techniczne, pozwalające na przeprowadzanie np. testów konfiguracji czy testów penetracyjnych, oraz doświadczenie w ocenie architektury bezpieczeństwa, a pozostali audytorzy mają doświadczenie w zakresie zagadnień Governance–Risk–Compliance (Zarządzania–Ryzyka–Zgodności) i audytu cyberbezpieczeństwa w różnej wielkości organizacjach.

Audyt spełnienia wymagań ustawy KSC ma odpowiedzieć na pytanie: na jakim poziomie dojrzałości w zakresie cyberbezpieczeństwa jest moja organizacja? Czy potrzebne są działania naprawcze ? Może działania naprawcze nie są w ogóle potrzebne? Albo wręcz przeciwnie – jestem na początku drogi.

W sposób szczególny analizie podlegają systemy niezbędne do świadczenia usługi kluczowej lub cyfrowej. Jako kryteria mogą zostaną przyjęte wymagania ustawy, norm i standardów w zakresie bezpieczeństwa: ISO/IEC 27001, ISO 22301, NIST SP 800-82, NIST SP 800-53 oraz wymagania i wytyczne Rządowego Centrum Bezpieczeństwa. Wykorzystanie norm w audycie KSC przynosi największą wartość w zakresie wymogów ustawy dotyczących środków technicznych i organizacyjnych, zapewniających bezpieczeństwo systemów informatycznych wspierających realizację usługi kluczowej. Normy NIST ułatwią pracę audytorów usługi w obszarze Industrial Control Systems (ICS) – Systemów Kontroli Przemysłowej, a norma 27001 pozwala na efektywną ocenę takich obszarów, jak: kontrola dostępu, kryptografia czy ochrona przed szkodliwym oprogramowaniem. Wsparciem dla audytora w zakresie ciągłości jest norma ISO 22301.

Departament Cyberbezpieczeństwa Ministerstwa właściwego ds. Informatyzacji (do 2020 r. Ministerstwo Cyfryzacji, obecnie Kancelaria Prezesa Rady Ministrów) opublikował Szablon sprawozdania z Audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa, który został przygotowany przez osoby zrzeszone w stowarzyszeniach ISSA Polska oraz IIA Polska. Szablon (https://www.gov.pl/attachment/0aac2ab8-1b72-46ec-823b-2c9f05c95506) jest nieobowiązkowy, może być modyfikowany zarówno przez audytorów, jak i Operatorów Usług Kluczowych. Należy go interpretować jako wzór audytu oceny Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa. Pozwoli poszczególnym OW na porównywanie wyników, ponieważ ujednolica podejście do raportowania, wskazuje zakres weryfikacji, której powinien dokonać audytor, oraz minimalizuje subiektywizm badania.

Jednocześnie należy wziąć pod uwagę, że ograniczenie audytu KSC do samooceny opartej na prostych listach kontrolnych, nawet takich jak w zawarte w szablonie, a także brak komponentu oceny technicznej czy nadmierna koncentracja na problemach, nie zaś na możliwych rozwiązaniach, powodują, że audyt może nie przynieść spodziewanych korzyści dla organizacji.

Warto pamiętać, że na bazie wyników z dobrze przeprowadzonego audytu możemy:

- zdefiniować strategię cyberbezpieczeństwa,
- ograniczać ryzyka i planować działania doskonalące w ramach poprawy wdrożonych zabezpieczeń organizacyjnych i technicznych.

Zgodnie z szablonem należy zbadać 10 obszarów związanych z systemem/ami obsługującymi usługę kluczową:

1. Organizacja zarządzania bezpieczeństwem informacji.
2. Procesy zarządzania bezpieczeństwem informacji.
3. Zarządzanie ryzykiem.
4. Monitorowanie i reagowanie na incydenty bezpieczeństwa.
5. Zarządzanie zmianą.
6. Zarządzanie ciągłością działania.
7. Utrzymanie systemów informacyjnych.
8. Utrzymanie i rozwój systemów informacyjnych.
9. Bezpieczeństwo fizyczne.
10. Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług.

Ponadto operator usługi kluczowej powinien utworzyć Dokumentację Systemu Informacyjnego wspierającego Usługę Kluczową, w jej skład powinny wchodzić dokumenty:

1. Raporty z audytów systemów informacyjnych wspierających Usługę Kluczową.
2. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka Systemów Informacyjnych Usługi Kluczowej.
3. Dokumentacja architektury zastosowanych zabezpieczeń.
4. Dokumentacja architektury sieci.
5. Baza danych konfiguracji urządzeń aktywnych.
6. Dokumentacja zmian w systemach informacyjnych.
7. Dokumentacja dotycząca monitorowania w trybie ciągłym.
8. Umowy z dostawcami (wsparcie techniczne) itp.
9. Umowy z dostawcami usług z zakresu cyberbezpieczeństwa.
10. Wyniki audytów u dostawców usług cyberbezpieczeństwa.
11. Dokumentacja zabezpieczeń fizycznych i środowiskowych.

Tak więc zakres audytu zgodnego z KSC jest ogromny, a wymagania – wysokie. Mniejsze organizacje na niskim poziomie dojrzałości mogą im nie sprostać.

W Polsce duży atak cybernetyczny miał miejsce 27 czerwca 2017 r., kiedy to wirus NotPetya w ciągu kilku godzin od ujawnienia się dotarł z Ukrainy do wielu punktów na świecie, w tym do jednej z polskich spółek giełdowych, która musiała zatrzymać swoje działanie. Początkowo wirus uważany był za ransomware, ale okazało się, że to Wiper (wycieraczka), czyli mimo zapłacenia okupu dane i systemy nie zostaną odzyskane, bo exploit je wymazuje. Odzyskanie danych z systemów zapasowych zajęło spółce kilka dni, przynosząc ogromne straty. W wyniku tego ataku ucierpiały światowe koncerny: Merck, FedEx, Saint-Gobain i wiele innych, w tym rosyjska spółka naftowa Rosnieft. Straty oszacowano na wieleset tysięcy dolarów.

Zmiany w obsłudze incydentów

Zmiany w organizacji struktur w proponowanej nowelizacji ustawy KSC zmieniają zasady obsługi incydentów. Operatorzy Usługi Kluczowej będą mieli obowiązek przesłać informacje o incydentach poważnych do CSIRT sektorowego, który będzie miał ustawowe 8 godzin na przekazanie ich dalej – do CSIRT poziomu krajowego (obecnie incydenty zgłaszane są równolegle). Przekroczenie terminów może spowodować karę finansową nakładaną na kierownika CSIRT sektorowego. Obowiązkiem Operatora Usługi Kluczowej jest usunięcie wskazanej podatności oraz poinformowanie organu właściwego o jej usunięciu.

Inna ważna zmiana to Certyfikat Aktu o Cyberbezpieczeństwie, który przewiduje trzy poziomy zaufania: podstawowy, istotny i wysoki, określające poziom cyberbezpieczeństwa, jaki gwarantuje dany produkt. Certyfikaty wydawane w ramach tego systemu będą precyzyjne wskazywać, jakiego poziomu dotyczą. Opis wymagań bezpieczeństwa i proces badania produktów zostanie określony w europejskich i krajowych programach certyfikacji.

Ustawodawca przewiduje również powołanie operatora strategicznej sieci bezpieczeństwa, którego wyznaczy Prezes Rady Ministrów. Celem działania tego nowego operatora będzie świadczenie usług na rzecz podmiotów publicznych, sił zbrojnych, straży pożarnej i instytucji kontroli państwa. Prezes Rady Ministrów wyznaczy operatora w terminie 30 dni od wejścia w życie nowelizacji ustawy KSC. Powołanie takiego operatora świadczy o rosnącym znaczeniu cyberbezpieczeństwa w życiu społecznym.

Stanowisko PTI w sprawie projektu ustawy o zmianie ustawy o Krajowym Systemie Cyberbezpieczeństwa publikujemy na następnej stronie.

Historia ataków cybernetycznych nie jest długa. Pierwszy poważny globalny atak miał miejsce 2 listopada 1988 r. Spowodowany został przez Morris Worm – kod liczący 3 tys. linijek kodu, który został wprowadzony do Internetu przez Roberta Morrisa. Wirus ten zainfekował ponad 6 tys. komputerów (ok. 10% całego ówczesnego Internetu), a jego usunięcie zajęło ponad 8 dni ze względu na to, że duża część serwerów została odłączona od sieci. Dopiero 10 listopada udało się przywrócić jej normalne funkcjonowanie – łączne straty szacowano na kilkadziesiąt mln dolarów.

W raporcie ENISA – opublikowanym w październiku 2021 r., a obejmującym okres od kwietnia 2020 r. – do połowy lipca 2021 r. podano 9 najczęściej występujących zagrożeń cybernetycznych. Wśród nich pierwsze miejsca zajmują: ransomware (blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych), malware (złośliwe oprogramowanie) i cryptojacking (program wykorzystujący moc zainfekowanego komputera do „wykopywania" kryptowaluty). Jeden z największych cyberataków ransomware w 2021 r. na infrastrukturę miał miejsce 7 maja, gdy został zainfekowany skomputeryzowany sprzęt zarządzający rurociągiem Colonial Pipeline, amerykańskiego systemu rurociągów naftowych, który transportuje benzynę i paliwo lotnicze z Houston w Teksasie głównie do południowo-wschodnich Stanów Zjednoczonych. Aby zablokować atak, Colonial Pipeline Company wstrzymała wszystkie operacje rurociągu i przy pośrednictwie FBI zapłaciła żądany okup (75 bitcoinów, wtedy około 4 mln dolarów) w krótkim czasie po ataku.

Okazało się jednak, że oprogramowanie dostarczone przez hakerów, które miało przywrócić prawidłowe funkcjonowanie rurociągu działa niezwykle wolno, co zmusiło właściciela rurociągu do odtworzenia systemów z backupów. Eksploatacja rurociągu, została wznowiona dopiero 12 maja o godzinie 17, kończąc sześciodniowe zamknięcie, jednak powrót do pełnej wydajności systemu nastąpił dopiero 15 maja. Koszt tego ataku to częściowe zamknięcie lotnisk Charlotte Douglas i Hartsfield-Jackson w Atlancie, wzrost cen paliw od 9 do 16 centów w Karolinie, Tennessee, Wirginii i Georgii oraz brak benzyny na 10 600 stacji benzynowych.

Fot. Beata Sołtys

Wiesław Paluszyński
prezes PTI

Jako stowarzyszenie z 40-letnim doświadczeniem, skupiające informatyków działających we wszystkich dziedzinach informatyki, w tym również tych związanych z zapewnieniem cyberbezpieczeństwa, Polskie Towarzystwo Informatyczne czuło się szczególnie zobowiązane do zajęcia stanowiska w sprawie projektu ustawy o zmianie ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Ponad dwa lata funkcjonowania Krajowego Systemu Cyberbezpieczeństwa w Polsce wskazały, naszym zdaniem, na ewidentną potrzebę dokonania zmian na poziomie ustawowym.

Zmiany te dotyczą głównie Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, która z jednej strony zdefiniowała podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym, a z drugiej była odpowiedzią na potrzebę implementacji dyrektywy NIS, którą często określano jako pierwsze europejskie prawo w zakresie cyberbezpieczeństwa.

Naszą intencją było, aby opracowane przez PTI uwagi do nowej wersji projektu ustawy z dnia 12.10.2021 r. miały przede wszystkim charakter konstruktywny i możliwy do zaimplementowania pomimo złożoności przedmiotu opiniowania i nieadekwatnie krótkich terminów konsultacji.

Proponujemy m.in., aby w warstwie pojęciowej dokonać przeglądu użytych definicji i skrótów w celu ich doprecyzowania i weryfikacji pod kątem spójności zarówno w ramach samej Ustawy o KSC, jak w relacji z innymi obowiązującymi aktami prawnymi. Dotyczy to m.in. definicji usługi ICT.

W projekcie pojawiają się też niezdefiniowane pojęcia, których potencjalna swoboda interpretacyjna może znacząco wpłynąć na jakość zapewnienia bezpieczeństwa teleinformatycznego. Mamy tu m.in. pojęcie „dynamiczna analiza ryzyka", które jak dotąd nie zostało zdefiniowane w znanych źródłach. Również wprowadzenie z pozoru oczywistego pojęcia, jakim są „kontrole techniczne", wymaga zdefiniowania.

Proponujemy również, aby zamienić pojęcie „krajowy system certyfikacji cyberbezpieczeństwa" na „krajową organizację certyfikacji cyberbezpieczeństwa" z uwagi na zapisy rozporządzenia EU 2019/88. Pod rozwagę poddajemy również trafność użytych w projekcie definicji „certyfikatu", jak i „deklaracji zgodności". Jeśli ma być wydawany certyfikat spełniający wymagania rozporządzenia UE 2019/881, to będzie to certyfikat europejski i europejska deklaracja zgodności.

Ustawodawca konsekwentnie proponuje utworzenie systemu takiego, jak europejski – określony w rozporządzeniu UE 2019/881 – ale ma to być system krajowy. Tyle tylko, że wielokrotnie przywoływane powyżej rozporządzenie w art. 57 pkt 2. wprost zabrania takiej konstrukcji. Dlatego też cała koncepcja krajowego systemu certyfikacji cyberbezpieczeństwa wymaga przepracowania z uwagi na ewidentne sprzeczności z przywoływanym w projekcie rozporządzeniem EU 2019/881.

Należy rozważyć także – z uwagi na złożoność zadań, wymogi bezpieczeństwa i efektywność realizowanych procesów – dopuszczenie możliwości wskazania, aby ISAC mógł również funkcjonować w formule partnerstwa publiczno-prywatnego.

W projekcie zabrakło też wskazań dotyczących wymogów w zakresie kwalifikacji, wiedzy i umiejętności zarówno personelu podmiotów świadczących usługi z zakresu cyberbezpieczeństwa (zwłaszcza SOC i CSIRT-ów sektorowych), jak i personelu wewnętrznych struktur organizacji mających wpływ na bezpieczeństwo teleinformatyczne.

Warto trzymać rękę na pulsie

Patentowanie w 5G jest jednym z najbardziej gorących tematów, ponieważ rynek licencyjny, obejmując wiele nowych sektorów gospodarki, wzrośnie do ogromnych rozmiarów. Styk technologii i prawa w obszarze sieci 5 generacji będzie szczególnie gorący dla rodzimych firm, bo nie mamy w Polsce praktyki sporów patentowych, a sędziowie nie są przygotowani do oceny wysokości opłat licencyjnych.

To główne wnioski z październikowego webinarium SIECI 5G – STANDARDY I PATENTOWANIE A CYBERBEZPIECZEŃSTWO. – *W obszarze sieci 5G Polska jest aktywnym graczem, dlatego kwestie standaryzacji i patentowania są kluczowe dla tych z polskich firm, które swoją przyszłość wiążą z tą technologią. Elementem 5G jest oprogramowanie i to jest szansa dla polskich firm programistycznych nie tylko w obszarze core'owym, ale także zarządzania informacją, która będzie wykorzystywana do Internetu Rzeczy* – rozpoczął webinarium Wiesław Paluszyński, prezes PTI i współorganizator spotkania.

Rozwój technologii generuje coraz więcej patentów

Wraz z kolejnymi standardami 2, 3, 4 i 5G rośnie złożoność technologii, a więc rośnie również liczba patentów. Co więcej, te patenty muszą mieć na uwadze już nie tylko producenci telefonów czy tabletów, lecz także firmy działające na nowych rynkach: motoryzacyjnym, inteligentnych domów, smart energy, służby zdrowia czy Internetu Rzeczy.

Swoimi przemyśleniami na temat 5G z punktu widzenia prawa własności intelektualnej i prawa patentowego podzielił się z uczestnikami webinarium prof. Rafał Sikorski. – *Spory dotyczące standardów w jurysdykcjach krajów bardziej rozwiniętych patentowo są częste. W Niemczech spory pomiędzy dysponentami patentów: Ericssonem, Nokią a głównymi producentami motoryzacyjnymi są najgłośniejsze. Nokia poprzez jedno postępowanie sądowe potrafi zatrzymać połowę produkcji Mercedesa z uwagi na jakiś patent 4G, wykorzystywany dzisiaj w każdym samochodzie. Niemcy szybko zrozumieli, że w sporach patentowych potrzeba dużo większej elastyczności. W Polsce takie spory się nie toczą, ale ich przedsmak mieliśmy przy implementacji telewizji cyfrowej* – mówił.

Ze sporym wzrostem liczby licencjodawców mieliśmy do czynienia w latach 80. i 90. XX w. podczas rozwoju elektroniki konsumpcyjnej: CD czy DVD. Wielość podmiotów i patentów znacząco wpływa na wzrost kosztów transakcyjnych i zagrożenie tzw. royalty stacking – czyli nakładaniem się licznych opłat licencyjnych pochodzących od różnych podmiotów. To może być wyzwanie dla start-upów, małych, a nawet średnich przedsiębiorstw. – *W omawianym okresie poradziliśmy sobie z tymi zjawiskami za pomocą tzw. patent pools, czyli pakietów licencyjnych polegających na tym, że w wyznaczonym obszarze jeden podmiot reprezentował licencjodawców. Przykładowo w USA licencjodawców dla branży motoryzacyjnej reprezentuje Avanci. Jednak z czasem koszty zarządzania patent pools zaczęły być balastem dla gospodarki patentowej* – mówił prof. Sikorski.

O patent pools rozmawia też Komisja Europejska. Licencjobiorcy próbują się łączyć, żeby wzmocnić swoją pozycję, co generuje wiele problemów związanych z prawem konkurencji. Licencje muszą być dostępne dla wszystkich podmiotów, dlatego wszystkie organizacje standaryzacyjne na

Webinarium SIECI 5G – STANDARDY I PATENTOWANIE A CYBERBEZPIECZEŃSTWO było kolejnym z cyklu spotkań „Prezesi zapraszają", współorganizowanych przez Polskie Towarzystwo Informatyczne i Związek Cyfrowa Polska. W dyskusji udział wzięli:

prof. dr hab. Rafał Sikorski
– Senior Partner,
kieruje departamentem własności intelektualnej w kancelarii SMM Legal, wykładowca w Zakładzie Prawa Europejskiego na Uniwersytecie im. Adama Mickiewicza w Poznaniu

dr inż. Elżbieta Andrukiewicz
z Instytutu Łączności – Państwowego Instytutu Badawczego, kieruje ważnymi projektami w obszarze standaryzacji i certyfikacją sieci 5G.

Michał Szczęsny
przedstawiciel firmy Exatel

dr inż. Sławomir Pietrzyk
prezes IS-Wireless

dr inż. Jacek Falkiewicz
przedstawiciel firmy Ericsson

Łukasz Bromirski
ekspert i popularyzator wiedzy z zakresu cyberbezpieczeństwa, reprezentuje firmę Cisco

Wiesław Paluszyński
prezes PTI

Dyskusję poprowadził **Jarosław Mojsiejuk** – prawnik, manager w Hewlett Packard Enterprise Polska, reprezentujący także Związek Polska Cyfrowa.

Nagranie webinarium dostępne jest pod adresem: https://www.youtube.com/watch?v=k-hee0lmlFU

świecie od lat 20. XX w. optują za licencjami udzielanymi na warunkach FRAND (*Fair, Reasonable and Non-Discriminatory*).

Umowy licencyjne FRAND

W tej szczególnej kategorii umów licencyjnych ważne są kwestie interpretacji nieostrych wymogów – tu szczególne znaczenie ma wkład doktryny prawnej zarówno krajowej, jak i anglojęzycznej. Orzecznictwo pełni w tym zakresie wyjątkową rolę, ponieważ wytyczne organów unijnych oraz wskazówki interpretacyjne pochodzące z literatury są wyjaśniane czy dookreślane w publikowanych wyrokach sądów i trybunałów. Złożoność licencjonowania na zasadach FRAND potęguje jej globalny charakter, brak jednorodnych systemów przetwarzania oraz weryfikacji danych, a także niedostateczne zaplecze techniczne o międzynarodowym charakterze, niezbędne do wzmocnienia pewności takich licencji.

– Oceną licencji FRAND z punktu widzenia globalnego najwcześniej zajęły się sądy brytyjskie i sądy niemieckie; amerykańskie też są gotowe to robić. Coraz aktywniej działają też sądy chińskie, które też chcą globalnie rozstrzygać w takich sprawach. Musimy sobie zdawać sprawę, że perspektywa polska w tych sądach nie istnieje – ostrzegał prof. Sikorski.

Realna groźba dla polskich przedsiębiorstw

Polskie firmy zamierzające wykorzystywać elementy rozwiązań 5G muszą mieć świadomość, że ewentualne spory będą z reguły załatwiane globalnie. Będziemy jedynie wykonawcą ugód czy decyzji podejmowanych gdzie indziej. Dysponenci patentów mają pozycję monopolistyczną, do tego dochodzi niepewność, jak te opłaty liczyć. Nie do końca wiadomo, czy każdy z patentów ma istotny wpływ na standard 5G, z pewnością część jest nadmiarowa, generowana na potrzeby negocjacyjne. Pytań jest więcej – na jakim poziomie powinno dojść do licencjonowania: produktu końcowego czy komponentu.

Te globalne spory patentowe z pewnością dotkną polskie firmy. *– W związku z rosnącą liczbą patentów, związane z nimi opłaty będą rosnąć, więc czeka nas walka na rynku małych i średnich przedsiębiorstw, które będą chciały być innowacyjne. Będzie coraz trudniej zbudować jakikolwiek produkt nie wpadając w pułapkę np. wstrzymania produkcji z powodu*

fragmentu rozwiązania objętego patentem. Dla małych firm to oznacza śmierć – ostrzegał Łukasz Bromirski z firmy Cisco.

Patentowe pole minowe

Dr inż. Elżbieta Andrukiewicz zwróciła uwagę na specyfikę polityki patentowej, wrażliwej na kontekst biznesowo-polityczny. – *Rosyjskie organizacje standaryzacyjne nie angażują się specjalnie w prace normalizacyjne, mimo że są założycielami ISO. Ale w obszarze algorytmów czy mechanizmów kryptograficznych są aktywne, dlatego że kraje byłego Związku Radzieckiego bardzo chętnie korzystają z rozwiązań technicznych dostarczanych przez Federację Rosyjską z jednym zastrzeżeniem – te rozwiązania muszą być w standardach międzynarodowych. W związku z tym wiele algorytmów czy mechanizmów kryptograficznych mających cechy własności intelektualnej jest zgłaszanych do ISO. Rozwój standardu jest rozciągnięty w czasie, więc zdarza się, że podmiot wypełniający formularz po kilku latach już nie istnieje. Kilka standardów nie mogło być opublikowanych właśnie dlatego, że właściciel patentu się nie odzywał.*

Prace związane z europejskim schematem certyfikacji cyberbezpieczeństwa w obszarze 5G toczą się m.in. z wykorzystaniem specyfikacji 3GPP. 3GPP (3rd Generation Partnership Project) to międzynarodowa organizacja normalizacyjna mająca na celu rozwój systemów telefonii komórkowej, która powstała w 1998 r. jako wspólny projekt siedmiu regionalnych organizacji standaryzacyjnych w celu opracowania norm dla systemów telefonii komórkowej trzeciej generacji. Wszystkie organizacje wchodzące w skład 3GPP mają własną politykę patentową.

Inne zasady patentowania niż pozostałe europejskie organizacje standaryzacyjne ma także ETSI (Europejski Instytut Norm Telekomunikacyjnych) – niezależny instytut standaryzacyjny, którego podstawowym zadaniem jest opracowywanie norm niezbędnych do stworzenia europejskiego rynku telekomunikacyjnego.

Bardzo trudno trzymać rękę na pulsie wszystkich prac patentowych i standaryzacyjnych, dlatego w obszarze 5G trzeba oczekiwać wielu niespodzianek, wynikających z wykorzystania własności intelektualnej i prawa patentowego. – *Standardy są dobrym kierunkiem, ale diabeł tkwi w szczegółach* – ostrzegała Elżbieta Andrukiewicz.

Instytut Łączności prowadzi (razem z firmą IS-Wireless i Politechniką Warszawską) prace badawczo-rozwojowe nad koncepcją Open RAN, bo w Open RAN – na zasadach niedyskryminowania i odpowiednich porozumień i kompatybilności technicznej na różnych warstwach sieci – będą ze sobą współpracowały różne komponenty od różnych dostawców. – *Nie ma jeszcze takiej polityki ewaluacji, która by nam podpowiedziała, jak oceniać pod względem bezpieczeństwa tak skomplikowane środowiska* – mówiła Elżbieta Andrukiewicz.

– *5G jest standardem innym od dotychczasowych, nie wszyscy to dostrzegają. Część sieciowa jest de facto zaszyta w oprogramowaniu i od niedawna wiemy, że może ono pochodzić od różnych dostawców. Dezagregacja łańcucha wartości jest czymś nowym w branży telekomunikacyjnej. 3GPP umożliwiło, że telefon może być produkowany przez jednego dostawcę, część radiowa przez innego – bo opracowaliśmy interfejsy i funkcjonalności – a część core'owa jeszcze przez innego. Obniżyło to próg wejścia dla wielu graczy, a zyskał klient. Jednocześnie 3GPP jest narzędziem walki konkurencyjnej i to jest problem. Technika wyprzedza mentalność monopolisty, która to mentalność blokuje rozwój branży* – mówił dr inż. Sławomir Pietrzyk, prezes IS-Wireless (rozmowę ze Sławomirem Pietrzykiem opublikowaliśmy w Biuletynie PTI nr 2–4/2020).

Dr inż. Jacek Falkiewicz z firmy Ericsson zwrócił uwagę, że w przemyśle 4.0 nie tylko ludzie będą dokonywać autoryzacji, lecz także urządzenia, więc elastyczność rozwiązań cybersecurity musi być większa. Kolejne wyzwania to zwiększenie ochrony prywatności abonentów i zwiększenie integralności danych. – *Cyberbezpieczeństwo zaczyna się od standardów, a kończy na zarządzaniu siecią. Potrzebne jest holistyczne podejście do tego zagadnienia. Musimy pamiętać zarówno o standardach, jak i o procesach projektowania, produkcji i eksploatacji urządzeń sieciowych. Operator powinien mieć zaufanie do wyprodukowanego sprzętu i oprogramowania* – mówił.

Wiedza u źródła

Polskie firmy są biorcami technologii, więc powinniśmy starać się, żeby opłaty licencyjne były na rozsądnym poziomie. Musimy walczyć o ocenę proporcjonalności, żeby patent obejmujący znikomą część produktu finalnego nie mógł być podstawą do blokowania całego produktu.

Jak to robić? Decydują większości eksperckie, a przejście na zdalne spotkania sprawiło, że pojawiło się więcej ekspertów z krajów, które do tej pory ze względów finansowych nie były w stanie uczestniczyć w spotkaniach fizycznych. – *Warto mieć na uwadze, że są kraje, które przewagę ekonomiczną uzyskują poprzez działania standaryzacyjne* – podkreśliła Elżbieta Andrukiewicz.

– *PTI wspólnie z Instytutem Łączności występowało do premiera, żeby zapewnić polskim ekspertom środki na udział w ważnym ciele standaryzacyjnym: ETSI. Jest nadzieja, że w NASK-u powstanie rozwiązanie systemowe, ustanawiające polskich ekspertów w najbardziej newralgicznych projektach standaryzacyjnych. W I kw. 2022 r. w porozumieniu z Polskim Komitetem Standaryzacyjnym i Urzędem Patentowym organizujemy konferencję, bo powraca pomysł patentowania oprogramowania. Nie możemy zapominać, że własność intelektualna przekłada się na konkretne korzyści materialne* – podsumował webinarium Wiesław Paluszyński.

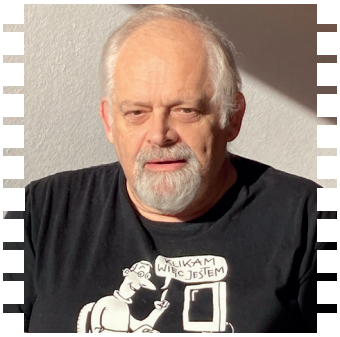
Anna Kniaź

Wysyłamy Wam mejl

Proponując polską formę nazwy poczty i listu elektronicznego – mejl, liczymy na Wasze zaangażowanie w jej rozpowszechnienie we własnych tekstach oraz wśród rodziny, przyjaciół, znajomych, współpracowników i korespondentów. Podobny apel kierujemy do redaktorów tekstów blogów, artykułów, książek itp.

prof. dr hab. Andrzej Jacek Blikle

prof. dr hab. inż. Wojciech Cellary



dr inż. Wacław Iszkowski

W 2002 r. (19 lat temu) Rada Języka Polskiego (RJP) uchwałą zdecydowała: *Poprawna forma nazwy listu elektronicznego to e-mail, potocznie mejl.*[1] Wkrótce decyzja ta była kontestowana. W tym samym roku sekretarz RJP stwierdziła: *Sądzę, że nazwa listu elektronicznego „przeżywa" teraz okres przejściowy – obecna jest ciągle jej anglojęzyczna forma (e-mail), lecz jednocześnie coraz częściej pojawia się wersja spolszczona (mejl). Która z nich zwycięży – pokaże czas. Jednak obie są poprawne*[2].

W 2006 r., w odpowiedzi na list do Poradni Językowej w PWN, prof. Mirosław Bańko stwierdził: *Mejl jest spolszczoną formą maila, na razie jeszcze potoczną. Zachęcam do używania jej w korespondencji i w ogóle w różnego rodzaju tekstach z wyjątkiem najbardziej oficjalnych. Kiedy się bardziej upowszechni, szerzej zagości w słownikach. Już teraz można ją znaleźć np. w Wielkim słowniku ortograficznym PWN.* Prof. Jan Miodek potwierdzał termin *mail*, ale w mówieniu używał [mejl]. W książce „Wszystko zależy od przyimka" prof. Andrzej Markowski stwierdził, że mówi [mail], a prof. Jerzy Bralczyk opowiedział się za formą *mejl*.

Informatycy, będąc aktywnymi uczestnikami rozwoju informatyki, w ślad za kształtowaniem się terminologii angielskiej, tworzyli – często wspólnie z polonistami – terminologię polską i dzięki temu pojawiły się takie terminy, jak: komputer, informatyka, magistrala, szyna, asembler, debuger, debugować, kompilator, konsolidacja, implementacja, interfejs, mysz, konsolidacja, folder, katalog, plik, pamięć wirtualna, pamięć kieszeniowa, przepytywanie, instancja, krotka, klikać, zakleszczenie, kapsułkowany, serwer, ruter, systemy wbudowane, systemy teleinformatyczne, teleinformatyka, przetwarzanie w chmurze itp.

Uważamy, że wzorem naszych starszych kolegów z mechaniki czy chemii, w informatyce należy się również posługiwać językiem polskim. Początkowo pojęcie poczta elektroniczna (będąca usługą przesyłania listów elektronicznych) próbowano nazywać el-poczta czy listel. Te formy jednak się nie przyjęły. Brak jednoznacznego polskiego terminu spowodował rozpowszechnienie formy angielskiej *e-mail*, *email* lub *mail* oraz spolszczonej *mejl*.

Argumenty dotyczące zapisu mejl

Forma *mejl* dobrze wpisuje się w fonetyczną strukturę języka polskiego, nie sprawiając kłopotu w jej wymowie, w przeciwieństwie do formy *e-mail*, różnie wymawianej [poprawnie i-mail, ale też często e-mail, emajl czy też emajlem, emalią, …], która nie tyle jest anglicyzmem, co słowem angielskim, którego używanie jest pretensjonalne.

Forma *mejl* jest anglicyzmem, ale umożliwia prostą deklinację oraz możliwość jej używania jako czasownika, przymiotnika, przysłówka z odpowiednimi odmianami. Pozwala również tworzyć literackie opisy związane z wysyłaniem czy odbieraniem mejli – (...) w powodzi mejli szukałem tego zamejlowanego tylko do mnie (...). Dla postaci *e-mail* i *mail* takie odmiany są sztuczne i odmieniane w postaci obcej im językowo – nie powinny podlegać polskiej odmianie.

Szczególny problem powstaje z rozróżnieniem, czy termin ten dotyczy techniki przekazania wiadomości czy też samej wiadomości: zamierzałem wysłać mu e-mail, ale podany przez niego adres e-mail jest chyba błędny. To samo stwierdzenie w postaci: zamierzałem wysłać mu mejl, ale jego adres mejlowy jest chyba błędny, lub: zamierzałem do niego zamejlować, ale jego adres mejlowy jest chyba błędny, jest bardziej zrozumiałe.

Formy alternatywne

Proponując poprawną formę *mejl*, dopuszczamy też używanie formy *email*, ale nie *e-mail*. Dlaczego?

W zapisie w języku angielskim, według słowników brytyjskich i amerykańskich, obecnie preferowany jest zapis *email*, a jedynie dopuszczalny *e-mail*. Taka jest też rekomendacja IETF RFC 524 oraz firmy Microsoft.

W słownikach brytyjskich i amerykańskich odnajdujemy:

- **Miriam Webster** [3] – email (variant e-mail) – message sent and received electronically through email system (since 1979); mail – letters and packages carried in a postal system, (since XIII c. and 1827);
- **UK Oxford Dictionary** – email (also e-mail) – the system of sending messages by electronic means. (since 1970s, abbreviation of electronic mail); mail – postal system (historical);
- **Collins** – e-mail (synonim email) – system for sending messages from one computer to computer;
- **Cambridge Dictionary**[4] (tłumaczenie na polski) – e-mail – poczta elektroniczna, email – jako system e-mail – email, wiadomość, mejl *(wysyłać email lub mejla)*; mail – poczta.

Do tej formy dopasowują się również automatyczni tłumacze, zachowując formy z łącznikiem lub bez według źródłowego tekstu. W języku niemieckim pojawia się też *Email* lub *E-mail*, co jest cechą niemieckich rzeczowników.

Przedrostek *e* – jest kłopotliwy przy dzieleniu wyrazów na kolejne wiersze, w składzie tekstów.

Przypominamy jeszcze o kłopotliwej wymowie – poprawnie (i mail), ale w praktyce częściej słyszymy (e majl).

Jesteśmy również za usunięciem formy *mail*, czasem też używanej, gdyż:

- Forma *mail* nie była dopuszczona w decyzji RJP z 2002 r.
- Poprawne tłumaczenie terminu *mail* to: *poczta, list, przesyłka, system pocztowy*, a dopiero z przymiotnikiem electronic mail staje się pol. terminem: *pocztą elektroniczną* oraz *listem elektronicznym* (jeszcze często używanymi), a po ang. *electronic mail* – w skrócie e-mail lub poprawniej email.
- Słowniki brytyjskie i amerykańskie (patrz wyżej) wyraźnie stwierdzają, że w Wlk.Brytanii *mail* oznacza pocztę królewską (Royal Mail), a w jęz. ang. *mail* jest listem, paczką itp. przesyłanymi pocztą (już od 1827 r.).
- Pojęcie *mail* niepotrzebnie jako słowo angielskie konkurowałoby z poprawnym w języku polskim zapisem *mejl*.

Warto aktywnie poprzeć nasz apel

Wszyscy popierający tę propozycję mogą wyrazić to osobiście, przesyłając na adres mejlowy:

popieram-mejl@pti.org.pl

swoje imię i nazwisko wraz ze zgodą na jego publikację. Lista poparcia zostanie wydrukowana w następnym Biuletynie PTI. Możemy mieć istotny wpływ na powszechne przyjęcie formy ***mejl***. Nie zwlekaj – napisz ten mejl poparcia i namów do tego swoją rodzinę, znajomych… Odpowiemy również na Wasze polemiki związane z tą propozycją.

Gramatyka słowa mejl i jego pochodnych

- rzeczownik mejl – odmiana: [5]

Przypadek	l.p.	l.m.	Przykłady
mianownik	mejl	mejle	*To jest ten mejl i tamte mejle*
dopełniacz	mejla	mejli, mejlów	*Nie mogę znaleźć tego mejla i tamtych mejli (lub tamtych mejlów)*
celownik	mejlowi	mejlom	*Zaufałem temu mejlowi*
biernik	mejl	mejle	*Wysłałem ci mejl, a im mejle*
nadrzędnik	mejlem	mejlami	*Tę informację wyślę ci mejlem lub mejlami*
miejscownik	mejlu	mejlach	*W tym mejlu, ani w tamtych mejlach, nie ma tej informacji*
wołacz	mejlu	mejle	*Mejlu, gdzie cię szukać*

- czasownik z odmianą przez czasy, osoby, rodzaje łącznie z trybem rozkazującym i warunkowym oraz jako bezokolicznik i imiesłów przysłówkowy – np.: mejlujesz, mejlowałem, będzie mejlowała, mejlujcie, mejlowałby, mejlowano by, mejlować, mejlując
- przymiotnik – np. mejlowany, mejlowy, mejlujący
- przysłówek – np. mejlowo
- rzeczownik – np. mejlowość

1 Uchwała ortograficzna nr 7 Rady Języka Polskiego w sprawie zapisu nazwy listu elektronicznego (przyjęta na XII posiedzeniu plenarnym dn. 21 maja 2002 r.) https://rjp.pan.pl/index.php?option=com_content&view=article&id=79:zapis-nazwy-listu-elektronicznego&catid=43&Itemid=59

2 Słownik Języka Polskiego https://sjp.pwn.pl/poradnia/haslo/mejl;6918.html

3 https://www.merriam-webster.com/dictionary/email

4 https://dictionary.cambridge.org/dictionary/english-polish/email?q=e-mail

4 Słownik gramatyczny języka polskiego http://sgjp.pl/leksemy/#69307/mejl

Roboty nie tylko spawają

Bez automatyzacji procesów przemysłowych trudno już wyobrazić sobie nowoczesny przemysł. Niemal 30 lat temu zaczęła się automatyzacja obsługiwanych informatycznie procesów biznesowych w firmach i instytucjach. Przed dwoma laty pojawił się termin „hiperautomatyzacja" określający koncepcję dalszego rozwoju robotyzacji procesów.

Słowo „robot" zostało stworzone przez Josefa Čapka, czeskiego malarza, poetę i autora książek dla dzieci, ale na całym świecie przyjęło się dzięki jego dużo bardziej znanemu bratu, pisarzowi i dramaturgowi Karelowi Čapkowi, który wykorzystał je w 1920 r. w swojej sztuce „R.U.R.", znanej też pod tytułem „Roboty Uniwersalne Rossuma". Przez lata roboty występowały jednak tylko w literaturze science-fiction. W 1942 r. Isaac Asimov w opowiadaniu „Zabawa w berka" sformułował trzy prawa robotów, które w dalekiej przyszłości miały regulować współpracę myślących maszyn z ludźmi.

Narodziny robotów przemysłowych

Już w starożytności pojawiały się urządzenia zwane automatonami, a we wczesnym średniowieczu zaawansowane automaty mechaniczne konstruowali arabscy uczeni i wynalazcy. Plany humanoidalnego urządzenia zamieścił w swoich dziełach Leonardo da Vinci, zaś w XVIII w. europejscy zegarmistrzowie konstruowali skomplikowane automaty-zabawki dla królów i arystokratów. Nowożytna historia robotów także zaczęła się od zabawki. W 1938 r. w marcowym wydaniu „Meccano Magazine", czasopisma dla młodych majsterkowiczów korzystających z metalowych elementów „małego mechanika" firmy Meccano, ukazał się artykuł opisujący automat-dźwig, skonstruowany przy użyciu firmowego zestawu przez studenta, Griffitha 'Billa' Taylora. Na towarzyszącej artykułowi ilustracji widoczny jest dźwig nazwany przez Taylora „robot Gargantua", napędzany silniczkiem elektrycznym zasilanym z 4 bateryjek i sterowany programem zapisanym na taśmie papierowej zbliżonej do stosowanej w pianolach. Jest też informacja, że samodzielne zbudowanie widocznego na ilustracji stosu klocków zajęło robotowi 50 minut[1].

Andrzej Sobczak
dr hab., profesor i kierownik Zakładu Zarządzania Informatyką w Szkole Głównej Handlowej w Warszawie. Założyciel inicjatywy Liderzy.AI – polskiej społeczności hiperautomatyzacji, twórca serwisu Robonomika.pl. W swojej działalności naukowej, dydaktycznej i doradczej zajmuje się m.in. zarządzaniem strategicznym IT, ładem danych i architekturą korporacyjną oraz zaawansowaną automatyzacją i robotyzacją procesów biznesowych.

Tomasz Kulisiewicz
sekretarz Sektorowej Rady ds. Kompetencji – Informatyka

[1] http://cyberneticzoo.com/robots/1937-the-robot-gargantu-bill-griffith-p-taylor-australiancanadian/

Na prawdziwe roboty przemysłowe wspomagające lub zastępujące człowieka w pracach żmudnych i niebezpiecznych trzeba było jednak poczekać jeszcze niemal 20 lat. W 1954 r. George Devol opatentował urządzenie o nazwie *Programmed Transfer Article*, nie mając zresztą pojęcia, do czego mogłoby służyć. Dopiero spotkanie z Josephem Engelbergerem, inżynierem technologii kosmicznych i miłośnikiem twórczości Asimova zaowocowało założeniem firmy „Unimation" i opracowaniem pierwszego robota przemysłowego nazwanego Unimate. Był on rezultatem przemyśleń obu założycieli firmy po ich „rajdzie" po kilkunastu fabrykach, głównie przemysłu motoryzacyjnego.

Pierwszy Unimate zainstalowany został na próbę na stanowisku do odlewania kokilowego w fabryce General Motors w Trenton. Próbna eksploatacja była tak udana, że niedługo potem GM zainstalował 66 robotów w zakładach w Ohio; niemal równolegle roboty Unimate (które nie były sprzedawane, ale użyczane, co okazało się kolejnym źródłem sukcesu firmy) zamówił do swoich fabryk Ford. W Europie pierwsze roboty przemysłowe pojawiły się w 1967 r. w szwedzkiej fabryce Svenska Metallverken, gdzie podawały elementy do montażu. W 1969 r. GM zastosował 26 robotów spawalniczych na linii spawania nadwozi, w 1972 r. linię spawalniczą zrobotyzował Fiat. Norweska firma Tralffa, dla której roboty Unimate były za drogie, w 1967 r. zbudowała 10 razy tańszego robota lakierniczego. W 1971 r. szwedzki koncern ASEA (późniejszy ABB), który wcześniej korzystał z robotów Unimate, skonstruował robota IRB 6, w którym w 1972 r. zastosowano wczesną wersję procesora Intel 8008[2]. W 1973 r. do gry włączyła się inna europejska firma, niemiecka KUKA, założona w Augsburgu jeszcze w 1898 r. i od 1905 r. zajmująca się urządzeniami spawalniczymi. Już w 1956 r. zaczęła dostarczać automaty spawalnicze fabrykom urządzeń AGD, a potem zakładom Volkswagena i Daimler Benz. W 1973 r. KUKA opracowała elektromechanicznego robota FAMULUS, a dziś jest wielkim międzynarodowym koncernem automatyki i robotyki, mającym swoją filię także w Polsce.

> ***Według normy EN ISO 8373:2012 robot przemysłowy jest „automatycznie sterowaną, programowalną, wielozadaniową maszyną manipulacyjną o wielu stopniach swobody, posiadającą własności manipulacyjne lub lokomocyjne. Maszyna ta może być stacjonarna lub mobilna".***[3]

Od połowy lat 70. XX w. zaczął się szybki rozwój zastosowań robotów przemysłowych, które dziś spotkać możemy we wszystkich obszarach produkcji przemysłowej – od stanowisk wykonawczych po logistykę (np. autonomiczne wózki magazynowe i transportowe).

Zaawansowane zdolności manipulacyjne wykorzystywane są także w robotach medycznych – m.in. w najpopularniejszym obecnie amerykańskim robocie chirurgicznym da Vinci, który coraz powszechniej wykorzystywany jest także w polskich szpitalach. W I kwartale 2021 r. roboty da Vinci zainstalowane były już w 15 autoryzowanych ośrodkach w kraju, i w tym czasie wykonano nimi już 415 zabiegów chirurgicznych[4]. Warto jednak zauważyć, że da Vinci jest urządzeniem „manualnie" wspomagającym sterującego nim chirurga, nie działa w sposób autonomiczny, więc określenie „robot" jest tu trochę na wyrost.

Robotyzacja procesów

W połowie lat 90. zaczyna się wdrażanie rozwiązań „klasycznej" automatyzacji obsługiwanych informatycznie procesów biznesowych – poprzez odpowiednie budowanie aplikacji dziedzinowych albo przez podłączanie się do szyn integracyjnych lub platform i systemów do zarządzania procesami (BPMS – *Business Process Management Systems*). Obsługę procesów można też automatyzować w prostszy sposób, czasem wymuszony przez środowisko systemowe. Zwłaszcza w systemach zastanych (*legacy*) korzysta się z techniki przechwytywania danych wyjściowych programów nazywanej *screen scraping* (zeskrobywaniem z ekranu). Programy czytają dane z pamięci ekranu terminala albo przetwarzają kod HTML ze stron WWW.

Mniej więcej od połowy dekady 2010–2020 zaczyna się szybki rozwój zaawansowanej robotyzacji procesów biznesowych. Pojawiają się złożone narzędzia do zrobotyzowanej automatyzacji procesów (RPA – *Robotic Process Automation*) oraz do zrobotyzowanej automatyzacji stanowiska pracy (RDA – *Robotic Desktop Automation*). W miarę stosowania w tych narzędziach rozwiązań sztucznej inteligencji i uczenia maszynowego pojawiają się narzędzia do kognitywnej/inteligentnej automatyzacji procesów (CPA/IPA – *Cognitive/Intelligent Process Automation*). Wykorzystują one wyniki działania narzędzi do eksploracji procesów (*process mining*) oraz działań i zachowań użytkowników (*task mining*), towarzyszy im oprogramowanie do zarządzania interfejsami programowymi

2 http://liu.diva-portal.org/smash/get/diva2:316930/FULLTEXT01.pdf

3 https://pl.wikipedia.org/wiki/Robot_przemys%C5%82owy

4 https://www.rynekzdrowia.pl/Aparatura-i-wyposazenie/Pierwsze-operacje-na-Podkarpaciu-z-zastosowaniem-robota-da-Vinci-Takich-zabiegow-jest-coraz-wiecej,221982,5.html

(*API Management*). W interfejsach zewnętrznych korzysta się z chatbotów i voicebotów. Chatboty to programy automatyzujące komunikację tekstową w języku naturalnym, często wykorzystuje się w tym celu interfejsy popularnych komunikatorów, można je stosować także na stronach WWW. Natomiast voiceboty to programy wykorzystujące mechanizmy rozpoznawania wypowiedzi głosowej (NLU – *Natural Language Understanding*), które przetwarzają komunikaty głosowe na teksty poddawane analizie z użyciem metod AI. Po sformułowaniu odpowiedzi silnik voicebota uruchamia mechanizmy przetwarzania tekstu z powrotem na głos (*text-to-speech*).

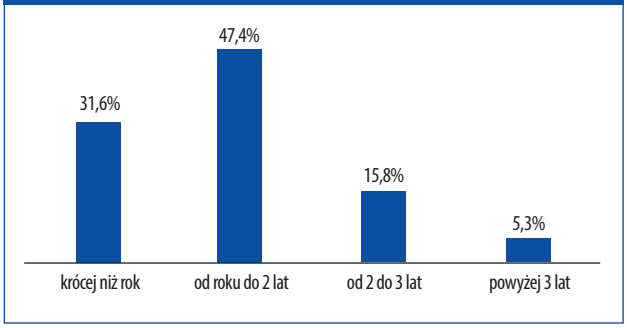
Coraz ściślejszą współpracę programistów z pracownikami merytorycznymi z działów biznesowych zapewniają platformy i narzędzia niskokodowe i bezkodowe (*Low-Code/No-Code*), które umożliwiają tworzenie robotów programowych przez specjalistów dobrze znających procesy biznesowe, ale niebędących programistami i nieznających „tradycyjnych" języków i zrębów. Tworzą oni rozwiązania posługując się wizualnymi kreatorami i formularzami, a wykorzystują do tego predefiniowane komponenty.

Tworzone wymienionymi technikami i narzędziami coraz bardziej złożone roboty programowe działają jako „cyfrowi pracownicy", automatyzujący prace wykonywane do tej pory przez ludzi. Robot programowy może działać jako:

- robot nadzorowany (*software assistant*), współpracujący z człowiekiem-operatorem na jego stanowisku pracy i uruchamiany oraz zatrzymywany przez operatora. Automatyzuje proste czynności wykonywane dotąd przez operatora, który może nadzorować pracę kilku robotów, będąc koordynatorem (orkiestratorem) ich działania;
- robot nienadzorowany (*standalone robot*), działający z dużym zakresem autonomii i wykonujący kilka działań składowych danego procesu biznesowego. Bywa też integratorem pomiędzy różnymi systemami, zwłaszcza systemami legacy. Startuje i działa według wcześniej zdefiniowanych reguł biznesowych; operator nadzoruje jego działanie, interweniując tylko w sytuacjach nadzwyczajnych. Robot nienadzorowany zazwyczaj pracuje na oddzielnym serwerze fizycznym lub wirtualnym.

Jak wskazują wyniki badania serwisu robonomika.pl z 2020 r., robotyzacja procesów biznesowych jest w Polsce jeszcze nowością. Prawie 50% badanych w połowie 2020 r. firm miało za sobą tylko rok do 2 lat wdrożeń robotyzacji (wykres1).

Wykres 1. Od kiedy wdrażana jest robotyzacja procesów biznesowych (n=238)



Źródło: robonomika.pl

Narzędzia do robotyzacji procesów

Klasa narzędzi	Procesy automatyzowane	Obszary zastosowań	Środowisko działania
Zrobotyzowana automatyzacja procesów (RPA)	procesy o charakterze powtarzalnym, czasochłonne w realizacji	procesy operacyjne i wspierające, zwykle nie na styku z klientami zewnętrznymi firmy czy organizacji	zazwyczaj pracują na dedykowanych serwerach fizycznych lub wirtualnych, często związane z systemami legacy
Zrobotyzowana automatyzacja stanowiska pracy (RDA)	automatyzują zwykle działania składowe procesów, w których pozyskiwano dane z różnych źródeł, a ludzie większość czasu poświęcali na przesyłanie danych pomiędzy aplikacjami, ich weryfikację, wizualizację itp.	procesy na styku firmy z klientami zewnętrznymi, a także procesy wspierające	współpracują z chatbotami i voicebotami
Kognitywna/inteligentna automatyzacja procesów (C-RPA/I-RPA)	złożone procesy wymagające przetwarzania bardzo dużej ilości danych, zwłaszcza nieustrukturalizowanych oraz podejmowania decyzji na podstawie wyników przetwarzania	wszystkie rodzaje procesów, zwłaszcza strategiczne procesy biznesowe	zastosowanie zaawansowanych rozwiązań AI i ML

Źródło: robonomika.pl

Robotyzacja w Polsce

W latach 2018 i 2020 serwis robonomika.pl przeprowadził dwa badania zakresu, oceny i efektów robotyzacji w polskich firmach. W drugiej, głównej edycji badania w pełni wypełnione ankiety badawcze przysłało 238 firm produkcyjnych, handlowych i usługowych z różnych branż – od finansów przez produkcję po media. Trzy czwarte badanej populacji stanowiły firmy duże, resztę –średnie. Wybrane wyniki badania przedstawiają wykresy 1 i 2.

Hiperautomatyzacja

Termin hiperautomatyzacja pojawił się przed dwoma laty i od razu trafił na pierwsze miejsce listy „Top 10 Strategicznych trendów technologicznych na rok 2020" firmy doradczej Gartner. W ujęciu Gartnera oraz innych firm analitycznych i dostawców rozwiązań IT zaprezentowane powyżej narzędzia RPA/RDA są zarówno prekursorami, jak i głównymi elementami hiperautomatyzacji.

Poziom automatyzacji działań możliwy do osiągnięcia dzięki hiperautomatyzacji jest dużo wyższy niż automatyzacji osiąganej przy oddzielnym użyciu poszczególnych narzędzi RPA/RDA. Dlatego hiperautomatyzacja jest wykorzystywana do doskonalenia lub zmiany składowych modelu biznesowego organizacji, np. poprzez wprowadzenie nowych produktów lub usług dla nowego segmentu klientów. Wdrażanie ich tradycyjnymi metodami, nawet przy wykorzystaniu automatyzacji, byłoby albo nieopłacalne, albo trudne i pracochłonne.

Pionierami zastosowań robotyzacji, a następnie hiperautomatyzacji procesów biznesowych są firmy sektora finansowego oraz operatorzy telekomunikacyjni. Działają w warunkach bardzo silnej konkurencji, w sektorach mocno regulowanych, więc bardzo ważne jest dla nich utrzymywanie w ryzach poziomu kosztów, a także podwyższanie poziomu satysfakcji klientów, dzięki czemu można zwiększać poziom lojalności klientów i obniża wartość współczynnika odejść (*churn*). Podwyższanie poziomu zaufania społecznego (banki chcą być postrzegane jako instytucje zaufania publicznego) i satysfakcji klientów można osiągać m.in. poprzez redukcję stopy błędów popełnianych przez ludzi oraz podwyższanie sprawności działania całej organizacji.

Czynnikiem dodatkowo motywującym banki do wczesnego wprowadzania robotów programowych jest duży udział systemów legacy. W takich przypadkach dużo prostsze jest wprowadzanie robotów programowych korzystających tylko z technik przechwytywania wyników działania w interfejsach zewnętrznych (wspomnianego *screen scrappingu*), niż „wcinanie się" w kod systemów stworzone nierzadko w niemal zapomnianych już dziś językach programowania. Dodatkowym problemem systemów legacy bywają wprowadzane przez całe lata zmiany w kodzie – udokumentowane niedostatecznie lub wcale.

Hiperautomatyzacja postrzegana jest obecne jako ważne narzędzie cyfrowej transformacji nie tylko firm, ale także instytucji publicznych. Dzięki narzędziom *Low-Code/No-Code* wiele elementów hiperautomatyzacji tworzą i wdrażają nie działy IT (jak w przypadku „tradycyjnej" automatyzacji), ale działy biznesowe albo dedykowane CoE (*Center of Excellence*), tworzone zwykle w działach operacji biznesowych lub pomiędzy działami IT i biznesowymi.

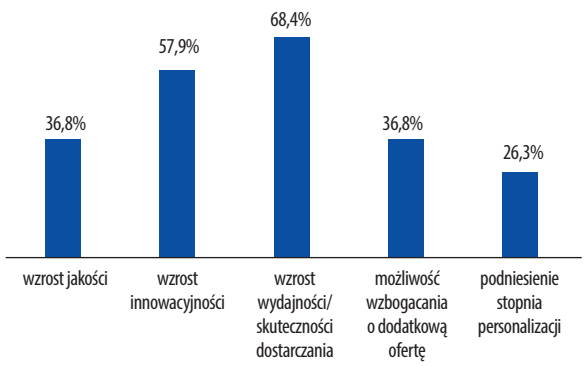
Hiperautomatyzacja to wykorzystywanie połączonych ze sobą zaawansowanych narzędzi robotyzacji procesów biznesowych (RPA/RDA), chatbotów i voicebotów, platform i narzędzi *Low-Code/No-Code* do zautomatyzowanego wykonywania zadań realizowanych wcześniej przez człowieka. We wspomnianych narzędziach, platformach i rozwiązaniach coraz częściej stosowane są elementy sztucznej inteligencji i metody uczenia maszynowego. Hiperautomatyzacja pozwala na uwolnienie pracowników od czynności monotonnych i pracochłonnych, umożliwiając im skoncentrowanie się na działaniach o wyższej złożoności i wartości.

Wbrew wyrażanym obawom hiperautomatyzacja nie służy do pozbywania się pracowników z wdrażających ją firm i organizacji, nie rozwiązuje zresztą problemu deficytu pracowników o odpowiednich kompetencjach, zwłaszcza specjalistycznych. Z doświadczeń wdrożeniowych wynika, że hiperautomatyzacja nie jest też metodą radykalnej obniżki kosztów działania, ani równie radykalnego zwiększenia przychodów wdrażających ją firm. Wdrożenie hiperautomatyzacji jest bowiem dużo bardziej złożone od samej robotyzacji procesów, tym bardziej że wdrażana jest zwykle wtedy, gdy dzięki podstawowej robotyzacji „nisko zwisające kiście" zostały już zerwane – spektakularne efekty uzyskano już na wstępnych etapach robotyzacji. Natomiast już we wstępnych fazach robotyzacji widoczne są efekty pozafinansowe (wykres 2).

Regtech i etyka

Rozwój robotyzacji w sektorach silnie regulowanych pociągnął za sobą pojawienie się firm opracowujących rozwiązania

Wykres 2. Pozafinansowe korzyści dla produktów/usług firmy wynikające z robotyzacji procesów (n=238)



Źródło: robonomika.pl

automatyzacji/robotyzacji badania i zapewniania zgodności procesów z regulacjami. Rozwiązania takie nazywane są regtechem. Rozwój i wdrażanie rozwiązań klasy regtech najprawdopodobniej pociągnie za sobą regulacje w dwóch obszarach:

- regulację zastosowań hiperautomatyzacji w instytucjach finansowych i w innych dziedzinach ściśle regulowanych (np. komunikacja elektroniczna, ochrona środowiska);
- regulację metod automatyzacji i robotyzacji działania samych organów regulacyjnych (prowadzenia audytów regulacyjnych, pozyskiwania oraz analizy danych pobieranych od regulowanych podmiotów, zasad wspierania narzędziami klasy regtech formułowania ocen i wydawania decyzji regulatorów).

Rozwój zastosowań narzędzi RPA w regulacjach wymagać będzie pobierania przez regulatorów wymaganych przez nich danych on-line i reagowania w trybie niemal rzeczywistym. Będzie to duże wyzwanie zarówno dla legislacji dotyczącej podstaw i zasad działania organów regulacyjnych, jak i dla samych pracowników organów regulacyjnych, którzy będą musieli zdobyć nowe dla nich kompetencje.

Wyzwaniem są też aspekty etyczne automatyzacji, robotyzacji i hiperautomatyzacji. Dotyczą one zarówno pracowników firm i instytucji, w których wprowadzane są narzędzia robotyzacji, jak i ich klientów. Pracownicy robotyzowanych organizacji boją się, że roboty odbiorą im pracę. W miarę upowszechniania się rozwiązań AI, wspierających procesy rekrutacji pracowników oraz oceny ich wydajności i przydatności w firmie, nasilają się też obawy, że decyzje dotyczące pracowników podejmowane będą w sposób zrobotyzowany. Podnosi to znaczenie budowania i trenowania robotów programowych wspomagających HR na danych dobranych w sposób niedyskryminujący z uwagi na: pochodzenie etniczne, kolor skóry, wyznanie, płeć, wiek i status ocenianych osób.

Jeden z dostawców narzędzi RPA zaproponował etyczne ramy robotyzacji (*Robo-Ethical Framework*)[5]. Są wśród nich m.in.: minimalizacja ryzyka stronniczości decyzji, obowiązek umożliwienia audytu automatycznych decyzji, możliwość monitorowania akcji podjętych przez roboty, stosowanie do treningu zweryfikowanych i możliwych do zidentyfikowania źródeł danych, informowanie ludzi o możliwościach i ograniczeniach automatyzacji, ochrona przed nadużyciami i nielegalnym dostępem.

Natomiast aspekty dotyczące klientów podlegających robotyzowanym procesom dotyczą głównie decyzji podejmowanych m.in. w ocenie zdolności kredytowej klienta banku, definiowaniu warunków prowadzenia kont (oprocentowanie, limity autoryzacyjne) czy stawek ubezpieczeniowych[6]. Wobec stałego rozbudowywania i rozszerzania mechanizmów bezpieczeństwa (ochrona przed nieautoryzowanymi transakcjami, procedury antyfraudowe, ochrona przed praniem brudnych pieniędzy i działalnością terrorystyczną) podnosi się kwestie zarówno zbyt słabego działania algorytmów i narzędzi (przepuszczanie transakcji niedozwolonych), jak i zbyt silnego (blokowanie działań legalnych i prawidłowych w wyniku źle dobranych danych do trenowania robotów). Pojawiają się też obawy związane z coraz szerszym stosowaniem nie tylko narzędzi cyfrowego marketingu usług finansowych, lecz także metod AI w analizach behawioralnych klientów.

Wraz z pojawieniem się „cyfrowych pracowników" rośnie rola prawidłowej współpracy ludzi z robotami programowymi. Równie ważne jak tworzenie i wdrażanie robotów programowych jest dostarczanie pracownikom kompetencji potrzebnych do pracy z robotami, zwłaszcza w procesach nazywanych *Human-in-the-Loop*, przede wszystkim w sytuacjach wyjątkowych, nie obsługiwanych w całości przez roboty i wymagających interwencji człowieka.

5 https://www.nice.com/rpa/assets/media/pdf/nice-robo-ethical-framework.pdf

6 W art. 105a polskiego Prawa bankowego jest już ust. 1a: „Banki (….) mogą podejmować decyzje, opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, danych osobowych – również stanowiących tajemnicę bankową – pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska".

Specjaliści coraz bardziej do wynajęcia?

Na przyszłość rynku pracy będą miały wpływ nie tylko nowe zawody, lecz także nowe formy zatrudnienia związane z nowymi, technicznymi możliwościami świadczenia usług oraz nowymi modelami biznesowymi wynikającymi z postępującej cyfryzacji gospodarki.

Trwają dyskusje, jak zmieni się rynek pracy pod wpływem automatyzacji i robotyzacji. Zastanawiamy się, w jakich zawodach ludzi zastąpi sztuczna inteligencja. Tymczasem już dzisiaj za sprawą technik informacyjnych dokonują się niemniej istotne dla przyszłości rynku pracy zmiany w obszarze form zatrudnienia. Warto śledzić i analizować zarówno wynikające z nich korzyści, jak i zagrożenia.

Andrzej Gontarz
ekspert ds. monitoringu rynku w zespole Sektorowej Rady ds. Kompetencji – Informatyka.

Gig ekonomia w natarciu

Jedną z nich jest tzw. ekonomia współdzielenia, której integralną częścią jest też gig ekonomia. Jej rozwój istotnie wspiera rosnąca popularność platform cyfrowych i aplikacji do łączenia zleceniodawców ze zleceniobiorcami.

Gig economy stała się już w zasadzie faktem. Według szacunkowych danych, obecnie około 20–30% aktywnych zawodowo osób w USA i Unii Europejskiej wykonuje swoją pracę poprzez jednorazowe zlecenia lub kontrakty krótkoterminowe. A prognozowany jest dalszy, jeszcze szybszy wzrost tego zjawiska. Niektóre przewidywania mówią, że niebawem nawet połowa pracujących będzie niezależnymi kontraktorami. Według opinii ekspertów, ten segment rynku pracy w 2023 r. będzie miał globalną wartość 455 mld dolarów.

Do elastycznych form zatrudnienia przekonuje się coraz więcej firm. Według raportu Gartnera, prawie 33% praco-

dawców rezygnuje z zatrudniania pracowników etatowych na rzecz współpracy z niezależnymi specjalistami. Z kolei według raportu firmy Morgan Stanley, już w 2027 r. gigerzy stanowić będą ponad połowę amerykańskiej siły roboczej.

Jednorazowo i na odległość

Gig ekonomia charakteryzuje się tym, że powszechną formą zatrudnienia są tymczasowe stanowiska pracy i ograniczone do określonych działań umowy, a pracownicy są angażowani przez firmy tylko do realizacji konkretnych, krótkoterminowych projektów, zadań i zleceń. Ta forma pracy jest też określana mianem gospodarki fuch czy gospodarką zleceniową.

Osoby, które stanowią dla pracodawców tymczasową siłę roboczą, to gigerzy, zwani też freelancerami, zleceniobiorcami, niezależnymi profesjonalistami czy pracownikami kontraktowymi. Samo określenie „gig" zostało zaczerpnięte ze świata muzycznego, gdzie oznaczało jednorazowy występ lub koncert w jednym miejscu.

Według amerykańskiego Departamentu Pracy, branżami szczególnie sprzyjającymi rozwojowi gig gospodarki są: sztuka i projektowanie, technologie komputerowe i informacyjne, media cyfrowe i drukowane, budownictwo i usługi pokrewne, komunikacja i transport. Za sprawą rozwoju technik cyfrowych do grupy gigerów mogą też jednak dołączać specjaliści z innych sektorów. Na przykład w opiece zdrowotnej pojawiają się lekarze specjaliści od analizy i opisu wyników diagnostyki obrazowej, którzy nie są związani z żadną placówką medyczną, tylko wykonują zlecenia dla wielu przychodni czy szpitali, otrzymując pliki z USG czy zdjęcia rentgenowskie przez internet.

Grupą najbardziej zainteresowaną pracą na zlecenia, wykonywaną zdalnie z dowolnego miejsca na świecie, są przedstawiciele pokolenia millenialsów. Według prognoz Forbesa, w 2025 r. będą oni stanowić 75% globalnej siły roboczej. Jak wynika z raportu EY i Giglike „GIG on. Nowy Ład na rynku pracy", już 42% millenialsów jest freelancerami. To często bardzo mobilni, wysoko wykwalifikowani specjaliści, którzy nie chcą na trwałe wiązać się z żadnym pracodawcą ani konkretnym miejscem pracy. Wolą, wedle własnych potrzeb i oczekiwań, wykonywać pojedyncze zlecenia czy zadania zamiast podejmować długoterminowe zobowiązania. Grupa osób zwanych cyfrowymi nomadami szybko się powiększa. – *Pokolenie millenialsów i generacji Z są to osoby ceniące sobie swobodę, elastyczność i samodzielność w działaniu* – oceniają autorzy wspomnianego raportu EY i Giglike.

Wśród gigerów są też jednak osoby wykonujące proste, nisko płatne prace: kurierzy rowerowi czy kierowcy przewozów pasażerskich. Zdaniem analityków Mastercard, 58% pracowników gig economy związanych jest obecnie z branżą logistyczną, która rozwinęła się bardzo mocno pod wpływem skutków pandemii. Warto przy tej okazji pamiętać, że w realiach dzisiejszej gospodarki jedni stają się gigerami z wyboru, inni z konieczności.

Większa niezależność, niższe koszty

Rozwój gospodarki zleceniowej jest jednak generalnie wzmacniany przez coraz większą dostępność platform cyfrowych, portali i aplikacji mobilnych, ułatwiających kojarzenie ze sobą firm poszukujących pracowników tymczasowych i osób zainteresowanych wykonaniem pojedynczego zadania czy udziałem w pojedynczym projekcie. Tego typu rozwiązania zyskały na popularności w okresie pandemii, która udowodniła, że wiele prac można faktycznie wykonywać na odległość, bez konieczności pobytu pracownika w biurze.

Główne korzyści z angażowania gigerów

- Elastyczność i szybkość reakcji – możliwość szybkiego uzupełniania luki kompetencyjnej w celu odpowiedzi na potrzebę na konkurencyjnym rynku.
- Wzrost innowacyjności – włączenie osób spoza organizacji stwarza okazję do wymiany wiedzy i praktyk ponad organizacyjnymi silosami.
- Oszczędności kosztowe – firmy mogą generować oszczędności poprzez dopasowywanie zasobów do potrzeb biznesowych.

Źródło: GIG on. Nowy Ład na rynku pracy, EY i Giglike, 2021

Osoby decydujące się na status niezależnego kontraktora cenią sobie przede wszystkim niezależność wynikającą z tej formy zatrudnienia. Wśród jej zalet, jak podają autorzy raportu „GIG on. Nowy Ład na rynku pracy", znajdują się także: możliwość stałego rozwoju i zdobywania doświadczenia, różnorodność ofert pozwalająca uczestniczyć w różnych projektach i pracować dla różnych zleceniodawców oraz satysfakcjonujące dochody. Korzyści te są w stanie zrównoważyć czy niejednokrotnie wręcz przewyższyć w opinii gigerów ryzyko związane z niestabilnością dochodów czy też ich chwilową utratą, wynikającą z braku zamówień.

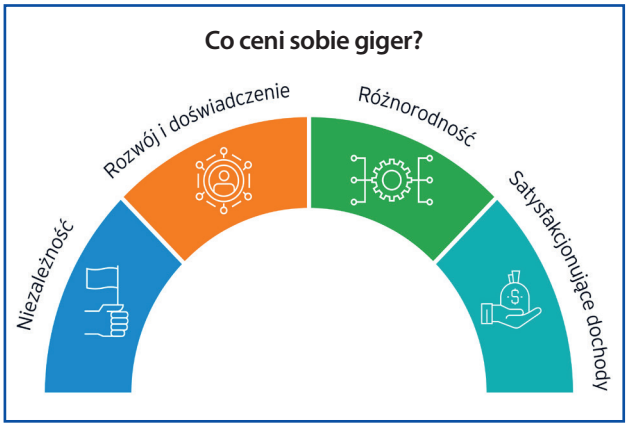
Z kolei dla pracodawców, jak wynika z dostępnych na rynku badań i analiz, korzyścią z zatrudniania gigerów jest zmniejszanie obciążeń finansowych związanych z utrzymaniem stałego pracownika. Za pracujących na własny rachunek kontraktorów nie trzeba płacić składek zdrowotnych czy emerytalnych. Korzyści, jak pokazuje również pandemia, mogą wynikać ze zmniejszenia przestrzeni biurowej, której nie trzeba zapewniać pracownikom zdalnym, czy też z braku innych wydatków na utrzymanie stałego stanowiska pracy.

Nie bez znaczenia dla pracodawców jest również możliwość wyboru najlepszych w danej dziedzinie specjalistów. Firma nie jest ograniczona tylko do własnej, zatrudnionej na stałe kadry, może swobodnie wybierać i zatrudniać dowolnych, najbardziej pasujących i potrzebnych do danego projektu czy zadania fachowców.

Prawo do ochrony

Z korzyściami gig ekonomii idą jednak w parze również liczne zagrożenia. Wiążą się one głównie z brakiem należytej ochrony socjalnej i praw pracowniczych dla wykonujących ten rodzaj pracy. Są one realne, nawet jeśli mający dostatek zleceń gigerzy wypierają związane z nimi ryzyka. W Polsce pojawiają się nawet głosy ostrzegające przed nowym rodzajem umów śmieciowych. W ostatnim czasie, w związku z rosnącą popularnością platform cyfrowych do dzielenia się pracą, pojawiły się również obawy o odhumanizowanie relacji pracownik – pracodawca. Wiążą się one głównie z tym, że zarządzanie zleceniami będzie miało coraz bardziej algorytmiczny charakter, a przydzielanie pracy będzie się odbywać w sposób całkowicie automatyczny.

Ekonomia zleceń pozwala na bardziej efektywne i swobodne wykorzystanie umiejętności przez specjalistów świadczących niezależne usługi dla wielu pracodawców. Z drugiej strony pozostawia gigerów samym sobie, uzależniając ich los jedynie od koniunktury na rynku pracy i własnej umiejętności w zdobywaniu kolejnych zleceń. Zagrożeniem w takiej sytuacji może być chociażby to, że nie nabywają prawa do ochrony na wypadek bezrobocia.



Źródło: GIG on. Nowy Ład na rynku pracy, EY i Giglike, 2021

Poprawie ochrony pracowników z obszaru gig ekonomii mają służyć nowe regulacje unijne. Wiosną 2019 r. Parlament Europejski zatwierdził przepisy określające minimalne prawa pracownicze dla wszystkich zatrudnionych w Unii Europejskiej. Mają one zapewnić szczególną ochronę zatrudnionym na podstawie nietypowych form i umów oraz wykonującym niestandardową pracę, w tym właśnie gigerom. Te grupy, w myśl unijnego ustawodawcy, są najbardziej narażone na naruszenia praw pracowniczych. Po zatwierdzeniu przepisów przez Radę UE, kraje członkowskie będą miały 3 lata na wdrożenie nowych zasad do krajowych porządków prawnych. Zdaniem Parlamentu Europejskiego, współczesny rynek pracy wymaga elastycznych form zatrudnienia, powinny one jednak iść w parze z odpowiednią ochroną pracowników.

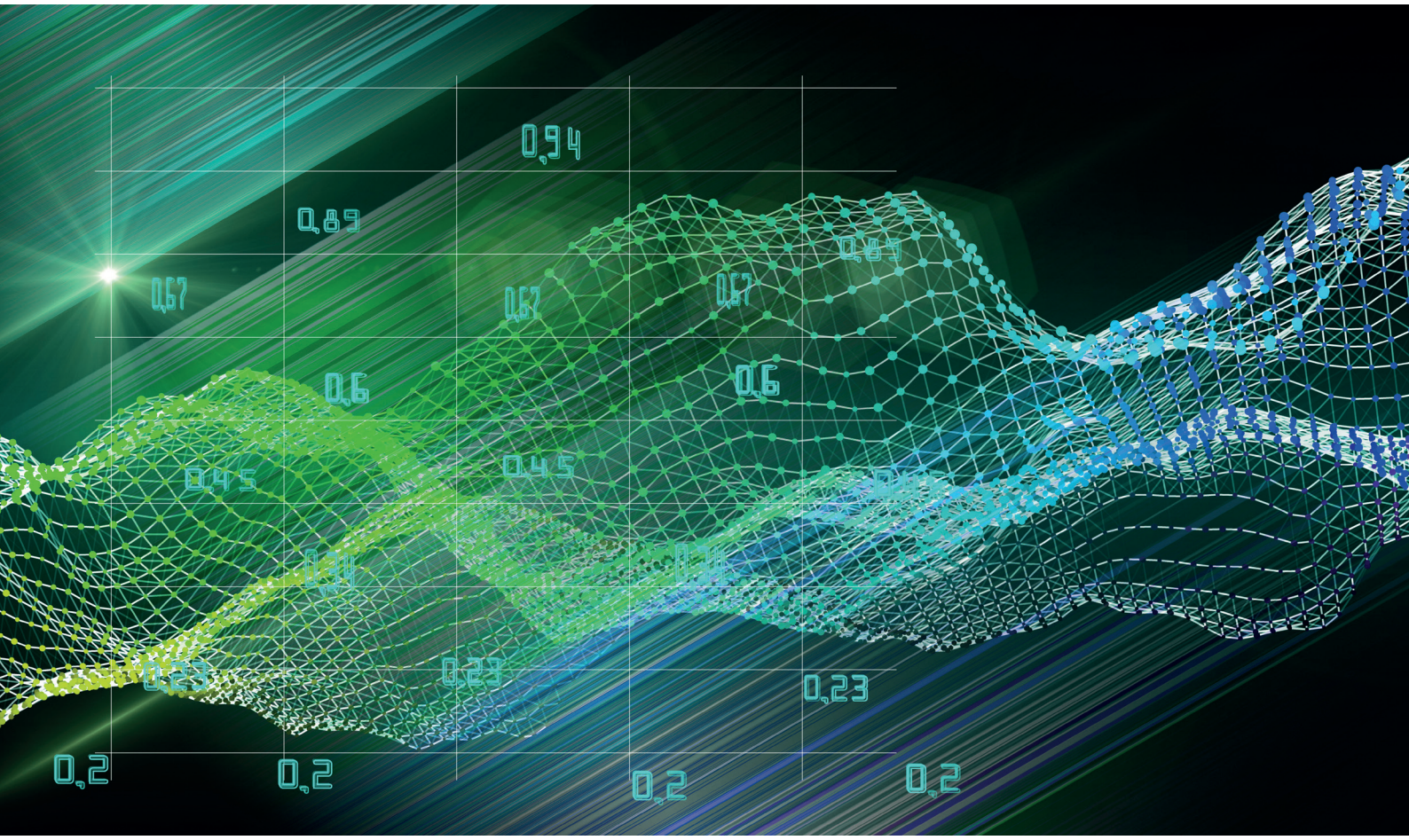
Informatycy najbardziej poszukiwanymi freelancerami

Według tegorocznego raportu platformy Useme.com, programiści DevOps i developerzy gier są obecnie najlepiej opłacanymi wolnymi strzelcami na polskim rynku. Ich stawki godzinowe wynoszą odpowiednio 149 zł brutto i 134 zł brutto. Na dobre zarobki mogą też liczyć: analitycy digital data i e-commerce (119 zł brutto za godzinę pracy) oraz programiści Java (100 zł). W rankingu TOP 10 najlepiej zarabiających polskich freelancerów znalazł się także specjalista ds. bezpieczeństwa IT, który zajął szóste miejsce w zestawieniu.

Zdaniem autorów raportu, pandemia nie zmniejszyła, wbrew wcześniejszym obawom, zapotrzebowania na pracę wolnych strzelców. Obecnie mamy nawet do czynienia ze znaczącym wzrostem zainteresowania pracą zdalną i zatrudnianiem freelancerów.

Próby uregulowania sytuacji prawnej pracowników kontraktowych pojawiają się również na rynku amerykańskim. Wśród pomysłów na legislacyjne uporządkowanie zjawiska gig ekonomii są m.in. postulaty zapewnienia gigerom dostępu do opieki zdrowotnej, ubezpieczenia od bezrobocia oraz systemu emerytalnego. Według wielu specjalistów, dostęp do świadczeń socjalnych nie powinien być uzależniony od statusu pracownika i formy świadczenia przez niego pracy. Pojawiają się też głosy, by stworzyć regulacje specjalnie przeznaczone dla gigerów, by zapewnić im z jednej strony ochronę socjalną, a z drugiej – zagwarantować dotychczasową elastyczność świadczenia pracy.

W Polsce miało pojawić się ujednolicenie wszystkich form zatrudnienia w programie Polski Ład. Ostatecznie nic z tych zapowiedzi nie wyszło i pomysł ten nie znalazł się w projekcie ustawy. Gigerzy na naszym rodzimym rynku powinni jednak, zdaniem autorów raportu „GIG on", zainteresować się zmianami podatkowymi wprowadzanymi w ramach Polskiego Ładu. Najważniejsze z nich dotyczą m.in. niższej stawki ryczałtu PIT dla branży IT, likwidacji zryczałtowanej składki zdrowotnej, nowej skali podatkowej składającej się z dwóch progów, czy nowej, stałej kwoty wolnej od podatku.



O algorytmach inaczej

Informatyka jako teoria i praktyka – z racji rozległych zastosowań – wywołuje nie tylko różnorodne zachowania, lecz także emocje oraz wyobrażenia, z których wiele odbiega od jej racjonalnej istoty. Przeoczamy jej rzeczywiste funkcje, a nawet fałszujemy je. Wymownym przykładem jest ekscytacja „tymi strasznymi algorytmami", które mają dotyczyć milionowych rzeszy uczestników grup społecznościowych używających Facebooka i jego komunikatorów.

Marek Hetmański
profesor zwyczajny w Instytucie Filozofii Uniwersytetu Marii Curie-Skłodowskiej, kierownik Katedry Ontologii i Epistemologii, członek Polskiego Towarzystwa Filozoficznego i Polskiego Towarzystwa Kognitywistycznego. Filozof i epistemolog, zajmuje się problemami poznania i wiedzy w ich uwarunkowaniu społecznymi i technicznymi czynnikami, w tym zwłaszcza technologiami informatycznymi.

Przypisywanie algorytmom – bezpośrednio regulującym (1) *funkcjonowanie* komputerów, w których są one implementowane, pośrednio kierującym (2) *zachowaniem* się użytkowników narzędzi i urządzeń informatycznych, w dalszej kolejności ich (3) *działaniem* w konkretnych sytuacjach, na dalszym zaś etapie ich (4) *myśleniem*, w tym *wyobrażaniem* sobie i *emocjonalnym* doświadczaniem rzeczy i zjawisk poddanych algorytmicznemu przetwarzaniu – wyłącznie zła, niszczycielskiej mocy, a nawet perfidii jest pomieszaniem faktów, wartości i znaczeń, które współtworzą informatykę. Każdy z tych aspektów i etapów, na jakich algorytmy funkcjonują – różne ich rodzaje, mniej lub bardziej złożone czy skuteczne w funkcjonowaniu, implementowane komputerowo – decyduje o złożoności oraz odmienności ich działania; fakt ich tak wielostronnego funkcjonowania jest wciąż przeoczany. Wynika to nie tylko z niezrozumienia specyfiki informatyki jako nauki i praktyki, jej rozlicznych uwarunkowań technologicznych i społecznych, ale także z niezdrowej sensacji, jaką tworzą masowe media, politycy, sami internauci wokół kłopotów internetowego giganta, który nadużywa jednej z funkcji algorytmów.

> *Znamienne, że większość z nas o algorytmach formułuje opinię, której rzeczowość i precyzja są tak niskie, jak wysoka jest z kolei ignorancja co do ich istoty, a już na pewno nieumiejętność posługiwania się nimi czy też ich tworzenia.*

Co z tymi algorytmami?

Proponuję rozpatrzeć każdy z tych wątków po kolei, aby podać przesłanki do udzielenia sensownej odpowiedzi na to pytanie. Na początek konieczne jest uściślenie terminologiczno-definicyjne, które zdejmie z algorytmu niesprawiedliwą i niekorzystną opinię, przynajmniej w pewnej jej części. Algorytm jako procedura o skończonej liczbie kroków i określonym czasie wykonania jest podstawą zautomatyzowanych i zmechanizowanych procesów i zadań realizowanych przez szeroką klasę urządzeń.

Użytkownik obserwuje efekty działania algorytmów. Algorytm nie służy do rozwiązywania ani wszystkich, ani w jednakowy sposób przeprowadzanych przez człowieka zadań; skuteczny dla jednych przedsięwzięć, nie gwarantuje rozwiązywalności innym operacjom i działaniom, które algorytm wykorzystują.

Algorytmy zawsze są uwarunkowane techniczną stroną urządzeń je implementujących oraz warunkami, w jakich funkcjonują urządzenia i narzędzia nimi sterowane. To one decydują, czy dany algorytm (w żadnym przypadku wszystkie) uznajemy za dobry czy zły; na opinię o algorytmie składać się mogą jego formalne własności, jak również ocena skutków jego funkcjonowania, a te mogą być dalekie od prostoty i jednoznaczności.

Funkcjonowanie jakichkolwiek komputerowych urządzeń sterowanych algorytmicznymi programami, w tym łączności internetowej, nie gwarantuje pełnej niezawodności zachowań użytkownika; ocena ich skutków i wyników nie jest logiczną konsekwencją własności algorytmów. Można nieefektywnie i błędnie działać, mając w rękach urządzenie kierowane skończeniewymiarowym programem, podobnie jak skutecznie i satysfakcjonująco się zachować w oparciu o program z rodzaju NP-trudnych lub nierozwiązywalnych. W ocenie algorytmu uwzględnić trzeba tak samo jego matematyczno-informatyczną *formę*, jak i pragmatyczne *funkcjonowanie*, w którym z kolei uwzględnić należy zarówno psychologiczny, jak i socjologiczny aspekt.

Algorytm to cecha instrumentu określonego działania. Ludzie podejmują te działania nie z powodów informatycznych, lecz życiowych (np. produkcja, komunikowanie się, edukacja czy prowadzenie badań), a jego formalne cechy (skończeniewymiarowość procedury) są zaledwie środkiem, a nie celem samym w sobie. Z kolei większość celów działania człowieka, nawet jeśli jest ono podejmowane według standardów informatycznych oraz ekonomicznych motywów (w globalnej gospodarce są one nierozłączne), osiągnąć można zarówno tą właśnie drogą, jak i poza, obok, a nawet pomimo niej.

Algorytm, mówiąc skrótowo, rządzi komputerem, a nie człowiekiem, dla którego jest on jednym ze środków, które na ogół dobiera (spośród niealgorytmicznych) odpowiednio do swojego, a nie komputerowego celu.

Większość algorytmów działa w urządzeniach bez świadomego udziału człowieka, bez wiedzy o ich strukturze i funkcjonowaniu (w tym ograniczeniach), co najwyżej przy bezwolnej aprobacie dla ich użycia, która na ogół sprowadza się do bezrefleksyjnej zgody na rynkowe reguły, które rządzą wszystkimi zalgorytmizowanymi urządzeniami.

I tutaj zaczyna się problem rozbieżności, jak również konfliktu, między algorytmicznymi procesami i procedurami a głównie *niealgorytmicznymi* zachowaniami i działaniami człowieka. Większość naszych zwykłych działań nie tylko nie odbywa się przy pełnej świadomości ich natury i funkcjonowania, lecz również ich długotrwałe wykonywanie, powtarzanie i spożytkowywanie jest nieświadome; tym bardziej oryginalne i twórcze *działania* (jako niealgorytmiczne

i nieopisywalne algorytmicznie) również nie zakładają tej świadomości w swoim jednorazowym akcie. O ile w pierwszym przypadku tłumaczy nas z tego faktu ewolucja gatunku homo sapiens, która uwolniła ludzki umysł z nadmiaru informacji koniecznych dla obliczania korzystnych decyzji, sprowadzając je do postaci algorytmu, o tyle przypadek drugi jest bardziej złożony i wymaga głębszej analizy.

Zauważmy, że standardy oraz normy społecznego współdziałania, produkcji czy walki, a nade wszystko skutecznego porozumiewania się, wymagają uświadamiania sobie przez ludzi, z jednej strony, algorytmicznych procedur ich funkcjonowania, z drugiej zaś (i co najważniejsze), różnic między nieświadomym i uświadamianym funkcjonowaniem algorytmicznych urządzeń. Bez tego będą się tylko jeszcze bardziej rozpowszechniały fałszywe wyobrażenia o algorytmach.

All that jazz

Przejdę w tym miejscu do Facebooka, manifestów jego szefa i całego szumu medialnego wokół algorytmów używanych przez internetowego giganta. Znaleźć można tutaj wszystkie konsekwencje społecznego wcielania się informatyki w masowe technologie, zwłaszcza wikłania się w grę rynkowych globalnych interesów, które wraz z radykalnymi opiniami użytkowników współtworzą cały ten szum wokół używanych przez komunikatory algorytmów.

Mark Zuckerberg wytworzył wokół swoich internetowych produktów i usług komunikacyjnych aurę wolnych, twórczych i prospołecznych mediów tworzących globalną, ogólnoludzką wspólnotę. Idea ta została tak sformułowana w głośnym manifeście z 2017 r., aby przedstawić domniemane, wyolbrzymione, wyłącznie pozytywne skutki łączności za pomocą facebookowych komunikatorów i usług, na plan dalszy przesuwając, a nawet ukrywając, wszystkie niedoskonałości algorytmicznych narzędzi. Naiwna wizja globalnej wspólnoty, składającej się z grup tworzących społecznościowe portale i mających jakoby jeden cel – dzielić się własną wiedzą i wytwarzać altruistyczne wartości – jest obecnie osłabiona wymownymi opisami używania Facebooka czy Instagrama do mobbingu, molestowania, siania mowy nienawiści czy terrorystycznych ataków; z równą emfazą i skrajnością meliorystyczna wizja zaczyna być zastępowana obrazem szatańskich intencji i środków.

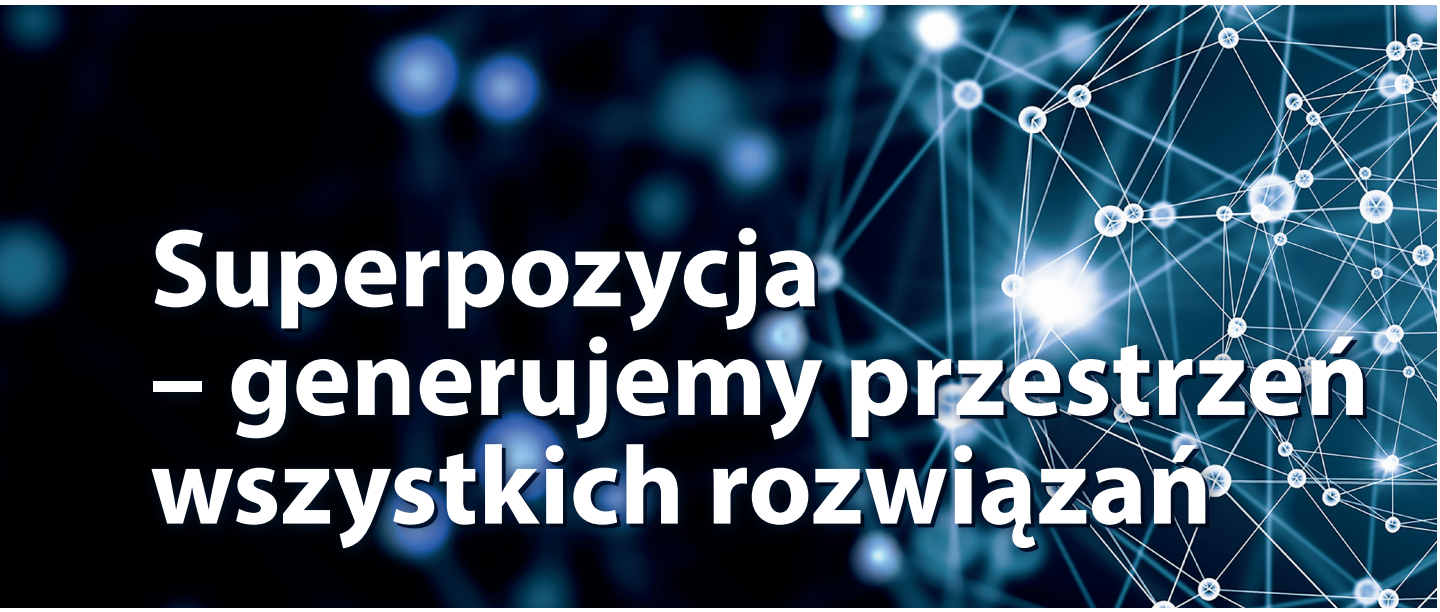
Skrzętnie ujawniane fakty nadużyć internetowych komunikatorów – wcale nie różne co do istoty od „symbolicznej przemocy" (według określenia Pierre'a Bourdieu) tradycyjnych mediów jak brukowa prasa czy telewizja, a tylko bardziej masowe – należy właściwe zrozumieć, aby pojąć w tym rolę owych algorytmów. Zuckerberg mówił o nich jako środkach tworzenia wspólnych zainteresowań, poglądów i postaw, które miałyby się swobodnie propagować i upowszechniać w małych grupach i na społecznościowych portalach. Promował je jednocześnie jako środki samokontroli i ograniczania nadużyć w postaci radykalnych i szkodliwych treści (genderowych, rasistowskich, religijnych). Internetowe narzędzia posługujące się wyspecjalizowanymi algorytmami – opatentowanymi, strzeżonymi, traktowanymi jako korporacyjny zasób, najważniejszy środek produkcji – przedstawione zostały jako samodyscyplinujące się, a nawet kształtujące postawy altruizmu oraz odpowiedzialności za słowo.

W świetle uczynionych powyżej dystynkcji i analiz trzeba powiedzieć, że: (1) funkcjonalną i formalną własność swoich algorytmów Facebook zminimalizował, ukrył i nadinterpretował, przedstawiając jako bezproblemowe i wyłącznie korzystne, zaś (2) użytkowanie komunikatorów przez nie sterowanych uprościł poprzez zautomatyzowanie czynności użytkowników, czyniąc je nieświadomymi (bezrefleksyjnymi, niekontrolowalnymi) zachowaniami, łatwo sterowalnymi, głównie jednak (3) wygenerował, wręcz propagował zachowania o radykalnym charakterze, przedstawiając je jako altruistyczne, obywatelskie, opiniotwórcze działania prospołeczne, nakierowane na obronę wolności słowa, prywatności i bezpieczeństwa (dające się jakoby jednocześnie i bezkonfliktowo zrealizować).

Dopiero w takim ujęciu – uwzględniającym każdą z dziedzin informatyki i jej narzędzia rozpatrywane z perspektywy kognitywistycznej, socjologicznej i filozoficznej – widać, jak jej funkcjonalne własności bywają albo eksponowane, albo ukrywane, zaś konkretne użycia i wygenerowane zachowania użytkowników stają się przedmiotem nie tylko rynkowej konkurencji, lecz także fałszujących opinii ze strony twórców czy dysponentów informatycznych narzędzi, jak również skrajnych ocen ze strony tych, którzy dają się w taką sytuację wplątać.

Sensownym wyjściem z tego jest nieustanne analizowanie, zawsze interdyscyplinarne, wszystkich aspektów informatycznej cywilizacji oraz rozmyślne i samokontrolujące posługiwanie się informatycznymi narzędziami.

Jeszcze jedno – powierzenie któregokolwiek z tych zadań wyłącznie sztucznej inteligencji skończy się nieuchronnie jeszcze większym kryzysem cywilizacyjnym niż ten, który powoli nas obejmuje.



Superpozycja – generujemy przestrzeń wszystkich rozwiązań

Przewodnik po nauczaniu informatyki kwantowej cz. 3.

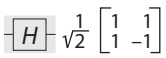
Marek Perkowski

absolwent Wydziału Elektroniki Politechniki Warszawskiej, tu również zdobył tytuł doktora automatyki. Od 1983 r. pracuje na Wydziale Inżynierii Elektrycznej i Komputerowej w Portland State University, gdzie jest profesorem zwyczajnym i dyrektorem Laboratorium Robotów Inteligentnych.
Jeden ze współautorów WARP – pierwszego kompilatora języka VHDL dla układów FPGA. Twórca Diagramów Decyzyjnych Kroneckera, struktury krat logicznych i koncepcji robotów kwantowych. Przyczynił się do powstania oprogramowania dla syntezy logicznej, używanego w przemyśle USA. Pracował jako profesor wizytujący w Holandii, Francji, Japonii, Korei Południowej i Ludowej Republice Chin. W latach 2002–2004 był profesorem zwyczajnym w KAIST – Korean Advanced Institute of Science and Technology, gdzie zajmował się robotyką humanoidalną i komputerami kwantowymi. Kierował Komitetem Logiki Wielowartościowej IEEE w latach 2003–2005 i grupą roboczą Towarzystwa Inteligencji Obliczeniowej IEEE dla Inżynierii Kwantowej w latach 2006–2007. Autor ponad 515 publikacji o automatycznym projektowaniu, syntezie logicznej, logice wielowartościowej, logice odwracalnej, uczeniu maszynowym, robotyce i informatyce kwantowej.

Źródło: GetReal-WordPress.com

„**Przewodnik po nauczaniu informatyki kwantowej**" przedstawia metodologię rozwiązywania decyzyjnych Problemów ze Spełnianiem Ograniczeń (PSO) i problemów optymalizacyjnych z wykorzystaniem hybrydowego systemu komputera klasycznego i komputera kwantowego z algorytmem Grovera. Po wprowadzeniu układów odwracalnych jako rozszerzenia układów boolowskich pokazujemy superpozycję i splątanie kwantowe w sposób prosty, ale ścisły. Następnie przedstawiamy podstawowe dla wielu algorytmów kwantowych pojęcie wyroczni. Omawiamy, w jaki sposób wyrocznie są stosowane do rozwiązywania problemów decyzyjnych i optymalizacyjnych. Przykład znalezienia wszystkich „Optymalnych Zbiorów Suportujących" dla funkcji boolowskiej, który znajduje zastosowania w uczeniu maszynowym, dokładnie ilustruje proponowaną metodologię. Na koniec wyjaśniamy, jak działa algorytm Grovera. Po przeczytaniu tego cyklu uważny Czytelnik powinien być w stanie tworzyć podobne systemy kwantowe dla nowych, podobnych do przedstawionych, problemów.

Macierze unitarne mają składowe zespolone i operują na stanach kwantowych reprezentujących stany bazowe, ale również na stanach będących w superpozycji lub w splątaniu kwantowym. Bramki „istotnie kwantowe", jak bramka Hadamarda, służą do tworzenia superpozycji. Natomiast wraz z bramkami permutacyjnymi bramki Hadamarda tworzą splątania kwantowe.



Rys. 1. Symbol bramki Hadamarda i macierz unitarna tej bramki kwantowej

Gdy bramka Hadamarda operuje na bazowym stanie wejściowym $|0\rangle$, otrzymujemy:

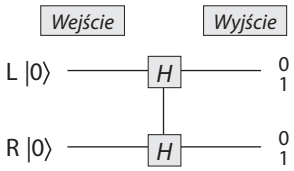
H * $|0\rangle$ (gdzie * jest symbolem mnożenia macierzy przez wektor):

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} * \begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 \times 1 + 1 \times 0\\ 1 \times 1 + (-1) \times 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Zauważmy że współczynnik c_0 dla stanu kwantowego $|0\rangle$ jest $\frac{1}{\sqrt{2}}$ oraz współczynnik c_1 dla stanu kwantowego $|1\rangle$ jest $\frac{1}{\sqrt{2}}$. $|c_0|^2 / (|c_0|^2 + |c_1|^2) = 50\%$, $|c_1|^2 / (|c_0|^2 + |c_1|^2) = 50\%$. Widzimy więc, że zastosowanie bramki Hadamarda do stanu bazowego $|0\rangle$ tworzy superpozycję. Gdy zmierzymy ten stan superpozycji, to otrzymamy wartość 0 z prawdopodobieństwem 50% i wartość 1 z prawdopodobieństwem 50%. Przed pomiarem stan kwantowy na wyjściu bramki Hadamarda jest $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Ten stan kwantowy nazywany jest „Cat State", na cześć słynnego Kota Schrödingera. Stan ten jest elementarną superpozycją. Teraz już matematycznie rozumiemy, co to jest nasz Kot Schrödingera. Możemy go wykorzystać praktycznie, gdyż nie jest już on dla nas jedynie metaforą stworzoną przez słynnego fizyka dla ułatwienia zrozumienia problemu (co było źródłem wielu mylących wytłumaczeń w pracach popularnonaukowych).

> *Nie starając się zrozumieć fizyki tego zadziwiającego zjawiska ani jego konsekwencji filozoficznych, będziemy jedynie stosować matematyczne zrozumienie pojęcia stanów splątanych do tworzenia algorytmów kwantowych.*

Rys. 2 pokazuje transformatę Hadamarda dla dwóch kubitów. Jeśli rozwiązanie problemu ma być wektorem binarnym o dwóch bitach, to układ ten generuje przestrzeń wszystkich rozwiązań.



Rys. 2. Układ generujący pełną przestrzeń rozwiązań $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

W układzie tym mamy dwie bramki Hadamarda połączone równolegle, więc macierz tego układu to H ⊗ H, czyli iloczyn tensorowy bramek H.

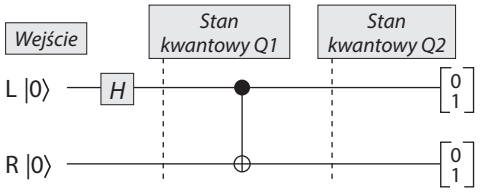
$$H \otimes H = \frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix} \otimes \frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix} = \frac{1}{2}\begin{vmatrix}1\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix} & 1\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix}\\ 1\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix} & -1\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix}\end{vmatrix} = \frac{1}{2}\begin{vmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & -1\end{vmatrix}$$

$$\text{Output} = H \otimes H \times \begin{vmatrix}1\\ 0\\ 0\\ 0\end{vmatrix} = \frac{1}{2}\begin{vmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{vmatrix} \times \begin{vmatrix}1\\ 0\\ 0\\ 0\end{vmatrix} = \frac{1}{2}\begin{vmatrix}1\\ 1\\ 1\\ 1\end{vmatrix} = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11$$

Dokonując pomiaru tego stanu kwantowego, nazwijmy go $|FULL\_SPACE\rangle$, mamy 25% szansy pomiaru każdego możliwego stanu 00, 01, 10, 11 naszej przestrzeni binarnych wektorów. Jeśli jednak jako następny operator po transformacie Hadamarda podamy układ „wyrocznię" (oracle), to sytuacja się zmienia, bo wyrocznia wyróżnia pewne stany bazowe, co zostanie wyjaśnione w następnej sekcji.

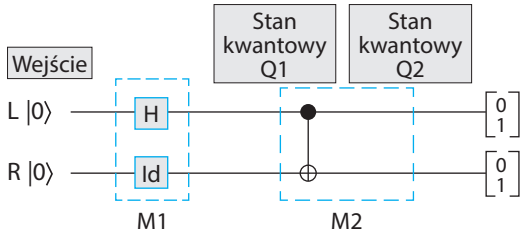
Splątanie kwantowe

Gdy rozumiemy już, jak działają superpozycja i pomiar, przeanalizujmy, jak powstaje splątanie kwantowe. Na rys. 3 widzimy układ kwantowy nazywany bramką EPR (bramką Einsteina-Podolsky'ego-Rosena). Autorzy ci chcieli udowodnić, że pewien model mechaniki kwantowej jest nonsensem, a przy okazji, myląc się, stworzyli podstawy pod komputery kwantowe. Ten układ można nazwać „ojcem komputerów kwantowych". Mamy tu dwa wejścia L i R, startujące ze stanu $|0\rangle$. H jest bramką Hadamarda, a następnie po prawej mamy znaną nam już bramkę Feynmana. Podczas gdy H generuje znaną już nam superpozycję, CNOT działając na tej superpozycji, tworzy splątanie kwantowe.



Rys. 3. Bramka Einsteina-Podolskyego-Rosena generująca proste splątanie kwantowe na wyjściu Q2

Przerysujmy układ z tego rysunku tak, aby składał się on z równoległych i szeregowych połączeń bramek, których macierze unitarne znamy lub możemy obliczyć. Symbol Id oznacza macierz jednostkową. Rys. 4 pokazuje więc układ obliczany macierzą M2*M1, gdzie M1 jest równoległym połączeniem bramki H i bramki Id, a więc macierz unitarna M1 jest iloczynem tensorowym macierzy bramki H z macierzą bramki Id.



Rys. 4. Analiza bramki EPR

Obecnie zilustrujemy obliczenia, które symulator kwantowy robi dla tego układu.

$$M1 = H \otimes I = \frac{1}{\sqrt{2}}\begin{vmatrix}1 & 1\\ 1 & -1\end{vmatrix} \otimes \begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix} = \frac{1}{\sqrt{2}}\begin{vmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{vmatrix}$$

$$Q1 = M1 \begin{vmatrix}1\\0\\0\\0\end{vmatrix} = \frac{1}{\sqrt{2}}\begin{vmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{vmatrix}\begin{vmatrix}1\\0\\0\\0\end{vmatrix} = \frac{1}{\sqrt{2}}\begin{vmatrix}1\\0\\1\\0\end{vmatrix}$$

$$Q2 = M2\ \ Q1 = \begin{vmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{vmatrix}\frac{1}{\sqrt{2}}\begin{vmatrix}1\\0\\1\\0\end{vmatrix} = \frac{1}{\sqrt{2}}\begin{vmatrix}1\\0\\0\\1\end{vmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Załóżmy, że stan początkowy $|LR\rangle = |0\rangle \otimes |0\rangle = |00\rangle$. Gdybyśmy zmierzyli separowalny stan $Q1 = (|0\rangle + |1\rangle) \otimes |0\rangle$, to otrzymalibyśmy stan 00 w 50% i stan 10 w 50%. Trakty górny i dolnypropagacji sygnału w kubitach są więc niezależne – dolny kubit zawsze jest mierzony do 0. Układ jest probablistyczny. Gdy natomiast zmierzymy stan Q2 na wyjściu bramki EPR, to otrzymamy stan 00 w 50% i stan 11 w 50%. Prawdopodobieństwo, z którym mamy do czynienia w tym przypadku, jest prawdopodobieństwem kwantowym. Jak widzimy, stany 01 i 10 nigdy nie mogą się wydarzyć. To jest właśnie wynik pomiaru stanu będącego splątaniem kwantowym.

Stany 00 i 11 są jedynymi możliwymi. Zauważmy, że z całej przestrzeni rozwiązań 00, 01, 10 i 11 nasz układ wybrał tylko dwa rozwiązania. Ponadto, nie można separować tego stanu kwantowego na część pochodzącą z górnego kubitu i oddzielną część pochodzącą z dolnego kubitu, jak było to dla stanu Q1. Stan Q2 to jest właśnie splątanie kwantowe. Zauważmy też, że gdyby oba kubity w stanie Q2 były stanami dwóch fotonów, pomiędzy którymi nastąpiło splątanie, to jeden mógłby być tu na Ziemi, a drugi na krańcu Wszechświata, ale mierząc jeden, znalibyśmy stan drugiego. Takie korelacje są podstawą najciekawszych algorytmów kwantowych.

Informacja w układzie kwantowym może być zakodowana w amplitudzie kwantowej lub w fazie kwantowej. Załóżmy, że mamy układ trzech kubitów z których dwa górne są jak na rys. 4, a pod spodem jest trzeci kubit z bramką Hadamarda. Stan wyjściowy tego układu jest

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (|0\rangle + |1\rangle) = \tfrac{1}{2}|000\rangle + \tfrac{1}{2}|001\rangle + \tfrac{1}{2}|110\rangle +$$

$$\tfrac{1}{2}|111\rangle = |Stan1\rangle$$

W wyniku pomiaru otrzymalibyśmy 000, 001, 110 lub 111, każdy wynik z prawdopodobieństwem ¼. Jest to reprezentacja rozwiązania z pomiarem amplitudy. Wyobraźmy sobie natomiast następujący stan kwantowy:

$$-|000\rangle - |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle - |110\rangle - |111\rangle = |Stan2\rangle.$$

Załóżmy, że interesują nas stany bazowe (rozwiązania), które mają fazę ujemną, czyli $|000\rangle$, $|001\rangle$, $|110\rangle$, $|111\rangle$. Gdybyśmy umieli znaleźć w tym stanie $|Stan2\rangle$ te stany bazowe, które mają ujemną fazę, to poznalibyśmy wszystkie rozwiązania. Algorytm Grovera transformuje właśnie tego typu stan $|Stan2\rangle$ do stanu = $|Stan1\rangle$. Informacja z fazy przechodzi do amplitudy. Mierzymy i znajdujemy losowo wybrane jedno z rozwiązań pozostających w superpozycji kwantowej opisanej przez $|Stan1\rangle$.

Problemy ze Spełnianiem Ograniczeń

Istnieją dwie ważne i duże klasy problemów: Problemy ze Spełnianiem Ograniczeń (PSO) (CSO – *Constraint Satisfaction Problems*) i problemy optymalizacyjne. Problemy PSO są opisywane przez zbiór ograniczeń, które rozwiązanie musi spełniać. Aby rozwiązać problem PSO, należy znaleźć wektor – rozwiązanie, który spełnia wszystkie ograniczenia. Na przykład wyznaczyć trajektorię mobilnego robota w labiryncie tak, by nie dotknął żadnej ściany. W problemach optymalizacyjnych celem jest znalezienie wektora, który optymalizuje pewną funkcję kosztu (na przykład znaleźć trajektorię robota, który przejeżdża z pokoju A do pokoju B, minimalizując energię czerpaną z baterii). Matematyczne sformułowania problemów, takich jak kolorowanie grafu czy najkrótsza droga są abstrakcjami ważnych problemów z życia, które chcemy rozwiązywać optymalnie lub prawie optymalnie. Jedną z metod rozwiązywania problemów optymalizacyjnych jest wielokrotne rozwiązywanie problemów PSO, czyli problemów decyzyjnych. W tym wariancie każdy następny problem w sekwencji problemów jest rozwiązywany z dodanymi czy zmienionymi ograniczeniami aż do znalezienia optymalnego rozwiązania.

Jako prosty przykład omówimy problem PSO – kolorowanie wierzchołków grafu. Problem ten można sformułować następująco: znaleźć takie pokolorowanie węzłów grafu *n* kolorami, żeby każde dwa węzły n_i i n_j, dla których istnieje krawędź $e_{ij} = (n_i, n_j)$, dostały różne kolory, albo udowodnić, że takie kolorowanie jest niemożliwe. Wariant optymalizacyjny tego problemu to dodatkowo jak najlepsze zminimalizowanie wartości *n*, czyli liczby użytych kolorów, zwanej liczbą chromatyczną grafu. Aby rozwiązać ten problem optymalizacyjny, możemy postępować następująco: najpierw ustalić pewną liczbę K, dla której rozwiązanie na pewno istnieje; w najgorszym przypadku jest to liczba węzłów. Z tą liczbą rozwiązujemy problem PSO, który daje nam potwierdzenie i konkretne rozwiązanie, czyli pokolorowanie. Teraz zakładamy, że graf jest kolorowalny przy użyciu K-1 kolorów i rozwiązujemy ponownie problem PSO. Jeśli znajdziemy takie pokolorowanie, powtarzamy procedurę dla K-2 kolorów itd. Jeśli natomiast nie istnieje rozwiązanie dla K-2 kolorów, wtedy wiemy, że K-1 jest liczbą chromatyczną grafu i znamy odpowiednie optymalne kolorowanie. Ta prosta metoda redukcji problemu optymalizacyjnego do ciągu problemów PSO ze zmienianymi ograniczeniami jest stosowalna do bardzo wielu problemów optymalizacyjnych. Jest ona podstawą metod opartych na „wyroczni". Metoda ta jest niezależna od technologii, w której zbudujemy naszą wyrocznię.

Co to jest wyrocznia?

Wyrocznia w klasycznych układach cyfrowych to po prostu funkcja boolowska z jednym wyjściem, która daje odpowiedz „tak" = 1, gdy wektor wartości binarnych wejść tej funkcji odpowiada rozwiązaniu problemu, oraz „nie" = 0, gdy wektor wartości wejść nie jest rozwiązaniem.

Wyrocznia może być zrealizowana jako oprogramowanie klasycznego komputera, układ FPGA czy układ w jakiejś nanotechnologii. W naszym przypadku wyrocznia będzie permutacyjnym układem kwantowym, będącym częścią algorytmu Grovera[1]. Algorytm Grovera daje kwadratowe przyspieszenie czasu realizacji programu w sensie liczby ewaluacji (wywołań) wyroczni – w porównaniu do klasycznego algorytmu poszukiwania dla problemu pełnego przeglądu, czyli takiego problemu, o którym nie ma żadnej dodatkowej informacji. Takie wyrocznie istnieją w innych algorytmach kwantowych, jak np. kwantowe chodzenie (*quantum walk*), inne metody kwantowego poszukiwania[2], kwantowe sieci neuronalne[3] czy algorytm faktoryzacji Shora[4].

Zarówno w klasycznej wyroczni, jak w algorytmach kwantowych opartych na wyroczniach, potrzebny jest pewien generator, który tworzy wszystkie potencjalne kombinacje. Kombinacje te są następnie weryfikowane przez wyrocznię jako rozwiązania lub nie są weryfikowane. W układach kwantowych jako generator przestrzeni na ogół używany jest wektor bramek Hadamarda, jedna bramka na każdą zmienną wejściową problemu – inicjalizowany do stanu kwantowego $(|0\rangle + |1\rangle)^n$. Przykładem dla przestrzeni dwukubitowej jest stan $|FULL\_SPACE\rangle$. W ogólności inicjalizacja może być również dokonana inaczej, dając pewnym stanom większe amplitudy lub fazy, a więc faworyzując je do pewnego typu transformacji lub pomiarów. Pozwala to na wyróżnienie niektórych stanów, dając im na wstępie większe prawdopodobieństwo bycia rozwiązaniem przy mniejszej liczbie iteracji pętli poszukiwania.

Jak programista kwantowy korzysta z kwantowej wyroczni?

Języki programowania kwantowego, takie jak QISKIT, QSHARP czy Quipper, są używane do projektowania, weryfikacji, symulowania i dokumentacji układów i algorytmów kwantowych. Pozwalają one użytkownikowi – który zna pokazane tu podstawy teoretyczne, a jednocześnie nauczy się metod opisu układów kwantowych w tych językach – na eksperymentowanie z różnymi wariantami

1 Polecane lektury:

Grover, L.: A fast quantum mechanical algorithm for database search, CONFERENCE 28th Annual ACM Symposium on Theory of Computing, pp. 212–219, (1996).

Grover, L.K.: Quantum Mechanics Helps in Searching for a Needle in a Haystack, Physical Rev. Letters, Vol. 78, pp. 325–328, 1997.

Grover, L.K.: Rapid sampling though quantum computing. STOC. 1998, pp. 618–626.

Grover, L.K.: Quantum Search on Structured Problems, QCQC 1998, pp. 126–139.

2 Hogg, T.: Single-Step Quantum Search Using Problem Structure, Los Alamos preprint quantph/9812049, Los Alamos Nat'l Lab, Albuquerque, N.M., 1998.

Hogg, T.: Solving Highly Constrained Search Problems with Quantum Computers, J. Artificial Intelligence Research, Vol. 10, 1999, pp. 39-66; http://www.jair.org/ abstracts/hogg99a.html

3 Kak, S.C.: Quantum neural computing. Adv. Im. And Electr. Physics, 94, pp. 259–313, 1995.

4 Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1484–1509, 1997.

poszukiwania kwantowego czy innych algorytmów, zwłaszcza w dziedzinie kwantowego uczenia maszynowego.

Porównajmy klasyczną wyrocznię z wyrocznią kwantową zbudowaną dla algorytmu Grovera. W przypadku klasycznej wyroczni musimy dawać na jej wejściu kolejno wszystkie możliwe kombinacje wartości, czyli całą przestrzeń rozwiązań, a wyrocznia odpowiada "tak" lub "nie" na każdy z podanych binarnych wektorów. Natomiast w przypadku algorytmu kwantowego przestrzeń wszystkich rozwiązań tworzona jest jako superpozycja wszystkich potencjalnych rozwiązań generowana przez wektor bramek Hadamarda . Z tej przestrzeni algorytm Grovera wybiera wszystkie rozwiązania jako wektory – argumenty funkcji boolowskiej, dla których wartość funkcji jest 1. Algorytm ten używa równoległości kwantowej (*quantum parallelism*), co oznacza, że dzięki superpozycji wyrocznia działa na wszystkich danych w sposób równoległy. Algorytm Grovera tworzy splątany stan kwantowy, który zawiera rozwiązania jako stany bazowe o zwiększonej amplitudzie.

Jednym z podejść jest uproszczona metoda, w której nowe problemy są rozwiązywane jedynie przez zaprojektowanie wyroczni z bramek odwracalnych a następnie „wstawieniu" tej wyroczni do pełnego układu kwantowego pętli Grovera w algorytmie Grovera. Zatem projektant, który nie ma głębszego zrozumienia teorii algorytmów kwantowych czy syntezy na bramkach odwracalnych, może zaprojektować taki nieoptymalny układ wyroczni, który potem może być zoptymalizowany narzędziami programowymi syntezy i layoutu. Projektant opisuje wyrocznię jako hierarchiczny układ kwantowy przy użyciu języka programowania kwantowego, a następnie analizuje jego działanie na symulatorze kwantowym czy prawdziwym uniwersalnym komputerze kwantowym. Takie podejście jest dobrym pierwszym krokiem dla studenta.

Kiedy mówimy o praktycznych problemach, takich jak kolorowanie grafu czy rozwiązywanie problemu pokrycia, to musimy pamiętać, że obecnie komputery kwantowe mogą rozwiązywać te problemy tylko dla bardzo małych rozmiarów danych.

Synteza z permutacyjnych bramek kwantowych, jak również z realizowalnych bramek kwantowych niepermutacyjnych, opisana jest w bardzo przydatnej pracy Barenco i in.[5] Pionierskie a ciągle użyteczne są publikacje Shende i in.[6] Znany algorytm syntezy funkcji rewersyjnych bez dodatkowych kubitów można znaleźć w pracy Dueck, Maslov, Miller[7]. Syntezie optymalnych bramek permutacyjnych z realizowalnych bramek nie-permutacyjnych poświęcona jest praca Hung i in.,[8] natomiast publikacja Jin i in.[9] omawia syntezę z multiplekserów kwantowych dla dowolnych bramek sterowanych.

5 Barenco, A., Bennett, C.H., Cleve, R, DiVincenzo, D.P., Margolus, N., Schor, P., Sleator, T., Smolin, J. Weinfurter, H.: Elementary Gates for Quantum Computation, Physical Rev (A), no. 52, pp. 3457–3467, March 1995.

6 Shende, V.V., Bullock, S.S., Markov, I.L.: A Practical Top-down Approach to Quantum Circuit Synthesis, Proc. Asia and South Pacific Design Automation Conference, pp. 272–275, Shanghai, China, 2005, quant-ph/0406176.

Shende, V.V., Prasad, A.K., Markov, I.L., Hayes , J.P.: Reversible Logic Circuit Synthesis, Proc. 11th IEEE/ACM Intern. Workshop on Logic Synthesis, 2002, pp. 25–130.

7 Dueck, G., Maslov, D., Miller, D.M.: A Transformation Based Algorithm for Reversible Logic Synthesis, Proc. DAC. 2003, Anaheim, CA, pp. 318–323.

8 Hung, W.N.N., Song, X.,Yang, G.,Yang, J., Perkowski, M.: Quantum Logic Synthesis by Symbolic Reachability Analysis, Proc. 41 DAC, San Diego, California, June 2004, pp. 838–841.

9 Jin, K., Saffat, T.,Morgan, J., Perkowski, M.: A Polarity-based Approach for Optimization of Multivalued Quantum Multiplexers with Arbitrary Single-qubit Target Gates. FLAP 7(1), pp. 5–28, 2020.

Literacka misja ratunkowa

Gra *Lorem Ipsum* zwyciężyła w tegorocznym, organizowanym przez PTI ogólnopolskim konkursie GEEK– Gry Eksperymentalne Edukacyjne Komputerowe (w kategorii implementacja gry na poziomie szkół średnich). Wykreowany przez uczniów z Zakopanego unikatowy, złożony i przemyślany świat ma ogromny potencjał do dalszego rozwoju oraz rozbudowy.

Lorem Ipsum wprost skrzy się pomysłami, jak tchnąć nieco współczesnego ducha w świat klasyków literatury. Gra została osadzona w mitycznej Krainie Pisarzy, nad którą wisi widmo straszliwej klątwy, zwiastującej nadejście końca wszelkiej literatury. W wersji demo fabułę osnuto wokół II cz. „Dziadów", bo już sama atmosfera utworu zapewniała odpowiedni poziom tajemniczości.

Gracz wciela się w Adama Mickiewicza, ale możliwe jest odblokowywanie postaci innych pisarzy. Imponuje mnóstwo pomysłowych artefaktów – **Wieczne pióro** pozwala poecie wejść do świata swojego utworu, by odkryć tajemnicę skażenia **Fontanny Weny**, w której napełniają swoje kałamarze wszyscy mieszkańcy Krainy Pisarzy. Skażenie pozbawiło mieszkańców ich głównego źródła energii twórczej, przez co utracili zdolność wykorzystywania swego unikatowego **Warsztatu Pisarza**. Nawet nazwy narzędzi świadczą o erudycji autorów gry: **Wietrzna istota** pozwala na wzmocnienie wybicia, **Skrzydła młodości** umożliwiają podwójny skok, a **Czarna polewka** to tryb furii.

Aż kipi od pomysłów

Postęp w grze to nie zwykłe przemierzanie kolejnych kart wybranego utworu, ale odkrywanie niedostępnych wcześniej miejsc, sekretów czy wątków. Cytaty i materiały dotyczące twórczości pisarza są subtelnie wplecione w fabułę. Wykreowano imponujący świat fantasy z jego nieodłącznymi elementami sekretów i tajemnic aż do finałowej walki z przyczyną wszelkiego Zła.

Celem jest uratowanie Krainy Pisarzy, a przez to twórczości i literatury w ogóle. Stąd przewrotna nazwa gry (Lorem Ipsum to obecnie standardowy tekst, pochodzący z klasycznej łaciny, wzorowany na traktacie Cycerona „O granicach dobra i zła", używany do demonstracji krojów czcionek, kompozycji kolumny przy składzie tekstów). Tytuł ma – w założeniu autorów gry – symbolizować postępujące niezrozumienie treści utworów we współczesnym świecie i zerwanie więzi pomiędzy twórcą a odbiorcą – litery zostają obdarte z treści, stając się jedynie bezbarwną formą, tak jak to się stało z traktatem Cycerona.

Gracz ma oryginalnego sprzymierzeńca w postaci **E-booczka**, współczesnego mola książkowego. – *Chcieliśmy w ten sposób pokazać, że świat literatury nie jest przeciwieństwem świata technologii, a ekran może być tak samo wartościowym*

źródłem wiedzy jak papier. Kraina Pisarzy może dostosować się do zmieniających się czasów, a E-booczek będzie idealnym symbolem tej możliwej do uzyskania harmonii – mówią członkowie nagrodzonego zespołu.

Sympatycznym pomysłem są **Pocztówki z Litwy**, rozsiane po różnych etapach gry, które odblokowują nie tylko kolejne wspomnienia z życia pisarza, lecz przywracają również część utraconego zdrowia. To tylko jeden z przykładów poczucia humoru autorów gry i sprawnego poruszania się w świecie literatury.

– Na potrzeby wersji demo stworzyliśmy dwa poziomy gry. Pierwszy to swoisty samouczek wprowadzający do historii i pozwalający zapoznać się z podstawową mechaniką gry. Drugi to początkowy etap ze świata „Dziadów", gdzie za zadanie mamy odnaleźć Guślarza, a w międzyczasie pomóc napotkanym duszyczkom – Józiowi i Rózi. Zależało nam na stworzeniu możliwie jak najbardziej zróżnicowanych i dopracowanych poziomów, pozwalających wykorzystać choć namiastkę naszych licznych pomysłów, techniki czy opracowanych systemów – mówi Adrian Zając, opiekun nagrodzonego zespołu i nauczyciel informatyki w Zespole Szkół Hotelarsko-Turystycznych w Zakopanem.

Nieprawdopodobna grafika gry

Warta podkreślenia jest niezwykle dojrzała oprawa graficzna gry. Nie tylko konsekwentnie nawiązująca do skojarzeń z pisarstwem (pożółkłe pergaminy, plamy po atramencie, pióra), lecz także imponująca mistrzowskim operowaniem światłem, dodającym atmosfery tajemniczości wszystkim planom.

Czujemy mrok lasu, zwodniczość jaskiń rozświetlonych blaskiem kryształów, grozę zjaw na ogarniętym burzą cmentarzu (można go rozświetlić – kolejny smaczek – jedynie **Anielskim promykiem** otrzymanym od Józia i Rózi). Zespół przeanalizował mnóstwo grafik, żeby ostatecznie stworzyć bazę ponad 250 elementów dekorujących grę. W czasie długotrwałego procesu projektowania gry powstała bardzo duża liczba grafik koncepcyjnych, szkiców, a nawet scenorysów z pomysłami na przerywniki filmowe, które nie zmieściły się w wersji demo. Część z nich jest prezentowana w galerii odblokowywanej po przejściu gry.

Zadbano też o atrakcyjną ścieżkę dźwiękową, odpowiednią do atmosfery gry. Każdej akcji, animacji czy zdarzeniu towarzyszą odpowiednio dobrane efekty dźwiękowe.

Przygoda i nauka

Proces przygotowania konkursowej wersji demo był niezwykle pracochłonny, bo uczniowie nie mieli żadnego doświadczenia, a potrzebną wiedzę gromadzili metodą żmudnych prób. Pasja i kreatywność całego zespołu sprawiły, że efekt przerósł oczekiwania.

– Wykorzystaliśmy wiele poznanych w trakcie prac technik, jak np. paralaksa dalszych planów, efekty cząsteczkowe (choćby spadające liście, dynamiczny deszcz czy smuga pikseli, którą pozostawia E-booczek), fizyka obiektów (np. dające się zniszczyć lampy na łańcuchach), dynamiczne oświetlenie (np. pioruny), czy promienie świetlne, wykrywanie i śledzenie postaci (system ataku przeciwników i poruszanie się E-booczka) – mówi z dumą Adrian Zając.

Zgodnie z regulaminem konkursu, członkowie zespołu oraz zespół jako całość zachowują prawa autorskie i majątkowe do całej pracy i związanych z nią materiałów i programów. Zachęcamy do komercyjnego zainteresowania się *Lorem Ipsum* – to solidna i przemyślana podstawa oraz baza pomysłów, mechanik i grafik pod projekt kompletnej gry.

Gra *Lorem Ipsum* została przygotowana przez zespół Yacoper Inc. z Zespołu Szkół Hotelarsko-Turystycznych w Zakopanem, złożony z uczniów: Daniel Pawlikowski, Jan Świder, Dominik Możdżeń, Angelika Ciołek i Jordan Jira. Opiekunem zespołu był nauczyciel informatyki – Adrian Zając.

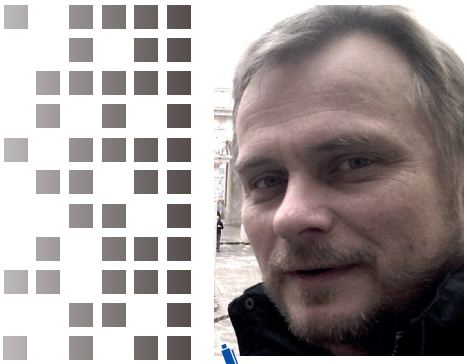
Spory fragment demo gry *Lorem Ipsum* jest dostępny pod adresem:
https://www.youtube.com/watch?v=Lgt9TKtZ6Wo

O certyfikacji subiektywnie

Z dziką rozkoszą, odrywając się od gorsetu formalizmów i powagi, postanowiłem podzielić się kilkoma obserwacjami dotyczącymi certyfikacji jako takiej. Obserwacjami, które na tyle mnie zaintrygowały, że chciałem je początkowo opatrzyć parafrazą tytułu sztuki Edwarda Albee'go: „Kto się boi certyfikacji?".

Niestety, podobnie jak w dramacie Albee'go, w którym młode małżeństwo z przerażeniem obserwuje swoją metamorfozę, tak i ja skonstatowałem ze smutkiem, że również uległem przemianie i należę do grona tych, którzy obawiają się certyfikacji.

Szok i niedowierzanie. Chwila osłupienia i postanowiłem swój strach zracjonalizować. Bez przekonania, ale jednak uznałem, że moje obawy to tylko przejaw empatii w rodzaju tej, jaką odczuwa lekarz w stosunku do chorego. Uspokojony, postanowiłem doprecyzować diagnozę i rozważyć właściwą kurację.



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

Wszyscy za…

Można zaryzykować twierdzenie, że zasadność potrzeby wdrażania procesów certyfikacji wydaje się być bezdyskusyjna i powszechnie uznana. Tak więc **deklaratywnie** większość pożąda certyfikacji w takim samym stopniu, jak deklaratywnie chciałaby, aby osoby wykonujące dla nas dowolne usługi posiadały odpowiednie kompetencje. Najlepiej, aby te kompetencje zostały zweryfikowane przez **niezależny podmiot**. Lekarze specjaliści powinni zostać sprawdzeni w Centrach Egzaminów Medycznych, a osoby chcące prowadzić działalność gospodarczą w zakresie transportu drogowego powinni uzyskać certyfikat kompetencji zawodowych Instytutu Transportu Samochodowego.

> *Innymi słowy chcemy, aby wiedza, umiejętności i kompetencje społeczne osób, które wprost lub pośrednio realizują dla nas jakieś usługi, były potwierdzone przez ekspertów w danej dziedzinie.*

Takie instytucje w każdej branży potwierdzają, czy dana osoba uzyskała odpowiednie efekty uczenia się. Oceniają to w procesie walidacji – zgodnie z określonymi kryteriami i zasadami zapewniania jakości. **Uwieńczeniem tego procesu jest uzyskanie certyfikatu**.

Walidacja nasza powszechna

Również w sferze codziennych działań nieformalnych stykamy się z procesem walidacji, przykładowo gdy znajomi remontują łazienkę. Ich zadowolenie z rezultatu oznacza zakończenie procesu walidacji z sukcesem mierzonym zgodnością efektu z deklarowaną wiedzą, umiejętnościami i kompetencjami społecznymi wynajętych fachowców, którym wydają swego rodzaju wirtualny certyfikat w postaci rekomendacji. Łazienka nadaje się do użytku i spełnia wyspecyfikowane oczekiwania zgodnie z projektem. W powyższym przykładzie mamy de facto do czynienia z jedną z formalnych metod walidacji – „analizą dowodów i deklaracji".

Przy czym dowody i deklaracje powinny być:
- dobrane odpowiednio do efektów uczenia się, które mają potwierdzać;
- autentyczne;
- wystarczające;
- aktualne.

Niczym molierowski pan Jourdain, który dowiaduje się, że całe swe życie mówi prozą, i my na co dzień nieświadomie **jesteśmy zamieszani w procesy walidacyjne**, a w przytoczonym przypadku remontu łazienki – w analizę dowodów i certyfikację.

Nie rób bliźniemu…

Brak nam świadomości powszechności i wagi procesów certyfikacji. Jeśli ktoś jakiś certyfikat posiada, cieszy się uznaniem. No właśnie ktoś – nie my. Bo jeśli o nas chodzi, to twierdzę, że zarówno w wymiarze osobistym, jak zawodowym – pojawia się strach.

Bo jak inaczej wytłumaczyć niechęć Polaków do uczenia się przez całe życie (lifelong learning), rozumianego jako uczenie się w różnych formach i miejscach (w kontekście formalnym, pozaformalnym i nieformalnym) oraz na wszystkich etapach życia?

Stawiam tezę, że przyczyną jest strach wyniesiony ze szkoły, uczelni i miejsca pracy, w których domyślnym celem przeprowadzenia egzaminu czy testu jest wykazanie niewiedzy egzaminowanego, a nie wskazanie kierunków dalszego rozwoju.

Jak wiemy, strach jest zaraźliwy. Boją się nie tylko uczniowie, studenci, lecz także pracownicy, w tym urzędnicy. Przenoszą swój strach, często nieuświadomiony, na swoje życie zawodowe. Jeśli tylko mogą, to również nieświadomie, niejako z dobrego serca, starają się usunąć z horyzontu zagrożenie dla bliźnich, rugując z programów szkoleniowych finansowanych ze środków publicznych wszelkie formy wspierające zapewnienie jakości, w tym – niestety – również obowiązek przeprowadzenia egzaminu zewnętrznego zakończonego certyfikacją rozumianą jako egzamin. Źródło stresu i poniżenia. Wszak może być przyjemnie. Zamiast egzaminu – lista obecności, zamiast certyfikatu – dyplom uczestnictwa, zamiast wiedzy – kawa i lunch.

Mówi się, że dobrymi chęciami piekło jest wybrukowane.

Cena strachu

Zaraźliwy strach sprawił, że zarówno w projekcie Programu Fundusze Europejskie dla Rozwoju Społecznego na lata 2021–2027, jak i w Krajowym Planie Odbudowy zabrakło rekomendacji, aby wszystkie szkolenia lub ich zdecydowana większość – niezależnie jakiego typu i jakiego poziomu kompetencji cyfrowych dotyczą – kończyły się egzaminem zewnętrznym. Nie chcemy wiarygodnego miernika skuteczności szkoleń mimo, że dałby podstawę do doskonalenia szkoleń i wdrażania korekt.

Po raz kolejny jako mierniki mają służyć listy obecności i wewnętrzne egzaminy, które trudno uznać za mierniki jakościowe.

Pomimo milionowych nakładów na podnoszenie kompetencji cyfrowych w poprzednich perspektywach finansowych, nie widać w tym obszarze znaczącej poprawy (patrz indeks DESI). Dotychczasowe doświadczenia wskazują, że zarówno niska jakość szkoleń, jak i ich niedopasowanie do potrzeb w istotnym stopniu wynikały z braku wskaźników oceny szkoleń, a przede wszystkim braku jakościowej oceny ich skuteczności, którą jest w stanie zapewnić tylko wiarygodna certyfikacja.

Czy wiemy, jak certyfikować poprawnie? Czy wiemy, jakie warunki muszą być spełnione, aby proces walidacji był wiarygodny, a uzyskany certyfikat potwierdzał nabytą wiedzę?

Moim zdaniem, tak. Wiemy to dzięki koncepcji tzw. kwalifikacji rynkowych rozwijanego od wielu lat Zintegrowanego Systemu Kwalifikacji, które z powodzeniem mogą w przyszłości pełnić funkcję praktycznego łącznika rynku z edukacją. Ich metodyka i praktyka wpisują się w deklarowaną w programach wolę wspierania rozwoju kompetencji cyfrowych. Wiemy to też dzięki wieloletnim doświadczeniom ECDL/ICDL (European Computer Driving Licence / International Computer Driving Licence) w wymiarze nie tylko krajowym i europejskim, lecz także światowym.

Certyfikacja ECDL istnieje od 1997 r. i od tego czasu przeszła bardzo wiele zmian i istotnie się rozwinęła. Z certyfikacji europejskiej stała się certyfikacją światową – jako ICDL (International Computing Driving Licence albo International Certification of Digital Literacy). Pojawiły się nowe moduły z obszaru IoT, Cloud Computing, AI, VR, AR, 3D, blockchain oraz cyberbezpieczeństwa. Podobnie jak i przemyślane sylabusy – często powiązane z dobrze zdefiniowanym e-learningiem – czekają, aby stać się bazą dla niezbędnego powszechnego transferu i weryfikacji wiedzy.

To Polskie Towarzystwo Informatyczne, jako członek CEPIS-u, podjęło inicjatywę rozpropagowania idei i wdrożenia Europejskiego Certyfikatu Umiejętności Komputerowych w Polsce. Uwieńczeniem tego procesu było powstanie w 1997 r. Polskiego Biura ECDL, które do dziś odpowiada za koordynację prac, obsługę informacyjną systemu wydawania certyfikatów ECDL i nadzór nad rzetelnością przeprowadzania egzaminów.

Dobrej jakości certyfikacja na każdym poziomie nie tylko oswaja i przybliża technologię, lecz również zachęca do rozwoju. Każdy z certyfikatów wiarygodnie potwierdzających, że efekty uczenia się zostały osiągnięte, jest dla egzaminowanego osobistym kamieniem milowym i kierunkowskazem. Wskazówką do szukania swojej indywidulanej ścieżki, tak jak to się dzieje w przypadku ECDL/ICDL Profile. To twardy grunt, od którego można się odbić i śmiało kroczyć z poczuciem sukcesu. Indywidualnego sukcesu, którym może być zarówno obsługa edytora tekstu na poziomie podstawowym, jak i druk 3D z granulatu tytanowego. To sukcesy różnych ludzi, z różną osobistą historią.

Pamiętajmy: brak certyfikacji to jak przeprowadzenie audytu przez samego siebie!

Lumenalna elektroniczna mechaneurystyka

Nie wiem, czy ktokolwiek z nas, informatyków, zgodzi się ze mną, ale uważam, że Lem dla pewnej części był i – dłużej lub krócej – będzie punktem odniesienia, inspiracją, źródłem wiedzy i wzorem postrzegania świata, radzenia sobie z nim i z naszą profesją.

Janusz Dorożyński
adiunkt badawczo-dydaktyczny Instytutu Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Absolwent Moskiewskiego Instytutu Subtelnej Technologii Chemicznej im. Łomonosowa (obecnie część Moskiewskiego Uniwersytetu Technologicznego). W 1984 r. na tej uczelni uzyskał stopień doktora nauk technicznych. W pracy zawodowej do 2017 r. związany z przemysłem informatycznym. Członek PTI od 1985 r.

Dla tej części informatyków, którzy nie są tylko dokładnymi, precyzyjnymi, zorientowanymi na cel istotami tworzącymi programy, budującymi systemy czy zarządzającymi nimi. Tej części, na którą składają się nie tylko ci mędrcy od oka i szkiełka, lecz ludzie, w których ich suchej, nudnej, dokładnej naturze matematycznej towarzyszy czasami czuły, czasami postrzelony, nawet niekiedy gwałtowny, ale wrażliwy, łatwy do zranienia pierwiastek humanistyczny. Albo, jeśli ktoś woli, towarzyszy romantyzm czy wręcz sentymentalizm lub, jak ma się odwagę tak powiedzieć – czułość. I – last but not least – którym jak najbardziej nieobce jest poczucie dystansu do siebie i poczucie humoru – subtelnego, często paradoksalnego, lemowskiego.

Jest tak dlatego, że niewątpliwie informatyka to nie tylko sprzęt, to nie tylko programy, nie tylko bity, bajty, słowa, rejestry i adresy. Nie zawaham się powiedzieć, że to wszystko to tylko dodatek, gadżet. Inny niż cokolwiek dotychczas, nowy, zajmujący, ale tylko dodatek dla nas – tym razem mam na myśli nas jako ludzi ogólnie, istot obdarzonych zdolnością abstrakcyjnego myślenia w interakcji z uczuciami. Tak, dodatek DLA nas. Dopóki pozostaniemy ludźmi.

Takie spojrzenie z pewnego punktu widzenia – tym razem nas, którzy jesteśmy bardziej niż inni biegli w obsłudze i produkowaniu tych dodatków – jest pełne pokory. Umiejętność takiego podejścia, wręcz pogodzenia się z nim, jest dla mnie kamieniem probierczym naszej, informatyków, odpowiedzialności wspólnotowej jako ludzi. A takiego podejścia nauczyły mnie dzieła Lema. Jego spuścizna jest różnorodna. Począwszy od utworów współczesnych, poprzez dzieła humorystyczne osadzone w fantastycznych dekoracjach, powieści stricte fantastyczno-naukowe, w tym mocno informatyczne, a skończywszy na publicystyce oraz na obszernych pracach i rozprawach społecznych, politycznych, filozoficznych i naukowych.

Wspomniane dzieła ściśle fantastyczno-naukowe po części nazwałem informatycznymi. Faktycznie mocno były związane z techniką i z obszarem działalności ludzkiej początkowo nazywanej cybernetyką, a teraz swojsko informatyką. Sporo tych dzieł może nie zadowalać, a często nie zadowala młodszych czytelników brakiem fajerwerków, razi prostotą pomysłów, zwłaszcza technicznych. Ale to nie ma znaczenia. Informatyka, jeśli pominąć błyskotki w postaci gier i wbudowane w komórki quasi aparaty fotograficzne, też jest mało widowiskowa, nudna i żmudna. Więc jeśli nawet we wspomnianych dziełach nie było feerii pomysłów technicznych, to technika była, i była tak czy inaczej informatyka, ale przede wszystkim byli ludzie. Do nich wrócę, bo przez chwilę zatrzymam się nad tym, czy faktycznie utwory Lema są o informatyce. Pomijając już to, że kwestia informacji i jej przetwarzania przewijała się w wielu dziełach (przede wszystkim w „Dialogach", a także jako mechanoeurystyka[1] i termodynamika logiki[2] w „Obłokach Magellana"), to dla mnie utworami o informatyce, też o informatyce, są zarówno „Niezwyciężony", jak i „Solaris" i – to już trywialne stwierdzenie – „Golem XIV". W pewnym sensie takim utworem jest „Głos Pana".

1 Eufemistycznie: cybernetyka, z której wyrosła informatyka.

2 Równie aluzyjnie: teoria informacji.

Pierwszy utwór może nie jest oczywisty, jak niby nie są oczywiście informatyczne elementy Y. Tyle że te elementy składają się co jakiś czas w zaprogramowaną, mającą cel działania chmurę, a same przez swoją trójwartościowość (trójkończowość) jakoś dziwnie przypominają pomysł najbardziej oszczędnego zapisu liczb, bo w systemie z podstawą e. Z kolei planetarny twór też jest nie wiadomo czym, ale działa w sposób celowy, więc może być biotycznym, globalnym komputerem. A w ostatnim przypadku, choć tylko jako pretekst do prowadzenia narracji, jest aluzja do jakże informatycznego i informatyce potrzebnego generowania liczb losowych. Ale co ważniejsze – we wszystkich utworach są ludzie, również w „Golemie". Ludzie zderzani z niewiadomym w jakiejś przyszłości, uzbrojeni w rozwinięte rozwiązania techniczne, bo tak będzie, nieważne, czy i ile Lem nawymyślał takich rozwiązań. Ale są to ludzie i to jest clou lemowskiego przesłania do mnie, którzy praktycznie się nie zmieniają. Nie zmieniają się bez względu na to, co ich w sensie gadżetów otacza, z czego korzystają, co im ułatwia byt, przemieszczanie, komunikowanie się. Nie tylko z gwiazd przynoszą swoje ja, swoje słabości, radości i ułomności, ale z tym samym udają się do gwiazd. I nie ma możliwości, aby od tego uciekli. Nawet w kosmos. I tak samo jest w kontekście interakcji ludzi z informatyką. I dlatego to uczy pokory. Pozwala zatrzymać percepcję, lub do niej wrócić, na tych, co nas otaczają.

Ilustracja na podstawie: https://lubimyczytac.pl/wizjoner-autor-arcydziel-wielki-pisarz-sf-stanislaw-lem-czy-dzis-jeszcze-o-nim-pamietamy

Jest pewne, że dzieła Lema można odczytać jeszcze na inne sposoby. Można się zachwycać choćby jego zabawami z językiem albo ciętymi alegoriami polityczno-społecznymi. To tylko potwierdzi wielkość jego twórczości. Nawet jeśli będzie budziła odczucia, które by go dziwiły, czy przeciw którym protestował, jak rozumienie „Solaris" przez Tarkowskiego, któremu w pasji powiedział „wy durak".

Dla mnie Lem był erudytą, humanistą, wizjonerem, który pojmował i uczył się cywilizacyjnych rzeczy nowych, potrafił je objaśniać i najczęściej trafnie wskazywał kierunki ich rozwoju. Tak czy inaczej twierdził, że współczesne społeczeństwo przekształca w społeczeństwo informacyjne. Sam nie tworzył nic informatycznego, ale rozumiał ten obszar działalności, i wskazywał, jaki jest jego właściwy wymiar. Ze znakomitymi memento – utworami „Bomba megabitowa" i „Profesor Dońda". Wspomniana umiejętność uczenia się znakomicie koreluje z pewnym stwierdzeniem, z którym zresztą zgadzam się – prawdziwym informatykiem jest ten, kto potrafi się uczyć.

Z tego też powodu, ale przede wszystkim z wymienionych wcześniej był – dla mnie, i może nie tylko dla mnie – honorowym, społecznym, humanistycznym informatykiem, jak najbardziej godnym, aby być honorowym członkiem naszego towarzystwa. Nawet jeśli PTI nie zaznaczyło jego odejścia choćby zdawkowym, oficjalnym czy lakonicznym pożegnaniem – czego żałuję.

To, że byłem obok niego w czasie, jest wielką rzeczą, jest nieocenionym podarunkiem od losu. Jest, bo tak wiele pozostawił. Mnie. I nam informatykom – którzy myślą podobnie jak On, Świet(l)ny Informatyk.

29 marca 2006 r.

Powyższe słowa, napisane w emocji i z wielkiej mojej atencji do twórcy, który właśnie wtedy odszedł na zawsze, po piętnastu latach nie wymagają odjęcia czegokolwiek. Łącznie z passusem o quasi aparatach fotograficznych – wtedy było to uprawnione. A dodania – oczywiście tak. Jak chociażby tego, co jego, arcypolskiego pisarza, łączyło z innym arcypolskim, choć z innych obszarów literackich – Igorem Newerlym. Gdyż zarówno utwory, jak i życie Lema, to szkatułkowe misterne konstrukcje, zawierające niekiedy nieznane (do czasu) również wcielenia pisarza. Szkatułki, do których kluczyki chował, wyrzucał czy gubił. Nam pozostawił możliwość odnajdywania tropów, w przypadku dzieł – interpretacji. A wielość interpretacji każdego dzieła, również nawet nieuświadamianych sobie przez twórcę, w opozycji do próby formułowania jednej słusznej, świadczy o wybitności tegoż dzieła.

Z perspektywy wspomnianego czasu, który nieubłaganie upłynął, i percepcji otaczającego nas świata, niewątpliwie interpretacje nawet wydawałoby się drobnych utworów rodzą się nowe czy nieoczekiwane. Taką pewnie jedną z wielu jest skojarzenie dwóch rozdziałów Wielkości urojonej o Ekspelopedii Vestranda z Wikipedią. Oczywiście dotyczy to tylko jednej cechy tej wyimaginowanej encyklopedii – możliwości ciągłego, praktycznie natychmiastowego utrzymywania haseł w aktualności, choć w odróżnieniu od Ekstelopedii – praktycznie bezkosztowego i ponadto bez nośnika indywidualnego. Niewątpliwie sam Lem opisując Ekstelopię nie mógł wyimaginować sobie Wikipedii, ale jednocześnie wskazał potrzebę oczekiwaną wobec zbioru będącego sumą wiedzy, zwłaszcza sumą wiedzy ludzkości, jaką deklaruje się być Wikipedia. Jednocześnie takie skojarzenie nie było oczywiste, nawet dla piszącego te słowa – wtedy. Pomimo tego, że Wikipedia już istniała – od 2001 r., i że byłem aktywnym wikipedianinem. Uświadomiłem to sobie z czasem, i takie stwierdzenie oznajmione na konferencji rosyjskiej wikipedii w Kostromie w 2015 r. było przyjęte jako oczywiste.

Niewątpliwie przed nami wiele nowych, podobnych tropów do szkatułek Lema.

Janusz Dorożyński, wikipedianin Ency
8 grudnia 2021 r.

Ryszard Tadeusiewicz

Archipelag sztucznej inteligencji

Akademicka Oficyna Wydawnicza Exit
Warszawa 2021

Prof. dr hab. inż. Ryszard Tadeusiewicz, profesor zwyczajny w krakowskiej AGH (trzykrotny rektor tej uczelni) i członek honorowy PTI, jako autor i współautor ma w swoim dorobku nie tylko setki publikacji naukowych, lecz także wielkie osiągnięcia w popularyzacji nauki i techniki w czasopismach, radiu i telewizji oraz internetowych kanałach multimedialnych. Działalność popularyzatorska rozciąga się na wszystkie dziedziny zainteresowań Profesora – od informatyki, automatyki i robotyki, przez inżynierię biomedyczną po sieci neuronowe i sztuczną inteligencję. Od lat zagadnienia te prezentuje także młodzieży. Wśród (średniego już) pokolenia informatyków na pewno można znaleźć takich, którzy w latach 70. i 80. XX w. zaczynali swoją informatyczną karierę od skryptów uczelnianych krakowskich uczelni na temat języków programowania (PLAN, Fortran, Algol, PL/1), a wcześniej np. od przewodników po oprogramowaniu komputerów domowych (np. „AtariWriter Plus" z popularnej serii PPP miniksiążeczek WNT) czy książek dla młodocianych adeptów informatyki („Atari Logo – Komputerowe przygody" z 1991 r.).

W nurcie publikacji dla młodzieży jest też prezentowany „Archipelag sztucznej inteligencji". Jak pisze autor w jednej z jej zapowiedzi, wiele osób zajmujących się od lat zagadnieniami sztucznej inteligencji zbliża się do kresu działalności zawodowej. Dla podtrzymania sztafety pokoleń konieczne jest zainteresowanie tą problematyką młodzieży ze szkół średnich. To właśnie do nich kieruje swoją książkę, zakładając, że to właśnie od ich zainteresowania problemami sztucznej inteligencji i przygotowaniem do studiów w tym zakresie zależeć będzie miejsce Polski w świecie w najbliższej przyszłości. Dlatego treść publikacji podzielona jest na krótkie „pigułki wiedzy" dostosowane do sposobu percepcji dzisiejszej młodzieży, zawiera też dużo materiału ilustrującego poglądowo omawiane zagadnienia.

Całość omawiana jest w układzie oddzielnych wysp–zagadnień, tworzących tytułowy archipelag wiedzy o sztucznej inteligencji. Na poszczególnych wyspach są sieci neuronowe, zbiory rozmyte i przybliżone, rozpoznawanie obrazów, analiza skupień, algorytmy generyczne i uczące się drzewa decyzyjne. Jako ciekawe przykłady tzw. inteligencji roju służą króciutkie omówienia algorytmów mrówkowych, stosowanych np. w szukaniu najkorzystniejszej ścieżki w grafie. Jest też przegląd historii programów grających w gry strategiczne – od programu, który już w 1954 r. pokonał w warcabach czwartego gracza w amerykańskim rankingu przez przełomowy dla programów szachowych 1997 r., kiedy to Deep Blue pokonał ówczesnego szachowego mistrza świata Garriego Kasparowa, po lata 2015–2017, kiedy kolejne programy AlphaGo/AlphaZero pokonały europejskich i światowych arcymistrzów gry Go – choć jeszcze kilkanaście lat wcześniej wydawało się, że z uwagi na złożoność tej gry takiego programu wręcz nie da się napisać.

Na ostatniej wyspie archipelagu mowa jest o przetwarzaniu języka naturalnego. Autor zwraca młodym czytelnikom uwagę, że programy z tej dziedziny są nie tylko silnikami chatbotów czy voicebotów i systemów tłumaczenia tekstów, ale służą także do porządkowania zbiorów tekstów i ustalania związków między nimi oraz do automatycznego tworzenia streszczeń i wyszukiwania wątków w wielkich zbiorach dokumentów. Można mieć nadzieję, że niepozorna graficznie okładka nie przeszkodzi młodym czytelnikom w odnalezieniu tej cennej dla nich książki na półkach księgarni realnych czy internetowych.

tmk

PREZESI ZAPRASZAJĄ...

CYKL WEBINARÓW
O INFORMATYCE ORAZ STYKU TECHNOLOGII I PRAWA

PRZYGOTOWANY PRZEZ
POLSKIE TOWARZYSTWO INFORMATYCZNE
ORAZ ZWIĄZEK CYFROWA POLSKA

SPRAWDŹ KOLEJNE SPOTKANIA:
https://sdsi.pl/webinaria

CYFROWA POLSKA

40 PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE