POLSKIE TOWARZYSTWO INFORMATYCZNE

NUMER 4/2023

PRZYSZŁOŚĆ ZACZYNA SIĘ DZISIAJ

Domena

ISSN 2720-6513

Cyber-stan

Teresa Wierzbowska
O walce z pirackim rynkiem telewizyjnym

Hakowanie ciała

Wielkie małe kropki

EMULATORY, SYMULATORY I KLONY

Spis treści

PTI Domena

nr 4/2023

Wydawca:
Polskie Towarzystwo Informatyczne

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

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

Rada Programowa „Domeny”:
Wiesław Paluszyński
– przewodniczący Rady
Marek Bolanowski
Marian Bubak
Beata Chodacka
Bogusław Dębski
Wojciech Kiedrowski

Współpraca redakcyjna:
Tomasz Kulisiewicz

Korekta:
Jolanta Jamiołkowska

Skład i opracowanie graficzne:
Agencja HEADOUT

Headout

Szanowni Państwo,

każdy Nowy Rok nierozerwalnie kojarzy się z nadzieją. Gdy kończy się stary, zaciskamy z całych sił powieki i przekonujemy siebie i bliskich, którym życzymy pomyślności – to na pewno będzie dobry rok! Późniejsza rzeczywistość na ogół dość brutalnie obchodzi się z naszymi zaklęciami losu. Część filozofów uważa, że właściwa nadzieja zaczyna się tam, gdzie wkracza zło, które podcina skrzydła nie tylko naszym oczekiwaniom, lecz i nam samym. Niekiedy po prostu trzeba tak długo czekać na lepszy czas, że większość z nas traci nadzieję. Ale warto się jej trzymać, żeby móc w pełni przeżyć to, co właśnie staje się naszym udziałem. Za progiem rok 2024, który nad Wisłą ma szansę być niczym świeży powiew wpuszczony do zatęchłych pomieszczeń.

W zamierzchłym czasach, na rok przed moją maturą, Nagrodę Nobla w dziedzinie literatury dostał chilijski poeta Pablo Neruda, wielki wizjoner rewolucyjnych idei społecznych i politycznych, który mawiał: możesz ściąć wszystkie kwiaty, ale nie możesz powstrzymać wiosny przed nadejściem. Życzę wszystkim Czytelnikom „Domeny", żeby doświadczyli tej wiosny w sercach i żebyśmy wszyscy umieli ją spożytkować, budując lepszą Polskę.

Lepsza Polska to także kraj lepiej przygotowany na wyzwania cywilizacyjne. Publikowany w tym numerze artykuł Tomasza Kulisiewicza „Jak rosła branża" uzmysławia nam, jak bardzo od rozsądnych decyzji gospodarczych zależy kondycja sektora IT. Nic więc dziwnego, że wiąże on ze zmianą władzy nadzieje na lepszy rozwój.

Nadzieja jest paliwem nowych technologii nie tylko w Polsce. Zawirowania wokół OpenAI i pełen iście filmowych suspensów spór Sama Altmana z zarządem firmy, jakich byliśmy świadkami jakiś czas temu, to dowód nadziei na ulepszenie świata (jak twierdzą idealiści) lub spieniężenie przewagi technologicznej (wg realistów). Impulsem był program Q-Star, rzekomo zdolny do samodzielnego rozwiązywania problemów matematycznych, uważany – być może na wyrost – za reprezentanta tzw. silnej sztucznej inteligencji.

Na razie obawy, że sztuczna inteligencja wygeneruje rzesze bezrobotnych nieco zmalały, polecam tekst Andrzeja Gontarza „Sztuczna inteligencja potrzebuje ludzi". Z ciekawostek – potrzebuje także do trenowania swoich danych… poetów, zwłaszcza nieangielskojęzycznych, żeby wznieść się ponad poziom rymów częstochowskich. Przed nami jeszcze wiele zaskoczeń, oby równie przyjemnych jak translacja symbolu ośmiu gwiazdek na: udało się.

Wszystkiego dobrego w Nowym Roku!

Anna Kniaź
redaktor naczelna

Cyber-stan

Mamy nowy rząd, w wielu resortach zapowiadane są audyty. Jako certyfikowany audytor systemów informatycznych zalecam zbadanie wielu obszarów dotyczących cywilnego cyberbezpieczeństwa.

Joanna Karczewska

absolwentka Wydziału Elektroniki PW z ponad 40-letnim doświadczeniem w informatyce. Jako certyfikowany audytor systemów informatycznych – CISA – specjalizuje się w audytach informatycznych w jednostkach sektora finansów publicznych. Pełni także rolę inspektora ochrony danych w placówkach oświatowych. Jako Expert Reviewer uczestniczyła w opracowaniu metodyk COBIT5 i COBIT 2019, ITAF 4th Edition oraz publikacji ISACA dotyczących Digital Trust Ecosystem Framework. Bierze udział w konsultacjach aktów prawnych dotyczącychbezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych osobowych, również na forum Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP. Uznana w 2022 roku za jedną z Europe's Top Cyber Women. Ekspert Najwyższej Izby Kontroli.

Po wielu latach starań i ośmiu podejściach w dniu 22 października 2019 r. Rada Ministrów przyjęła Strategię Cyberbezpieczeństwa RP na lata 2019–2024.

Strategia na papierze

Przypomnę główny cel: *podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.* Czy po czterech latach podnoszenia i zwiększania ktokolwiek widział jakąkolwiek informację o stopniu realizacji Strategii? Czy ktokolwiek wie, czy został osiągnięty którykolwiek z pięciu wyznaczonych celów szczegółowych? Jeżeli nie, to co udało się wprowadzić czy wdrożyć, a co jeszcze wymaga pracy?

Ponad rok temu, w dniu 6 lipca 2022 r. na posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (CNT) Sejmu RP Janusz Cieszyński, sekretarz stanu w Kancelarii Prezesa Rady Ministrów i zarazem pełnomocnik rządu do spraw cyberbezpieczeństwa, przedstawił najważniejsze – według niego – informacje ministra cyfryzacji na temat realizacji Strategii. Skorzystałam z okazji i zadałam konkretne pytania dotyczące celów szczegółowych. Do dziś dnia nie otrzymałam pisemnej odpowiedzi, którą chciałam się podzielić z czytelnikami „Domeny".

Pisemne informacje przekazywane komisjom sejmowym przez ministrów i prezesów urzędów nie są udostępniane innym zainteresowanym oprócz posłów. Jeżeli szukamy informacji, to pozostaje nam mozolne przeglądanie sprawozdań z posiedzeń komisji oraz odpowiedzi na interpelacje i zapytania poselskie publikowane na stronie internetowej Sejmu.

W przypadku Komisji CNT są sprawozdania z posiedzeń:

- z 9 marca 2023 r., na którym rozpatrzono informację na temat przygotowania państwa na płynące z zagranicy zagrożenia związane z cyberprzestępczością;
- z 12 lipca 2023 r., na którym rozpatrzono informację Najwyższej Izby Kontroli o wynikach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości";
- z 16 sierpnia 2023 r., na którym rozpatrzono informacje ministra cyfryzacji dotyczące niedoboru wykwalifikowanej kadry z zakresu IT i cyberbezpieczeństwa, podnoszenia kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa oraz szczególnych zasad wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

W minionej kadencji Sejmu interpelacji dotyczących cyberbezpieczeństwa było sporo. Ostatnia o numerze 44299 z 9 października 2023 r. dotyczyła wykorzystania Funduszu Cyberbezpieczeństwa. Z zapytań najciekawsze jest z 16 sierpnia 2023 r. o realizację przez Pełnomocnika Rządu do spraw Cyberbezpieczeństwa zadań w obszarze zarządzania ryzykiem niewłaściwego użycia informacji chronionej przez najwyższe kierownictwa instytucji publicznych.

> *Dla zainteresowanych wymienione dokumenty wraz z odpowiedziami stanowią pierwszą wskazówkę, jaki może być faktyczny stan cywilnego cyberbezpieczeństwa RP oraz co wymaga poprawy lub zmiany, bowiem nawet lakoniczne lub hurraoptymistyczne odpowiedzi pozwalają dokonać oceny bieżącej sytuacji, także za pomocą analizy lingwistycznej.*

Tropem raportów NIK

Najwyższa Izba Kontroli przez ostatnie dziewięć lat przeprowadziła wiele kontroli. Pierwsza dotyczyła realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP i została przeprowadzona w 2014 r. (wyniki opublikowano w 2015 r.). W kolejnych latach były m.in. kontrole:

- zapewnienia bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych;
- zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego;
- wdrożenia przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych;
- wdrożenia przez administrację publiczną regulacji dotyczących ochrony danych osobowych po wejściu w życie RODO;
- bezpieczeństwa teleinformatycznego RP;
- bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych.

Warto sięgnąć do wniosków pokontrolnych i sprawdzić, czy zostały wdrożone. Czy też, jak w przypadku wymienionej wcześniej kontroli zapobiegania i zwalczania skutków wybranych przestępstw internetowych, badana jednostka nie wdrożyła rekomendacji, bo w raporcie jest pewne *pomieszanie z poplątaniem*, a głównym efektem raportu jest *nieprawdziwe i zmanipulowane pokazanie rzeczywistości, przypisanie różnym organom kompetencji, których nie miały i pominięcie absolutnie całego kontekstu funkcjonowania internetu* – jak stwierdził Paweł Lewandowski, podsekretarz stanu w Ministerstwie Cyfryzacji, na posiedzeniu Komisji CNT 12 lipca 2023 r.

Ministerstwo Cyfryzacji w stanie hibernacji

Koordynatorem wdrażania Strategii Cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji. Zajrzałam na oficjalną stronę Ministerstwo Cyfryzacji > Co robimy > Cyberbezpieczeństwo na portalu gov.pl. Ostatnia modyfikacja miała miejsce 15.07.2020 o godz. 13:10. Podstrona > Strategia jest datowana 20.12.2019. Czyżby w cyberbezpieczeństwie RP nic się nie zmieniło od 3–4 lat?

Sprawdziłam także zakres obowiązków Departamentu Cyberbezpieczeństwa, którym kieruje dyrektor i trzech zastępców. Otóż zadania Departamentu to:

- koordynowanie prac związanych z: Krajowym Systemem Cyberbezpieczeństwa, Krajowym Systemem Certyfikacji Cyberbezpieczeństwa, Strategią Cyberbezpieczeństwa RP i Narodowymi Standardami Cyberbezpieczeństwa;
- przygotowanie i prowadzenie programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa;

- prowadzenie spraw związanych z nadzorem ministra nad Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK-PIB).

Na wspomnianym lipcowym posiedzeniu Komisji CNT okazało się, że *w pionie ministerstwa, który się zajmuje cyberbezpieczeństwem, są 63 osoby bardzo wysoko wykwalifikowane, które mają olbrzymie doświadczenie na rynku, w służbach i zajmują się tymi kwestiami w sposób bardzo systemowy*. Biorąc pod uwagę chociażby wcześniej wymienione dokumenty oraz moje artykuły, w których od trzech lat opisuję różne cyber-odklejki, cyber-absurdy i cyber-bambików, wykonywanie zadań Departamentu wymaga gruntownej weryfikacji.

Jak wykazała kontrola NIK dotycząca zapobiegania i zwalczania skutków wybranych przestępstw internetowych, *w KPRM zostały utworzone odrębne, rozbudowane struktury przeznaczone do obsługi kancelaryjno-biurowej Pełnomocnika (Biuro Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa), w której na koniec 2021 r. było zatrudnione 17 osób)*. Na stronie www.gov.pl/web/premier/pelnomocnik-rzadu-do-spraw-cyberbezpieczenstwa opublikowana jest tylko podstawa prawna powołania Pełnomocnika, zaś na portalu gov.pl znalazłam jedynie 3 komunikaty, 1 informację, 1 rekomendację i 1 oświadczenie obecnego jeszcze Pełnomocnika, opublikowane po jego powołaniu w czerwcu 2021 r. Dowiedziałam się także, że w Biurze jest nawet Wydział Promocji Polityki Cyfrowej (cokolwiek to znaczy). Pełnomocnik jest ustawowo zobowiązany do opracowania i przedłożenia sprawozdań Radzie Ministrów w terminie do 31 marca każdego roku za poprzedni rok kalendarzowy. Dla audytorów sprawozdania będą kolejnym tropem.

NASK nie bez skazy

NASK jest dziwnym podmiotem. Powstał w 1991 r. jako zespół na Uniwersytecie Warszawskim, późniejsze zmiany następowały aż do 2017 r., gdy został państwowym instytutem badawczym (PIB). Prowadzi „badania naukowe, prace rozwojowe", a jego misją jest „poszukiwanie i wdrażanie rozwiązań, służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa". Deklaracja pokrywa się z zapisami ustawy o instytutach badawczych (Dz.U. nr 498 z 2022 r. z późn. zm.), według której do podstawowej działalności każdego PIB należy:

– prowadzenie badań naukowych i prac rozwojowych – przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki,
– wdrażanie wyników badań naukowych i prac rozwojowych oraz
– wykonywanie zadań szczególnie ważnych dla planowania i realizacji polityki państwa w zakresie opracowywania i opiniowania standardów, a także monitoringu zjawisk i wydarzeń mogących stwarzać zagrożenie publiczne.

Jednocześnie, jak przyznają jego przedstawiciele, NASK prowadzi „działalność operacyjną na rzecz bezpieczeństwa polskiej cywilnej cyberprzestrzeni", bowiem od 2018 r. jako CSIRT jest kluczowym cywilnym elementem krajowego systemu cyberbezpieczeństwa. Zajmuje się też edukacją użytkowników internetu. Powstały dualizm działalności naukowej i operacyjnej wprowadza pewne pomieszanie z poplątaniem, szczególnie gdy mówimy o odpowiedzialności i rozliczalności.

NASK został ustawowo uznany za wiodący ośrodek wiedzy o cyberbezpieczeństwie. Zatem można oczekiwać od niego najwyższej dbałości i staranności zawodowej. Niestety, tak nie jest.

Oto kilka przykładów poważnych wpadek:

- rok 2019: kontrola NIK „Realizacja programu Ogólnopolskiej Sieci Edukacyjnej (OSE)" wykazała brak Polityki bezpieczeństwa dla sieci OSE, której budowa rozpoczęła się w 2017 r. Stosowne normy i standardy wyraźnie wskazują, że NASK powinien był opracować i wdrożyć Politykę nie później niż w dniu rozpoczęcia procesu korzystania z OSE przez szkoły. Nie zrobił tego przez dwa lata, chociaż w ramach OSE dostarcza szkołom bezpłatne usługi bezpieczeństwa teleinformatycznego, obejmujące ochronę przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego;

- rok 2020: wyniki badania bezpieczeństwa stron internetowych placówek oświatowych, wykonanego przez NASK na zlecenie Ministerstwa Cyfryzacji, z nieznanych powodów nigdy nie trafiły do osób najbardziej zainteresowanych. Jeżeli badanie miało coś wnieść, to dyrektorzy wszystkich jednostek objętych badaniem powinni byli otrzymać indywidualne raporty, by móc podjąć stosowne działania kontrolne i naprawcze. Wielu nawet nie wiedziało o badaniu. NASK nie wyciągnął żadnych wniosków dotyczących procedur, o czym się przekonałam w tym roku, gdy badanie jest powtarzane bez ładu i składu;

- rok 2021: poważną wpadkę NASK-u dotyczącą formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa JST, wymaganej w ramach programu „Cyfrowa Gmina", opisałam w numerze 4/2021 Biuletynu PTI. Na szczęście Centrum Projektów Polska Cyfrowa nie dopuściło do blamażu. Z kolei o zamieszaniu i kontrowersjach dotyczących przeprowadzenia samej diagnozy w jednostkach samorządu terytorialnego możemy przeczytać w artykule „Audyt za 1 zł" Katarzyny Żółkiewskiej-Malickiej w numerze 3/2023 „Domeny";

- rok 2022: wspomniana już kontrola NIK dotycząca zapobiegania i zwalczania skutków wybranych przestępstw internetowych wykazała brak wdrożenia przez NASK mechanizmów ewaluacji efektów prowadzonych działań edukacyjnych z zakresu cyberbezpieczeństwa, które umożliwiłyby zwiększenie skuteczności tych działań, w tym dopasowanie sposobów docierania z komunikatami do poszczególnych grup docelowych.

- rok 2023: w poprzednim numerze „Domeny" wykazałam błędy i niedoróbki w poradnikach przygotowanych przez NASK w ramach programów „Cyberbezpieczny Samorząd" i „Firma Bezpieczna Cyfrowo". Moje uwagi zostały odebrane przez zainteresowanych jako kąśliwości, bo przecież są to *specjaliści najlepsi w regionie, a może nawet w Europie*. Ponadto, jak mi tłumaczono, poradniki zostały zatwierdzone przez 30-osobową Radę Naukową NASK-u.

Należy zaznaczyć, że w 2022 r. NASK realizował, na zlecenie Ministerstwa Cyfryzacji, następujące projekty finansowane ze środków budżetu państwa (https://www.nask.pl/pl/projekty-dofinansowane/projekty-realizowane-ze):

- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla kluczowych osób w państwie: dotacja celowa w wysokości 1 630 264,57 zł w 2022 r. (w 2021 r. dotacja celowa wyniosła 1 351 593,75 zł);**
- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla przedstawicieli jednostek samorządu terytorialnego (JST) w województwie podlaskim: dotacja celowa w wysokości 2 080 077,00 zł w 2022 r.;**
- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa dla pracowników Podstawowej Opieki Zdrowotnej (POZ) – pilotaż w powiecie pajęczańskim: dotacja celowa w wysokości 278 275,00 zł w 2022 r.**

Razem dotacje wyniosły prawie 4 mln złotych. W 2023 r. NASK-owi również przyznano dotacje celowe na:

- **działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa w 2023 r. – podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej w wysokości 8 950 244,50 zł;**
- **realizację kampanii informacyjno-edukacyjnych dotyczących edukacji społeczeństwa w obszarze cyberbezpieczeństwa i rozwoju społeczeństwa informacyjnego w wysokości 5 406 106,50 zł.**

Razem to ponad 15 mln złotych do rozliczenia i ewaluacji efektów ich wydatkowania.

Na stronie https://laptopdlaucznia.gov.pl w zakładce Centrum informacji > Darmowe oprogramowanie > Program do obsługi poczty elektronicznej oprócz znanego Thunderbirda rekomendowany jest program Blue-Mail amerykańskiej firmy Blix, Inc. z siedzibą w Jersey City, USA. Dlaczego właśnie ten produkt spośród wielu innych dostępnych na rynku? Jako audytor czekam na przedstawienie uzasadnienia wyboru oraz szczegółowej oceny skutków dla ochrony danych dla tego produktu – informacja zawarta na stronie https://bluemail.me/privacy nie wystarczy.

Może nadszedł czas na analizę i zmianę struktury NASK-u, by lepiej podkreślić jego rolę operacyjną w krajowym systemie cyberbezpieczeństwa i doprecyzować odpowiedzialność za podejmowane działania.

> *Czy Rada Naukowa zatwierdzała także listę darmowego oprogramowania proponowanego przez NASK czwartoklasistom, którym właśnie rozdano laptopy?*

Nie trzymamy ręki na pulsie

Sztuczna tzw. inteligencja wzbudza skrajne emocje. Jedni się zachwycają i liczą, że rozwiąże wiele problemów naszego świata. Inni straszą, że pozbawi nas pracy czy wręcz wykończy. Przypominam, że jeszcze 5 lat temu administratorzy systemów AI skarżyli się na brak dostatecznego wsadu danych. Potem nastała pandemia, która wymusiła nagminne i powszechne korzystanie z internetu. Przez dwa lata karmiliśmy bestie naszymi danymi bezrefleksyjnie i bez opamiętania. Wystawiliśmy bestiom także nasze dzieci, wprowadzając naprędce naukę zdalną. Już w 2020 r. alarmowałam o zagrożeniu na konferencji Security First oraz w moim artykule w numerze 2–4/2020 Biuletynu PTI – bez jakiegokolwiek zainteresowania i reakcji ze strony Ministerstwa Edukacji i Nauki.

Teraz musimy nauczyć się z bestiami żyć. W sukurs przychodzi Unia Europejska, przyjmując kolejne przepisy. Niestety, po RODO-wych doświadczeniach mam obawy, czy w Polsce poradzimy sobie z ich skutecznym wdrożeniem i stosowaniem. A problemów przybywa, co wykazała m.in. Podkomisja stała do spraw regulacji prawnych dotyczących algorytmów cyfrowych w trakcie swoich prac w minionej kadencji Sejmu RP.

Ku mojemu zdziwieniu Polska nie uczestniczyła w konferencji AI Safety Summit (www.aisafetysummit.gov.uk), która odbyła się na początku listopada w Bletchley Park z inicjatywy premiera Wielkiej Brytanii i z udziałem znaczących polityków i reprezentantów czołowych firm technologicznych z całego świata. W Deklaracji podpisanej przez rządy 29 państw czytamy m.in.: *There is potential*

*for **serious, even catastrophic, harm**, either deliberate or unintentional, stemming from the most significant capabilities of these AI models. Given the rapid and uncertain rate of change of AI, and in the context of the acceleration of investment in technology, we affirm that **deepening our understanding of these potential risks and of actions to address them is especially urgent**.* W związku z tym premier Rishi Sunak zapowiedział powołanie pierwszego na świecie AI Safety Institute, którego zadaniem będzie testowanie bezpieczeństwa kolejnych pojawiających się rodzajów sztucznej inteligencji.

Tymczasem w Polsce odchodzący minister edukacji i nauki powołuje Instytut Badań nad Renesansem i Barokiem przy Akademii Zamojskiej, który będzie prowadził badania naukowe w zakresie historii literatury polskiej i pedagogiki (https://akademiazamojska.edu.pl/pl/news/1163-instytut-badan-nad-renesansem-i-barokiem-powstal).

Samo MEiN od 8 listopada br. zachęcało do wypełnienia ankiety dotyczącej roli sztucznej inteligencji w edukacji (https://www.gov.pl/web/edukacja-i-nauka/rola-sztucznej-inteligencji-w-edukacji-z-perspektywy-dyrektorow-nauczycieli-i-uczniow-zapraszamy-do-wypelnienia-ankiety), by zebrać – **poniewczasie** – opinie na temat:

- roli sztucznej inteligencji (AI) w edukacji,
- **potencjalnych korzyści i zagrożeń**, które wiążą się z wykorzystywaniem narzędzi opartych na AI,
- wsparcia, którego oczekuje środowisko szkolne w tym obszarze.

Badanie jest skierowane do dyrektorów i nauczycieli oraz uczniów klas VI–VIII szkół podstawowych i szkół ponadpodstawowych. Najwyraźniej to oni zostali uznani przez ministra edukacji za najlepszych specjalistów od oceny zagrożeń ze strony sztucznej inteligencji w oświacie. Instytut Badań Edukacyjnych im tylko asystuje.

Czas na weryfikację przez audytorów procesu realizacji „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" przyjętej 28 grudnia 2020 r. uchwałą nr 196 Rady Ministrów.

Cyber-kadry

Ostatnie posiedzenie Komisji CNT w mijającej kadencji Sejmu RP (16 sierpnia 2023 r.) poświęcone było problemom z kadrami dla cyberbezpieczeństwa. Podsekretarz stanu w MC Paweł Lewandowski przedstawił bardzo ogólną informację o podejmowanych działaniach szkoleniowych. Niestety, nie powiedział, jak jest mierzona skuteczność organizowanych szkoleń.

Na posiedzeniu dowiedzieliśmy się także o stanie wymienionych wcześniej indywidualnych szkoleń z zakresu cyberbezpieczeństwa organizowanych od 2021 r. dla najważniejszych osób w państwie – parlamentarzystów oraz kadry kierowniczej administracji centralnej i samorządowej. Okazało się, że na koniec kadencji mniej więcej 1/3 parlamentarzystów nadal nie przeszła szkolenia. Szkoda, że lista owych posłów nie jest publiczna.

Czy w nowej kadencji wszyscy parlamentarzyści potraktują własne cyberbezpieczeństwo poważnie? W czwartek 26 października br. nowo wybrani posłowie byli szkoleni z:

- ochrony informacji niejawnych przez przedstawicieli ABW,
- ochrony danych osobowych przez pracowników Kancelarii Sejmu,
- cyberbezpieczeństwa przez przedstawiciela NASK.

Chyba szkolenie nie było skuteczne, skoro na portalu X (dawny Twitter) jeden z nowych posłów już w pierwszym dniu pierwszego posiedzenia Sejmu kwestionował środki bezpieczeństwa informatycznego obowiązujące w Sejmie. Do myślenia daje także liczba odsłon owego wpisu (1,3 mln) i treść komentarzy pod nim, szczególnie pseudofachowców.

Temat cyberbezpieczeństwa prawie nie pojawiał się w debatach politycznych w minionej kampanii wyborczej do Sejmu i Senatu RP. Nieliczne wzmianki w programach poszczególnych partii znajdziemy w zestawieniu przygotowanym przez redaktorkę Nikolę Bochyńską z portalu CyberDefence24 na stronie https://cyberdefence24.pl/polityka-i-prawo/wybory-2023-co-w-cyberbezpieczenstwie-obiecywali-politycy. Nasz kolega Jarosław Deminet w numerze 2/2023 „Domeny" starannie uzasadnił konieczność likwidacji Ministerstwa Cyfryzacji, wiemy jednak z doniesień medialnych, że ministerstwo pozostanie. Należy zatem wspierać działania nowego ministra na rzecz naszego cyberbezpieczeństwa.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 15 listopada 2023 r.

Wielkie małe kropki

Od nowoczesnych telewizorów przez elastyczną elektronikę po techniki obrazowania medycznego i analizy chemicznej – kropki kwantowe pozwoliły wykorzystać możliwości nanotechnologii w przedmiotach, z których korzystamy na co dzień. A ich potencjał dopiero zaczynamy poznawać.

Piotr Kościelniak
dziennikarz, popularyzator nauki

Kropki kwantowe większości z nas kojarzą się zapewne z reklamami telewizorów, w których technologia ta odpowiada za wyświetlanie obrazu. Dla tych, którzy interesują się nauką, kropki kwantowe (quantum dots) to osiągnięcie, za które trzech naukowców – Aleksiej Jekimow, Louis Brus i Moungi Bawendi – otrzymało w 2023 r. Nagrodę Nobla w dziedzinie chemii. Technologia ta nie jest jednak tak, bardzo nowa, jak mogłoby się wydawać, a jej zakres zastosowań wykracza daleko poza wyświetlacze telewizorów.

Rewolucja na ekranie

Technologia kropek kwantowych polega na wykorzystaniu nanokryształów półprzewodnikowych, które emitują światło o różnych kolorach w zależności od ich rozmiaru i kształtu. Technologia ta obecnie jest stosowana do produkcji ekranów telewizorów i laptopów. Najwięksi producenci, którzy wykorzystują technologię kropek kwantowych w swoich produktach, to m.in.:

- Samsung technologię opartą na nanokryształach stosuje od wielu lat w telewizorach oznaczanych jako QLED, które oferują lepszą jakość obrazu, większy zakres kolorów i większą jasność niż tradycyjne telewizory LCD. Najnowsza wersja tej technologii – Neo QLED – wykorzystuje ok. 40 razy mniejsze diody LED do podświetlania warstwy z kropkami kwantowymi, co pozwala zmieścić ich znacznie więcej w wyświetlaczu i precyzyjnie sterować jasnością i czernią.
- LG używa kropek kwantowych w telewizorach określanych jako NanoCell. Udoskonalona wersja, wykorzystująca podświetlenie diodami mini LED, jest określana skrótem QNED (skrót od Quantum NanoCell Emitting Diodes).
- Sony była jedną z pierwszych firm, które wprowadziły technologię kropek kwantowych do komercyjnie dostępnych urządzeń konsumenckich. Ekrany tego typu, znane pod nazwą Triluminos, stosowane były w laptopach, a obecnie w telewizorach japońskiej marki.
- Chińska firma TCL również oferuje telewizory QLED wykorzystujące kropki kwantowe oraz mini LED, pozwalające uzyskać bardzo wysoką jasność obrazu przy jednoczesnym zachowaniu doskonałego kontrastu. To obecnie firma z pierwszej trójki największych producentów telewizorów na świecie, mająca swoje zakłady również w Polsce.

Rozmiar ma znaczenie

W świecie makro opisywanym przez chemię właściwości materii zależą od tego, ile elektronów i protonów ma atom danego pierwiastka. W świecie nano sprawy wyglądają inaczej. Kiedy posługujemy się miarami rzędu jednej milionowej milimetra (czyli nanometrem), w grę wchodzą nowe zjawiska – efekty kwantowe zależne od rozmiarów, a nie liczby atomowej.

Czym zatem są kropki kwantowe? To kryształy o rozmiarach rzędu nanometrów, co sprawia, że wykazują niezwykłe właściwości optyczne i elektronowe. W dodatku zjawiska te często przeczą intuicji i zdrowemu rozsądkowi – na przykład mogą emitować lub pochłaniać światło o barwie zależnej od kształtu i rozmiaru takiego kryształu. Jak małe są to struktury, niech świadczy porównanie – kropka kwantowa składająca się z kilku tysięcy atomów tak się ma rozmiarem do piłki futbolowej, jak piłka do całej Ziemi.

Zasada działania kropek kwantowych opiera się na ograniczeniu ruchu cząstek w nanokryształach – wewnątrz uwięziona jest cząstka o długości fali porównywalnej z rozmiarami kropki. W wyniku tego energia cząstek zależy od rozmiaru i kształtu kropki kwantowej, co z kolei przekłada się m.in. na kolor i intensywność światła, które emituje lub pochłania. Im mniejsza jest kropka kwantowa, tym bardziej niebieskie jest światło, które emituje. Im większa jest kropka kwantowa, tym mniejsza jest energia cząstek i tym bardziej czerwone jest światło, które emituje.

Emisja światła to nie wszystko (choć to właśnie ta cecha decyduje o popularności technologii kropek kwantowych) – inne właściwości, którymi można sterować przez zmianę rozmiaru kryształów, to m.in. potencjał redoks, temperatura topnienia czy przejścia fazowe.

Kwantowa historia

Co ciekawe, właściwości nanocząstek przewidziano blisko 90 lat temu. Herbert Fröhlich, wnioskując na podstawie słynnego równania Schrödingera, uznał, iż nanokryształy, ze względu na swoje rozmiary, powinny mieć właściwości całkowicie odmienne od materii w skali makro. Ale to, co tak pięknie dawało się opisywać równaniami matematycznymi, znacznie trudniej było potwierdzić w świecie rzeczywistym. Przyczyna była oczywista – nie dysponowaliśmy narzędziami i technikami pozwalającymi manipulować materią w tak małej skali.

Manipulować, czyli świadomie wywoływać efekty kwantowe – bo same nanocząsteczki wykorzystywane były od stuleci. Na przykład opracowana w epoce greckiej substancja pozwalająca na barwienie włosów na ciemniejszy kolor wykorzystywała kryształy siarczku ołowiu o wielkości 5 nanometrów. Innym fascynującym przykładem jest pochodzący z IV w. n.e. rzymski puchar Likurga. Wykonany jest ze szkła, które zmienia kolor z czerwonego na zielony w zależności od umiejscowienia źródła światła. Tę zdumiewającą właściwość zawdzięcza nanocząsteczkom złota i srebra „zawieszonym" w szkle. Zresztą eksperymenty z nanokryształami wytworzonymi w szkle to również specjalność laureatów Nagrody Nobla.

Oczywiście nikt nie przypuszcza, że twórca czernidła czy rzymski (lub aleksandryjski – bo historia pucharu Likurga ma kilka luk) rzemieślnik wiedzieli o właściwościach nanocząsteczek. Korzystali z nich bez świadomości istoty zjawisk, które odpowiadały za niezwykłe efekty finalne. Praktyczne badania efektów kwantowych rozpoczęły się na dobrą sprawę dopiero w latach 70. XX wieku. Naukowcy IBM i Bell Laboratories równolegle stworzyli tzw. studnie kwantowe pozwalające ograniczyć przestrzennie ruch cząstek. Kolejne lata – i coraz doskonalsze techniki litograficzne – umożliwiły konstruowanie doskonalszych studni kwantowych (tzw. drutów kwantowych) i wreszcie całkowite zablokowanie swobodnego ruchu elektronów. Za osiągnięcia w tej dziedzinie Komitet Noblowski przyznawał nagrody już dwukrotnie: w 1986 i 1998 roku.

Trzej malarze nanoświata

Badanie efektów kwantowych w układach o ograniczonej wymiarowości dało początek pracom nad kropkami kwantowymi dopiero na początku lat 80. XX w. Aleksiej Jekimow eksperymentował ze szkłem barwionym chlorkiem miedzi, które poddawał temperaturze od 500 do 700 st. Celsjusza przez nawet kilkadziesiąt godzin. Po ostygnięciu prześwietlał je promieniami rentgenowskimi, badając powstałe struktury. Okazało się, że w szkle powstawały nanokryształy o wielkości od kilku do 30 nanometrów. Niektóre z nich absorbowały różne barwy światła. Im mniejsze były kryształy w szkle, tym intensywniej pochłaniały kolor niebieski.

Jekimowowi udało się pierwszy raz wytworzyć kropki kwantowe w sposób celowy. Niestety, pracował wówczas w rosyjskim Państwowym Instytucie Optyki i publikował wyniki w rosyjskich magazynach naukowych, jego prace na Zachodzie były praktycznie nieznane. Dość podobną drogą, zupełnie niezależnie od Jekimowa, poszedł Louis Brus, który wykorzystywał do eksperymentów kryształy siarczku kadmu w zawiesinie – głównym celem badań była absorpcja energii słonecznej i wykorzystanie jej do zasilania reakcji chemicznych. Brus zauważył jednak ciekawą rzecz – kiedy kryształy się powiększały, zmieniały się również ich właściwości optyczne. Porównał te o rozmiarach 12,5 nm oraz te o średnicy ok. 4,5 nm – te mniejsze absorbowały światło niebieskie.

Obaj naukowcy wiedzieli, że mają do czynienia z efektami kwantowymi zależnymi od rozmiarów cząstek. I choć takie cząstki udawało się wytworzyć, problemem pozostawała jakość. Sterowanie wielkością kryształów i eliminowanie

defektów można było wprawdzie zrobić w laboratorium wielkim nakładem pracy i czasu, jednak o przeniesieniu tych procesów na skalę przemysłową nie było mowy.

To udało się dopiero kilka lat później, a dokonał tego uczeń Brusa – Moungi Bawendi. W 1993 r. przedstawił metodę otrzymywania kropek kwantowych w roztworze, którego podgrzewanie i schładzanie pozwalało na kontrolowanie wielkości i kształtu kryształów. Dzięki temu osiągnięciu kropki kwantowe stały się stabilne w roztworach, łatwiej było nimi manipulować i łączyć z innymi materiałami. To właśnie Bawendi otworzył drogę do masowej produkcji urządzeń wyposażonych w technologię kropek kwantowych, co pozwoliło na opracowanie ekranów nowej generacji, urządzeń do detekcji molekularnej czy terapii fotodynamicznej.

Technika trafiła pod strzechy

Znaczenie kropek kwantowych w mikroelektronice wynika z ich zdolności do generowania i przetwarzania sygnałów świetlnych na poziomie pojedynczych fotonów. Jak to działa np. w wyświetlaczach? Niebieskie światło jest wytwarzane przez LED – jak w zwykłych płaskich telewizorach. Kropki kwantowe – w zależności od swoich rozmiarów – mogą zmieniać barwę światła na czerwoną lub zieloną – jeżeli chcemy otrzymać barwę niebieską, po prostu przepuszczamy światło bez wykorzystywania kropek kwantowych. W ten sposób punkt na ekranie może „produkować" trzy kolory podstawowe. Takie ekrany mają znacznie wyższą jasność, a wyświetlane kolory są odbierane jako czystsze. Mogą być również cieńsze niż tradycyjne ekrany LCD.

Jeszcze bardziej zaawansowane odmiany wyświetlaczy wykorzystują kropki kwantowe (np. kryształy selenku kadmu) do wytwarzania światła. Pozwalają one osiągnąć jasność obrazu od 50 do nawet 100 razy większą niż w przypadku telewizorów kineskopowych i z ekranami LCD. Paleta kolorów poszerzona jest o ok. 30 proc. Wszystko to dzieje się przy zużyciu energii niższym o połowę w stosunku do ekranów LCD. Co więcej – wyświetlacze mogą być bardzo cienkie i elastyczne.

Takie ekrany nie są jednak idealne – podobnie jak panele OLED mają one problemy z wypaleniem, czyli szczątkowym „duchem" na ekranie pozostałym po długotrwałym wyświetlaniu statycznego obrazu. Mogą to być np. czarne pasy z boku ekranów przy wyświetlaniu starszych filmów w formacie 4:3 lub paski wiadomości w telewizjach informacyjnych.

Nie tylko telewizory

Kropki kwantowe mogą być wykorzystane jako źródła światła, detektory, przełączniki, wzmacniacze, lasery, modulatory, tranzystory, diody, komórki pamięci i logiczne. Mają wiele zalet w porównaniu z tradycyjnymi materiałami półprzewodnikowymi, takie jak wysoka sprawność, niska temperatura pracy, mała wrażliwość na zakłócenia, duża szybkość i niski pobór mocy. Kropki kwantowe mogą również być zintegrowane z innymi materiałami, takimi jak krzem, szkło, polimery czy metale, a także z materiałem biologicznym.

Szczególnie obiecujące jest zastosowanie kropek kwantowych w fotowoltaice do poprawy wydajności i obniżenia kosztów ogniw słonecznych. Ponieważ mogą pochłaniać i emitować światło o różnych długościach fal, pozwalają na lepsze wykorzystanie widma promieniowania słonecznego. Kropki kwantowe nanoszone na powierzchnię lub wtopione w strukturę innych materiałów fotowoltaicznych, takich jak perowskity, tworzą ogniwa tandemowe o wysokiej sprawności (przekraczającej 23 proc.).

W biologii i medycynie kropki kwantowe mogą być użyte do obrazowania i terapii różnych procesów i chorób. Mają lepsze właściwości niż tradycyjne barwniki fluorescencyjne – są jaśniejsze, a zatem łatwiejsze do zaobserwowania, bardziej stabilne i można je „stroić" do pożądanej długości fali.

Kropki kwantowe nadają się również do oznaczania i śledzenia różnych struktur, takich jak komórki, tkanki, białka czy nawet łańcuchy DNA i RNA. Pozwala to śledzić rozwój infekcji i wykrywać przerzuty nowotworowe. Kropki kwantowe mogą być także użyte do obrazowania in vivo w zakresie zarówno promieniowania widzialnego, jak i bliskiej podczerwieni, co pozwala na lepszą rozdzielczość niż konwencjonalne techniki obrazowania.

Kropki kwantowe można modyfikować za pomocą dołączanych do nich materiałów biologicznych, takich jak przeciwciała, peptydy czy leki, co daje selektywne wiązanie się z docelowymi komórkami, molekułami lub patogenami. Trwają prace nad wykorzystaniem kropek kwantowych w terapii fotodynamicznej, w której światło aktywuje kropki, które następnie generują np. reaktywne formy tlenu zabijające komórki nowotworowe lub bakterie. Można do nich również doczepić leki, które zostaną uwolnione w pożądanym miejscu wewnątrz ciała po naświetleniu światłem o konkretnej barwie.

Hakowanie ciała

W technokulturze ciało, rozumiane jako mechanizm podlegający nieustannym rekonstrukcjom i udoskonaleniom, staje się doświadczalnym poligonem medykalizacji, generując nowe dylematy antropologiczne i etyczne. Ludzkie ciało łączy się z wieloma obszarami, będącymi przedmiotem interdyscyplinarnych analiz, takich jak: emocje, zmysły, seksualność, śmiertelność, zdrowie i choroba czy artystyczny wizerunek ciała. Sposób w jaki myślimy o ciele, wpływa na to, jak myślimy o tożsamości, inności, podmiotowości i wspólnocie.

Ada Florentyna Pawlak

antropolożka technologii, prawniczka i historyczka sztuki. Wykładowczyni akademicka (IEiAK UŁ, Artes Liberales UW, Wydział Zarządzania UŁ, Akademia im. Leona Koźmińskiego w Warszawie, „Trendwatching & Future Studies" na Wydziale Humanistycznym AGH w Krakowie), popularyzatorka nauki i spikerka w obszarze społecznych kontekstów nowych technologii i towarzyszących im idei. Specjalizuje się w dyskursach kapitalizmu afektywnego, kultury cyfrowej, transhumanizmu i sztucznej inteligencji, technointymności, współpracy człowieka z maszyną i projektów art@science. Współpracuje z Digital University, Polsko-Amerykańską Fundacją Wolności, Rzecznikami Nauki i łódzkim Fotofestiwalem.

Human Enhancement najczęściej jest tłumaczone jako wzmocnienie i doskonalenie człowieka – nieterapeutyczna optymalizacja obejmująca zabiegi wykraczające poza utrzymanie organizmu przy życiu, dokonywane poprzez poprawę lub przywrócenie pewnych funkcji. Wśród przedstawicieli nurtów i stanowisk akceptujących ulepszanie istnieje dużo rozbieżności – tak w kwestii definicji, funkcji, jak i zakresu udoskonalania. Panorama możliwości rozciąga się od całkowicie nierealistycznych wizji do wąsko ujętych, możliwych dziś konkretnych rozwiązań inżynierii biomedycznej w rodzaju neuroprotezy słuchu (implant ślimakowy) czy zastosowania bionicznych protez kończyn. Przez ostatnie dwie dekady optymalizacja wzbogacona została cyborgicznymi rozszerzeniami: chatbotami i asystentami głosowymi, wirtualną i rozszerzoną rzeczywistością, robotami społecznymi czy technologią ubieralną.

Biohaking. Cielesne modyfikacje

Uznanie cielesności za przestrzeń, którą można poddać kulturowej rekonstrukcji, postuluje społeczność biohakerów, przyczyniająca się do popularyzacji idei transhumanistycznych. Biohaking (zbitka od ang. *biology* i *hack*) jest terminem parasolowym dla różnorodnych działań, mających na celu włamanie się do ludzkiej biologii w celu rozszerzenia możliwości organizmu w warunkach pozainstytucjonalnych, poza oficjalnymi jednostkami badawczymi[1]. Biohakerzy samodzielnie wszczepiają urządzenia do swoich ciał bez znieczulenia i jakiegokolwiek nadzoru medycznego. Interesuje ich, w jaki sposób można wykorzystać technologię do rozwinięcia nowych zmysłów i organów, które umożliwią postludziom postrzeganie i doświadczanie rzeczywistości na nowe sposoby[2]. Ingerencje w cielesność mają na celu optymalizację ciała oraz umysłu, dlatego biohaking odróżnić należy od przywrócenia funkcjonalności niepełnosprawnego ciała i wyrównania szans na poziomie genetycznym, co stanowi tradycyjny cel medycyny (np. bioniczne kończyny dla niepełnosprawnych, które testują Jessi Sullivan czy Nigel Ackland; implanty bezprzewodowe sterujące protezami; restytucja zmysłu wzroku np. dzięki urządzeniu The Argus II Retinal Prosthesis System znanemu jako „bioniczne oko", przywracanie słuchu przez implant ślimakowy). Kultura biohakerów skupia nie tylko niezależnych wynalazców, innowatorów i projektantów, lecz także wszelkiej maści hobbystów i „cielesnych majsterkowiczów".

1 A. Delfanti, *Biohackers. The Politics of Open Science*, Palgrave Macmillan, New York 2013.

2 M. O'Connell, *To Be a Machine: Adventures among Cyborgs, Utopians, Hackers, and the Futurists Solving the Modest Problem of Death*, Granta, London 2017.

Ruch biohakingu czerpie inspirację z powieści i kultury wizualnej cyberpunku. Ciało w narracjach cyberpunkowych postrzegane jest jako przedmiot, który można dowolnie kształtować. W powieściach przybiera ono rozmaite formy: jest zmodyfikowane za pomocą „cyberwszczepów", poddaje się implantacji, uzupełnieniom w formie podzespołów i sztucznych kończyn, aż po ingerencję w mózg i fuzję ze sztuczną inteligencją. Estetyka szoku i obsceniczności, przekraczanie granicy cielesności oraz motyw przemiany zarówno w sferze fizycznej, jak i psychologicznej zbliża manifestacje biohackerów do nowofalowego kina transgresji.

Biohaking obejmuje wiele technik i metod – od nieinwazyjnych po inwazyjne, od temporalnych po trwałe. Może przyjąć formę *bodyhackingu*, czyli ingerencji w cielesność w celu jej optymalizacji bez udziału technologii za pomocą różnorodnych metod i technik, powodujących poprawę wydajności ciała, takich jak: specjalna dieta, medytacja czy wspieranie ciała urządzeniami noszonymi w celu zbierania i archiwizowania danych biometrycznych, tzw. *quantify self* za pomocą technologii ubieralnej (*wearable technology: hearing aids, smart-watches, fitness bands, e-skin*).

Biohaking inwazyjny zakłada ingerencję biotechnologiczną w cielesność i polega bądź to na wzmocnieniu za pomocą urządzeń technicznych (implanty, mikroczipy, głęboka stymulacja mózgu, interfejsy mózg-komputer), bądź na przekształcaniu cielesności chemicznymi środkami farmakologicznymi, takimi jak: leki nootropowe, propagowane m.in. przez Michaela Brandta (Nootrobox) czy poprzez modyfikacje genetyczne.

Warto podkreślić, że cielesne modyfikacje są według transhumanistycznych eksperymentatorów źródłem poczucia sensu i dobrostanu. Wydaje się istotne, że biohaker poznaje świat ciałem poszerzonym, zwiększającym możliwości dotykowo-kinestetyczne i motoryczne funkcje organizmu. Biohakerzy to społeczność, która w atmosferze rytualnych performance'ów stawia istotne pytania dotyczące społecznej akceptacji transhumanistycznej filozofii. Performatywny bunt wobec ograniczeń ciała jest zarazem wizualizacją procesu adaptacji do otoczenia technologicznego. W pracy „Symbole naturalne. Rozważania o kosmologii" Mary Douglas dochodzi do wniosku, że zainteresowanie otwarciem ciała połączone jest ze społecznym poszukiwaniem dróg ucieczki i inwazji, „wejściami i wyjściami"[3]. Antropolożka zauważa, że jeśli nie istnieje troska o zachowanie granic społecznych, to można się spodziewać, że nie istnieje także troska o granice ciała.

Magnetyzm cyborga

Cyborgizacja, rozumiana jako proces denaturalizacji biologicznych aspektów egzystencji człowieka, następująca poprzez zniesienie granicy między tym co naturalne, a tym co mechaniczne, wpisuje się w ramy dyskursu o cielesności i tematykę transgresji, rozumianej jako przekraczanie granic niedoskonałej fizyczności.

W 1998 r. Kevin Warwick, profesor cybernetyki na Uniwersytecie w Reading i pionier biohakingu, w ramach projektu „Cyborg 1.0", wszczepił sobie w rękę specjalny chip, dzięki któremu zdalnie kontrolował obsługę komputera i zarządzał oświetleniem: wszystkie elektroniczne drzwi na kampusie otwierały się przed nim automatycznie, a gdy wchodził do swojego laboratorium, zapalały się światła[4]. Warwick jest też autorem „Cyborg Project 2.0", w ramach którego kierowany przez niego zespół stworzył sztuczną rękę, powielającą ruchy zwykłej ręki (obleczonej specjalną „bransoletą" z sensorami) i kierowaną za pośrednictwem internetu, dzięki czemu Warwick był w stanie podnosić kubek znajdujący się na innym kontynencie i doznawać równocześnie odpowiednich wrażeń dotykowych. W kolejnej wersji projektu do organizmu jego żony został wprowadzony czujnik chirurgicznie podłączony do włókien nerwowych. Dzięki temu małżonkowie zyskali możliwość somatycznego komunikowania się na odległość, sterowania motoryką cudzego ciała z potencjałem komunikacji emocjonalnej.

Rewolucja technologiczna przynosi nie tylko zmiany społeczno-ekonomiczne, lecz także transhumanistyczne sposoby posługiwania się ciałem, zachęcając do jego optymalizacji i wzmacniania. Drogą do postczłowieczeństwa ma być szerokie zastosowanie technologii wszczepianej w ciało dzięki implantacji, która wpisuje się w tzw. „konwersję cybernetyczną"[5]. Jest to proces, w ramach którego poszczególne naturalne elementy cielesności będą zastępowane przez bardziej wydajne elementy cybernetyczne.

Postaciami znanymi w środowisku wspólnot cyborgicznych są m.in.: Lepht Anonym, mająca magnesy w opuszkach palców; Tim Cannon, który zainstalował w przedramieniu urządzenie odczytujące sygnały dotyczące temperatury, wilgotności skóry i tętna; Wafaa Bilal posiadający wszczepiony z tyłu czaszki aparat fotograficzny; Liviu Babitz, założyciel

3 M. Douglas, *Symbole naturalne. Rozważania o kosmologii*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2004.

4 K. Warwick, *Transhumanism: Some Practical Possibilities*, „FifF Kommunikation" (2), 2016, s. 24–27, https://core.ac.uk/download/pdf/228145468.pdf (dostęp1.12.2023).

5 N. Agar, *Humanity's End: Why We Should Reject Radical Enhancement*, The MIT Press, Cambridge, London 2010, s. 29.

firmy Cyborg Nest, oferującej dodawanie do ciał sztucznych zmysłów (np. zmysł północy, umożliwiający łączenie ludzkiego ciała z ziemskim w polu magnetycznym; po skierowaniu ciała na północ artefakt wszczepiony w tors zaczyna drżeć).

Przykładem transhumanistycznych ekstensji jest również poszerzenie sensorium przez Todda Huffmana, który zaimplantował sobie magnes w koniuszek palca. W wyniku modyfikacji Huffman odkrył, że stał się czuły na urządzenia generujące zmienne pola (silniki, kable) i nabył umiejętność odróżniania wibracji mechanicznych od magnetycznych[6]. Zwolennikiem ekstensji jest również cierpiący na achromatopsję Neil Harbisson, który traktuje przymocowaną chirurgicznie do czaszki sonifikującą[7] antenę jako część swojego ciała. Antena zaopatrzona w kamerę pozwala interpretować sygnały i rozpoznawać kolory dzięki dźwiękom.

Sztuczna ręka prof. Kevina Warwicka

Źródło: https://futurespodcast.net/episodes/01-kevinwarwick

Rozszerzanie sensorium

Przedstawiciele ruchu cyborgicznego, funkcjonujący pod nazwą „Międzygatunkowa społeczność" (*Transpecies Society*), skupiają swoją działalność w Barcelonie w ramach Cyborg Fundation – organizacji non-profit. Projektują nowe zmysły, których funkcje inspirowane lub zapożyczone są od innych organizmów żywych czy zjawisk przyrodniczych. Przykładem takiego cyberorganu jest czujnik, który pozwala odczuwać wibracje w ciele wraz z występującym w dowolnym miejscu trzęsieniem ziemi. Dla członków Transpecies Society celem scalenia ciała z tego typu cybernetycznym zmysłem jest zwiększenie powiązania cyborga ze zjawiskami naturalnymi, czy nawet częściowego utożsamienia się z przedstawicielami innych niż ludzkie gatunków. Konsekwencją takiego scalenia ma być zwiększenie altruizmu wobec środowiska przyrodniczego, a co za tym idzie pozytywne zmiany w codziennych praktykach i podejściu do problemów klimatycznych i przyrody.

Artyści cyborgiczni eksplorują obszary związane z dotykiem i kinestetycznie aktywnym ciałem. Jednym z częściej wszczepianych urządzeń jest chip identyfikacji radiowej (RFID) pozwalający otworzyć drzwi lub odblokować iPhone'a ruchem ręki. Hakerka ciała Lepht Anonym, w wykładzie zatytułowanym „Cybernetics for the Masses", opisała swoje próby osiągnięcia wzmocnienia sensorycznego za pomocą narzędzi kuchennych i łatwo dostępnych wszczepialnych urządzeń elektronicznych[8]. W prelekcji zatytułowanej „Cyborgasms", wygłoszonej na konwencie BDYHAX, Rich Lee zaprezentował implant „Lovetron 9000" – wibrujące urządzenie poprawiające doznania seksualne, które można wszczepić pod skórę. zapowiada nowe formy „cyborgazmu" dzięki podskórnym czujnikom wszczepianym w kręgosłup, które mogą być aktywowane przez inne osoby noszące podobne czujniki. Urok wielu implantowanych pod skórę urządzeń (magnesy, diody LED[9], Circadia[10]) wykracza poza sferę użyteczności, praktyczności czy rozszerzonej skuteczności i posiada walor estetyczny bądź tożsamościowy, ilustrując termin ukuty przez Jeana Baudrillarda – „alibi wartości użytkowej"[11]. Jako zwolennicy open source postrzegają siebie jako część rozwijającego się obywatelskiego ruchu naukowego i twierdzą, że urzeczywistnienie obietnicy nauki i technologii nie wymaga formalnego wykształcenia akademickiego, laboratoriów i dużych kont bankowych. Bryan Bishop tłumaczy, że transhumanizm

6 S. Laratt, *The Gift of Magnetic Vision. Body Modification Ezine*, London, N.L. & London, 2004.

7 Sonifikacja to zastosowanie dźwięków niebędących mową do wyrażenia, przetworzenia informacji lub poznania danych. Podobnie jak wizualizacja znajduje zastosowania naukowe, przemysłowe, edukacyjne, estetyczne i artystyczne. Pozwala jednostce postrzegać struktury poprzez słuch. Zob: T. Hermann, A. Hunt, *Znaczenie interakcji w sonifikacji*, materiały z dziesiątego spotkania ICAD International Conference on Auditory Display, Sydney, Australia, 2004.

8 L. Anonym, *Cybernetics for the Masses,* wykład na YouTube. https://youtu.be/a-Dv6dDtdcs?si=nWH33R43bOixsGYr

9 Chip Northstar V1, wielkości dużej monety, zawiera pierścień diod LED i został zaprojektowany tak, aby mógł oświetlać tatuaże spod skóry, naśladując bioluminescencję meduz. Zob: E. Zolfagharifard, *Would YOU implant lights under your skin? Bizarre trend sees people transform themselves into glowing cyborgs,* „The Daily Mail", www.dailymail.co.uk/sciencetech/article-3314388/Would-implant-lights-skin-Bizarre-trend-sees-peopletransform-glowing-cyborgs.html"

10 Circadia to wszczepialne urządzenie odczytujące dane biomedyczne i przesyłające je do internetu przez Bluetooth. W rzeczywistości wszczepienie urządzenia Circadia należy rozumieć jako artystyczną demonstrację tego, co może być możliwe w przyszłości, a niekoniecznie jako realistycznie przydatny system QS. Zob: P. Rothman, *Biohacking/Grinder Update: Tim Cannon Implants Circadia 1.0*, „Humanity + Magazine", http://hplusmagazine.com/2013/10/21/grinder-update-tim-cannon-implants-circadia-1-0"

11 J. Baudrillard, *For a Critique of the Political Economy of the Sign*, tłum. Charles Levin, Telos Press, St. Louis 1981.

DIY (Do IT Yourself) łączy ludzi, którzy są zainteresowani „demokratyzacją nauki poza tradycyjnymi laboratoriami uniwersyteckimi lub narzędziami dla naukowców-amatorów i naukowców-obywateli, aby mogli faktycznie realizować różne technologie badawcze, których inaczej by nie realizowali"[12].

Niezależnie od tego, czy obejmują estetyczne czy poznawcze hakowanie ciała, inicjatywy transhumanistyczne nie są napędzane jedynie przez działania rynku, lecz celebrowane jako zaangażowanie w radykalnie zmienioną przyszłość ludzkości i prezentowane jako projekty społeczne, ideologiczne, a nawet kosmologiczne, projektujące szerszy cel, jakim jest radykalnie przekształcona ludzka przyszłość społeczna[13]. Innowator DIY – biohaker to przedsiębiorca społeczny sugerujący, że wiedza instytucjonalna, z jej czasochłonnymi protokołami badawczymi i restrykcyjnymi regułami będzie utrudniać ewolucję gatunku.

> *Popularność rozpowszechnianej technologii noszonej, wywodzącej się często z biohakingu, potwierdza, że „wyobraźnia technologiczna" staje się potężną siłą w kształtowaniu życia społecznego i przyszłości. Żyjemy w społeczeństwie, w którym zostaliśmy zsocjalizowani do myślenia, że technologia odgrywa nadrzędną rolę w konstytucji i organizacji naszego gatunku, dla którego szybkość jest synonimem atrakcyjności i który utożsamia to, co nowe, z tym, co dobre.*

Ciało jako miejsce inskrypcji kulturowej

W nowoczesnych systemach społecznych ciało stało się fundamentalnym polem politycznej i kulturowej działalności, a termin „społeczeństwo somatyczne" podkreśla, że status ciała we współczesnej kulturze jest odzwierciedleniem bezprecedensowego zjawiska jego indywidualizacji. Staje się ono plastycznym tworem, który może być czasami kształtowany jako prywatny zasób, a czasem jako społeczny symbol, przekazujący informacje tożsamościowe. Wygląd ciała, jego rozmiar, kształt są potencjalnie otwarte na proces rekonstrukcji, zgodnie z założeniami właściciela i stopniem zaabsorbowania transformacją.

Antropolog Terrance Turner zauważył, że ciało stanowi jedną z głównych granic, nad którymi sprawowana jest władza społeczeństwa[14]. W każdym ludzkim społeczeństwie ciała są kluczowymi miejscami inskrypcji i reprodukcji kulturowych wartości i rozróżnień. W eseju „The Social Skin" (Skóra społeczna) badacz przekonuje, że ozdoby ciała we wszystkich kulturowo różnorodnych odmianach (od malunków na ciele, pióropuszy, biżuterii, skaryfikacji, tatuaży po kosmetyki) są jednym z głównych środków, dzięki którym jednostki są uspołeczniane i integrowane do swoich społeczności[15]. Porządek kulturowy, a tym samym ciało, jest zorganizowany wokół zestawu symbolicznych opozycji między naturą a kulturą, tym, co ludzkie, a tym, co nieludzkie, między jednostką a tym, co kolektywne, między tym, co biologiczne, a tym, co społeczne.

> *Ciało jest tekstem kulturowym, środkiem wyrażania porządku i wyznaczonego w nim miejsca lub pełnionej funkcji. Cielesne akty oporu, podobnie jak cielesne akty konformizmu, są motywowane kulturowo.*

Uczeń Turnera, Daniel Rosenblatt, zwrócił uwagę na sposoby, w jakie „współcześni pierwotni" żyjący w społecznościach alternatywnych w Stanach Zjednoczonych przywłaszczają rdzenne formy modyfikacji ciała, aby zakomunikować wyobcowanie ze społeczeństwa[16]. Transhumaniści traktują ciało nie jako stabilne miejsce do wpisywania stałych znaczeń i wartości, lecz jako ciągły projekt,

12 DIY Transhuman Tech, Bryan Bishop https://youtu.be/i4ex52LYDe8?si=0RuoHfU74LJvyMxS

13 D. Valentine, *Exit Strategy: Profit, Cosmology, and the Future of Humans in Space*, „Anthropological Quarterly", 85, 2012, s. 1049.

14 T. Turner, *The Social Skin*, (1980) 2017, przedruk: „Hau: Journal of Ethnographic Theory", 2, nr 2, s. 486–504.

15 Brytyjskiego antropologa interesował system znaczeń i wartości ukryty w rozbudowanym kodzie okazywania ciała, ożywiający sposoby jego zdobienia wśród plemienia Kayapo żyjącego na południowych rubieżach Amazonii w Brazylii: „Widok dobrze zbudowanego dorosłego mężczyzny Kayapo, z dużym krążkiem w dolnej wardze (podobny do spodka dysk o średnicy około sześciu centymetrów), osłoną na penisa (mały stożek wykonany z liści palmowych pokrywający żołądź prącia), dużymi otworami przebitymi w płatkach uszu, z których zwisają sznureczki z paciorków, całym ciałem pomalowanym w czerwone i czarne wzory, z wyskubanymi brwiami, rzęsami i zarostem oraz głową ogoloną do czubka głowy z długimi włosami pozostawionymi po bokach i z tyłu, na pewno nie wywołają w podróżniku wrażenia, że zdobienie ciała jest wśród Kayapo sztuką zaniedbaną". Duże otwory umieszczone w płatkach uszu wskazują na wagę, jaką Kayapo przywiązują do słuchania jako sposobu zdobywania wiedzy, podczas gdy krążki w ustach noszone przez starszych mężczyzn reprezentują ich siłę oratorską i wpływy polityczne. T. Turner, *The Social Skin*, (1980) 2017, przedruk: „Hau: Journal of Ethnographic Theory", 2, nr 2, s. 487.

16 D. Rosenblatt, *The Anti-Social Skin: Structure, Resistance, and „Modern Primitive" Adornment in the United States*, „Cultural Anthropology", 12, 1997, nr 3, s. 290.

nad którym należy pracować i nieustannie go przekształcać – to narzędzie, które można modyfikować i „hakować", aby pomóc ludzkim i postludzkim potomkom osiągnąć ulepszone formy doświadczenia. Proponowane formy modyfikacji ciała celowo zacierają granice między naturą a kulturą oraz między człowiekiem a nie-człowiekiem. – „Aby być transczłowiekiem, trzeba chcieć zaakceptować fakt, że ma się unikatową tożsamość osobową, wykraczającą poza ciało czy oprogramowanie, i że tej unikatowej tożsamości osobowej nie da się wyrazić po prostu jako ludzkiej lub nie. Wymaga ona wyjątkowej, transludzkiej ekspresji" – pisze Martine Rothblath[17].

Monstrualność

Rycina z XVI w. przedstawiająca monstrum „blemmyae".
Źródło: https://www.messynessychic.com/2023/10/19/the-unexpected-relevance-of-medieval-monsters/

Poszerzana technologicznie cielesność biohakerów, inspirowanych transhumanistycznym imaginarium, mającym korzenie w kulturach wizualnych science-fiction, może jawić się jako monstrualna. Zauważmy, że świat, w którym żyją monstra, sytuuje się zwykle na peryferiach kultury – jest nieznany z bezpośredniego doświadczenia lecz inspiruje wyobraźnię. Historia monstrów i potworów łączy się z ciekawością i fascynacją, które wypływają ze zderzenia z anomalią fizyczną. Potwór – istota o odmiennym, niesamowitym kształcie – sytuuje się w „strefie pomiędzy": jest zarówno nasz/taki sam, jak i obcy.

Wizerunki hybryd, istot z manuskryptów i bestiariuszy, straszyły ludzi średniowiecza, stając się elementem społecznej wyobraźni – czymś zarazem eksponowanym, oglądanym jak przerażającym. Średniowieczne monstra zamieszkiwały jednak odległe krainy, o których niewiele wiedziano. Opowieści o hybrydach odnosiły się początkowo do porządku religijnego, potem medycznego, lecz zawsze do pomieszania porządków zastanych, otwierając imaginacyjną przestrzeń dla powiązań porządku ludzkiego z nieludzkim. Przyjmując pozycję „pomiędzy", monstrum niesie ze sobą obietnicę transgresji, dzięki której wszelkie granice i kategoryzację ulegają rozmyciu, rozproszeniu. Jest więc „znakiem ostrzegawczym", na co wskazuje istotny aspekt etymologiczny terminu „monstrum", odsyłający do łacińskiego *moneo*, które oznacza „ostrzegać"[18]. Oszołomienie widokiem dziwnego ciała mieszało się z czcią dla ponadludzkiego bytu i jego formy mającej coś ludziom sygnalizować. W obszarze wiedzy potocznej panowało przekonanie, że zniekształcone ciało niesie pewną naukę. Obrazy monstrów, kryjąc w sobie szczególnie potencjał perswazyjny, funkcjonowały jako niezwykle pojemne toposy, mogące służyć złożonym celom, tj. utwierdzać w zmieniających się porządkach ideologicznych, moralnych czy politycznych. Obraz osobliwej cielesności zmusza też do szczególnego rodzaju refleksji nad granicami tego, co ludzkie. Istota ludzka zostaje „poszerzona", a podział na podmiot (człowieka) i przedmiot (nie-człowieka) staje się coraz bardziej problematyczny.

tak się miesza
tak się miesza we mnie
to co siwi panowie
podzielili raz na zawsze
i powiedzieli
to jest podmiot
a to przedmiot[19]

16 D. Rosenblatt, *The Anti-Social Skin: Structure, Resistance, and „Modern Primitive" Adornment in the United States*, „Cultural Anthropology", 12, 1997, nr 3, s. 290.

17 M. Rosenblatt, *From Transgender to Transhuman: A Manifesto on the Freedom of Form*, Ashgate Press, Burlington 2011, s. 14.

18 R. Braidotti, *Signs of Wonder and Traces of Doubt: on Teratology and Embodied Differences*, [w:] Between Monsters, Goddesses and Cyborgs. Feminist Confrontations with Science, Medicine and Cyberspace, eds. N. Lykke, R. Braidotti, London – New Jersey 1996, s.135.

19 Z. Herbert, *Chciałbym opisać*, z tomu Hermes, Pies i gwiazda, 1957 [w:] *Wiersze zebrane*, Wydawnictwo a5, Kraków 2018, s.87.

Zderzenie z podatkiem w IT

Zaroiło się ostatnio od doniesień o kolejnych kontrolach podatkowych wśród informatyków, które mają być prowadzone na szeroką skalę. Przedmiotem zainteresowania urzędów skarbowych stały się rozliczenia podatku dochodowego. Wydaje się, że są dwa wiodące obszary podlegające szczególnemu zainteresowaniu urzędników. Pierwszy z nich dotyczy osób zatrudnionych na podstawie umowy o pracę, korzystających ze szczególnych warunków ustalania kosztów uzyskania przychodu przysługujących twórcom. Drugi obejmuje jednoosobowe działalności gospodarcze rozliczające się na podstawie ryczałtu kwalifikowanego.

Nie podejmę próby znalezienia w tych dwóch obszarach jakiejkolwiek odkrywczej części wspólnej, poza samą informatyką jako obszarem aktywności zawodowej. Zanim jednak uznamy całą sytuację za spisek czy zamach na polską innowacyjność, warto zastanowić się, co spowodowało to zainteresowanie urzędników.

Podatek od utworu

W wyniku zmian podatkowych każdy twórca, wytwarzający utwory spełniające definicję z Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, ma prawo do zastosowania podwyższonych kosztów uzyskania przychodu. Choć pojęcie twórcy może kojarzyć się raczej z kompozytorami, muzykami i pisarzami, to w rzeczywistości obejmuje o wiele szersze grono zawodów. W obszarze teleinformatyki w wielu przypadkach wytwarzany

Tomasz Klasa

absolwent Wydziału Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie oraz Wydziału Nauk Ekonomicznych i Zarządzania Uniwersytetu Szczecińskiego, adiunkt Zachodniopomorskiej Szkoły Biznesu w Szczecinie, konsultant SAP, członek Zarządu Głównego PTI od 2014 r.

kod programu czy opracowywana dokumentacja systemu spełniają ustawową definicję utworu. To sprawia, że ich autorzy stają się w myśl ustawy twórcami, co (z kolei) daje prawo do zastosowania ulg podatkowych.

Wydawać by się mogło, że w takim razie wszystko jest jasne – skąd więc doniesienia o pojawiających się kontrolach? Przyczyn, jak zwykle, jest kilka. Status twórcy i płynące z niego uprawnienia nabywa się bez względu na liczbę czy wielkość opracowanych utworów – czy jest nim jeden artykuł, opasła książka, krótki utwór muzyczny czy program komputerowy.

> *W czym więc problem? Moim zdaniem w powszechnej, niestety, w środowisku IT praktyce nieoznaczania autorstwa.*

Mnóstwo programów tworzonych jest przez wieloosobowe zespoły, których członkowie pozostają anonimowi, a powstający kod programu nie zawiera informacji o jego autorach. Choć w myśl ustawy o prawie autorskim twórca nadal jest twórcą, a prawa autorskiego nie da się zrzec ani przenieść, skorzystanie z preferencji podatkowych dla twórców jest powiązane z wytworzeniem utworu, a nie samym faktem nadania komuś statusu twórcy. Niestety, tu sami nagminnie działamy na swoją niekorzyść, poddając się zapędom korporacyjnej kadry zarządzającej, której łatwiej jest potem sprzedawać dalej takie niepodpisane produkty.

Kompozytorzy piosenek, autorzy fotografii, malarze, pisarze i wielu innych „klasycznych" twórców dba o to, by oznaczać swoje dzieła. Dobrze wiedzą, że tylko w ten sposób mogą zbudować swoją markę i ochronić efekty swojej pracy. Trudno sobie wyobrazić pisarza, który anonimowo napisze książkę na zlecenie wydawnictwa. Dlaczego więc programista czy autor instrukcji użytkownika nie podaje, że ją wykonał?

Tu docieramy do kluczowego problemu – po wprowadzeniu zmian w systemie podatkowym wśród informatyków wręcz zaroiło się od twórców, systematycznie produkujących utwory. Można by rzec – i słusznie. Tyle tylko, że jednocześnie nie widać tego „na rynku", zalanym przez programy wytworzone przez anonimowe zespoły. To, niestety, miało prawo wzbudzić wątpliwości, czy deklarowane utwory faktycznie nimi są w rozumieniu ustawy. Szczególnie, gdy nie każdy z licznego grona technologicznych twórców jest np. programistą…

Ryczałt grozy

Zupełnie inna sytuacja jest w przypadku osób rozliczających się na podstawie ryczałtu. Wprowadzone zmiany umożliwiają rozliczanie się na podstawie ryczałtu znacznie szerszej grupie osób, w tym wielu informatykom. Wśród zmian znalazła się nowa stawka podatku (12%), przypisana do wybranych usług informatycznych. Niestety, w tym miejscu zapisy w ustawie o podatku dochodowym odnoszą się m.in. do niedookreślonych podzbiorów wybranych kodów z klasyfikacji autorstwa GUS. To sprawiło, że poza w miarę oczywistymi przypadkami (np. usługi doradcze w zakresie oprogramowania) pojawiło się wiele wątpliwości co do zakwalifikowania danej usługi do właściwej stawki (12% lub 8,5% jak dla pozostałych usług). Zgodnie z założeniami ustawy, podatnik powinien samodzielnie dobrać do świadczonej usługi właściwą stawkę podatku. Tyle tylko, że bardzo nieprecyzyjne zapisy wrzuciły do „interpretacyjnej szarej strefy" całe mnóstwo usług informatycznych.

Bezpieczną przystań miały zapewnić interpretacje indywidualne, wydawane na podstawie opisu i opinii GUS co do klasyfikacji statystycznej wykonywanej usługi pod innym kodem niż przypisany do stawki 12%. Opieranie decyzji podatkowych na jakichkolwiek interpretacjach zawsze jednak wiąże się z dużym ryzykiem, czego można się było spodziewać. Teoretycznie wiążące interpretacje indywidualne okazały się bardzo łatwe do unieważnienia – najpierw przez podważenie prawdziwości opisu sytuacji (na podstawie którego wydawana jest decyzja), a później już w sposób systemowy. W świetle kolejnych zmian interpretacji zasad kwalifikacji usług do kodów statystycznych powiązanych ze stawką 12% wiele osób rozliczających się na podstawie stawki 8,5% mierzy się właśnie z perspektywą narzucenia przez urząd zaległości podatkowej.

Klasyfikacja statystyczna w obecnej formie powstała wiele lat przed reformą podatkową, ale jako środowisko informatyków nie czuliśmy potrzeby jej poprawy. Choć od czasu do czasu podnoszona była kwestia jej nieprecyzyjności, nie było z naszej strony woli walki o zmiany. Może uznaliśmy, że to nie jest ciekawy temat dla informatyków i niech lepiej zajmą się tym statystycy i prawnicy podatkowi, ale w rezultacie to podatki przyszły do nas.

Z obserwacji bieżących wydarzeń powinniśmy wyciągnąć istotną lekcję. Przede wszystkim – jeśli sami (jako środowisko) nie zadbamy o siebie i własne bezpieczeństwo (w tym podatkowe), to nikt tego za nas nie zrobi. Jeśli sami nie zaczniemy czuć się twórcami i zachowywać jak twórcy ze wszystkimi tego konsekwencjami, nie będą nas tak traktować. Jeśli my, informatycy, nie opracujemy zasad klasyfikacji świadczonych przez nas usług – to zrobią to inni. Niekoniecznie w sposób odpowiadający praktyce w świecie IT i naszym potrzebom.

Rynek telewizyjny może odzyskać 2,85 mld zł z rynku pirackiego

Polscy widzowie mają dostęp do jednej z relatywnie najtańszych i najbardziej zróżnicowanych usług audiowizualnych w Europie. Dotyczy to zarówno pakietów płatnej telewizji, które w przystępnej cenie zapewniają bogaty wybór kanałów w jakości HD, jak i usług cyfrowych.

Jesteśmy bowiem drugim w Europie krajem pod względem bogactwa usług VOD, których jest w naszym kraju ponad 120. W ostatnich siedmiu latach legalne usługi VOD przyciągnęły 7,7 mln nowych widzów, proponując coraz bogatszą ofertę w atrakcyjnej cenie i w wysokiej jakości. Można powiedzieć, że rynek odrobił bardzo dobrze lekcję z tworzenia ofert odpowiadających potrzebom widzów. Jednak, jak pokazują najnowsze dane firmy Deloitte na temat skali strat wynikających z piractwa treści, potrzebna jest nie tylko przysłowiowa „marchewka", lecz także „kijek".

> *„Atrakcyjna legalna oferta sama w sobie, bez skutecznych narzędzi zwalczania przestępczości przeciwko własności intelektualnej, nie jest w stanie samodzielnie przynieść spodziewanych efektów w zakresie przeciwdziałania kradzieży treści audiowizualnych.*

Teresa Wierzbowska

prezeska Zarządu Stowarzyszenia Sygnał, które od ponad 20 lat zrzesza rynek audiowizualny w zakresie ochrony treści i przeciwdziałania kradzieży treści telewizyjnych. Prezeska Związku Pracodawców Prywatnych Mediów Lewiatan. Wiceprezeska Polskiej Izby Informatyki i Telekomunikacji. Wiceprzewodnicząca Rady Nadzorczej Związku Pracodawców Branży Internetowej IAB Polska.

Równolegle do szybkiego rozwoju legalnej oferty i transformacji usług telewizyjnych wynikających ze zmian technologicznych i konsumenckich, trwa nieustanna walka podmiotów z rynku telewizyjnego z przestępcami, którzy uczynili sobie źródło dochodu z monetyzacji kradzionych treści wideo, wyprodukowanych bądź oferowanych przez legalne usługi medialne.

Granice samoobrony

Czołowi nadawcy, operatorzy telewizyjni i platformy VOD nieustannie monitorują sieć, identyfikują i zgłaszają miliony naruszeń, prowadzą działania prawne przeciwko przestępcom. W ramach współpracy rynkowej realizowane są wyjątkowe w skali Europy projekty samoregulacyjne i edukacyjne, jak realizacja strategii "follow the money", czyli odcinanie serwisów pirackich od źródeł finansowania czy realizowane na spektakularną skalę projekty szkoleniowe dla organów ścigania. Działania te przynoszą efekty – chociaż nie eliminują całkowicie problemu, a jedynie miejscowo je niwelują. **W 2023 r. z serwisów pirackich korzystało o 900 tys. osób mniej niż siedem lat wcześniej**, co w zestawieniu z danymi o wzroście oglądalności legalnych źródeł obrazuje pozytywny trend. W ostatnich latach zostało

zamkniętych kilkadziesiąt dużych serwisów pirackich, zarządzono rekordowe jak dotychczas wyroki, a wysokość naprawy szkody sięga kilkudziesięciu milionów złotych.

To efekty konsekwentnej pracy podmiotów poszkodowanych, na których barkach spoczywa obecnie praktycznie cały ciężar związany z ochroną treści. Wydaje się, że osiągnęliśmy granice możliwości w zakresie efektywnej walki z piractwem przy wykorzystaniu obecnie dostępnych rozwiązań prawnych. Bez systemowych mechanizmów stosowanych od lat w innych krajach europejskich nie sposób zrobić kroku do przodu i w pełni skutecznie chronić treści, szczególnie wymagających natychmiastowych reakcji transmisji na żywo.

Co mówią dane?

Jak wynika z najnowszego raportu firmy Deloitte, **wartość konsumpcji treści audiowizualnych w nielegalnych źródłach wynosi 7,36 mld zł rocznie**. To kwota, za którą można by było zapewnić roczny abonament do platformy VOD wszystkim internautom korzystającym z tego typu usług.

> *Straty rynku audiowizualnego z tytułu piractwa cyfrowego wynoszą około 3 mld zł, dodatkowo straty Skarbu Państwa wynikające m.in. z tytułu utraconych danin sięgają 1,86 mld zł. Poszkodowany jest cały łańcuch finansowania produkcji i dystrybucji treści, np. straty Polskiego Instytutu Sztuki Filmowej szacowane są na ponad 100 mln zł.*

Po weryfikacji, jaka część z użytkowników korzystających z pirackiego obiegu jest skłonna zaprzestać tego procederu na rzecz legalnych źródeł, wyliczono potencjał transferu budżetów związanych z konsumpcją treści do legalnego streamingu. Wedle analizy **do odzyskania jest nawet 2,85 mld zł rocznie**. To są konkretne kwoty, które przy uszczelnieniu systemu i wprowadzeniu skutecznych mechanizmów walki z kradzieżą treści mogą zasilić legalny obieg treści, trafiając do twórców, producentów, dystrybutorów i zasilając budżet państwa.

Z nielegalnych serwisów korzysta 7,3 mln internautów. To więcej niż liczy jakakolwiek z czołowych platform VOD. Polscy widzowie odwiedzają serwisy pirackie blisko 130 mln razy miesięcznie. Z perspektywy ostatnich lat, z korektą na moment kumulacji spraw sądowych, które zakończyły się zamknięciem serwisów i zasądzeniem wyroków, obserwować można stały wzrost ruchu na serwisach pirackich. Z tą różnicą, że w celu uniknięcia odpowiedzialności coraz wyraźniej korzystają z globalnych hostingów, utrudniając postępowania i działania. Jest to jeden z kluczowych problemów – polscy piraci VOD chętnie rejestrują działalność na fikcyjne zagraniczne podmioty – zarówno domena, jak i hosting zlokalizowane są nieraz po drugiej stronie globu.

W przypadku serwisów oferujących **nielegalnie treści sportowe ponad 90% wykorzystywanych pośredników jest poza polską jurysdykcją**. Wielowarstwowe ukrywanie rzeczywistych danych prowadzi do przewlekłości i zwiększonych kosztów postępowań. Dotychczasowe rozwiązania prawne mają bardzo ograniczony zakres działania.

> *Z tego względu konieczne są rozwiązania stosowane powszechnie w Europie i na innych kontynentach, czyli blokowanie dostępu do strony oferującej nielegalne treści bez względu na techniczną lokalizację usługi.*

O kierunku rozwoju usług audiowizualnych przesądza widz i jego oczekiwania. Przyczyny sięgania po nielegalne źródła są natury ekonomicznej, to także brak refleksji na temat uwarunkowań prawnych. Część internautów trafia do serwisów pirackich po to, by zapłacić na rozrywkę mniej niż w legalnych usługach. Wprawdzie użytkownicy są skłonni wydać na dostęp do nielegalnych transmisji 30 zł, a do usług VOD 26 zł, co stanowi porównywalną wartość do usług legalnych, jednak kupujący liczą na to, że w pirackim serwisie znajdą treści z różnych legalnych źródeł, co w efekcie ma przynieść oszczędności. Ta wrażliwość cenowa jest związana z wiekiem i aktywnością osób korzystających z nielegalnych źródeł. Dane jednoznacznie pokazują, że to głównie młodsze grupy widzów sięgają do pirackich stron. Ponad połowa widzów online w wieku do 30. roku życia sięga do nielegalnych źródeł, w kolejnych grupach wiekowych odsetek ten spada aż do 26% w grupie 60+. Druga istotna obserwacja dotyczy aktywności osób sięgających do nielegalnych źródeł – jest ona znacznie wyższa niż w przypadku osób, które oglądają materiały wideo tylko w legalnych serwisach. To ta wzmożona aktywność, nawet przy spadku liczby użytkowników, generuje tak duże straty po stronie rynku.

Po omacku

Wielu użytkowników nadal ma trudność z rozróżnieniem serwisu licencjonowanego od nieposiadającego uprawnień do dystrybucji materiałów. Internauci nawet nie zastanawiają się nad tym. Szukając określonych treści w internecie, trafiają na różne serwisy, często później nawet nie pamiętają ich nazw. Zakładają, że jeśli inne nielegalne usługi nie są łatwe do znalezienia w otwartym internecie i są blokowane, to podobnie jest w przypadku kradzionych na komercyjną skalę treści. Stąd brak refleksji, a tym bardziej chęci rozstrzygania o stanie prawnym poszczególnych usług. Ponadto, podczas badania postaw konsumenckich wobec

serwisów pirackich, zrealizowanego przez Stowarzyszenie Sygnał w 2022 roku, internauci wyraźnie wskazali blokowanie stron pirackich jako kluczowy i oczywisty mechanizm przeciwdziałania nielegalnej dystrybucji treści. W wielu krajach europejskich jest to też element akcji edukacyjnych pomagających widzom online znalezienie legalnych źródeł. Blokowanie nielegalnych treści przynosić może korzyści nie tylko uprawnionym i całemu łańcuchowi dystrybucji treści wideo oraz skarbowi państwa, lecz także użytkownikom poprzez dbanie o bezpieczeństwo i jakość środowiska cyfrowego, w którym funkcjonują.

Live blocking

Najgorętszym obecnie tematem w Europie w zakresie metod walki z kradzieżą treści online jest *live blocking*, czyli blokowanie natychmiastowe stron oferujących nielegalne transmisje wydarzeń na żywo, w tym sportowych. Jest to kolejny – po *web blockingu i dynamic blockingu* – model walki z piratami. *Web blocking* polega na wydaniu przez sąd lub jednostkę administracji publicznej nakazu wobec ISP zablokowania dostępu do określonej strony. *Dynamic blocking* nadaje uprawnionemu możliwość wnioskowania do ISP o zablokowanie nie tylko strony, wobec której toczyło się postępowanie, lecz także tzw. stron lustrzanych, pojawiających się w miejsce zamkniętej strony. Taki model nie wymaga osobnego procedowania wobec każdej nowej strony i jest prawem, które nadawane jest uprawnionym, ligom sportowym, na określony czas, przeważnie związany z sezonem w danej dyscyplinie. W przypadku transmisji sportowych konieczne było wprowadzenie jeszcze szybszego trybu.

> *Zgodnie z Rezolucją Komisji Europejskiej nielegalne streamy mają być blokowanie w ciągu maksymalnie 30 minut.*

W 2023 r. Komisja Europejska wydała komunikat podkreślający kluczową rolę pośredników w reakcji na nielegalne treści online, a na 2024 r. zaplanowane jest trzyetapowe badanie weryfikujące, czy kraje członkowskie skutecznie blokują nielegalne transmisje, a tym samym, czy miękkie regulacje w tym zakresie są wystarczające.

Co ważne, pierwsze kraje europejskie już teraz, nie czekając na twarde regulacje, wprowadziły mechanizmy natychmiastowego blokowania stron z nielegalnie oferowanymi transmisjami i innymi treściami audiowizualnymi. W Grecji specjalny komitet składający się z przedstawiciela administracji publicznej oraz reprezentantów sektorów telekomunikacyjnego i uprawnionych weryfikuje zgłoszenia nielegalnych transmisji i wydaje nakazy blokady. We Włoszech decyzja o wydaniu nakazu jest dokonywana przez urzędników regulatora rynku na podstawie zgłoszeń otrzymywanych najczęściej od zaufanych organizacji reprezentujących uprawnionych. Tryb działania i szybkość reakcji zależy od typu treści, a tym samym potencjalnych strat wynikających z dalszej nielegalnej dystrybucji. W przypadku książek jest to przeważnie tryb standardowy trwający 48 dni, treści VOD – tryb przyspieszony realizowany w ciągu 5 dni, a transmisji na żywo – natychmiastowy, czyli w czasie maksymalnie 30 minut.

Polska stoi przed wyzwaniem wypracowania optymalnego systemu. Mamy w kraju doświadczenia związane z blokowaniem dostępu do stron hazardowych, mamy wzorce z innych krajów europejskich, mamy też otwarty dialog między różnymi interesariuszami – od regulatora po operatorów telekomunikacyjnych. To daje solidne podstawy, by wypracować skuteczne rozwiązanie, które będzie chronić własność intelektualną w świecie cyfrowym przy jednoczesnym zachowaniu neutralności dostawców usług dostępu do internetu.

Autorka tekstu była panelistką podczas dyskusji na temat udziału Polaków w światowym IT oraz potrzebie ochrony dóbr intelektualnych, zorganizowanego w ramach webinaru z cyklu „Prezes PTI zaprasza…" (7 grudnia 2023 r. https://sdsi.pl/webinaria/wielcy-polacy-w-it/).

Podczas webinaru prezentacje przedstawili:

- **Marcin Fidler, autor książki „WynalazcyPL. Polacy, którzy zmienili świat" (o pochodzących z naszego kraju konstruktorach i innowatorach w branży IT);**
- **Aka Beata Chodacka, przewodnicząca Sekcji Informatyki Szkolnej PTI (o konkursie GEEK);**
- **Włodzimierz Marciński, były prezes PTI, promotor dorobku polskiej myśli matematycznej (o projekcie „PoLand of IT masters").**

W panelu dyskusyjnym, oprócz wykładowców, wzięli udział także: dr hab. Katarzyna Chałubińska-Jentkiewicz, zastępca dyrektora NASK PIB, dyrektor ACPC Akademii Sztuki Wojennej, członek Rady ds. Cyfryzacji; Marcin Olender, Public Policy and Government Relations Manager Central and Eastern Europe z firmy Google i Michał Otrębski, członek Zespołu Antypirackiego „Litigation, Investigation, Intelligence" Nagravision, w Nagra Kudelski Group.

Webinar prowadzili prezes PTI Wiesław Paluszyński i Jarosław Mojsiejuk, członek Rady ds. Cyfryzacji.

NIS2, czyli (r)ewolucja?

Czekamy na transpozycję dyrektywy NIS2 do prawa krajowego. Czy będzie to rewolucja czy ewolucja? Czy nadzór będzie miał zęby czy nie?

Paweł Henig
absolwent Wydziału Elektroniki Politechniki Warszawskiej. Od połowy lat 90. budował dla centralnej administracji rządowej centra przetwarzania danych i sieci rozległe. Audytor wewnętrzny systemów zarządzania obejmujących normy: zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), zarządzania bezpieczeństwem i higieną pracy (OHSAS 18001), bezpieczeństwem produkcji wartościowej (CWA 14641 – Intergraf) oraz zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001. Certyfikowany audytor systemów IT (CISA), posiadacz certyfikatu ITIL Foundation. Rzeczoznawca PTI, ekspert PIIT. Dyrektor operacyjny Trusted Information Consulting Sp. z o.o.

Zacznijmy od tego, że obszar cyberbezpieczeństwa jest trudny regulacyjnie.

Po pierwsze, z uwagi na nieuchwytny charakter informacji. W przypadku dóbr materialnych każda strata jest łatwo dostrzegalna. Jak ktoś komuś ukradnie portfel, to okradziony po prostu go nie ma, o czym niechybnie się dowie przy pierwszej próbie skorzystania z jego zawartości. Natomiast ujawnienie (utrata) informacji w większości przypadków nie skutkuje brakiem dostępu do tej informacji. Złożoność systemów powoduje, że bardzo trudno dostrzec, gdzie ten wyciek nastąpił lub następuje i jak długo trwa. Atak, czyli wykorzystanie zebranych informacji, może nastąpić wtedy, gdy będzie „kumulacja", czyli strata będzie najbardziej dotkliwa dla okradanego, a złodziej może jeszcze swobodnie działać.

Po drugie, złożony charakter informacji. Często nie zdajemy sobie sprawy, w jaki sposób połączenie różnych, wydawałoby się zupełnie nieistotnych faktów, pozwala na uzyskanie bardzo wartościowych informacji oraz manipulowanie nimi (np. działalność Cambridge Analytica). „Atakujący" może wykorzystać uzyskaną w ten sposób przewagę w celu sprzedaży dóbr (marketing), ale również może zamykać nas w bańce informacyjnej, doprowadzając do polaryzacji społeczeństwa (głównie media społecznościowe) w celu destabilizacji całych państw. Przykładem może być brexit czy atak na Kapitol po nieudanej reelekcji Donalda Trumpa.

Po trzecie, bezkrytyczna akceptacja. Wszechogarniająca technologia wspiera nas w wielu działaniach. Od nawigacji wspomagającej nas w doborze trasy przejazdu, wyszukiwa-

nia informacji w Internecie, poprzez zautomatyzowane procesy produkcyjne czy kasy w sklepach samoobsługowych, arkusze kalkulacyjne wspomagające wykonywanie złożonych zestawień, aż do sztucznej inteligencji „rozwiązującej za nas problemy". Skoro raz, drugi czy trzeci wszystko poszło dobrze, to powoli przestajemy się zastanawiać nad sensem otrzymywanych wyników i bezwarunkowo przyjmujemy wynik za poprawny (brak krytycyzmu), powoli tracimy również umiejętności samodzielnego wykonywania zadań (uzależnienie), a tym samym tracimy bezpowrotnie możliwość zweryfikowania tego wyniku (nawet szacunkowo). W ten sposób powoli stajemy się bezbronni wobec technologii.

Po czwarte, złożoność technologiczna. W początkowym okresie rozwoju systemów informatycznych były one postrzegane jako rozwiązania skomplikowane i niezrozumiałe, jako wymagające specjalistycznej wiedzy i wykształcenia „zabawki" dla nielicznych.

> *Upowszechnienie rozwiązań IT daje złudzenie pozornej prostoty, gdyż są one projektowane głównie pod kątem łatwości użytkowania, a nie aspektów bezpieczeństwa. Celem jest działanie produktu po wyjęciu z pudełka, bo inaczej klient nie kupi. Bezpieczeństwo jest na drugim, o ile nie na znacznie dalszym planie.*

Bezpieczeństwo przeszkadza w upowszechnieniu technologii. Wiele rozwiązań działających po wyjęciu z pudełka albo w ogóle nie ma ustawionego hasła, albo ma domyślnego użytkownika i domyślne hasło, którego zmiany nie żąda w momencie uruchomienia (po co utrudniać życie klientowi?). Marketingowe uproszczenie technologii ma jeszcze jeden, bardzo poważny skutek uboczny. Jest nim oczekiwany zakres wiedzy i umiejętności. Pożądane stało się szybkie osiągnięcie „działającego rozwiązania", niekoniecznie wymagające zrozumienia zasad działania całego systemu, a tym samym skutków podejmowanych decyzji wdrożeniowych.

Po piąte, dług nie tylko technologiczny. Wiele eksploatowanych obecnie rozwiązań zostało uruchomionych dawno temu. Eksploatowane rozwiązania mają nierzadko ponad dekadę. Niestety, nie wszystkie były aktualizowane zgodnie z czasem życia produktów użytych do ich budowy. Ostatnio u jednego z klientów spotkałem instalację bazującą na Windows Serwer 2003 R2, którego wsparcie podstawowe zakończyło się 13 lipca 2010 r., a wsparcie rozszerzone 14 lipca 2015 r. System nadal działa, chociaż nie dostaje już żadnych poprawek, w tym w szczególności poprawek bezpieczeństwa, a podatności tego systemu są nadal wykrywane po upływie okresu wsparcia. Niestety, aktualizacja oprogramowania do nowych wersji nie jest rzeczą prostą, a występujące ograniczenia techniczne wynikające ze zmian w budowie (architekturze) nowszych wersji mogą być barierą nie do przejścia, gdyż wymagają zmian w całym stosie technologicznym, który korzysta z tego systemu. Często też brakuje informacji, które umożliwiłyby oszacowanie faktycznego zakresu niezbędnych zmian. Powody są często prozaiczne. Gdzieś „zagubiła się" dokumentacja. Dokumentacja była „niepełna", a osoba, która „znała system" już od kilku lat nie pracuje. Kiedyś „na szybko" trzeba było coś poprawić, a teraz już nikt nie pamięta co. A poza tym „przecież działa". Awersję do inwestowania pogłębiła jeszcze pandemia, podnosząc stopień niepewności prowadzenia działalności, a także ogólna koniunktura gospodarcza postrzegana poprzez wysoką inflację oraz rosnące koszty pracy i energii.

Po szóste, chciwość. Więcej i szybciej. Kultura startupowa, czyli bycie pierwszym za wszelką cenę. Ciągła presja na cięcie kosztów, której efektem jest offshoring. Chiny stały się światową fabryką zaawansowanych technicznie rozwiązań, a takie kraje jak Indie przejęły funkcję światowego centrum usług wsparcia. W ten sposób Chiny otrzymały know how (o co zadbała Komunistyczna Partia Chin, określając odpowiednie wymagania dla inwestorów zagranicznych), a Indie – praktycznie nieograniczony dostęp do systemów komputerowych na całym świecie wraz dostępem do know how producentów rozwiązań IT, dla których świadczą usługi wsparcia. Pandemia tylko przyspieszyła „pracę zdalną", która w firmach technologicznych istniała również wcześniej.

> *Dążąc do „optymalizacji kosztów", wiele firm utraciło realną kontrolę nad procesami wytwórczymi oprogramowania. W szczególności nie są w stanie zweryfikować, kto tę pracę wykonuje i czy jednocześnie nie pracuje dla innych, wrogich organizacji lub państw. Mechanizmy demokratyczne chronią osoby (RODO) i utrudniają możliwość weryfikacji ich zatrudnienia czy zachowań i postaw (screening), co skrupulatnie wykorzystują wrogie organizacje lub państwa.*

Innymi słowy, Lenin wiecznie żywy. To jemu przypisuje się słynne powiedzenie „Kapitaliści sprzedadzą nam sznurek, na którym ich powiesimy". Obecnie na tym sznurze, zwanym ładnie łańcuchem dostaw, wisi już i Unia Europejska, i Stany Zjednoczone, Kanada i Wielka Brytania. Podejmowane działania „obronne" wobec takich dostawców, jak Huawei, ZTE, Hikvision czy Dachua są mocno spóźnione, a ich skuteczność jest wątpliwa. Lobbing silnie stymulowany materialnie w połączeniu z prawnikami chroniącymi „konkurencję i wartości demokratyczne" (które de facto nie istnieją u ich mocodawców) stara się jak najbardziej osłabić działania regulatorów próbujących chronić najsłabszych uczestników rynku, czyli konsumentów.

Po siódme, silosy. Funkcjonalność, bezpieczeństwo i ergonomia to immanentne własności rozwiązania, które są ze sobą ściśle powiązane na poziomie architektonicznym. Nie można poprawnie zaprojektować funkcjonalności bez uwzględnienia aspektów ergonomii i bezpieczeństwa. W biznesie jednak podobno można. W Manifeście Agile[1] skupiono się właśnie na funkcjonalności. Podstawowymi założeniami są:

- ludzie i interakcje ponad procesy i narzędzia,
- działające oprogramowanie ponad szczegółową dokumentację,
- współpraca z klientem ponad negocjacje umów,
- reagowanie na zmiany ponad realizację założonego planu.

Na podstawie tych założeń sformułowano 12 zasad. Siódma zasada brzmi: „Działające oprogramowanie jest podstawową miarą postępu". Założenia piękne, podobnie jak założenia komunizmu[2] (ale nie w rozumieniu bolszewickim, marksistowsko-leninowskim) i podobnie utopijne. Szczególnie utopijna jest zasada jedenasta: „Najlepsze rozwiązania architektoniczne, wymagania i projekty pochodzą od samoorganizujących się zespołów", w szczególności w związku za zasadą piątą: „Twórzcie projekty wokół zmotywowanych ludzi. Zapewnijcie im potrzebne środowisko oraz wsparcie i zaufajcie, że wykonają powierzone zadanie". Działa, ale tylko w grupie nerdów[3], o ile ich zaburzenia funkcji społecznych umożliwią komunikację z pozostałymi osobami. Wie o tym dobrze każdy, kto miał możliwość zarządzania zespołem liczącym kilkanaście osób. Niestety, nikt nie zastanowił się, jak tych wszystkich nerdów zebrać w jednym miejscu i czasie. W rzeczywistości wdrożenia metodyk zwinnych przypominają bardziej wariacje na temat komunizmu na Kubie lub w Korei Północnej, a rzadziej w modelu chińskim, który bez wątpienia może być efektywny, chociaż najwyższym poziomem zaufania jest w tym przypadku kontrola (co już nie jest *agile*).

Ktoś w tym momencie może mi zarzucić tendencyjność, gdyż w zespole często jest osoba odpowiedzialna za tzw. *user experience*, a ścisły kontakt z klientem zapewnia ergonomię. Zgoda, ale takie podejście bazuje na dojrzałości klienta, z czym może być różnie. Niestety, ergonomia i bezpieczeństwo najczęściej nie są brane pod uwagę. Zasada druga brzmi: „Bądźcie gotowi na zmiany wymagań nawet na późnym etapie jego rozwoju. Procesy zwinne wykorzystują zmiany dla zapewnienia klientowi konkurencyjności". Jej kreatywnym rozwinięciem jest „to się poprawi później" lub „to jest problem innego zespołu".

Podejście zwinne (*agile*) wpisuje się w oczekiwania motywowane chciwością. Decyzja jest zazwyczaj podejmowana na podstawie tabelek księgowych przez osoby niemające niezbędnej wiedzy. Podejście powinno być zrównoważone i powinno uwzględniać wszystkie aspekty. Niestety, dziś testerem jest użytkownik dostający produkt nie w pełni przetestowany, a często również obciążony wieloma błędami konstrukcyjnymi.

Na kłopoty NIS2?

Wszystkie te wyzwania nasiliły się znacznie przez ostatnie 10 lat, a więc od czasu przygotowania wersji finalnej Dyrektywy NIS.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS) już w chwili opublikowania była z lekka spóźniona. Jej finalny projekt (po konsultacjach) został zamknięty na początku 2013 r. Natomiast koncepcyjnie potrzeba regulacji w tym obszarze to mniej więcej rok 2010, czyli przyjęcie europejskiej agendy cyfrowej. Dyrektywa ta, jak to często bywa w demokracji, jest pewnym kompromisem.

Podmioty podlegające regulacji dysponują rzeszą prawników i lobbystów, którzy „łagodzą" skutki regulacji, szafując często argumentem wysokich kosztów dostosowania tych podmiotów do nakładanych obowiązków. W efekcie regulacja często nie przynosi oczekiwanych rezultatów, ale każda regulacja ma swój „bezpiecznik". W tym przypadku jest to wpisany wprost obowiązek przeglądu funkcjonowania Dyrektywy NIS (art. 23).

Dlaczego powstała Dyrektywa NIS2? Odpowiedź to pytanie przynoszą jej motywy. Nie występują one w krajowych aktach normatywnych, przez co są często traktowane jako nieistotne, a jest wręcz odwrotnie. Wspólny przewodnik praktyczny Parlamentu Europejskiego, Rady i Komisji przeznaczony dla

1 https://agilemanifesto.org/iso/pl/manifesto.html

2 Program całkowitego zniesienia ucisku i wyzysku społecznego, postulujący powszechność, równość i sprawiedliwość społeczną oraz zbudowanie społeczeństwa bezklasowego opartego na społecznej kontroli gospodarki, własności środków produkcji i sprawiedliwym podziale dóbr.

3 Nerd, czyli osoba przesadnie fascynująca się naukami ścisłymi, zwłaszcza informatyką, oraz grami komputerowymi. Synonimicznym określeniem nerda jest geek (https://pl.wikipedia.org/wiki/Nerd). Osoba, zwłaszcza mężczyzna, który nie jest atrakcyjny i jest niezręczny lub społecznie niedostosowany (https://dictionary.cambridge.org/dictionary/english/nerd)

osób redagujących akty prawne Unii Europejskiej[4] wskazuje, iż „celem motywów jest zwięzłe uzasadnienie podstawowych przepisów części normatywnej bez ich przytaczania czy parafrazowania. Nie zawierają one wypowiedzi normatywnych ani apeli politycznych". W szczególności w punkcie 10.2 możemy przeczytać: „Rozporządzenia, dyrektywy oraz decyzje muszą zawierać uzasadnienie. Ma to na celu wyjaśnienie okoliczności, w których instytucja przyjmująca akt skorzystała ze swych uprawnień prawodawczych tak, aby strony w sporze miały możliwości obrony swoich praw, jak również aby Trybunał Sprawiedliwości Unii Europejskiej mógł wykonywać swoje uprawnienia kontrolne". Kwintesencją jest brzmienie punktu 10.5: „Motywy powinny w zwięzły sposób wskazywać powody przyjęcia głównych przepisów części normatywnej aktu".

> *Motywy mają kluczowe znaczenie dla zrozumienia przyczyn powstania aktu oraz interpretacji zapisów jego części normatywnej adekwatnie do intencji, a nie semantyki użytych zwrotów językowych. Musimy mieć świadomość niuansów językowych w poszczególnych językach urzędowych Unii Europejskiej. Motyw to „bodziec skłaniający do określonego działania"[5], motywator, a nie element kompozycyjny utworu.*

143 motywy NIS2

Ich lektura może być żmudna, ale można wyłonić i zsyntetyzować pewne słowa klucze, wskazujące, czego i dlaczego można oczekiwać od tej regulacji.

Po pierwsze, skuteczności (motyw 2) – została ona nadwątlona między innymi poprzez istotne różnice w podejściu do wdrożenia w poszczególnych państwach członkowskich (motyw 4). Nota bene słowo „skuteczność" występuje w dyrektywie NIS2 w różnych kontekstach aż 62 razy, natomiast w dyrektywie NIS jest prawie nieobecne. Skuteczność jest jednym z trzech najważniejszych słów-kluczy obok słowa incydent (233 razy) oraz słowa ryzyko (147 razy).

Po drugie, zakres stosowania (motyw 6) został znacznie rozszerzony, w tym w szczególności w aspekcie kryterium identyfikacji podmiotów (motyw 7). Oznacza to znaczny wzrost liczby podmiotów podlegających regulacji, ale przede wszystkim odejście od uznaniowości decyzji o kwalifikacji podmiotu. Rola regulatora w tym przypadku sprowadzi się do czynności technicznej, jaką jest prowadzenie rejestru. Państwa członkowskie mogą ustanowić krajowe mechanizmy umożliwiające podmiotom samodzielną rejestrację, ale to na podmiocie spoczywa obowiązek zgłoszenia danych do tego rejestru (art. 3 ust. 4 i art. 27). Zakres podmiotowy obejmie dodatkowo w szczególności administrację publiczną, z niewielkimi możliwymi wyłączeniami (motyw 8 oraz art. 2 ust. 6 do 9) dostawców usług zaufania, o których mowa w rozporządzeniu eIDAS (motyw 11) oraz usług pocztowych i kurierskich (motyw 12). Pełna lista sektorów, podsektorów oraz rodzajów podmiotów objętych dyrektywą NIS2 została ujęta w załącznikach. Przyjęte kryterium wielkości podmiotu jest również mierzalne, gdyż dotyczy podmiotu kwalifikowanego jako co najmniej średnie przedsiębiorstwo (art. 2 ust. 1). Oznacza to, że wszystkie przedsiębiorstwa zatrudniające co najmniej 50 osób lub o rocznym obrocie przekraczającym 10 mln EUR mogą podlegać rygorom dyrektywy NIS2 niezależnie, czy jest to podmiot prywatny, czy publiczny. Decyduje wtedy rodzaj prowadzonej przez podmiot działalności określony w załącznikach I i II. Niezależnie od wielkości przedsiębiorstwa może ono podlegać rygorom dyrektywy NIS2 w przypadku, gdy prowadzi rodzaj działalności opisany w art. 2 ust. 2 do 4. Co więcej, państwa członkowskie mogą rozszerzyć zakres stosowania dyrektywy NIS2 do podmiotów administracji publicznej na poziomie lokalnym oraz instytucji edukacyjnych, zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu (art. 2 ust. 5).

Po trzecie, racjonalność i kompletność podejmowanych działań (motyw 81 i 82). Celem zarządzania opartego na ryzyku nie jest minimalizowanie ryzyka, co prowadzi do nieproporcjonalnie dużych obciążeń finansowych i administracyjnych. Podejmowane środki zarządzania ryzykiem powinny być proporcjonalne do ryzyka, czyli potencjalnych strat, z uwzględnieniem kosztu wdrożenia tych zabezpieczeń. W artykule 21 ust. 1 mówi się wprost o odpowiednich i proporcjonalnych środkach technicznych, operacyjnych i organizacyjnych w odniesieniu do kosztów wdrożenia tych środków, co nakłada znacznie wyższe wymagania w zakresie zarządzania ryzykiem w stosunku do obecnie powszechnie przyjętych praktyk. Będące w powszechnym użyciu tzw. mapy ciepła nie pozwalają na ocenę proporcjonalności środków postępowania z ryzykiem w aspekcie kosztu odniesionego do potencjalnej straty (dotkliwości wystąpienia ryzyka). Istnieją wprawdzie metodyki oceny ryzyka pozwalające na ocenę proporcjonalności podejmowanych działań, jednakże praktycznie nie są stosowane. Sygnalizowałem ten problem w artykule pt. „Zarządzanie ryzykiem – Święty Graal czy wielka mistyfikacja?"[6] opublikowanym w numerze

4 Wersja polska: Print ISBN 978-92-79-49105-4 doi:10.2880/00371 KB-02-13-228-PL-C; PDF ISBN 978-92-79-49113-9 doi:10.2880/64050 KB-02-13-228-PL-N dostępna do pobrania https://eur-lex.europa.eu/content/techleg/KB0213228PLN.pdf

5 https://sjp.pwn.pl/slowniki/motyw.html

6 https://portal.pti.org.pl/wp-content/uploads/2023/03/9_zarzadzanie-ryzykiem.pdf

1/2023 „Domeny". Jest on nadal aktualny i w mojej ocenie będzie nabrzmiewał, w szczególności w związku z odpowiedzialnością nałożoną personalnie na organy zarządzające.

Po czwarte, łańcuch dostaw (motyw 85) i odpowiedzialność za zlecanie działań (motyw 83), w szczególności w połączeniu z podejmowaniem działań proaktywnych (motyw 105). Jest to bezpośrednia odpowiedź na narastające problemy bezpieczeństwa, których źródło leży poza podmiotem podlegającym regulacji. Mit „transferu ryzyka", który pod taką nazwą nadal pojawia się w normach, runął bezpowrotnie.

> *Ryzykiem można się jedynie podzielić*[7]*, co nie zwalnia właściciela ryzyka z odpowiedzialności.*

Jest to zgodne z innymi regulacjami, takimi jak np. kodeks cywilny. Podzielenie się ryzykiem może co najwyżej złagodzić skutki wystąpienia niekorzystnej okoliczności. Nigdy ich jednak nie zniweluje. O kwestiach ryzyka związanego z łańcuchem dostaw pisałem wcześniej.

Po piąte, nadzór (motyw 122). W dyrektywie NIS2 podzielono podmioty na kluczowe i ważne. Każdy z tych podmiotów ma w praktyce jednakowe obowiązki, a różnica pomiędzy nimi wynika z przyznanych środków nadzorczych. Podmioty kluczowe powinny być objęte kompleksowym systemem nadzoru *ex ante*[8] i *ex post*[9], natomiast podmioty ważne należy objąć uproszczonym systemem nadzoru wyłącznie *ex post*. Nadzór *ex post* nad podmiotami ważnymi może być uruchamiany na podstawie przekazanych właściwym organom dowodów, wskazówek lub informacji, gdy organy te uznają, że zachodzi podejrzenie naruszenia dyrektywy NIS2. Natomiast nadzór *ex ante* powinien być prowadzony na bieżąco, niezależnie od przesłanek uprawdopodobniających możliwość naruszenia dyrektywy NIS2.

Po szóste, egzekwowanie obowiązków, czyli kary (motyw 129 i 133 oraz art. 20 ust. 1 i art. 34). W przypadku dyrektywy NIS2 kary mogą być nakładane na podmiot (kluczowy – o maksymalnej wielkości co najmniej 10 milionów euro lub 2% łącznego światowego obrotu; ważny – odpowiednio 7 milionów euro lub 1,4% łącznego światowego obrotu; przy czym zastosowanie ma kwota wyższa) oraz na członków organu zarządzającego. Co więcej, jak zapisano w motywie 133, „aby jeszcze bardziej wzmocnić skuteczność i odstraszający charakter środków egzekwowania przepisów mających zastosowanie do naruszeń niniejszej dyrektywy, właściwe organy powinny być uprawnione do tymczasowego zawieszenia certyfikacji lub zezwoleń dotyczących części lub całości odpowiednich usług świadczonych przez podmiot niezbędny lub prowadzonej przezeń działalności oraz do żądania nałożenia tymczasowego zakazu sprawowania funkcji zarządczych przez osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego". Jak wskazano w treści przepisów, kary powinny być skuteczne, proporcjonalne i odstraszające. W tym przypadku mamy ewidentnie do czynienia z pewnym *novum*. Należy jednak pamiętać o jeszcze jednym aspekcie egzekwowania prawa. Kara, aby była skuteczna, powinna przede wszystkim być nieunikniona. Wtedy dopiero jej odstraszający charakter będzie oddziaływał.

Po siódme, wiedza i umiejętności. W przypadku organów zarządzających podmiotów kluczowych i ważnych w art. 20 ust. 2 wprowadzono zobowiązanie następującej treści: „Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom." Zapis ten utrudni członkom organów zarządzających ekskulpowanie. Ostatecznie, nikt pod przymusem nie zostaje członkiem organów zarządzających. Niestety, nieco „zapomniano" o organie nadzoru. Jedynie w art. 31 ust. 1 zapisano „państwa członkowskie zapewniają, aby ich właściwe organy skutecznie monitorowały przestrzeganie niniejszej dyrektywy i stosowały środki niezbędne do zagwarantowania tego przestrzegania".

Tu rodzi się pytanie, czy i w jakim stopniu „bazując na wiedzy i umiejętnościach już zdobytych w związku z dyrektywą (UE) 2018/1972 w odniesieniu do środków bezpieczeństwa i zgłaszania incydentów" (motyw 95) organ nadzoru jest przygotowany, aby skutecznie monitorował przestrzeganie dyrektywy NIS2?

Obecnie, zgodnie z art. 15 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa „operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej". Za nieprzeprowadzenie tego audytu operator usługi kluczowej może być ukarany karą pieniężną w wysokości od 15 tys. do 200 tys. złotych (art. 73 ustawy o ksc). Jest to co najmniej o kilka rzędów wielkości mniejsza kara niż przewidziana w dyrektywie NIS2. Ale problem nie leży w wysokości kary,

7 Ang. *to share*; zamiast ang. *to transfer*

8 z góry, przed wydarzeniem się czegoś (https://sjp.pwn.pl/sjp/ex-ante;2557307.html)

9 po (fakcie), później (https://sjp.pwn.pl/sjp/ex-post;2458197.html)

zwłaszcza że jej nie wymierzano. Nie wiadomo (jawnie), co robi obecnie organ nadzoru z wynikami tych audytów: w jaki sposób je wykorzystuje i w jakim celu? Jakie wnioski, o których mowa w motywie 95, wyciągnął?

Nie wiadomo także, na jakiej podstawie opublikowany został tzw. szablon sprawozdań z audytu dla operatorów usług kluczowych[10]. Podstaw do takiej publikacji nie ma w żadnym akcie normatywnym związanym z ustawą o krajowym systemie cyberbezpieczeństwa.

Obecnie organ nadzoru scedował prawa do wykonywania audytów bezpieczeństwa na akredytowaną jednostkę oceniającą zgodność, sektorowy zespół cyberbezpieczeństwa oraz osoby fizyczne, które posiadają praktykę (nie wiadomo do końca jak udokumentowaną) lub certyfikat określony we właściwym rozporządzeniu. Nigdzie nie określono żadnej odpowiedzialności tych osób lub jednostek z tytułu wad wykonanych przez nich audytów. Co więcej, lista ta zawiera nie tylko certyfikaty z zakresu audytu (np. CISA), lecz również z zakresu zarządzania (np. CISM). Umiejętności wykonywania audytu odbiegają od wymagań w zakresie zarządzania. Certyfikaty nie tylko istotnie różnią się w zakresem przedmiotowym (rodzaj wiedzy i umiejętności), ale przede wszystkim zakresem odpowiedzialności zawodowej. Np. certyfikat CISA wymaga przestrzegania kodeksu etyki oraz regularnej aktualizacji wiedzy (tzw. CPE[11]) pod rygorem utraty certyfikatu. Jest to certyfikat nastawiony na samodzielne wykonywanie pracy. Natomiast np. certyfikat audytora wiodącego ISO/IEC 27001 nie wymaga przestrzegania kodeksu etyki czy regularnej aktualizacji wiedzy, gdyż jest skierowany do osób wykonujących zadania w organizacjach podlegających takim regułom w ramach programów akredytacji. Co więcej, uzyskanie certyfikatu CISA wymaga udokumentowanej wiedzy i doświadczenia w zakresie IT, natomiast certyfikat audytora wiodącego ISO/IEC 27001 nie posiada takiego wymagania. Stąd wniosek, że lista certyfikatów ujęta w rozporządzeniu nie zapewnia żadnej równoważności kryteriów wyboru. Zdradzając nieco „kuchni", propozycja opierała się na liczbie dostępnych „zbliżonych" certyfikatów „aby nie ograniczać rynku". Innymi słowy, dobro operatora usługi kluczowej zwyciężyło w starciu ze skutecznością regulacji. Więcej na temat tak realizowanych audytów przez „certyfikowanych audytorów, o których mowa w Rozporządzeniu", można przeczytać w artykule „Audyt za 1 zł"[12] opublikowanym w numerze 3/2023 „Domeny".

Bardzo obawiam się o skuteczność działania organów nadzoru. Nie wszyscy dziś pamiętają rok 2002, w którym wybuchła w Stanach Zjednoczonych afera Enronu. Firmę tę audytowała firma z ówczesnej tzw. Wielkiej Piątki, Arthur Andersen. Na skutek poświadczenia nieprawdy po 90 latach firma przestała istnieć, gdyż została uznana za winną niszczenia dowodów, a rząd Stanów Zjednoczonych przyjął Sarbanes–Oxley Act (SOX) celem poprawy nadzoru nad firmami. My ostatnio mieliśmy „własny Enron", czyli aferę GetBack. W sprawozdaniach finansowych „nic nie widział" Deloitte Audyt, firma z tzw. Wielkiej Czwórki[13]. Co prawda z dużym opóźnieniem, ale jednak, Deloitte Audyt dostał trzyletni zakaz badania sprawozdań finansowych. Karę nałożyła Polska Agencja Nadzoru Audytowego[14]. Pod koniec października 2023 r. Wojewódzki Sąd Administracyjny w Warszawie wstrzymał wykonanie decyzji Polskiej Agencji Nadzoru Audytowego w zakresie nałożenia kary zakazu świadczenia usług przez Deloitte Audyt. Jak możemy przeczytać: „Sąd zwraca uwagę na istotny szczegół. Bowiem po wykonaniu decyzji, jej ewentualne uchylenie przez sąd administracyjny nie miałoby już dla funkcjonowania skarżącej spółki istotnego znaczenia. Trudno byłoby przywrócić stan sprzed decyzji". Na dzień pisania tego artykułu, wyrok WSA nie jest prawomocny, a – przypomnijmy – afera GetBack wybuchła 5 lat temu. W jej efekcie 9 tys. obligatariuszy straciło prawie 3 mld zł. Zarząd GetBacku fałszował księgi, ukrywał straty i doprowadził firmę do spektakularnej plajty.

Teraz pozostało nam już tylko czekać. Odpowiedzi na pytania otwierające moje dywagacje powinny nadejść w ciągu najbliższych miesięcy.

10 https://www.gov.pl/web/baza-wiedzy/szablony-audytu-dla-operatorow-uslug-kluczowych

11 Od Continuing Professional Education – program wymagający podejmowania systematycznych aktywności edukacyjnych kwalifikowanych do określonej liczby punktów CPE. Zazwyczaj punkty rozliczane są w okresie 3-letnim (np. 120), przy czym wymagane jest corocznie zdobycie minimalnej liczby CPE (np. 20).

12 https://portal.pti.org.pl/wp-content/uploads/2023/10/10_Audyt-za-1zl.pdf

13 Po upadku Arthur Andersen, tzw. Wielka Piątka stała się tzw. Wielką Czwórką, w skład której wchodzą obecnie: Deloitte, EY, KPMG, PWC.

14 Polska Agencja Nadzoru Audytowego (PANA) działa na podstawie ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym. PANA jest właściwym organem w rozumieniu rozporządzenia UE nr 537/2014 z dnia 16 kwietnia 2014 r. w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego, uchylającego decyzję Komisji 2005/909/WE, w zakresie niezastrzeżonym dla innych organów. Cyberbezpieczeństwo w rozumieniu dyrektywy NIS nie leży w zakresie kompetencji PANA. W zakresie cyberbezpieczeństwa nie ma odpowiednika PANA.

Walidacja podpisów kwalifikowanych

Stosowanie kwalifikowanych podpisów elektronicznych rozwiązuje wiele problemów, z którymi borykano się przy dokumentach papierowych. Nie tylko wzrosła wygoda i szybkość obiegu dokumentów, lecz również wyeliminowano problem fałszerstw, podrabiania podpisów czy antydatowania dokumentów. W teorii użytkownik otrzymując dokument elektroniczny, uruchamia odpowiedni program i uzyskuje informacje, kto podpisał dany dokument, czy podpisy są ważne oraz czy dokument nie został zmodyfikowany po podpisaniu. Niestety, w praktyce sprawa jest bardziej skomplikowana niż na pierwszy rzut oka wygląda.

W rozporządzeniu eIDAS (https://digital-strategy.ec.europa.eu/pl/policies/eidas-regulation) w artykule 18 czytamy: „Podpis elektroniczny lub pieczęć elektroniczna weryfikowane za pomocą certyfikatu wywołują skutki prawne, jeżeli zostały złożone w okresie ważności tego certyfikatu". Ta prosta i oczywista zasada jest jednak trudna do zastosowania w praktyce.

Artur Krystosik

dyrektor Działu Rozwoju Produktów w Enigma Systemy Ochrony Informacji Sp. z o.o. Wieloletni pracownik naukowy Instytutu Informatyki Politechniki Warszawskiej. Twórca i współtwórca większości rozwiązań firmy bazujących na technologii PKI. Bierze czynny udział w życiu naukowym w kraju i za granicą. Autor wielu publikacji naukowych. Prywatnie kapitan jachtowy i taternik.

Problem z datą powstania podpisu

Po pierwsze, skąd mamy wiedzieć, kiedy został złożony podpis? Uzyskanie ścisłej informacji jest niemożliwe, gdyż podpis elektroniczny nie zawiera prawnie wiążącej daty jego powstania, a stosowanie znakowania czasem odbywa się już po złożeniu podpisu. Oczywiście różnica w czasie może być nieduża, liczona w sekundach, ale o tym, że są to sekundy, a nie godziny czy nawet dni, wie tylko podpisujący. Na szczęście ten brak precyzji nie ma dużego wpływu na proces weryfikacji.

> *Jeśli bowiem wykażemy, że certyfikat był ważny w momencie oznakowania czasem podpisu, to oznacza również, że był ważny wcześniej (w szczególności w momencie złożenia podpisu), gdyż raz unieważniony certyfikat nie może ponownie stać się ważny.*

A co jeśli podpisujący nie oznakował czasem dokumentu? W takim przypadku dowodem może być fakt wpłynięcia podpisanego dokumentu do odbiorcy. Posiłkując się zapisami kancelaryjnymi czy logami z serwerów poczty, można wykazać, że w danym momencie dokument już istniał. Niestety, ciężar takiego dowodu spoczywa na odbiorcy dokumentu. Z upływem lat, w wyniku kasowania logów, usuwania starej poczty itp. może stawać się on coraz trudniejszy do przeprowadzenia.

Aby temu zaradzić, odbiorca dokumentu może samodzielnie znakować wpływające dokumenty czasem (jeśli nie są oznaczone). Jest to jednak dodatkowy nakład pracy, koszt, a co gorsza znakowanie czasem nie rozwiązuje problemu ostatecznie. Wynika to z faktu, że znakowanie czasem również

posługuje się certyfikatami, których okres ważności wynosi około 9–11 lat. Po upływie tego czasu znacznik przestaje być ważny, a użytkownik traci kryptograficzny dowód istnienia dokumentu. Wymyślono rozwiązanie i dla tego problemu. Podpisane dokumenty elektroniczne mogą być poddawane procesowi tzw. konserwacji. Polega on na tym, że przed upływem okresu ważności znacznika czasu (ściślej: certyfikatu znacznika czasu) wszystkie oznakowane czasem dokumenty opatrywane są kolejnym znacznikiem czasu, ważnym następne 9-11 lat, co przedłuża okres ważności dowodu istnienia dokumentu. Proces ten musi być powtarzany przez tyle lat, przez ile wymagana jest zdolność do udowodnienia ważności podpisanego dokumentu. Trudno sobie jednak wyobrazić, żeby te wszystkie czynności były wykonywane manualnie. Niezbędny jest do tego sprawny system przechowywania dokumentacji elektronicznej, wyposażony w takie funkcje i mający stały dostęp do dokumentów (a co z archiwami na taśmach?). Jak widać, oddalamy się od prostej aplikacji z jednym klawiszem, a to dopiero początek problemów.

Ważność certyfikatu

Zajmijmy się teraz drugą częścią artykułu 18 rozporządzenia eIDAS, czyli określeniem ważności certyfikatu zakładając, że dysponujemy posiadającą moc dowodową datą istnienia podpisu. Teoretycznie informacja o ważności certyfikatu jest łatwo dostępna. Sam certyfikat posiada zapisany w sobie okres ważności, który łatwo jest porównać z datą istnienia podpisu, a dostawcy usług zaufania publikują informacje o unieważnieniach w postaci list CRL czy usług OCSP[1].

Normy ETSI odnoszące się do weryfikacji podpisu definiują następujące wyniki weryfikacji podpisu:

- **Pozytywny oznaczający w szczególności, że certyfikat użyty do złożenia podpisu był ważny w momencie jego składania.**
- **Negatywny, którego jedną z przyczyn może być fakt nieważności certyfikatu w momencie składania podpisu.**
- **Nieokreślony, którego najczęstszą przyczyną jest brak możliwości określenia ważności certyfikatu w momencie składania podpisu. Wynik ten może ulec zmianie, np. jeśli otrzymamy nowszą niż posiadana listę CRL.**

Powodem braku możliwości określenia ważności certyfikatu zwykle jest brak odpowiednio świeżej informacji o unieważnieniach, czyli listy CRL lub odpowiedzi OCSP. Co to jest odpowiednio świeża informacja? Warunkiem uzyskania ostatecznego wyniku weryfikacji (tj. wyniku pozytywnego lub negatywnego) jest zapewnienie, aby:

1) data wystawienia listy CRL lub odpowiedzi OCSP była późniejsza niż data istnienia podpisu oraz

2) lista CRL/odpowiedź OCSP zawierała unieważnienia z okresu ważności certyfikatu.

Warunek pierwszy wynika z wymagania, że nowo wydana lista CRL nie może zawierać nowo dodanych informacji o unieważnieniach, które byłyby wcześniejsze niż data poprzednio wydanej listy CRL. Innymi słowy na listę CRL nie mogą trafiać unieważnienia antydatowane, czyli takie, które powinny znajdować się już na poprzedniej liście. Dzięki tej zasadzie – dysponując listą CRL późniejszą niż data złożenia podpisu – mamy pewność, że żadna nowa lista CRL nie zmieni statusu ważności certyfikatu na dzień złożenia podpisu, a więc wynik weryfikacji jest ostateczny.

Warunek drugi wynika z faktu, że ogromna większość dostawców usług zaufania na listach CRL publikuje wyłącznie certyfikaty znajdujące się w okresie ważności. Informacje o pozostałych certyfikatach są usuwane z list CRL celem ograniczenia ich rozmiaru.

Jakie ma to wszystko konsekwencje dla procesu weryfikacji? Po wpłynięciu dokumentu użytkownik musi czekać na pojawienie się takiej listy, aby proces weryfikacji dał wynik rozstrzygający. W zależności od dostawcy może to być od kilkunastu minut (CenCert publikuje listy CRL co 20 minut) do nawet kilkunastu godzin. Użytkownik (a właściwie jego oprogramowanie) może również skorzystać z usługi OCSP, o ile taka usługa jest przez danego dostawcę świadczona, co – niestety – nie jest regułą w krajach EU (wszyscy polscy dostawcy usług zaufania taką usługę świadczą, choć nie wszyscy robią to w sposób pozwalający wygodnie i wiarygodnie z niej skorzystać). Spełnienie warunku drugiego jest szczególnie trudne, gdy chcemy dokonać weryfikacji podpisu złożonego wiele lat temu. W tym celu musielibyśmy dysponować listą CRL wydaną w okresie ważności certyfikatu. Ponieważ archiwalne listy CRL nie są udostępniane za pomocą zestandaryzowanego mechanizmu, to ich zdobycie wymaga indywidualnego kontaktu z dostawcą usługi zaufania.

1 OCSP (ang. *Online Certificate Status Protocol*) – standard opisujący protokół komunikacyjny pomiędzy systemem informatycznym odbiorcy usług certyfikacyjnych a serwerem usługowym. Protokół ten określa format i strukturę zapytania (żądania) o status certyfikatu oraz format i strukturę odpowiedzi (tokenu), która zawiera wynik weryfikacji w postaci statusu: „poprawny", „unieważniony", „nieznany".

Rozwiązaniem może być skorzystanie z OCSP, jeśli dany dostawca udostępnia za pomocą tego protokołu informacje o certyfikatach spoza okresu ich ważności, co również nie jest regułą.

Wiarygodność dokumentu

Czy jeśli użytkownik uzyska pozytywny wynik weryfikacji wszystkich podpisów, to może on zaakceptować dokument jako wiarygodny? Niestety, nie. Niektóre formaty danych, takie jak XML czy PDF, pozwalają w jednym dokumencie umieścić dane podpisane i niepodpisane, a także obejmować podpisami różne obszary danych. Można sobie wyobrazić, że jedna strona podpisała umowę, a druga wprowadziła do niej zmiany i podpisała ją ze swojej strony. Graficznie dokument wygląda jakby był podpisany zgodnie przez obie strony, lecz faktycznie tak nie jest.

Format PDF pozwala również na umieszczenie w dokumencie aktywnej zawartości, czyli skryptów uruchamianych podczas prezentacji dokumentu. Zwykle służą one do programowania zachowania formularzy, ale mogą być również używane do zmiany prezentowanych na ekranie treści. Niestety, popularne oprogramowanie do weryfikacji podpisów na ogół nie wykrywa takich zagrożeń, pozostawiając to zadanie aplikacjom przeznaczonym do wizualizacji danego formatu (Acrobat Reader potrafi sygnalizować takie sytuacje, ale nie jest to zbyt czytelne).

Jak widać, dokonanie weryfikacji podpisanego dokumentu wcale nie jest zadaniem łatwym. Zważywszy, że:

- dzisiaj podpisy mogą pochodzić z całej Unii Europejskiej,
- podpisane dokumenty często zawierają rozmaite usterki,
- podpisy czasem nie są w pełni zgodne z normami, z którymi powinny być zgodne,
- programy do weryfikacji podpisów niejawnie przyjmują założenia wpływające na wynik weryfikacji,
- w implementacjach zdarzają się błędy,

widać, z jaką skalą trudności się mierzymy. Praktyka pokazuje, że użytkownicy mają z tym duży problem. Regułą jest stosowanie kilku programów do weryfikacji i porównywanie ich wyników, jak również korzystanie z porad ekspertów w wątpliwych i szczególnie ważnych przypadkach.

Problemami weryfikacji zajmują się również sądy i inne organy. W 2019 r. KIO wydała orzeczenie, w którym wskazała, że opatrzenie oferty podpisem kwalifikowanym wykorzystującym algorytm SHA-1 jest dopuszczalne i nie stanowi przesłanki do odrzucenia oferty. Wspominam o tym dlatego, że stosowanie SHA-1 bywa przyczyną weryfikacji nierozstrzygającej (bezpieczeństwo algorytmu zostało podważone, zademonstrowano dwa różne dokumenty posiadające sensowną i kontrolowaną przez napastnika treść i ten sam skrót SHA-1), ale na gruncie obowiązującego prawa nie można takiego dokumentu odrzucić.[2]

Dużym problemem podczas weryfikacji jest fakt, że podpisy często składane są za pomocą oprogramowania, które nie spełnia norm i standardów albo wymaga specjalnej konfiguracji, o czym przeciętny użytkownik nie ma pojęcia. Przykładowo, domyślnym trybem podpisywania w aplikacji Acrobat Reader (wersja 2023.006.20320) jest tryb niezgodny z eIDAS. Sprawia to, że certyfikat osoby podpisującej nie jest obejmowany podpisem. Jeśli dysponowalibyśmy dwoma certyfikatami wystawionymi na ten sam klucz publiczny, ale zawierającymi różne dane osobowe, to nie dałoby się stwierdzić, kto jest faktycznym autorem dokumentu. Tryb ten można oczywiście zmienić w konfiguracji, tylko kto o tym wie? Problem prawdopodobnie dotyczy ogromnej większości dokumentów podpisanych za pomocą tego oprogramowania.

Sztuka przewidywania

Załóżmy jednak, że użytkownik pokonał wszystkie rafy i używany przez niego program poprawnie zweryfikował podpisy pod dokumentem. Czy to koniec problemów? Odpowiedź na to pytanie wymaga rozważenia dwóch kwestii:

1. Co zrobić, jeśli po upływie pewnego czasu od momentu weryfikacji dokumentu dojdzie do sporu i zajdzie konieczność wykazania, że faktycznie kiedyś uzyskano pozytywny wynik weryfikacji? Narzucającym się rozwiązaniem jest użycie tego samego programu i ponowne wykonanie weryfikacji. Pytanie tylko, czy mimo upływu czasu program na pewno zwróci ten sam wynik? Niestety, mogą zdarzyć się sytuacje, w których wynik weryfikacji będzie inny niż w przeszłości. Przyczyną może być np. wygaśnięcie certyfikatu użytkownika podpisującego dokument, wygaśnięcie certyfikatu znacznika czasu czy

2 Jeśli przyjąć, że algorytm SHA-1 nie gwarantuje cechy, że podpis jest „powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna" (wymaganie z art. 26 pkt d eIDAS), to oznacza, że podpis z SHA-1 nie jest „zaawansowany", a więc nie jest też „kwalifikowany". Jest więc mechanizm prawny na usuwanie z obrotu niebezpiecznych algorytmów, ale w tej konkretnej sprawie KIO zdecydowała inaczej.

unieważnienie certyfikatu użytkownika, jeśli stosowane oprogramowanie przyjmuje czas bieżący jako datę złożenia podpisu, co się często zdarza.

2. W jaki sposób utrwalić wynik weryfikacji, aby miał on własności dowodowe i mógł być przedstawiony w sądzie? Pytanie to jest zasadne zwłaszcza w świetle negatywnej odpowiedzi na pytanie pierwsze.

Oczywiście i te kwestie daje się rozwiązywać, choćby środkami organizacyjnymi, ale jest to kolejna rzecz, o którą należy zadbać, a przecież wydawało się, że wystarczy nacisnąć jeden klawisz.

W celu zweryfikowania dokumentu należy:

- **Zadbać o posiadającą moc dowodową datę istnienia podpisanego dokumentu.**
- **Zadbać o dostęp oprogramowania weryfikującego do odpowiedniej informacji o unieważnieniach (w tym historycznych).**
- **Sprawdzić, czy mimo ważności podpisów dokument nie został zmanipulowany.**
- **Zadbać o utrwalenie wyników weryfikacji tak, aby miały one moc dowodową w przyszłości, lub zapewnić, że dokument będzie się weryfikował w przyszłości, dając identyczny wynik weryfikacji (np. poprzez przekształcenie dokumentu do tzw. postaci archiwalnej oraz okresową konserwację znaczników czasu).**

Warto korzystać z usług walidacji

Wychodząc naprzeciw problemom weryfikacji podpisów elektronicznych, eIDAS zdefiniował kwalifikowaną usługę walidacji dokumentów, która ma zdjąć z użytkownika większość przedstawionych tu problemów. Obecnie w Polsce działają dwaj tacy usługodawcy na terenie państw UE jest ich jeszcze kilku. Korzystanie z usługi walidacji jest bardzo łatwe. Użytkownik przesyła dokument, który chce zwalidować, a dostawca usługi wykonuje wszystkie niezbędne kroki procesu walidacji, zwracając raport na ogół w formacie PDF.

Raport określa m.in.:

- liczbę i rodzaj podpisów oraz pieczęci. Usługi krajowe powinny rozróżniać podpisy/pieczęcie kwalifikowane oraz niekwalifikowane pochodzące od dostawców usług zaufania z krajów UE umieszczonych na listach zaufanych usług TSL, polskie podpisy osobiste wykonane dowodem osobistym oraz podpisy platformy ePUAP;
- status weryfikacji każdego z podpisów (pozytywny, negatywny lub nieokreślony);
- dane osobowe poszczególnych sygnatariuszy;
- szczegóły walidacji poszczególnych podpisów, a jeśli wynik walidacji jest inny niż pozytywny – listę przyczyn takiego stanu.

W zależności od dostawcy usługi taki raport może zawierać także ostrzeżenia o możliwych manipulacjach treścią dokumentu (aktywna zawartość, obszary niepodpisane czy podpisy obejmujące różne obszary dokumentu).

Raporty opatrywane są pieczęcią elektroniczną usługi walidacji i z mocy eIDAS mają bezpośrednią wartość dowodową. Przechowanie raportu wraz z dokumentem eliminuje potrzebę ponownej weryfikacji dokumentu w przyszłości. Odpadają więc problemy przekształcania dokumentów do postaci archiwalnej i konserwacji podpisów. Przy czym należy pamiętać, że konserwując podpisy pod dokumentem gwarantujemy, że dokument będzie w przyszłości bez problemu walidowany. Natomiast przechowując raport gwarantujemy zachowanie dowodu dołożenia należytej staranności i uzyskania właściwego wyniku walidacji, czego nie daje nam sama usługa konserwacji.

Wysłanie dokumentu do walidacji nie oznacza, że dokument musi być przesyłany na serwery usługodawcy. Po stronie klienta może być zainstalowana tzw. bramka, do której za pośrednictwem aplikacji webowej użytkownicy przekazują dokumenty. Bramka pobiera z dokumentu podpisy, oblicza wymagane skróty z danych i przesyła je do serwerów usługodawcy, gwarantując, że żadne dane należące do klienta nie opuszczają infrastruktury klienta. Na podstawie przesłanych danych realizowana jest walidacja dokumentu. Służy do tego dedykowane oprogramowanie walidacyjne, którego zadaniem jest realizacja wszystkich kroków niezbędnych do uzyskania rozstrzygającego wyniku walidacji. Serwery usługi automatycznie pobierają niezbędne informacje o unieważnieniach. W przypadku braku wystarczająco świeżej informacji aktywnie oczekują na jej dostępność, co uwalnia użytkownika od konieczności ponawiania procesu walidacji. Dla walidacji dokumentów historycznych oprogramowanie może sięgać do archiwum gromadzącego listy CRL pochodzące o dostawców usług zaufania całej Unii Europejskiej. Usługi walidacji są dostępne również w formie uproszczonej, która nie wymaga instalacji po stronie klienta żadnego oprogramowania. W takim przypadku wymagane jest przesyłanie całych dokumentów na serwery usługodawcy. Zwykle odbywa się to poprzez stronę www.

Czy usługi walidacji to panaceum na wszystkie problemy walidacji dokumentów? Oczywiście nie, ale są one znacznym ułatwieniem w codziennej pracy z dokumentami elektronicznymi.

Oszukać system

„System" jest pojęciem bardzo pojemnym, stąd nasze skojarzenia z tym słowem są różne, zależnie od doświadczenia. Im to doświadczenie jest bogatsze, tym częściej skojarzenia ze słowem „system" są bardziej negatywne i rodzą myśl „jak oszukać system", gdyż wszystkie „systemy" mniej lub bardziej utrudniały nam życie.

Każdy „system" ma swoje zarówno dobre, jak i złe strony. Był „system sprawiedliwości społecznej w bloku socjalistycznym", o którego „zaletach" część już chyba zapomniała (gdyż sądząc po sympatiach politycznych, duża część społeczeństwa tęskni za jego powrotem), a część w nie uwierzyła, chociaż nie widziała i chciałaby spróbować (tylko dlaczego kosztem innych).

Jest „system" w biologii (obejmujący narządy lub inne części żywego organizmu pełniące razem określoną funkcję), prawie, matematyce lub innej dziedzinie, którego nauczenie się spędzało wielu osobom sen z powiek.

Jest też „system" w informatyce, który często nie działa tak, jak tego oczekiwano i trzeba to jakoś obejść. „System" ten kosztował zazwyczaj „duże" pieniądze, a jego zmiana i dopasowanie będą kosztowały jeszcze więcej. Stąd trzeba „oszukać system", czyli coś zrobić w sposób, którego nie przewidziano. Każdy z nas miał już podobne doświadczenia z „systemem IT". Dlatego jak ktoś zaczyna mówić o konieczności zbudowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), bo ustawa o krajowym systemie cyberbezpieczeństwa, a poza tym jakiś NIS2, to wielu osobom zapala się czerwona lampka.

Fałszywe skojarzenia

Pierwsze: bezpieczeństwo informacji = bezpieczeństwo informatyczne (bo IT, czyli *Information Technology*, tłumaczy się na język polski jako informatyka). Czyli: informatycy znów chcą wydać pieniądze na kolejny system. Nakupią

sprzętu i oprogramowania, a później będą jeszcze chcieli się ciągle szkolić (pieniądze) i stwierdzą, że potrzebują jeszcze kolejnych etatów (pieniądze) i kolejnych serwerów czy innych macierzy i przełączników (pieniądze). I tu pojawia się pierwszy pomysł „jak oszukać system" – a może kupimy certyfikat? Nie wystarczy? Ile może kosztować wydanie „kwitu" (na pewno taniej niż te ich „systemy")? Powiesi się na ścianie i będzie pięknie (pani Zosia zamówi ładne ramki i dopilnuje, aby wisiało we wszystkich eksponowanych miejscach).

Kolejne, również niestety fałszywe skojarzenie: bezpieczeństwo = zabezpieczenia (zgodne z listą zawartą w załączniku normatywnym A). Czyli: przeczytałem normę i generalnie wszystko mamy, co najwyżej potrzebna będzie jakaś dokumentacja (ładnie nazywana w normie „udokumentowanymi informacjami"). Generalnie lektura norm nie jest frapująca, a ich suchy, sformalizowany język bardziej przypomina lekturę książki telefonicznej niż bestselera w naszym ulubionym gatunku. Dlatego każdy zaczynający taką lekturę będzie skupiał się na obszarach, które są dla niego bliskie. Stąd informatycy skupią się na zabezpieczeniach informatycznych, pomijając pozostałą, trudną w odbiorze treść. Dodatkowo sama informacja, że załącznik ma charakter normatywny, zwiedzie ich i założą, iż pozostała treść ma jedynie walor informacyjny.

Tymczasem to treść normy zawiera zbiór wymagań, które stanowią podstawę wdrożenia systemu (systemu zarządzania, a nie systemu zabezpieczeń). Załącznik (normatywny) A wskazuje jedynie minimalny zbiór zabezpieczeń, których celowość oraz sposób wdrożenia należy rozważyć na podstawie analizy ryzyka i nadzorować ich skuteczność i adekwatność mechanizmami systemu zarządzania.

Kolejne, również niestety fałszywe skojarzenie: system = dokumentacja systemu. Czyli zróbmy audyt i niech audytorzy przygotują dokumentację, bo przy okazji audytu poznają, jak to u nas działa i będą wiedzieli, czego brakuje (podobno znają się na „systemie" i jego wymaganiach). W ten sposób przygotują nas do certyfikacji. W ten sposób „oszukamy system", bo będziemy mieć i audyt, i dokumentację za jednym zamachem (obydwa te hasła przewijają się w normie). Brawo my!

Audyt ma za zadanie dostarczyć niezależną ocenę, w tym przypadku zgodności SZBI z wymaganiami normy EN ISO/IEC 27001 (nadzór). Audytor powinien wskazać obszary wymagające podjęcia działań następczych (korygujących), lecz nie powinien wskazywać, w jaki sposób należy te działania zrealizować. Za to odpowiedzialna jest osoba, która zarządza tym obszarem.

Takie, niestety nieodosobnione, myślenie wskazuje, iż świadomość w zakresie podstawowych zasad zarządzania[1] (ang. *governance*) nie jest powszechna.

1. **Zarządzanie przede wszystkim powinno być skuteczne (skutecznie osiągać cele), a w perspektywie doskonalenia również efektywne, czyli nie tylko skutecznie osiągać cele, lecz również w sposób optymalny (minimalizując szeroko rozumiane koszty operacyjne).**

2. **Zarządzanie powinno uwzględniać ryzyko prowadzenia działalności, w szczególności w zakresie:**

   a) **przestrzegania prawa (ryzyko prawne związane z interpretacją przepisów skutkujących możliwością ponoszenia kar);**

   b) **etyki postępowania (ryzyko utraty wizerunku (zaufania interesariuszy) lub ryzyko prowadzenia sporów (obsługi roszczeń));**

   c) **nadużyć (ryzyko konfliktu interesów, w tym w szczególności rozdzielenie nadzoru (ang. *governance*) od zarządzania (ang. *management*)).**

> *Włączenie audytora (nadzór) do zarządzania pozbawia go atrybutu niezależności.*

Należy jeszcze raz podkreślić, że w przypadku systemu zarządzania istotą jego oceny jest skuteczność, a nie dokumentacja. Dokumentacja jest jednym ze środków pozwalających na osiągnięcie skuteczności poprzez zapewnienie komunikacji, która jest niezbędna dla efektywnej współpracy wszystkich zaangażowanych stron.

Jak zatem „oszukać system"? Może kupić gdzieś taką „sprawdzoną" dokumentację? Wtedy można wybrać kilka „kluczowych"[2] osób, które nauczą się jej na pamięć i będą opowiadać audytorom, jak to wspaniale działa nasz system. Teoretycznie może się to udać, ale na krótką metę.

1 W polskim systemie prawnym (ustawa o finansach publicznych) występuje pojęcie „kontroli zarządczej" odpowiadające angielskiemu pojęciu „governance".

2 Oszukując system, mamy na myśli osoby, których brak nie będzie dla organizacji odczuwalny, ale z różnych względów organizacja nie może się z nimi rozstać.

Jak zatem zbudować SZBI, aby miał więcej zalet niż wad? Od czego zacząć? Komu zaufać?

Element zarządzania

Po pierwsze, należy założyć, że SZBI jest jednym z elementów systemu zarządzania organizacją, a bezpieczeństwo informacji jest jednym z aspektów jej działalności. SZBI nie może być odrębnym bytem, lecz elementem każdego z aspektów działalności organizacji.

Po drugie, system zarządzania wymaga przywództwa. Kierownictwo powinno być zaangażowane w ten system, czyli powinno wskazywać kierunki i cele, zapewniać zasoby oraz interesować się osiąganymi wynikami. System wymaga lidera, a nie karbowego.

Po trzecie, wszyscy interesariusze powinni nie tylko wiedzieć, czemu ma system służyć (zakres, cele, wymagania) i jaka jest ich rola w systemie (uprawnienia i odpowiedzialność), lecz przede wszystkim osiągnąć konsensus w tym zakresie, tak aby w przyszłości nie podważać założeń systemu. Oczywiście z biegiem czasu zakres, cele, wymagania, uprawnienia i odpowiedzialność mogą ulegać zmianie. Zawsze jednak zmiana ta powinna przebiegać w sposób kontrolowany i uzgodniony.

System wymaga zbudowania na bazie zasobów organizacji, a nie według szablonów lub innych gotowych opracowań. Dobry dostawca powinien być mentorem, coachem, który przekazuje organizacji wiedzę, i – obserwując – dobiera najlepsze w danym przypadku rozwiązania. Jego zadaniem jest niejako „wbudowanie" systemu w organizację. A organizacja musi się zmienić tak, aby przyjęła system jako swój sposób działania.

Łatwiej zatem powiedzieć, komu nie ufać. Każdy, kto oferuje „gotowy system" (z pudełka) lub mówi, że jest to zadanie proste i niewymagające zaangażowania ze strony organizacji, zachowuje się nieetycznie. Mówi to, co zarządzający chcieliby usłyszeć, lecz jest to jedynie sposób na uzyskanie zamówienia. Jest to zarazem sposób na oszukanie systemu udzielania zamówień (czyli *de facto* oszukanie klienta).

Paweł Henig

Uniwersalna recepta na SZBI nie istnieje. Każdy system wymaga dopasowania do specyfiki organizacji. Dopasowanie powinno uwzględniać wszystkie tzw. czynniki umożliwiające (ang. *enabler*).

Można wyróżnić siedem podstawowych czynników umożliwiających.

1. **Zasady, polityki i metodyki są środkami przekładającymi pożądane zachowania na praktyczne wskazówki w codziennym zarządzaniu.**
2. **Procesy opisują zorganizowany zestaw praktyk i działań zmierzających do osiągnięcia określonych celów i wytworzenia zestawu produktów wspierających osiągnięcie ogólnych celów związanych z bezpieczeństwem informacji.**
3. **Struktury organizacyjne są kluczowymi jednostkami wykonawczymi i decyzyjnymi w przedsiębiorstwie.**
4. **Kultura, etyka i zachowanie odnoszą się zarówno do jednostek, jak i do przedsiębiorstwa. Są często niedocenianym czynnikiem sukcesu w działaniach związanych z zarządzaniem i kierowaniem.**
5. **Informacje dotyczą wszystkich informacji wytwarzanych i wykorzystywanych przez przedsiębiorstwo. Informacje są niezbędne do zapewnienia funkcjonowania organizacji i dobrego zarządzania nią. Na poziomie operacyjnym informacja jest również często kluczowym produktem przedsiębiorstwa jako takiego. Informacje są podstawowym aktywem[3], którego własności, takie jak poufność, integralność i dostępność[4] pozwalają określić wymagania bezpieczeństwa.**
6. **Usługi, infrastruktura i aplikacje obejmują infrastrukturę, technologię i aplikacje, które zapewniają przedsiębiorstwu przetwarzanie informacji i usługi IT.**
7. **Ludzie, umiejętności i kompetencje są powiązane z osobami niezbędnymi do pomyślnego zakończenia wszystkich działań, w celu podejmowania właściwych decyzji i podejmowania działań naprawczych.**

Budując system, należy uwzględnić łącznie, w sposób wzajemnie uzupełniający się, wszystkie czynniki umożliwiające.

3 Aktywo = wszystko co ma wartość.

4 Dodatkowo można brać pod uwagę inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Najlepsi z najlepszych

– nagrodzone projekty inżynierskie

12 października 2023 r. mieliśmy okazję spotkać się z najlepszymi młodymi inżynierami IT – laureatami Ogólnopolskiego Konkursu PTI na najlepsze prace i projekty inżynierskie z informatyki. – *To niezmiernie istotna inicjatywa, bo dyplom inżyniera jest dowodem zdobycia umiejętności praktycznych, tak cenionych na rynku pracy* – podkreślił Prezes PTI Wiesław Paluszyński.

Uroczysty finał konkursu odbył się w siedzibie Instytutu NASK, który wpierał nas jako partner w organizacji konkursu. Jak wyglądała jego III edycja? Krótkie podsumowanie przedstawił Bartłomiej Śnieżyński, szefujący jury. Na konkurs wpłynęło 106 prac z 21 różnych uczelni; w ich ocenę zaangażowanych było 101 recenzentów – naukowców i ekspertów z całej Polski. Każda praca podlegała dwóm niezależnym recenzjom. Oceniano m.in. umiejętność analizy problemu, uzasadnienie wybranych rozwiązań oraz innowacyjność podejścia i możliwości wdrożenia. – *Tematyka prac była bardzo różnorodna – od aplikacji webowych i mobilnych po wykorzystanie sztucznej inteligencji, uczenia maszynowego i blockchain* – podkreślił Bartłomiej Śnieżyński.

Pierwsze miejsce jury przyznało autorom pracy **„Narzędzia wspierające uruchamianie modeli obliczeniowych z dziedziny medycyny in-silico”**, zrealizowanej na Wydziale Informatyki, Elektroniki i Telekomunikacji AGH. Karol Zając, Piotr Kica, Adam Nowak i Krzysztof Gądek rozwinęli aplikację służącą symulacjom medycznym prowadzonym na grupach (kohortach) pacjentów i stworzoną przez Cyfronet (Model Execution Environment). Praca była realizowana w ramach projektu In Silico World, we współpracy z krakowskim Centrum Sano. – *Główny cel naszego projektu zakładał zwiększenie wydajności aplikacji – szybszy i bezpieczniejszy dostęp do danych oraz wprowadzenie możliwości obliczeń równoległych dla BigData* – podsumował Krzysztof Gądek.

Dzięki pracy młodych inżynierów dane medyczne mogą być teraz przechowywane nie tylko w modelu HPC (*high performance computing*), ale także w chmurze, a operator bez problemu wybierze najdogodniejszy w danym momencie magazyn. Wszelkie obliczenia w systemie prowadzone są równolegle, można je uruchomić jednocześnie jednym kliknięciem. Udało się zrealizować także bardzo ambitne zadanie integracji różnych metod symulacji, przygotowanych przez specjalistów z całego świata (w formie osobnych usług). Do sprawdzania poprawności tych wszystkich modeli służy osobny moduł o bardzo wysokiej wydajności (uzyskanej nie tylko dzięki obliczeniom równoległym, ale także możliwości korzystania z mocy obliczeniowej usług serverless dowolnego dostawcy). Okazuje się, że zastosowanie tych rozwiązań najnowszej generacji nie było najtrudniejszym elementem pracy. – *Dużym wyzwaniem było połączenie rozmaitych systemów, z których niektóre były ultranowoczene, a inne miały charakter legacy. To sytuacja często spotykana w warunkach wdrożeniowych* – uznali zgodnie autorzy projektu.

Drugie miejsce w konkursie zdobył zespół z Politechniki Poznańskiej, który również zajął się usprawnianiem istniejącego systemu na potrzeby naukowców z całego świata. W projekcie **„RNAPDBEE 3.0: Webserwer do analizy struktur 3D RNA”** Kamil Niżnik, Paweł Śnioszek, Gabriel Wachowski i Mikołaj Żurawski pracowali nad moderniza-

cją aplikacji RNApdbee, służącej ona do przewidywania drugo- i trzeciorzędowej struktury RNA, co pozwala na określenie funkcji kwasu nukleinowego w organizmie. W dobie pandemii Covid i prac nad kolejnymi generacjami szczepionek system ten stał się niezmiernie popularny wśród biotechnologów.

– *Bardzo istotne było dla nas, że nasza praca nie będzie projektem tylko „do szuflady". Gdy tylko dowiedzieliśmy się, że jednym z celów jest rozbicie aplikacji monolitycznej na system w architekturze mikroserwisowej od razu stwierdziliśmy, że to projekt idealny dla nas. Koncept mikroserwisów jest bowiem bardzo często używany w branży webowej, w której na co dzień pracujemy* – podkreślał Gabriel Wachowski.

Autorzy podkreślają, że zmodernizowany system (RNApdbee 3.0) umożliwia naukowcom szybką i komfortową analizę, wizualizację oraz porównywanie uzyskanych wyników. Udało się wyeliminować konieczność żmudnej i czasochłonnej konfiguracji narzędzi, co zazwyczaj wymaga specjalistycznej wiedzy informatycznej. Dodatkowo użytkownik jest zwolniony z trudnego zadania przygotowywania danych w różnych formatach. Co więcej, otrzymuje on wyniki przedstawione w sposób przejrzysty i zilustrowany zgodnie z najlepszymi praktykami.

Trzecie miejsce w konkursie zdobyła praca studentów z Politechniki Warszawskiej – Zofii Wrony, Piotra Witkiewicza i Mikołaja Stańczyka: **„Explorations in practical aspects of autonomic computing"**. Jej przedmiotem było badanie mechanizmów autonomicznych i stworzenie systemu samoadaptującego się. Zmienność środowiska, do którego system musiał się przystosować polegała na korzystaniu z odnawialnych źródeł energii, zależnych od warunków pogodowych. Studenci musieli wprowadzić do systemu proces monitorowania aktywności (i wykrywania stopnia popytu/podaży energii, ewentualnych awarii) oraz mechanizm samoistnych zmian schematu działania w odpowiedzi na wykryte anomalie.

– *Systemy samoadoptujące się mają ogromny potencjał biznesowy – pozwalają ograniczyć zatrudnienie specjalistów i tym samym obniżyć całkowity koszt własności (ang. total cost of ownership – TCO) przy jednoczesnym utrzymaniu jakości dostarczanych usług (ang. quality of service – QoS)* – przekonywała Zofia Wrona. Mimo tak znacznej przewagi nad systemami tradycyjnymi, mechanizmy autonomiczne rzadko spotykane są w praktyce – ze względu na skomplikowane założenia oraz architekturę. Wydaje się więc, że studenci Politechniki Warszawskiej odkryli lukę na rynku, pozwalająca skomercjalizować opracowane rozwiązania. Współautorka pracy rozwija dalej badania nad systemami autonomicznymi, z wykorzystaniem bardziej zaawansowanego modelu – cyfrowego bliźniaka usług chmurowych[1].

Nagrodzone ambitne projekty – zarówno w sferze naukowej, jak i komercyjnej – dają nadzieję, że Polska nie przegra „wyścigu zbrojeń" w kolejnej fali rewolucji cyfrowych. Część autorów prac związała swój dalszy rozwój zawodowy z krajowymi instytucjami naukowymi, inni – pracujący komercyjnie – wprawdzie wykonują zlecenia dla firm z całego świata, ale na razie nie myślą o emigracji.

Komisja konkursowa przyznała także wyróżnienia czterem projektom:

- **„Gary – Kompleksowy System Obsługi Incydentów Ratunkowych" (autorzy: Aleksandra Mira, Adam Szerszenowicz, Stanisław Godwod, Borys Kotnowski, Bartosz Semeniuk, Julia Urbaniak, Rafał Osica, Wiktor Czech, Aleksander Kozakowski i Jan Zwolan), Wydział Informatyki, Polsko-Japońska Akademia Technik Komputerowych w Warszawie;**
- **„Indoor positioning system based on Ultra-Wideband technology" (autorzy: Sebastian Szczepański i Aleksander Wójtowicz), Wydział Informatyki, Elektroniki i Telekomunikacji, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie;**
- **„Adaptation of a continual learning method that alleviates the problem of forgetting for Generative Adversarial Networks" (autor: Bartosz Cywiński), Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska;**
- **„Klasyfikacja ligandów z wykorzystaniem głębokich sieci neuronowych" (autorzy: Jacek Karolczak, Anna Przybyłowska, Konrad Szewczyk i Witold Taisner), Wydział Informatyki i Telekomunikacji, Politechnika Poznańska.**

Organizatorami konkursu z ramienia Zarządu Głównego PTI są Oddziały Małopolski i Podkarpacki.

Paulina Giersz

[1] https://www.pw.edu.pl/engpw/News/WUT-student-with-AIR-Institute-award

Jak rosła branża

Warto prześledzić rozwój polskiego rynku informatycznego i telekomunikacyjnego z perspektywy ostatniej dekady.

Z kilku inicjatyw badania rynku, jakie w postaci publikowanych raportów pojawiały się w ciągu minionych ponad 30 lat, najstarszy jest raport IDG Computerworld TOP 200, który do maja 2024 r. zbiera właśnie dane do 32. edycji badania. Raporty dotyczące polskiego rynku ICT publikują na podstawie własnych badań m.in. IDC Polska (filia International Data Corporation, należącej do grupy IDG), PMR (ICT jest jednym z pięciu obszarów badawczych firmy – obok budownictwa, farmacji i ochrony zdrowia, handlu oraz przemysłu), a specjalistyczne raporty z różnych obszarów ICT – kilka innych firm analitycznych i doradczych (np. Audytel, koncentrujący się na rynku data center i telekomunikacyjnym).

Wydawałoby się, że najprościej jest pozyskiwać dane spółek giełdowych. Jednak obowiązane są one publikować tylko dane finansowe i to zunifikowanym dla firm giełdowych układzie, zgodnym z obowiązującymi regulacjami krajowych i międzynarodowych regulatorów giełd. Natomiast dane dotyczące wolumenów i kategorii obrotu rynkowego pozostają głównie na poziomie dodatkowych (i w większości dobrowolnych) prezentacji dla inwestorów giełdowych.

dr Tomasz Kulisiewicz
wykładowca i analityk rynku ICT

W dodatku zunifikowany układ danych finansowych oraz informacje z prezentacji nie zawsze zaspokajają oczekiwania autorów raportów i list rankingowych, choć oczywiście korzystne informacje wykorzystywane są w materiałach promocyjnych firm.

Dane na temat sektora ICT zbiera w ramach statystyki publicznej GUS. Są to m.in. dane na temat liczby firm, zatrudnienia i ogólnych wskaźników ekonomiczno-finansowych podmiotów z Sekcji J PKD (Informacja i komunikacja), części Sekcji C (Przetwórstwo przemysłowe – 26.2 Produkcja komputerów i urządzeń peryferyjnych oraz 26.3 Produkcja sprzętu (tele)komunikacyjnego) oraz Sekcji G (Handel hurtowy i detaliczny – Sprzedaż hurtowa (46.5) i detaliczna (47.4) narzędzi technologii informacyjnej i komunikacyjnej, czyli sprzętu ICT i oprogramowania). Według GUS w rejestrze REGON w sekcji J na 31 grudnia 2022 r. zarejestrowane było 260,4 tys. podmiotów gospodarczych (z czego niemal 207 tys. to osoby fizyczne prowadzące działalność gospodarczą), natomiast produkcją komputerów oraz wyrobów elektronicznych i optycznych zajmowało się 6240 podmiotów, w tym 3498 osób fizycznych prowadzących dg).

Podmioty z Sekcji J w 2022 r. wykazały przychody łączne w wysokości 182,1 mld zł, koszty w wysokości 167,2 mld zł, wynik finansowy netto w wysokości 11,7 mld zł i wskaźnik rentowności obrotu netto w wysokości 6,5%. Trzeba jednak pamiętać, że Sekcja J PKD obejmuje nie tylko informatykę, lecz także tak wielkie segmenty rynku jak wydawanie książek i czasopism, produkcję filmów, nagrań wideo, programów telewizyjnych, nagrań dźwiękowych i muzycznych, nadawanie programów telewizyjnych i radiowych wszystkimi kanałami komunikacji elektronicznej, w tym także IPTV, VOD i radia internetowego oraz wszystkie rodzaje transmisji danych ujęte w działalności telekomunikacyjnej, a więc przychody wszystkich operatorów telekomunikacyjnych.

Branżowy miesięcznik ITwiz w 2015 r. dołączył do grona światowych i krajowych zespołów przygotowujących i publikujących coroczne raporty z ocenami i podsumowaniami stanu rynku teleinformatycznego. Od pierwszej edycji w 2015 r. (za rok 2014) ukazało się dziewięć raportów zatytułowanych ITwiz BEST100. Zespół ITwiz BEST100 wspiera się danymi uzyskanymi z IDC i PMR dotyczącymi całości rynku, we własnym zakresie pozyskując przede wszystkim dane z poszczególnych firm, służące do zestawiania list rankingowych w poszczególnych (licznych) kategoriach.

Jak niemal zawsze w tego typu wydawnictwach, danym tabelarycznym i komentarzom zespołu autorskiego ITwiz BEST100 towarzyszą opinie, spostrzeżenia i komentarze uczestników rynku – przedstawicieli firm teleinformatycznych i telekomunikacyjnych. Warto przy tym zauważyć, że Adam Jadczak, redaktor naczelny miesięcznika ITwiz (prowadzący projekty raportów ITwiz BEST100) w swoich komentarzach do kolejnych edycji badania starannie podkreśla, że zespół raportów zbierający dane koryguje je w celu eliminacji kilkukrotnego liczenia przychodów ze sprzedaży tego samego produktu czy usługi na kolejnych piętrach rynku, np. w przypadku rynku IT – dostawców, integratorów, dystrybutorów i dealerów. W przypadku dużych dystrybutorów konsumenckiego sprzętu IT i telekomunikacyjnego dodatkowym elementem procedury „czyszczenia" danych jest konieczność nakłonienia ankietowanych firm do ujawnienia, jaki jest udział w ich sprzedaży np. telefonów komórkowych i akcesoriów do nich, zabawek elektronicznych czy sprzętu RTV i AGD. Na ile jest to ważne, wskazują dane już z pierwszego raportu (za rok 2014): w przychodach ABC Data telefony i urządzenia telekomunikacyjne stanowiły wtedy 31%, elektronika użytkowa, w tym sprzęt RTV/AGD ok. 6% zaś inne produkty „nieinformatyczne" ok. 3%. W rezultacie do przychodów z IT uwzględnianych na listach rankingowych raportu zaliczono tylko 60% sprzedaży ABC Data. W przypadku Action udział IT za rok 2014 oszacowano na 71%, zaś w AB – 73%. W przypadku dystrybutorów działających w kilku krajach naszego regionu dane dotyczące eksportu trzeba było też korygować szacowaną wartością produktów przewożonych między magazynami dystrybutora ulokowanymi w Polsce i np. na terenie sąsiedniego kraju.

Sinusoidalny wzrost

Korzystając z dostępnych na stronach ITwiz corocznych podsumowań poszczególnych edycji oraz udostępnionej nam bezpośrednio edycji 2023, pokusiliśmy się o przegląd niemal dekady polskiego rynku – tak jak rynek ten oceniał i szacował zespół autorski raportów. Ich dziewięć kolejnych edycji odwzorowuje nie tylko stan ogólny gospodarki w poszczególnych latach, lecz także takie elementy, jak terminarze programów operacyjnych w kolejnych perspektywach finansowych Unii Europejskiej oraz duże projekty budowy i rozbudowy systemów informacyjnych i informatycznych administracji publicznej. W danych dotyczących całości rynku IT autorzy raportu bazowali na kwotach ogólnych podawanych zwykle (np. przez IDC Polska) w dolarach, dla wartości złotowych stosując średnioroczny kurs NBP w analizowanym roku.

Rok 2014

W 2014 r. całkowita wartość polskiego rynku IT oszacowana została na ponad 34 mld zł (w ujęciu walutowym 10,8 mld USD) i nie zmieniła się w stosunku do roku 2013.

Największe przychody z IT miała firma Hewlett-Packard Polska, która osiągnęła niemal 10% udział w całym rynku. W pierwszej piątce edycji 2015 były trzy firmy dystrybucyjne – kolejno Action, AB i ABC Data – oraz Lenovo Technology Poland na miejscu piątym.

Rok 2015

Wartość polskiego rynku IT nadal zbliżona była do 11 mld USD, jednak słabszy kurs złotego podniósł wartość wyrażoną w złotych do ponad 41 mld zł. Na kolejność firm w czołówce listy ogólnej wpłynął podział HP dokonany ostatecznie w roku 2015 r. na firmę HP Inc. (komputery osobiste i urządzenia wydruku) oraz HP Enterprise (rozwiązania i usługi dla klientów korporacyjnych). W Polsce obie firmy działały już jako niezależne podmioty od 1 sierpnia 2015 r. W rezultacie w rankingu ogólnym za rok 2015 HP Inc. znalazło się na miejscu 7. (szacowane przychody na poziomie 1,6 mld zł), a HPE na miejscu 8. (1,59 mld zł). Na czołowe miejsca rankingu ogólnego przesunęli się dystrybutorzy: na pierwsze awansowała ABC Data, drugie miejsce zajmował Action (po odjęciu wspomnianego wcześniej „eksportu wewnętrznego"), trzecie AB, czwarte Komputronik. Miejsce piąte utrzymało Lenovo Technology Poland.

W niektórych kategoriach w czołówce pojawił się CD Projekt dzięki prawie dwudziestokrotnemu wzrostowi przychodów, w którym dominującą część miała sprzedaż gry Wiedźmin 3: Dziki Gon – ponad 20 mln egzemplarzy. Firma CD Projekt wyprzedziła dotychczasowych liderów w kategorii zysku brutto (414 mln zł, 58% przychodów firmy). Zajęła też pierwsze miejsce wśród eksporterów, wyprzedzając Wincor Nixdorf, polską filię Atosa, firmę Ericpol (outsourcing usług IT przede wszystkim dla ówczesnego wieloletniego partnera, telekomunikacyjnej firmy Ericsson) oraz Comarch. Duży wzrost widoczny był też w usługach centrów usług IT dla klientów zagranicznych (w pierwszej dziesiątce eksportu znalazły się polskie oddziały Luxoftu i Tieto), zaś Ericpol jako pierwsza firma z Polski znalazł się w w grupie „Rising Star" światowego rankingu The Global Outsourcing 100.

Rok 2016

W przypadku firm, których przychody przeliczane były z walut (dolarów i euro), wynik trochę poprawiło osłabienie kursu złotego w porównaniu z rokiem 2015. W rezultacie

wynik dla całości rynku przekroczył 40 mld zł. Firmy obecne na listach raportu ponownie odnotowały w 2016 r. spore spadki w sprzedaży sprzętu IT, które jednak częściowo skompensował wzrost sprzedaży usług i oprogramowania. Setka największych firm IT miała przychody niższe o prawie 3 mld zł (spadek o 6%), głównie z powodu dużego spadku sprzedaży dla administracji publicznej – w tym segmencie przychody firm były niższe aż o 4 mld zł, czyli o połowę. Ujemny wpływ na duże zamówienia publiczne miały zwłaszcza zmiany planów informatyzacji administracji centralnej po zmianie ekipy rządzącej oraz oczekiwanie na uruchomienie nowych środków europejskich na lata 2014–2020. Według przytoczonych w komentarzu do ITwiz BEST100 oszacowań Ministerstwa Rozwoju przetargi publiczne stanowiły w tych latach do 25% przychodów firm informatycznych działających w kraju.

W 2016 r. zaznaczył się bardzo istotny wzrost wydatków na usługi chmurowe, wynoszący w stosunku do roku poprzedniego aż 25% – do ok. 630 mln zł (160 mln USD).

Na pierwsze miejsce rankingu ogólnego awansowała ABC Data, drugie miejsce zajęła firma Action (będąca wtedy w trakcie formalnej restrukturyzacji), na trzecim. miejscu znalazło się Lenovo Technology Poland jako największa wówczas zagraniczna firma IT w Polsce, na czwartym. miejscu – dystrybutor AB.

W rezultacie podziału HP Inc. zajęła piąte. miejsce na polskiej liście za 2016 r., zaś HPE – siódme. Natomiast ogłoszone w październiku 2015 r. ale zakończone we wrześniu 2016 r. połączenie Della z EMC w Dell Technologies w Polsce spowodowało, że firma Dell EMC Poland wspięła się na szóste. miejsce w rankingu ogólnym.

Rok 2017

Wartość rynku IT w Polsce w 2017 r. (według danych uzyskanych z IDC Polska) przekroczyła 11 mld USD (11,2 mld). W wartościach dolarowych oznaczało to wzrost o niemal 5% w stosunku do roku poprzedniego. Przeliczenie na złotówki dało kwotę 42,2 mld zł.

W pierwszej połowie roku nadal widoczne było przyhamowanie przychodów ze sprzedaży dla administracji publicznej w Polsce. Przetargi na realizację projektów wspieranych środkami z UE – opóźnione czasem o 3 lata – ruszyły dopiero w drugiej połowie roku (e-podatki, systemy dla Ministerstwa Sprawiedliwości i przetarg na utrzymanie systemu KSI ZUS). Dzięki skumulowaniu rozstrzygnięć postępowań pod koniec roku wartość tego segmentu rynku wzrosła o 27,5% w stosunku do roku poprzedniego.

Zmieniła się kolejność czołówki dystrybutorów, zajmujących tradycyjnie pierwsze miejsca rankingu ogólnego: na pierwsze miejsce wyszła AB, drugie zajmowała ABC Data, na trzecim znalazł się Komputronik, czwarte zajmowało Lenovo Technology (formalnie – jej spółka zarejestrowana w Holandii), na piąte awansowała Dell EMC Polska. Action, będący nadal w trakcie restrukturyzacji, utrzymał miejsce w pierwszej dziesiątce, ale już tylko ósme.

Rok 2018

Po odjęciu powielania się przychodów w łańcuchu dostaw IDC szacowało wartość rynku IT na ok. 45 mld zł (co oznaczało wzrost o 7,4% w stosunku do poprzedniego roku). Do wzrostu przyczyniły się zarówno dwukrotny wzrost zamówień administracji publicznej (do 10,2 mld zł), jak i zakupy konsumentów dysponujących m.in. dodatkowymi przychodami pochodzącymi ze świadczeń 500+ i 300+. W danych dotyczących sprzedaży konsumenckiego sprzętu ICT uwzględniona została sprzedaż urządzeń mobilnych (smartfonów i tabletów). Sprzedaż telefonów przyniosła 2,9 mld zł, sprzedaż notebooków 1,19 mld zł, komputerów stacjonarnych 0,51 mld zł.

Choć dwaj najwięksi dystrybutorzy – AB i ABC Data – odnotowali spadki sprzedaży rzędu 2–3%, to jednak utrzymali dwa pierwsze miejsca w rankingu ogólnym. Na trzecim miejscu znalazła się Lenovo Technology, na czwartym HP Inc. na piątym Dell EMC Polska. Kolejne miejsca poza pierwszą piątką zajmowali trzej dystrybutorzy: Komputronik, Tech Data Polska oraz Action.

Rok 2019

Opierając się na danych IDC Polska, wielkość sprzedaży na rynku IT w 2019 r. oszacowano na 12,24 mld USD, co w przeliczeniu kursem średniorocznym oznaczało ok. 47 mld zł. W złotych oznaczało to wzrost o ok. 11%. Ok. 64% tej wartości wniosła sprzedaż pierwszej pięćdziesiątki spośród ponad 400 badanych firm. Dolna granica przychodów dająca miejsce w pięćdziesiątce wynosiła 272 mln zł – w 2014 r. wystarczyły przychody rzędu 155 mln zł. Kwoty dolnych progów pierwszej setki wynosiły odpowiednio 117 mln i 47 mln zł.

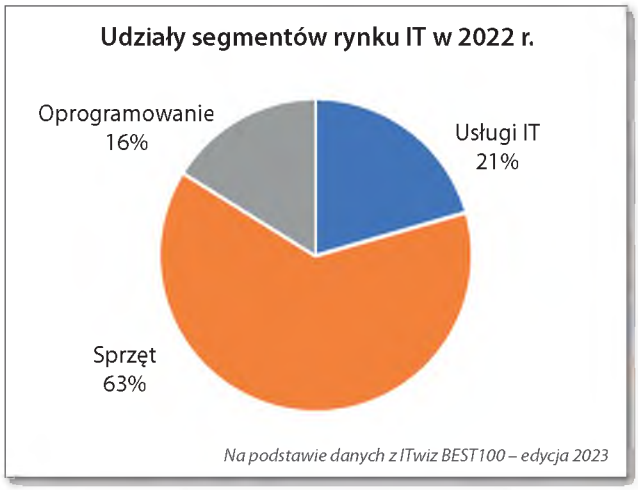
Sprzedaż sprzętu IT w 2019 r. osiągnęła 23,8 mld zł, usług IT niemal 13,6 mld zł, oprogramowania – 7,9 mld zł. Wartość eksportu wyniosła niemal 5,1 mld zł. W wartości tej zawierają się głównie sprzedaż oprogramowania (w tym prawie 1 mld zł za gry) oraz usługi programistów. Natomiast wartość rynku usług chmurowych sięgnęła 1,5 mld zł.

Pierwsze miejsca w rankingu ogólnym zajmowali nadal dwaj najwięksi dystrybutorzy – AB oraz ALSO Polska, która w 2019 roku przejęła ABC Data. Na trzecie miejsce awansował Dell EMC. Czwarte miejsce utrzymało HP Inc., na piąte zostało zepchnięte Lenovo. Trzy kolejne miejsca poza piątką nadal zajmowali dystrybutorzy, którzy pozamieniali się pozycjami – Action, Tech Data Polska oraz Komputronik.

Rok 2020

Podczas pierwszego wielkiego ataku koronawirusa do maja 2020 r. wszyscy spodziewali się głębokiego załamania rynku, były nawet prognozy spadku przekraczającego 10%. Jednak w połowie roku nastąpił mocny zwrot dzięki dużym inwestycjom wszystkich nabywców w narzędzia pozwalające działać w sposób zdalny. Dzięki temu, według danych IDC Polska, w 2020 r. polski rynek ICT wzrósł do 19,3 mld USD (o 4%), co w wartości złotowej oznaczało 75 mld zł.

Do ok. 1,85 mld zł (według IDC Polska) czy do ponad 2 mld zł (według PMR) wzrósł rynek *cloud computingu*. Sprzedaż terminali konsumenckich (głównie komputerów) bardzo podbiły zakupy dla szkół w ramach programów Szkoła zdalna/Szkoła zdalna+.



Spore wzrosty sprzedaży odnotowali przede wszystkim dystrybutorzy IT, zajmujący czołowe miejsca w rankingu ogólnym. AB utrzymał pierwsze miejsce (przy wzroście sprzedaży produktów IT aż o 37%). Na drugim miejscu nadal była ALSO Polska (ze wzrostem sprzedaży rzędu 15%). Trzecie miejsce utrzymał Dell EMC, czwarte odzyskało Lenovo Technology, natomiast piąte zdobył CD Projekt RED dzięki aż czterokrotnej poprawie wyników. Za nimi pozycje utrzymali dystrybutorzy Action i Tech Data Polska, na ósme spadło HP Inc. Dziesiątkę zamykały Microsoft i Komputronik.

Rok 2021

Według danych IDC Polska, w 2021 r. miał miejsce wzrost wartości rynku o 13%, do 21,8 mld USD, co w złotówkach oznaczało 84,2 mld zł. Nadal silny był wzrost sprzedaży sprzętu (aż o 27%), w oprogramowaniu odnotowano 10% wzrostu, w usługach 4%. Do 886 mln USD (ok. 3,7 mld zł) wzrosła sprzedaż usług chmurowych, co oznaczało ponad 2,5-krotny wzrost. Przychody z eksportu firm z rankingu wyniosły ponad 19,2 mld zł, głównie dzięki przychodom Grupy Asseco Poland, Intel Technology Poland, Comarchu, CD Projekt RED, Ten Square Games i Samsung Electronics Polska.

Zajęcie miejsca wśród 50 największych firm wymagało przychodów na poziomie 298 mln zł (260 mln zł w 2020 r.), a w przypadku pierwszej setki – 150 mln zł (w 2020 r. – 120 mln zł).

Lider rynku dystrybutor AB w 2021 r. miał sprzedaż produktów i usług IT na poziomie 8 mld zł, co oznaczało wzrost o 19% w porównaniu do roku poprzedniego. Drugie miejsce utrzymało ALSO Polska (wzrost sprzedaży na poziomie 27%), trzecie Dell EMC (21% wzrostu), a czwarte Lenovo Technology. Do pierwszej piątki wróciło HP Inc. Kolejne miejsca zajęły Intel Technology Poland, Asseco Poland (powrót do dziesiątki z 15. miejsca). Dziesiątkę zamykały Tech Data Polska, Komputronik oraz Samsung Electronics Polska, którzy jedną trzecią przychodów uzyskiwał z tworzenia w warszawskim centrum R&D oprogramowania na zlecenie centrali korporacji.

Rok 2022

Wydanie dostępne obecnie podsumowuje rok 2022, w którym wartość rynku ICT osiągnęła 24,5 mld USD, co w przeliczeniu kursem średniorocznym oznacza pokonanie progu 100 mld zł. Na rynek IT przypadało 18 mld USD (wzrost o 14,7%), na usługi telekomunikacyjne – 6,5 mld USD (wzrost nieco ponad 3%).

> *Dla porównania naszej pozycji w Europie: rynek ICT Hiszpanii, do której często się porównujemy z uwagi na zbliżony rząd liczebności populacji (46,4 mln w 2022 r., czyli o ok. 22% więcej niż Polska), osiągnął wtedy wartość niemal 51 mld USD, czyli ponad dwa razy więcej.*

Wartość rynku usług, w tym biznesowych, takich jak BPO czy doradztwo wyniosła 4,6 mld USD (18,7 mld zł), natomiast samego rynku usług IT ok. 3,7 mld USD (15,1 mld zł). Aż 30 % wzrostu odnotowano na rynku usług chmurowych, który osiągnął 1,3 mld USD (5,3 mld zł). O 13,8% wzrósł rynek oprogramowania – do wartości 2,9 mld USD (11,8 mld zł), w tym na sprzedaż aplikacji przypadało 1,5 mld USD (6,1 mld zł). Sprzedaż sprzętu przyniosła 11,4 mld zł, z czego 9 mld zł przypadło na segment zwany Devices: komputery, peryferia, telefony komórkowe i tzw. wearables (wzrost o 18%). Segment Infrastructure (serwery, pamięci masowe, urządzenia sieciowe) wykazał wzrost o 23%. Do wzrostów sprzedaży sprzętu przyczyniła się poprawa działania globalnych łańcuchów dostaw, po wcześniejszych opóźnieniach produkcyjnych głównie na Dalekim Wschodzie.

	Największe firmy	Przychody (w tys. zł)		Zmiana 2022/2021	Liczba pracowników
		2022	2021		
1	AB	9 144 292	7 724 095	18%	bd
2	ALSO Polska*	7 911 858	7 000 000	13%	bd
3	Lenovo Technology B.V.*	3 607 000	2 070 000	74%	bd
4	Dell EMC Polska*	3 064 000	2 279 000	34%	210
5	Nokia (IT)*	2 818 000	2 539 000	11%	bd
6	Microsoft*	2 624 000	1 500 000	75%	331
7	Ingram Micro*	2 500 000	2 250 000	11%	bd
8	HP Inc.*	2 404 000	2 054 000	17%	573
9	Capgemini Polska (IT)*	2 169 000	1 625 318	33%	12 000
10	Asseco Poland	2 077 052	1 883 397	10%	4601

** oszacowanie*

Źródło: ITwiz BEST100 – edycja 2023

Pierwszą pozycję utrzymał dystrybutor AB, wykazując wzrost sprzedaży o 18% w porównaniu do roku 2021. Drugie miejsce niezmiennie zajmowało ALSO Polska, ze wzrostem sprzedaży na poziomie 13% do 7,9 mld zł (również zajmujące się dystrybucją). Na trzecie miejsce rankingu weszło Lenovo Technology, wyprzedzając Dell EMC. Na piąte miejsce awansowała Nokia. Kolejne miejsca zajęły Microsoft, Ingram Micro, HP Inc. i Capgemini Polska, dziesiątkę zamykało Asseco Poland.

Aby dostać się do pierwszej pięćdziesiątki, w 2022 r. trzeba było osiągnąć przychody rzędu 402 mln zł (296 mln zł w roku poprzednim), a do pierwszej setki – 190 mln zł (rok wcześniej 148 mln zł).

Aż 62% ankietowanych przez zespół ITwiz firm-uczestników rankingu ITwiz Best100 twierdziło, że rok 2022 był lepszy lub dużo lepszy niż 2021 (rok wcześniej opinię taką wyrażało aż 73% ankietowanych przedstawicieli firm). Firmy IT w Polsce nadal zwiększały zatrudnienie (54% odpowiedzi), tylko 7% dokonało zwolnień – co oznaczało zupełnie odmienne podejście niż w USA, gdzie według danych TradingPlatforms.com firmy sektora BigTech zwolniły prawie 120 tys. pracowników.

Coroczne raporty o stanie rynku telekomunikacyjnego w Polsce publikuje Urząd Komunikacji Elektronicznej. Początkowo raporty UKE koncentrowały się na geograficznym pokryciu terytorium kraju sieciami i usługami telekomunikacyjnymi, od kilku lat zawarte są w nich także dane dotyczące liczby poszczególnych kategorii usług oraz przychodów z tych usług, a także planowanych inwestycji operatorów. UKE ma „uprzywilejowaną pozycję" w gromadzeniu danych, gdyż dysponuje nie tylko rozbudowanym systemem elektronicznego zbierania danych od niemal 4 tys. przedsiębiorców telekomunikacyjnych oraz ponad 500 świadczących takie usługi jednostek samorządu, lecz także stosownymi regulacjami zobowiązującymi (pod groźbą sankcji) operatorów i JST do dostarczania tych danych według stanu na 31 grudnia poprzedniego roku – są nimi dwa rozporządzenia Ministra Cyfryzacji z grudnia 2022 r., dotyczące przekazywania danych dotyczących działalności telekomunikacyjnej oraz inwentaryzacji infrastruktury i usług telekomunikacyjnych. Prezes UKE ma natomiast prawny obowiązek publikowania corocznego raportu o stanie rynku. Na razie wspomniane obowiązki wynikają z art. 7 oraz 192 Prawa telekomunikacyjnego. Zmiany dotyczące m.in. dostarczania danych według stanów dwa razy w roku miały wejść w życie wraz z procedowanym od lipca 2020 r. Prawem Komunikacji Elektronicznej wdrażającym Europejski Kodeks Łączności Elektronicznej, ale projekt został wycofany przez rząd z procesu legislacyjnego we wrześniu 2023 r. i już nie wrócił przed końcem kadencji.

Według „Raportu o stanie rynku telekomunikacyjnego w 2022 roku" przychody z tytułu wykonywania działalności telekomunikacyjnej spadły w stosunku do 2021 r. o 0,4% i wyniosły 40,63 mld zł. Wydatki na inwestycje telekomunikacyjne osiągnęły 11,24 mld zł (wzrost o 26,3% w stosunku do 2021 r.).

Eyetracking: widzieć więcej

Metody śledzenia ruchu gałek ocznych znamy od ponad 100 lat. Nowe technologie zrewolucjonizowały okulografię (tak początkowo nazywano tę technikę) i poszerzyły zakres jej zastosowań.

Beata Chodacka

nauczyciel informatyki w V LO i SP 33 w Krakowie, wiceprezes Oddziału Małopolskiego PTI, animator 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 PTI.

Danuta Smołucha

z wykształcenia matematyk i informatyk, doktor nauk humanistycznych w zakresie kulturoznawstwa, jej pasją są podróże do miejsc związanych z historią i kulturą krajów iberoamerykańskich. Współautor podręcznika do informatyki do liceum, autorka książek: „Humanistyka cyfrowa w badaniach kulturowych"; „Kultura religijna w cyberprzestrzeni", a także współautorka i autorka przewodników.

Od zarania dziejów człowiek dążył do coraz głębszego poznawania świata. Chciał zdobywać nowe doświadczenia i wiedzieć coraz więcej o otaczającej go rzeczywistości. W naturalny sposób wykorzystywał w tym celu zmysły, wśród których wiodącą rolę odgrywa wzrok. Zmysły ludzkie nie są jednak doskonałe, podlegają wielu ograniczeniom, nawet w porównaniu z tymi samymi zmysłami w świecie zwierząt. Człowiek widzi rozpościerający się wokół niego świat, ale nie dostrzega wszystkich obiektów, bo oko, choć jest doskonałym organem, ma jednak ograniczone możliwości.

Stąd też wiele obiektów ma zbyt małe rozmiary, aby człowiek mógł je dostrzec bez wspomagania się urządzeniami wykorzystującymi zdobycze technologii. Słyszy też dźwięki, ale tylko te, których źródło znajduje się odpowiednio blisko niego.

Wiele wynalazków powstało właśnie w tym celu, aby udoskonalić możliwości ludzkiego odbioru rzeczywistości i wzmocnić ludzkie zmysły. Wynalazek Grahama Bella umożliwił rozmowy na odległość w czasie rzeczywistym, fonograf pozwolił na rejestrację dźwięków, przez co możliwe stało się słuchanie głosu nawet tych, którzy już opuścili ziemski padół. Fotografia zatrzymała w czasie ulotne chwile, film dał szansę na wirtualne uczestnictwo w zdarzeniach, które miały miejsce w innej przestrzeni czasowej, aniżeli ta, w której znajduje się odbiorca przekazu. Z pomocą lunety ludzie mogli oglądać odległe od Ziemi gwiazdy, przez oko mikroskopu analizowali strukturę niezmiernie małych obiektów, nawet takich, których istnienia wcześniej się nie domyślali. Ludzka wyobraźnia nie ma granic, a w ich przekraczaniu pomaga technologia.

Obraz zyskuje na znaczeniu

Już w latach 50. XX w. Ernst Gombrich, austriacki historyk sztuki, wieścił nadejście czasów, gdy tekst przestanie mieć znaczenie, a wszechobecne obrazy przejmą jego rolę i to one głównie będą decydować o odbiorze rzeczywistości przez człowieka. Zaczęto się więc zastanawiać, na co rzeczywiście patrzymy i co faktycznie dostrzegamy, czyli – jakbyśmy to dzisiaj sformułowali – na znaczeniu zaczęła zyskiwać problematyka aktywnej percepcji obiektów w przestrzeni publicznej. Szczególną wagę do wyników badań przykładali reklamodawcy, dla których skuteczny odbiór ich przekazu stanowił być albo nie być na rynku i pozwalał osiągnąć komercyjny sukces.

Rozważanie takich kwestii wymagało jednak umiejętności śledzenia ścieżki wzroku patrzącego. Problem podejmowali już badacze na początku XX w. Opierali się jednak wyłącznie na szkicach czynionych ołówkiem na kartce, które tworzyli w czasie rzeczywistym podczas obserwacji ruchów źrenic osoby obserwującej obiekt, będącej obiektem badań. Wyniki badań nie miały do końca charakteru obiektywnego, bo bazo-

wały na subiektywnych wrażeniach badaczy. Pomimo błędów wynikających z niedoskonałości metody badań, ich wyniki wniosły jednak wiele do nauki.

Kreślenie ścieżki wzroku bazujące na obserwacji źrenic osoby patrzącej

Źródło: http://widzenie.net/okulograf.htm

Badania miały na celu wskazanie, na co ludzie zwracają uwagę, jeśli chcą uzyskać konkretną wiedzę o danej osobie. Okazało się, że ogromne znaczenie ma cel obserwacji. Inaczej oglądana jest osoba, jeśli celem jest ocena stanu jej zamożności, inaczej, gdy ocenie ma podlegać jej inteligencja czy środowisko, z jakiego się wywodzi. Te bardzo niedokładne wówczas jeszcze eksperymenty dały początek badaniom eyetrackingowym, bazującym na nowoczesnych technologiach.

W czasie jednej sekundy ludzkie oko wykonuje średnio trzy, cztery ruchy, gdy człowiek przemieszcza swoją uwagę wzrokową pomiędzy elementami sfery widzialnej. Moment zatrzymania uwagi nazywany jest fiksacją, natomiast szybkie przemieszczenie pomiędzy dwoma fiksacjami zwane jest sakkadą.

Do badań śledzenia ścieżki wzroku wykorzystuje się tzw. eyetrackery – urządzenia monitorujące pracę gałek ocznych, wykorzystujące odbicie od oka światła w bliskiej podczerwieni (niewidocznego dla człowieka), które jest przechwytywane przez kamery. Dane są przetwarzane. Uzyskana i zwizualizowana sekwencja fiksacji i sakkad osoby badanej umożliwia tłumaczenie wielu zjawisk związanych z przyswajaniem informacji wizualnej.

Metoda wizualizacji sposobu obserwacji otoczenia przez człowieka jest dobierana w zależności od informacji, jakie badacz chce uzyskać. Jedną z nich jest przedstawienie ścieżki wzroku za pomocą kół i łączących je odcinków. Koła oznaczają miejsca fiksacji, a ich wielkość jest wprost proporcjonalna do czasu ich trwania. Często poszczególne fiksacje są oznaczane numerami, wskazującymi kolejność patrzenia. Pozwala to także zwrócić uwagę na te miejsca, na które badany kieruje uwagę wielokrotnie. Przenoszenie wzroku pomiędzy fiksacjami oznaczane jest łączącymi je odcinkami. Ten sposób wizualizacji pozwala na dokładną analizę ścieżki wzroku w sytuacjach, gdy ma znaczenie kolejność skupienia uwagi czy liczba powrotów do elementów już odwiedzonych.

Przykładowa sekwencja fiksacji i sakkad przedstawiająca ścieżkę wzroku osoby badanej techniką eyetrackingu

Źródło: opracowanie własne

Innym sposobem wizualizacji problemu „na co patrzą ludzie" jest przedstawienie oglądanych obszarów za pomocą mapy cieplnej (ang. *heat map*), gdzie nie tyle ważne są fiksacje i sakkady, co identyfikacja obszarów zainteresowań. W zależności od intensywności skupiania uwagi przez badaną osobę (grupę osób), obszary zainteresowań oznaczane są od koloru czerwonego (te najbardziej oglądane), poprzez żółty (na których osoba badana skupiła mniejszą uwagę) do zielonego, oznaczającego najmniejszą uwagę badanego. Brak zaznaczenia kolorem oznacza, że obszar został zignorowany przez badanego, pominięty w jego postrzeganiu otaczającej go przestrzeni. Ten typ wizualizacji jest przydatny szczególnie wówczas, gdy istotna jest nie tyle kolejność, w jakiej badany penetruje otaczającą go przestrzeń, co identyfikacja obszarów, które budzą jego największe zainteresowanie.

Przedstawienie obszarów uwagi osoby przeglądającej stronę internetową za pomocą mapy cieplnej

Źródło: https://de.wikipedia.org/wiki/Eye-Tracking

Przydatność w wielu obszarach

Badania eyetrackingowe znalazły zastosowanie w wielu dziedzinach. Jedne z pierwszych dotyczyły projektowania kokpitu pilota tak, aby ten mógł skupić uwagę na najistotniejszych parametrach lotu, bez rozpraszania uwagi na elementach

mniej istotnych, dzięki czemu lot stawał się bezpieczniejszy. Dzisiaj eyetracking pomaga przy projektowaniu użytecznych interfejsów, ergonomicznych wnętrz, pozwala ocenić, czy przygotowany przekaz reklamowy skupia wzrok klienta na elementach stanowiących kluczowy element przekazu, czyli na reklamowanym produkcie, nazwie firmy itd.

To właśnie wyniki badań eyetrackingowych przyczyniły się do tego, że zwykle wybieramy w sklepach produkty eksponowane na półkach znajdujących się na wysokości naszych oczu. Pomijamy tym samym ekspozycje umiejscowione niżej/wyżej stref skupiających naszą uwagę, bez świadomości, że zostały tam umieszczone artykuły, które zwykle nie ustępują jakością tym z wyższych półek, mają za to o wiele niższą cenę.

Chociaż technologia eyetrackingu kojarzona jest powszechnie głównie z zastosowaniami komercyjnymi, znalazła także zastosowanie w medycynie, psychologii oraz w szeroko pojętej edukacji.

Eyetracking w edukacji

Ta metoda badawcza znalazła zastosowanie w badaniach edukacyjnych, związanych zarówno ze szkoleniem dzieci, jak i dorosłych. Szczegółowa analiza ścieżki wzroku ucznia podczas czytania tekstu pozwala m.in. na identyfikację przyczyn trudności i zaburzeń w czytaniu i przyswajaniu treści, które wynikają głównie z trudności utrzymania uwagi na poszczególnych fragmentach tekstu.

Przed wprowadzeniem do badań metody eyetrackingowej nie było możliwości dokonania tak wnikliwej jak obecnie analizy procesu zapoznawania się ucznia z materiałem edukacyjnym, a także oceny stopnia skupienia uwagi ucznia nad tekstem, z którym się zapoznaje. Dzisiaj możemy dokonać pogłębionej oceny, w jaki sposób uczniowie czytają i rozumieją teksty. Można ocenić, na których elementach przygotowanego materiału edukacyjnego skupiają większą uwagę, na których mniejszą, a które są zupełnie pomijane. Dla badaczy ważne jest też, do których fragmentów materiału uczniowie wracają po raz drugi, by przyswoić je ponownie, a także które fragmenty czytają lub oglądają wielokrotnie, by zrozumieć ich sens. Równie istotne jest, po jak długim czasie uczniowie dostrzegają poszczególne elementy materiału, z którym się zapoznają, oraz jak długo skupiają na nich uwagę.

> *Analiza wzrokowej uwagi ucznia szczególnie przydatna jest przy testowaniu zadań – jeśli okaże się, że duża liczba uczniów czyta wielokrotnie fragment zadania przed przystąpieniem do jego wykonania, może to stanowić sygnał, że treść zadania została sformułowana w niejasny i mało przystępny dla ucznia sposób.*

Współczynnik niepowodzenia wykonania zadania może więc wynikać wówczas nie tyle z braku odpowiednich umiejętności ucznia, ile ze złego sformułowania zadania.

W ostatnich latach popularna stała się tendencja fabularyzacji treści zadań, którym sprostać mieli uczniowie zarówno na egzaminie maturalnym, jak i ci uczestniczący w różnego typu zawodach przedmiotowych. Częstokroć celem tego typu zabiegów było wskazanie, że nauki ścisłe są bliskie codziennemu życiu i że wiedza zdobyta w tym zakresie może być przydatna. W rezultacie „przerost formy nad treścią" sprawia, że uczeń – nie zrozumiawszy dokładnie poleceń, które powinien wykonać w zadaniu – po prostu ich nie wykona, choć byłby w stanie to zrobić przy innym, mniej karkołomnym sformułowaniu zadania. Testy wykorzystujące metodę eyetrackingu pozwalają uwidocznić problem: czy uczeń zwraca należytą uwagę na najistotniejsze fragmenty treści zadania czy raczej pożytkuje ją na te elementy, które choć ją uatrakcyjniają, to nie wnoszą nic istotnego z punktu widzenia analizy i rozwiązania zadania.

Z tych właśnie względów doskonałą metodą oceny podręczników szkolnych i stron internetowych czy prezentacji multimedialnych skierowanych do uczniów byłaby analiza ścieżki wzroku badanych uczniów. Byłaby to szansa na końcową modyfikację materiałów przeznaczonych do druku i projektowanie lepszych interfejsów edukacyjnych. To przecież wyniki badań z użyciem tej technologii wskazały obszary na stronach internetowych, w których powinny zostać umieszczone najistotniejsze treści z punktu widzenia odbioru przekazu. Oczywiście wspomniane rozwiązania wiązałyby się z wysokimi nakładami finansowymi, co obecnie uniemożliwia jeszcze ich wdrożenie w plan powszechnej edukacji.

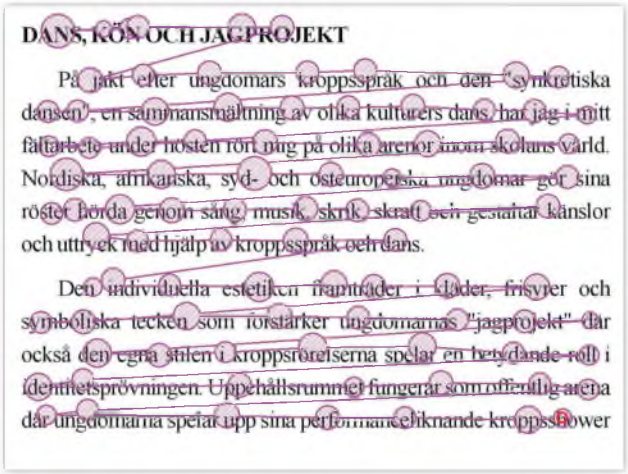
Eyetracking jest też niezastąpioną metodą oceny problemów z czytaniem osób z dysleksją. Nie tylko pozwala na ocenę ich tempa czytania tekstów, lecz także na identyfikację problemów szczególnie istotnych z punktu widzenia rozumienia tekstu, z którym się zapoznają. Precyzja wyników badań dotyczy słów, a nawet fragmentów tekstu, które zostają przez takie osoby pomijane. Stanowi to punkt wyjścia do opracowania metod, które pomogą osobom z dysleksją na lepsze rozumienie tekstów czytanych. Ma to szczególne znaczenie, bo wraz z doskonaleniem umiejętności czytania maleje zarówno liczba fiksacji, jak i czas z nimi związany.

Wzrokocentryczni

We współczesnej kulturze ogromna liczba przekazów informacji przedstawiana jest w formie obrazowej, w tym za pomocą wykresu lub infografiki, które są szybsze w odbiorze niż tekst, a także łatwiejsze do przyswojenia przez użytkowników urządzeń mobilnych o niewielkich ekranach. Jak się jednak okazuje, taka obrazowa forma może zarówno uczynić przekaz łatwiejszym do zrozumienia, jak i odwrotnie, w odpowiedni sposób skonstruowana, może sugerować błędne wnioski.

> *Obraz jest medium, za pomocą którego łatwo można manipulować odbiorcą poprzez na przykład odpowiedni dobór proporcji i kolorów, kadrowania obrazu, a – w przypadku wykresu – dodatkowo także poprzez wybór jego typu czy wartości jednostki osi.*

Wyniki badań bazujących na analizach eyetrackingowych pomagają specjalistom przygotować materiały dla uczniów i odpowiednie wsparcie terapeutyczne, w tym to wspomagające trening funkcji poznawczych, związany głównie ze szkoleniem ukierunkowanym na koncentrację uwagi.


DANS, KÖN OCH JAG-PROJEKT

På jakt efter ungdomars kroppsspråk och den "synkretiska dansen", en sammansmältning av olika kulturers dans, har jag i mitt fältarbete under hösten rört mig på olika arenor inom skolans värld. Nordiska, afrikanska, syd- och östeuropeiska ungdomar gör sina röster hörda genom sång, musik, skrik, skratt och gestaltar känslor och uttryck med hjälp av kroppsspråk och dans.

Den individuella estetiken framträder i kläder, frisyrer och symboliska tecken som förstärker ungdomarnas "jagprojekt" där också den egna stilen i kroppsrörelserna spelar en betydande roll i identitetsprövningen. Uppehållsrummet fungerar som offentlig arena där ungdomarna spelar upp sina performanceliknande kroppsspråk

Sekwencja fiksacji i sakkad przedstawiająca ścieżkę wzroku podczas czytania tekstu

Źródło: https://upload.wikimedia.org/wikipedia/commons/e/ef/Reading_Fixations_Saccades.jpg

Nie sposób byłoby przecenić zastosowanie technologii eyetrackingu w pomocy osobom z zaawansowaną niepełnosprawnością ruchową, w szczególności tym, które przy całkowitym paraliżu ciała mają sprawny narząd wzroku. Osoby te mogą obsługiwać komputer, pisać teksty i przetwarzać dane, komunikując się z maszyną wyłącznie za pomocą ruchu gałek ocznych. Współpracujący z komputerem użytkownika eye-tracker rejestruje miejsca na ekranie, na których użytkownik skupia uwagę, odczytuje wysyłane przez niego sygnały w postaci ruchów źrenic, w wyniku czego inicjowane są żądane przez użytkownika instrukcje.

Pomoc niesiona osobom z różnym stopniem niepełnosprawności ma szczególne znaczenie w przypadku osób młodych. Uczniom o dużej niepełnosprawności ruchowej śledzenie ścieżki wzroku umożliwia sprawną obsługę interfejsu, sterowanie aplikacjami, co przekłada się na możliwość korzystania ze sprzętu komputerowego niemal na poziomie osoby pełnosprawnej.

Edukacja uczniów w spektrum autyzmu

Jednym z zaburzeń neurorozwojowych, którego zdiagnozowanie na wczesnym etapie rozwoju dziecka ma ogromne znaczenie dla jego późniejszego rozwoju, jest autyzm. Eyetracking niesie ogromną pomoc diagnostom nie tylko w zdiagnozowaniu autyzmu, lecz także przy wyborze metody edukacji uczniów już zdiagnozowanych. Autyzm nie jest jedynym zaburzeniem neurologicznym, w którego diagnozowaniu technologia śledzenia wzroku i analizy skupienia odgrywa ważną rolę. Eyetracking wykorzystywany jest także przy przeprowadzaniu różnego typu testów psychologicznych, często mało znanych nawet wśród osób zainteresowanych tą tematyką. Przykładem tego typu badań jest opracowany w latach 90. XX w. przez Anthony'ego Greenwalda test utajnionych skojarzeń IAT (ang. *Implicite Association Test*). Celem testu jest wykrycie preferencji, skojarzeń i uprzedzeń badanego, często przez niego nieuświadomionych, których istnienia nie podejrzewa. Tym samym test ten pozwala na zbudowanie profilu badanej osoby na podstawie przesłanek, których uzyskanie inną drogą byłoby niemożliwe.

Wspomniane przykłady to tylko niewielki ułamek możliwości zastosowania tej technologii. Przyspieszenie jej wykorzystania nastąpi zapewne wraz ze zmniejszeniem kosztów sprzętu niezbędnego do prowadzenia badań.

W ciągu ostatnich lat eyetracking trafił także do gier i aplikacji mobilnych, poszerzając interfejs użytkownika o dodatkowe możliwości i poprawiając jego czytelność i użyteczność. Śledzenie ruchu źrenic gracza jest źródłem dodatkowych informacji, których wykorzystanie pozwala graczom na bardziej intensywne zanurzenie się w świecie wirtualnym, m.in. na rozglądanie się w różnych kierunkach tylko na podstawie ruchu gałek ocznych, dostosowanie oświetlenia w zależności od kierunku patrzenia czy też dostarczenie systemowi informacji, czy nastąpiło nawiązanie kontaktu wzrokowego z rozmówcą.

Wciąż trwają prace nad wykorzystaniem tej technologii przy weryfikacji tożsamości użytkownika systemu komputerowego. Badanie wzorca ruchu gałek ocznych już w niedalekiej przyszłości pozwoli zapewne na wiarygodną ocenę, czy osoba korzystająca z systemu jest rzeczywiście tym, za kogo się podaje.

Bywa tak, że technologia wygląda na przełomową, ale nie znajduje zbyt wielu zastosowań. Eyetracking jest przydatny w wielu dziedzinach – ich lista nie została zamknięta.

Konkurs GEEK czeka na zgłoszenia

Gry fascynują ludzi niezależnie od wieku. Potencjał gier w edukacji długo pozostawał niedoceniony, ale ostatnie lata przyniosły przełom. Wraz z rozwojem technologii i lepszym rozumieniem ludzkiej psychologii gry i zjawisko gamifikacji zyskują na znaczeniu jako narzędzia skutecznie wspierające proces edukacyjny.

Beata Chodacka
nauczyciel informatyki w V LO i SP 33 w Krakowie, wiceprezes Oddziału Małopolskiego PTI, animator 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 PTI.

Ich największą zaletą jest zdolność do angażowania uczniów na różnych poziomach edukacyjnych. Gry edukacyjne oferują nie tylko atrakcyjną formę przekazywania wiedzy, lecz także podnoszą motywację do nauki i większego zaangażowania, rozwijają umiejętności poznawcze, dążenie do znalezienia sposobu rozwiązania problemu, co sprzyja rozwijaniu umiejętności logicznego myślenia. Wykorzystanie gier pozwala na indywidualizację nauki, umożliwiając dostosowanie poziomu trudności do umiejętności każdego ucznia.

Gamifikacja w edukacji, czyli zastosowanie mechaniki, narzędzi i elementów gry, takich jak zdobywanie punktów, osiąganie poziomów czy otrzymywanie nagród, stymuluje zaangażowanie uczniów w proces nauki.

Dlaczego warto tworzyć gry edukacyjne?

- **Nowoczesna forma edukacji:** gry edukacyjne umożliwiają interaktywne, angażujące i dynamiczne metody nauki. Poprzez wciągające rozgrywki uczą, bawiąc i angażując uczniów w proces zdobywania wiedzy. Jeśli dodatkowo uczniowie mają możliwość zaprojektowania gier dla swoich rówieśników, atrakcyjność zajęć wzrasta.
- **Rozwój kompetencji:** tworzenie gier wspiera rozwój umiejętności krytycznego myślenia, zdolności rozwiązywania problemów, pracy zespołowej i umiejętności technicznych – niezbędnych w świecie nowoczesnej technologii.
- **Przydatne narzędzie:** sprzyja lepszemu poznawaniu wielu narzędzi i metod zarówno programowania, jak i przygotowania zadań, grafik, wspiera przyswajanie wiedzy oraz przetwarzanie informacji przez uczniów.
- **Innowacyjność i kreatywność:** zaprojektowanie gry wymaga kreatywności, co rozwija umiejętności twórczego myślenia, planowania oraz projektowania.
- **Rozwijanie umiejętności praktycznych:** to również doskonały sposób na rozwijanie umiejętności technicznych, programistycznych i graficznych, które mogą znaleźć praktyczne zastosowanie w przyszłej karierze zawodowej.

Umożliwia także nauczycielom lepsze monitorowanie postępów, co może stanowić dodatkową motywację dla uczniów. Gry stanowią integralną część innowacyjnych metod nauczania – wykorzystanie interakcji, symulacji to ważne narzędzia dla nauczycieli.

Sztuka kreacji

Kolejnym etapem, do którego możemy zaprosić uczniów, jest tworzenie gier – to zadanie wymagające starannego planowania i uwzględnienia celów edukacyjnych oraz realnej oceny różnych możliwości. Tworzenie gier komputerowych, zwłaszcza tych o charakterze edukacyjnym, stanowi nie tylko atrakcyjną formę nauki, przynosi także wiele korzyści w dzisiejszym świecie cyfrowym.

Wiedza o programowaniu, projektowaniu gier czy pracy w zespołach technologicznych jest niezwykle cenna, przygotowuje młodych ludzi do wejścia na rynek pracy. Zaangażowanie uczniów w takie projekty to droga do rozwoju kompetencji przyszłości. Młodzi ludzie mogą wkroczyć w świat nowoczesnych technologii, co otwiera im drzwi także do kariery w dziedzinie IT.

Tworzenie gier edukacyjnych to nie tylko sposób na naukę, lecz także wsparcie w rozwijaniu umiejętności potrzebnych w przyszłym życiu zawodowym. Dlatego konkurs GEEK staje się niezwykle cenną okazją dla młodych pasjonatów gier i technologii, otwierając drzwi do nowych, fascynujących możliwości rozwoju.

Trwa nabór

Konkurs Gry Eksperymentalne Edukacyjne Komputerowe (GEEK) jest inicjatywą Polskiego Towarzystwa Informatycznego oraz Federacji Stowarzyszeń Naukowo-Technicznych (FSNT-NOT). Skierowany jest do uczniów szkół podstawowych i ponadpodstawowych w Polsce. Główny cel najnowszej edycji konkursu to pobudzanie i rozwijanie zainteresowań związanych z tworzeniem edukacyjnych gier komputerowych, popularyzacja wiedzy o wynalazcach, rozwijanie kompetencji informatycznych, propagowanie nauki programowania i zwiększanie świadomości młodych osób w obszarze licencji Open Source i Creative Commons.

> *Tegoroczna edycja konkursu to zespołowe zadanie dla uczniów, polegające na opracowaniu i przedstawieniu scenariusza lub prototypu, demo czy też pełnej implementacji gry edukacyjnej o tematyce dotyczącej wynalazków lub wynalazczyń i wynalazców związanych z różnymi obszarami nauki.*

Ważnym elementem jest zobowiązanie uczestników do przestrzegania prawa autorskiego poprzez korzystanie z oprogramowania opartego na licencjach Open Source oraz materiałów na licencjach Creative Commons.

Udział w konkursie dla uczniów jest dobrowolny i całkowicie bezpłatny. Rejestracja uczestników i szkół odbywa się na stronie konkursu: https://mlodzi.pti.org.pl/. Tam również znajdują się wszystkie bieżące informacje, w tym regulamin. Konkurs ma zasięg ogólnopolski, a ogłoszenie wyników regionalnych odbędzie się w kwietniu 2024 r., w ramach obchodów Światowego Dnia Społeczeństwa Informacyjnego. Finał konkursu oraz uroczyste wręczenie nagród dla najlepszych uczniów zaplanowane jest w Warszawie na 7 czerwca 2024 r.

Konkurs objęty został patronatem honorowym Ministerstwa Edukacji i Nauki oraz Govtech.

Źródło: Droniada.eu

Sztuczna inteligencja potrzebuje ludzi

Udział człowieka jest niezbędny w różnych obszarach tworzenia i wykorzystania systemów sztucznej inteligencji, podobnie jak w przypadku wszystkich innych rozwiązań informatycznych.

Media pełne są opowieści o zagrożeniach polegających na zabieraniu ludziom pracy przez sztuczną inteligencję i zastępowaniu pracowników przez różnej maści roboty. Zgoła inne wnioski wypływają z prowadzonej przez piszącego te słowa dyskusji, która miała miejsce podczas konferencji Droniada Tech 2023. Uczestnicy odbywającego się pod merytorycznym patronatem Sektorowej Rady ds. Kompetencji – Informatyka panelu „Jakich kompetencji potrzeba, by opanować AI?" nie mieli wątpliwości co do tego, że ludzie są niezbędni do właściwego, pełnego wykorzystania potencjału tej nowej technologii.

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

Ludzie od danych

O powodzeniu projektów dotyczących rozwiązań bazujących na sztucznej inteligencji decydują nie tylko specjaliści z najbardziej spektakularnymi, nagłośnionymi medialnie kwalifikacjami. Owszem, programiści są niezbędni. Zanim jednak przystąpią do działania, ktoś musi przygotować dane potrzebne do stworzenia właściwego modelu. Jak zauważył Dominik Ogonowski, CEO Data Julce Lab, reguła GIGO (*Garbage in, garbage out* – śmieci na wejściu, śmieci na wyjściu) wciąż obowiązuje.

Potrzebni są więc ludzie, którzy rozumieją potrzebę odpowiedniej obróbki danych i potrafią to robić. – *To zazwyczaj trudna, żmudna praca, mało kto chce się jej podjąć. To jednak praca niezbędna, praca organiczna, praca u podstaw. Od jej wyników zależy w dużej mierze sukces całego przedsięwzięcia* – podkreśla Dominik Ogonowski. Na dodatek to praca długotrwała, bardzo angażująca zespół projektowy. Przykładowo, spośród 12 miesięcy potrzebnych na opracowanie modelu, 9 miesięcy może zajmować czyszczenie i przygotowanie danych.

Ludzie od relacji

Z drugiej strony, w firmach tworzących produkty lub usługi wykorzystujące sztuczną inteligencję nie może zabraknąć tych, którzy potrafią rozmawiać z klientami. Chodzi nie tylko o umiejętności zdefiniowania zakresu i sposobu realizacji projektu oraz negocjowania warunków umowy. Potrzebni są ludzie, którzy potrafią wytłumaczyć, na czym polega działanie stosowanej technologii (metody sztucznej inteligencji są skomplikowane a wiedza na ich temat nie jest jeszcze powszechnie dostępna), jakie jest w tym kontekście zadanie dostawcy zamówionych rozwiązań, jakich efektów pracy można się ostatecznie spodziewać.

Często też klientowi trzeba pomóc uświadomić jego faktyczne potrzeby i podpowiedzieć, jak przy użyciu nowych narzędzi można rozwiązać jego problemy. – *Trzeba umieć odróżnić to, co mówi klient, od tego, jaki ma naprawdę problem, co chce uzyskać. Bo nie zawsze to, co mówi, jest tym, czego naprawdę potrzebuje. Trzeba umieć odczytać faktyczne potrzeby klienta – tak jak w negocjacjach trzeba umieć odróżnić stanowisko od interesów* – tłumaczył Karol Kapuściński, Head of Strategic Sales w No Fluff Jobs. Klient oczekuje rozwiązania problemu, który ktoś musi najpierw zrozumieć, aby potem można było dobrać odpowiednie sposoby zaradzenia mu.

Na dodatek rozmowy z klientami są często pełne emocji, napięć, rozbieżnych oczekiwań i różnych sposobów rozumienia tych samych zagadnień. Do ich prowadzenia nie wystarczą tylko tzw. twarde kompetencje, specjalistyczna, inżynierska wiedza i takież umiejętności. Tutaj przyda się znajomość wyzwań biznesowych, umiejętność negocjacji, rozumienia intencji rozmówcy, przydadzą się zdolności psychologiczne czy też po prostu zwykłe życiowe doświadczenie. Pojawienie się sztucznej inteligencji nic w tym zakresie nie zmienia – nadal w kluczowych aspektach współpracy z partnerami biznesowymi decydujące są relacje międzyludzkie.

Ludzie od współpracy

Ważna jest też umiejętność komunikowania się ludzi pracujących w jednym zespole projektowym czy w tej samej firmie realizującej zadania związane z wykorzystaniem technik AI. Chodzi o zdolność porozumiewania się między sobą (dogadywania się), wzajemnego rozumienia się i odpowiedniego reagowania na podejmowane przez innych działania.

Nie jest to łatwe, bo w skład zespołów wchodzą różni specjaliści, mówiący różnymi językami zawodowymi, mający różne zasoby profesjonalnej wiedzy i fachowych umiejętności. Poza tym są to różni ludzie – z bagażem różnych doświadczeń życiowych, wywodzący się z różnych środowisk, cechujący się różnymi predyspozycjami psychologicznymi i mający różne charaktery. Do tego dochodzą, mające miejsce w każdym projekcie, sytuacje stresowe, na które każdy inaczej reaguje.

Tych kompetencji u pracowników – zwanych czasem kompetencjami miękkimi, a czasem społecznymi – najbardziej pracodawcom z sektora IT w naszym kraju brakuje. Edukacja na studiach ich nie zapewnia, czego potwierdzenie znaleźć można m.in. w wynikach Branżowego Bilansu Kapitału Ludzkiego w sektorze IT. – *Z twardymi kompetencjami wśród specjalistów nie mamy problemu. Uczelnie dobrze kształcą w tym zakresie. Problemem jest natomiast znalezienie specjalistów z umiejętnością komunikowania się z innymi. Musimy uczyć ludzi tych kompetencji już w firmie, by mogli poradzić sobie również z występującymi w każdym biznesie wyzwaniami pozatechnologicznymi* – mówił podczas panelu Dominik Ogonowski.

Ludzie od zarządzania

Czy to znaczy, że programista-introwertyk, genialny w swojej dziedzinie profesjonalista, ale mający trudności w porozumiewaniu się z innymi nie może znaleźć się wśród członków grupy pracującej biznesowo nad produktami z zakresu sztucznej inteligencji? Oczywiście dla takich osób też jest miejsce w zespole projektowym. Potrzebny jest jednak sprawny menedżer, lider, kierownik projektu, który będzie potrafił umiejętnie zarządzać zespołem złożonym z różnych osobowości, tworzących mocno zróżnicowane środowisko pracy.

Zdaniem Rafała Łuczaka, IT and Implementation Managera w ESA logistika, dobre zarządzanie zespołem to zarządzanie wiedzą – na temat potrzeb klienta, potencjału zespołu, możliwości poszczególnych jego członków, dostępnych na-

rzędzi i technologii. Gdy się dysponuje odpowiednią wiedzą, wtedy można dobrać odpowiednich ludzi do zespołu, który skutecznie zrealizuje postawione zadanie. Ta wiedza tworzona jest przez wszystkich uczestników biznesowo-technicznych relacji. Wszyscy się od wszystkich wzajemnie uczą. – *Dostawcy technologii dają wiedzę techniczną, my, użytkownicy narzędzi technicznych, dajemy wiedzę biznesową* – tłumaczy Rafał Łuczak.

Duża wartość dodana dla firmy powstaje wtedy, gdy pracownik rozumie nie tylko materię techniczną, lecz także kontekst biznesowy, czyli wartość projektu i związane z jego realizacją ryzyka. Dobór ludzi jest więc bardzo ważny, menedżer musi umieć zbalansować różne potrzeby i uwarunkowania. Musi wiedzieć kiedy postawić na rozwój kompetencji komunikacyjnych zespołu, a kiedy skupić się na poszukiwaniu specjalisty z konkretnymi umiejętnościami technicznymi, na przykład w zakresie budowy sieci neuronowych. Jeden i drugi obszar kompetencyjny jest ważny i musi być w zespole projektowym obecny.

Trzeba się też nauczyć zarządzania problemami, stresem, ryzykiem. Tylko człowiek będzie sobie w stanie z tymi wyzwaniami poradzić. Ludzie kreatywni nigdy nie znikną z rynku. Zawsze będą potrzebne osoby, które będą potrafiły połączyć wszystkie, różnorodne elementy procesów i środowisk organizacyjnych w spójną całość. – *Procesy księgowe, na które składają się stałe, powtarzalne działania, jesteśmy w stanie zastąpić przez automaty czy roboty. Księgowej, która zna uwarunkowania prawne, potrafi zarządzać ryzykiem w kontekście finansowym, nie zastąpi sztuczna inteligencja. Zbyt dużo warunków brzegowych trzeba by było wziąć pod uwagę i zbyt długo trenować system, by stworzyć odpowiednie oprogramowanie* – uważa Rafał Łuczak.

Ludzie od komunikacji

Jak pokazują światowe trendy, sztuczna inteligencja jest i będzie wykorzystywana w głównej mierze do automatyzacji różnorodnych procesów i działań, zazwyczaj powtarzalnych, dających się zestandaryzować. Nie oznacza to jednak pozostawienia jej samej sobie. Potrzebni będą ludzie, którzy będą potrafili w odpowiedni i skuteczny sposób korzystać z dobrodziejstw sztucznej inteligencji.

W pierwszej kolejności, jak pokazują wyniki różnych badań, będą poszukiwane osoby z umiejętnością krytycznego myślenia. Posłużyć im ono może m.in. do diagnozowania uprzedzeń zapisanych w algorytmach stosowanych w narzędziach AI.

> *Zjawisko przechyłu czy stronniczości systemów bazujących na sztucznej inteligencji (tzw. biasu poznawczego) jest dzisiaj dużym problemem przy korzystaniu z narzędzi AI.*

Kompetencje pozwalające na skuteczne radzenie sobie z tym problemem będą z pewnością jednymi z najbardziej poszukiwanych kompetencji przyszłości. Dla dobrego wykorzystania sztucznej inteligencji potrzebne będą generalnie umiejętności radzenia sobie z etycznymi aspektami zastosowania tej technologii.

Inną, równie cenną umiejętnością będzie umiejętność komunikowania się z systemami sztucznej inteligencji. W przypadku narzędzi generatywnych, jak chociażby Chat GPT, w cenie będą specjaliści od budowania tzw. promptów. – *W Polsce już widzimy trend związany z tworzeniem się nowej dziedziny, nowej specjalności na rynku pracy – prompting engineering. W Stanach Zjednoczonych tej grupie specjalistów już oferuje się bardzo wysokie zarobki* – mówił Karol Kapuściński. Zwracał przy tym uwagę, że cały czas istnieje też zapotrzebowanie na deweloperów, chociaż dla efektywnego tworzenia i wykorzystania technik sztucznej inteligencji potrzebna jest również reprezentacja wielu zawodów okołotechnicznych, okołoinformatycznych, na które wraz z rozwojem AI będzie z pewnością rosło zapotrzebowanie.

Ludzie od nauczania

Dużym wyzwaniem jest stworzenie i realizacja odpowiedniego modelu kształcenia i przygotowywania do aktywności zawodowej przyszłych specjalistów od różnych aspektów sztucznej inteligencji. – *Praca w grupie, komunikacja między członkami zespołu z pewnością ma kluczowe znaczenie dla realizacji projektów. Być może ten aspekt kształcenia jest rzeczywiście zaniedbany na polskich uczelniach. Prace dyplomowe są w zasadzie robione jednoosobowo, grupowe są niechętnie widziane* – mówił prof. Konrad Wojciechowski z Polsko-Japońskiej Akademii Technik Komputerowych i Politechniki Śląskiej.

Zwracał przy tym uwagę, aby nie podchodzić do tej kwestii zbyt dogmatycznie, zbyt rygorystycznie. Ludzie są bowiem różni. Zdolni programiści mają często nikłe skłonności czy umiejętności kontaktu z innymi osobami. Ich zachowania i potrzeby trzeba uwzględniać zarówno w procesach kształcenia, jak i potem organizacji pracy. Może to być też z korzyścią dla wszystkich, gdy na przykład wiele skomplikowanych zadań będzie w stanie rozwiązać właśnie tylko ten pracujący w pojedynkę programista.

Zdaniem prof. Konrada Wojciechowskiego, trzeba uczyć przede wszystkim myślenia, krytycznego podejścia zarówno do możliwości technik sztucznej inteligencji, jak i własnych kompetencji. Nie warto próbować robić wszystkiego samemu. Uczeni na całym świecie tworzą olbrzymią ilość publikacji, tak samo jak firmy wypracowują całą masę zaawansowanych algorytmów. Sztuczna inteligencja wymaga do uczenia modeli olbrzymich ilości danych, które posiadają tylko największe, światowe koncerny. Przede wszystkim trzeba nastawiać się na rozwiązywanie problemów, a nie na

tworzenie sztucznej inteligencji. Nie można też zapominać o tym, że to wymaga ogromnego wysiłku. AI czy ML dobrze brzmi, ale przy tworzeniu tego typu rozwiązań trzeba się mocno napracować.

Ludzie od rozwoju

Zdaniem Rafała Łuczaka, wielu młodych ludzi, w tym m.in. studenci, potrafi dobrze radzić sobie z problemami, bo nie szukają rozwiązań tam, gdzie starsi. Bo czasy są inne, bo są nowe możliwości, o których my możemy jeszcze nie pomyśleć. Olbrzymią rolę w kształtowaniu postaw młodych pracowników i specjalistów mają też zatem do odegrania pracodawcy i menedżerowie.

Zdaniem Karola Kapuścińskiego, nie możemy od następnych pokoleń oczekiwać, by zachowywały się tak jak my, bo żyją już w innych warunkach, w innych okolicznościach. Liderzy muszą stworzyć ludziom środowisko do wzrostu, do rozwoju, pozwolić im w tym celu również na popełnianie błędów, chociaż w biznesie jest to trudne. Ściśle wytyczone ścieżki działania ograniczają jednak rozwój. Podejście menedżerskie wiele znaczy – potrafi wyzwolić kreatywność, ale może też ją zabić. Dobre wykorzystanie czasu i potencjału pracowników najbardziej kreatywnych, najbardziej aktywnych to, zdaniem Karola Kapuścińskiego, duże wyzwanie dla biznesu. Szczególnie w kontekście rozwoju sztucznej inteligencji, której praktyczne zastosowania będą szły głównie w kierunku automatyzacji, optymalizacji i przyspieszania procesów oraz zwiększania efektywności działań.

Już po raz dziesiąty Fundacja Instytut Mikromakro zorganizowała Droniadę – konkurs technologiczny dla zespołów akademickich oraz drużyn złożonych z innowatorów i pasjonatów nowych technologii. Tegoroczna Droniada Challenge, która odbywała się na Polach Marsowych w Parku Śląskim, wymagała połączenia kompetencji z obszaru IT, robotyki i sztucznej inteligencji. Od samego początku Droniada pomyślana jest jako impreza interdyscyplinarna, nastawiona na promocję rozwiązań integrujących różne technologie, głównie technologie cyfrowe. Drony są w tym ujęciu przede wszystkim elementem systemu gromadzenia i przetwarzania danych i informacji, a nie tylko statkami powietrznymi w ujęciu lotniczym. Uczestniczące w zmaganiach zespoły miały w tym roku do wyboru sześć konkurencji, w których mogły wystartować: Drzewo życia, Rurociąg, Intruz, Fly to Rescue, Sztafeta. Zadania polegały m.in. na wykryciu i oznaczeniu określonego stanu rzeczy, identyfikacji zmian, wskazaniu „intruza", poszukiwaniu zaginionych osób czy sprawdzeniu ścieżki ewakuacji dla ratowników. Obowiązkowa dla wszystkich była natomiast demonstracja przygotowanego systemu.

Częścią X Droniady była konferencja Droniada Tech poświęcona sztucznej inteligencji w dronach i robotyce. Na temat perspektyw rozwoju zastosowań sztucznej inteligencji oraz związanych z tym szans i zagrożeń wypowiadali się przedstawiciele środowisk naukowych i biznesowych, sektora publicznego oraz organizacji pozarządowych. Sektorowa Rada ds. Kompetencji – Informatyka była patronem merytorycznym przeprowadzonego w ramach konferencji panelu dyskusyjnego „Jakich kompetencji potrzeba, by opanować AI?".

Emulatory, symulatory i klony

Odpowiedź na pytanie, po co nam w informatyce emulatory, wydaje się oczywista: żeby opracowywać różne produkty IT szybciej i taniej. Emulatory są narzędziami inżynierii oprogramowania, często wykorzystywanymi także w dydaktyce informatyki. Od lat są też obiektem działalności hobbystycznej – dzięki nim starsi informatycy mogą powspominać sobie czasy, kiedy byli młodzi i piękni…

Warto przypomnieć definicje emulatorów oraz symulatorów i różnice między nimi. Pojęcia te wydają się bowiem trochę na siebie nakładać.

W dziedzinie inżynierii oprogramowania emulatorem nazywane jest oprogramowanie, dzięki któremu zachowanie systemu operacyjnego jednej platformy sprzętowej (pełniącej funkcję gospodarza, czyli hosta) „imituje" zachowanie środowiska systemowego innego systemu (gościa). Imitacja taka realizowana jest poprzez translację zestawu instrukcji gościa do poziomu kodu maszynowego hosta. Emulować można pracę jednostki centralnej (procesora), systemu dostępu do pamięci, systemu urządzeń peryferyjnych – zazwyczaj stosowane są wszystkie te rozwiązania na raz.

dr Tomasz Kulisiewicz
wykładowca i analityk rynku ICT

Symulator natomiast modeluje środowisko programistyczne, w którym ma działać jakiś produkt – ale nie jest to całościowe „imitowanie" tego środowiska, a tylko zmiennych programowych w różnych konfiguracjach. Dlatego symulatory można tworzyć w językach wysokiego poziomu i nie ma potrzeby schodzenia aż do poziomu kodu maszynowego, jak w emulatorach.

Formalne definicje emulatorów i symulatorów znaleźć można w oficjalnych dokumentach – słownikach organizacji standaryzacyjnych[1] oraz w słownikach opracowanych przez Grupę Roboczą International Software Testing Qualification Board (ISTQB)[2]. W polskiej wersji językowej definicje dostępne są dzięki tłumaczeniom kolejnych wersji słowników ISTOB[3], wykonanym przez zespoły Stowarzyszenia Jakości Systemów Informatycznych (będącego członkiem stowarzyszenia ISTOB).

Definicje formalne nie wyznaczają ostrej granicy między emulatorami a symulatorami, łatwiej ją zauważyć, rozpatrując obszary ich zastosowań.

Sfera zastosowań emulatorów rozciąga się od emulatorów domowych komputerków 8-bitowych, które pisane są przez hobbystów, chcących dzięki nim grać w swoje ulubione gry z czasów młodości, aż po emulatory dawnych komputerów (w tym systemów mainframe) lub systemów

	Emulator	Symulator
Według ISO/IEC/IEEE 24765:2017	Urządzenie, program komputerowy lub system, który przyjmuje takie same wejścia i generuje takie same wyjścia jak dany system	Urządzenie, program komputerowy albo system używany podczas testowania, który przy zadanym zbiorze wejść zachowuje się lub działa tak jak dany system
Wersja skrócona ze słownika ISTOB	Oprogramowanie używane podczas testowania, które naśladuje zachowanie sprzętu	Moduł systemu używany podczas testowania, który zachowuje się lub działa jak dany moduł lub system

Staruszek emulator

Historycznie teoria i praktyka emulacji wywodzi się z połowy lat 60. W 1965 r. pojawił się emulator umożliwiający użytkownikom starszych systemów IBM – serii 1400/1620 i 7000 – pracę używanego przez nich oprogramowania na nowych maszynach serii 360 (które pojawiły się od 1964 r.) i 370 (1970 r.), które miały już architekturę bajtową w odróżnieniu od poprzednich architektur słowowych (o różnych długościach słów, przez co systemy nawet wewnątrz serii 1400/1620/7000 nie były ze sobą kompatybilne). Emulatory w systemach 360/370 realizowane były na poziomie dodatkowych elementów mikrokodu, przy czym w serii 360 do wejścia w tryb emulacji trzeba było restartować komputer w tym trybie (wyjątkiem była jedna z największych maszyn serii – 360/85), natomiast w systemie 370 tryb emulacji można było już uruchomić z poziomu systemu operacyjnego. Dla produkowanych od połowy lat 70. maszyn nowej serii ICL 2900, o architekturze bajtowej, działających pod kontrolą systemu VME opracowano dodatkową opcję – oprogramowanie DME (Direct Machine Environment) w dwóch wersjach, dla dwóch architektur systemów ICL: emulującej środowisko ICL 1900 oraz emulującej środowisko Systemu 4. Później powstała też wersja CME (Concurrent Machine Environment), umożliwiająca jednoczesną pracę zarówno emulowanych systemów operacyjnych, jak i oprogramowania użytkowego serii 1900 i Systemu 4 na jednej maszynie fizycznej[4].

1 *Systems and software engineering vocabulary* – norma ostatnio przeglądana i zatwierdzona we 2022 r. (https://www.iso.org/standard/71952.html)

2 *Standard Glossary of Terms Used in Software Testing*. Słownik dostępny jest w formie usługi webowej na stronie https://glossary.istqb.org. ISTOB jest stowarzyszeniem non-profit zarejestrowanym w Belgii.

3 https://sjsi.org/ist-qb/do-pobrania/. Pełen słownik *Standardowy słownik terminów wykorzystywanych w testowaniu oprogramowania* generowany jest obecnie w wersji 4.3.2. na otwartej licencji CC 4.0 International (dostęp: 22.11.2023).

4 A. Szczerba, *Firma ICL w Polsce* (https://historiainformatyki.pl/common/files_download.php?fid=225, dostęp 21.11.2023).

W kilku systemach Odra 1305 pracujących jeszcze w latach 90. (a nawet dłużej – maszyny na stacjach PKP Lublin Tatary i Wrocław Brochów zostały wyłączone z eksploatacji w 2010 r.) zastosowano emulatory urządzeń peryferyjnych działające na komputerach klasy IBM PC, m.in. emulatory konsoli operatorskiej DZM 180. Programy-emulatory (np. Konsola 5.0) współpracowały z jednostką centralną Odry poprzez specjalnie w tym celu opracowane karty Superkon S2 i z interfejsem RS232C[5].

Natomiast w latach 1984–1987 we wrocławskim Instytucie Komputerowych Systemów Automatyki i Pomiarów powstał emulator całego systemu Odra 1305 na maszyny R-32 i R-34. Emulowany system operacyjny Odry 1305 (E6RM, a nawet wielodostępny system GEORGE3) obsługiwał wirtualną jednostkę centralną i wirtualne urządzenia peryferyjne: dyski 30 MB, pamięci taśmowe PT3, drukarkę wierszową, konsolę operatorską DZM180, a nawet czytniki tasiemki papierowej (CT) i kart dziurkowanych (CK). Później emulator został rozbudowany o moduł teleprzetwarzania systemu 1305 obsługujący lokalne i zdalne monitory ekranowe. Na maszynach R-34 emulator działał jako zadanie w systemach OS 5.01 VS1 i VM. Emulatory te działały m.in. w ZETO Łódź i ZETO Lublin, a także w ośrodku komputerowym producenta farmaceutycznego Gedeon-Richter w Budapeszcie oraz w jednym z ośrodków w ówczesnej Czechosłowacji[6].

operacyjnych, tworzone nie tylko w celach hobbystycznych czy dydaktycznych, lecz także użytkowych. Dzięki emulatorom można bowiem uniknąć portowania starych systemów użytkowych (nazywanych systemami legacy czy odziedziczonymi) do innego środowiska systemowego, co wymaga pracochłonnej re-inżynierii – zwłaszcza w sytuacji braku pełnej dokumentacji systemów legacy nierzadko przerabianych czy uzupełnianych przez lata i dekady, tworzonych w językach programowania, dla których brakuje dziś specjalistów.

Wyrazistym przykładem takich sytuacji są systemy bankowe czy finansowo-księgowe tworzone kiedyś w COBOL-u. Budowanie systemów od nowa jest z wielu powodów często odkładane na później – zwłaszcza w administracji publicznej. Problemy eksploatacji systemów legacy występowały w kraju np. w połowie lat 80. Po zakończeniu w 1983 r. produkcji (a potem stopniowo także eksploatacji) systemów Odra 1305 w administracji państwowej, w ośrodkach ZETO oraz w głównie państwowych wtedy jeszcze przedsiębiorstwach pojawiło się zapotrzebowanie na eksploatację systemów opracowanych dla środowiska Odry 1305 na nowszych maszynach kompatybilnych z systemami IBM 360/370 – zwłaszcza na produkowanych wtedy przez ELWRO systemach R-32/34 serii RIAD. Odpowiedzią było opracowanie emulatorów systemu Odra 1305 działających w środowisku systemu OS maszyn R-32/R-34.

Emulowanie zamiast re-inżynierii lub portowania stosowane było też m.in. w systemach bankowych i innych systemach transakcyjnych w Polsce (i ogólnie w Europie Środkowej i Wschodniej) w czasach prywatyzacji banków lokalnych dokonywanej z udziałem inwestorów branżowych – banków z Europy Zachodniej i USA, które dość często stosowały stare systemy. Systemy legacy do dziś występują też w administracji publicznej[7], ale nie znalazłem krajowych przykładów emulowania ich środowisk w nowszych systemach.

Ciekawymi przykładami emulacji starszych systemów dla celów hobbystycznych i historycznych są emulatory niemal wszystkich sławnych brytyjskich komputerów, zgromadzone lub stworzone przez brytyjskie Computer Conservation Society – od Manchester „Baby"/Small Scale Experimental Machine z 1948 r. i komputera EDSAC z 1949 r. zbudowanego w Laboratorium Matematycznym Uniwersytetu Cambridge przez maszyny serii ICL 1900 aż po emulator domowego komputerka BBC Micro, produkowanego przez firmę Acorn Computers w latach 1981–1994 w ramach Computer Literacy Project stacji telewizyjnej BBC.

Dziś bezsprzecznie najciekawszym polskim emulatorem jest EM400 Jakuba Filipowicza – emulator Mery 400, któremu towarzyszy portal/wiki mera400.pl, biblioteka wiedzy o Merze 400 (a przy okazji także o K-202) wraz z autorskimi serwisami na kanale YT oraz Facebooku[8]. Jak pisze autor

5 https://www.elektroda.pl/rtvforum/topic1167261-60.html (dostęp; 23.11.2023). W dyskusji na forum jeden z uczestników wspomniał też o emulatorze Odry 1305, działającym na mainframe IBM, ale nie udało mi się znaleźć śladów eksploatacji emulatorów Odry 1305 np. na sprowadzanych do Polski pod koniec lat 80. używanych maszynach IBM serii 3031-3033, 3081-3833, 4331-4381 czy ich „klonach" (np. Hitachi Data Systems, Comparex Comparex Informationssysteme GmbH, Siemens Data Systems).

6 http://elwro.info.pl/files/rys/163_1987_11_1.pdf (dostęp 21.11.2023).

7 A. Sobczak *Modele postępowania z systemami legacy w administracji publicznej* (https://rocznikikae.sgh.waw.pl/p/roczniki_kae_z52_18.pdf – dostęp 21.11.2023).

8 https://www.facebook.com/mera400/ oraz https://www.youtube.com/@MERA400

na portalu, emulowanymi elementami systemu są: procesor (także w wersji z przeróbkami wprowadzonymi w komputerze MX-16, następcy Mery 400 produkowanym przez Amepol w latach 1985–1988), arytmometr wielokrotnej precyzji (FPU), pamięć ferromagnetyczna produkcji ELWRO, półprzewodnikowa pamięć MEGA Amepolu, kanał znakowy, procesor peryferyjny MULTIX, dysk Winchester oraz terminal znakowy. EM400 poprawnie wykonuje oryginalne oprogramowanie Mery 400, łącznie z systemem operacyjnym CROOK, a także fabryczne testy procesora.

Za emulator środowiska Windows uważane bywa oprogramowanie Wine dla środowiska uniksowego. Jednak jest ono raczej metodą uruchamiania oprogramowania w innym środowisku systemowym, polegającą na translacji wywołań Windows API na wywołania POSIX API dla systemów GNU/Linux, FreeBSD czy Solaris – jest więc warstwą implementacyjną WinAPI w środowisku Unix/X11. Choć twórcy Wine podkreślili w jego „rekurencyjnej" nazwie, że *Wine is not an emulator*, to według niektórych definicji jest to rodzaj emulacji – emulacja API.

Różnicę mocy obliczeniowej i pojemności pamięci między komputerami z lat 60. i 70. a układami dzisiejszymi pokazują udane próby realizacji emulatorów wielkich kiedyś systemów na takich komputerkach, jak Raspberry Pi czy realizowany przez J. Filipowicza projekt MERA-400f – reimplementacja jednostki centralnej komputera MERA-400 na układzie FPGA wykonana w języku Verilog[9]. MERA 400f emuluje pracę komputera w środowisku systemu CROOK-5.

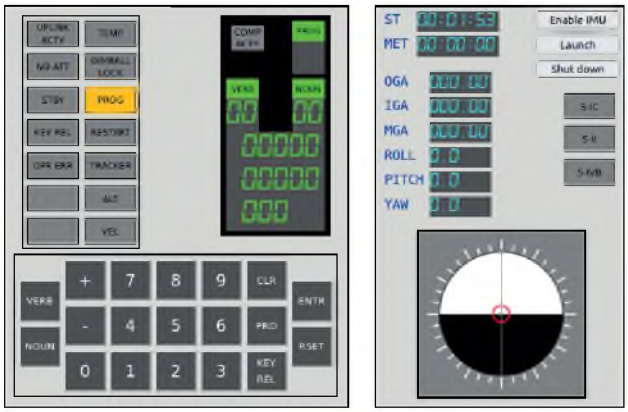
Obszerne listy emulatorów najpopularniejszych konsol do gier dostępne są pod adresemi:

https://github.com/alnacle/awesome-emulators,

zaś komputerów (od systemów 64-bitowych aż po kalkulatory programowalne) pod adresem:

https://en.wikipedia.org/wiki/List_of_computer_system_emulators

W 2005 r. John Pultorak, inżynier oprogramowania w firmie Lockheed Martin Space, uruchomił budowaną w piwnicy przez 4 lata sprzętową działającą replikę sławnego Apollo Giudance Computer (AGC), komputera pokładowego statków Apollo. Koszt zwykłych układów kupowanych w sklepach elektronicznych wyniósł ok. 3 tys. dolarów. AGC w końcu lat 60 kosztował ok. 200 tys. dolarów, co odpowiada dzisiejszej kwocie ok. 1,5 mln USD. W 2019 r. 50 rocznica lądowania Apollo 11 na Księżycu (21 lipca 1969 r.) zaowocowała wysypem emulatorów i symulatorów komputera AGC.



Konsola DSKY symulatora Apollo Guidance Computer

Źródło: https://svtsim.com/moonjs/agc.html

Symulatory i obszary ich zastosowań

Symulatory jednoznacznie kojarzą się z urządzeniami symulującymi pracę czy działanie całych złożonych urządzeń z wykorzystaniem zaawansowanych rozwiązań programowych i wizualizacyjnych.

W lotnictwie symulatory (trenażery) służą zarówno do uczenia sztuki pilotażu początkujących pilotów, jak i do uzyskiwania, utrzymywania lub podwyższania uprawnień oraz treningu dla pilotów zawodowych. Historia symulatorów lotniczych sięga czasów przed I wojną światową, kiedy we Francji zbudowano urządzenia do wstępnego szkolenia pilotów.

Drewniany symulator Antoinette z 1910 r.

Źródło: https://www.halldale.com/articles/20498-the-antoinette-barrel-a-training-device-upon-request

Na prostych symulatorach uczono też celowania i strzelania pilotów i strzelców pokładowych podczas I wojny światowej. Pierwsze urządzenie odwzorowujące kabinę pilota umieszczoną na stelażu z siłownikami umożliwiającymi ruch kabiny opracował w 1927 r. amerykański wynalazca i pilot Edwin Link. Produkcję symulatora nazwanego Link Trainer zaczął w 1929 r. w rodzinnej fabryczce pianin i organów. Początkowo instalowano je w parkach rozrywki, bo dowództwo U.S. Army Air Force nie było tym wynalazkiem zainteresowane. Dopiero

9 https://github.com/jakubfi/mera400f (dostęp 21.11.2023).

po serii wypadków pilotów wojskowych w 1934 r. lotnictwo USA kupiło 6 symulatorów Linka[10]. Podczas II wojny na ponad 10 tys. udoskonalonych symulatorach Link Trainer przeszkolono ok. 50 tys. alianckich pilotów. Dziś symulatory lotnicze (określane zbiorczym skrótem FSTDF – *Flight Simulation Training Device*) są urządzeniami nakazanymi, regulowanymi i certyfikowanymi przez międzynarodowych i narodowych[11] regulatorów transportu lotniczego na całym świecie.

Symulator Boeing 737 #3 EASA ID PL-14 w ośrodku szkoleniowym AFG-Enter Air w Warszawie

Źródło: https://www.afgsim.com/pl/symulatory-lotu-full-flight/boeing/737-easa-pl-14-03

Przykładami dzisiejszych krajowych zastosowań mogą być symulatory samolotów Boeing 737 NG oraz Embraer 190 w LOT Flight Academy czy symulator CAE 7000 XR Boeingów 737 NG w warszawskim centrum szkoleniowym operatora czarterowego Enter Air. Na symulatorach produkcji firmy Airbus we współpracy z warszawską firmą ETC-PZL Aerospace Industries szkolą się piloci wojskowi w dęblińskiej Szkole Orląt (4. Skrzydle Lotnictwa Szkolnego), zaś na zaawansowanym dedykowanym symulatorze śmigłowca Eurocopter EC135 – piloci Lotniczego Pogotowia Ratunkowego[12]. Symulatory wykorzystuje się do szkolenia mechaników lotniczych, kierowców, maszynistów kolejowych, sterników statków, a od kilku lat – także chirurgów[13]. W rozwijaniu najsłynniejszego symulatora „gamingowego", Flight Simulatora Microsoftu, uczestniczyło i nadal uczestniczy wielu profesjonalnych pilotów i specjalistów lotniczych[14].

Już w latach 70. XX w. działało na świecie kilka symulatorów/trenażerów dla operatorów elektrowni jądrowych. Budowa takich symulatorów oraz ich wykorzystywanie w szkoleniach wzrosło po wypadku w elektrowni jądrowej Three Mile Island w USA w marcu 1979 r. Komisja badająca przyczyny, przebieg i skutki wypadku (po którym elektrownię zamknięto) jako jedną z przyczyn przerodzenia się stosunkowo drobnej usterki jednego z zaworów w poważne zagrożenie (stopienie się ok. 1/3 rdzenia reaktora) uznała brak odpowiedniego wyszkolenia i nieprawidłowe decyzje operatorów siłowni. Zalecenia Międzynarodowej Agencji Energii Atomowej[15] oraz regulacje krajów, w których działają elektrownie jądrowe, spowodowały, że dziś większość elektrowni ma pełnoskalowe symulatory, wiernie odwzorujące konkretną instalację (*plant specific full-scope simulator*), na których prowadzone są obowiązkowe szkolenia operatorów.

„Odwrócona emulacja"

Kilka przedsięwzięć znanych z historii informatyki można by nazwać „odwróconą emulacją". Przedsięwzięcia takie polegały na odzwierciedleniu (skopiowaniu) architektury logicznej istniejących konstrukcji znanych systemów z zachowaniem kompatybilności na poziomie kodu maszynowego, ale przy użyciu innego sprzętu, przede wszystkim innej bazy technologicznej, na którą składały się dostępne podzespoły oraz możliwe do opanowania procesy produkcyjne. W opracowaniu „Własne konstrukcje, licencje, klony"[16] opisuję kilka najbardziej znanych przedsięwzięć krajów naszego regionu Europy, przed 1989 r. mniej lub bardziej szczelnie odciętych od reszty świata Żelazną Kurtyną oraz ograniczeniami eksportowymi komitetu COCOM.

Taką „odwróconą emulację" – transpozycję architektury logicznej jednego systemu na inną bazę sprzętową – realizo-

10 Lotnictwo wojskowe USA zdobyło wtedy rządowy kontrakt na przewożenie poczty lotniczej, co wymagało latania w różnych warunkach meteorologicznych, z czym nie dawali sobie rady wojskowi piloci (https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196852/link-trainer/ dostęp: 22.11.2023).

11 W Polsce takim regulatorem jest Urząd Lotnictwa Cywilnego.

12 Zakupiony w ramach kontraktu na dostawę Eurocopterów dla LPR symulator kosztował ok. 25 mln zł, czyli ok. 25% więcej niż koszt jednego śmigłowca EC 135 (https://www.lpr.com.pl/pl/symulator-lotu-juz-odebrany/ dostęp 21.11.2023).

13 https://www.czd.pl/aktualnosci/symulator-do-szkolenia-z-zakresu-wykonywania-zabiegow-chirurgicznych-przy-uzyciu-robota-da-vinci-w-ipczd (dostęp 21.11.2023).

14 Opracowany w 1976 r. przez Bruce'a Artwicka i stworzony w jego firmie subLOGIC program Flight Simulator zadebiutował w wersjach na 8-bitowe komputery domowe Altair 8800 i IMSAI 8080 w 1977 r. W 1982 r. subLOGIC udzielił licencji na FS w wersji IBM PC Microsoftowi.

15 *Use of control room simulators for training of nuclear power plant personnel* (https://www-pub.iaea.org/MTCD/Publications/PDF/te_1411_web.pdf – dostęp 21.11.2023).

16 T. Kulisiewicz, Własne konstrukcje, licencje, klony. W: M. Noga, H.S. Nowak (red.), Polska informatyka: wizje i trudne początki (s. 55–94). PTI, Warszawa 2017.

wały m.in. elwrowskie systemy Odra serii 1300 (ok. 90 sztuk Odry 1304 oraz ponad 500 systemów Odra 1305/1325, binarnie kompatybilnych z maszynami ICL 1900 i zaprojektowanych na podstawie tzw. porozumienia software'owego z ICL) czy węgierskie maszyny TPA – „klony" minikomputerów DEC serii PDP-8, PDP-11 oraz VAX-11. Łącznie zakład produkcyjny Instytutu Fizyki Węgierskiej Akademii Nauk (MSZKI KFKI) wyprodukował ich ponad 1600 sztuk, z czego ok. 1400 było własnymi konstrukcjami KFKI, a więc realizowało transpozycję architektury logicznej na inny sprzęt, a tylko 200 najpóźniejszych (w latach 1989-1990, po zawarciu formalnej umowy z DEC) było kopiami wykonanymi metodą „karta-karta". Produkowaną na podstawie umowy licencyjnej transpozycją francuskich maszyn CII 10010/Mitra-15 były węgierskie minikomputery VT1010B, bardziej znane jako R-10 i w kolejnych wersjach „dokooptowane" do systemu RIAD/JS EMC (z którym w zasadzie nie miały nic wspólnego z wyjątkiem oddzielnie zaprojektowanego systemu interfejsów do urządzeń peryferyjnych serii JS EMC).

Na podstawie licencji z Bull-General Electric pod koniec lat 60. komputery Tesla 200 i 370 kompatybilne z systemami Gamma 140/145 produkowały zakłady VHJ Tesla Pardubice w ówczesnej Czechosłowacji. Najbardziej znaną transpozycję zrealizowano we wspólnym projekcie RWPG produkcji maszyn jednolitego Systemu (JS EMC) – wytwarzanych przez kraje RWPG (z wyjątkiem Rumunii) na podstawie systemu IBM S/360 (a później S/370) – ale już „bez żadnego trybu", bez porozumienia z IBM. Przedsięwzięcie to, a także inne „odwrócone emulacje" tamtych czasów, np. jugosłowiańskie komputery Iskra Delta (licencyjne klony PDP) i rumuńskie Felixy (licencja francuskich Irisów firmy CII) opisuję w przywołanym opracowaniu.

Wirtualizacja

Rozwiązaniem zbliżonym do emulacji jest wirtualizacja, w tym wirtualizacja systemu operacyjnego. Według niektórych definicji wirtualizacja to emulowanie pracy maszyny z danym systemem operacyjnym, umożliwiająca uruchamianie wielu kompletnych maszyn wirtualnych (łącznie z ich systemem operacyjnym i obsługą urządzeń peryferyjnych) na jednym komputerze fizycznym. Między sprzętem „gospodarza" a oprogramowaniem „gościa" działa oprogramowanie nazywane hipernadzorcą (hypervisor). Zarządza ono maszynami wirtualnymi działającymi na maszynie fizycznej, obsługując wykorzystywanie przez maszyny wirtualne fizycznych zasobów sprzętowych i decydując, które procesy maszyn wirtualnych mogą korzystać bezpośrednio zasobów, a które procesy muszą być emulowane przez system hosta. Rozróżnia się hipernadzorców typu 1, działających bezpośrednio na sprzęcie fizycznym hosta (*bare-metal hypervisors*), oraz typu 2, działających jako programy uruchomione w systemie operacyjnym hosta.

Wirtualizacja jest wykorzystywana m.in. do uruchamiania w bezpieczny sposób oprogramowania testowanego już w jego środowisku pracy – ale wirtualnym. W wirtualnych środowiskach testuje się też oprogramowanie sterowników PLC (*Programmable Logic Controller*), tworzonych przeważnie w środowiskach wirtualnych. Specjalizowane narzędzia stosowane są często np. w systemach tworzenia sterowników używanych w przemyśle motoryzacyjnym – co stało się jedną ze specjalności firm działających w Polsce.

Niejako poniżej wirtualizacji ulokowana jest konteneryzacja, polegająca na „zamykaniu" aplikacji – jej procesów, konfiguracji i zależności – w wirtualnym zasobniku/kontenerze. Aplikacja otrzymuje własny obszar pamięci RAM i pamięci zewnętrznej, ewentualnie także prywatny adres IP. Kontenery są od siebie odseparowane, ale mogą się komunikować między sobą. Często wykorzystywanymi narzędziami konteneryzacji są Docker oraz Kubernetes, platformy do zarządzania, automatyzacji i skalowania skonteneryzowanych aplikacji, zwłaszcza w przypadku korzystania z wielu kontenerów w danym systemie.

Ten przegląd emulacji, symulacji i wirtualizacji można zakończyć pytaniem: czy któryś z tych terminów można odnieść np. do hybrydowego przetwarzania algorytmów kwantowych opisywanego przez prof. Marka Perkowskiego w 7 kolejnych odcinkach „Przewodnika po nauczaniu informatyki kwantowej", opublikowanego w wydaniach 2-4/2021 Biuletynu PTI i w 4 wydaniach „Domeny" w 2022 r.?

	Emulator	Symulator
Cel zastosowania	Zastąpienie rzeczywistego systemu/urządzenia	Sprawdzenie zachowywania się różnych systemów w różnych środowiskach
Kodowanie	W językach niskopoziomowych	W językach wysokopoziomowych
Obiekty „imitowane"	Sprzęt i oprogramowanie	Oprogramowanie
Prędkość działania	Zwykle mniejsza z uwagi na konieczność translacji aż do kodu maszynowego	Zwykle większa, bo nie jest potrzebna translacja do kodu maszynowego
Obszar zastosowań	Sprawdzanie wewnętrznego działania urządzenia/systemu	Sprawdzanie zewnętrznego zachowania się systemu/programu

Marek Valenta

Żegnamy i będziemy pamiętać

9 listopada 2023 r. z ogromnym smutkiem pożegnaliśmy na Cmentarzu Rakowickim w Krakowie Marka Valentę, niezwykłego Człowieka, informatyka, wyjątkowego pedagoga, serdecznego przyjaciela i społecznika. Jego życie, które zakończyło się 3 listopada 2023 r., było pełne pasji, zaangażowania i wielkiego oddania ludziom.

Marek Valenta urodził się 21 września 1947 r. w Krakowie jako syn lekarza Jana Alfreda i działającej społecznie Ireny. Ukończył studia na Wydziale Elektrotechniki Górniczej i Hutniczej w AGH, zdobywając tytuł magistra inżyniera, a w roku 1976 uzyskał stopień doktora nauk technicznych.

Od zawsze robił coś pożytecznego dla innych. Wszystko zaczęło się od ZHP: już w 1969 r. został szczepowym krakowskiego Szczepu „Żurawie", co było wyrazem wielkiego zaufania i wyzwaniem, bo Marek obejmował tę funkcję po jednej z harcerskich legend Krakowa – hm. Bogusławie Rybskim.

Marek był wyjątkowym instruktorem harcerskim. Miał dwie pasje: żeglarstwo i narciarstwo; jako jachtowy kapitan żeglugi bałtyckiej i instruktor narciarstwa przekazywał młodym nie tylko umiejętności, lecz także wartości, takie jak odwaga, uczciwość i szacunek dla innych. Wyrazem uznania było przyznanie Markowi Krzyża za zasługi dla ZHP, Honorowego Odznaczenia z okazji 100-lecia Harcerstwa w Krakowie, Srebrnej Odznaki 45-lecia Krakowskiego Okręgowego Związku Żeglarskiego oraz dwukrotnie Srebrnej Odznaki za pracę społeczną dla m. Krakowa.

Lata 80. XX w. to trudny czas zmian, narodziny i rozwój nowych dyscyplin naukowych i technologii. Na AGH powstaje pomysł częściowego uprządkowania organizacyjnego w obszarze młodej informatyki. Jak zwykle w takich przypadkach – wszystko zależało od zainteresowanych, a wśród nich dużą grupę zapaleńców stanowili pracownicy Instytutu Automatyki Wydziału Elektrotechniki, Automatyki i Elektroniki (pod dyrekcją profesora Henryka Góreckiego), pracujący w Zakładzie Informatyki kierowanym przez dr. hab. inż. Edwarda Nawareckiego oraz w Zakładzie Maszyn Matematycznych, kierowanym przez dr. hab. inż. Andrzeja Gościńskiego. Druga grupa entuzjastów pracowała w Międzyresortowym Instytucie Fizyki i Techniki Jądrowej (pod dyrekcją profesora Mariana Mięsowicza) w Samodzielnej Pracowni Techniki Obliczeniowej, kierowanej przez dr. hab. inż. Jacka Mościńskiego, zajmując się badaniami symulacyjnymi dużej skali. W 1980 r. został powołany Instytut Informatyki w ramach Wydziału Elektrotechniki, Automatyki i Elektroniki AGH, w którego skład weszła znaczna część zespołów tych jednostek, a dyrektorem został dr hab. inż. Jacek Mościński.

W tym środowisku Marek Valenta znakomicie odnalazł się naukowo i organizacyjnie.

> *Był niespokojnym i ożywczym duchem nowego Instytutu – o wielkiej wiedzy i równie wielkiej kulturze osobistej. Potrafił gromadzić podobnych do siebie zapaleńców wokół wspólnej idei czy też aktywności. Informatykę wówczas zaczynały coraz bardziej doceniać inne dyscypliny naukowe, w grę wchodziły zastosowania przemysłowe.*

W połowie lat 80. XX w. Marek został zastępcą dyrektora Instytutu Informatyki do spraw współpracy z otoczeniem naukowym i gospodarczym. Jego aktywność i skuteczność w nawiązywaniu kontaktów i kierowaniu realizacją wspólnych prac była wyjątkowa. Przyczyniały się do tego posiadane dobre podstawy teoretyczne i praktyczne w zakresie inżynierii oprogramowania i systemów baz danych oraz znajomość rozwiniętych na tej bazie nowatorskich w owym czasie rozwiązań z wykorzystaniem sztucznej inteligencji. Efektem było wiele systemów ekspertowych zastosowanych w praktyce, zwłaszcza w obszarze diagnostyki medycznej oraz profilaktyki i rozpoznawania zakażeń szpitalnych.

Marek pełnił także wiele innych ważnych funkcji na Uczelni: zastępcy dyrektora Uczelnianego Centrum Informatyki, pełnomocnika Rektora AGH ds. komputeryzacji uczelni, kierownika Studiów Podyplomowych „Systemy baz danych", członka Rady Wydziału Elektrotechniki, Automatyki i Elektroniki. Wszystkie te obowiązki wykonywał z ogromnym zaangażowaniem i odpowiedzialnością.

Cechowała Go nie tylko ogromna wiedza i doświadczenie, lecz także ciepło, życzliwość i niezwykłe poczucie humoru. Zawsze służył wsparciem, dzieląc się swoją mądrością z tymi, którzy tego potrzebowali, a Jego obecność pozwalała poczuć się bezpiecznie i komfortowo wszystkim członkom zespołu, bo zabiegał o docenienie każdego. Marek umiał wspaniale mówić o swoich pasjach. Pokój, w którym pracował, zawsze był otwarty dla rozmówców – na wejściu witał gości wspaniały model wielomasztowego żaglowca.

W Polskim Towarzystwie Informatycznym, które wypełniało wiele miejsca w Jego życiu, odegrał kluczową rolę. Był założycielem Oddziału Małopolskiego PTI i wielokrotnie pełnił funkcję prezesa tego Oddziału, był członkiem Zarządu Głównego przez dwie kadencje, jego opinie i rady zawsze były ważne, na czasie, wyważone, merytoryczne, emanujące spokojem i wyjątkowym poczuciem humoru, godne Członka Honorowego PTI. Marek był inicjatorem licznych przedsięwzięć edukacyjnych i naukowych, mających na celu propagowanie informatyki w społeczeństwie, wspierał edukację młodych, zdolnych osób zaczynając od uczniów szkół podstawowych.

Za wkład w polską informatykę i działalność w Polskim Towarzystwie Informatycznym został nagrodzony Medalem Komisji Edukacji Narodowej, Medalem 70-lecia Polskiej Informatyki, Srebrnym i Złotym Krzyżem Zasługi.

> *Swoim przykładem pokazywał nam, jak być lepszymi ludźmi. Dzięki Niemu wiele osób znalazło swoją drogę w informatyce, w PTI, w życiu. Odszedł od nas nie tylko nasz Przyjaciel, lecz także mentor i wzór do naśladowania.*

Jesteśmy wdzięczni za każdą chwilę spędzoną w Jego towarzystwie, za mądre rady, za każde uśmiechnięte „cześć". I każdego dnia będziemy.

Marian Bubak
wiceprezes PTI ds. naukowych, Oddział Małopolski oraz Scientific Affairs Director Sano Centre for Computational Medicine, Krakow (http://sano.science); kierownik Laboratorium Metod Informatycznych w Medycynie ACK Cyfronet AGH Kraków (http://dice.cyfronet.pl).

Beata Chodacka
nauczycielka informatyki w V LO i SP 33 w Krakowie, wiceprezeska Oddziału Małopolskiego PTI, animator działań na rzecz edukacji informatycznej, współtwórczyni zbioru zadań z informatyki exeBOOK. Współtwórczyni i współorganizatorka projektu „Klasa z ECDL". Koordynatorka merytoryczna w Centrum Mistrzostwa Informatycznego przy AGH, członek grupy SuperBelfrzy RP, inicjatorka i przewodnicząca Sekcji Informatyki Szkolnej PTI.

Jacek Kitowski
prof. dr hab. inż. na Wydziale Informatyki i ACK Cyfronet AGH Kraków, członek Oddziału Małopolskiego PTI. Kierownik Laboratorium Programu PLGrid ACK Cyfronet AGH, kierownik współpracy pomiędzy AGH a eksperymentem ALICE w Laboratorium CERN i Grupy CSG na Wydziale Informatyki AGH, https://www.icsr.agh.edu.pl/

Wiesław Paluszyński
prezes PTI

Fot. Beata Sołtys

Sztuka pisania listów

Siadłem do pisania 13 grudnia. Ten dzień kojarzył mi się dotychczas nierozerwalnie z pieszą wędrówką przez zaspy z domu do przyjaciół, których obudziłem rano informacją, że jest „wojna", a my musimy coś zrobić. Najpierw pomyśleli, że zwariowałem, a potem … to już inna opowieść. W tym roku 13 grudnia zaczął się jednak inaczej – od obserwacji, jak tam przebiegnie powrót demokratycznych zwyczajów w dziwnym dotychczas pałacu. Oglądałem, kto i za co będzie odpowiadał i zaraz siadłem do biurka, żeby przypominieć sobie trudną sztukę epistolografii. Część koleżeństwa zdążyła już mnie dopaść i wypytać, czy do tego ministra już napisałeś, a do tej ministry też?

Patrzę więc na listę i wybieram. Na pierwszy ogień wicepremier i minister cyfryzacji Krzysztof Gawkowski. Tu najłatwiej, bo jakoś z nami zaprzyjaźniony. W prowadzonym przez naszą Radę Naukową od wielu lat konkursie na najlepszą książkę informatyczną książka jego autorstwa „Cyberkolonializm. Poznaj świat cyfrowych przyjaciół i wrogów" została nagrodzona w 2019 r. I to jest odpowiedź na wątpliwości, po co nam Rada Naukowa. Jest przewidująca!

Ale co można napisać ministrowi od cyfryzacji na jednej stronie? Że jesteśmy, że cyfryzacja jest dla nas ważna, że oczekujemy uporządkowania wizji? Część kolegów na liście dyskusyjnej namawiała, aby napisać o natychmiastowej kontroli bezpieczeństwa zaufanego profilu, ePUAPu i mObywatela. Propozycja bliska memu sercu, bo kilka lat temu publicznie mówiłem, że nie będę z niego korzystał, bo jest niebezpieczny. Stan ten, niestety, pozostaje stabilny, bo do dzisiaj rozwiązanie nie otrzymało certyfikacji unijnej na najniższą nawet kategorię bezpieczeństwa. Czy jednak od razu w pierwszym liście … Więc zmieściłem się na jednej stronie i zaproponowałem, że jesteśmy w wielu wymienionych sprawach jako stowarzyszenie profesjonalistów do dyspozycji Pana ministra. Zobaczymy i po efektach poznamy.

Kolejny list i tu od razu problem, kobieta. W prasie piszą „ministra", a mnie to nie chce przez klawiaturę przejść, języka polskiego i gramatyki uczył mnie były asystent prof. Chrzanowskiego z UJ na gramatyce Doroszewskiego, chyba jednak zostawię „Pani Minister".

Może się nie obrazi, w końcu ma reformować deformy edukacji? Napisałem, że mamy sekcję informatyki szkolnej, konkursy dla dzieci, konferencję Informatyka w edukacji i chcemy certyfikować kompetencje informatyczne uczniów i nauczycieli. Jaki będzie odzew – zobaczymy. Wspomniałem o nieszczęsnych komputerach dla czwartoklasistów i konieczności pilnego przyjrzenia się temu programowi od strony jego efektów edukacyjnych. Może, wzorem swojego poprzednika, nie napisze do mnie nocą kolejnego „listu otwartego"? Uff, jest jedna strona.

Po edukacji nauka, znowu osobno. Nie znam tego ministra, ale znam poprzedniego, więc może być tylko lepiej. Pozdrowiłem też od Przewodniczącego naszej Rady Naukowej, prof. Janusza Kacprzyka. Nie omieszkałem wspomnieć o punktacji naszej konferencji fedCSIS, o naszym zaangażowaniu w kwestie nauki i edukację na poziomie wyższym, konkursy na prace inżynierskie i magisterskie i że oczywiście jesteśmy do dyspozycji. Kolejna jedna strona.

Już miałem kończyć, gdy przypomniałem sobie o zdrowiu. Tak, dzisiaj zdrowie bez informatyki stoi w miejscu, problemy ważne to m.in. cyberbezpieczeństwo danych medycznych, diagnostyka ze sztuczną inteligencja, systemy dostępu do lekarzy. Nasza sekcja e-Zdrowie aż się pali do działań. Zmieściło się na jednej stronie z deklaracją, że jesteśmy do dyspozycji i moim prywatnym dopiskiem, bo z Panią minister Izabelą Leszczyną w ostatnich latach przegadaliśmy trochę czasu.

Na tym zmęczony skończyłem, po raz pierwszy od dawna nie potraktowałem tej korespondencji zdawkowo i formalnie. Pozostaje nadzieja, że adresaci też nie potraktują jej w ten sposób.

> *Ale czy jesteśmy przygotowani do tej „dyspozycji", którą w imieniu towarzystwa zadeklarowałem? Na razie Tadeusz Kifner liczy szable, na które możemy liczyć w ekspertyzach, wykładach, webinariach. Oby oczekiwania wobec nas nie przerosły naszych możliwości.*

Ostatnio mieliśmy problemy z wypowiadaniem naszych opinii. Mam nadzieję, że wynikało to tylko z niewiary, że ktoś je potraktuje poważnie… Zobaczymy, co nas czeka w Nowym 2024 Roku. Oby był on – dla nas wszystkich i adresatów listów – rokiem sukcesów i radości.

Michał Ogórek
satyryk i felietonista, od 1989 r. związany z „Gazetą Wyborczą". Obecnie pisuje w „Angorze". Autor wielu książek. Ostatnio wydał „Sto lat! Jak czciliśmy przywódców w ostatnim stuleciu", o kulcie przywódców – od Piłsudskiego przez Bieruta i Gomułkę po braci Kaczyńskich.

Co da się wykopać z sądu

Wielu czytelników pewnie ominęło informację: „Kopalnia kryptowalut w Naczelnym Sądzie Administracyjnym w Warszawie", mogąc się spodziewać, że kopalnia została wezwana do sądu. Tymczasem jest całkiem odwrotnie: nie tyle ona została postawiona przed sądem, co sąd przed nią. To już wyznacza nowe standardy.

W naszym górniczym kraju, gdzie kopalnia jest czymś tak konkretnym i mało żartobliwym, jej użycie jako przenośni działalności przestępczej utrudnia tylko zrozumienie tego fenomenu.

> *Wiele osób zresztą uważa, że każda kopalnia – czego by nie była – szantażem wymusza na nas swoje istnienie i każdą należałoby zamknąć, a nie robi się tego tylko z obawy przed tymi, którzy kopią.*

Co do pojęcia „kopalni walut", to byłaby jeszcze możliwa do wyobrażenia nie tyle w sądzie, co w banku, w czym pomagają klasyczne filmy kryminalne, na czele z „Vabankiem". Umorusane ekipy budowlane robią jakieś podkopy pod skarbcem, z którego wyciągają potem (brudną) gotówkę. Eliminuje to najgorszy w zwykłej kopalni etap, kiedy na gotówkę dopiero należy zamienić to, co się z niej wykopało, a czego często właśnie spieniężyć się nie daje.

To, co w przypadku kryptowalut nazwano kopalnią jest w dodatku jej zaprzeczeniem. Rzekoma ta kopalnia polega na zużywaniu wielkich zasobów energii elektrycznej i mówiąc szczerze, jest to zwykła i prymitywna kradzież prądu. W polskiej gospodarce byłaby to kolejna próba takiego zachachmęcenia wyników ekonomicznych kopalń i elektrowni, żeby już w ogóle nie było wiadomo, co dopłaca do czego i które finansuje które.

> *To, co się wydobywa z takiej kopalni, jest wyłącznie wirtualne i wszystko polega na jakichś złudzeniach elektromagnetycznych i wzrokowych, w czym również wykazuje duże podobieństwo do punktów sprzedaży węgla na jesieni.*

Smaczkiem jest naturalnie to, że prąd do produkcji był wykradany w ogromnej ilości z najwyższej instancji instytucji, która jest od karania takich procederów, a nawet się zorientowała.

Petenci, którzy nie uzyskali tam przez lata sprawiedliwości (znam paru, łącznie ze mną), mieć będą szczególną satysfakcję, jeśli sądowi wyjdzie z wieloletnich szykujących mu się na ten temat rozkminek, że takiego przestępstwa, jak podłożenie składowi orzekającemu kopalni, nie da się – na podstawie obowiązujących przepisów – ani wykazać, ani tym bardziej skazać. Tym samym poszkodowany sąd satysfakcji w sądzie też nie uzyska.

Jest to nawet raczej więcej niż pewne, jeśli zważyć, że podłożone w szybach wentylacyjnych sądu elektroniczne centrum dowodzenia całą przestępczą operacją miało wyjątkową okazję i czas, aby się czegoś na ten temat nauczyć i czerpać z zasobów sądowej wiedzy, zgromadzonych na sąsiednich serwerach. Kierownictwo sądu uspokaja, że zainstalowane tam systemy operacyjne kryptowalut nie próbowały się dobrać do przechowywanych akt sądowych i można mu nawet wierzyć, bo czytanie ich uznały prawdopodobnie za nudne, nieatrakcyjne i do niczego niepotrzebne. Ale to nie znaczy, że gdyby im to nie było potrzebne, to by tego nie zrobiły.

Ten, kto wymyślił, że nielegalną serwerownię najłatwiej podłożyć w sądzie, musiał mieć dobre rozeznanie. Ignorancja prawników w tych kwestiach jest legendarna. Sam padłem kiedyś ofiarą zbankrutowanej hurtowni książek, której właściciele przekonali syndyka masy upadłościowej, że jedyny majątek, jaki im pozostał – czyli park komputerowy, który mógłby zaspokoić żądania finansowe wierzycieli – nie może zostać wystawiony na sprzedaż. Spowodowałoby to bowiem utratę całej dokumentacji. I Sąd Gospodarczy dla m.st. Warszawy argumentację podzielił, nawet nie próbując sprawdzić, czy danych nie można by zabezpieczyć na innych nośnikach. Robi się z tego już reguła, że przestępcom komputerowym najłatwiej jest ukryć się w sądzie.

Nikt na całym świecie nie lubi prawników, a w Polsce tylko trochę i na krótko pomógł im prokurator Ziobro, lekko represjonując niektórych z nich. Nie starczy tego na długo, albowiem buta i przekonanie o swej nieomylności i wyjątkowości w tej grupie zawodowej ciągle dają o sobie znać i posągowa „walka o praworządność" okazuje się coraz częściej być ambicjonalną przepychanką. Trudno zresztą nadążyć za tym, którzy to są neo-, a którzy dobrzy sędziowie czy prokuratorzy, który nominat, a który denominat czy laminat. Trudno nawet choćby z grubsza zorientować się w tym, za co się wszyscy oni nawzajem pozywają i wyzywają. Zajmując się tak od lat sami sobą, nawet nie zajrzą do szybu wentylacyjnego, gdzie obok piętnowanych kryptosędziów wygodnie ulokowały się nieniepokojone kryptowaluty.

SDSI ŚWIATOWY DZIEŃ SPOŁECZEŃSTWA INFORMACYJNEGO

CYFROWE INNOWACJE
DLA ZRÓWNOWAŻONEGO ROZWOJU

Technosfera przemysłu i edukacji przyszłości

- **15 maja** 10:00-17:15 — KONFERENCJA **Technosfera przemysłu przyszłości**
- **15 maja** 19:00-24:00 — UROCZYSTA KOLACJA POŁĄCZONA Z NETWORKINGIEM **Wielka Gala**
- **16 maja** 10:00-17:00 — KONFERENCJA **Technosfera edukacji przyszłości**
- **07 czerw** ok. godz. 11 — FINAŁ KONKURSU **GEEK na najlepszą grę edukacyjną**

www.sdsi.pl

PTI POLSKIE TOWARZYSTWO INFORMATYCZNE