

# POLSKA 5.0. DLA OBYWATELA

Priorytety Transformacji Cyfrowej w Polsce  
Wyzwania i rekomendacje na lata 2025-2028  
Perspektywa Obywatela



krajowa  
izba  
gospodarki  
cyfrowej



# Wstęp

---

Transformacja cyfrowa w Polsce dokonuje się w niezwykle dynamicznym tempie, wpływając na różne aspekty życia codziennego obywateli. Raport "Polska 5.0 dla Obywatela" ma na celu przedstawienie priorytetów w zakresie cyfryzacji na lata 2025-2028, w szczególności z perspektywy potrzeb i oczekiwań obywateli. W obliczu rewolucyjnych zmian technologicznych, kluczowe jest zrozumienie wyzwań, które stoją przed społeczeństwem oraz wskazanie konkretnych rekomendacji, które umożliwią skuteczną adaptację do nowych realiów. Transformacja cyfrowa nie tylko przyspiesza rozwój gospodarczy, ale również wpływa na jakość życia, dostęp do usług publicznych oraz partycypację

obywatelską. W niniejszym raporcie przeanalizowano główne obszary wymagające interwencji, zidentyfikowano potencjalne bariery i zaproponowano strategię, które pozwolą na ich przezwyciężenie. Perspektywa obywatelska powinna być - naszym zdaniem - kluczowym elementem w kształtowaniu polityk cyfrowych, dlatego też rekomendacje zawarte w raporcie stawiają w centrum transformacji cyfrowej człowieka, konieczność adaptacji do zmian oraz wyzwań związanych z rozwojem technologicznym.



**ANITA TOMASZEWSKA**

PREZES ZARZĄDU  
KRAJOWA IZBA GOSPODARKI  
CYFROWEJ

# Debata otwarta

---

Transformacja cyfrowa to nie tylko kwestia technologii, ale także proces społeczno-kulturowy. Kluczowym wyzwaniem jest projektowanie rozwiązań cyfrowych, które są bezpieczne, intuicyjne, dostępne i odpowiadają na potrzeby obywateli, co wymaga współpracy administracji publicznej, sektora prywatnego i społeczeństwa. Prawdziwa siła transformacji tkwi w aktywnym udziale obywateli oraz zwiększaniu ich umiejętności cyfrowych – bez ich zaangażowania nawet najlepsze narzędzia mogą zawieść.

Nasz raport nie tylko diagnozuje obecny stan, ale także zawiera rekomendacje przyspieszające rozwój cyfrowy Polski w sposób zrównoważony i inkluzywny.

Wskazuje na znaczenie edukacji cyfrowej, inwestycji w infrastrukturę technologiczną oraz budowy zaufania do technologii, szczególnie w kontekście cyberbezpieczeństwa w obliczu hybrydowych zagrożeń.

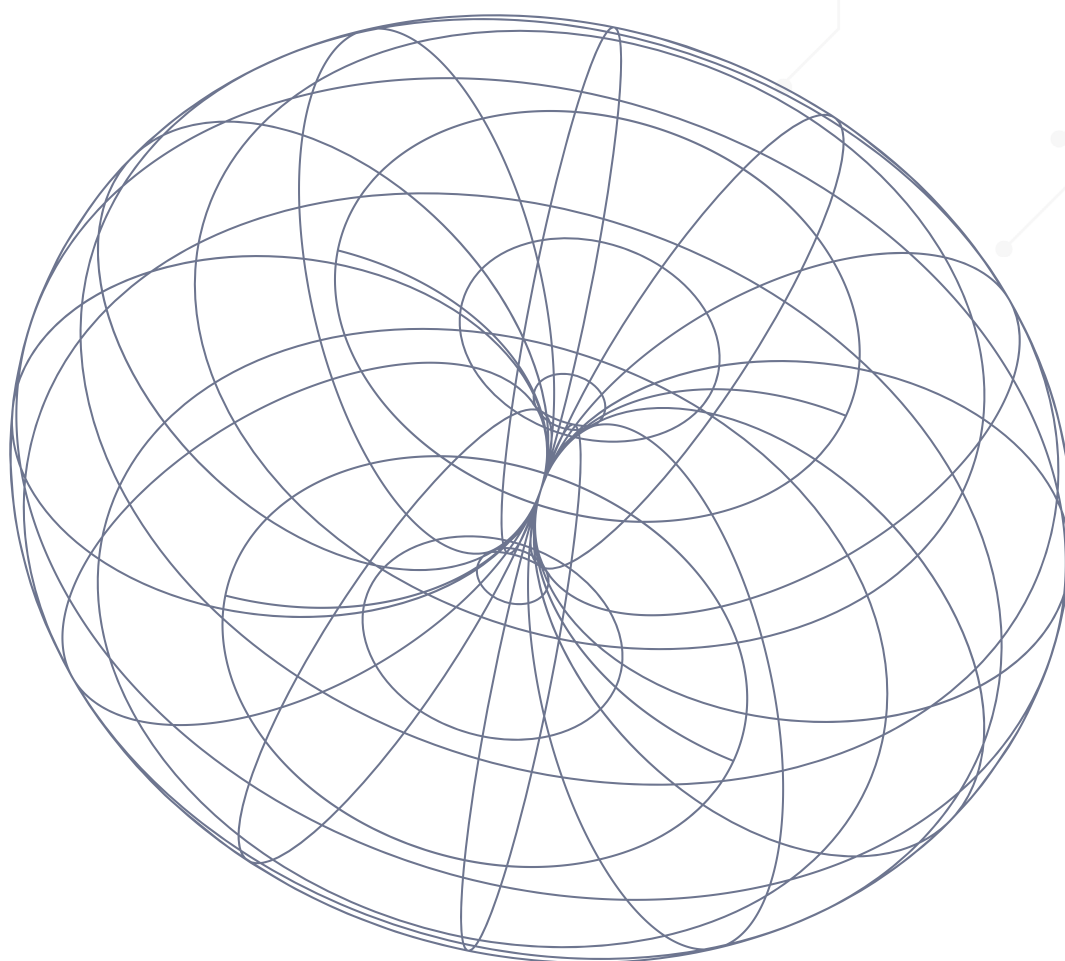
Zapraszamy do zapoznania się z pełną treścią raportu, który wskazuje kierunki budowy odpowiedzialnego społeczeństwa cyfrowego i inspirowanie do działania.

Bardzo dziękujemy ekspertom za ich cenny wkład w tę ważną publiczną debatę.



**BARTOSZ LOBA**

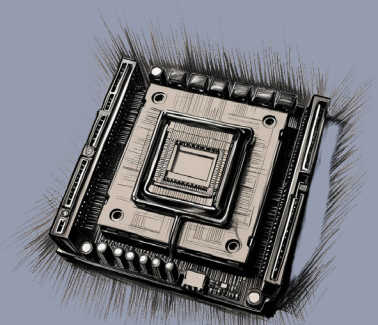
PEŁNOMOCNIK ZARZĄDU KIGC  
DS. TRANSFORMACJI CYFROWEJ  
SEKTORA PUBLICZNEGO



## Priorytety polskiej cyfryzacji 2024

Ponad rok obecnej kadencji Parlamentu RP oraz blisko rok rządu Donalda Tuska to dobra okazja do rozmowy na temat priorytetów polskiej cyfryzacji, a także kierunków rozwoju gospodarki cyfrowej. Nie powinniśmy jednak myśleć tylko w perspektywie najbliższych trzech lat, ponieważ takie podejście nie sprzyja długofalowemu rozwojowi. Dziś przypominamy nasze opracowanie, które nadal stanowi aktualny punkt wyjścia do debaty na temat kierunków, w jakich mogłaby rozwijać się nasza krajowa cyfryzacja. Jesteśmy także bogatsi o wiedzę zaprezentowaną przez Ministerstwo Cyfryzacji w postaci projektu Strategii Cyfryzacji Polski do 2035 roku.

*Dyskusja jest zatem nadal bardzo aktualna, a pogłębiona refleksja niezwykle pożądana.*



Priorytetowe działania w zakresie cyberbezpieczeństwa, poszerzenie dostępu do szybkiego

internetu, stworzenie strategii dla wdrażania rozwiązań z obszaru sztucznej inteligencji oraz wspieranie rozwoju cyfrowych kompetencji przedsiębiorstw to najważniejsze wyzwania dla rządu w tej kadencji. Istotnym elementem jest także wdrożenie DSA.

Polska znacząco rozwinęła się w obszarze cyfryzacji, ale nadal istnieje wiele do zrobienia. Ministerstwo Cyfryzacji stoi przed szeregiem kluczowych wyzwań, których pokonanie jest niezbędne dla zwiększenia innowacyjności i konkurencyjności naszego kraju. Wśród nich znajduje się likwidacja „białych plam internetu” za pomocą środków z KPO, uchwalenie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, wdrożenie Aktu o Usługach Cyfrowych oraz AI Act, a także rewizja strategii rozwoju sztucznej inteligencji.

### Po pierwsze: cyfrowa polityka, nie cyfryzacja

Zacznijmy od pryncypiów. Skoro mówimy o cyfrowym państwie i Polska szczeni się tym, że ma wyższy poziom cyfryzacji usług publicznych niż inne państwa w regionie, to najwyższy czas zmienić nazwę „Ministerstwo Cyfryzacji” na jakąś inną, bardziej odpowiadającą nadchodzącym wyzwaniom. „Ministerstwo Polityki Cyfrowej” wydaje się zdecydowanie bardziej adekwatnym określeniem dla resortu, który za rządów Zjednoczonej Prawicy został rozwiązany, aby potem - również za rządów Zjednoczonej Prawicy, tylko w kolejnej kadencji - powstał z martwych.

Skąd taka propozycja? Przede wszystkim dlatego, że to, co cyfrowe, jest polityczne.

*Nie ma sensu udawać, że kwestie cyfrowe są dziś niezależne od polityki; że „to tylko technologie” i ich wdrożenie do rzeczywistości współdzielonej przez obywateli i obywatelki.*

Jak bardzo polityczne potrafią być sprawy związane z tym, co cyfrowe, pokazała sprawa Pegasusa, a także pandemia koronawirusa, w której liczne kraje udowodniły, że kwestie zdrowia publicznego mogą być doskonałym pretekstem do przystrzyżenia prawa do prywatności.

Polityczna jest również kwestia obecności wielkich firm technologicznych w życiu społecznym, a także czynionych przez nie inwestycji. Najdobitniejszym przykładem jest zagadnienie suwerenności cyfrowej, jak i temat transferu danych, na których operują państwowe instytucje za oceanem. Problematyka ta nasuwa się zwłaszcza w kontekście zastosowania amerykańskich usług cyfrowych w administracji publicznej.

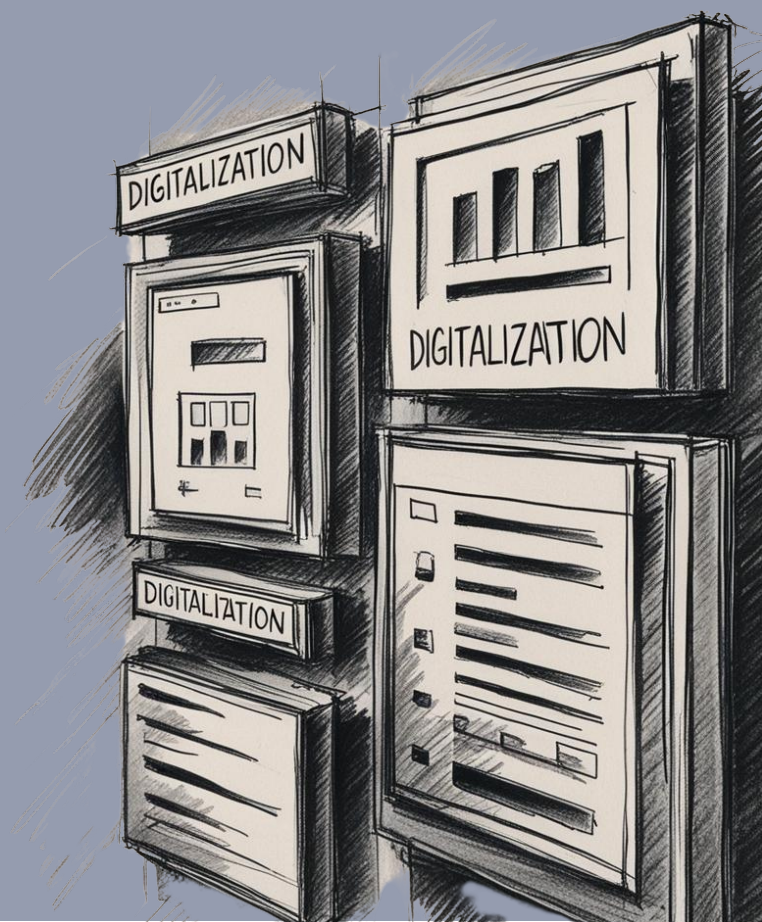
Wreszcie, polityczne są regulacje. Polska dwóch ostatnich kadencji bardzo niechętnie podchodziła do tego tematu, spoglądając z ukosa na ponadnarodowe inicjatywy zmierzające do regulacji Big Techów, na których inwestycjach i obecności w kraju jej zależy. Regulacje jednak stały się faktem: pakietowe Akt o usługach cyfrowych i Akt o rynkach cyfrowych, nadchodzący Akt o sztucznej inteligencji czy obowiązujące już 5,5

roku RODO. Wniosek? To słoń w pokoju, którego trzeba wreszcie dojrzeć. To polityka cyfrowa, która zapukała do polskich drzwi i nie można dłużej jej ignorować.

## Po drugie: cyfrowa edukacja na serio

W kampanii wyborczej pojawiały się propozycje usprawnienia edukacji. PiS postulowało lekcje programowania przez cały okres kształcenia dla każdego dziecka.

**Nie każdy musi być programistą. Nie każdy powinien.** Powiedzmy sobie to szczerze, raz i proszę to w oczy - bo nie każdy ma do tego kwalifikacje i predyspozycje i nie chodzi tylko o umiejętność kodowania (która jest jedną z kwalifikacji, jakie trzeba posiadać, aby być programistą czy programistką). Czy egzekwowanie umiejętności kodowania od wszystkich - niezależnie od tego, czy chcą



to robić i czy mają do tego uwarunkowania - ma sens? Nie. To stworzenie lekcji-koszmaru, która zniechęci do poznawania nowych technologii i odepchnie uczniów oraz uczennice od edukacji cyfrowej. Samo w sobie jest to ogromnym, bogatym w konsekwencje błędem, w szczególności, jeśli przyjrzymy się temu, jak dziś wygląda krajobraz zagrożeń i ryzyko, z którym codziennie stykamy się jako cyfrowi tubylcy.

Cyfrowa edukacja powinna być priorytetem, bo na tym polu Polska wciąż plasuje się relatywnie nisko w rankingach europejskich, a dysproporcje pomiędzy umiejętnościami poszczególnych grup demograficznych są znaczne. Skupmy się jednak na edukacji szkolnej.

*Co powinno wejść w skład dobrego programu cyfrowej edukacji? Przede wszystkim podstawy wiedzy o cyberbezpieczeństwie, prywatności, mechanizmach działania nowoczesnych urządzeń łączących się z internetem (i internetu w ogóle); kwestie związane z zagadnieniami takimi jak profilowanie behawioralne, wykorzystywanie danych do marketingu (również politycznego); tematy związane z wojną handlową, wykorzystaniem technologii w geopolityce, jak i ich znaczeniem dla obronności i bezpieczeństwa narodowego.*

Kurs oczywiście powinien być dostosowany do etapów kształcenia szkolnego, jednak całość

jego realizacji można zamknąć w ośmiu klasach szkoły podstawowej. To dobry moment, aby uczniowie i uczennice mogli zdecydować, czy będą chcieli kształcić się w kierunku bycia programistami.

Dodatkowo, odpowiedzialne za edukację w szkole powinno być państwo. Kadry pedagogiczne. Nie NGO-sy. Nie prywatne firmy technologiczne, wykorzystujące każdą okazję do tego, by łowić użytkowników swoich usług i od najmłodszeo wieku budować lojalność względem marki.

## Po trzecie: cyberbezpieczeństwo. Cywilne też

Cyberbezpieczeństwo jest priorytetem. To rzecz oczywista, biorąc pod uwagę chociażby naszą sytuację geopolityczną.

W kontekście cyberbezpieczeństwa bardzo dużo dzieje się na polu militarnym. Cyberbezpieczeństwo w kontekście wojskowym to jednak tylko jedna strona medalu.

**Nie mniej istotne jest cyberbezpieczeństwo w sektorze cywilnym**, po stronie dzisiejszego resortu cyfryzacji i zależnych od niego instytucji. To one w naturalny sposób - na wzór krajów Zachodu, takich jak USA - są drogowskazami dla sektora prywatnego, gdy mowa o cyber. To one powinny służyć wsparciem w tym zakresie firmom, organizacjom Trzeciego Sektora, jak i wszelkim cywilnym instytucjom administracji na szczeblu samorządowym.



Warto inwestować w kadry, budowę zakresu samodzielnych kompetencji cywilnego cyberbezpieczeństwa, a także rozpoznawalność cywilnych instytucji za nie odpowiedzialnych tak, by komunikacja wykraczała poza grono dziennikarsko-eksperckie i sięgała tam, gdzie jest najbardziej potrzebna, czyli do osób, które codziennie odpowiadają za cyberbezpieczeństwo struktur swoich firm i organizacji. Jest przed czym się chronić, bowiem zagrożeniem jest nie tylko Rosja, ale także Chiny nastawione na m.in. cyberszpiegostwo gospodarcze.

### Po czwarte: przejrzystość lobbingu

Lobbing. Nigdy nie był tak ważny, jak w erze gospodarki cyfrowej. Dlaczego?

*Zagwarantowanie przejrzystości działań lobbingsowych, których wynikiem niejednokrotnie jest zapóźnienie regulacyjne Polski lub nawet wprost - brak realizacji niektórych postulatów niezbędnych dla zrównoważonego, ale realnego rozwoju naszego kraju na polu gospodarki cyfrowej, to konieczność.*

Polska nie poradzi sobie dobrze w cyfrowej przyszłości, jeśli o kształcie prawa będą decydować wielkie firmy technologiczne lub związane z nimi grupy interesu. Nie poradzi sobie, jeśli nie będzie samodzielnie decydować o kształcie własnych regulacji prawnych i wdrożeniu tych, które tworzone są w Unii Europejskiej. Nie poradzi sobie, jeśli przeniesie odpowiedzialność za działania regulacyjne i obsługę usług publicznych

de facto na Big Techy. Prędzej czy później obudzi się w roli cyfrowej kolonii, w której to wielkie firmy technologiczne decydują o kształcie prawa, programów nauczania w szkołach (jak słynne lekcje historii we współpracy z Metą, co do których nigdy nie rozwiano wątpliwości dotyczących edukacji nauczycieli, rodziców i uczniów na temat ryzyka dla prywatności niesionego przez technologie AR i VR) oraz innych kluczowych ze społecznego punktu widzenia kwestiach.

Na tapecie już niebawem pojawią się dyskusje o przejrzystości algorytmów odpowiedzialnych za wsparcie w podejmowaniu decyzji w administracji. Warto zdążyć rozprawić się z lobbingsiem, zanim będziemy mieli w tej kwestii problemy takie, jak występują już w USA czy Wielkiej Brytanii.

### Cztery priorytety na cztery lata

W powyższym tekście wskazaliśmy cztery priorytety na cztery lata nowej kadencji. To oczywiście tylko zarys i subiektywny wybór. Z innego punktu widzenia, na przykład tego wyrażanego przez biznes lub środowiska regulacyjne, najważniejsze kwestie mogą rysować się zupełnie inaczej.

Te wskazane powyżej to perspektywa prospołeczna i proobywatelska, a jak twierdzili liczni liderzy polityczni w kampanii, to przecież właśnie ona jest najważniejsza i to dla niej idzie się po zwycięstwo.



# Struktura raportu

---

- **I Gospodarka cyfrowa dla obywatela**

  - [Gospodarka cyfrowa oparta na centrach danych \(s. 13\)](#)

- **II Gospodarka cyfrowa dla przedsiębiorstw**

  - [Innowacje i bezpieczeństwo w centrum strategii przedsiębiorstw \(s. 17\)](#)

- **III Sztuczna Inteligencja w służbie obywateli**

  - [Sztuczna inteligencja zmienia nasze życie \(s. 24\)](#)

  - [Cyfryzacja w sektorze zdrowia \(s. 30\)](#)

# Struktura raportu

---

## IV Sztuczna inteligencja dla edukacji

[Edukacja cyfrowa na ścieżkach kształcenia \(s. 36\)](#)

[Edukacja goni technologię czy odwrotnie? \(s. 39\)](#)

[Czas na edukację cyfrową w szkołach \(s. 43\)](#)

[Polska transformacja cyfrowa w edukacji to szansa i wyzwanie \(s. 48\)](#)

## V Cyberbezpieczeństwo dla obywateli

[Cyberbezpieczeństwo dla obywateli: klucz do bezpiecznej przyszłości cyfrowej Polski \(s. 57\)](#)

[Certyfikacja to filar cyberbezpieczeństwa \(s. 60\)](#)

[Predykcje kierunków rozwoju Cyberbezpieczeństwa 2024 \(s. 65\)](#)

[Cyberbezpieczeństwo najwyższej klasy dostępne dla administracji publicznej jako usługa \(s. 69\)](#)



# Gospodarka cyfrowa dla obywatela

---

## Gospodarka cyfrowa oparta na centrach danych

Adam Ponichetra

# Gospodarka cyfrowa oparta na centrach danych

**Centra danych to filary naszej cyfrowej rzeczywistości - to tam znajdują się dane, które konsumujemy, wymieniamy i generujemy w coraz większej ilości. Odpowiednie inwestycje i rozwój centrów są kluczowe dla zapewnienia efektywnego procesu cyfryzacji - bez infrastruktury fizycznej cyfrowa transformacja nie będzie możliwa lub będzie o wiele trudniejsza, a co za tym idzie - nie wypełni potrzeb obywateli. W najbliższych latach Polska będzie stanowić jeden z najdynamiczniej rozwijających się rynków dla sektora centrów danych - odpowiadając na zapotrzebowanie technologicznych spółek, a także rosnącego tempa digitalizacji życia, w tym coraz szerszego zastosowania sztucznej inteligencji. Utrzymanie tempa wzrostu, zarówno sektora, jak i całej gospodarki cyfrowej, będzie możliwe jedynie przy efektywnej współpracy biznesu z przedstawicielami administracji rządowej i lokalnej.**

## Budowanie świadomości i akceptacji wśród lokalnych społeczności

Przez wiele lat centra danych były postrzegane jako energochłonne i niemożliwe do zdobycia

fortece. Operatorzy stają przed nowym wyzwaniem, jakim jest zbudowanie wiedzy, zrozumienia i akceptacji przez lokalne społeczności i władze, bowiem centra danych, prócz funkcjonowania nieingerującego w codzienne życie najbliższego otoczenia, zapewniają wymierne korzyści. Kampusy centrów danych nie mogą być projektowane bez spojrzenia na otoczenie i funkcjonować w losowej czy nieodpowiedniej lokalizacji - muszą być częścią przemysłowego i lokalnego krajobrazu. Dzięki temu, w połączeniu z innymi sektorami gospodarki, mogą zapewniać zrównoważoną przyszłość.

Lokalizacja centrów danych w Polsce przynosi wymierne korzyści zarówno lokalnemu biznesowi, jak i obywatelom, m.in. szybsze działanie infrastruktury IT, chmury czy poprzez zachowanie bezpieczeństwa i suwerenności danych - czyli przechowywania danych na własnym terytorium lub w europejskim systemie prawnym. W cyfrowym świecie opartym o dane, należy zatem traktować infrastrukturę centrum danych jako krytyczną, który wymaga uwzględnienia w procesie planowania przestrzennego, rozumianego przez projektowanie sieci energetycznych, komunikacyjnych, teleinformatycznych, czy nawet bezpieczeństwa cywilnego. Co znamienne, obecna regulacja planowania przestrzennego wciąż traktuje centra danych jako „przestrzeń magazynową”.

## integracja na poziomie lokalnym i krajowym

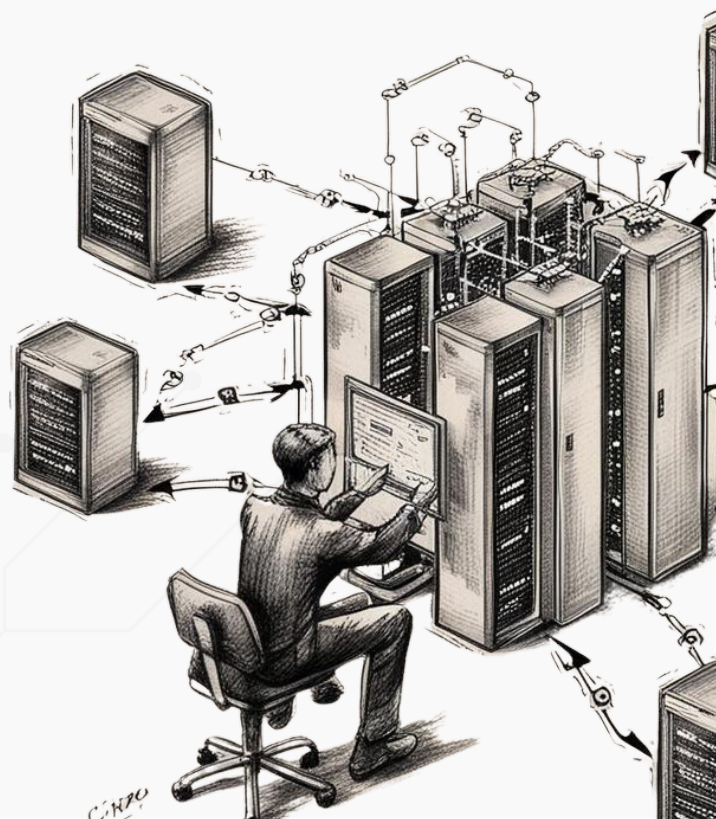
Proces planowania i rozwijania nowych kampusów powinien opierać się na współpracy inwestorów oraz władz na szczeblu lokalnym i państwowym. To stwarza większe możliwości, m.in. integrację z infrastrukturą miejską. Jednym z warunków wstępnych podczas rozwoju nowych lokalizacji powinna być możliwość wykorzystywania ciepła odpadowego, czyli energii cieplnej generowanej przez centra danych. Rozwiązania umożliwiające wykorzystanie ciepła odpadowego, np. do ogrzewania obszarów miejskich, są coraz szerzej stosowane w krajach skandynawskich. Inną możliwością jest współpraca z sektorem spożywczym – w tej perspektywie ciepło odpadowe można przekierować m.in. do szklarni czy hodowli ryb. Mimo że przypadki wykorzystywania ciepła odpadowego nadal są rzadkością, często ze względu na ograniczenia technologiczne czy finansowe, konieczne jest nawiązywanie partnerstw wielosektorowych w celu przejścia na skalę przemysłową.

*Musimy zacząć traktować energię ciepłą nie jako „odpad”, ale jako kolejny produkt, który możemy wykorzystać w rozwijaniu gospodarki, z myślą o korzyściach dla obywateli.*

### Inwestycja w przyszłe kadry

Rosnący sektor oraz poziom cyfryzacji w Polsce wymaga także inwestycji w edukację. Już dziś

obserwujemy niedobór pracowników w obszarze IT, jak wskazuje raport ManpowerGroup, a z pewnością w najbliższych latach zapotrzebowanie na ekspertów z kompetencjami z sektora technologicznego będzie jeszcze większe. Branża centrów danych to kolejna specjalizacja, która wymaga wykwalifikowanych kadr, a popyt na usługi kolokacyjne będzie generował zapotrzebowanie na specjalistów z obszaru bezpieczeństwa, zarządzania czy prowadzenia inwestycji tego typu obiektów. Odpowiednia podaż ekspertów wymaga już dziś tworzenia specjalistycznych kierunków na uczelniach technicznych i biznesowych, co mogłoby być efektem współpracy biznesu i szkolnictwa wyższego. W Data4 zauważamy tę potrzebę, dlatego nawiązujemy partnerstwa na różnych rynkach w Europie, a także zapraszamy uczniów i studentów z uczelni wyższych i technicznych, aby poznali centra danych od środka i mieli szansę się przekonać, że to obiecująca ścieżka kariery. Z potencjałem ludzkim wiąże się



także niesłabnąca popularność i zastosowanie sztucznej inteligencji. Wraz z jej rozwojem musi postępować wzrost infrastruktury krytycznej, jaką są centra danych. Dzięki nim Polska ma szansę przyciągać globalnych graczy z sektora AI, a co ważniejsze, stać się dostawcą i deweloperem tej technologii, a nie wyłącznie konsumentem. A to stwarza kolejne możliwości wzrostu dla gospodarki.

## Sztuczna inteligencja - szansa i wyzwanie dla Polski

Przez popularyzację nowych modeli AI, takich jak ChatGPT czy Gemini, możemy na własne oczy oglądać rewolucję technologiczną w obszarze cyfryzacji i codziennym życiu. Rozwój sztucznej inteligencji wywarł i będzie wywierał istotny wpływ również na sektor centrów danych. Popyt na moc obliczeniową i przechowywanie danych stale rośnie, ponieważ generatywna sztuczna inteligencja opiera się na ogromnych zasobach danych i energii potrzebnej do jej wytrenowania. W niedalekiej przyszłości ze sztucznej inteligencji zaczną szerzej korzystać wrażliwe sektory: naukowy, wojskowy energetyczny czy finansowy. Biorąc pod uwagę kontekst bezpieczeństwa obywateli i suwerenności innych danych, centra obsługujące wymienione

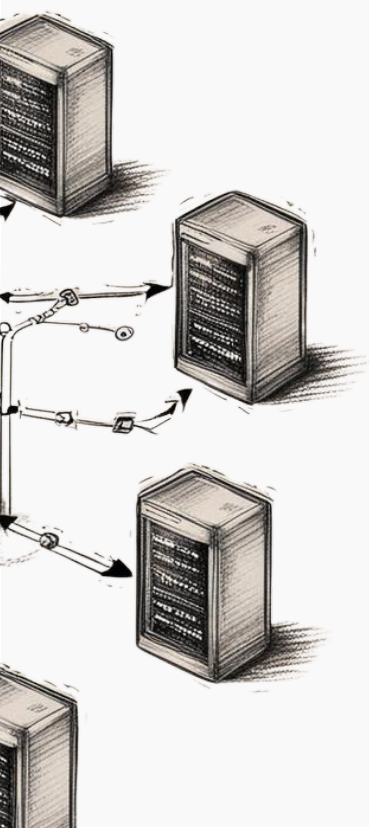
branże bezsprzecznie powinny być lokalizowane w strategicznych regionach z odpowiednim dostępem do mocy, ale też w pobliżu ośrodków, które w największym stopniu będą potrzebowały mocy obliczeniowych w swojej codziennej działalności.

*Operatorzy centrów danych, aby rozwijać je w tempie odpowiadającym dzisiejszemu popytowi, a jednocześnie działać w sposób zrównoważony, potrzebują uproszczenia procedur, skrócenia czasu realizacji wniosków o przyłączenie do sieci, a przede wszystkim zapewnienia dostępu do niskoemisyjnej energii ze źródeł odnawialnych i niskoemisyjnych.*

## Energia podstawą wzrostu

Operatorzy centrów danych mierzą się również z wyzwaniem optymalizacji energetycznej. Z pomocą przychodzą różne rozwiązania i opcje - zaczynając od współpracy z operatorami sieci energetycznej w celu zmniejszenia zużycia w godzinach szczytu, poprzez wykorzystywanie generatorów czy magazynowanie energii w centrum danych. Jednak dalsze inwestycje oraz działania państwa w kierunku transformacji energetycznej mogą przyspieszyć rozwój sektora, a co za tym idzie - wzmocnić cyfryzację w naszym kraju.

W zasięgu są nowe, lokalne źródła energii (np. fotowoltaika czy farmy wiatrowe) i linie bezpośrednie, ale konieczna jest również modernizacja sieci elektroenergetycznej kraju, której szkielet



wciąż odzwierciedla potrzeby przemysłu sprzed kilkudziesięciu lat, a dziś nie jest w stanie sprostać obecnemu zapotrzebowaniu na moc.

Choć centra danych nie skupiają na sobie tyle uwagi, co nowe drogi, porty czy elektrownie, to w nowoczesnym państwie pełnią podobnie istotną rolę. W zaawansowanej gospodarce każdy proces wymaga udziału infrastruktury obliczeniowej, a efektywne przetwarzanie danych wnosi dodatkową wartość dodaną do

procesów produkcyjnych. Aby polskie firmy mogły nadal cieszyć się wzrostem, a obywatele podnosić jakość, komfort i bezpieczeństwo życia, odpowiedzialna administracja musi zadbać, aby dane swobodnie krążyły w krwio-biegu sieci, a której sercem są centra danych.



## ADAM PONICHETRA

DYREKTOR POLSKIEGO ODDZIAŁU  
DATA4, INWESTOR I OPERATOR  
CENTRÓW DANYCH, EKSPERT KIGC







# Gospodarka cyfrowa dla przedsiębiorstw

---

**Innowacje i bezpieczeństwo w centrum strategii przedsiębiorstw**

Dariusz Piotrowski

# Innowacje i bezpieczeństwo w centrum strategii przedsiębiorstw

**W obliczu nieustających wyzwań biznesowych firmy intensywnie poszukują nowoczesnych rozwiązań, by zachować wysoką operacyjność i konkurencyjność. W ostatnich latach kluczowym aspektem funkcjonowania organizacji stało się bezpieczeństwo. Organizacje podejmują wiele wysiłków, by zapewnić je w ramach organizacji, ale w dobie cyfrowego rozwoju niezwykle ważnym elementem staje się również często pomijane bezpieczeństwo łańcucha dostaw.**

Zakłócenia łańcucha dostaw – katastrofy naturalne, cyberataki czy problemy z jakością – mogą poważnie wpłynąć na działalność firmy. Dobrze funkcjonujący łańcuch dostaw ma zasadnicze znaczenie dla stabilności działania firmy, utrzymania jej reputacji, konkurencyjności, optymalizacji procesów oraz minimalizacji zbędnych wydatków. Jednak w kontekście globalnym bezpieczeństwo produktów zależy nie tylko od producentów, ale również od ich sieci dostawców i partnerów.

## Zaangażowanie w zaawansowane strategie bezpieczeństwa

W dynamicznie zmieniającym się świecie technologii wciąż pojawiają się nowe cyberzagrożenia, dlatego Dell nie zwalnia tempa i stawia na rozwiązania, które sprawdzają się w takich warunkach. Dzięki ciągłemu monitorowaniu zagrożeń przez wyspecjalizowane zespoły bezpieczeństwa, firma sprawnie adaptuje się do zmieniających warunków. Dell regularnie aktualizuje także swoje systemy i procedury, dzięki czemu utrzymuje wysoki poziom bezpieczeństwa produktów i usług.

*- Globalizacja i postęp technologiczny sprawiają, że łańcuchy dostaw stają się coraz bardziej złożone i cyfrowo zintegrowane, a rola cyberbezpieczeństwa jest fundamentalna – podkreśla Sebastian Antkiewicz, Products & Solutions Senior Manager w Dell Technologies Polska.*

*- Cyberatak może nie tylko zakłócić operacje i przepływ towarów, ale również doprowadzić do utraty danych krytycznych, narazić na szwank wizerunek firmy i spowodować utratę zaufania klientów.*

Inwestycje w zaawansowane rozwiązania ochrony jak i regularne audyty bezpieczeństwa, są kluczowe nie tylko dla ochrony cennych danych, ale także dla zapewnienia ciągłości działania w obliczu rosnących zagrożeń.

## Bezpieczeństwo w łańcuchu dostaw

Firma Dell Technologies stosuje całościowe i wieloaspektowe podejście do ochrony swojego łańcucha dostaw i dostarczania rozwiązań, którym klienci mogą zaufać. Niezależnie od tego, czy jest to komputer stacjonarny, laptop, serwer czy macierz do przechowywania danych, funkcje są opracowywane, projektowane, prototypowane, wdrażane, wprowadzane do produkcji, utrzymywane i weryfikowane z najwyższym priorytetem bezpieczeństwa łańcucha dostaw.

Bezpieczeństwo łańcucha dostaw to praktyczne stosowanie środków kontroli prewencyjnej i detektywistycznej, które chronią aktywa rzeczowe, zapasy, informacje, własność intelektualną i ludzi. Bezpieczeństwo fizyczne pomaga zapewnić bezpieczeństwo łańcucha dostaw, zmniejszając możliwości wprowadzenia złośliwego oprogramowania i podrobionych komponentów do łańcucha dostaw.

## Bezpieczeństwo danych

Bezpieczeństwo danych obejmuje praktyki i zasady stosowane do ochrony danych cyfrowych przed nieautoryzowanym dostępem lub użyciem, które może spowodować ujawnienie, wykorzystanie, usunięcie lub uszkodzenie danych.

Firma Dell wdraża innowacyjne praktyki w celu zabezpieczenia danych cyfrowych, korzysta ze sprawdzonych rozwiązań administracyjnych oraz przeprowadza kontrolę fizyczną i utrzymuje

wielowarstwowe protokoły dostępu w celu ochrony wrażliwych danych naszych klientów.

Działania związane z zarządzaniem danymi koncentrują się na optymalizacji relacji i stanu zabezpieczeń w celu proaktywnego identyfikowania luk w zabezpieczeniach i ograniczania ryzyka. W celu ochrony poufności, integralności i dostępności danych klientów, zwiększamy zaufanie i pewność w całym łańcuchu tych wartości.

Firma Dell podejmuje nadzwyczajne kroki w celu ochrony danych cyfrowych i innych poufnych informacji klientów.

## Bezpieczeństwo w całym cyklu życia produktu

Dell Technologies idzie o krok dalej niż inni dostawcy nieustannie monitorując oraz doskonaląc produkt o nazwie Dell Secure Development Lifecycle (SDLC). SDLC jest holistycznym procesem kontrolującym tworzenie i rozwój produktów zgodnie z najbardziej rygorystycznymi normami zawierający w sobie analizę rynku, nowych zagrożeń, oraz podatności na zagrożenia. Zgodnie z SDLC bezpieczeństwo jest kluczowym elementem, wokół którego tworzy się nowy produkt – od projektu poprzez dobór komponentów i dostawców, bezpieczny i odporny na ataki firmware, oraz kolejne aktualizacje i nowe usprawnienia.

Dell ocenia kilka funkcji przy ustalaniu, jakie elementy powinny zostać wdrożone na

każdym etapie łańcucha dostaw. Obejmują one obejmują bezpieczeństwo, integralność, jakość i odporność:

— **Bezpieczeństwo** - zapewnia poufność, integralność i dostępność informacji opisujących łańcuch dostaw IT lub przechodzących przez łańcuch dostaw IT, a także informacji o stronach uczestniczących w łańcuchu dostaw IT.

— **Integralność** - zapewnia, że produkty lub usługi IT w łańcuchu dostaw IT są autentyczne, niezmienione i będą działać zgodnie ze specyfikacjami nabywcy oraz bez dodatkowych niepożądanych funkcjonalności.

— **Jakość** - zmniejsza podatności, które mogą ograniczać planowaną funkcję komponentu, prowadzić do jego awarii lub stwarzać możliwości wykorzystania go przeciw użytkownikowi.

— **Odporność** - gwarantuje, że łańcuch dostaw IT będzie dostarczał wymagane produkty i usługi IT pomimo zakłóceń.

## Innowacyjne podejście do cyberzagrożeń

Nowe możliwości wykrywania i neutralizowania cyberzagrożeń w systemach bezpieczeństwa można stworzyć także dzięki zastosowaniu m.in. sztucznej inteligencji i uczenia maszynowego. Dzięki AI i ML duże wolumeny danych można analizować w czasie rzeczywistym, co umożliwia identyfikację anomalii i potencjalnych zagrożeń,

zanim zdążą wyrządzić szkody. Automatyzacja procesów monitorowania nie tylko zwiększa skuteczność ochrony, ale także pozwala na bardziej zaawansowane przewidywanie i zapobieganie atakom.

W kontekście tych technologii niezwykle ważna jest demokratyzacja AI, która dzięki narzędziom takim jak Chat GPT przybliża ją szerszej grupie użytkowników. Dell Technologies nieustannie inwestuje w badania i rozwój AI. Firma posiada już **ponad 28 tys. patentów w tym obszarze i aktywnie wprowadza innowacje (takie jak m.in. serwery przystosowane do potrzeb sztucznej inteligencji)**, które umacniają pozycję lidera w tworzeniu bezpieczniejszych rozwiązań technologicznych

— *Bezpieczeństwo nie jest punktowym wysiłkiem. To stworzenie całej architektury, która zaczyna się już od bezpiecznego łańcucha dostaw i obejmuje urządzenia końcowe, dane i aplikacje klienta, przetwarzanie danych i stworzenie odpowiedniego data center. Bezpieczeństwo jest niejako wpisane w DNA wszystkich naszych produktów, co stanowi kluczowy element naszej strategii i pozwala nam wyznaczać nowe standardy w branży - podkreśla Sebastian Antkiewicz.*

ell Technologies posiada globalne centrum monitoringu dostaw, które w czasie rzeczywistym śledzi wszystkie transporty z fabryk Dell. Każdy kontener posiada nadajniki GPS oraz wiele

dodatkowych sensorów, które pozwalają na upewnienie się że transport z fabryki Dell dotarł do klienta nienaruszony. Komponenty składowe produktów Dell posiadają własne unikalne numery seryjne, które są ściśle powiązane z urządzeniem, w którym zostały zamontowane. Dzięki nim klienci Dell Technologies podczas przyłączania ich do własnej infrastruktury mogą upewnić się że dostarczony komputer, serwer czy macierz są w 100% oryginalnym produktem, który podczas transportu lub magazynowania nie został zmieniony poprzez podmiianę komponentów (np. na posiadające złośliwy firmware).

## Międzynarodowe standardy bezpieczeństwa to klucz do sukcesu

Do zapewnienia wysokiego poziomu bezpieczeństwa w globalnych łańcuchach dostaw niezbędne jest także dostosowanie się do międzynarodowych standardów, takich jak obecny w Dell Technologies ISO 28000. Taka certyfikacja nie tylko podnosi poziom zaufania wśród

klientów i partnerów biznesowych, ale również usprawnia procesy operacyjne, zapewniając zgodność z najlepszymi praktykami i regulacjami branżowymi.

Firma Dell posiada również certyfikaty w wielu programach handlowych dotyczących bezpieczeństwa, takich jak Protection Association (TAPA), American Society for Industrial Security (ASIS), International Standards Organization (ISO), and the Business Alliance for Secure Commerce (BASC). United States Customs and Border Protection's Customs, Trade Partnership Against Terrorism (C-TPAT), Canada's Partners in Protection (PIP), Singapore's Secure Trade Partnership, and Authorized Economic Operator (AEO).

Poprzez ustanowienie jednolitych procedur i metod oceny ryzyka, firmy mogą lepiej zarządzać swoimi łańcuchami dostaw, minimalizując potencjalne zakłócenia i zwiększając swoją odporność na zmieniające się warunki rynkowe. Przestrzeganie tych standardów ułatwia również ekspansję na nowe rynki, otwierając drzwi do międzynarodowej współpracy i nowych możliwości biznesowych.

## Zrównoważony rozwój a bezpieczny łańcuch dostaw

Ostatnim, ale nie mniej ważnym aspektem zapewnienia stabilności operacyjnej i pozytywnego wizerunku marki jest integracja zasad



zrównoważonego rozwoju. Poprzez odpowiedzialne pozyskiwanie surowców firmy mogą nie tylko zmniejszać wpływ na środowisko, ale także budować silniejsze i bardziej zrównoważone relacje z dostawcami, co przekłada się z kolei na większą odporność łańcucha dostaw na potencjalne zakłócenia. W tym kontekście równie ważna jest minimalizacja odpadów i optymalizacja procesów produkcyjnych, które przyczyniają się do ochrony zasobów naturalnych oraz pozwalają zwiększać efektywność operacyjną, redukując koszty i ryzyko związane z przestojami. Wprowadzając praktyki ekologiczne, firmy mogą lepiej reagować na zmieniające się oczekiwania konsumentów, którzy coraz częściej preferują produkty pochodzące z odpowiedzialnych źródeł.

Warto podkreślić, że zakład Dell w Łodzi jest zasilany w 100% energią pochodzącą z odnawialnych źródeł. Zaangażowanie w ekologiczne praktyki operacyjne w połączeniu z elastycznością i odpornością operacyjną firmy sprawiło, że fabryka Dell nie zatrzymała produkcji nawet w czasie lockdownu i pandemii.



**DARIUSZ PIOTROWSKI**

DYREKTOR ZARZĄDZAJĄCY  
DELL TECHNOLOGIES POLSKA





# Sztuczna Inteligencja w służbie obywateli

---

**Sztuczna inteligencja zmienia nasze życie**

Karol Antczak

**Cyfryzacja w sektorze zdrowia**

Adam Paczuski

## Sztuczna inteligencja zmienia nasze życie

**AI już dawno przeniknęła do codziennego życia — zarówno prywatnego, jak i publicznego. Są to, z jednej strony, oczywiste zastosowania, które łatwo wyodrębnić i wskazać palcem, w rodzaju chatbotów czy modeli generatywnych. Z drugiej zaś strony, olbrzymie znaczenie mają również "ukryte" modele AI, których nie widać na pierwszy rzut oka, ale które przetwarzają i generują olbrzymie ilości danych.**

### Stan obecny, czyli integracja AI z codziennym życiem

Takie niewidoczne zastosowania AI określa się mianem Ambient Intelligence (Aml). Chodzi tu o rozwiązania stosowane w smartfonach, urządzeniach typu smart home, ale również aplikacjach internetowych, które przetwarzają nasze dane osobowe w celu profilowania. Nawet jeśli nie jesteśmy tego świadomi, nasze dane są często przetwarzane przez AI.

Przykłady zastosowań Aml w codziennym życiu to na przykład inteligentne termostaty, takie jak Nest Learning Thermostat, które automatycznie dostosowują temperaturę w domu do naszych

nawyków. To również inteligentne oświetlenie, np. Philips Hue, które pozwala sterować światłami za pomocą smartfona lub głosu. Wliczamy w to również platformy smart home, takie jak Samsung SmartThings czy Apple HomeKit, które umożliwiają sterowanie różnymi urządzeniami domowymi z jednego miejsca, automatyzację zadań i tworzenie scenariuszy np. "wyjście z domu" lub "powrót do domu" właśnie przy użyciu Aml.

Polacy prezentują pozytywne podejście do sztucznej inteligencji. Według danych z raportu digitalpoland "Technologia w służbie społeczeństwu\_2023. Czy polacy zostaną społeczeństwem 5.0?" **85% społeczeństwa wyraża tolerancję, akceptację lub silne poparcie dla tej technologii.** Szczególnie młodsze pokolenie jest do niej nastawione optymistycznie. Prawie połowa, bo aż **40% badanych, reaguje z ciekawością na myśl o AI**, dostrzegając jej potencjał w ułatwianiu życia (47%) i rozwiązywaniu strategicznych wyzwań Polski (**39%**). Świadomość potencjalnych zagrożeń, takich jak gromadzenie danych o użytkownikach, powoduje pewną ostrożność w podejściu do tej technologii, dlatego jedynie **17% badanych** deklaruje większe zaufanie do firm wykorzystujących AI.

Mimo pewnych obaw Polacy dostrzegają ogromny potencjał AI w wielu dziedzinach życia. To stawia przed nami wyzwanie budowania zaufania do tej technologii i edukowania społeczeństwa w zakresie jej bezpiecznego i odpowiedzialnego wykorzystania. AI oraz Aml wpływa na wiele aspektów naszego życia i, choć



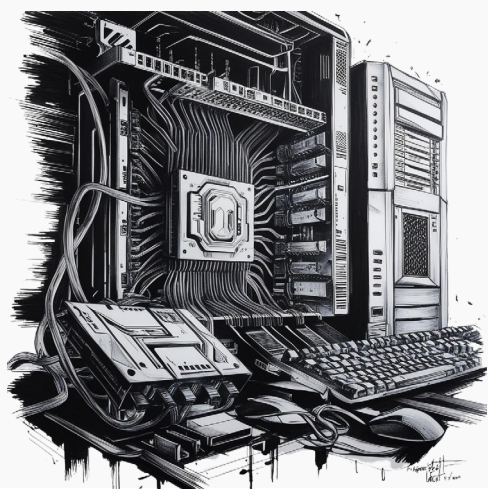
nie zawsze jest to widoczne, AI staje się coraz bardziej integralną częścią naszej codzienności.

## Czy AI jest obecne w polskim sektorze publicznym

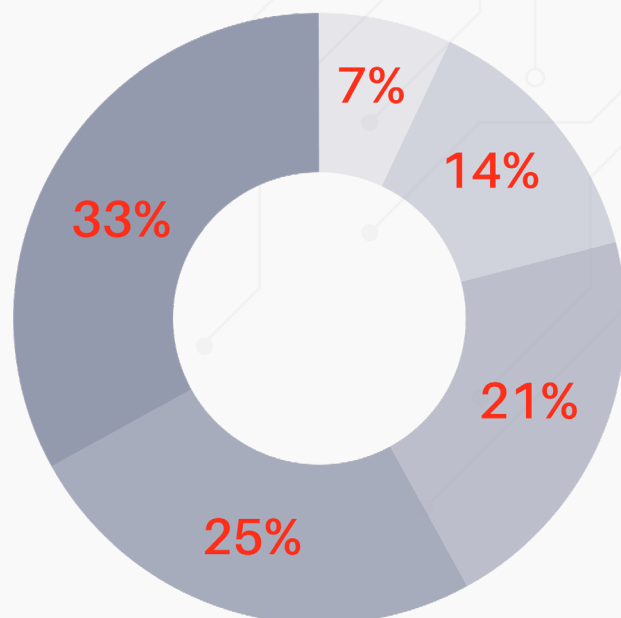
Adaptacja AI w sektorze publicznym nie jest jeszcze na tym samym poziomie, co w sektorze prywatnym. Niemniej jednak już sama dyfuzja technologii powoduje pojawianie się rozwiązań opartych o sztuczną inteligencję w tym obszarze.

Sektor publiczny nie może pozwolić sobie na zignorowanie rozwiązań, które są bardziej efektywne i tańsze niż klasyczne systemy. Ta świadomość spółek z sektora publicznego powoduje coraz szybsze tempo adaptacji rozwiązań opartych o AI w instytucjach publicznych. Nie jest to jeszcze tempo odpowiadające sektorowi prywatnemu, ale i tak jest ono imponujące, biorąc pod uwagę typową inercję sektora publicznego.

Firmy z sektora prywatnego z kolei bardzo szybko i w dużym stopniu implementują rozwiązania AI. Według danych Forbes aż **83% firm, twierdzi, że wykorzystanie AI w strategii biznesowej to dla nich najwyższy priorytet** - głównie w zadaniach takich jak automatyzacja komunikacji i chatboty.



Wykres 1: Użycie AI w firmach



- 33% - Rozpoczęliśmy wdrażanie z niewieloma przypadkami użycia AI
- 25% - Mamy procesy, które są w pełni obsługiwane przez AI i są powszechnie stosowane
- 21% - Mamy kilka koncepcji, które chcemy wdrażać na większą skalę
- 14% - Przetestowaliśmy kilka sprawdzonych koncepcji ale z umiarkowanym powodzeniem
- 7% - Nie używają AI, ale planują

Polacy są otwarci na technologie, ale dostrzegają też potencjalne zagrożenia. Według danych z raportu digitalpoland "Technologia w służbie społeczeństwu\_2023. Czy polacy zostaną społeczeństwem 5.0?" aż **94% Polaków uważa umiejętności cyfrowe za klucz do lepszej pracy**, a 93% twierdzi, że technologie ułatwiają codzienne życie. Najlepiej ocenianym narzędziem AI według tego samego raportu są indywidualni asystenci (np. chatboty, voiceboty), wspierający w zadaniach zawodowych i edukacyjnych, którzy uzyskali aż 73% głosów.

Nie jest to jednak tylko optymizm, ponieważ, jak wskazują dane, **54% Polaków wyraża obawy co do technologii robotyki i AI**. Jest to wzrost do poziomu z 2020 roku. Pomimo pewnych obaw co do AI, Polacy deklarują w badaniu, że chętnie korzystają z jej dobrodziejstw w codziennym życiu, takich jak tłumaczenie tekstów, wirtualni asystenci, prognozy pogody i chatboty obsługi klienta.

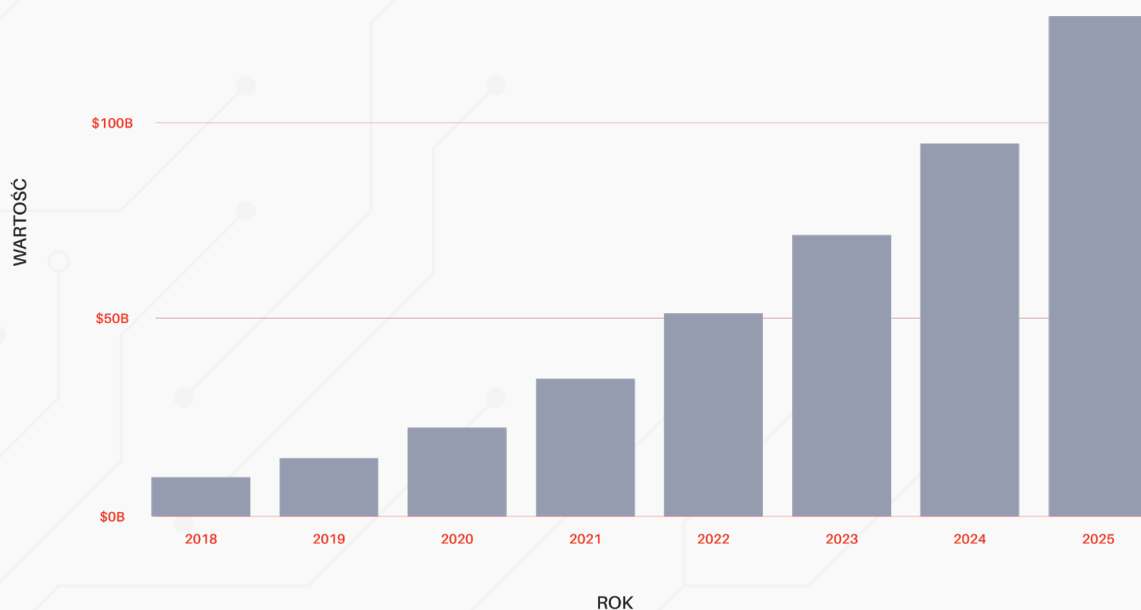
Istotnym elementem wdrażania zaawansowanych rozwiązań technologicznych na skalę krajową jest również edukacja. Należy zwrócić uwagę na kształcenie kadr w sektorze publicznym, które będą wdrażać i wykorzystywać rozwiązania oparte na AI, oraz społeczeństwa, aby obywatele byli świadomi potencjału oraz słabości sztucznej inteligencji i korzystali z niej w sposób odpowiedzialny.

## Mocne strony i sukcesy Polski w obszarze AI

Polski rynek AI charakteryzuje się dynamicznym wzrostem, w 2023 roku, według Ntiative, liczył on 10 900 specjalistów, którzy deklarowali na LinkedInie umiejętności AI na swoim profilu. Duża część z nich (15%) zajmuje stanowiska wysokie i kierownicze, a 58% z nich nabyło umiejętności AI zaledwie w ciągu ostatniego roku.

Ten wynik nie powinien dziwić, ponieważ to właśnie poprzedni rok był na polskim rynku ogromnym skokiem w rozwoju i implementacji AI w branży IT oraz marketingu. Ta ostatnia w kontekście AI ma najszybciej rosnące zapotrzebowanie na taką pulę talentów jak: marketing w mediach społecznościowych (+280%), digital marketing (+206%), SEO (+199%), wsparcie techniczne (+162%) i e-commerce (+128%).

## Wykres 2: Przychody globalnego rynku oprogramowania sztucznej inteligencji



Przewiduje się, że **do 2025 roku w obszarze AI na całym świecie będzie zatrudnionych aż 97 milionów osób**, a sama wielkość globalnego rynku AI ma rosnać o co najmniej 120% rok do roku.

Rozwój Polski w obszarze AI potwierdza też rosnąca liczba start-upów, które inwestują w badania i rozwój swoich produktów opartych na AI i odnoszą przy tym komercyjne sukcesy. Takie firmy jak Nomagic, DataPlace, Sentione czy Infermedica z powodzeniem działają i eksportują swoje produkty i usługi na skalę międzynarodową.

Dla przykładu DataPlace to platforma do udostępniania i analizy danych dla różnych sektorów gospodarki, która zdobyła nagrodę European Data Platform of the Year 2022. Sentione, czyli platforma do monitorowania mediów społecznościowych i analizy opinii publicznej, jest wykorzystywana przez agencje rządowe, firmy i organizacje pozarządowe w wielu krajach.

Infermedica to z kolei polski start-up, który opracował system AI do wspomagania diagnostyki medycznej oparty na bazie wiedzy medycznej i algorytmach uczenia maszynowego. Pomaga lekarzom w stawianiu trafnych diagnoz poprzez analizę symptomów pacjenta i sugerowanie dalszych badań. Infermedica współpracuje z lekarzami i placówkami medycznymi w Polsce i na świecie, a jej system został wdrożony w języku polskim, angielskim, niemieckim, hiszpańskim i portugalskim. Potencjalnie może mieć wpływ zarówno na sektor prywatny jak i publiczny.

Sztuczna inteligencja ma również realny wpływ na wzrost gospodarczy i efektywność sektora publicznego. Przykładem może być e-Urząd, czyli inteligentny bot, który automatyzuje procesy administracji publicznej i udziela informacji na temat spraw urzędowych i jest oparty na modelu GPT.

### Gdzie czeka nas jeszcze trochę pracy?

Jedną z podstawowych przeszkód związanych z wykorzystaniem AI jest wieloaspektowe zagadnienie przetwarzania danych. – na przykład przetwarzania danych przez zewnętrzne usługi AI. Wysyłanie danych — zwłaszcza danych obywateli — na zewnętrzne serwery budzi uzasadnione obawy dotyczące bezpieczeństwa i prywatności danych. Istniejące dyrektywy i przepisy dotyczące przetwarzania danych nie są jeszcze wystarczająco precyzyjne w kwestii AI. Jest to o tyle istotne, że przetwarzanie danych przez AI jest procesem istotnie różnym od przetwarzania ich przez systemy "klasyczne".

Osobną kwestią związaną z przetwarzaniem danych przez AI są dane treningowe. Wiedza modeli AI pochodzi z danych, którymi są one "karmione" podczas procesu treningu. Jeżeli dane nie są odpowiednio przetworzone czy zanonimizowane, istnieje ryzyko, że model zdobędzie wiedzę, której nie powinien posiadać, jak np. dane wrażliwe.

Nie jest to ryzyko czysto teoretyczne – w branży IT głośno było o incydentach związanych z asystentami AI, które, nauczone wyłącznie publicznie

dostępny danymi, były w stanie generować kody źródłowe zamkniętych, komercyjnych rozwiązań.

Jeszcze osobnym (i wciąż nierozwiązanym) problemem jest kwestia praw autorskich dzieł i materiałów stworzonych za pomocą AI. Wykorzystanie modeli generatywnych budzi również uzasadnione obawy w kontekście wiarygodności generowanych danych. Jakość generowanych przez AI tekstów, filmów czy obrazów jest już na tyle wysoka, że przeciętny odbiorca o niewprawionym oku ma trudności z odróżnieniem ich od treści rzeczywistych lub stworzonych przez człowieka.

## Wyzwania wobec implementacji AI na szeroką skalę

Sztuczna inteligencja już teraz mocno wpłynęła na rynek pracy – zwłaszcza w zawodach kreatywnych, takich jak graficy 2D/3D, muzycy, scenarzyści, copywriterzy, czy dziennikarze. Automatyzacja wielu czynności w tych zawodach powoduje zmniejszenie zapotrzebowania na ludzkich specjalistów, co prowadzi do realnych problemów na rynku pracy.

Automatyzacja pracy kreatywnej budzi również wiele obaw i kontrowersji. Nie dziwią więc głosy, które domagają się regulacji prawnych i zakazu stosowania AI w niektórych branżach. Przykładem może być strajk scenarzystów w USA, którzy protestowali przeciwko rosnącej roli AI w tworzeniu treści filmowych.

Konieczne jest stworzenie systemów edukacyjnych, które będą przygotowywać ludzi do pracy w zautomatyzowanym świecie. Pracownicy

*Podjęcie luddystyczne wydaje się jednak tylko rozpaczliwą próbą ucieczki przed nieuniknionym. Odrzucanie AI i próba zatrzymania postępu technologicznego nie jest racjonalnym podejściem ani rozwiązaniem. Kluczowym elementem adaptacji do zmian na rynku pracy jest edukacja i przekwalifikowanie pracowników.*

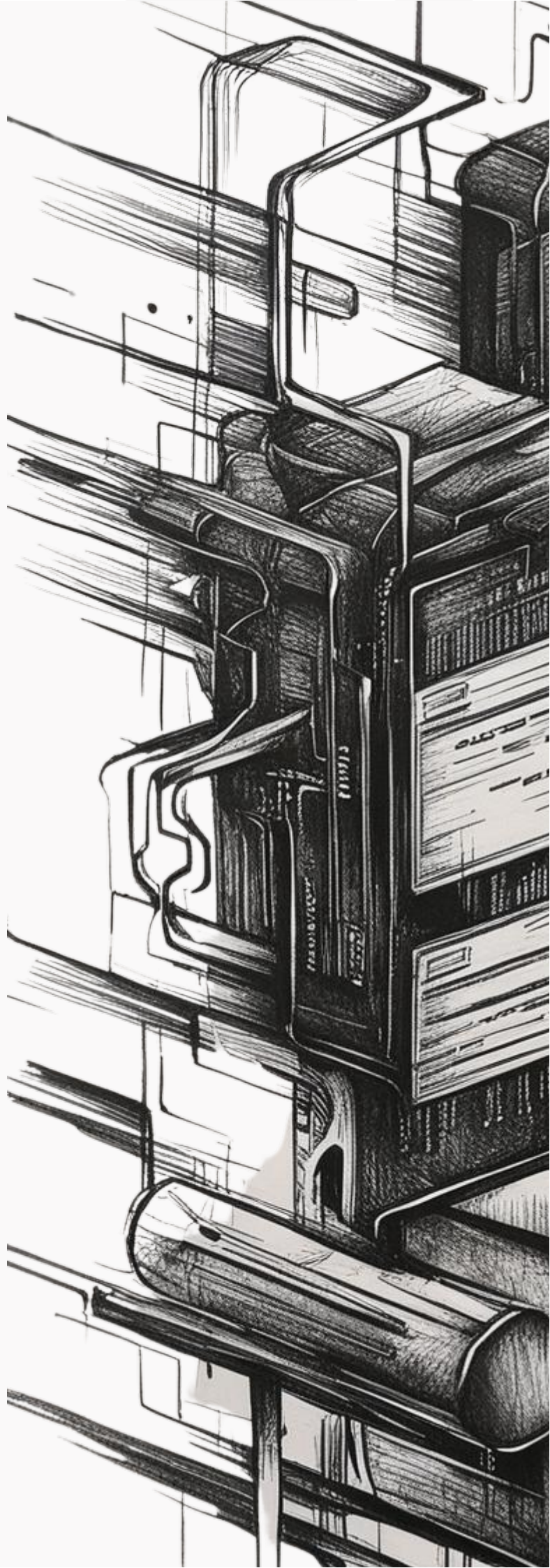
powinni już teraz zdobywać nowe umiejętności, które pozwolą im wykorzystać AI jako narzędzie do usprawniania swojej pracy, a nie jako zagrożenie dla ich pozycji na rynku pracy.

## Synergia biznesu i nauki

Wsparcie rozwoju AI w Polsce powinno odbywać się na kilku płaszczyznach. Na płaszczyźnie technicznej, konieczny jest rozwój rodzimych modeli AI – takich jak modele językowe dedykowane dla języka polskiego. Obecnie trwają już badania nad tym zagadnieniem.<sup>2</sup> Wyliminuje to konieczność przetwarzania danych przez rozwiązania komercyjne, hostowane przez zagraniczne firmy w rodzaju OpenAI czy Microsoft i pozwoli na przetwarzanie danych w całości w infrastrukturze organizacji. W konsekwencji pozwoli na zastosowanie ich, chociażby w sektorze publicznym.

Rozwój takich modeli będzie możliwy dzięki wsparciu finansowemu z programów rządowych. Firma TSS korzystała i korzysta z takiego wsparcia, czego rezultatem były nowatorskie modele AI, które, oprócz tego, że stanowiły innowację na poziomie naukowym, miały również rzeczywiste zastosowanie.

Jednak największy postęp w dziedzinie AI, co widać w innych krajach, można osiągnąć wyłącznie na drodze synergii instytucji naukowych oraz biznesowych. Placówki naukowe dostarczają wówczas niezbędną wiedzę teoretyczną, zaś sektor prywatny — generuje konkretne przypadki użycia i wspiera ich realizację.



DR INŻ. **KAROL ANT CZAK**  
AI SOLUTIONS ARCHITECT, TSS

## Cyfryzacja w sektorze zdrowia

**Starzejące się społeczeństwo, coraz więcej chorób cywilizacyjnych oraz finansowanie zależne od decyzji politycznych to tylko niektóre z problemów, z którymi musi mierzyć się nasz system opieki zdrowotnej. W czasie rosnących kosztów nowoczesnych rozwiązań i niedoboru wykwalifikowanego personelu cyfryzacja tej branży przestaje istnieć tylko w teorii snutej na temat jutra, a zaczyna stawać się nową rzeczywistością.**

**Pandemia COVID-19 uwidoczniała głęboko zakorzenione problemy strukturalne w systemach opieki zdrowotnej na całym świecie. W Polsce podobnie jak w innych krajach pandemia wymusiła zwiększenie wydatków na ochronę zdrowia o prawie jedną trzecią w porównaniu z rokiem 2019. Te wydarzenia pokazały, że zdrowie jest fundamentem odpornej i produktywnej gospodarki. W kontekście tych wyzwań koncepcja 5P - partycypacja, personalizacja, precyzja, prognozowanie i prewencja - staje się realną odpowiedzią na rosnące potrzeby zdrowotne społeczeństwa.**

### **5P - partycypacja, personalizacja, precyzja, prognozowanie i prewencja**

Kampania Global Future of Health, rozpoczęta przez firmę Deloitte w 2017 roku, zakłada, że do 2040 roku system opieki zdrowotnej będzie zorganizowany wokół obywateli, a nie instytucji. Model „5P” to nowoczesne podejście w ochronie zdrowia, które kładzie nacisk na holistyczne zarządzanie zdrowiem. Zamiast koncentrować się jedynie na leczeniu chorób, model ten promuje partycypację pacjentów w procesie leczenia, personalizację terapii, precyzyjne interwencje, prognozowanie problemów zdrowotnych oraz prewencję. Dzięki temu możliwe jest poprawienie stanu zdrowia populacji ogólnej i znaczne zmniejszenie liczby zachorowań na choroby przewlekłe.

Wprowadzenie podejścia 5P pozwala na wcześniejsze wykrywanie problemów zdrowotnych, co ogranicza konieczność leczenia w nagłych przypadkach. Eksperti od foresightu już od lat wskazują, że czeka nas przejście od reaktywnego modelu leczenia do proaktywnego zarządzania zdrowiem. Według mnie będzie to możliwe w najbliższych latach właśnie dzięki wykorzystaniu w medycynie nowoczesnych technologii - w tym sztucznej inteligencji. Nadchodząca (a może już trwająca?) transformacja w obszarze opieki zdrowotnej koncentruje się na profilaktyce, wczesnej diagnostyce oraz utrzymaniu dobrego samopoczucia pacjentów, co w efekcie zwiększy wydajność kosztową całego systemu.

Zgodnie z szacunkami, redukcja częstości występowania niektórych chorób dzięki podejściu 5P może zmniejszyć wydatki na opiekę zdrowotną. W Europie szacuje się około 250 miliardów euro do 2030 roku, a w perspektywie kolejnej dekady nawet 595 miliardów euro.<sup>3</sup> Większy nacisk na profilaktykę, jak np. szczepienia na HPV dla dziewczynek, może przynieść znaczące korzyści zdrowotne i finansowe, ponieważ zredukowane w systemie zostaną koszty diagnozowania i leczenia m.in. raka szyjki macicy.

Revolucja neurotechnologiczna, która obejmuje rozwój zaawansowanych interfejsów mózg-komputer, neuroimplantów i technologii do głębokiej stymulacji mózgu, również wpisuje się w model 5P. Innowacje w medycynie regeneracyjnej nie tylko poprawiają jakość życia osób z niepełnościami, ale także oferują nowe możliwości w leczeniu chorób neurodegeneracyjnych i psychiatrycznych.

### Wykres 3: Wydatki na opiekę zdrowotną przesuną się w kierunku promocji zdrowia i profilaktyki



## Jak zmieniła się praca lekarza rodzinnego w perspektywie pandemii COVID-19?

Pandemia COVID-19 znacząco przyspieszyła wdrażanie technologii cyfrowych w medycynie, szczególnie tych umożliwiających zdalny kontakt z pacjentami. Analiza firmy doradczej Deloitte wykazała, że niemal 65% instytucji zwiększyło wykorzystanie technologii cyfrowych wspierających pracę medyków, a 64,3% respondentów potwierdziło ich zastosowanie w zdalnym wsparciu i kontakcie z pacjentami. Lekarze pierwszego kontaktu (74,7%) najczęściej korzystał z tych rozwiązań, przyjmując zdalne formy wstępnej oceny pacjentów, co stało się powszechną praktyką w obliczu koronawirusa.<sup>4</sup>

Pandemia zmusiła lekarzy rodzinnych do adaptacji i wdrożenia nowych technologii, co było pierwszym przełomem w świadczeniu usług medycznych w scyfryzowanej formie. Zdalne konsultacje stały się normą, umożliwiając lepszy dostęp do opieki zdrowotnej, nawet w trudnych warunkach epidemiologicznych. Cyfryzacja opieki zdrowotnej poprawiła efektywność oraz zwiększyła komfort pacjentów, pozwalając na lepsze zarządzanie swoim zdrowiem zdalnie, bez konieczności osobistych wizyt w placówkach medycznych w przypadkach tego niewymagających.

System opieki zdrowotnej w Polsce znacząco się zmodernizował również dzięki technologii informacyjnej i telekomunikacyjnej. Internetowe Konto Pacjenta (IKP), e-recepty, e-skierowania

oraz elektroniczna dokumentacja medyczna (EDM) stały się już w całej Polsce pewnym standardem, ułatwiając dostęp do usług zdrowotnych pacjentom. Ponad 17,1 mln osób korzysta z IKP, umożliwiającego szybki dostęp do danych medycznych, a ponad 37 mln osób otrzymało 1,61 miliarda e-recept. Od stycznia 2021 roku wystawiono ponad 136 milionów e-skierowań, zrealizowano prawie 42 miliony z nich.<sup>5</sup>

Pandemia przyspieszyła także rozwój aplikacji *mojeIKP*, która powstała w 2021 roku i wprowadziła szereg udogodnień postpandemicznych. Aplikacja ta umożliwia pacjentom upoważnienie lekarza, pielęgniarki czy farmaceuty do wglądu w dane medyczne, co jest szczególnie użyteczne w nagłych przypadkach zagrożenia zdrowia. Dzięki aplikacji pacjenci mogą łatwo zarządzać e-skierowaniami, sprawdzać terminy konsultacji oraz przeglądać historię wizyt.

## Nowoczesne narzędzia do regularnej kontroli zdrowia

Do roku 2040, a nawet wcześniej, przewiduje się znaczący wzrost kompetencji cyfrowych społeczeństwa, co przełoży się na powszechne wykorzystanie urządzeń typu *wearables*. Dzięki rosnącej biegłości cyfrowej społeczeństwo będzie proaktywnie zarządzać ryzykiem zdrowotnym, wykorzystując technologie takie jak *AgeTech*, *FemTech* oraz medycynę precyzyjną i regeneracyjną. Spersonalizowane porady zdrowotne,



dostępne za pośrednictwem zatwierdzonych aplikacji oraz połączonych urządzeń mają sprzyjać dbaniu o zdrowie fizyczne i psychiczne.

Smartwatche czy opaski sportowe wyposażone w zaawansowane technologie, już teraz umożliwiają monitorowanie parametrów zdrowotnych w czasie rzeczywistym, takich jak tętno czy poziom nasycenia tlenem we krwi (pulsoksymetr). Monitorują również poziom stresu na podstawie tętna i są w stanie wykryć atak paniki, a następnie poinstruować, co trzeba w takiej sytuacji zrobić — np. wykonać ćwiczenia oddechowe. Dzięki temu diagnostyka bez wychodzenia z domu może być normą, a dane generowane przez te urządzenia pozwolą na opracowanie personalizowanych planów zdrowotnych.

## Rewolucja technologiczna i niedobór personelu medycznego

Obecnie sektor opieki zdrowotnej zmagają się z poważnym problemem niedoboru personelu medycznego. Już w 2020 roku w krajach Europy brakowało około miliona pracowników ochrony zdrowia. Wiele pracowników medycznych, w tym pielęgniarek oraz lekarzy ma ponad 55 lat, co grozi poszerzeniem luki kadrowej w najbliższych latach.<sup>6</sup> Tymczasem, zamiast zajmować się pacjentem lub odpoczynkiem, co również jest istotnym elementem zarządzania własnymi zasobami, muszą oni spędzać wiele godzin na wypełnianiu dokumentacji, która w części szpitali, szczególnie tych w mniejszych

miejsowościach, jest w formie papierowej. Wobec tego brakuje zautomatyzowanych systemów, które mogłyby usprawnić te procesy.

Cyfryzacja pracy klinicznej i automatyzacja zadań administracyjnych to kluczowe obszary, które mogą znacząco poprawić tę sytuację. Wprowadzenie zaawansowanej sztucznej inteligencji (AI oraz ML) opartej na narzędziach OCR (optycznym rozpoznawaniu znaków) mogłoby przyczynić się do usprawnienia funkcjonowania zaplecza administracyjnego, diagnostyki obrazowej oraz przyspieszenia procedur opracowywania leków i badań klinicznych.

## Zastosowanie Machine Learningu w radiologii

W Polsce następuje znaczący postęp technologiczny w dziedzinie radiologii, co modyfikuje sposób diagnozowania i monitorowania pacjentów. Algorytmy sztucznej inteligencji (AI), zwłaszcza głębokie uczenie się, wykazują niezwykłą skuteczność w rozpoznawaniu obrazów medycznych, co prowadzi do fundamentalnych zmian w codziennej praktyce radiologów.

W tym kontekście warto wspomnieć o TraumaScan — projekcie szybkiej, zautomatyzowanej analizy tomografii komputerowej całego ciała, nad którym pracujemy w TSS. Wykorzystując zaawansowane technologie przetwarzania obrazu i sztucznej inteligencji, nasze narzędzie wspiera proces diagnostyczny u pacjentów z podejrzeniem urazów

wielonarządowych, często będących wynikiem wypadków komunikacyjnych.

System skanuje głowę, klatkę piersiową, brzuch i miednicę, a w razie potrzeby także kończyny, a następnie szybko analizuje wyniki, identyfikując obrażenia narządów miękkich, aorty, mózgu oraz układu kostnego. TraumaSkan oznacza na skanach miejsca z uszkodzeniami tkanek, co ułatwia szybsze i dokładniejsze rozpoznanie stanu pacjenta. System składa się z pięciu modułów: wstępnego przetwarzania obrazów, wnioskowania, wizualizacji, raportowania oraz z modułu administracyjnego. Dzięki TraumaSkan możliwe jest przyspieszenie procesu diagnostycznego, co poprawia jakość opieki zdrowotnej i efektywność leczenia.

Szczególnie cieszy mnie jednak widoczny postęp w dziedzinach, gdzie nowoczesne rozwiązania, takie jak TraumaSkan, mogą przyspieszyć i usprawnić proces diagnostyczny, co jest niezwykle ważne, chociażby w kontekście niedoboru personelu medycznego. Warto inwestować w rozwój narzędzi, które sprawią, że system opieki zdrowotnej będzie bardziej efektywny, dostępny dla każdego obywatela i zrównoważony.



## ADAM PACZUSKI

CEO & CO-FOUNDER TSS,  
PEŁNOMOCNIK ZARZĄDU KIGC  
DS. SZTUCZNEJ INTELIGENCJI

## Nowe technologie, nowe nadzieje

Nowe technologie, nowe nadzieje

Cyfryzacja, automatyzacja i zaawansowane technologie oparte na AI i uczeniu maszynowym mają potencjał do tego, aby na stałe zmienić sposób funkcjonowania całego systemu opieki zdrowotnej w Polsce.

Dzięki pojawiającym się nowym technologiom możemy oczekiwać wcześniejszego wykrywania problemów zdrowotnych oraz skuteczniejszej prewencji, co w sposób bezpośredni może przełożyć się m.in. do redukcji kosztów w ochronie zdrowia.



# Sztuczna Inteligencja dla edukacji

---

## **Edukacja cyfrowa na ścieżkach kształcenia**

Adam Bednarek

## **Edukacja goni technologię czy odwrotnie?**

Lidia Mirowska

## **Czas na edukację cyfrową w szkołach?**

Radosław Potrac

## **Polska transformacja cyfrowa w edukacji to szansa i wyzwanie**

Zyta Czechowska

## Edukacja cyfrowa na ścieżkach kształcenia

**Podstawowym wyzwaniem jest wdrożenie środowiska nauczania uwzględniającego systemowe rozwiązania technologiczne oferujące immersyjne podejście do kształcenia w postaci treści oraz urządzeń XR.**

Przepisy polskiego prawa oświatowego stanowią:

- *Upowszechnianie wśród dzieci i młodzieży wiedzy i umiejętności niezbędnych do aktywnego uczestnictwa w kulturze i sztuce narodowej i światowej (Art.1. pkt. 13);*
- *Dostosowanie kierunków i treści kształcenia do wymogów rynku pracy (art. 1 pkt 17);*
- *Kształtowanie u uczniów postaw przedsiębiorczości i kreatywności sprzyjających aktywnemu uczestnictwu w życiu gospodarczym, w tym poprzez stosowanie w procesie kształcenia innowacyjnych rozwiązań programowych, organizacyjnych lub metodycznych (art. 1 pkt 18);*

Środowisko XR jest zatem zgodna zasadą wspieraniu transformacji cyfrowej gospodarki oraz przygotowanie osób do nowego rynku pracy.

Istnieją trzy rodzaje immersji oferowane przez technologie XR: w pełni immersyjne, półimmersyjne

i nieimmersyjne. W pełni immersyjne treści wymagają użycia specjalnych urządzeń, takich jak VR HMD (wyświetlacze montowane na głowie), które pozwalają użytkownikom zanurzyć się w wirtualnym środowisku, blokując wszystkie informacje zewnętrzne. Z drugiej strony, treści nieimmersyjne nie wymagają żadnych specjalnych urządzeń do interakcji z użytkownikiem; wykorzystują ekrany mobilne i stacjonarne i są uważane za najniższy poziom immersji. Wreszcie, semi-immersyjne mieści się pomiędzy tymi dwoma typami; wykorzystuje rzeczywiste środowisko lub sprzęt, który jest kompatybilny i podłączony do ekranu komputera stacjonarnego, aby zwiększyć poziom immersji bez odcinania wszystkich informacji zewnętrznych.

Jedną z głównych zalet narzędzi XR jest to, że zapewniają one wciągające doświadczenia, które pozwalają użytkownikom na interakcję z wirtualnymi obiektami w sposób, który wydaje się naturalny i intuicyjny. VR pozwala wejść do w pełni wciągającego środowiska, które może symulować praktycznie każde środowisko. Z drugiej strony AR nakłada informacje cyfrowe na świat rzeczywisty, umożliwiając tworzenie interaktywnych doświadczeń, które poprawiają rzeczywiste sytuacje. Na przykład mechanik mógłby użyć okularów AR, aby wyświetlić cyfrowe nakładki silnika, podkreślając różne części i dostarczając informacji o tym, jak je naprawić. AR może być wykorzystywana w edukacji, aby ożywić podręczniki, umożliwiając uczniom odkrywanie modeli 3D złożonych koncepcji

i angażowanie się w nie w bardziej interaktywny sposób. Jak sama nazwa wskazuje, MR łączy w sobie elementy VR i AR, aby zapewnić bardziej wciągające wrażenia. Użytkownicy mogą wchodzić w interakcje z wirtualnymi obiektami, które są płynnie zintegrowane ze światem rzeczywistym za pomocą MR, umożliwiając poziom interakcji, który nie jest możliwy w przypadku tradycyjnych interfejsów opartych na ekranie.

Tworzenie interaktywnych materiałów edukacyjnych będzie wiązało się z wyzwaniami. Kluczową kwestią są tutaj adaptacyjne lub inteligentne systemy nauczania. Wielu nauczycieli zgłasza swoje obawy, ponieważ mają bardzo ograniczoną dostępność projektów instruktażowych. Odnosi się to do ograniczonych materiałów dostępnych w VR/AR, bez pewności, że materiały te spełnią cele edukacyjne uczniów. Co więcej, interoperacyjność treści VR na różnych platformach jest trudna do osiągnięcia, więc VR jest często dostarczana jako zastrzeżone rozwiązanie stworzone lub będące własnością organizacji lub osoby fizycznej. Inną kwestią jest to, że w literaturze opublikowano wiele badań i przeglądów dotyczących edukacyjnego wykorzystania technologii XR, ale większość z nich, jeśli nie wszystkie, nie ma na celu pokazania, jakie różne podejścia są dostępne dla przeciętnego nauczyciela do tworzenia materiałów edukacyjnych XR. W jednym z badań przeanalizowano rynek VR dla edukacji i szkoleń w kilku dziedzinach w latach 2019-2021 za pośrednictwem sklepu internetowego jednego z głównych graczy VR HMD,

Oculus. Odkrycia ujawniły, że **ponad połowa dostępnych aplikacji jest bezpłatna, większość jest w języku angielskim, a najlepiej oceniane aplikacje pochodzą z dziedzin przyrody, astronomii, medycyny, sztuki i historii.**

Polska, podobnie jak wiele innych krajów europejskich, nie jest obca firmom i startupom oferującym rozwiązania XR. Przykładowo, firma 3WAY Monika Mitoraj prowadziła prace badawczo-rozwojowe w wyniku grantu z Kujawsko-Pomorskiej Agencji Innowacji w ramach programu Fundusz Badań i Wdrożeń, których celem było opracowanie elementu metodyki prowadzenia zajęć językowych w obszarze VR/AR, a także niezbędnych prototypów systemów. 3WAY opracował pierwsze na rynku polskim i europejskim narzędzie do nauczania języków obcych w przestrzeni VR, w którym nauczyciel i uczeń lub grupa uczniów spotykają się na zajęciach w czasie rzeczywistym. Seria testów potwierdziła, że wybrana ścieżka jest najlepsza dla dalszych prac i rozwoju projektu. Firma stworzyła prototyp, który wzbudził duże zainteresowanie. Narzędzia zgromadzone w aplikacji, takie jak modele 3D, tablica, możliwość rysowania 3D, czy zamieszczone grafiki, ułatwiają prowadzenie zajęć i dodają im kontekstowości, będąc jednocześnie unikalną nowością dla użytkowników, stanowiącą dodatkowy element dowartościowujący prowadzenie zajęć w konkretnej przestrzeni.

Kolejne wyzwanie to rozwój edukacji w chmurze. Jest to system zarządzania nauczaniem, w skrócie LMS, czyli wielofunkcyjne narzędzie, które

pomaga w zarządzaniu szkoleniami i rozwojem pracowników. Cały proces nauki może być w pełni zautomatyzowany i obsługiwany za pomocą jednej platformy. Podstawowymi obowiązkami LMS są optymalizacja procesów, dostarczanie szkoleń i umożliwienie tworzenia kursów. Automatyzację można wykorzystać na przykład do zapewnienia, że nowi pracownicy w danym dziale otrzymają odpowiednie materiały szkoleniowe natychmiast po dołączeniu do struktury organizacyjnej firmy. Dodatkowo, system powiadomi ich po określonym czasie, jeśli będą potrzebowali powtórzyć lub odświeżyć szkolenie, odciążając tym samym pracowników działu HR/twórców materiałów akademickich/dzieci wykluczonych etc. Materiały szkoleniowe są bezpiecznie przechowywane w bibliotece na platformie LMS. Skuteczny system archiwizacji umożliwia szybkie wyszukiwanie danych, rozszerzanie bazy wiedzy i dostęp do materiałów z dowolnego miejsca i w dowolnym czasie. AHE buduje ten model studiowania w postaci Polskiego Uniwersytetu Wirtualnego (PUW).

Należy też pamiętać, że rok 2023 przyniósł ogromną poprawę wydajności AI, a jej wartość dla przedsiębiorstw wynika z pojawienia się dużych modeli językowych lub LLM (Large Language Models), takich jak ChatGPT. Modele głębokiego uczenia mogą być wstępnie wytrenowane na ogromnych ilościach nieoznakowanych, nieprzetworzonych danych; celem przyświecającym takim działaniom jest uniknięcie zafałszowania wyników na skutek

wprowadzenia wstępnie błędnych danych lub specjalnego ich przygotowania w celu osiągnięcia potencjalnego wyniku. Zatem uczelnie mogą tworzyć własne modele, które opierają się na badaniach własnych pracowników oraz prac magisterskich by stworzyć narzędzia badawcze AI wspomagające rozwój studentów oraz pracowników.

- *Stworzenie w szkołach, uczelniach i innych instytucjach edukacyjnych środowiska nauczania XR (nowoczesna klasa) poprzez 'przebudowę' tradycyjnej klasy lekcyjnej.*
- *Wsparcie firm i startupów tworzących materiały pozwalające na nauczanie w środowisku XR na podstawie zebranych 'dobrych praktyk'.*
- *Wsparcie rozwoju 'szkoły w chmurze' opartej na technologii LMS dla osób wykluczonych oraz szukających alternatywnej formy rozwoju.*
- *granty na rozwój instytucjonalnych modeli językowych opartych na dorobku instytucji w celu stworzenia 'wirtualnych asystentów' wspierających kreatywne odkrywanie.*



**DR ADAM BEDNAREK**

AKADEMIA  
HUMANISTYCZNO-  
EKONOMICZNA W ŁODZI

## Edukacja goni technologię czy odwrotnie?

Skoncentrujemy się na modelu nauczania z wykorzystywaniem metod i technik kształcenia na odległość, funkcjonującym w polskim szkolnictwie wyższym.

Kształcenie na odległość na poziomie studiów wyższych, czyli e-learning akademicki, ma bogatą historię w rodzimej edukacji. Po raz pierwszy kursy korespondencyjne zaoferował już w 1776 roku Uniwersytet Krakowski. Dziś „na odległość” – i pierwotne „e” (ang. electronic) – oznacza przede wszystkim wykorzystanie możliwości internetu, który przejął rolę poczty.

Większość ośrodków akademickich w Polsce wdraża i udoskonala rozwiązania technologiczne, umożliwiające nauczanie przez internet. Zaskakująco pozytywnie przyczyniła się do tego pandemia, która uruchomiła i przyspieszyła te procesy. Pandemia pokazała również, że można bardzo szybko nadrobić braki, by już w bardziej stabilnej rzeczywistości wznieść nauczanie na nowy poziom jakości i nowoczesności. Podczas pandemii edukacja online stała się standardem. Teraz nadszedł czas, by odejść od przymusu edukacji online i zadbać o jej jakość jako edukacji z wyboru. Czas „awaryjnego” nauczania na odległość szczęśliwie mamy za sobą. Sprzyja

to wyciąganiu wniosków oraz badaniu przemysłanych strategii wykorzystywania nowoczesnych technologii w edukacji na uczelniach wyższych.

Ośrodki akademickie coraz częściej korzystają ze wsparcia przeznaczonego na szkolenia oraz rozwój infrastruktury technicznej, wspomagającej nauczanie z wykorzystywaniem metod i technik kształcenia na odległość. Dzięki szkoleniom i wymianie doświadczeń uczelnie mają szansę być na bieżąco z trendami, pojawiającymi się na rynku. **Rządowy projekt „Doskonałość dydaktyczna uczelni” zakłada nie tylko wsparcie infrastruktury i zakup narzędzi, umożliwiających wdrożenie innowacyjnych metod do procesu kształcenia, ale również podnoszenia kompetencji kadry akademickiej.** <sup>6</sup>

Według Stowarzyszenia E-learningu Akademickiego (SEA) w polskim szkolnictwie wyższym obserwujemy właśnie dojrzałą fazę rozwoju e-learningu akademickiego (Stowarzyszenie E-learningu Akademickiego).<sup>7</sup>

To czas świadomego obcowania z narzędziami, badań naukowych, dzielenia się wiedzą i doświadczeniami. E-learning ma obecnie ugruntowaną pozycję na wielu uczelniach w kraju. Rozwijają się również działy metodyczne związane z e-learningiem. Są to często jednostki ponadwydziałowe, działające centralnie i realizujące spójną strategię w zakresie rozwoju e-learningu w danej placówce.

Obowiązkiem ośrodków akademickich jest nadążanie za rewolucją cyfrową, szczególnie w e-learningu, który bazuje na rozwiązaniach

technologicznych. Wraz ze zmieniającymi się możliwościami wsparcia edukacji rozwiązaniami technicznymi, projektanci programów nauczania i wszyscy członkowie społeczności uniwersyteckich i edukacyjnych są zobligowani do zrewidowania zarówno sposobu, w jaki odbywa się nauka, jak i doświadczenia edukacyjnego w ogólnym kontekście. Rolą uczelni, obok skupienia się na rozwoju naukowym pracowników, jest również pogłębianie ich kompetencji dydaktycznych.

Od ponad dziesięciu lat pytana o zawód, odpowiadam, że jestem metodyczką zdalnego nauczania i bardzo często słyszę prośbę o doprecyzowanie.

Metodyk to zazwyczaj specjalista, który bada istniejące metody lub tworzy nowe, dostosowane do potrzeb danej dziedziny. Metodyk zdalnego

*Nauczanie i uczenie się na odległość wymaga zmiany w sposobie myślenia o uczeniu się w ogóle. Wiąże się to z opracowaniem zestawu wieloaspektowych umiejętności, które umożliwiają właściwe radzenie sobie ze złożonością całego procesu.*

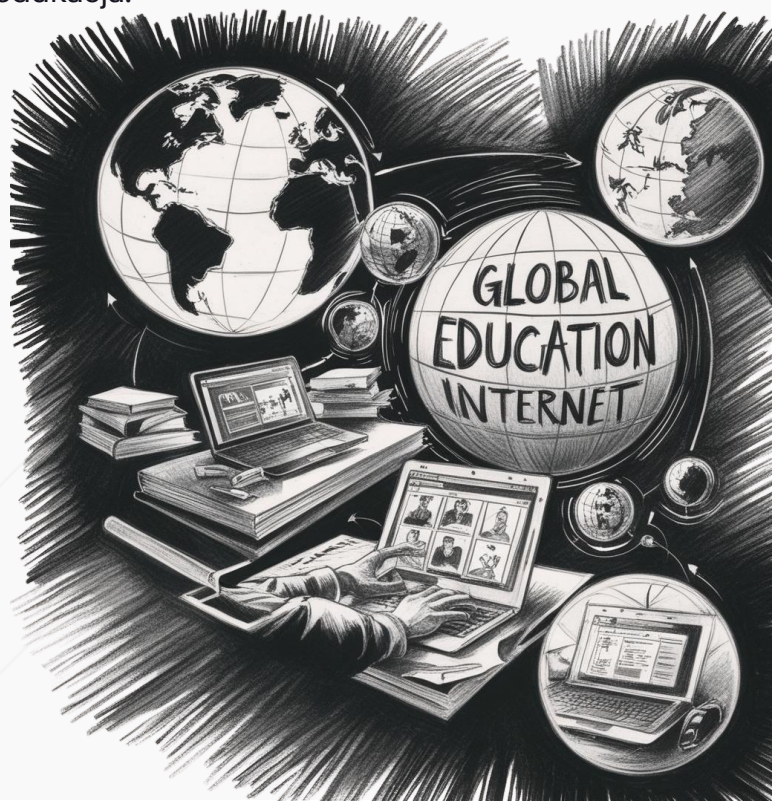
nauczania zapewnienia efektywność i skuteczność wykorzystywanych metod kształcenia, a także ich stałe udoskonalanie, by dotrzymały kroku rozwojowi edukacji. Może być m.in. zaangażowany w projektowanie programów nauczania, tworzenie materiałów dydaktycznych, prowadzenie szkoleń dla nauczycieli oraz badanie

skuteczności różnych strategii kształcenia. Celem metodyki jest zatem nie tylko przekazywanie wiedzy, ale również rozwijanie umiejętności i kompetencji uczniów/studentów w sposób odpowiedni dla ich potrzeb i możliwości.

Metodyka to niezwykle ważny obszar w edukacji, mający bezpośredni wpływ na jakość nauczania i efektywność uczenia się, co sprawia, że zajmuje ważne miejsce w procesie kształcenia.

Jaka jest więc rola metodyki w nieustannie zmieniającym się świecie technologii? Jak nadążać za rozwojem i wdrażać rozwiązania służące beneficjentom tej formy edukacji?

Wykorzystywanie technologii w kształceniu automatyzuje niektóre czynności, natomiast zaprojektowanie procesu nauczania wciąż stoi po stronie dydaktyka/metodyka. Metodyk bada pojawiające się na rynku trendy, analizuje możliwości ich wdrażania. To właśnie dzięki współpracy człowieka z technologią powstaje nowoczesna edukacja.





*Uczelnie powinny dawać przestrzeń do rozwoju metodologii nauczania, powinny promować i wyznaczać trendy w sposobach wykorzystywania nowoczesnych technologii, tworzyć swoiste centra kompetencyjne w zakresie metodyki, technologii właśnie oraz organizacji e-edukacji.*

Edukacja cyfrowa stawia aktualnie na interaktywność i mikronauczanie. Podczas projektowania zajęć uwzględnia się elementy grywalizacji oraz indywidualne ścieżki kształcenia. Na trendy w nauczaniu zdalnym wpływają pojawiające się regularnie nowe technologie oraz możliwości ich zastosowania w edukacji. Proces dydaktyczny jest coraz częściej wzbogacany technologią wirtualnej i rozszerzonej rzeczywistości (VR i AR), a także tworzone są otwarte bazy materiałów dydaktycznych, jak np. open AGH.

Wykorzystywane na uczelniach systemy LMS (Learning management system) to coraz częściej złożone platformy nie tylko służące do nauczania, ale również synchronizowane systemy zarządzania aktywnością akademicką i kompetencjami w organizacji. Platformy te pozwalają na interaktywne formy nauczania, dają możliwość udziału w grach edukacyjnych, grywalizacji (uczestnicy są angażowani i motywowani systemem punktów, odznak czy poziomów), wirtualnych laboratoriach oraz transmisjach wideo.

Nowoczesne platformy e-learningowe wyposażone są również w narzędzia analityczne

i monitorujące aktywność uczestników, śledzące postępy w nauce oraz stopień zaangażowania. Pozwalają generować raporty, dotyczące zarówno całych grup, jak i pojedynczych użytkowników, dając możliwość zaprojektowania złożonej informacji zwrotnej oraz reagowania na bieżące potrzeby użytkowników.

Dominującym trendem, nie tylko w edukacji, jest dziś wykorzystanie sztucznej inteligencji. Wraz z jej rozwojem, pojawiają się ułatwienia dla pracy nauczycieli, akademików i metodyków w postaci możliwości tworzenia scenariuszy kursów oraz automatyzacji procesów weryfikacji wiedzy. Z tej drogi nie ma odwrotu. Sztuczna inteligencja na stałe zagości w edukacji, będzie coraz szerzej dostępna i prostsza w użytkowaniu. To kolejne wyzwanie stojące przed metodykami zdalnego nauczania, które prowadzi do przededefiniowania sposobu, w jaki uczymy się i w jaki sposób to uczenie się będzie wyglądać w przyszłości.

Warto śledzić działania w zakresie metodyki zdalnego nauczania w Centrum Nowoczesnej Edukacji Politechniki Gdańskiej oraz Centrum e-Learningu i Innowacyjnej Dydaktyki AGH, które współtworzą konferencję „eTEE e-Technologie w Kształceniu Inżynierów”. W tym roku po raz trzynasty organizowana jest konferencja „Polski MoodleMoot”, która pozwala na dzielenie się pomysłami na efektywne nauczanie online.

Polski Uniwersytet Wirtualny [www.puw.pl](http://www.puw.pl) również organizuje wydarzenie, które od lat skupia się wokół edukacji zdalnej, angażując kadre

akademicką, nauczycieli ale i przedstawicieli biznesu. To „Akademia Online”, podczas której w tym roku zapytamy, co słycać w e-learningu.

Czy niedługo, odpowiadając znajomym na przywołane już wcześniej pytanie, że jestem metodyczką zdalnego nauczania, usłyszę odpowiedź inną niż „Czyli kim”? Czas pokaże. Na razie sprawdzam na bieżąco, jak ma się e-learning i czym nas zaskoczy w najbliższej przyszłości technologia w edukacji – a ta, aby nadążyć za rozwojem technologii, potrzebuje świadomej metodyki.

**Tylko proaktywne podejście do technologii i metodyki pozwoli na dostosowanie rozwiązań do potrzeb odbiorców i włączenie ich do**

**strategii uczenia i uczenia się.** To właśnie metodyka wskazuje wartości i cele, którym ma przyświecać technologia w edukacji. Dlatego warto na uczelniach inwestować w jej rozwój.

Źródła:

- <https://www.gov.pl/web/nauka/doskonalosc-dydaktyczna-uczeln-i-w-ramach-dzialania-34-zarzadzanie-w-instytucjach-szkolnictwa-wyzszego2>
- <https://samelane.com/pl/blog/immersive-learning-vr-i-ar-w-obszarze-nauki-i-rozwoju/>
- <https://www.puw.pl/pl/akademia-online>



**LIDIA MIROWSKA**

POLSKI UNIWERSYTET  
WIRTUALNY



# Czas na edukację cyfrową w szkołach

**Edukacja cyfrowa w dzisiejszym świecie stanowi kluczowy element transformacji cyfrowej, a jej rozwinięcie jest niezwykle istotne dla przyszłości społeczeństwa. Wynika to nie tylko z potrzeby kształtowania kompetencji przyszłości - wśród których znaleźć można:**

## Krytyczne myślenie i umiejętność rozwiązywania problemów

Umiejętność krytycznego myślenia i rozwiązywania pojawiających się problemów jest istotna dla oceny danych, z którymi pracują młodzi ludzie, analizy dostępnych perspektyw i użycia innowacyjnych rozwiązań skomplikowanych wyzwań. Krytyczne myślenie i twórcze podejście do rozwiązywania problemów stanowią podstawę skutecznego podejmowania decyzji, niezależnie od tego, czy chodzi o dylematy techniczne, czy też o międzyludzkie kwestie.

## Analiza i interpretacja danych

w erze Big Data umiejętność selektywnego gromadzenia, analizowania i interpretowania informacji jest niezbędna. Umiejętność obserwacji

zmian, optymalizacja wysiłku pozwala na wysnuwanie cennych spostrzeżeń z ogromnych zbiorów danych, wspomagających podejmowanie decyzji.

## Komunikacja i praca zespołowa

W erze Big Data umiejętność selektywnego gromadzenia, analizowania i interpretowania informacji jest niezbędna. Umiejętność obserwacji zmian, optymalizacja wysiłku pozwala na wysnuwanie cennych spostrzeżeń z ogromnych zbiorów danych, wspomagających podejmowanie decyzji.

## Kompetencje cyfrowe

Wraz z transformacją technologiczną w niemal każdym aspekcie życia, umiejętności cyfrowe nie są już atutem, ale konieczną kompetencją. Biegłość w korzystaniu z technologii pozwala uczniom pewnie poruszać się w cyfrowym środowisku.

## Zdolność adaptacji i elastyczność

Zdolność dostosowywania się do zmian i uczenia się przez całe życie ma kluczowe znaczenie w świecie galopujących zmian i postępu. Otwartość na nowe doświadczenia i rozwijające się technologie umożliwia szybkie dostosowanie się do zmieniających się okoliczności.

## Inteligencja emocjonalna

Zrozumienie i zarządzanie emocjami, zarówno własnymi, jak i innych, jest istotną umiejętnością w procesie budowania silnych relacji interpersonalnych i skutecznego przywództwa. Dzięki rozwiniętej inteligencji emocjonalnej uczniowie są bardziej empatyczni, samoświadomi i w sposób bardziej umiejętny poruszają się w świecie społecznym.

## Umiejętności przywódcze

Cecha niezbędna dla osób aspirujących do ról kierowniczych i każdego, kto chce osiągnąć sukces w na ścieżce swojej kariery. Bycie skutecznym liderem oznacza inspirowanie i kierowanie zespołami, podejmowanie świadomych decyzji i tworzenie pozytywnego środowiska pracy.

## Odporność

Zdolność reagowania na niepowodzenia jest istotna gdy mamy w perspektywie długoterminowe cele. Odporni psychicznie uczniowie lepiej znoszą przeciwności losu, radzą sobie ze stresem i postrzegają wyzwania jako okazję do rozwoju. Utrzymują pozytywne nastawienie i koncentrują się na celach pomimo nieuniknionych niepowodzeń.

Obecnie system nauczania powinien sprostać wyzwaniom stawianym przez transformację

cyfrową, integrując technologie w proces dydaktyczny oraz przygotowując młodzież do funkcjonowania w cyfrowej rzeczywistości – w której bezpieczeństwo cyfrowe, dobrostan cyfrowy są równie ważne, jak umiejętności.

Dzisiejsza edukacja cyfrowa w założeniu wygląda pozytywnie – lekcje informatyki są jednak nadal skupione na trenowaniu obsługi programów – które można realizować na innych lekcjach, zbyt mało czasu jest poświęcane obsłudze współczesnych środków komunikacji, programów związanych z bezpieczeństwem, gamifikacja wciąż jest nowinką – mimo, iż Polska jest na szczycie rynku gamingowego itd. Na pozostałych zajęciach w większości tylko od zaangażowania nauczyciela zależy, czy TIK pozostanie na papierze – czy znajdzie się w codzienności uczniów.

Badania przeprowadzone w 2024 przez Digitalpoland pokazują jak wygląda kwestia umiejętności cyfrowych dorosłych Polaków – tutaj, pośród kilku obszarów kwestie cyberbezpieczeństwa oraz umiejętności korzystania z danych – wciąż pozostawiają wiele do myślenia.

Podobnie jest w szkołach – IT Fitnes Test Cyfrowej Polski również obnażył wiele braków – choć wyniki na poziomie 46% w podstawowych kategoriach stawiają uczniów podstawówek i szkół średnich w nienajgorszej pozycji.

Obserwując zmiany postępujące przez lata – zauważam, że zmienił się sposób postrzegania internetu i sieci społecznościowych w porównaniu z ich początkami. Dzisiaj FB odchodzi do lamusa

wśród młodych – ponieważ mają Instagrama i Tik Toka – mimo sporych zastrzeżeń co do bezpieczeństwa tych ostatnich. To jednak nie jedyne obszary, które wciąż wymagają działań.

Diagnoza dotycząca edukacji cyfrowej uczniów w Polsce dotyka wielu innych obszarów, wśród których należy wymienić:

**Infrastruktura technologiczna:**

**Bezpieczeństwo cyfrowe:** Edukacja w zakresie bezpieczeństwa online powinna być priorytetem. Uczniowie powinni być świadomi zagrożeń związanych z internetem i umieć chronić swoje dane osobowe i reagować na problemy związane z hejtem, przemocą w sieci i innymi zagrożeniami – także związanymi z brakiem higieny cyfrowej.

**Kompetencje cyfrowe:**

**Szkolenia dla nauczycieli:** nauczyciele powinni być przygotowani do wykorzystywania narzędzi cyfrowych w nauczaniu. Szkolenia z zakresu e-learningu, programowania czy korzystania z aplikacji są niezbędne – nie tylko warte przejścia. Nauczyciel wchodzący na nową ścieżkę zawodową – powinien swobodnie poruszać się po cyfrowym świecie i znać zagrożenia płynące z ich stosowania i możliwości, jakie dają w pracy.

**Zmiany w realizacji przedmiotu "Informatyka":** podstawa programowa informatyki oraz treści nauczania powinny zostać dostosowane do wymogów współczesności. Mniej teorii, więcej wykorzystania narzędzi w praktyce – mniej Painta – więcej aplikacji do urządzeń ekranowych wykorzystujących

potencjał. Aplikacje biurowe w praktyce i na konkretach – nie tylko na danych, które nie budują motywacji i nie są związane z zainteresowaniami dzieci.

**Zawartość programowa:**

**Nowoczesne metody nauczania:**

Wykorzystanie technologii w procesie dydaktycznym, takie jak platformy e-learningowe, interaktywne materiały czy symulacje, może zwiększyć efektywność nauki – i wpłynąć pozytywnie na motywację uczniów.

**Rozwijanie umiejętności praktycznych:**

Oprócz teorii, uczniowie powinni zdobywać praktyczne umiejętności, takie jak tworzenie stron internetowych, obróbka grafiki czy programowanie – z wykorzystaniem ich w codziennym życiu, konkursach itd.

**Współpraca z rodzicami:**

**Edukacja rodziców:** Rodzice powinni być świadomi korzyści i zagrożeń związanych z technologią. Współpraca z rodzicami w zakresie budowy świadomości ale także odpowiedzialności za wychowanie dzieci i obecność w ich cyfrowym życiu – powinna wpłynąć na relacje i poczucie więzi – ale też wzmocnić poczucie bezpieczeństwa obu stron.

W tym momencie warto zauważyć, że **Fundusze Europejskie na Rozwój Cyfrowy 2021-2027** wspierają projekty związane z edukacją cyfrową, takie jak budowa społeczeństwa gigabitowego, udostępnienie zaawansowanych e-usług czy rozwój gospodarki opartej na danych i nowych technologiach. Obok nich, istnieje w Polsce kilka inicjatyw związanych z edukacją cyfrową, które mają na celu wspieranie procesu transformacji cyfrowej w polskich szkołach.

Te inicjatywy stanowią ważny krok w kierunku rozwijania kompetencji cyfrowych wśród uczniów i nauczycieli w Polsce. Wspólnie działając, możemy przyczynić się do lepszej przyszłości społeczeństwa cyfrowego.

Powinny stanowić uzupełnienie działań szkolnych i ich rozwinięcie – z powodów przytoczonych powyżej. Sumując: uczniowie powinni korzystać ze wsparcia edukacji cyfrowej z kilku ważnych powodów.

**Rozwój kompetencji cyfrowych:** Wspieranie uczniów w nabywaniu umiejętności cyfrowych jest kluczowe. Kompetencje cyfrowe pozwalają na efektywne korzystanie z technologii, rozumienie mediów, bezpieczne przeglądanie internetu i tworzenie treści. Powinno się promować programy szkoleniowe dla nauczycieli i uczniów, aby rozwijać te umiejętności.

**Dostęp do narzędzi cyfrowych:** Uczniowie powinni mieć dostęp do nowoczesnych narzędzi, takich jak komputery/laptopy, smartfony czy tablety. Infrastruktura technologiczna w szkołach

jest kluczowa, aby umożliwić skuteczne nauczanie i naukę online. By korzystać z tych narzędzi bezpiecznie – powinno się działać wspólnie z rodzicami i środowiskiem NGO-sów i mediów – by z każdej strony wykorzystać pozytywne strony narzędzi – pamiętając o bezpiecznych strefach bez technologii – cyfrowy dobrostan.

**Przygotowanie do przyszłości:** Kompetencje cyfrowe są niezbędne w dzisiejszym świecie. Uczniowie, którzy opanują umiejętności korzystania z technologii, będą lepiej przygotowani do pracy w przyszłości. Powinno się zatem promować edukację cyfrową jako element kluczowy dla rozwoju osobistego i zawodowego uczniów.

**Zwalczanie dezinformacji:** W erze informacji i internetu ważne jest, aby uczniowie potrafili krytycznie oceniać źródła informacji. Powinno się wprowadzać programy edukacyjne, które uczą umiejętności weryfikacji faktów i rozpoznawania dezinformacji online – oraz uczą reagowania na dezinformację.

**Inwestycje w infrastrukturę i wykształcenie nauczycieli:** Powinno się inwestować w infrastrukturę informatyczną w szkołach, zapewniając dostęp do szybkiego internetu, nowoczesnych urządzeń i bezpiecznych platform edukacyjnych. To kluczowe dla skutecznego nauczania i rozwijania kompetencji cyfrowych uczniów. Równie ważna jest nowa sylwetka nauczyciela, wychowawcy, edukatora – który potrafi korzystać i angażować nowe technologie w ciekawy i motywujący sposób.

Wprowadzenie edukacji cyfrowej do programów nauczania jest nie tylko koniecznością, ale także inwestycją w przyszłość młodego pokolenia. Dzięki odpowiedniemu wsparciu i rekomendacjom w obszarze edukacji, uczniowie będą mogli lepiej wykorzystać potencjał technologii i stać się aktywnymi obywatelami społeczeństwa cyfrowego.



## RADOSŁAW POTRAC

NAUCZYCIEL ROKU 2023,  
PREZES TOWARZYSTWA  
PRZYJACIÓŁ WARSZAWY



# Polska transformacja cyfrowa w edukacji to szansa i wyzwania

Nowe technologie stały się nieodłącznym elementem naszego życia. Wykorzystujemy je nie tylko w biznesie, zakupach, życiu towarzyskim, ale także w edukacji i coraz częściej w terapii, na przykład dzieci z dysleksją rozwojową czy spektrum autyzmu.

Niestety, w ostatnim czasie Internet, smartfony, gry komputerowe i tablety stały się kozłem ofiarnym i często wymieniane są jako czynniki stanowiące zagrożenie dla dzieci i młodzieży.

Ponadto opinię publiczną rozgrzewa temat związany z zakazem używania smartfonów w przestrzeni szkolnej.

Zakaz korzystania ze smartfonów w polskich szkołach jest tematem kontrowersyjnym, z różnymi argumentami zarówno za, jak i przeciw.

**W mojej ocenie drastyczne zakazy nigdy nie przynoszą zamierzonego efektu, zawsze kluczem jest edukacja i równowaga, a w tym kontekście także właściwe wzorce dorosłych i alternatywa do spędzania czasu w świecie offline.**

**Oczywiście, że smartfony mogą być poważnym rozpraszaczem, odciągając i rozpraszając**

**uwagę uczniów od zajęć. Bez dostępu do smartfonów uczniowie mogą skupić się na nauce i interakcji z nauczycielami oraz rówieśnikami. Ograniczenie dostępu do smartfonów może zmniejszyć ryzyko cyberprzemocy i nieodpowiedniego zachowania w internecie podczas lekcji i przerw.**

**Redukcja czasu spędzanego przed ekranem może mieć pozytywny wpływ na zdrowie psychiczne uczniów, zmniejszając stres związany z ciągłym byciem online i porównywaniem się z innymi. Bez smartfonów uczniowie mogą być bardziej skłonni do aktywności fizycznej i interakcji w rzeczywistości, co jest korzystne dla ich zdrowia fizycznego i społecznego.**

## Technologie z pomocą edukacji

Uważam jednak, że mądrze wykorzystywane smartfony mogą być używane jako pomoc dydaktyczna, umożliwiając dostęp do zasobów edukacyjnych, aplikacji do nauki i szybkiego wyszukiwania informacji, rozwijania kompetencji językowych, są też narzędziem do komunikacji alternatywnej dla uczniów, którzy nie komunikują się werbalnie. Smartfony są integralną częścią współczesnego życia młodych ludzi.

Uczniowie muszą nauczyć się, jak odpowiedzialnie korzystać z technologii, a zakaz może ograniczać rozwój tych kluczowych umiejętności.

Wprowadzenie takiego zakazu może być trudne do egzekwowania i może prowadzić do konfliktów



między nauczycielami a uczniami, a także do ukrywania urządzeń, co może potęgować problemy zamiast je rozwiązywać.

Prawidłowo i metodycznie zastosowane technologie mogą znacząco wspierać proces edukacyjno-terapeutyczny. Mogą uatrakcyjnić zajęcia, motywować uczniów do nauki, pomagać w konstruowaniu dostosowań wymagań edukacyjnych, uczyć krytycznego myślenia i wspierać

tworzenie zindywidualizowanych materiałów edukacyjnych.

Nowe technologie oferują dostęp do ogromnych zasobów materiałów i treści dydaktycznych, stanowią platformę dla samorozwoju, współpracy, komunikacji oraz coraz częściej terapii.

Co jest nam zatem potrzebne w obszarze edukacji, aby nowe technologie stały się jej sprzymierzeńcem?

*- Edukacja w zakresie kompetencji cyfrowych  
- umożliwienie dzieciom i młodzieży zdobycia umiejętności efektywnego korzystania z nowych technologii.*

*- Integracja technologii z tradycyjnymi metodami nauczania - wykorzystywanie nowych mediów do uatrakcyjnienia i wzbogacenia procesu edukacyjnego. TIK nie ma zastąpić tradycyjnych, analogowych metod nauczania, a być ich uzupełnieniem.*

*- Promowanie odpowiedzialnego korzystania z technologii - kształtowanie świadomego i odpowiedzialnego podejścia do nowych mediów wśród młodych ludzi. Zwrócenie uwagi na higienę cyfrową i bezpiecznego korzystanie z wirtualnej przestrzeni, ale także na ochronę swoich danych osobowych.*

*- Wsparcie dla rodziców i nauczycieli - zapewnienie szkoleń i warsztatów, ale także opracowanie materiałów, które pomogą dorosłym efektywnie wspierać dzieci w korzystaniu z technologii.*

*- Promowanie właściwych postaw zarówno w świecie offline jak i online, w oparciu o wartości, które są takie same bez względu na to gdzie w danym momencie funkcjonujemy.*

*- Efektywne i etyczne wykorzystywanie AI w edukacji i wskazanie jej możliwości i wyzwań, z którymi przyjdzie nam się mierzyć - w zakresie tworzenia materiałów edukacyjnych, grafik, rozwijania kompetencji językowych czy dostosowanych dla uczniów ze SPE treści. Krytyczne myślenie wobec generowanych za pomocą sztucznej inteligencji ośmieszających i nieprawdziwych treści.*

Takie podejście umożliwi maksymalne wykorzystanie potencjału nowych technologii w edukacji i codziennym życiu, jednocześnie minimalizując ryzyko związane z ich nadużywaniem.

Od nowych technologii nie ma już odwrotu, a polska transformacja cyfrowa w edukacji staje się coraz bardziej istotnym elementem współczesnego systemu nauczania. Z perspektywy nauczyciela, priorytety w tej dziedzinie mogą obejmować kilka kluczowych aspektów:

### **1. Infrastruktura Technologiczna**

Wyposażenie szkół, czyli zapewnienie dostępu do nowoczesnych komputerów, tabletów, projektorów, interaktywnych tablic i stabilnego internetu w każdej placówce.

Platformy edukacyjne poprzez implementację i optymalizację platform e-learningowych, takich jak Moodle, Google Classroom, czy Microsoft Teams, które ułatwiają zdalne nauczanie i interakcję z uczniami.

### **2. Szkolenia i Rozwój Kompetencji Cyfrowych**

Szkolenia dla nauczycieli poprzez organizację regularnych kursów i warsztatów z zakresu metodycznego, a nie odtwórczego i incydentalnego wykorzystania nowych technologii w edukacji. W tym programowania, bezpieczeństwa w sieci, higieny cyfrowej oraz wykorzystania narzędzi e-learningowych.

Wsparcie techniczne poprzez dostęp do specjalistów IT, którzy mogą pomagać nauczycielom

w rozwiązywaniu problemów technicznych i optymalnym wykorzystaniu dostępnych narzędzi TIK.

### **3. Integracja Technologii z Programem Nauczania**

Cyfrowe zasoby edukacyjne poprzez tworzenie i udostępnianie cyfrowych materiałów dydaktycznych, takich jak e-podręczniki, wideo-lekcje, interaktywne ćwiczenia i gry edukacyjne, dostosowane do podstaw programowych.

Personalizacja nauczania w kontekście wykorzystania narzędzi do analizy danych uczniów, co pozwala na indywidualne podejście do każdego ucznia i dostosowanie materiału do jego potrzeb, w tym również uwzględniając AI.

### **4. Bezpieczeństwo i Prywatność**

Ochrona danych poprzez zapewnienie bezpieczeństwa danych uczniów i nauczycieli, w tym ochrona przed cyberatakami i nieautoryzowanym dostępem do ich urządzeń.

Cyberbezpieczeństwo w kontekście edukacji zarówno nauczycieli, jak i uczniów na temat bezpiecznego korzystania z internetu, rozpoznawania zagrożeń i odpowiedniego reagowania na niepokojące incydenty.

### **5. Współpraca i Wymiana Doświadczeń**

Społeczności nauczycielskie poprzez tworzenie platform do wymiany doświadczeń i materiałów między nauczycielami z różnych szkół i instytucji edukacyjnych.

Współpraca międzynarodowa, warto uwzględnić i postawić na udział nauczycieli, specjalistów, terapeutów, ale także uczniów w międzynarodowych projektach edukacyjnych i wymiana praktyk z nauczycielami z innych krajów. Dobrą praktyką w tym obszarze są na przykład programy eTwinning i Erasmus +.

## 6. Motywacja i Zaangażowanie Uczniów

Interaktywne metody nauczania i wykorzystanie gier edukacyjnych, quizów, aplikacji VR/AR (Wirtualna i Rozszerzona Rzeczywistość) do angażowania uczniów i uatrakcyjnienia zajęć.

Feedback i ocena poprzez implementację narzędzi umożliwiających bieżące monitorowanie postępów uczniów i udzielanie szybkiego feedbacku.

## 7. Zrównoważony Rozwój

Ekologiczne podejście i promowanie wykorzystywania technologii w sposób zrównoważony, np. poprzez ograniczanie zużycia papieru do kserowania kart pracy, podręczników, ćwiczeń i dokumentacji na rzecz e-materiałów.

## 8. Sztuczna Inteligencja

Wskazywanie możliwości i wyzwań związanych z rozwojem sztucznej inteligencji i jej etycznego wykorzystywania zarówno przez uczniów jak i nauczycieli.

Wyposażenie nauczycieli i rodziców w wiedzę i konkretne umiejętności wykorzystania AI do tworzenia spersonalizowanych ćwiczeń i zadań,

grafik, ale także treści edukacyjnych.

Transformacja cyfrowa wiąże się także z pewnymi wyzwaniami, które trzeba przezwyciężyć, aby była skuteczna. Należą do nich między innymi:

*- Zróżnicowany poziom kompetencji cyfrowych wśród nauczycieli i uczniów. Nadal występuje znaczne zróżnicowanie w poziomie kompetencji cyfrowych zarówno wśród uczniów, jak i nauczycieli. Często brakuje jednolitego standardu edukacji w tym zakresie. Wielu nauczycieli wymaga dodatkowych szkoleń w zakresie wykorzystania technologii informacyjno-komunikacyjnych (TIK) w nauczaniu.*

*- Nierówności w dostępie do technologii - zwłaszcza w mniejszych miejscowościach i szkołach wiejskich. W wielu szkołach, szczególnie na terenach wiejskich, brakuje odpowiedniej infrastruktury, takiej jak nowoczesne komputery, stabilne łącza internetowe, czy interaktywne tablice. Nie wszyscy uczniowie mają dostęp do własnych urządzeń cyfrowych w domu, co utrudnia realizację zadań domowych wymagających korzystania z internetu.*

*- Opór przed zmianą - potrzeba zmiany mentalności i podejścia do technologii zarówno wśród nauczycieli, jak i uczniów oraz rodziców, a efektywna transformacja cyfrowa wymaga zaangażowania wszystkich zainteresowanych stron: nauczycieli, uczniów, rodziców, administracji szkolnej oraz decydentów na szczeblu krajowym. Odpowiednie wsparcie, szkolenia i infrastruktura mogą przyczynić się do znaczącej poprawy jakości edukacji i przygotowania uczniów do przyszłości w coraz*

bardziej zdigitalizowanym świecie.

- *Brak dostosowanych materiałów. Mimo coraz lepiej funkcjonującej Zintegrowanej Platformy Edukacyjnej, takich platform jak Learning Apps, Canva, Wakelet, Khan Academy, Pistacja TV, Matemaks.pl, Geogebra to nadal występuje niedobór cyfrowych zasobów edukacyjnych, które są dostosowane do podstaw programowych, w szczególności na poziomie szkoły ponadpodstawowej i w nauczaniu przedmiotów zawodowych. Dostępne materiały często są fragmentaryczne i nierównomiernie rozłożone pomiędzy przedmiotami.*

- *Świadomość zagrożeń. Uczniowie często nie są odpowiednio edukowani na temat bezpieczeństwa w sieci i higieny cyfrowej, co naraża ich na różne zagrożenia, takie jak cyberprzemoc czy oszustwa internetowe. Mimo dość dużej oferty bezpłatnych programów w zakresie bezpiecznego funkcjonowania w sieci, jeszcze nie wszystkie szkoły, w tym dyrektorzy i nauczyciele widzą potrzebę zaangażowania swoich uczniów w ich realizację.*

- *Osoby z specjalnymi potrzebami edukacyjnymi (SPE), zwłaszcza te z niepełnosprawnością intelektualną, są szczególnie narażone na wykluczenie cyfrowe. Liczne badania wskazują, że w porównaniu z ich pełnosprawnymi rówieśnikami, osoby z niepełnosprawnościami, szczególnie intelektualnymi, korzystają z internetu rzadziej. <https://bia4all.eu/pl/> Często robią to w sposób bezrefleksyjny i głównie w celach rozrywkowych, ponieważ*

*nikt wcześniej nie pokazał im jego praktycznych zastosowań ani nie nauczył, jak z niego efektywnie korzystać.*

## **Jak można poprawić jakość cyfrowej edukacji i metodyczne wykorzystanie TIK w edukacji?**

Na pewno poprzez inwestycje w technologie. Rząd powinien kontynuować i zwiększać inwestycje w infrastrukturę cyfrową, zwłaszcza w szkołach na terenach wiejskich i szkołach ponadpodstawowych, ponieważ nie korzystały one z programu Laboratoria Przyszłości.

Programy wsparcia dla uczniów, poprzez wprowadzenie programów zapewniających dostęp do sprzętu komputerowego dla uczniów z rodzin o niższych dochodach.

Nadal niezbędne są profesjonalne i metodyczne szkolenia dla nauczycieli. Regularne i obowiązkowe szkolenia z zakresu TIK, obejmujące nowe narzędzia, metodyki i dobre praktyki. Warto też rozwijanie tych kompetencji uwzględnić w programie kształcenia studentów pedagogiki.

Zasadne wydaje się rozszerzenie treści dotyczących edukacji medialnej dla uczniów.

Mogłaby ona polegać na wszechstronnym przygotowaniu ich do świadomego, krytycznego i odpowiedzialnego korzystania z mediów. Kilka kluczowych elementów, które mogłyby wchodzić w skład takiej edukacji:

- *Krytyczne myślenie poprzez uczenie uczniów, jak*

*analizować i oceniać informacje, które spotykają w mediach. W tym kontekście istotne jest rozwijanie umiejętności rozpoznawania dezinformacji, fałszywych wiadomości oraz manipulacji.*

*Tego typu treści realizują już niektóre programy prowadzone i wdrażane przez NGOsy i instytucje edukacyjne. Do najciekawszych programów zaliczyć można:*

*Asy Internetu*

*MegaMisja*

*Cyfrowe Drogowskazy- Stacja Galaxy*

*Edu 360*

*Be. Net*

*- Bezpieczeństwo online, czyli edukacja na temat ochrony prywatności, zarządzania danymi osobowymi oraz rozpoznawania zagrożeń w sieci, takich jak cyberprzemoc, phishing czy nieodpowiednie treści.*

*- Odpowiedzialne korzystanie z mediów społecznościowych w zakresie rozumienia zasad etykiety w sieci, wpływu mediów społecznościowych na zdrowie psychiczne oraz konsekwencji publikowania treści online.*

Warto nadal inwestować w rozwój e-podręczników i stworzenie wysokiej jakości, kompleksowych e-podręczników dostosowanych do programów nauczania na każdym etapie edukacyjnym i w każdym typie szkoły. Ponadto kontynuować udoskonalanie i promowanie platform

e-learningowych, które umożliwiają łatwy dostęp do materiałów dydaktycznych.

Nie bez znaczenia jest rozwijanie i kontynuowanie edukacji w zakresie bezpieczeństwa cyfrowego i inicjowania kampanii, które edukują uczniów na temat higieny cyfrowej, cyfrowego obywatelstwa, zagrożeń w sieci oraz sposobów ich unikania.

Wsparcie psychologiczne uczniów w obszarze cyfrowej transformacji jest kluczowe, aby pomóc im w radzeniu sobie z wyzwaniami związanymi z intensywnym korzystaniem z technologii, hejtem w sieci, przemocą psychiczną czy nękaniami. Jakiego działania warto podjąć w tym zakresie?

*- Skuteczne okazać się mogą programy profilaktyczne, realizowane w formie warsztatów i zajęć na temat zdrowia psychicznego, radzenia sobie ze stresem, lękiem i presją związaną z korzystaniem z technologii.*

*- Radzeniem sobie z sytuacjami niepożądanymi poprzez informowanie o nich dorosłych i właściwe instytucje.*

Ważnym elementem edukacji jest stałe informowanie uczniów o potencjalnych zagrożeniach związanych z nadmiernym korzystaniem z mediów cyfrowych, takich jak uzależnienia, cyberprzemoc czy izolacja społeczna. Na pewno pomocne okazać się może zapewnienie łatwego dostępu do specjalistów, którzy mogą udzielać wsparcia psychologicznego uczniom, zarówno indywidualnie, jak i w grupach, a ponadto

promowanie linii wsparcia telefonicznego i on-line dla uczniów, którzy potrzebują porady lub wsparcia w sytuacjach kryzysowych.

Warto częściej organizować i zachęcać uczniów do udziału w zajęciach rozwijających umiejętności społeczne, które w możliwe są do realizacji w ramach pomocy psychologiczno- pedagogicznej. Sprawdzą się w tym obszarze na przykład zajęcia, które uczą umiejętności komunikacji, współpracy i rozwiązywania konfliktów. Ponadto promowanie aktywności grupowych, które sprzyjają budowaniu relacji między uczniami i wzmacniają poczucie wspólnoty. Zawsze skuteczne jest promowanie aktywności fizycznych. Zachęcanie uczniów do udziału w zajęciach sportowych, spacerach, grach terenowych i innych formach aktywności fizycznej na świeżym powietrzu. Wiele szkół wprowadza dni bez technologii, podczas których uczniowie skupiają się na aktywnościach offline i interakcjach z przyjaciółmi.

Jestem zwolenniczką wprowadzenia programów mentoringowych, w których starsi uczniowie pomagają młodszym w radzeniu sobie z wyzwaniami związanymi z technologią.

Warto także tworzyć grupy, w których uczniowie mogą dzielić się swoimi doświadczeniami i wspólnie szukać rozwiązań problemów.

Podjęcie tych działań pomoże w stworzeniu środowiska, w którym uczniowie będą mogli bezpiecznie i świadomie korzystać z technologii, jednocześnie dbając o swoje zdrowie psychiczne i rozwój społeczny.

Nadal istnieje potrzeba tworzenia sieci współpracy między nauczycielami, które umożliwiają wymianę doświadczeń i dobrych praktyk w zakresie wykorzystania TIK. Dobrą praktyką takiej współpracy mogą być na przykład projekty edukacyjne.

Nie bez znaczenia są tutaj odpowiednie ośrodki doskonalenia nauczycieli, które współpracują z odpowiednią kadrą i trenerami, którzy posiadają wieloletnie doświadczenie i praktykę w obszarze cyfryzacji i bezpieczeństwa w sieci.

Realizacja tych rekomendacji wymaga współpracy pomiędzy rządem, samorządami, szkołami oraz społecznością lokalną. Wprowadzenie kompleksowej strategii transformacji cyfrowej w edukacji może znacząco podnieść jakość kształcenia i przygotować uczniów na wyzwania współczesnego, cyfrowego świata.

Zgodnie z puentą książki "Jak nie zgubić dziecka w sieci", której jestem współautorką " Nie pozwólmy dzieciom zagubić się w sieci, pomóżmy im się w niej odnaleźć".

Źródła:

- <https://bia4all.eu/pl/toolkit/>



**ZYTA CZECHOWSKA**

NAUCZYCIEL ROKU 2019,  
DYREKTOR NIEPUBLICZNEGO  
OŚRODKA DOSKONALENIA  
NAUCZYCIELI





# Cyberbezpieczeństwo dla obywateli

---

## **Cyberbezpieczeństwo dla obywateli: klucz do bezpiecznej przyszłości cyfrowej Polski**

Arkadiusz Lefanowicz

## **Certyfikacja to filar cyberbezpieczeństwa**

Aleksandra Kostrzewa

## **Predykcje kierunków rozwoju Cyberbezpieczeństwa 2024**

Grzegorz Łatosiński

## **Cyberbezpieczeństwo najwyższej klasy dostępne dla administracji publicznej jako usługa szansa i wyzwanie**

Ewa Sztyber



# Cyberbezpieczeństwo dla obywateli: klucz do bezpiecznej przyszłości cyfrowej Polski

**W erze cyfrowej, gdzie nasze życie codzienne w coraz większym stopniu przenosi się do przestrzeni wirtualnej, cyberbezpieczeństwo staje się fundamentem, na którym budowana jest zaufana i bezpieczna przyszłość każdego obywatela. Polska, podążając ścieżką transformacji cyfrowej w ramach inicjatywy Polska 5.0, stoi przed wyzwaniem nie tylko technologicznej modernizacji, ale również zapewnienia cyberbezpieczeństwa, które chroniłoby każdego obywatela przed rosnącymi zagrożeniami cyfrowymi.**

## Diagnoza obecnej sytuacji

W ostatnich latach obserwujemy znaczący wzrost cyberataków, które dotyczą zarówno indywidualnych obywateli, jak i instytucje publiczne. Od phishingu, przez malware, po ataki na urządzenia mobilne – zagrożenia są wszechobecne i ewoluują. Pandemia COVID-19 jeszcze bardziej uwypukliła potrzebę solidnego fundamentu

cyberbezpieczeństwa, gdyż przyspieszony transfer aktywności do sieci ujawnił nowe luki i wyzwania bezpieczeństwa.

## Mocne i słabe strony

Polska zdołała osiągnąć pewne sukcesy w dziedzinie cyberbezpieczeństwa, realizując kampanie edukacyjne i zwiększając współpracę międzynarodową. Jednak nadal istnieją znaczące luki, szczególnie w świadomości społecznej i dostępności edukacji, co stanowi słaby punkt w naszej krajowej obronie przed cyberzagrożeniami.

## Wyzwania

Stojące przed nami wyzwania są wielowymiarowe. Ewolucja zagrożeń wymaga ciągłej aktualizacji i adaptacji strategii bezpieczeństwa. Internet Rzeczy (IoT) znacząco rozszerza powierzchnię ataku, a zwiększona cyfryzacja życia codziennego wymaga od nas znalezienia równowagi między bezpieczeństwem a prywatnością.



## Rekomendacje

*1. Edukacja i świadomość: Niezbędne jest wprowadzenie szeroko zakrojonych programów edukacyjnych, które podniosą świadomość cyfrową wśród Polaków. Edukacja powinna obejmować nie tylko młodzież, ale i osoby starsze, dla których cyberzagrożenia mogą być szczególnie obce.*

*2. Dostęp do narzędzi: Kluczowe jest, aby każdy obywatel miał łatwy dostęp do skutecznych i prostych w obsłudze narzędzi cyberbezpieczeństwa. Współpraca z sektorem prywatnym może tutaj odegrać kluczową rolę w dostarczaniu rozwiązań dostosowanych do różnych potrzeb użytkowników.*

*3. Wzmocnienie infrastruktury: Inwestycje w nowoczesne technologie i infrastrukturę są niezbędne, aby zapewnić wysoki poziom bezpieczeństwa danych i usług cyfrowych.*

*4. Współpraca międzysektorowa: Współpraca pomiędzy rządem, sektorem prywatnym i organizacjami pozarządowymi jest kluczowa dla wymiany wiedzy i najlepszych praktyk w dziedzinie cyberbezpieczeństwa.*

*5. Zabezpieczenie danych: Ochrona danych osobowych wymaga surowszych regulacji i zachęcania do stosowania najlepszych praktyk w zakresie bezpieczeństwa informacji.*

## Zakończenie

Cyberbezpieczeństwo nie jest wyłącznie problemem technicznym, ale fundamentalnym elementem budowania zaufanej i bezpiecznej przyszłości cyfrowej dla wszystkich obywateli Polski. Wyzwania, przed którymi stoją zarówno jednostki, jak i całe społeczeństwo, wymagają zintegrowanego podejścia, w którym edukacja, dostęp do narzędzi oraz współpraca międzysektorowa odgrywają kluczowe role. Podejmując proaktywne działania w zakresie cyberbezpieczeństwa, możemy nie tylko chronić się przed istniejącymi zagrożeniami, ale również budować podstawy dla bezpiecznej przyszłości cyfrowej, w której każdy obywatel czuje się chroniony i jest świadomy zagrożeń.

## Dodatkowe elementy

Inspirując się najlepszymi praktykami z innych krajów, Polska może przyjąć innowacyjne rozwiązania, które już udowodniły swoją skuteczność w poprawie cyberbezpieczeństwa. Na przykład, model skandynawski kładzie duży nacisk na edukację cyfrową już od najmłodszych lat, jednocześnie promując transparentność i współpracę między rządem a sektorem prywatnym. Z kolei Singapur wdrożył krajowy program cyberbezpieczeństwa, który łączy surowe regulacje z intensywnymi inwestycjami w nowoczesne technologie.

Wskazówki dla indywidualnych obywateli, takie jak regularne aktualizacje oprogramowania, korzystanie z silnych haseł i dwuetapowej

weryfikacji, czy świadomość w zakresie phishingu i oszustw internetowych, mogą znacząco zwiększyć ich bezpieczeństwo online. Edukacja na temat tych prostych, ale skutecznych praktyk powinna stać się standardem, dostępnym dla każdego Polaka.

Wzmacniając cyberbezpieczeństwo, Polska stawia krok ku przyszłości, w której technologia służy wszystkim obywatelom, zapewniając im bezpieczeństwo, prywatność i dostęp do innowacyjnych usług cyfrowych. To właśnie cyberbezpieczeństwo jest kluczem do otwarcia pełnego potencjału Polski 5.0, umożliwiając rozwój społeczeństwa w pełni korzystającego z korzyści płynących

z cyfryzacji, przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa i zaufania.

Polska, stawiając na edukację, współpracę i innowacje, może stać się modelowym przykładem dla innych krajów, demonstrując, jak skutecznie integrować cyberbezpieczeństwo z codziennym życiem obywateli i transformacją cyfrową.



**ARKADIUSZ  
LEFANOWICZ**

PRZEWODNICZĄCY RADY  
FUNDACJI - FUNDACJA IT LEADER  
CLUB POLSKA



# Certyfikacja to filar cyberbezpieczeństwa

**W obecnych czasach, kiedy informacja równa się potężde, a dane są traktowane jak nowoczesna waluta, ochrona środowiska IT i poufnych danych stała się priorytetem dla każdej firmy.**

## Cyberbezpieczeństwo to klucz do bezpiecznego biznesu

Niezależnie od wielkości przedsiębiorstwa, audyty bezpieczeństwa IT odgrywają kluczową rolę w identyfikowaniu słabych punktów systemu, które mogą stać się potencjalnymi wejściami dla cyberataków. Regularne przeglądy i oceny nie tylko pomagają w utrzymaniu bezpieczeństwa na najwyższym poziomie, ale także budują zaufanie wśród klientów i partnerów biznesowych, świadcząc o odpowiedzialnym podejściu do zarządzania danymi. Certyfikat to ważny element tego zaufania. Certyfikacja to filar cyberbezpieczeństwa, dlatego tak ważne jest szukanie solidnych partnerów, którzy w certyfikacji nie idą na skróty.



## Biznes na ścieżce jakości

Projakościowe podejście w zarządzaniu, w biznesie procentuje. Potwierdzają to rynkowe doświadczenia. Nie warto iść na skróty, a zdecydowanie lepiej jest podjąć wysiłek rzetelnej certyfikacji.

*PCBC S.A. od lat stawia bardzo wysoko poprzeczkę nie tylko certyfikowanym podmiotom, ale i naszej organizacji. Jesteśmy rzetelną firmą z 65-letnim doświadczeniem i nie oferujemy szybkich ścieżek ani uproszczonych procedur. Naszą reputację i obiektywizm najlepiej potwierdza fakt naszego członkostwa w międzynarodowej organizacji IQNET. Jest to prestiżowa organizacja, działająca w 135 krajach, skupiająca wiodące firmy z branży certyfikacji z 35 krajów. Polskie Centrum Badań i Certyfikacji S.A. reprezentuje Polskę jako członek rzeczywisty IQNET od 1997 roku i nie jest to członkostwo honorowe: wiąże się ono ze stałym nadzorem nad jakością naszej pracy i regularnymi audytami. Posiadamy też akredytacje Polskiego Centrum Akredytacji (PCA), które potwierdzają zgodność naszych kompetencji w odniesieniu do zakresu zadań, jakie możemy wykonywać w obszarach: certyfikacji systemów zarządzania, certyfikacji wyrobów i badań laboratoryjnych. Intensywnie pracujemy nad doskonaleniem naszych kompetencji, czujemy dużą odpowiedzialność za naszą misję i cieszymy się z upowszechniania wysokich standardów w audytowanych firmach.*

Sam proces audytu może być dla firmy bardzo istotnym etapem w podnoszeniu jakości, kompetencji i bezpieczeństwa. Są też twarde dane i analizy, które potwierdzają, że **wymagający proces certyfikacji, zrealizowany przez kompetentny zespół jednostki certyfikującej wiąże się z dużo większymi korzyściami dla firm**. Do takiego wniosku doszli autorzy raportu *“Exploring Business Benefits of Internationally Recognized Certifications - Empirical Evidence from a Global Company Survey”*, którzy przeanalizowali dane z badań przeprowadzonych wśród 3 500 firm z 40 krajów przez International Accreditation Forum IAF (Mangelsdorf Axel, Denkler, Tilman, Exploring Business Benefits of Internationally Recognized Certifications - Empirical Evidence from a Global Company Survey, 2013).

## Codzienne bezpieczeństwo w sferze cyfrowej

Nasi eksperci uważają, że pierwszym krokiem na ścieżce stałego zapewniania bezpieczeństwa firmy w cyfrowym świecie są przede wszystkim stałe szkolenia dla kadry zarządzającej oraz pracowników. Duży nacisk kładziemy zatem na rozwój szkoleń, które są jednym z filarów budowania odporności na cyberzagrożenia dla jednostek oraz organizacji. Dzięki nim można lepiej zrozumieć i zarządzać rynkiem związanym z cyberbezpieczeństwem oraz skuteczniej chronić swoje zasoby i dane.

Kolejny lub równoległy krok, to wybór ścieżki certyfikacji/audytu, który zależy od specyficznych potrzeb i celów firmy, jej branży oraz rodzaju wyrobów czy oferowanych usług, a także danych, jakimi zarządza. Oczywiście warto rozważyć zaplanowanie konsultacji z ekspertami ds. bezpieczeństwa informatycznego. Bez wątpienia w wymiarze związanym z cyberbezpieczeństwem **pierwsza norma ISO, po którą nowoczesna firma może, a nawet powinna sięgnąć, aby należycie zadbać o swoje bezpieczeństwo w tej sferze, to norma ISO/IEC 27001 System Zarządzania Bezpieczeństwem Informacji**. System ten skupia się na zachowaniu poufności, integralności i dostępności posiadanych informacji. ISO/IEC 27001 definiuje standardy i wymagania dla tworzenia, wdrażania, utrzymywania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji i jest bardzo ważnym krokiem w kierunku zwiększenia bezpieczeństwa cyfrowego w firmie. Wiele wyjaśnia sama nazwa aktualnej normy, opisującej ten system: „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności”. Nazwa jest spójna z tym, co na co dzień dzieje w naszym otoczeniu, gdzie coraz więcej osób i firm rozumie, jak cennym zasobem są informacje i jak ważna jest ochrona informacji i naszej prywatności przed cyberatakami i dostępem osób nieuprawnionych.

Posiadanie certyfikatu ISO/IEC 27001 oznacza, że firma po wdrożeniu systemu powiedziała: „sprawdzam!” i pozwoliła, by niezależna

jednostka oceniła czy wdrożenie było skuteczne i czy wymagania normy są spełnione. Certyfikat potwierdza zatem, że firma ustanowiła zabezpieczenia, identyfikuje zagrożenia i zmniejsza ich wpływ na działalność organizacji, ustanowiła cele i zasady bezpieczeństwa informacji, ale również że stale podnosi świadomość pracowników. Firma z certyfikatem ISO/IEC 27001 komunikuje za jego pośrednictwem, że podchodzi do tych zagadnień systemowo, spełnia wymagania prawne oraz jest wiarygodnym parterem w biznesie. W dużej mierze to rodzaj takiej gwarancji, o ile inne czynniki nie zawiodą. Szczególnie czynnik ludzki, który bywa, niestety, zawodny – czasem przez brak wiedzy, czasem przez nieostrożność. I o tym należy nieustannie przypominać.

Również postępująca informatyzacja niesie za sobą zagrożenia związane z bezpieczeństwem informacji. Zagrożenia te można scharakteryzować za pomocą trzech podstawowych składowych bezpieczeństwa informacji, jakimi są: utrata poufności, ograniczenie dostępności i naruszenie integralności informacji. Mogą one mieć charakter zdarzeń przypadkowych (awarie, błędy oprogramowania i pomyłki ludzkie), mogą być powodowane przez czynniki naturalne jak pożar, powódź czy piorun, a mogą być także wynikiem celowych działań ludzi.



Zapewnienie skutecznego i spójnego podejścia do zarządzania ochroną danych i infrastrukturą cyfrową, stwarza realne szanse zarządzania ryzykiem w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych.

Wykorzystanie usług w chmurze w zakresie przestrzeni dyskowej, mocy obliczeniowej, czy oprogramowania wzrasta. Jednak rozwiązania chmurowe to nie tylko usprawnienia ale też zagrożenia, takie jak np. nieuprawniony dostęp do informacji i danych osobowych, który może skutkować ich utratą lub naruszeniem integralności. Certyfikacja w oparciu o wymagania norm ISO/IEC 27017 i ISO/IEC 27018 jest dostosowana do specyficznych wymagań dostawców usług w chmurze.

Warto zwrócić uwagę na aspekt, o którym niewiele się mówi, a ma on ogromne znaczenie dla stałego podnoszenia wartości firmy. Ogromną korzyścią dla przedsiębiorstwa jest również sam proces certyfikacji, który wymaga od firmy wdrożenia rygorystycznych praktyk i procedur, związanych z bezpieczeństwem informacji. Firma musi dokumentować i wdrażać konkretne praktyki i procedury związane z bezpieczeństwem informacji. A to z kolei pomaga identyfikowaniu i likwidacji luk oraz usprawnieniu działań związanych z cyberbezpieczeństwem. To rodzaj dobrze poprowadzonego treningu, który pomaga skorygować błędy i dobrze się przygotować do meczu.

**Regularne audyty pomagają w utrzymaniu zgodności z międzynarodowymi standardami i regulacjami, co jest szczególnie ważne w kontekście rosnących wymagań prawnych, takich jak np. Rozporządzenie 2016/679 (RODO) i akty towarzyszące.** Wdrażając regularne audyty bezpieczeństwa IT, firmy nie tylko minimalizują ryzyko cyberataków i wycieków danych, ale także demonstrują swoje zaangażowanie w ochronę informacji, co jest nieocenione w budowaniu trwałych relacji biznesowych. W obliczu coraz bardziej zaawansowanych zagrożeń cyfrowych, inwestycja w audyty bezpieczeństwa IT jest inwestycją w przyszłość firmy, zapewniając jej stabilność, bezpieczeństwo i ciągłość działania w dynamicznie zmieniającym się świecie technologii, poprzez znaczące obniżenie ryzyka wystąpienia incydentów bezpieczeństwa i związanych z nim strat.

## Bezpieczeństwo cyfrowe - DNA organizacji

Praca nad zapewnieniem cyberbezpieczeństwa w organizacji nigdy się nie kończy i niezbędne jest tu planowanie długoterminowe. Firmy powinny stosować podejście wielowarstwowe do bezpieczeństwa cyfrowego, uwzględniając zarówno procesy, technologie, edukację pracowników, monitoring i reakcję na incydenty, aby zwiększyć swoją zdolność do obrony przed atakami cyfrowymi. Powinny również szkolić, regularnie przeprowadzać audyty i testy penetracyjne, aby ocenić skuteczność zabezpieczeń. Certyfikat ISO/IEC 27001, ale też certyfikat ISO

22301, czyli międzynarodowa norma dotycząca zarządzania ciągłością działania firmy, gdzie identyfikacja i zapobieganie ryzykom związanym z bezpieczeństwem cyfrowym stanowią istotny element, opierają się na sprawdzaniu procedur i dokumentów, ale też na rozmowach z pracownikami i obserwacji procesów. Dzięki temu są one bardzo dobrym i potrzebnym punktem wyjścia w budowaniu bezpieczeństwa firmy, ale nie mogą być jedynym środkiem zabezpieczającym.

**Bezpieczeństwo w cyfrowym świecie, podobnie jak każdy inny wymiar bezpieczeństwa, to jednak przede wszystkim ludzie, stan ich wiedzy na temat zagrożeń w sieci i wzajemne zaufanie.** W PCBC mamy ekspercki zespół złożony z profesjonalistów o kilkunastoletnim doświadczeniu zawodowym w branży cyberbezpieczeństwa. Mamy także ogromne doświadczenie w certyfikacji i audycie w ramach szeregu standardów, co sprawia, że jesteśmy wszechstronnie przygotowani do sprostania różnorodnym wyzwaniom w dziedzinie audytu. Jako podmiot, należący do Skarbu Państwa, gwarantujemy także najwyższy poziom wiarygodności i przekonania, że nasi audytorzy są obiektywni, niezależni, ale również wiarygodni, co nie jest bez znaczenia zwłaszcza w sytuacji, gdy podczas audytu cyberbezpieczeństwa trzeba udostępnić firmową sieć obcemu człowiekowi.



**ALEKSANDRA  
KOSTRZEWA**

PREZES ZARZĄDU POLSKIEGO  
CENTRUM BADAŃ  
I CERTYFIKACJI S.A.





# Predykcje kierunków rozwoju Cyberbezpieczeństwa 2025

W roku 2024, kwestie związane z cyberbezpieczeństwem stały się nie tylko priorytetem dla instytucji rządowych i korporacji, ale także dla zwykłych użytkowników internetu. W miarę postępu technologicznego i coraz większej cyfryzacji społeczeństwa, zagrożenia związane z bezpieczeństwem cyfrowym ewoluują, stając się coraz bardziej złożone. Cyberprzestępcy stale doskonalą swoje techniki, wykorzystując najnowsze osiągnięcia technologiczne do atakowania systemów informatycznych, infrastruktury krytycznej oraz prywatnych danych użytkowników.

Analizując najnowsze trendy, wyzwania i innowacje w tej dziedzinie. Wśród kierunków rozwoju znajdują się m.in. rozwój sztucznej inteligencji nowej generacji, rozbudowa regulacji dotyczących ochrony danych osobowych oraz strategie zapobiegania atakom z wykorzystaniem nowych technologii, takich jak komputery kwantowe. Ponadto, przyjrzymy się również rosnącej roli i odpowiedzialności zarządów w dziedzinie

kierowania rozwojem cyberbezpieczeństwa w organizacji.

W obliczu ciągłego rozwoju technologicznego i zwiększającej się roli cyfryzacji, wdrażanie skutecznych strategii cyberbezpieczeństwa staje się nieodłącznym elementem ochrony społeczeństwa oraz gospodarki przed coraz bardziej zaawansowanymi zagrożeniami cyfrowymi. Co nas czeka?

## Sztuczna Inteligencja (AI) zamienia "Plac Zabaw" dla szefów bezpieczeństwa informacji (CISO) w "Pole Minowe"

Działy biznesu i informatyki znajdują się w kłopotach z identyfikacją prawdziwych właścicieli obszaru sztucznej inteligencji (AI). Tymczasem, najlepsze praktyki z zakresu cyberbezpieczeństwa związane z AI są w tyle, a atakujący wykorzystują nowoczesne narzędzia typu LLMs (Large Language Models) oraz GenAI (Generic Artificial Intelligence), aby znacząco zwiększyć skuteczność wysyłanych np: spear phishingowych e-maili, łącząc je z technologią "deep fake" oraz innymi atakami opartymi na AI na przykład, aby zwiększyć wskaźniki tzw. "kliknięć".

Szefowie bezpieczeństwa informacji (CISO) muszą skoncentrować się na ułatwianiu i komunikowaniu ryzyka związanego z projektami wykorzystującymi sztuczną inteligencję w biznesie. Priorytetem powinny być projekty wspierające najcenniejsze zdolności oraz te, które mają

największy wpływ biznesowy na cyberbezpieczeństwo. CISO będą musieli wykorzystać także platformy zintegrowane z AI w celu zmniejszenia złożoności i zwiększenia skuteczności środków bezpieczeństwa, jednocześnie ucząc się od swoich kolegów najlepszych praktyk związanych z AI i cyberbezpieczeństwem.

## Generatywna forma AI zmienia cyberbezpieczeństwo w narzędzie ułatwiające pracę

Wraz z dojrzewaniem w 2024 roku modeli Generatywnych AI (sztuczna inteligencja potrafiąca generować różnego rodzaju obrazy, teksty, filmy i inne media) nastąpi wzrost produktywności operacji cyberbezpieczeństwa w zespołach szybkiego reagowania (SOC). To istotnie zmienia podejście z reaktywnego na proaktywne, kładąc znaczny nacisk na budowanie platform wczesnego wykrywania i ostrzegania o zagrożeniach opartych na AI. Większe skupienie na programach tzw. "polowania na zagrożenia" zapewnia lepszą widoczność powierzchni ataku jeszcze przed rozpoczęciem projektów opartych na technologii w procesach cyfryzacji.

Patrząc z tego punktu widzenia rola Szefa Bezpieczeństwa Informacji (ISO) ewoluuje w kierunku Szefa Bezpieczeństwa AI (CASIO), wykorzystując modele AI do pomocy w proaktywnym przewidywaniu zagrożeń za pomocą systemów działających w czasie rzeczywistym i w dużej mierze autonomicznych. Ponadto mają

oni unikalną okazję, aby zgromadzić liderów biznesu i wykorzystać cyberbezpieczeństwo jako kluczową podstawę do budowania projektów cyfrowych wykorzystujących AI. Pozwoli to także do definiowania tzw. metryk, które można śledzić, takich jak rozwiązywanie incydentów oraz ochrona AI przed zainfekowaniem lub degradacją danych.

## Konsolidacja bez Platformizacji jest zawodna

Jako jedno z głównych priorytetów biznesowych na rok 2024, konsolidacja cyberbezpieczeństwa obiecuje zmniejszenie kosztów i złożoności produktów oraz rozwiązań, ale niekoniecznie zwiększoną skuteczność cybernetyczną. Firmy odkryją, że konsolidacja nie równa się platformizacji, a projekty, które skupiają się na oszczędnościach kosztów bez uwzględnienia optymalizacji i lepszych wyników w zakresie cyberochrony, są skazane na porażkę.

Zespoły ds. bezpieczeństwa muszą dostarczać rozwiązania oparte na modularnej platformie jako element wyróżniający dla biznesu, znacząco redukując liczbę dostawców z ponad 30 do 2-3 zaufanych partnerów cyberochrony działających w ramach ekosystemu. Platformy bezpieczeństwa powinny koncentrować się na wynikach w czasie rzeczywistym i być w dużej części autonomiczne. Firmy powinny korzystać z innowacyjnych partnerów cybernetycznych, którzy mogą pomóc w konsolidacji, ale także poprawić wyniki

w zakresie cyberbezpieczeństwa, bardzo ważnym elementem jest ich prostota i łatwa integracja.

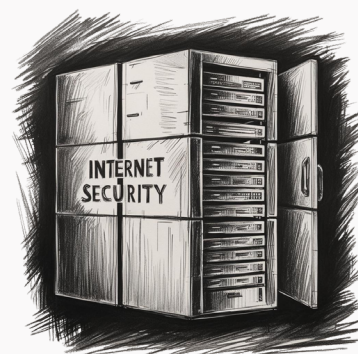
## Management przyłączają się do zarządzania cyberbezpieczeństwem w organizacji

Nowe przepisy, takie jak NIS2, wymagają większej odpowiedzialności członków zarządu w zakresie cyberbezpieczeństwa. W rezultacie organizacje będą dodawać więcej ekspertów lub byłych CISO do swoich zarządów i tworzyć dedykowane komitety ds. cyberbezpieczeństwa, aby przeciwdziałać rosnącej kontroli ze strony regulatorów. Ich gotowość do podnoszenia własnej wiedzy z zakresu cyberbezpieczeństwa będzie kluczowym czynnikiem decydującym o zaufaniu między Szefami Bezpieczeństwa Informacji a Zarządem.

Kluczowe będzie tu ustalenie ram zarządzania odpornością cybernetyczną, sponsorowane przez zarząd. Świadczenie usług doradczych dla zarządu oraz przeprowadzenie ćwiczeń przy tzw. "stole". Ustawienie regularnych corocznych spotkań informacyjnych dla zarządu i uwzględnienie partnerów ekosystemowych (np. strategicznych dostawców, klientów i/lub dostawców).

**Organizacje będą ponownie rozważać cyberbezpieczeństwo aplikacji, aby budować bezpieczeństwo już w trybie jej tworzenia**

Zastosowanie Generatywnej Sztucznej Inteligencji (GenAI) w inżynierii oprogramowania, na przykład poprzez narzędzia powszechnie używane takie jak Github czy CoPilot, stwarza ryzyko wzrostu liczby błędów w dynamicznie rozwijającym się oprogramowaniu oraz przyspieszenia ataków na te aplikacje, jak np. za pomocą przyspieszonego testowania metodą fuzzing. W połączeniu z rosnącym zagrożeniem ataków na łańcuchy dostaw, jak miało to miejsce w przypadku incydentów SolarWinds czy Codecov, oraz z wybuchowym wzrostem wykorzystania oprogramowania open source, przynajmniej 30% firm będzie stawiać na pierwszym miejscu Cyberbezpieczeństwo Aplikacji jako jedno z trzech kluczowych ryzyk cybernetycznych w roku 2024.



Firmy powinny ocenić swoje stanowisko w zakresie bezpieczeństwa aplikacji na każdym poziomie (wewnętrznego wytwórstwa oprogramowania, oprogramowania dostawców, oprogramowania ekosystemu wokół klienta) oraz opracować plan wdrożenia bezpieczeństwa w na etapie przygotowania aplikacji. Należy opracować strategię cyberbezpieczeństwa zgodnie z tzw. doświadczeniem dewelopera (DevEx), co

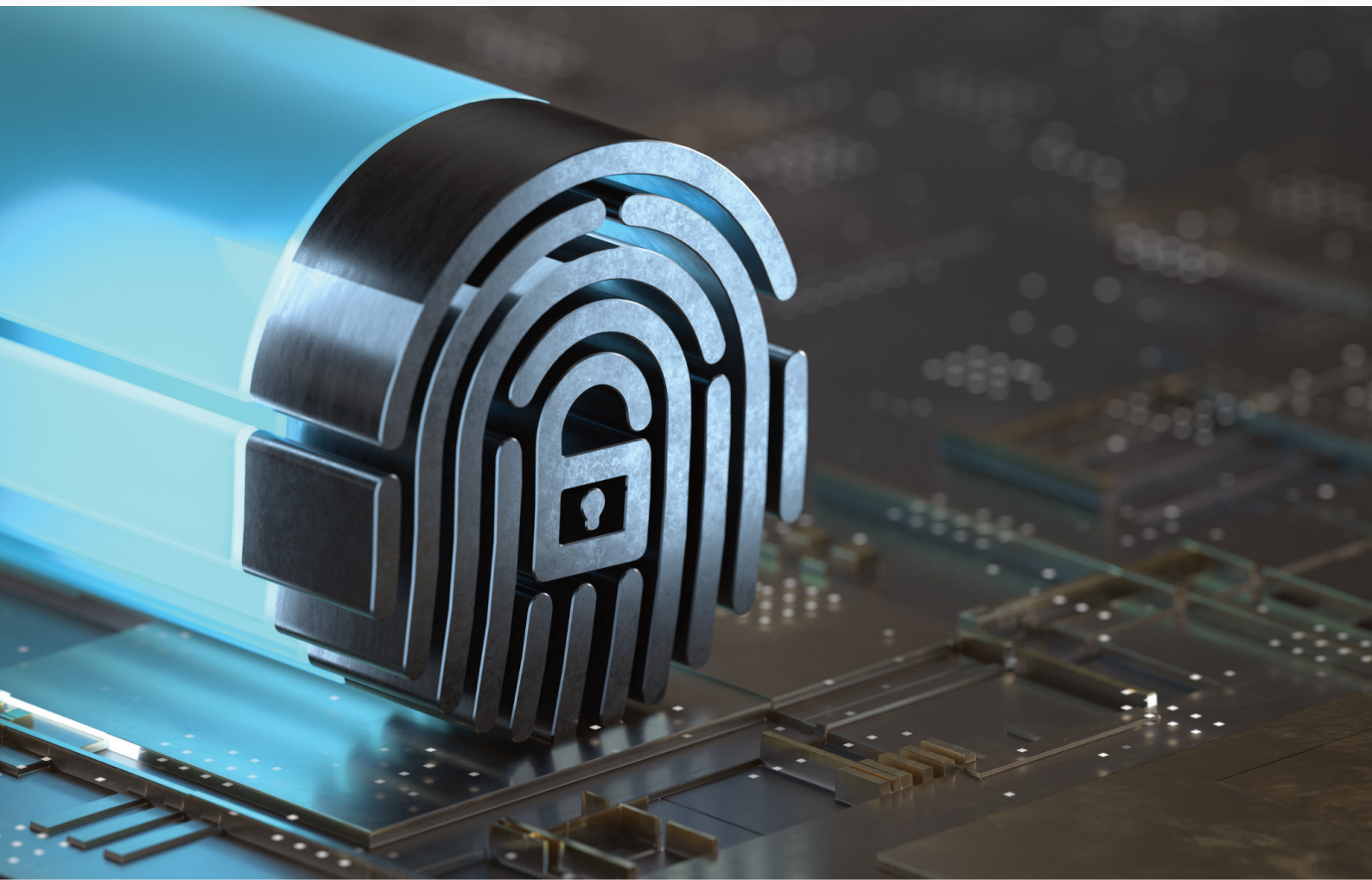
obejmuje integrację bez konfliktów w ekosystemie deweloperów oprogramowania, zachowanie kontekstu między kodem, budowaniem a uruchamianiem, wdrożenie tzw. kontroli jako kod oraz wykorzystanie wysokiej automatyzacji, korzystając z narzędzi bezpieczeństwa tzw. infrastruktury jako kod.

### **Organizacje rozpoczynają ocenę swojej infrastruktury pod kątem gotowości na erę Quantum Computers (Komputerów Kwantowych).**

Przynajmniej 50% firm w kluczowych sektorach, takich jak usługi finansowe czy bezpieczeństwo narodowe, rozpocznie projekty mające na celu ocenę wpływu pojawiających się komputerów kwantowych na ich misję, np. na komunikację

zaszyfowaną, podpisywanie kodu czy jednokrotne logowanie (SSO).

Firmy powinny ocenić ryzyko związane z potencjalnymi tzw. Złymi Użytkownikami, którzy mogą podsłuchiwać i przechwytywać zaszyfowaną komunikację, aby później zdekodować ją, gdy komputery kwantowe staną się dostępne. Należy sporządzić listę aplikacji własnych opracowanych przez firmę oraz technologii i aplikacji zewnętrznych dostawców, w których kryptografia post-kwantowa (PQC) będzie niezbędna, zarówno natychmiast, jak i w najbliższych latach.



# Cyberbezpieczeństwo najwyższej klasy dostępne dla administracji publicznej jako usługa

**Administracja publiczna pozostaje jedną z najbardziej zagrożonych cyberatakami branż. Doskonale zdaje sobie z tego sprawę coraz więcej instytucji - aż 90% jednostek samorządu terytorialnego złożyło wnioski o dofinansowanie w ramach państwowego projektu „Cyberbezpieczny Samorząd”. To pierwszy krok w stronę bezpieczeństwa, jednak w co zainwestować pozyskane środki?**

**Jak wynika z badania Dell Technologies Data Protection Index 2022, 67 proc. liderów IT obawia się, że środki ochrony danych, z których korzystają, mogą być niewystarczające w obliczu zagrożeń takich jak złośliwe oprogramowanie oraz ransomware. Innym wyzwaniem, z którym mierzą się organizacje, jest rosnąca luka kompetencyjna w obszarze cyberbezpieczeństwa. Aby chronić się przed współczesnymi zagrożeniami, instytucje potrzebują spójnej strategii bezpieczeństwa oraz kompleksowych, intuicyjnych rozwiązań,**

**które będą realnym wsparciem dla zespołów zajmujących się cyberbezpieczeństwem oraz IT.**

**SOC, SOC as a Service i MDR - czym są i jak z nich korzystać?**

Wiele dużych firm decyduje się na utworzenie wewnętrznego centrum operacji bezpieczeństwa (SOC - Security Operations Center), które zajmuje się obsługą wszystkich zadań związanych z cyberbezpieczeństwem. Zadaniem pracowników SOC jest monitorowanie, wykrywanie i reagowanie na wszelkie alerty i incydenty jak najszybciej, będąc na posterunku 24/7. Własny zespół specjalistów do spraw cyberbezpieczeństwa dostępnych przez całą dobę, jest niewątpliwie skutecznym rozwiązaniem, jednak niezwykle kosztownym. Na szczęście dla organizacji, które nie mogą sobie pozwolić na taką inwestycję, rynek oferuje inne rozwiązania. Świetną alternatywą dla wewnętrznego SOC-u jest chętnie wdrażana usługa MDR (Managed Detection and Response), czyli platforma funkcjonująca w ramach tzw. SOC as a Service łącząca monitorowanie zagrożeń w czasie rzeczywistym, narzędzia analizy danych oraz doświadczenie profesjonalistów zajmujących się cyberbezpieczeństwem.

**Kompleksowe rozwiązanie dla instytucji**

Wiele firm specjalizujących się w cyberbezpieczeństwie dostarcza usługę MDR, ponieważ jest to jedno z najbardziej kompleksowych

rozwiązań pomagających znacząco zredukować ryzyko cybernetyczne. Oferowana przez Maxto ITS usługa Dell MDR bazuje na narzędziu Secureworks Taegis XDR, co gwarantuje szybkie i skuteczne wykrywanie, reagowanie oraz usuwanie skutków cyberataku. Dodatkowo firma oferuje organizacji wsparcie we wdrożeniu rozwiązania, kwartalny przegląd oraz wsparcie wykwalifikowanych specjalistów do spraw cyberbezpieczeństwa wynajmowanych na określoną w umowie liczbę godzin. W praktyce oznacza to pomoc certyfikowanych inżynierów cyberbezpieczeństwa we wdrożeniu zaleceń powstałych na skutek incydentu bezpieczeństwa, np. zdalne połączenie się z instytucją i pomoc w konfiguracji firewalla. Jest to zatem realne wsparcie w sytuacji, w której organizacja nie dysponuje własnym zespołem specjalistów do spraw cyberbezpieczeństwa. Jednocześnie koszt usługi mieści się w budżecie, którym dysponują instytucje.

*Wykrywanie oraz efektywne reagowanie na zagrożenia stanowi kluczowy aspekt utrzymania wysokiego poziomu bezpieczeństwa. Organizacje powinny wykorzystywać zaawansowane technologie i metody wykrywania, aby poprawnie identyfikować oraz skutecznie reagować zarówno na znane, jak i nieznane ataki.*

Źródła:

- Raport „Cyberbezpieczeństwo w polskich firmach 2023” firmy Vecto.
- <https://www.pap.pl/aktualnosci/minister-gawkowski-ki-do-850-tys-zl-dla-samorzadow-na-dzialania-z-zakresu>



**EWA SZTYBER**

ACCOUNT EXECUTIVE, DELL  
TECHNOLOGIES POLSKA

## Kompleksowe rozwiązanie dla instytucji

Wykrywanie oraz efektywne reagowanie na zagrożenia stanowi kluczowy aspekt utrzymania wysokiego poziomu bezpieczeństwa. Aby to osiągnąć, organizacje powinny wykorzystywać zaawansowane technologie i metody wykrywania zagrożenia. To jedyna skuteczna metoda gwarantująca poprawną identyfikację oraz szybką reakcję zarówno na znane, jak i nieznane ataki, a co za tym idzie – bezpieczeństwo instytucji i znajdujących się w niej danych.



krajowa  
izba  
gospodarki  
cyfrowej

## Krajowa Izba Gospodarki Cyfrowej

to izba gospodarcza, zrzeszająca firmy oraz przedsiębiorców z rynku gospodarki cyfrowej w celu wspierania ich ekspansji i reprezentowania wspólnych celów rynkowych w przestrzeni publicznej oraz biznesowej.

[www.kigc.pl](http://www.kigc.pl)

[biuro@kigc.pl](mailto:biuro@kigc.pl)



---

### Koncepcja, redakcja i koordynacja merytoryczna:

Brtosz Loba

### Koordynacja redakcyjna:

Michał Szanter

---

## DigitalH

**DIG IT ALL**

### Skład , oprawa graficzna i komunikacja - Agencja Marketingowa DigitalH sp. z o.o.

Agencja zajmująca się kompleksowymi działaniami z zakresu marketingu internetowego, social mediów, kampanii reklamowych, strategii marketingowych, graphic designu, UX/UI oraz działań wizerunkowych

[www.digitalh.pl](http://www.digitalh.pl)

[hello@digitalh.pl](mailto:hello@digitalh.pl)





**krajowa  
izba  
gospodarki  
cyfrowej**

[www.kigc.pl](http://www.kigc.pl)