młody TECHNIK
Istnieje od 1932 roku

CHERCHEZ LA FEMME: Stephanie Kwolek
Chemiczka, która nie wylała „zepsutego” roztworu

wrzesień • 09/2026
www.mlodytechnik.pl

Tu przejrzysz i kupisz ten numer

NEWS 24/7
przeglądaj codziennie na swoim smartfonie

młody m.technik

Ciekawi świata są zawsze młodzi

Q-DAY

ZDĄŻYĆ PRZED KATASTROFĄ
KIEDY KOMPUTERY KWANTOWE ZŁAMIĄ SZYFRY ŚWIATA

Science fiction w „Młodym Techniku”
Tomasz Nowak: Entropia

ISSN 0462–9760 Indeks 365408
09>
9 770462 976267
cena: 19,90 zł (w tym 8% VAT)

pakiet promocyjny KOCHAM SZACHY
7 e-booków z rabatem 50%

pakiet promocyjny NA WARSZTACIE
9 e-booków z rabatem 50%

Dla prenumeratorów – 30% rabatu!
Promocja Internetowa – w formularzu zamówienia online zaznacz pole
„Jestem prenumeratorem wydawnictwa AVT, kupuję ze zniżką”
i podaj swój numer prenumeraty.

www.UlubionyKiosk.pl

Q-DAY, ZDĄŻYĆ PRZED KATASTROFĄ

Ktoś właśnie zapisuje na dysku strumień zaszyfrowanych danych, których nie potrafi odczytać. Nie po to, żeby przeczytać je dzisiaj. Pamięć masowa jest tania, a cierpliwość służb wywiadowczych dobrze udokumentowana. Rachunek jest prosty: jeśli wiadomość ma pozostać tajna przez piętnaście lat, a maszyna zdolna ją złamać powstanie za dziesięć – ta wiadomość jest już przegrana. Wysłano ją, zanim zdążyliśmy ją zabezpieczyć.

Q-Day to umowna nazwa dnia, w którym komputer kwantowy osiągnie doskonałość wystarczającą, by złamać szyfry chroniące bankowość, podpis elektroniczny, dokumentację medyczną i całą resztę internetu. **Nikt nie zna tej daty i nie trzeba jej znać, żeby wiedzieć, co robić.** Wystarczy dodać dwie liczby: ile lat nasze dane muszą pozostać tajne i ile lat zajmie wymiana zabezpieczeń. Jeżeli suma przekracza najostrożniejsze szacunki dotyczące momentu pojawienia się komputerów kwantowych, problem mamy już dziś.

Oczywiscie, komputery kwantowe nie powstały po to, żeby łamać szyfry. Richard Feynman zaproponował je w 1981 roku jako narzędzie do badania przyrody, bo zwykły komputer nie potrafi wiernie odtworzyć zachowania cząsteczki. Chemicy czekają na nie od czterdziestu lat. Kłopot w tym, że **sztandarowe zadanie chemii kwantowej i atak na kryptografię wymagają maszyny dokładnie tej samej wielkości**. Nie istnieje scenariusz, w którym chemia dostaje swoje narzędzie, a kryptografia zachowuje bezpieczeństwo. Chyba że zdąży się przezbroić wcześniej.

Nie wszystko przy tym pada. Szyfrowanie danych na dysku przetrwa, funkcje skrótu przetrwają, kopalnie bitcoinów przetrwają. **Pada natomiast cała infrastruktura zaufania**: certyfikaty, dzięki którym przeglądarka rozpoznaje bank, podpisy pod umowami i aktami notarialnymi, klucze wypalane w krzemie na etapie produkcji układów. Ta ostatnia kategoria jest najtrudniejsza. Samochód sprzedany w tym roku będzie jeździł do lat czterdziestych, satelita wyniesiony w tym roku będzie wtedy na orbicie – i do żadnego nie da się już podejść z aktualizacją.

Osobny rozdział poświęcamy przypadkowi, w którym nie ma nikogo, kto mógłby wydać polecenie. Ponad trzydzieści cztery procent wszystkich bitcoinów ma klucze publiczne widoczne w łańcuchu bloków, a sieć zbudowana tak, aby żadna instytucja nie mogła zmienić jej reguł, musi teraz zbiorowo zdecydować, czy woli monety zamrozić, czy pozwolić je ukraść. To pierwszy prawdziwy test zdolności decyzyjnej systemu, który z założenia miał władzy nie mieć.

Dobra wiadomość brzmi tak: rozwiązania już istnieją. Nowe postkwantowe szyfry są już znormalizowane od 2024 roku, darmowe i – wbrew intuicji – działają na zwykłych komputerach. Wyścig z czasem nie polega więc na wymyśleniu nowych szyfrów, tylko na aplikowaniu ich w miliardach urządzeń, z których wiele nikt nigdy nie policzył. **Pierwszy termin unijny wypada 31 grudnia tego roku** – za pięć miesięcy. Do tego czasu każde państwo Unii ma mieć krajową strategię przejścia i rozpoczętą inwentaryzację własnej kryptografii.

Na koniec pytanie, które zadaję sobie od kilku miesięcy. Co się stanie, gdy spotkają się dwie rewolucje naraz – sztuczna inteligencja i komputer kwantowy? Kusi odpowiedź prosta: powstanie turbo AI, inteligencja napędzana mocą kwantową. Rzecz w tym, że akurat ta droga jest najsłabiej udokumentowana: dla danych klasycznych przewaga kwantowa w uczeniu maszynowym pozostaje nieudowodniona, a bywała obalana. Znacznie ciekawszy jest kierunek odwrotny – i on już zachodzi. Szacunek zasobów potrzebnych do złamania RSA spadł od 2019 roku z dwudziestu milionów kubitów do niecałego miliona, bez najmniejszego postępu w sprzęcie. Zdecydowały lepsze algorytmy – czyli dokładnie ta praca, w której sztuczna inteligencja robi dziś największe postępy. **Jeśli więc czegoś powinniśmy się obawiać, to nie kwantowej sztucznej inteligencji, lecz tego, że AI może bardzo przyśpieszyć nadejście Q-Day, tworząc algorytmy obniżające poprzeczkę dla technologii komputerów kwantowych. Wypatrując w radosnym podnieceniu pierwszych komputerów kwantowych przypominamy karpie nie mogące doczekać się Świąt Bożego Narodzenia. Oby AI nie zaskoczył nas gwałtownym przyspieszeniem nadejścia tej radosnej chwili.**

Wiesław Marciniak

Spis treści

Miesięcznik „Młody Technik” (11 numerów w roku) wydawany przez Wydawnictwo AVT

Adres wydawnictwa:
03–197 Warszawa, ul. Leszczynowa 11,
tel. 22 257 84 99, faks: 22 257 84 00,
http://www.avt.pl, avt@avt.pl

Redaktor Naczelny:
Wiesław Marciniak
wieslaw.marciniak@avt.pl

Sekretarz redakcji:
Dariusz Welik
dariusz.welik@avt.pl

Kontakt z redakcją:
mt@mt.com.pl
http://www.mlodytechnik.pl
http://facebook.com/magazynMlodyTechnik

Dział Reklamy:
reklama@mt.com.pl

DTP: MAD Sp. z o.o.

Prenumerata:
www.ulubionykiosk.pl
tel. 22 257 84 22 (godz. 10.00–14.00)
e-mail: prenumerata@avt.pl

Redakcja nie ponosi odpowiedzialności za treści reklam i ogłoszeń zamieszczonych w numerze.

Poczta

Coś Cię poruszyło? Chcesz podzielić się z Redakcją i Czytelnikami MT swoją opinią, wiedzą, komentarzem? Wyślij e-mail na adres: **redakcja@mt.com.pl** lub list na adres: **ul. Leszczynowa 11, 03–197 Warszawa**.

Zapach utrwalacza

Czytając artykuł o historii fotografii byłem myślami pół wieku wstecz, w łazience mojego ojca, zamienianej co niedzielę w ciemnię. Powiększalnik Krokus, kuweta, czerwona żarówka i to charakterystyczne napięcie, gdy na białym papierze zaczyna się coś pojawiać. Nie wiedziałem wtedy, że patrzę na chemię. Myślałem, że patrzę na czary.

Dziś robię zdjęcia telefonem, jak wszyscy, i mam ich wiele tysięcy, z czego oglądałem może dwieście. Wtedy z jednej wycieczki zostawało dwanaście zdjęć i każde pamiętam do dziś. Nie twierdzę, że kiedyś było lepiej, bo to nieprawda. Twierdzę tylko, że coś się po drodze zgubiło, i nie jestem pewien, czy dało się tego uniknąć.

A.W.

Liczby ostatnie

Szanowna Redakcjo,

chciałem na waszych łamach poruszyć temat który od dawna mnie nurtuje. Chodzi o to że naturalną konsekwencją istnienia liczb pierwszych powinno być istnienie liczb ostatnich lub ostatecznych. Do opracowania teorii liczb ostatnich lub ostatecznych przyjąłem założenie że powinny być podzielne przez każdą z liczb od 1 do 9 bez reszty (wynik). Pierwszą taką liczbą jest 5040, drugą 40320, następną 362880 itd. Ciekawą właściwością tych liczb jest to że suma liczb zawartych w nich wynosi zawsze 9 (jednocyfrowa). W 5040 5+0+4+0=9, 40320 4+0+3+2+0=9 362880 = 27 2+7=9.

Może Czytelnicy mają inne pomysły na ten temat lub pomysły na zastosowania tych liczb.

Wasz stały czytelnik

Wojciech Starzec

Red. Pierwsza taka liczba to 2520, nie 5040

Warunek postawił Pan jasno: liczba ma się dzielić bez reszty przez każdą z liczb od 1 do 9. Najmniejsza taka liczba to ich najmniejsza wspólna wielokrotność, a ta wynosi 2520. Sprawdźmy najtrudniejsze przypadki: 2520 podzielone przez 7 daje 360, przez 8 daje 315, przez 9 daje 280. Warunek spełniony, a liczba jest dwa razy mniejsza od podanej przez Pana.

Idźmy dalej. Skoro 2520 jest najmniejszą taką liczbą, to wszystkie pozostałe są jej wielokrotnościami: 2520, 5040, 7560, 10080, 12600 i tak bez końca. To zwykły ciąg arytmetyczny o różnicy 2520 i nie ma w nim żadnego elementu ostatniego.

Skąd zatem wzięła się Pańska lista – 5040, 40320, 362880? To silnie: iloczyny kolejnych liczb naturalnych. 7! równa się 5040, 8! równa się 40320, 9! równa się 362880. Silnia liczby n z samej definicji zawiera w iloczynie wszystkie liczby do n, więc od siódmej wzwyż każda silnia dzieli się przez wszystkie liczby od 1 do 9. To prawda i spostrzeżenie jest trafne, ale silnie stanowią zaledwie garstkę wśród wszystkich liczb spełniających warunek. Między 5040 a 40320 leży jeszcze trzynaście innych, które Pan pominął.

Suma cyfr – reguła prawdziwa, ale ogólniejsza

Tu ma Pan rację co do faktu, ale własność jest znacznie szersza, niż się wydaje, i warto pokazać, skąd się bierze. Weźmy dowolną liczbę, powiedzmy 3542, i rozpiszmy ją tak, jak zapisuje ją system dziesiętny:

$$3542 = 3 \times 1000 + 5 \times 100 + 4 \times 10 + 2$$

Teraz jedna sztuczka. Każdą potęgę dziesiątki można zapisać jako liczbę złożoną z samych dziewiątek powiększoną o jeden: tysiąc to 999 plus 1, sto to 99 plus 1, dziesięć to 9 plus 1. Podstawmy to:

$$3542 = 3 \times (999 + 1) + 5 \times (99 + 1) + 4 \times (9 + 1) + 2$$

Po wymnożeniu i pogrupowaniu wyrazów otrzymujemy dwie części:

$$3542 = (3 \times 999 + 5 \times 99 + 4 \times 9) + (3 + 5 + 4 + 2)$$

Pierwszy nawias dzieli się przez 9 bez reszty, bo 999, 99 i 9 dzielą się przez 9. Cała reszta z dzielenia zależy więc wyłącznie od drugiego nawiasu – a ten jest po prostu sumą cyfr. To działa dla każdej liczby, bo w każdej podstawimy dokładnie te same dziewiątki.

Stąd wniosek: liczba dzieli się przez 9 wtedy i tylko wtedy, gdy dzieli się przez 9 suma jej cyfr. A jeśli ta suma jest jeszcze wielocyfrowa, można ją sumować dalej – reguła obowiązuje na każdym kroku, więc postępowanie kończy się na dziewiątce.

Sprawdźmy to na liczbach spoza Pańskiej listy. 18: suma cyfr wynosi 9. 99: suma wynosi 18, sumujemy dalej i wychodzi 9. 1233: suma wynosi 9 od razu. Wszystkie trzy dzielą się przez 9 i wszystkie trzy mają opisaną przez Pana własność – a żadna z nich nie dzieli się przez 7 ani przez 8, więc do zbioru liczb „ostatecznych" nie należy.

I to jest sedno sprawy. Pańskie liczby mają tę własność nie dlatego, że są wyjątkowe, lecz dlatego, że w warunku wyjściowym zażądał Pan od nich podzielności przez dziewięć. Własność jest więc konsekwencją założenia, a nie odkryciem czegoś ponad nie – przysługuje wszystkim wielokrotnościom dziewiątki, których jest nieskończenie wiele.

Nie umniejsza to jednak samego spostrzeżenia, bo reguła jest naprawdę użyteczna. Przez stulecia posługiwali się nią rachmistrze pod nazwą wyrzucania dziewiątek: żeby sprawdzić wynik mnożenia, liczono sumy cyfr obu czynników i wyniku, redukowano je do jednej cyfry i porównywano. Jeśli coś się nie zgadzało, w rachunku był błąd. Metoda nie wykrywa wszystkich pomyłek,

ale kosztuje kilka sekund i przez kilkaset lat, aż do upowszechnienia maszyn liczących, była podstawowym sposobem kontroli obliczeń.

A teraz rzecz najciekawsza: te liczby naprawdę są wyjątkowe

Pańska intuicja o dwóch biegunach jest trafna, tylko drugi biegun wygląda inaczej, niż Pan zakładał. Liczba pierwsza to taka, która ma najmniej dzielników, jakie w ogóle mieć można – dokładnie dwa. Naturalnym przeciwieństwem jest więc nie „liczba ostatnia", lecz liczba mająca dzielników wyjątkowo wiele.

Takimi liczbami zajął się w 1915 roku hinduski matematyk Srinivasa Ramanujan i nazwał je liczbami wysoko złożonymi. Definicja jest prosta i piękna: liczba wysoko złożona to taka, która ma więcej dzielników niż każda liczba od niej mniejsza. Początek listy wygląda tak: 1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840, 1260, 1680, 2520, 5040.

Na końcu tego wyliczenia stoją obie liczby z Pańskiego listu. 2520 ma 48 dzielników – więcej niż jakakolwiek liczba mniejsza. 5040 ma ich 60. Doszedł Pan zatem własną drogą do zbioru, który matematycy badają od stu lat, i to do dwóch jego najsłynniejszych elementów. Warto to powiedzieć wyraźnie, bo takie trafienie nie jest przypadkiem: warunek podzielności przez wiele małych liczb i warunek posiadania wielu dzielników prowadzą w tę samą okolicę.

Zastosowania? Używamy ich codziennie od tysiącleci

Pyta Pan o zastosowania, a te są tak powszechne, że przestaliśmy je zauważać. Koło dzielimy na 360 stopni, godzinę na 60 minut, dobę na 24 części, rok na 12 miesięcy, a dawną stopę na 12 cali. Żadna z tych liczb nie jest przypadkowa – wszystkie mają dużo dzielników, więc dają się dzielić bez reszty na połowy, trzecie, czwarte, szóste i dwunaste części. Gdyby Babilończycy podzielili koło na 100 stopni, jedna trzecia kąta pełnego byłaby liczbą z nieskończonym rozwinięciem.

Osobno warto wspomnieć o 5040. Platon w „Prawach" proponuje, by idealne miasto liczyło dokładnie tylu obywateli, i uzasadnia to wprost jej podzielnością: taką liczbę ludzi da się podzielić na równe grupy na kilkadziesiąt sposobów, co ułatwia pobór podatków, podział ziemi i organizację wojska. Filozof grecki doszedł do tej samej liczby co Pan i z bardzo podobnego powodu.

Współcześnie ta sama zasada rządzi doborem liczby zębów w przekładniach, wielkością opakowań zbiorczych, układaniem grafików zmianowych i długością bloków danych w cyfrowym przetwarzaniu sygnałów. Wszędzie tam, gdzie coś trzeba dzielić na równe części, a liczba tych części nie jest z góry znana, opłaca się wybrać liczbę o wielu dzielnikach.

Zadanie dla Czytelników

Pan Wojciech pyta o pomysły, więc rzućmy Czytelnikom wyzwanie. Po pierwsze: jaka jest najmniejsza liczba podzielna bez reszty przez wszystkie liczby od 1 do 20? Wynik jest zaskakująco duży i wart samodzielnego wyliczenia – podpowiadamy, że nie wystarczy pomnożyć wszystkie przez siebie, trzeba postąpić sprytniej.

Osobliwość, czyli osiem tekstów i jedno przemilczenie

Temat numeru o osobliwości przeczytałem dwa razy, najpierw z ciekawości, potem z ołówkiem. Zestaw ośmiu głosów uważam za pomysł znakomity, bo pozwolił pokazać, że spór nie przebiega między entuzjastami a sceptykami, tylko wewnątrz obu tych obozów. To rzadkie w polskiej publicystyce technicznej i należą się Państwu za to słowa uznania.

Mam jednak zastrzeżenie, które dotyczy nie tego, co napisano, lecz tego, czego zabrakło. W siedmiu tekstach z ośmiu dyskusja toczy się wokół pytania „kiedy" – czy za dwadzieścia lat, czy za sto, czy nigdy. Tymczasem pytanie o datę jest z gruntu jałowe, bo żadna ze stron nie ma metody, którą dałoby się tę datę wyliczyć. Krzywe wykładnicze rysowane w latach dziewięćdziesiątych opierały się na liczbie tranzystorów, a nie na czymkolwiek, co ma związek z myśleniem. Prognoza oparta na wykresie mocy obliczeniowej mówi tyle samo o powstaniu umysłu, ile prognoza oparta na liczbie stron zadrukowanego papieru mówiła o powstaniu literatury.

Brakuje mi więc tekstu ósmego, którego nie było: o tym, czym właściwie miałaby być inteligencja ogólna i po czym poznamy, że przed nią stoimy. Bez definicji spór o termin przypomina licytację o datę przybycia gościa, którego nikt nie umie opisać. Podejrzewam zresztą, że gdyby autorzy musieli zacząć od definicji, część sporu okazałaby się nieporozumieniem językowym.

Proszę potraktować to jako zachętę, nie jako pretensję. Numer był jednym z lepszych, jakie czytałem w MT w ostatnich latach.

T.Z. nauczyciel fizyki

Red. Zarzut trafny. Dodajmy tylko, że kłopot jest głębszy, niż wynika z listu: sensownej definicji inteligencji ogólnej nie ma także w literaturze fachowej, a każda kolejna próba przesuwa poprzeczkę tam, dokąd maszyny jeszcze nie doszły. Pewnie nie raz wrócimy do tego tematu.

Kilka stron rubryki Info Zoom to zaledwie czubek góry lodowej. Świat stoi u progu gwałtownego przyspieszenia, a każda godzina przynosi mnóstwo fascynujących doniesień o nowościach. Żaden redaktor nie

ASTROFIZYKA I KOSMOLOGIA

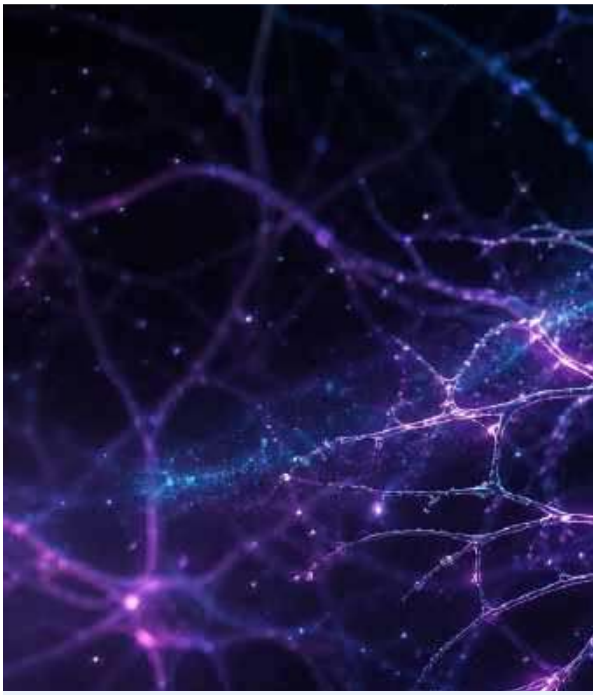
Słońce zamieni lasery w komputerach kwantowych?

Rzetelny rozwój technologii kwantowych od lat rozbija się o tę samą barierę: gigantyczne zapotrzebowanie na energię. Tradycyjne układy kwantowe – od superkomputerów po ultrapodręczne czujniki – wymagają skomplikowanych i niezwykle drogich laserów. To właśnie za pomocą precyzyjnych wiązek światła fizycy inicjują, kontrolują i odczytują stany kubitów. Koszt działania takich systemów oraz ich ślad węglowy stawały się jednak wyzwaniem na skalę przemysłową.

Międzynarodowy zespół naukowców zaprezentował rozwiązanie, które idealnie wpisuje się w ideę zrównoważonej nauki. Badacze opracowali innowacyjny system kolektorów, soczewek i filtrów optycznych zdolny do przechwytywania światła słonecznego i przekształcania go w stabilną, wysokojakościową wiązkę o właściwościach niezbędnych do pracy z układami kwantowymi.

Wyniki eksperymentów zaskoczyły samych twórców: przefiltrowane promienie Słońca okazały się wystarczająco spójne, by precyzyjnie operować na poziomach energetycznych cząstek bez wywoływania zakłóceń.

Wykorzystanie energii Słońca zamiast tradycyjnej infrastruktury elektrycznej otwiera zupełnie nowy rozdział w inżynierii. Pozwoli to na drastyczne obniżenie kosztów utrzymania ziemskich centrów obliczeniowych, a także ułatwi budowę całkowicie samowystarczalnych, autonomicznych satelitów kwantowych pracujących na orbicie Ziemi.. ■



Układ nerwowy dorosłego człowieka słynie z niezwykle ograniczonych zdolności do regeneracji. Gdy w wyniku urazu, udaru czy choroby neurologicznej dochodzi do obumarcia neuronów, w ich miejscu powstaje tzw. blizna glejowa. Stanowi ona fizyczną barierę, która choć chroni zdrową tkankę przed dalszymi uszkodzeniami, uniemożliwia również odbudowę połączeń synaptycznych. Najnowsze badania pokazują jednak, że komórki wspierające mózg kryją w sobie nieznany dotąd potencjał naprawczy.

Architekci komórkowej migracji

Sercem odkrycia jest unikalny mechanizm, w jakim astrocyty reagują na ubytek w tkance. Dotąd sądzono, że komórki te jedynie zmieniają swój kształt i zwiększają objętość w miejscu uszkodzenia. Badacze zaobserwowali jednak, że w odpowiedzi na sygnały chemiczne płynące z uszkodzonego obszaru, astrocyty potrafią aktywnie przemieszczać własne jądra komórkowe, a następnie przetłaczać całą strukturę komórki w stronę ubytku.

Ten precyzyjny ruch przypomina pełzanie: astrocyt wysuwa wypustkę w kierunku uszkodzenia, kotwiczy ją w macierzy zewnątrzkomórkowej, a następnie za pomocą włókien cytoszkieletu wciąga jądro i resztę organelli.

MEDYCYNA I NEUROBIOLOGIA

Mózg, który sam leczy swoje blizny. Niezwykła zdolność astrocytów

Przez dekady uważano je za zwykłe „spoiwo" utrzymujące strukturę mózgu. Najnowsze odkrycie naukowców opublikowane na łamach „Nature Neuroscience" wywraca jednak dotychczasową wiedzę do góry nogami. Astrocyty potrafią aktywnie przemieszczać się i regenerować uszkodzoną tkankę nerwową.

Dzięki temu komórki są w stanie fizycznie wypełnić powstałą lukę i zreorganizować lokalną mikrostrukturę mózgu bez konieczności gwałtownego podziału komórkowego, który mógłby prowadzić do powstawania nowotworów.

Przełom w walce z urazami mózgu

Odkrycie to otwiera zupełnie nowe możliwości w medycynie regeneracyjnej i neurochirurgii. Zrozumienie szlaków molekularnych, które aktywują ruch jądra komórkowego w astrocytach, może pozwolić na opracowanie leków stymulujących te komórki do szybszego i bardziej uporządkowanego naprawiania tkanki.

W przyszłości odpowiednia farmakoterapia mogłaby precyzyjnie kierować ruchem astrocytów u pacjentów po udarach lub ciężkich urazach mechanicznych, ograniczając powikłania i przyspieszając powrót sprawności neurologicznej. To jasny sygnał, że nasz mózg posiada znacznie bogatszy apteczkę naprawczą, niż dotąd przypuszczaliśmy. ■

MEDYCYNA I NEUROBIOLOGIA

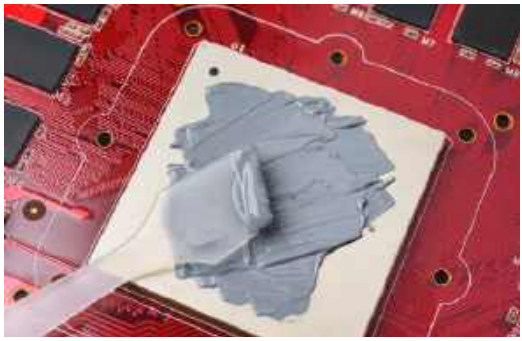
Rewolucja w leczeniu ran: koniec z lekoopornością

Przewlekłe i trudno gojące się rany – zwłaszcza w przebiegu zespołu stopy cukrowej czy owrzodzeń – stanowią jedno z najtrudniejszych wyzwań współczesnej medycyny. Głównym winowajcą powikłań jest tzw. biofilm bakteryjny: skomplikowana, wielowarstwowa struktura drobnoustrojów chroniona lepką macierzą. Powoduje ona, że nawet silne antybiotyki stają się bezskuteczne. Naukowcy z Wrocławia opracowali jednak innowacyjne podejście, które przełamuje tę barierę.

Przełomowa metoda opiera się na zastosowaniu dedykowanych kompozytów polimerowych połączonych z substancjami czynnymi biologicznie. Niszczą one osłonę biofilmu, uniemożliwiając bakteriom wytworzenie oporności i ułatwiając szybką regenerację uszkodzonych tkanek. Nowe opatrunki nie tylko eliminują infekcję, ale rzutują również na przyspieszenie naturalnego procesu odbudowy naczyń krwionośnych w miejscu ubytku.

Równolegle polscy badacze wzięli pod lupę naturalne właściwości miodów bartnych. Wyniki prac potwierdziły ich unikalne, niezwykle silne działanie przeciwdrobnoustrojowe i immunomodulujące. Naturalne związki organiczne obecne w miodzie zebranym tradycyjnymi metodami wykazują zdumiewającą skuteczność w hamowaniu namnażania lekoopornych szczepów bakterii.

Połączenie nowoczesnej inżynierii materiałowej z zaawansowaną analizą substancji naturalnych otwiera zupełnie nowy rozdział w traumatologii. Nowatorskie terapie pozwolą uniknąć groźnych amputacji, drastycznie skracając czas hospitalizacji pacjentów. ■



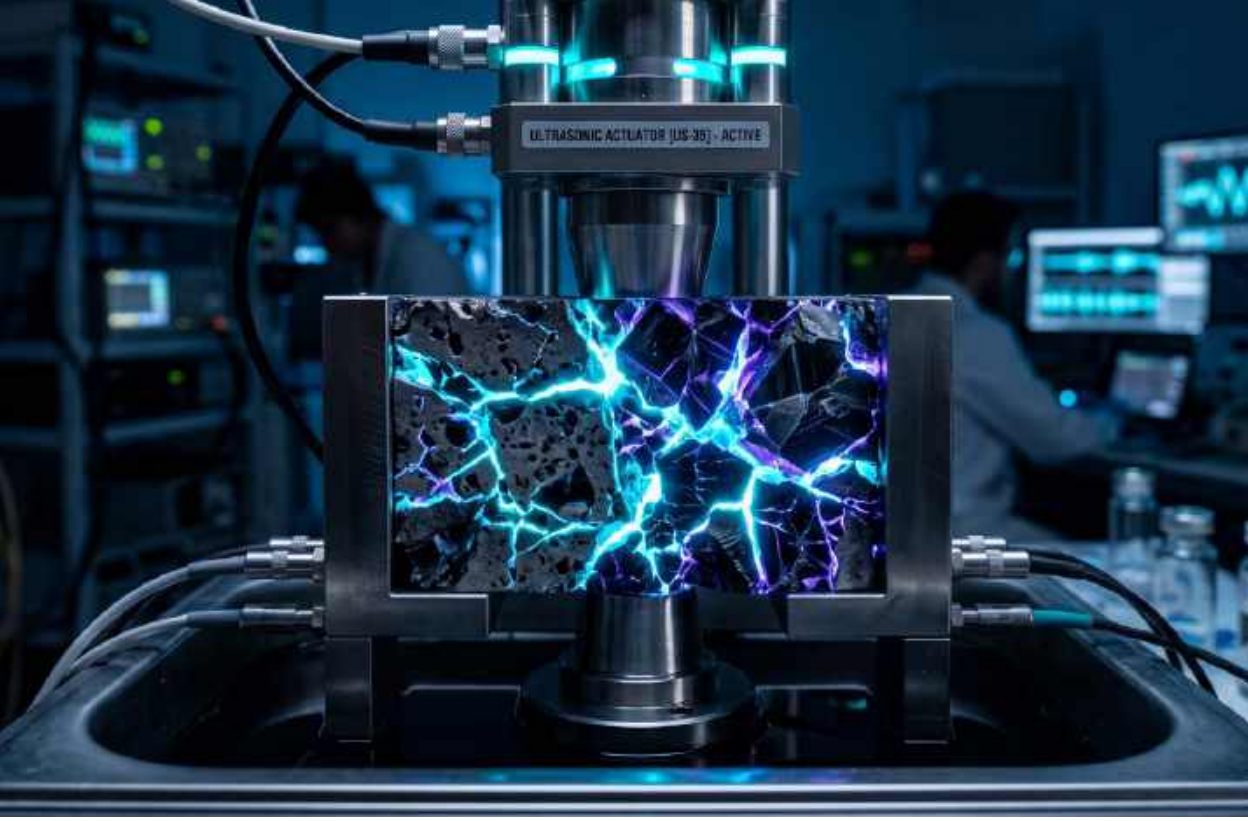
KOMPUTERY

Złoty wiek chłodzenia: Węgiel zamiast pasty przewodzącej

Tradycyjna pasta termoprzewodząca to stały element montażu każdego układu chłodzenia w komputerze. Choć skutecznie wypełnia mikroskopijne nierówności między procesorem a radiatorem, posiada poważną wadę: z czasem wysycha, traci swoje właściwości i wymaga regularnej, często uciążliwej wymiany. Przełom na rynku komponentów PC przynoszą nowatorskie podkładki termiczne na bazie nanoturbolin węglowych, które powoli wysyłają klasyczne pasty do lamusa.

Zaawansowane nakładki węglowe wykorzystują unikalne właściwości fizyczne grafenu i alotropowych odmian węgla. Dzięki ułożeniu włókien w pionowej strukturze, materiał ten przewodzi ciepło znacznie efektywniej niż złożone mieszanki silikonowo-metaliczne. Ekstremalnie wysoka przewodność cieplna pozwala na natychmiastowe odprowadzanie energii z procesora do układu chłodzenia, co przekłada się na niższe temperatury pracy nawet przy ekstremalnym obciążeniu jednostki.

Największą zaletą nowego rozwiązania jest jednak jego bezobsługowość i trwałość. Struktura węglowa nie płynnieje pod wpływem wysokiej temperatury, nie utlenia się ani nie wysycha. Raz zamontowana podkładka zachowuje swoje właściwości przewodzące przez całe życie procesora, eliminuje ryzyko pobrudzenia płyty głównej oraz pozwala na wielokrotny demontaż i ponowny montaż tego samego elementu. To rewolucja, która nie tylko podnosi wydajność komputerów, ale też ułatwia życie wszystkim entuzjastom sprzętu. ■



NOWE MATERIAŁY I TECHNOLOGIA

Ciemność rozświetlona dźwiękiem

Materiały zdolne do emisji światła pod wpływem czynników zewnętrznych od dawna fascynują naukowców. Dotąd znaliśmy głównie zjawiska luminescencji wywoływanej promieniowaniem UV, prądem elektrycznym czy tarciem mechanicznym. Zespół badaczy, z udziałem polskich naukowców, przesunął jednak granice fizyki materiałowej, tworząc innowacyjny kompozyt, który potrafi emitować silne promieniowanie świetlne pod wpływem niszczących lub stymulujących fal ultradźwiękowych.

Mechanizm stojący za tym niezwykłym zjawiskiem opiera się na tzw. mechanoluminescencji oraz mechanizmach piezoluminescencyjnych. Gdy falowanie ultradźwiękowe rozchodzi się wewnątrz struktury materiału, wywołuje szybkie, mikroskopowe odkształcenia w sieci krystalicznej. Powstające w ten sposób lokalne naprężenia oraz ładunki elektryczne wzbudzają jony zawarte w materiale, prowadząc do natychmiastowej emisji fotonów.

Co wyjątkowo istotne, syntezowany materiał wykazuje niezwykłą wszechstronność. Reaguje nie tylko na bezdotykowe impulsy akustyczne o wysokiej częstotliwości, ale również na klasyczne bodźce fizyczne, takie jak nacisk, tarcie, bezpośrednie uderzenie czy zmiany temperatury. Dzięki temu staje się wielofunkcyjnym wskaźnikiem stanu fizycznego otoczenia.

Odkrycie to niesie za sobą ogromny potencjał praktyczny. W inżynierii materiałowej nowa substancja może posłużyć do tworzenia bezinwazyjnych czujników naprężeń i uszkodzeń wewnątrz struktur lotniczych, budowlanych czy w łopatach turbin wiatrowych – miniaturowe pęknięcie pod wpływem drgań zaczęłoby dosłownie świecić, sygnalizując awarię przed jej wystąpieniem.

Z kolei w medycynie ultradźwiękowo wzbudzana luminescencja otwiera nowe możliwości w precyzyjnym obrazowaniu narządów wewnętrznych oraz w terapii fotodynamicznej, gdzie światło potrzebne do aktywacji leku niszczącego komórki nowotworowe mogłoby być generowane głęboko wewnątrz ciała pacjenta za pomocą bezpiecznych fal akustycznych. ■

Dodaj do obserwowanych

SZTUCZNA INTELIGENCJA

◆ Badacze z Google DeepMind oraz FutureHouse opisali w „Nature" systemy AI, które samodzielnie stawiają hipotezy biomedyczne. Algorytmy Co-Scientist i Robin wytypowały nowe leki na białaczkę oraz zwyrodnienie plamki żółtej, współpracując z ludźmi w cyklach laboratoryjnych. To przełom w automatyzacji odkryć naukowych, gdzie maszyna staje się pełnoprawnym partnerem badacza. ◆ Według publikacji w „Scientific Reports" integracja sztucznej inteligencji z superkomputerami gwałtownie przyspiesza procesy badawcze. Autorzy analizują, jak nowoczesne przepływy pracy łączą moc obliczeniową z algorytmami uczącymi się, by skracać czas od teorii do eksperymentu. Nowy model współpracy redefiniuje sposób, w jaki nauka radzi sobie z ogromnymi zbiorami danych. ◆

KOMPUTERY KWANTOWE

◆ Zespół z HRL Laboratories oraz QuTech ogłosił w magazynie „Nature" postępy w budowie krzemowych procesorów kwantowych. Inżynierowie uzyskali rekordowo niski błąd operacji na poziomie 0,2 proc. przy wykorzystaniu 18 kubitów spinowych. Nowa architektura przesyłu informacji ułatwia korygowanie błędów, co przybliża nas do stworzenia stabilnych i skalowalnych komputerów kwantowych.◆ Redakcja „Nature Biotechnology" podsumowała wyniki wyzwania Q4Bio, w którym metody hybrydowe pozwoliły symulować kompleksy białkowe liczące ponad 12 000 atomów. IBM przewiduje, że rok 2026 będzie momentem zwrotnym dla uzyskania przewagi kwantowej w biologii molekularnej. Połączenie klasycznych serwerów z procesorami kwantowymi pozwala modelować leki o niespotykanej dotąd złożoności. ◆

FIZYKA

◆ Fizycy z Advanced Science Research Center odtworzyli w laboratorium mechanizm pobierania energii z czarnych dziur. Wykorzystując urządzenie symulujące ultraszybką rotację, zespół potwierdził zjawisko superradiancji rotacyjnej w warunkach kontrolowanych. Wyniki opublikowane w „Nature" dowodzą, że ekstremalne procesy astrofizyczne można badać na Ziemi bez opuszczania ziemskiej atmosfery. ◆ Naukowcy z Imperial College London opracowali zaawansowane czujniki kwantowe przeznaczone do wykrywania ciemnej materii. Urządzenia te potrafią zarejestrować subtelne sygnały pochodzące z wczesnego wszechświata, w tym pierwotne fale grawitacyjne. Nowa technologia detekcji otwiera drogę do zrozumienia niewidzialnych składników kosmosu, które od dekad pozostają jedną z największych zagadek fizyki. ◆

EKSPLORACJA KOSMOSU

◆ Agencja NASA wybrała 41 technologii opracowanych przez 37 amerykańskich firm, przeznaczając 600 milionów dolarów na przygotowania do misji księżycowych i marsjańskich. Kluczowe projekty dotyczą walki z pyłem kosmicznym, który utrudnia eksploatację sprzętu na innych globach. Innowacje te mają umożliwić bezpieczne lądowania załogowe zaplanowane na koniec 2028 roku. ◆

ELEKTRONIKA

◆ Inżynierowie z MIT zaprezentowali nowy układ lidarowy na chipie, który nie posiada żadnych ruchomych części mechanicznych. Dzięki zastosowaniu fotoniki krzemowej i przeprojektowaniu anten, urządzenie oferuje szersze pole widzenia przy minimalnym poziomie szumów. Solid-state design to szansa na tańsze i bardziej niezawodne systemy nawigacji dla autonomicznych samochodów oraz dronów. ■

Źródła: Nature, ScienceDaily, Nature Biotechnology, Scientific Reports. Okres: 4 lipca – 1 sierpnia 2026.

Paliwo, które miało być wszystkim

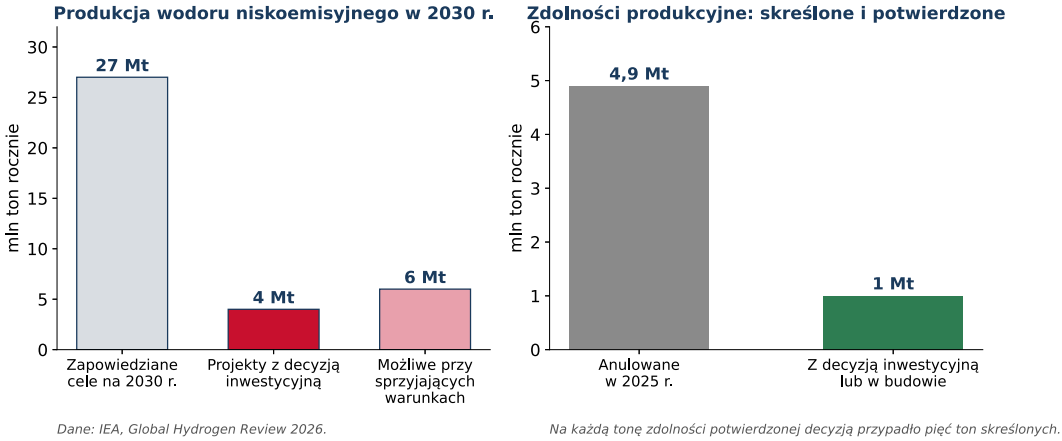
Wodór 2026 – od gospodarki wodorowej do kilku nisz, w których nie ma zamiennika

W połowie 2025 roku Rybnik ogłosił przetarg na dostawy wodoru do swoich autobusów. Nie wpłynęła ani jedna oferta. Miasto miało wtedy jedną z największych flot wodorowych w Polsce, kupioną z niemal stuprocentową dotacją, i nagle okazało się, że nie ma od kogo kupić paliwa. To zdanie mówi o gospodarce wodorowej więcej niż wszystkie strategie razem wzięte: pojazdy udało się sfinansować, rynku nie.

Rok, w którym zaczęto liczyć

Zacznijmy od stanu faktycznego, bo w przypadku wodoru różnica między zapowiedzią a produkcją jest szczególnie duża. Według opublikowanego w czerwcu 2026 roku raportu Międzynarodowej Agencji Energetycznej światowe zużycie wodoru przekroczyło w 2025 roku 100 milionów ton, rosnąc o niecałe trzy procent. Kluczowa jest jednak struktura tej liczby: 99 procent tego wodoru powstaje z paliw kopalnych bez wychwytu dwutlenku węgla. Sama produkcja wodoru wyemitowała w 2025 roku około miliarda ton CO_2 – mniej więcej tyle, ile wynosi roczna emisja Japonii i Korei razem wziętych.

Wodór niskoemisyjny, czyli ten, o którym mówią strategie, to niecały milion ton. Rósł w 2025 roku o 20 procent i w 2026 po raz pierwszy w historii ma przekroczyć jeden procent światowej produkcji. Jeden procent – po ćwierćwieczu zapowiedzi i po dekadzie rządowych programów.



1. Po lewej: cele na 2030 rok wobec projektów z podjętą decyzją inwestycyjną. Po prawej: bilans 2025 roku. Na każdą tonę zdolności potwierdzonej decyzją przypadło pięć ton skreślonych

Najbardziej wymowne jest jednak zestawienie planów z decyzjami. Ogłoszone cele produkcyjne na 2030 rok sięgają blisko 27 milionów ton rocznie. Projekty, które faktycznie przeszły przez decyzję inwestycyjną, dają nieco ponad 4 miliony ton, z możliwym dodatkiem kolejnych 2 milionów, gdyby warunki się poprawiły. Spośród wszystkich krajów, które ogłosiły cele, na kursie do ich realizacji są dwa: Chiny i Holandia. Do tego dochodzi arytmetyka samego 2025 roku: branża podjęła decyzje inwestycyjne albo rozpoczęła budowę zdolności rzędu miliona ton rocznie – i skreśliła projekty o zdolności 4,9 miliona ton.

Kapitał wyciągnął z tego wnioski szybciej niż administracja. Udział wodoru w finansowaniu wysokiego ryzyka w energetyce spadł z 13 procent w szczycie 2023 roku do 4 procent w 2025. Nakłady inwestycyjne na projekty wodorowe wprawdzie się podwoiły, do prawie 7 miliardów dolarów, ale to wciąż 0,7 procent globalnych inwestycji w dostawy energii. Innymi słowy: cała światowa gospodarka wodorowa jest dziś inwestycyjnie mniejsza niż zaokrąglenie.

Dlaczego to miało zadziałać

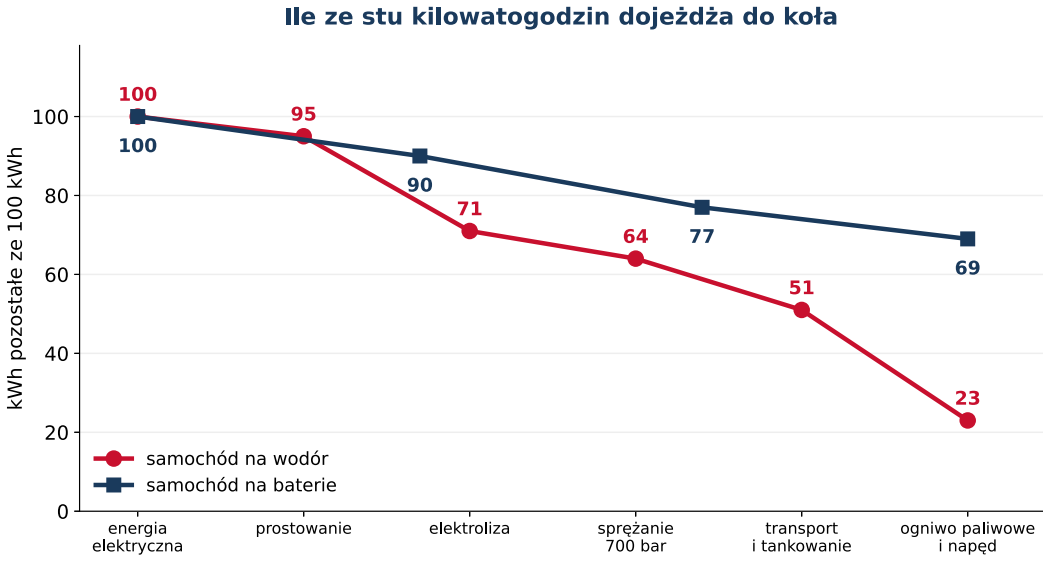
Pomysł nie był głupi – przeciwnie, jest jednym z najbardziej eleganckich w historii energetyki. Wodór ma najwyższą energię na kilogram spośród wszystkich paliw: 33,3 kilowatogodziny, prawie trzy razy więcej niż olej napędowy. Spalony albo utleniony w ogniwie paliwowym daje wodę. Można go wyprodukować wszędzie tam, gdzie jest prąd i woda. I – to była najbardziej uwodzicielska część obietnicy – ta sama cząsteczka miała ogrzewać domy, napędzać samochody, wytapiać stal i magazynować nadwyżki z wiatraków. Jeden nośnik zamiast pięciu.

Termin „gospodarka wodorowa" ukuł w 1970 roku elektrochemik John Bockris podczas wykładu w ośrodku badawczym General Motors. W 2003 roku prezydent George W. Bush ogłosił program wodorowy w orędziu o stanie państwa, obiecując, że dziecko urodzone tamtego roku odbierze prawo jazdy na samochód wodorowy. To dziecko ma dziś dwadzieścia trzy lata. W 2020 roku Unia Europejska przyjęła strategię wodorową, a za nią poszły 66 krajowych strategii na całym świecie.

Rachunek, który się nie zmienił

Trzeba w tym miejscu powiedzieć rzecz niewygodną dla obu stron sporu: fizyka, która dziś przesądza o wyniku, była znana od początku. Nic się w niej nie popsuło po drodze – po prostu zaczęto za nią płacić rachunki.

Prześledźmy sto kilowatogodzin prądu z wiatraka. Zamiana prądu przemiennego na stały zjada około pięciu procent. Elektroliza – nawet nowoczesna, membranowa – oddaje 65 do 75 procent włożonej energii; reszta ucieka jako ciepło. Sprężenie wodoru do 700 barów, bez czego nie zmieści się w zbiorniku samochodu, kosztuje kolejne 10 procent jego zawartości energetycznej. Skroplenie byłoby jeszcze droższe: wodór wrze w temperaturze minus 253 stopni Celsjusza, ledwie dwadzieścia stopni nad zerem bezwzględnym. Transport i tankowanie to następne



Etapy dla baterii rozmieszczono tak, by początek i koniec obu ścieżek się pokrywały. Wartości zaokrąglone; sprawności poszczególnych etapów wg analiz Uniwersytetu w Cambridge i danych DOE.

2. Łańcuch przemian energii dla obu napędów. Każdy etap jest technicznie poprawny; problemem jest ich liczba

straty. Wreszcie ogniwo paliwowe w samochodzie oddaje około połowy tego, co dostało.

Do koła dojeżdża od 20 do 30 kilowatogodzin ze stu. W samochodzie bateryjnym – około siedemdziesięciu. Auto wodorowe potrzebuje więc dwa do trzech razy więcej prądu na ten sam kilometr. Jeżeli energia z odnawialnych źródeł jest towarem rzadkim, a przez najbliższą dekadę będzie, to jest to argument rozstrzygający i żadna poprawa w elektrolizerach go nie odwróci: nawet elektroliza o stuprocentowej sprawności zostawiłaby wodór w tyle.

Do tego dochodzą kłopoty, o których mało się mówi. Wodór to najmniejsza cząsteczka w przyrodzie – przenika przez uszczelnienia i dyfunduje w głąb stali, gdzie powoduje kruchość wodorową, czyli utratę plastyczności i pękanie elementów, które w innych warunkach pracowałyby dziesięciolecia. Rurociąg gazowy nie nadaje się do wodoru bez przeróbki. A ulotniony wodór nie jest obojętny dla klimatu: przedłuża życie metanu w atmosferze, więc pośrednio działa jak gaz cieplarniany o sile kilkunastokrotnie większej niż dwutlenek węgla.

Cena, której nikt nie chciał zapłacić

Cała rzecz rozbija się o jedną lukę. Wodór szary kosztuje 1,5…2,5 dolara za kilogram. Zielony – od 4,5 do 7 dolarów. Żaden przemysłowy odbiorca nie zapłaci trzykrotności ceny za identyczną chemicznie cząsteczkę, jeżeli nie zmusi go do tego przepis albo nie dopłaci mu do tego państwo. Hutnictwo, wskazywane jako najbardziej naturalny odbiorca, potrzebuje wodoru po 2…3 euro za kilogram, żeby projekt się spinał. Nikt takiej ceny nie oferuje.

Unia próbuje tę lukę zasypać aukcjami Europejskiego Banku Wodoru: producent deklaruje,

Kolory wodoru – ściągawka

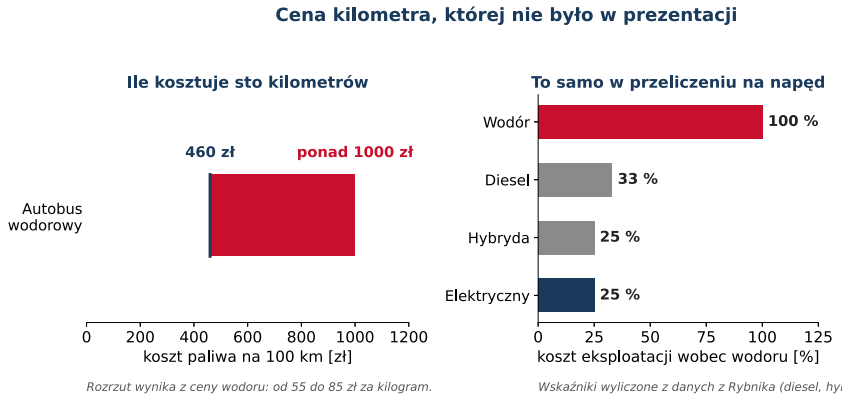
Szary – z gazu ziemnego metodą reformingu parowego. Ponad 95 procent dzisiejszej produkcji. Kosztuje 1,5…2,5 dolara za kilogram i emituje około 10 kg CO_2 na każdy kilogram wodoru.

Niebieski – to samo, ale z wychwytem dwutlenku węgla. Tańszy od zielonego, lecz skuteczność wychwytu w istniejących instalacjach bywa znacznie niższa od projektowej.

Zielony – z elektrolizy wody prądem ze źródeł odnawialnych. Koszt 4,5…7 dolarów za kilogram, zależnie od ceny prądu i wykorzystania elektrolizera.

Turkusowy – z pirolizy metanu; produktem ubocznym jest stały węgiel, nie CO_2. Na etapie instalacji pilotażowych.

Biały (naturalny) – wydobywany z podziemnych złóż, gdzie powstaje w reakcjach skał z wodą. Największa niewiadoma tej dziedziny.



3. Po lewej: trzecia aukcja Europejskiego Banku Wodoru. Po prawej: co zostało z drugiej aukcji, gdy przyszło do podpisywania umów

ilu eurocentów dopłaty do kilograma potrzebuje, a najtańsze oferty wygrywają. Trzecia aukcja, rozstrzygnięta 7 maja 2026 roku, przyznała 1,09 miliarda euro dziewięciu projektom o łącznej mocy elektrolizerów 1,1 gigawata. Zgłoszeń było 58, z jedenastu krajów, na łączną kwotę 8,4 miliarda – sześciokrotnie więcej, niż wynosił budżet. Dopłaty rozłożyły się od 44 eurocentów do 3,49 euro za kilogram, przy czym najwyższe trafiły do dwóch norweskich projektów obsługujących żeglugę.

Najciekawsze jest jednak to, co dzieje się po ogłoszeniu wyników. W drugiej aukcji Komisja wybrała 15 projektów i przyznała im 992 miliony euro. Do stycznia 2026 roku umowy podpisało sześć z nich, na łączną kwotę 270,6 miliona i moc 381 megawatów. Reszta odpadła w trakcie negocjacji. To jest dokładnie ta różnica, o której mówi ta rubryka: między wygraną w konkursie a podpisem pod umową leży cała przepaść ryzyka, którego nikt nie chce wziąć na siebie.

Dotacja tworzy projekt. Rynek tworzy odbiorca. To nie jest to samo.

Lista strat

Rok 2026 przyniósł serię decyzji, które w tej branży nazywa się dyscypliną kapitałową, a poza nią – wycofaniem się. W czerwcu BP skasowało australijski projekt H2 Kwinana o zdolności 44 ton dziennie, po tym jak nie udało się zdobyć wsparcia rządowego; koncern zapisał w tym samym okresie odpisy rzędu pięciu miliardów dolarów i sprzedał udziały w brytyjskich projektach wychwytu CO_2. ArcelorMittal zamroził budowę instalacji redukcji bezpośredniej rudy we Francji, Hiszpanii, Belgii i Niemczech – mimo że miał już przyznane 3,5 miliarda euro dotacji. Amerykański Cleveland-Cliffs porzucił swój projekt, podając jako powód brak dostępnego czystego wodoru. Francuski Lhyfe zawiesił instalację powyżej 100 megawatów. W Air Products akcjonariusze doprowadzili do odwołania prezesa po serii nieudanych inwestycji wodorowych. W Stanach Zjednoczonych obowiązuje ulga podatkowa oznaczana symbolem 45V – dopłata sięgająca trzech dolarów do każdego kilograma wodoru o najniższej emisyjności, wprowadzona w 2022 roku. Pierwotnie miała objąć wszystkie instalacje, których budowa ruszy do końca 2032 roku. Ustawa podatkowa podpisana 4 lipca 2025 roku skróciła ten termin o pięć lat: dopłatę dostaną wyłącznie projekty rozpoczęte przed końcem 2027 roku. Inwestorzy, którzy zakładali dekadę na przygotowanie przedsięwzięcia, zostali z kilkunastoma miesiącami – i wielu z nich uznało, że nie zdąży.

Osobny rozdział to transport ciężki, czyli obszar, w który wierzono najmocniej. Nikola – firma, która w szczycie hossy była warta więcej niż Ford – złożyła wniosek o upadłość w lutym 2025 roku, sprzedawszy wcześniej ponad 200 ciężarówek wodorowych. Hyzon Motors został zlikwidowany decyzją akcjonariuszy, niemiecki Quantron ogłosił upadłość, podobnie jak Hyvia, spółka firmowana przez Renault. Ze zobowiązań wodorowych wycofały się General Motors i Stellantis.

Samochód osobowy jest przypadkiem najbardziej jaskrawym. Toyota sprzedała w Stanach Zjednoczonych 147 egzemplarzy Mirai przez trzy kwartały 2025 roku. W całym kraju działa około 70 stacji tankowania wodoru, prawie wszystkie w Kalifornii, a Shell zamknął swoją sieć. Trzej właściciele złożyli pozew zbiorowy na 5,7 miliarda dolarów, zarzucając producentowi, że sprzedawał samochód, którego nie da się zatankować. Toyota mimo to wprowadziła Mirai do oferty na rok modelowy 2026 – z nowymi felgami.

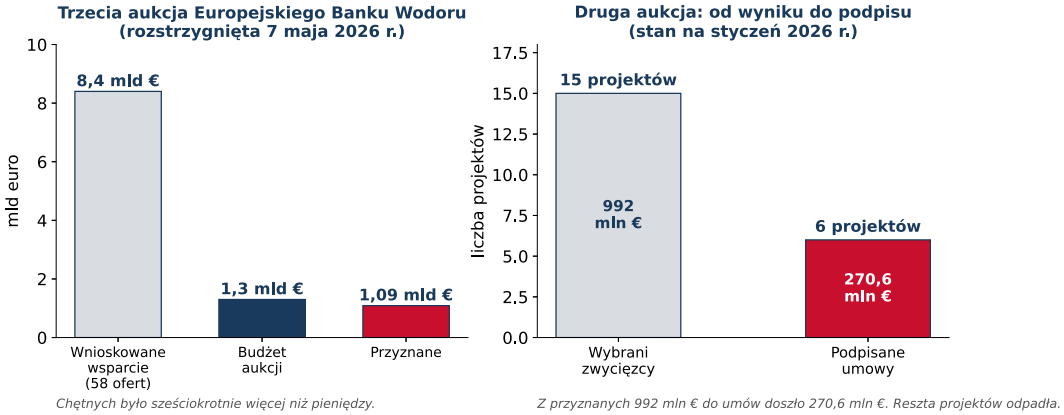
Kontrargument należy postawić w tym samym miejscu, bo istnieje. Światowa flota pojazdów na ogniwa paliwowe wzrosła w 2025 roku o 20 procent, do prawie 130 tysięcy sztuk. Wzrost pochodzi jednak z dwóch konkretnych miejsc: chińskich ciężarówek i koreańskich samochodów osobowych – czyli z rynków, na których państwo dopłaca do każdego egzemplarza. Daimler zapowiada dostarczenie stu ciężarówek NextGenH2 do końca 2026 roku. Historia nie jest więc zamknięta; jest tylko znacznie skromniejsza, niż zakładano.

Polska: sto pięćdziesiąt autobusów i dziewięć stacji

Polski wątek tej historii jest wyjątkowo pouczający, bo pokazuje mechanizm w czystej postaci. W czerwcu 2026 roku CEE Bankwatch Network i Polska Zielona Sieć opublikowały raport pod tytułem „Autobusy wodorowe w Polsce: co poszło nie tak?". Wnioski są jednoznaczne i warto je znać, zanim ktoś zaproponuje kolejny przetarg.

Do kwietnia 2026 roku zarejestrowano w Polsce około 150 autobusów wodorowych. Najwięcej mają Poznań, Rzeszów i Wałbrzych – po 34 sztuki; duże zamówienia złożyły też Chełm, Rybnik i Konin. Powód tej popularności jest prozaiczny: programy unijne refundowały nawet 100 procent kosztu zakupu autobusu wodorowego, podczas gdy przy elektrycznym wsparcie sięgało 60...80 procent. Samorząd, który liczy pieniądze, wybierał to, co dostawał za darmo. Powstał popyt, którego nie stworzyłby żaden rachunek eksploatacyjny.

Bo rachunek eksploatacyjny wygląda tak: przy cenie wodoru od 55 do 85 złotych za kilogram przejechanie stu kilometrów kosztuje od 460 do ponad tysiąca złotych. W Rybniku eksploatacja autobusu wodorowego okazała się ponad trzykrotnie droższa niż autobusu z silnikiem Diesla i czterokrotnie droższa niż hybrydy. W Koninie – czterokrotnie droższa niż autobusu elektrycznego. W Rzeszowie policzono, że samo paliwo dla dwudziestu autobusów przez piętnaście lat kosztowałoby ponad 120 milionów złotych,



4. Koszt eksploatacji autobusu miejskiego. Prawa część wykresu przelicza dane z Rybnika i Konina na wspólną skalę

czyli więcej niż zakup całej floty. We Wrocławiu analiza wykazała, że nawet przy stuprocentowej dotacji całkowity koszt posiadania wypada gorzej niż przy pojazdach konwencjonalnych – i miasto wycofało się z zakupu.

Infrastruktura nie nadążyła, bo nie miała jak. Do końca 2025 roku w całej Polsce działało dziewięć publicznych stacji tankowania wodoru; w 2026 roku uruchomiono cztery kolejne. Dla porównania kierowcy samochodów elektrycznych mają do dyspozycji ponad 12,5 tysiąca punktów ładowania. Orlen konsekwentnie rozbudowuje sieć – siódma ogólnodostępna stacja ruszyła w Gdyni w czerwcu 2026 roku, a wodór dowożą do niej naczepy z hubów we Włocławku i Trzebini – ale skala pozostaje mikroskopijna wobec zapowiedzi.

Warto przy tym zestawić dwa komunikaty tej samej firmy. W materiałach z 2024 roku Orlen podawał, że łączna moc elektrolizerów grupy sięgnie około 1 gigawata do 2030 roku, co pozwoli produkować ponad 130 tysięcy ton odnawialnego wodoru rocznie „na koniec obecnej dekady". W komunikatach z wiosny i lata 2026 roku ta sama liczba 130 tysięcy ton pojawia się z datą 2035, a moc elektrolizerów określana jest na około 0,9 gigawata. Ten sam wolumen, pięć lat później. To nie jest zarzut wobec spółki – to jest ilustracja tego, co w tej branży dzieje się z terminami.

Do tego dochodzą kłopoty ruchowe, które w prezentacjach nie występują. W Poznaniu i Wałbrzychu zanieczyszczone paliwo unieruchomiło większość floty na dwa tygodnie. W Chełmie autobusy zawodziły podczas silnych mrozów. Przewoźnik z Tychów tankuje w Katowicach, co kosztuje setki tysięcy złotych rocznie. Pod koniec 2024 roku przedstawiciele 21 miast wystąpili do rządu o dopłaty do paliwa wodorowego. A w Rybniku, jak wspomnieliśmy na wstępie, przetarg na dostawy nie przyciągnął żadnej oferty; miasto zawarło ostatecznie umowę na zielony wodór z Konina i rozważa budowę własnej instalacji, uznając zależność od jednego dostawcy za zbyt ryzykowną.

Gdzie wodór zostaje

Byłoby błędem wyjść z tego artykułu z przekonaniem, że wodór to pomyłka. Przeciwnie – jest niezbędny, tylko w innym miejscu, niż obiecywano. Klucz do zrozumienia całej sprawy mieści się w jednym zdaniu: wodór jest surowcem

Jak czytać zapowiedź projektu wodorowego – pięć pytań

1. Czy zapadła decyzja inwestycyjna? Bez niej projekt jest prezentacją, a nie budową.
2. Kto jest odbiorcą i czy podpisał umowę na odbiór? Deklaracja zainteresowania to nie kontrakt.
3. Po jakiej cenie za kilogram? Jeżeli cena nie pada, znaczy, że nie została uzgodniona.
4. Czy dotacja jest przyznana, czy podpisana? Między jednym a drugim odpada zwykle większość projektów.
5. Skąd prąd i przy jakim wykorzystaniu elektrolizera? Elektrolizer pracujący 2000 godzin w roku produkuje wodór po cenie, której nikt nie kupi.

5. Podział zastosowań według prostego kryterium: co wodór ma zastąpić. Im niżej, tym trudniej obronić rachunek

chemicznym, nie paliwem. Wszędzie tam, gdzie zastępuje cząsteczkę, nie ma dla niego zamiennika. Wszędzie tam, gdzie miałby zastąpić prąd, przegrywa z przewodem.

Amoniak i metanol to mniej więcej połowa światowego zużycia wodoru. Nawozów azotowych nie da się zrobić inaczej niż z wodoru – proces Habera-Boscha karmi dziś około połowy ludzkości i nie istnieje jego elektryczna wersja. Rafinerie potrzebują wodoru do odsiarczania paliw i hydrokrakingu. W hutnictwie wodór zastępuje węgiel jako reduktor rudy żelaza i to jest jedyna znana droga do stali bez emisji: szwedzka Stegra buduje w Boden zakład z 740-megawatowym elektrolizerem, choć i tam pierwotny termin pierwszej stali z 2025 roku przesunął się na 2026 i dalej. W lutym 2026 roku pierwsza partia zielonego żelaza gąbczastego dopłynęła do Europy z Australii. Wreszcie żegluga i lotnictwo, gdzie bateria jest zbyt ciężka, a paliwo musi być cząsteczką – nieprzypadkowo to właśnie projekty morskie zgarnęły w unijnej aukcji najwyższe dopłaty.

Gdzie jest mgła

Pierwsza niewiadoma to koszt – i tu warto uważać z ogłaszaniem końca historii. W 2025 roku zainstalowana moc elektrolizerów podwoiła się na świecie i przekroczyła 4 gigawaty, głównie

Słowniczek

Elektroliza: rozkład wody na wodór i tlen prądem elektrycznym. Urządzenie do tego służące to elektrolizer; jego moc podaje się w megawatach pobieranej energii elektrycznej, nie w tonach wodoru.

RFNBO: unijna kategoria paliw odnawialnych pochodzenia niebiologicznego. Aby wodór się do niej zaliczał, prąd musi spełniać wymogi dotyczące dodatkowości oraz zgodności w czasie i przestrzeni z produkcją.

Decyzja inwestycyjna (FID): moment, w którym inwestor przeznacza pieniądze na budowę. Wszystko wcześniej jest zapowiedzią.

Umowa odbioru (offtake): zobowiązanie odbiorcy do kupna określonego wolumenu po określonej cenie. Bez niej banki nie finansują projektu.

Reforming parowy (SMR): reakcja metanu z parą wodną w wysokiej temperaturze. Podstawowa metoda produkcji wodoru na świecie i źródło jego emisyjności.

DRI: redukcja bezpośrednia rudy żelaza – wytwarzanie żelaza gąbczastego bez wielkiego pieca. Reduktorem może być gaz ziemny albo wodór.

Kruchość wodorowa: utrata plastyczności stali wskutek wnikania atomów wodoru w jej strukturę. Powód, dla którego istniejących rurociągów nie da się użyć bez przeróbki.

dzięki uruchomieniu dużych instalacji w Chinach. Chińskie elektrolizery kosztują ułamek ceny zachodnich. Jeżeli powtórzy się scenariusz znany z fotowoltaiki i akumulatorów – a już raz i drugi się powtórzył – to rachunek, który dziś nie wychodzi, za dekadę może wyglądać inaczej. Chiny są jednym z dwóch krajów realizujących swoje cele wodorowe.

Druga niewiadoma to przepisy. Unijne wymogi wobec wodoru odnawialnego uznano powszechnie za tak restrykcyjne, że hamują to, co miały wspierać. Analitycy Wood Mackenzie przewidują, że państwa członkowskie porzucą cel 42 procent wodoru odnawialnego w przemyśle do 2030 roku, a Komisja już wiosną 2026 roku zapowiedziała rewizję kryteriów. Cel, który zostaje po cichu zdjęty, jest w tej dziedzinie zdarzeniem równie ważnym jak nowa inwestycja.

Trzecia to wodór naturalny – ten wydobywany z ziemi zamiast wytwarzanego. Jeśli okaże się, że da się go pozyskiwać w skali przemysłowej, cała powyższa arytmetyka idzie do kosza, bo znika najdroższy element łańcucha. Na razie jednak jesteśmy na etapie odwiertów poszukiwawczych, a ryzyko suchych odwiertów, niskiej czystości gazu i zbyt małej wydajności złóż pozostaje podstawową barierą. To jest właśnie ten rodzaj niepewności, dla którego istnieje ta rubryka: nie wiadomo, czy patrzymy na ślepy zaułek, czy na dziedzinę przed przełomem.

Co można powiedzieć z pewnością? Że gospodarka wodorowa w wersji z 2003 roku – wodór w każdym samochodzie, w każdym piecu, w każdej sieci – nie powstanie. Że wodór zostaje tam, gdzie jest surowcem, i odchodzi stamtąd, gdzie miał być paliwem. I że polska lekcja jest w tym wszystkim najbardziej konkretna: sto pięćdziesiąt autobusów kupionych za stuprocentową dotację i przetarg na paliwo bez ani jednej oferty to nie porażka technologii. To porażka założenia, że dotacja wystarczy zamiast rynku.

(red)

Bibliografia.

1. International Energy Agency (2026). Global Hydrogen Review 2026. Paris: IEA. Rozdziały: Demand, Production, Policy, Investment and innovation, Key questions about hydrogen. iea.org
2. Chemistry World (21.05.2026). Clean hydrogen project cancellations point to narrower future – bilans zdolności produkcyjnych z decyzją inwestycyjną wobec anulowanych w 2025 r.
3. ING Think (22.01.2026). Hydrogen stuck in the pilot phase – liczba projektów w fazie planów wobec projektów finansowanych.
4. Wood Mackenzie/Global Hydrogen Review (09.01.2026). Hydrogen: 5 things to look for in 2026 – prognoza porzucenia unijnego celu 42 % oraz odwrotu projektów bliskowschodnich.
5. Komisja Europejska (07.05.2026). Wyniki trzeciej aukcji Europejskiego Banku Wodoru: 9 projektów, 1,09 mld €, 1,1 GW; zakres dopłat 0,44–3,49 €/kg. energy.ec.europa.eu
6. Komisja Europejska (20.01.2026). Podpisanie umów z drugiej aukcji: 6 projektów, 270,6 mln €, 381,25 MW.
7. pv magazine (07.05.2026). EU allocates 1.1 GW of electrolyzer capacity in third hydrogen auction – 58 ofert z 11 krajów.
8. Fuel Cells Works (20.03.2026). European Hydrogen Bank's third auction draws €8.4bn in bids – skala nadsubskrypcji.
9. gasworld (08.05.2026). Third European Hydrogen Bank round selects nine projects – terminy decyzji inwestycyjnej i uruchomienia narzucone beneficjentom.
10. EnkiAI/analiza branżowa (07.2026). BP hydrogen 2026 – anulowanie projektu H2 Kwinana (44 t/dobę) i odpisy koncernu.
11. gasworld (2026, aktualizacja). ArcelorMittal freezes green hydrogen DRI projects – zamrożenie instalacji mimo przyznanych 3,5 mld € dotacji.
12. Strategic Energy Europe (2026). Analiza wstrzymania projektów ArcelorMittal – próg opłacalności wodoru dla hutnictwa na poziomie 2–3 €/kg.
13. Steel on the Net (09.07.2026). The hydrogen mirage: why green steel timelines keep slipping – przesunięcia harmonogramu zakładu Stegra w Boden.
14. EnkiAI (24.04.2026). Green steel projects Europe – Stegra (740 MW elektrolizerów), pierwsza dostawa zielonego DRI do Europy w lutym 2026 r., anulowanie projektu Cleveland-Cliffs.
15. CleanTechnica (2025–2026). Analizy upadłości w segmencie transportu wodorowego: Nikola, Hyzon, Quantron, Hyvia; odwołanie prezesa Air Products.
16. Jalopnik/AOL (07.2026). Why companies that make hydrogen-powered semi trucks keep going belly up – stan projektów ciężarówek wodorowych, zapowiedź 100 sztuk Mercedes-Benz NextGenH2.
17. CarBuzz (2025) oraz Autonocion (03.2026). Sprzedaż Toyoty Mirai, liczba stacji tankowania w USA, pozew zbiorowy na 5,7 mld USD.
18. CEE Bankwatch Network, Polska Zielona Sieć (23.06.2026). Autobusy wodorowe w Polsce: co poszło nie tak? – raport źródłowy dla części krajowej. zielonasiec.pl
19. Polska Agencja Prasowa (23.06.2026). Komunikat o raporcie: poziomy dotacji, koszty eksploatacji, przypadki Rzeszowa i Wrocławia.
20. rybnik.com.pl (29.06.2026). Omówienie raportu w części dotyczącej Rybnika: przetarg bez ofert, umowa na wodór z Konina, rozważana własna instalacja.
21. RaportCSR (26.06.2026). Zestawienie problemów eksploatacyjnych: zanieczyszczone paliwo w Poznaniu i Wałbrzychu, mrozy w Chełmie, tankowanie floty z Tychów w Katowicach.
22. Orlen (06.2026). Komunikat o uruchomieniu siódmej ogólnodostępnej stacji wodorowej w Gdyni; parametry dostaw i cele grupy do 2035 r. orlen.pl
23. Orlen (04.2026). Komunikat o stacji w Płocku – moc elektrolizerów ok. 0,9 GW i 130 tys. ton wodoru do 2035 r.
24. gasHD.eu (2024, materiał archiwalny). Zapis wcześniejszych celów Grupy Orlen: ok. 1 GW elektrolizerów i ponad 130 tys. ton rocznie „na koniec obecnej dekady".
25. Einride/prof. David Cebon, University of Cambridge (2023, aktualizacja 2026). Bilans sprawności łańcucha energetycznego dla napędu wodorowego i bateryjnego.
26. U.S. Department of Energy (2023) oraz California Air Resources Board (2022). Sprawności elektrolizy, sprężania i ogniw paliwowych przyjęte do obliczeń na rys. 2.
27. Congressional Research Service (30.03.2026). The Section 45V Clean Hydrogen Production Credit, IF12602. Washington: Library of Congress – wysokość ulgi, progi emisyjne i zmiany wprowadzone ustawą P.L. 119-21 z 4 lipca 2025 r. congress.gov

Oddajemy cześć kobietom, które odegrały wybitną rolę w rozwoju techniki i nauk ścisłych

Stephanie Kwolek

Chemiczka, która nie wylała „zepsutego” roztworu

1. Stephanie Kwolek w laboratorium DuPont, ok. 1965. Źródło: Wikimedia Commons, Science History Institute

Był rok 1965. W laboratorium DuPont w Wilmington Stephanie Kwolek mieszała mętny, mleczny roztwór polimeru. Każdy inny chemik wylałby go do zlewu – wyglądał jak zepsuty. Kwolek miała inne zdanie. Nalegała, żeby technik i tak przeprowadził test wytrzymałości włókna. Wyniki przerosły wszelkie oczekiwania. Material, który wyglądał jak pomyłka, okazał się pięć razy mocniejszy od stali. Dostał nazwę Kevlar i uratował życie ponad milionowi ludzi.

Córka polskich imigrantów, która chciała leczyć ludzi

Stephanie Louise Kwolek urodziła się 31 lipca 1923 roku w New Kensington w Pensylwanii, w rodzinie polskich imigrantów. Ojciec John pracował w hucie – był robotnikiem, ale zapalonym miłośnikiem przyrody. Zanim Stephanie skończyła dziesięć lat, zabierał ją na spacery po lesie, uczył rozpoznawać rośliny i obserwować owady. Zaszczepił w niej ciekawość świata, której nigdy nie straciła.

Ojciec zmarł, gdy Stephanie miała dziesięć lat. Matka Nellie – krawcowa z zamiłowania – wychowywała ją i brata sama. To od matki Kwolek przejęła miłość do tkanin, faktur i własnoręcznego szycia. Połączenie zainteresowania materiałami z umiłowaniem chemii i biologii okazało się po latach idealnym fundamentem kariery.

Studiowała na Carnegie Institute of Technology – dziś Carnegie Mellon University w Pittsburghu. Wybrała chemię, choć marzyła o medycynie. Dyplom z chemii zrobiła w 1946 roku i poszła do pracy w DuPont – tymczasowo, jak myślała, żeby zaoszczędzić na studia medyczne. Została czterdzieści lat.

DuPont i świat polimerów

DuPont był w 1946 roku jedną z najpotężniejszych firm chemicznych świata. Podczas II wojny światowej producent m.in. nylonu i neoprenu zaopatrywał armię w syntetyczne materiały,

2. Kamizelka kuloodporna z kevlaru, współczesna. Źródło: Wikimedia Commons, Autorstwa PMullahaa – Praca własna, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=37956474

a teraz wracał do rywalizacji o rynek cywilny. Kwolek trafiła do działu badań włókien w Buffalo. Miała szukać lżejszych i mocniejszych polimerów na potrzeby przemysłu – między innymi do produkcji opon, które pochłaniały ogromne ilości stali.

Jako jedna z nielicznych kobiet-chemiczek w firmie, szybko wykazała się talentem do cierpliwej, precyzyjnej pracy laboratoryjnej. Przeszła kolejne awanse i trafiła do Pioneering Research Laboratory w Wilmington w Delaware – miejsca, gdzie DuPont dawał naukowcom wolność eksperymentowania. Kwolek skupiła się na polimerach aromatycznych zwanych aramidami.

Jak to działa: polimer ciekłokrystaliczny

Zwykłe polimery to długie, splątane łańcuchy cząsteczek – jak garść spaghetti wrzucona do garnka. W roztworze ustawiają się chaotycznie, a włókno z nich powstałe jest stosunkowo miękkie.

Aramidy takie jak Kevlar mają w łańcuchach sztywne pierścienie benzenowe. W odpowiednim rozpuszczalniku i stężeniu te łańcuchy ustawiają się równolegle – jak patyczki do jedzenia ułożone w pęczek. To właśnie zobaczyła Kwolek: roztwór ciekłokrystaliczny, pierwszy tego typu w historii chemii.

Gdy taki roztwór przepuszcza się przez dyszę i rozciąga, łańcuchy zostają „zamrożone" w ułożeniu równoległym. Powstaje włókno, w którym wszystkie cząsteczki ciągną w tym samym kierunku. To dlatego Kevlar jest tak wyjątkowo mocny: siła rozciągająca rozkłada się na miliardy cząsteczek działających jednocześnie.

Efekt: Kevlar jest pięć razy mocniejszy od stali przy tej samej masie. Nie rdzewieje, jest odporny na ciepło do ok. 500°C i nie topi się – rozkłada się termicznie. Nie tłumi energii uderzenia tak jak stal – „rozprowadza" ją po całej powierzchni tkaniny.

Mętny roztwór, którego nikt nie chciał

W 1965 roku Kwolek pracowała nad polimerami, które mogłyby zastąpić stal w oponach samochodowych – lżejszy materiał oznaczałby mniejsze zużycie paliwa. Jedna z syntez dała niespodziewany rezultat: zamiast typowego, przejrzystego roztworu przypominającego melasę, w zlewce pojawiła się cienka, mętna, mleczna ciecz. Wlewała się jak woda.

W laboratorium obowiązywała niepisana reguła: jeśli roztwór jest mętny – jest zanieczyszczony, wyrzuć go. Technicy odmawiali przeprowadzenia testu przędzenia na tak wyglądającym materiale – bali się, że zniszczą precyzyjny sprzęt. Kwolek twardo obstawała przy swoim: „Było w tym coś innego. Pomyślałam, że może być bardzo użyteczne" – wspominała po latach.

Po kilku dniach namawiania technik Charles Smullen zgodził się. Sprzęt przeżył. Włókno też – i wykazało twardość oraz sztywność, jakich nikt wcześniej nie widział w syntetycznym materiale. Kwolek pobiegła po przełożonego.

Zastosowania kevlaru – od kamizelki do kosmosu

Ten pobiegł po kolejnego. Nikt nie mógł uwierzyć w wyniki.

Sześć lat od zlewki do rynku

Od odkrycia do komercjalizacji minęło sześć lat. DuPont musiał opracować metody masowej produkcji włókna z polimerów ciekłokrystalicznych – to wymagało zupełnie nowego podejścia do przędzenia. Kwolek pracowała w zespole razem z Herbertem Bladesem, Paulem Morganem i Josephem Riversem. „Okazało się to wielkim wysiłkiem zespołowym w finale" – mówiła skromnie.

Kobiety chemii: Stephanie Kwolek: https://youtu.be/L1pepaAdkWA

Życie i osiągnięcia chemiczki Stephanie Kwolek, wynalazczyni kevlaru

W 1971 roku DuPont opatentował Kevlar pod pełną nazwą chemiczną poli-p-fenylenotereftaloamid. Pierwsze komercyjne zastosowanie było zaskakująco przyziemne: opony rowerowe i samochodowe. Kevlarowe kordy oponowe były lżejsze i mocniejsze od stalowych.

Kamizelka, która zmieniła policję

W połowie lat 70. lekki Kevlar trafił do zupełnie nowego zastosowania: kamizelek ochronnych dla funkcjonariuszy policji. Richard Davis, twórca firmy Second Chance, w 1971 roku sam przeżył napad z bronią i postanowił skonstruować lżejszą alternatywę dla ówczesnych pancerzy – ciężkich, stalowych, których nikt nie chciał nosić na co dzień.

Pierwsza kamizelka z Kevlaru dla policji weszła do służby w 1975 roku. Przez następną dekadę tysiące funkcjonariuszy w USA zaczęło nosić je rutynowo. Szacuje się, że do dziś kamizelki z Kevlaru uratowały życie ponad milionowi ludzi na całym świecie – policjantów, żołnierzy, pracowników ochrony i cywilów. To liczba, której

żadna inna chemia organiczna z XX wieku nie może się równać.

Kevlar trafił szybko dalej: hełmy wojskowe, kombinezony strażackie, rękawice ochronne dla pracowników tartaków, kadłuby łodzi, kable światłowodowe, elementy Międzynarodowej Stacji Kosmicznej, skrzydła samolotów, rakiety tenisowe, żagle wyścigowe i buty trekkingowe. Dziś roczna sprzedaż przekracza miliard dolarów.

Nagrody bez Nobla

DuPont opatentował Kevlar jako własność firmy – Kwolek jako pracownica przeniosła prawa do wynalazku na pracodawcę i nie uczestniczyła finansowo w sukcesie, który przyniósł firmie miliardy. Tak działała większość umów o pracę w branży chemicznej w tamtych latach.

Pracowała w DuPont do 1986 roku. Po przejściu na emeryturę pozostała aktywna: konsultowała, prowadziła wykłady na uczelniach i angażowała się w programy edukacyjne dla dziewcząt zainteresowanych naukami ścisłymi.

Nagrody przychodziły stopniowo. W 1980 roku Chemical Pioneer Award. W 1994 roku – przyjęcie do National Inventors Hall of Fame: jako czwarta kobieta w historii tej instytucji. W 1996 roku National Medal of Technology and Innovation – najwyższe odznaczenie techniczne USA, przyznane przez prezydenta Clintona. W 1997 roku prestiżowy Perkin Medal Towarzystwa Chemicznego. Nagrody Nobla nigdy nie otrzymała.

Co zostało po Kwolek

Stephanie Kwolek zmarła 18 czerwca 2014 roku w Talleyville w Delaware. Miała 90 lat. Do końca pozostawała w kontakcie ze środowiskiem chemicznym i cierpliwie odpowiadała na listy młodych naukowców.

Jej historia jest przede wszystkim historią ciekawości, która nie daje się zniechęcić. Gdyby posłuchała panującej reguły i wylała „zepsuty" roztwór – Kevlar mógł powstać o lata później, w innym laboratorium, pod innym nazwiskiem. Kwolek go nie wylała, bo była przekonana, że coś jest nie tak jak zwykle. A coś niezwykłego warto zbadać.

Gdy pytano ją, co czuje, wiedząc, że wynalazek uratował milion istnień, odpowiadała spokojnie: „Jestem po prostu bardzo wdzięczna, że dano mi możliwość odkrycia czegoś tak użytecznego". Żaden inny komentarz nie był potrzebny. ■

Paweł Biernacki

3. Stephanie Kwolek z National Medal of Technology.
Źródło: Wikimedia Commons, Science History Institute

Dlaczego jej nie znasz?

Kevlar jest wszędzie – w kamizelkach policjantów, w butach górskich, w rakietach tenisowych, na Stacji Kosmicznej. A nazwisko Kwolek niemal nigdzie. Przyczyny są znane: kobiety-naukowcy przez dekady nie trafiały do podręczników i artykułów popularnonaukowych tak regularnie jak mężczyźni.

Było też coś specyficznego dla jej przypadku: Kevlar jest produktem firmy, nie osoby. DuPont przez lata promował „Kevlar" jako markę, nie „Stefanie Kwolek" jako wynalazczynię. W przemyśle chemicznym i materiałoznawstwie – inaczej niż w fizyce czy biologii – sława odkrywcy rzadko przekracza mury laboratorium.

Kwolek dostała tytuł honoris causa, medale i wejście do kilku Hall of Fame. Nie dostała Nobla, nie ma jej w podręcznikach szkolnych. Filmu o jej biografii nie nakręcono. Zmienia się to powoli – jej postać pojawia się w materiałach edukacyjnych dla dziewcząt zainteresowanych STEM. Może za późno. Ale lepiej późno niż wcale.

Q-DAY

Wyścig, którego zegar już tyka

Rozdział 1.

Zegar Mosca

Q-Day – dzień kwantowy – to umowna nazwa chwili, w której powstanie komputer kwantowy dostatecznie duży, by złamać szyfry chroniące dziś bankowość, pocztę, podpis elektroniczny i całą resztę internetu. Najważniejszą liczbą w tej historii nie jest jednak liczba kubitów. Jest nią pewna nierówność z trzema literami, którą można rozpisać na serwetce. Zanim do niej dojdziemy, trzeba zrozumieć, co dokładnie jest zagrożone – bo popularne wyobrażenie „komputer kwantowy złamie wszystkie szyfry" jest fałszywe. Jedne zabezpieczenia padną w całości, inne ani drgną.

1.1. Dwa algorytmy z lat dziewięćdziesiątych

Wiosną 1994 roku Peter Shor, matematyk pracujący wówczas w Bell Labs, przedstawił algorytm rozkładający duże liczby na czynniki pierwsze. Dwa lata później Lov Grover, z tych samych laboratoriów, pokazał algorytm przeszukiwania zbioru możliwości metodą prób i błędów – tyle że znacznie szybciej, niż potrafi to zwykły komputer.

Rozkład na czynniki pierwsze brzmi niewinnie. Piętnaście to trzy razy pięć, każdy to policzy w pamięci. Ale liczba używana w kluczu bankowym ma 617 cyfr. Dla zwykłego komputera znalezienie jej dwóch dzielników jest zadaniem beznadziejnym: wszystkie maszyny świata pracujące razem potrzebowałyby na to więcej czasu, niż istnieje Wszechświat. Na tej właśnie beznadziei zbudowano całe współczesne bezpieczeństwo

cyfrowe. Zaszyfrować jest łatwo, odszyfrować bez klucza – praktycznie niemożliwe.

Shor pokazał, że dla komputera kwantowego to zadanie przestaje być beznadziejne. Nie „staje się szybsze" – zmienia charakter. Zamiast wieczności: godziny albo dni.

Różnica między algorytmem Shora a algorytmem Grovera decyduje o wszystkim, co przeczytacie w tym numerze.

Algorytm Shora uderza dokładnie w dwa problemy matematyczne, na których opiera się cała dzisiejsza kryptografia klucza publicznego – czyli ta, która pozwala dwóm nieznajomym umówić się na wspólny sekret przez otwartą sieć. Pierwszy z nich to właśnie rozkład na czynniki pierwsze. Drugi nazywa się **logarytmem dyskretnym** i jest w gruncie rzeczy tym samym kłopotem w innym przebraniu: łatwo obliczyć wynik pewnego działania powtórzonego wiele razy, ale mając wynik, praktycznie nie sposób odgadnąć, ile razy je powtórzono.

Algorytm Grovera jest znacznie łagodniejszy. Służy do zgadywania hasła metodą sprawdzania po kolei wszystkich możliwości – z tym że komputer kwantowy potrzebuje na to pierwiastka z liczby prób. Zamiast miliarda sprawdzeń wystarczy około trzydziestu dwóch tysięcy. Brzmi groźnie, ale w praktyce oznacza tylko tyle, że klucz o długości 128 bitów zachowuje się jak klucz 64-bitowy. Odpowiedź jest równie prosta: używać kluczy 256-bitowych. Żadnej rewolucji, jedna linijka w konfiguracji.

Warto zatrzymać się na dolnych trzech wierszach, bo obalają dwa najczęstsze nieporozumienia. Po pierwsze: szyfrowanie samego pliku czy dysku nie jest głównym problemem – tu wystarczy dłuższy klucz. Po drugie – do czego wrócimy w rozdziale piątym – komputer kwantowy nie zagraża wydobyciu bitcoinów, bo wydobycie opiera się na funkcji skrótu SHA-256, a ta pozostaje bezpieczna.

Zagrożone jest coś innego i znacznie gorszego: **cała infrastruktura zaufania**. Certyfikaty TLS (*Transport Layer Security* – protokół, dzięki któremu w pasku przeglądarki widać kłódkę), podpis elektroniczny, sieci VPN (*Virtual Private Network* – szyfrowany tunel do firmowej sieci), zdalny dostęp SSH (*Secure Shell*), uwierzytelnianie urządzeń, podpisywanie aktualizacji oprogramowania. Wszystko, co pozwala dwóm stronom, które nigdy się nie spotkały, ustalić wspólny sekret i sprawdzić, z kim właściwie rozmawiają.

1.2. Maszyny zaszumione i maszyny groźne

Zacznijmy od podstawowego pojęcia. Zwykły komputer operuje bitami: każdy jest zerem albo jedynką. Komputer kwantowy operuje kubitami (od angielskiego *quantum bit*), które do momentu odczytu mogą znajdować się w obu stanach naraz. Pojedynczą operację na kubitach nazywa się bramką kwantową – to odpowiednik jednej instrukcji procesora.

Problem polega na tym, że kubity są rozpaczliwie delikatne. Drgnienie temperatury, pole magnetyczne, przypadkowy foton – i informacja przepada. Każda bramka wykonuje się z pewnym prawdopodobieństwem błędu, a błędy się kumulują. Dlatego dzisiejsze maszyny potrafią wykonać najwyżej kilkaset operacji, zanim obliczenie zamieni się w szum.

W 2018 roku John Preskill z Caltechu ukuł termin, który do dziś opisuje stan faktyczny: **NISQ** – *Noisy Intermediate-Scale Quantum*, czyli maszyny kwantowe zaszumione, średniej skali. Od kilkudziesięciu do ponad tysiąca kubitów,

Co znaczy „czas wielomianowy" i dlaczego to jest cała różnica

Matematycy dzielą zadania obliczeniowe według tego, jak szybko rośnie ich trudność, gdy rośnie sam problem.

Zadanie wielomianowe robi się trudniejsze umiarkowanie. Podwojenie długości liczby zwiększa nakład pracy kilka albo kilkanaście razy – nieprzyjemnie, ale do przeżycia. Mnożenie dwóch liczb jest właśnie takie: pomnożenie liczb tysiąccyfrowych trwa dłużej niż dwucyfrowych, ale wciąż ułamek sekundy.

Zadanie wykładnicze robi się trudniejsze katastrofalnie. Każda dodana cyfra podwaja nakład pracy. Po stu cyfrach jesteśmy poza zasięgiem czegokolwiek, co da się zbudować – i to niezależnie od tego, jak szybkie będą procesory za sto lat.

Rozkład dużej liczby na czynniki pierwsze jest dla zwykłego komputera zadaniem praktycznie wykładniczym. Algorytm Shora czyni go dla komputera kwantowego zadaniem wielomianowym. To nie jest różnica ilościowa. To jest różnica między „nigdy" a „w ten weekend".

Tabela 1.1. Co pada, co słabnie, co przeżyje

Mechanizm	Do czego służy	Los po Q-Day
RSA (od nazwisk twórców: Rivest, Shamir, Adleman)	uzgadnianie kluczy i podpis cyfrowy; szyfr serwerów i bankowości	**ZŁAMANY (Shor)**
ECDSA, EdDSA (podpisy na krzywych eliptycznych)	podpis cyfrowy, dowód własności portfela kryptowalutowego	**ZŁAMANY (Shor)**
ECDH, Diffie-Hellman (uzgadnianie klucza)	ustalenie wspólnego sekretu na czas jednego połączenia	**ZŁAMANY (Shor)**
AES-128 (*Advanced Encryption Standard*, klucz 128-bitowy)	szyfrowanie samych danych i plików	osłabiony – działa jak klucz 64-bitowy (Grover)
AES-256 (ten sam szyfr, klucz dwa razy dłuższy)	szyfrowanie samych danych i plików	**BEZPIECZNY**
SHA-256, SHA-3 (*Secure Hash Algorithm* – funkcje skrótu)	cyfrowe „odciski palca" danych, wydobycie kryptowalut	**BEZPIECZNE**

bez mechanizmu naprawiania błędów, zdolne do krótkich i wąsko wyspecjalizowanych obliczeń. Efektowne w laboratorium, nieszkodliwe dla kryptografii.

Na drugim końcu skali jest **CRQC** – *Cryptographically Relevant Quantum Computer*, komputer kwantowy istotny kryptograficznie. Czyli taki, który realnie łamie szyfry. Wymaga tysięcy kubitów logicznych – a to zupełnie co innego niż kubity, którymi chwalą się komunikaty prasowe.

Różnica jest sednem sprawy i jednocześnie miejscem, w którym najczęściej myli się prasa. Skoro pojedynczego kubitu nie da się uchronić przed błędem, buduje się z wielu kubitów sprzętowych – nazywamy je fizycznymi – jeden kubit odporny na zakłócenia, zwany logicznym. Kubity fizyczne układa się w siatkę i splata ze sobą tak, że część z nich przechowuje informację, a część nieustannie sprawdza sąsiadów i sygnalizuje, gdzie coś poszło nie tak. Taki układ nazywa się kodem korekcyjnym; najpopularniejszy z nich, ze względu na płaską siatkę, nosi nazwę kodu powierzchniowego.

Cena jest wysoka. Na jeden kubit logiczny potrzeba od około dwóch do stu kubitów fizycznych – zależnie od architektury i od tego, jak rzadko mylą się bramki. Dlatego zdanie „firma X ma 6100 kubitów" nie mówi nic, dopóki nie wiadomo, o które kubity chodzi – logiczne czy fizyczne.

Skalę dystansu do CRQC i tempo, w jakim ten dystans się kurczy, pokazują trzy daty:

- **2019** Craig Gidney i Martin Ekerå szacują, że złamanie klucza RSA-2048 wymaga 20 milionów kubitów fizycznych i zajmie 8 godzin.
- **maj 2025** Ten sam Gidney, już w firmie Google Quantum AI, publikuje nowy szacunek: mniej niż milion kubitów fizycznych i mniej niż tydzień obliczeń. Dwudziestokrotna redukcja sprzętu, okupiona dłuższym czasem pracy.
- **marzec 2026** Zespół Google, wspólnie z fundacją Ethereum i Danem Bonehem

Migracja z RSA na krzywe eliptyczne nie pomaga

Kryptografia krzywych eliptycznych – w skrócie ECC, od angielskiego Elliptic Curve Cryptography – bywa reklamowana jako nowocześniejsza i bezpieczniejsza od RSA. Przy znacznie krótszym kluczu daje ten sam poziom ochrony przed komputerem zwykłym i dlatego wyparła RSA z telefonów, kart płatniczych i kryptowalut.

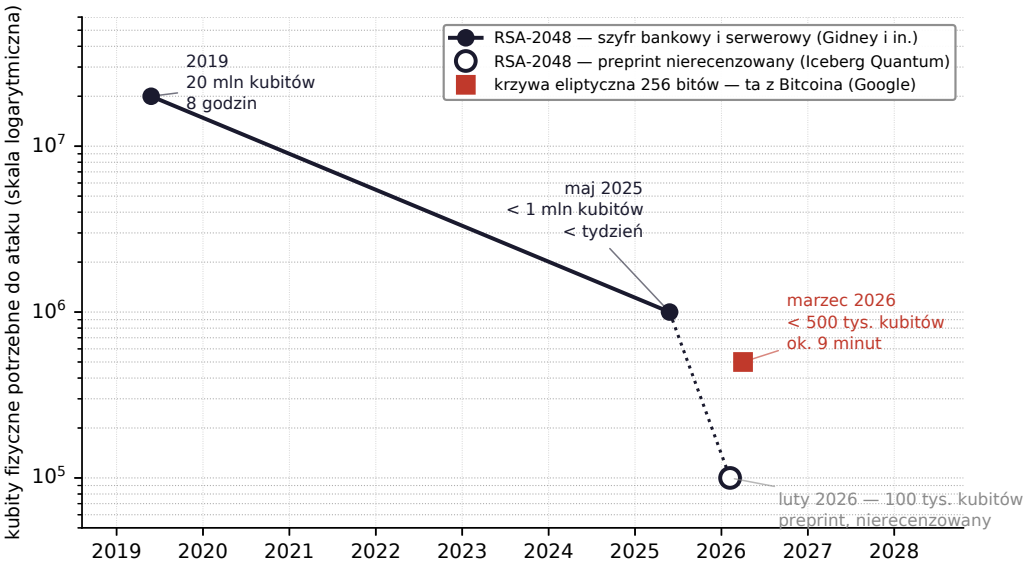
Wobec algorytmu Shora obie padają tak samo, bo rozkład na czynniki pierwsze i logarytm dyskretny to dla niego dwa warianty tego samego zadania. Co gorsza, **krzywe eliptyczne padają wcześniej**: złamanie klucza 256-bitowego wymaga według szacunków Google z marca 2026 roku około stukrotnie mniej operacji niż złamanie RSA z kluczem 2048-bitowym. Kto w 2020 roku przechodził z RSA na krzywe eliptyczne „na zapas", zrobił dobrą rzecz z niewłaściwego powodu i nie kupił sobie ani roku.

Rysunek 1.1. Jak z kubitów fizycznych powstaje jeden kubit logiczny. Czterdzieści dziewięć elementów sprzętowych przechowuje wspólnie jedną informację odporną na błędy: wypełnione kółka niosą treść, puste na bieżąco kontrolują sąsiadów. „Dystans 7" oznacza szerokość siatki – im większy, tym lepsza ochrona i tym więcej sprzętu. Podane po prawej proporcje dotyczą trzech konkurujących technologii budowy kubitu; opisujemy je w rozdziale drugim

z Uniwersytetu Stanforda, szacuje złamanie 256-bitowego klucza na krzywej eliptycznej na poniżej 500 tysięcy kubitów fizycznych – w około dziewięć minut.

Każda z tych liczb ma jednak drobnym drukiem dopisane założenia: kubity ułożone w kwadratową siatkę i połączone tylko z najbliższymi sąsiadami, jedna bramka na tysiąc kończąca się błędem, sprawdzenie całej siatki co jedną milionową sekundy, reakcja układu sterującego w dziesięć milionowych sekundy. Bez tych warunków liczby nie znaczą nic. **Jeśli ktoś podaje wam liczbę kubitów potrzebnych do złamania szyfru i nie mówi przy tym, jak często mylą się bramki, podaje wam liczbę bez treści.**

Dla porządku: najszybsza dziś zapowiadana maszyna z pełną korekcją błędów, IBM Starling, ma w 2029 roku osiągnąć



Uwaga: punkty dotyczą różnych szyfrów i różnych architektur sprzętowych. Wszystkie szacunki zakładają błąd bramki 0,1%, cykl kodu powierzchniowego 1 µs i czas reakcji układu sterującego 10 µs. Bez tych założeń liczby nie są porównywalne.

Rysunek 1.2. Nie zbudowano ani jednej z tych maszyn. Kurczy się natomiast szacunek, jak duża musiałaby być. Punkt z lutego 2026 pochodzi z pracy, która nie przeszła jeszcze recenzji naukowej (architektura Pinnacle, oparta na nowej rodzinie kodów korekcyjnych zwanych qLDPC), i wymaga niezależnego potwierdzenia – zaznaczyliśmy go innym symbolem. Uwaga: punkty dotyczą różnych szyfrów

200 kubitów logicznych. To wciąż kilkanaście razy mniej, niż trzeba. Kierunek jest jednak jednoznaczny – i to on jest wiadomością, nie obecny poziom.

1.3. Nierówność, która załatwia sprawę

Michele Mosca, współzałożyciel Institute for Quantum Computing – instytutu obliczeń kwantowych na kanadyjskim Uniwersytecie Waterloo – sformułował kilkanaście lat temu regułę pozwalającą podjąć decyzję bez znajomości daty Q-Day. Wygląda tak:

X + Y ≥ Z

gdzie **X** to liczba lat, przez które dane muszą pozostać tajne, **Y** to liczba lat potrzebnych na wymianę szyfrów w całej organizacji, a **Z** to liczba lat, jakie zostały do powstania komputera łamiącego szyfry.

Jeżeli suma X i Y jest większa lub równa Z, **problem istnieje dzisiaj**, a nie w dniu Q-Day.

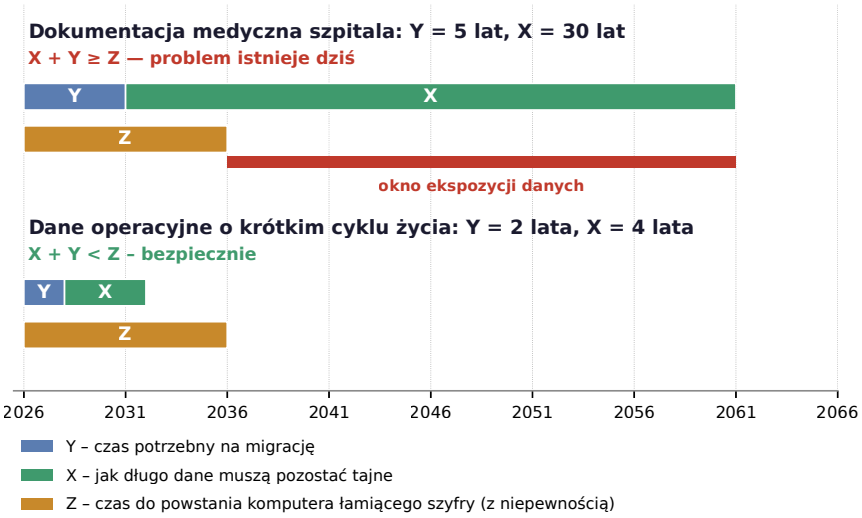
Podstawmy coś konkretnego. Elektroniczna dokumentacja medyczna polskiego pacjenta: X = 30 lat, bo mniej więcej tyle powinna pozostać tajemnicą. Wymiana szyfrów w dużym szpitalu wojewódzkim – w aparaturze, w systemie archiwizacji obrazów medycznych PACS (*Picture Archiving and Communication System*, czyli cyfrowym archiwum zdjęć rentgenowskich i tomografii) oraz w kopiach zapasowych sprzed lat: Y = 5 lat, przy założeniu, że ktoś się tym zajmie na poważnie. Razem 35.

Aby ten szpital był bezpieczny, Z musiałoby przekroczyć 35 lat – czyli komputer łamiący szyfry nie mógłby powstać przed rokiem 2061. Nie ma dziś eksperta, który podpisałby się pod taką prognozą.

Piękno reguły Mosca polega na tym, że **nie wymaga zgadywania daty**. Wystarczy stwierdzić, że Z jest z pewnością mniejsze niż 35 lat – a to jest bezpieczne stwierdzenie nawet dla największego sceptyka. Wniosek zapada bez rozstrzygania sporu o rok 2032 czy 2040.

Jak bardzo eksperci są zresztą niezgodni, pokazuje coroczna ankieta Global Risk Institute – kanadyjskiego instytutu badającego ryzyko w sektorze finansowym. W edycji z 2025 roku, opublikowanej w czerwcu 2026, dwudziestu sześciu specjalistów oceniło prawdopodobieństwo powstania komputera łamiącego szyfry na **28...49 procent w ciągu dziesięciu lat** i **51...70 procent w ciągu piętnastu**. Rok wcześniej te same pytania dawały 19...34 procent dla dekady.

Do tych liczb należy podchodzić z rezerwą, którą sami autorzy sygnalizują, a którą prasa zwykle gubi. Respondentów jest dwudziestu sześciu, z czego dwudziestu jeden pracuje w Ameryce Północnej i Europie. **Wśród ankietowanych nie ma nikogo z Chin**



Rysunek 1.3. Reguła Mosca w praktyce. Dopóki czas wymiany szyfrów i horyzont tajności danych kończą się przed powstaniem komputera łamiącego szyfry, organizacja jest bezpieczna. Gdy go przekraczają, powstaje okno ekspozycji – zaznaczone na czerwono – w którym archiwalne dane dają się odszyfrować, choć wysłano je jako zaszyfrowane

– czyli z kraju, który ten sam raport wskazuje jako mogący w ciągu pięciu lat dorównać Ameryce Północnej. Ankieta nie jest pomiarem. Jest zbiorem dobrze poinformowanych domysłów, z których część ma systematyczną lukę.

1.4. Scenariusz, który już się realizuje

Wszystko powyższe dotyczyło przyszłości. Jest natomiast jeden element tej układanki, który dzieje się teraz i którego nie da się cofnąć.

Nazywa się ***harvest now, decrypt later*** – zbieraj teraz, odszyfruj później; w skrócie HNDL. Mechanizm jest banalny: przeciwnik przechwytuje i zapisuje zaszyfrowany ruch, którego dziś nie potrafi odczytać, licząc na to, że odczyta go za dziesięć czy piętnaście lat. Pamięć masowa jest tania. Cierpliwość państwowych służb wywiadowczych jest w tej dziedzinie dobrze udokumentowana.

Holenderska AIVD (*Algemene Inlichtingen- en Veiligheidsdienst* – służba wywiadu i bezpieczeństwa), brytyjskie NCSC (*National Cyber Security Centre* – narodowe centrum cyberbezpieczeństwa, część agencji wywiadu GCHQ) i francuska ANSSI (*Agence nationale de*

SŁOWNICZEK – terminy używane w całym temacie numeru

Bit – najmniejsza porcja informacji w zwykłym komputerze: zero albo jedynka.

Kubit – kwantowy odpowiednik bitu; do chwili odczytu może być zerem i jedynką jednocześnie.

Bramka kwantowa – pojedyncza operacja wykonywana na jednym lub dwóch kubitach; mówimy o bramkach fizycznych albo logicznych, zależnie od poziomu opisu. Odpowiednik jednej instrukcji procesora, obarczony ryzykiem błędu.

Liczba bramek w obwodzie – ile operacji trzeba wykonać, żeby dane obliczenie doszło do końca. Jest cechą algorytmu, nie maszyny. Zapowiedź „sto milionów operacji" mówi o rozmiarze najdłuższego obwodu, jaki maszyna doprowadzi do końca, a nie o liczbie operacji na sekundę.

Czas jednej bramki – cecha sprzętu: od nanosekund w układach nadprzewodzących do dziesiątek mikrosekund w pułapkach jonowych. Czas obliczenia to w przybliżeniu liczba bramek pomnożona przez czas jednej bramki, powiększona o narzut cykli korekcji błędów.

Wierność bramki – odsetek operacji wykonanych bez błędu. Podawana zwykle dla bramek dwukubitowych; 99,9 procent oznacza jeden błąd na tysiąc operacji.

Czas wielomianowy – zadanie, którego trudność rośnie umiarkowanie wraz z rozmiarem problemu; przeciwieństwo zadania wykładniczego, które szybko staje się nierozwiązywalne.

Kubit fizyczny – pojedynczy element sprzętowy: obwód nadprzewodzący, jon w pułapce elektrycznej, atom przytrzymany wiązką lasera.

Kubit logiczny – jeden kubit odporny na błędy, zbudowany z wielu fizycznych połączonych kodem korekcyjnym. Dziś kosztuje od kilkudziesięciu do kilkuset kubitów fizycznych.

Kod powierzchniowy – najpopularniejszy sposób naprawiania błędów: kubity na płaskiej siatce, część liczy, część kontroluje sąsiadów.

Temperatura układu kubitowego – temperatura samego nośnika informacji, nie pomieszczenia ani obudowy. Instalacja z atomami neutralnymi stoi w zwykłej hali, ale atomy wewnątrz komory próżniowej mają temperaturę rzędu mikrokelwina.

CRQC – *Cryptographically Relevant Quantum Computer*; komputer kwantowy na tyle duży, by łamać dzisiejsze szyfry.

NISQ – *Noisy Intermediate-Scale Quantum*; obecna generacja maszyn: zaszumionych, średniej skali, bez korekcji błędów.

HNDL – *harvest now, decrypt later*; gromadzenie zaszyfrowanych danych z zamiarem odszyfrowania ich w przyszłości.

PQC – *post-quantum cryptography*, kryptografia postkwantowa: nowe szyfry odporne na atak kwantowy, działające na zwykłych komputerach.

QKD – *quantum key distribution*, kwantowa dystrybucja klucza: sprzętowa metoda uzgadniania klucza, wymagająca osobnego łącza światłowodowego.

Krypto-zwinność – zdolność organizacji do wymiany szyfru bez przebudowywania całej infrastruktury od zera.

Trzy daty, które trzeba znać

31 grudnia 2026 – wszystkie państwa Unii Europejskiej mają mieć krajową strategię przejścia na kryptografię postkwantową (PQC – post-quantum cryptography; nowe szyfry odporne na atak kwantowy, działające na zwykłych komputerach), wraz ze spisem miejsc, w których w ogóle używają szyfrowania. Polska przyjęła Strategię Cyberbezpieczeństwa RP na lata 2025–2029 w marcu 2026; plan wymiany szyfrów jest w niej przewidziany.

31 grudnia 2030 – w Unii infrastruktura krytyczna i zastosowania wysokiego ryzyka mają być już przestawione na nowe szyfry. W USA rozporządzenie wykonawcze prezydenta podpisane 22 czerwca 2026 roku ustala ten sam termin dla uzgadniania kluczy w kluczowych systemach federalnych, a **31 grudnia 2031** dla podpisów cyfrowych.

31 grudnia 2035 – domknięcie: w Unii dla pozostałych systemów, w Wielkiej Brytanii dla wszystkich, a w normach amerykańskiego NIST (*National Institute of Standards and Technology* – instytutu, który ustala światowe standardy szyfrowania) jako data, po której RSA i krzywe eliptyczne przestają być dozwolone.

Numer, który trzymacie w ręku, ukazuje się pięć miesięcy przed pierwszą z tych dat.

la sécurité des systèmes d'information – narodowa agencja bezpieczeństwa systemów informatycznych) wypowiadają się w tej sprawie zgodnie i bez ogródek: przechwytywanie danych z zamiarem późniejszego odszyfrowania jest **aktywną praktyką operacyjną**, a nie hipotezą z konferencji naukowej.

To odwraca całą logikę planowania. Jeśli wysyłacie dziś przez internet coś, co ma pozostać tajne w latach czterdziestych, to nie macie czasu do Q-Day. Nie macie go w ogóle – o tym, czy tajność tej konkretnej transmisji przetrwa, zdecydowaliście w chwili, gdy nacisnęliście „wyślij".

I to właśnie dlatego rządy nie czekają. ■

Peter Williston Shor (Fot. Autorstwa International Centre for Theoretical Physics – YouTube: https://www.youtube.com/watch?v=J-7HeDX_7Heg&t=7075 – Zobacz/zapisz zarchiwizowane wersje na archive.org oraz [$archivetoday archive.today], CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=75565986)

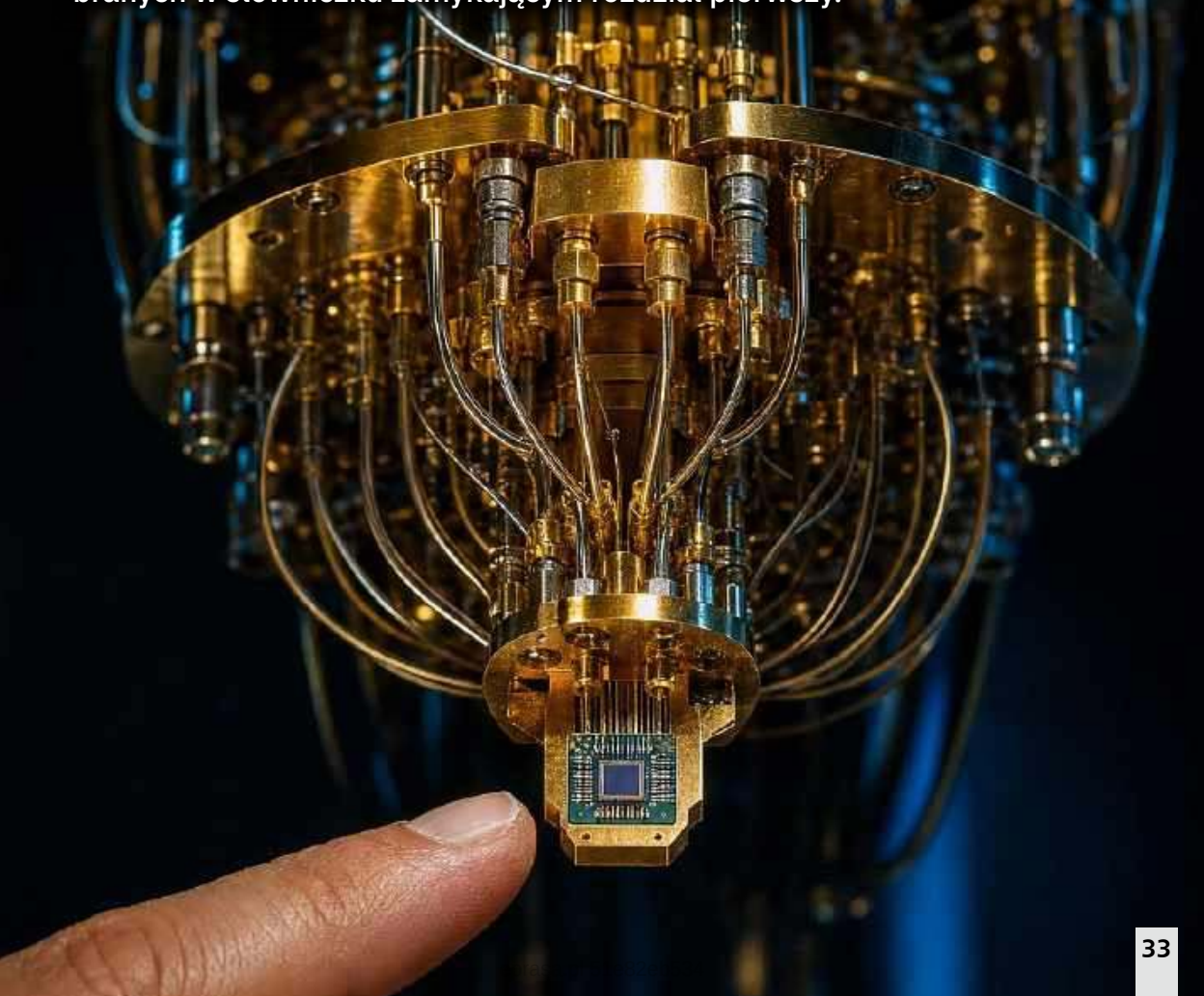
Bibliografia

[1] Shor P. W., Algorithms for Quantum Computation: Discrete Logarithms and Factoring, [w:] Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Santa Fe 1994, s. 124–134. DOI: 10.1109/SFCS.1994.365700.
[2] Grover L. K., A Fast Quantum Mechanical Algorithm for Database Search, [w:] Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96), ACM Press, Filadelfia 1996, s. 212–219. DOI: 10.1145/237814.237866. Preprint: arXiv:quant-ph/9605043.
[3] Google Quantum AI, Ethereum Foundation, Boneh D., Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations, Google, Santa Barbara, 30 marca 2026. https://quantumai.google/static/site-assets/downloads/cryptocurrency-whitepaper.pdf [dostęp: 4.08.2026].
[4] Preskill J., Quantum Computing in the NISQ Era and Beyond, „Quantum" 2018, t. 2, s. 79. DOI: 10.22331/q-2018-08-06-79.
[5] Gidney C., Ekerå M., How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits, „Quantum" 2021, t. 5, s. 433. DOI: 10.22331/q-2021-04-15-433.
[6] Gidney C., How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits, preprint arXiv:2505.15917 [quant-ph], 21 maja 2025. DOI: 10.48550/arXiv.2505.15917.
[7] Iceberg Quantum, The Pinnacle Architecture: Reducing the Cost of Breaking RSA-2048 to 100 000 Physical Qubits Using Quantum LDPC Codes, preprint arXiv:2602.11457 [quant-ph], 12 lutego 2026 – praca nierecenzowana.
[8] IBM Quantum, IBM Lays Out Clear Path to Fault-Tolerant Quantum Computing, blog IBM Quantum, Armonk 2025. https://www.ibm.com/quantum/blog/large-scale-ftqc [dostęp: 4.08.2026].
[9] Mosca M., Cybersecurity in an Era with Quantum Computers: Will We Be Ready?, „IEEE Security & Privacy" 2018, t. 16, nr 5, s. 38–41. DOI: 10.1109/MSP.2018.3761723.
[10] Mosca M., Piani M., Quantum Threat Timeline Report 2025, Global Risk Institute – evolutionQ, Toronto, czerwiec 2026. https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/ [dostęp: 4.08.2026].
[11] Kołodziejczyk J., Melaniuk T., Obara P., Ragankiewicz Z., Wyścig z Q-Day. Globalny stan przygotowań. Standardy, regulacje, strategie migracji do kryptografii postkwantowej, Instytut Łączności – Państwowy Instytut Badawczy, Warszawa, maj 2026.
[12] Agence nationale de la sécurité des systèmes d'information, Follow Up Position Paper on Post-Quantum Cryptography, ANSSI, Paryż, 21 grudnia 2023.
[13] NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, Komisja Europejska, Bruksela, czerwiec 2025. https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography [dostęp: 4.08.2026].
[14] Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks, The White House, Waszyngton, 22 czerwca 2026.
[15] National Institute of Standards and Technology, Transition to Post-Quantum Cryptography Standards, NIST IR 8547 ipd (wstępny projekt publiczny), Gaithersburg, listopad 2024. DOI: 10.6028/NIST.IR.8547.ipd.
[16] National Cyber Security Centre, Timelines for Migration to Post-Quantum Cryptography, NCSC, Londyn, marzec 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines [dostęp: 4.08.2026].
[17] Rada Ministrów, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029, Warszawa, przyjęta 10 marca 2026.

Rozdział 2.

Co naprawdę stoi w laboratoriach

Fotografia, która najczęściej towarzyszy doniesieniom o komputerach kwantowych – złocista konstrukcja z plątaniną rurek i kabli – nie przedstawia procesora. Przedstawia kriostat rozcieńczalnikowy, czyli urządzenie chłodzące. Procesor jest płytką wielkości paznokcia, przykręconą u samego dołu tej konstrukcji, w miejscu o najniższej temperaturze. Rozróżnienie to nie jest czepianiem się szczegółu. W tej dziedzinie niemal każde nieporozumienie bierze się z pomylenia dwóch podobnie brzmiących wielkości – dlatego w całym tym numerze trzymamy się znaczeń zebranych w słowniczku zamykającym rozdział pierwszy.



2.1. Pięć dróg do kubitu fizycznego

Nie wiadomo dziś, z czego zostanie ostatecznie zbudowany komputer kwantowy zdolny łamać szyfry. Konkuruje pięć odrębnych pomysłów na to, czym fizycznie ma być kubit fizyczny. Nie są to warianty jednej technologii, lecz pięć osobnych gałęzi inżynierii, korzystających z różnych działów fizyki, różnych materiałów i różnych metod wytwarzania. Żadna z nich nie odpadła i żadna nie wygrała.

Nadprzewodniki. Kubitem fizycznym jest tu obwód elektryczny wykonany z aluminium lub niobu, zawierający tak zwane złącze Josephsona – cienką przerwę izolacyjną, przez którą prąd przepływa dzięki zjawisku tunelowania. W takim obwodzie prąd może krążyć w obu kierunkach jednocześnie, i to właśnie ten stan przechowuje informację. Stanem steruje się impulsami mikrofalowymi, a odczytuje przez pomiar rezonatora sprzężonego z obwodem.

Warunkiem działania jest temperatura układu kubitowego rzędu 10...20 milikelwinów, czyli około stukrotnie niższa niż temperatura przestrzeni międzygwiezdnej. Uzyskuje się ją w kriostacie rozcieńczalnikowym, wykorzystującym mieszaninę dwóch izotopów helu. Zaletą tej drogi są najszybsze bramki w całej branży: operacja na parze kubitów fizycznych trwa od dwudziestu pięciu do stu nanosekund. Wadą jest okablowanie – każdy kubit fizyczny wymaga własnych linii sterujących wyprowadzonych na zewnątrz kriostatu, a każda taka linia doprowadza do wnętrza ciepło. Przy tysiącu kubitów fizycznych jest to trudny problem inżynierski. Przy milionie nikt nie zna rozwiązania i trwają prace nad sterowaniem wielokanałowym oraz układami kontrolnymi umieszczonymi wewnątrz samego kriostatu. Tą drogą idą IBM, Google, Rigetti i chiński USTC.

Jony w pułapkach. Kubitem fizycznym jest pojedynczy atom baru albo iterbu, pozbawiony

Dlaczego stan kwantowy jest tak ulotny

Superpozycja to nie „jedno i drugie naraz". Kubit nie przechowuje dwóch wartości obok siebie. Przechowuje jedną wielkość: ściśle określoną relację między możliwością zera a możliwością jedynki. Opisują ją dwie liczby – udział każdej z możliwości oraz przesunięcie fazowe między nimi. To właśnie faza niesie informację, na której opierają się algorytmy kwantowe, i to ona ginie najłatwiej.

Dekoherencja: otoczenie podgląda. Żeby zniszczyć taki stan, nikt nie musi patrzeć. Wystarczy, że kubit dozna oddziaływania z czymkolwiek – zabłąkanym fotonem podczerwonym, drganiem sieci krystalicznej, fluktuacją pola magnetycznego z sąsiedniego przewodu. Otoczenie unosi wtedy ze sobą strzępek informacji o tym, w jakim stanie był kubit, a to wystarczy: relacja fazowa przestaje być własnością samego kubitu i rozprasza się na zewnątrz. Informacja nie znika – przestaje być dostępna. Zjawisko to nazywa się dekoherencją i jest jedynym prawdziwym przeciwnikiem konstruktora.

Dlaczego tak zimno. Odstęp energetyczny między zerem a jedynką w kubicie nadprzewodzącym odpowiada energii mniej więcej dwudziestu mikroelektronowoltów. Energia drgań cieplnych w temperaturze pokojowej wynosi około dwudziestu sześciu milielektronowoltów – tysiąc dwieście razy więcej. W takich warunkach samo ciepło bez przerwy podrzucałoby kubit do stanu wzbudzonego i żadne obliczenie nie miałoby prawa się rozpocząć. Aby drgania cieplne przestały się liczyć, temperatura musi spaść do kilkunastu tysięcznych kelwina. Stąd biorą się kriostaty rozcieńczalnikowe – i stąd ta złocista konstrukcja ze zdjęć.

Nie każda technologia potrzebuje jednak tego samego. Jon w pułapce i atom w pęsecie optycznej są odizolowane próżnią, a nie zimnem; chłodzenie laserowe do mikrokelwinów służy tam do zatrzymania ruchu cząstki, a nie do wyciszenia jej poziomów energetycznych. Dlatego temperatur podawanych dla poszczególnych technologii nie wolno porównywać wprost: w jednym przypadku mówią o tłumieniu ciepła, w drugim o unieruchomieniu atomu.

Splątanie – i dlaczego to ta sama rzecz. Dwa kubity można wprowadzić w stan, którego nie da się opisać, opisując każdy z nich osobno. Nie znaczy to, że się ze sobą porozumiewają. Znaczy, że wyniki ich pomiarów są powiązane silniej, niż pozwala na to jakiekolwiek klasyczne uzgodnienie z góry. Splątanie jest właściwym źródłem mocy obliczeniowej tych maszyn i zarazem podstawą korekcji błędów: informację rozprasza się celowo po wielu kubitach fizycznych tak, aby żaden z osobna jej nie zawierał – i dzięki temu lokalne zakłócenie nie ma czego zniszczyć.

Warto zauważyć rzecz, którą łatwo przeoczyć: dekoherencja to nic innego jak splątanie z otoczeniem. To samo zjawisko, kontrolowane, daje komputer kwantowy, a niekontrolowane – rujnuje go. Cała inżynieria opisana w tym rozdziale sprowadza się więc do jednego zadania: splątać kubity ze sobą, nie splątując ich z resztą świata.

Nadprzewodniki

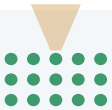
obwód z aluminium lub niobu, w którym prąd krąży w dwie strony naraz

temperatura układu kubitowego: **10–20 mK (kriostat rozcieńczalnikowy)**

Jony w pułapkach

atom baru lub iterbu pozbawiony elektronu, unieruchomiony polem elektrycznym

temperatura układu kubitowego: **jon: ok. 1 µK (chłodzenie laserowe)**



Atomy neutralne

obojętny atom cezu lub rubidu przytrzymany wiązką lasera — pęsetą optyczną

temperatura układu kubitowego: **atom: ok. 1 µK (chłodzenie laserowe)**

Fotonika

pojedynczy foton biegnący przez falowody w układzie scalonym z krzemu

temperatura układu kubitowego: **foton: bez temperatury; detektory 1–4 K**

Kubity topologiczne

stan zbiorowy układu nadprzewodnik–półprzewodnik, nie stan jednej cząstki

temperatura układu kubitowego: **poniżej 100 mK (kriostat rozcieńczalnikowy)**

Podana temperatura dotyczy nośnika informacji, nie pomieszczenia ani obudowy. Jony i atomy chłodzi się laserowo do mikrokelwinów wewnątrz komory próżniowej, która sama może mieć temperaturę otoczenia — w części instalacji z jonami komorę dodatkowo schładza się do kilkunastu kelwinów.

Rysunek 2.1. Pięć konkurujących odpowiedzi na pytanie, czym fizycznie jest kubit fizyczny. Podana temperatura dotyczy nośnika informacji, a nie pomieszczenia, w którym stoi aparatura

jednego elektronu i przez to naładowany dodatnio. Taki jon daje się utrzymać w próżni zmiennym polem elektrycznym wytwarzanym przez zestaw elektrod, a informację zapisuje się w dwóch poziomach energetycznych jego elektronów. Sterowanie i odczyt odbywają się wiązkami lasera.

Temperatura układu kubitowego to około jednego mikrokelwina – tyle wynosi energia ruchu jonu po schłodzeniu laserowym. Sama komora próżniowa może pozostać w temperaturze otoczenia, choć w części instalacji schładza się ją dodatkowo do kilkunastu kelwinów, aby ograniczyć drgania i osadzanie się zanieczyszczeń na elektrodach. Ta droga daje obecnie najwyższą jakość operacji: wierność bramek dwukubitowych sięga 99,9 procent, a każdy jon może zostać sprzęgnięty z każdym innym, bo jony przesuwa się wzdłuż pułapki między strefami roboczymi. Ceną jest szybkość – bramka trwa od dziesięciu do stu mikrosekund, czyli około tysiąc razy dłużej niż w nadprzewodnikach. Przy obliczeniu liczącym dziesiątki milionów bramek ta różnica przestaje być drobiazgiem i przekłada się wprost na czas pracy maszyny. Tą drogą idą Quantinuum i IonQ.

Atomy neutralne. Pomysł pokrewny, lecz bez odbierania elektronu: kubitem fizycznym jest cały, obojętny elektrycznie atom cezu lub rubidu, przytrzymywany w miejscu skupioną wiązką lasera, zwaną pęsetą optyczną. Metoda ta wywodzi się z prac nagrodzonych Nagrodą Nobla z fizyki w 2018 roku. Aby wykonać operację na parze atomów, wzbudza się je do stanu rydbergowskiego – takiego, w którym elektron krąży bardzo daleko od jądra, a atom rozdyma się do rozmiarów tysiąckrotnie większych niż zwykle i zaczyna oddziaływać z sąsiadem.

Temperatura układu kubitowego wynosi tu również około mikrokelwina i również pochodzi z chłodzenia laserowego; aparatura pracuje w warunkach zwykłego laboratorium. Zaletą jest

6100 kubitów fizycznych to jeszcze nie komputer

Rekord z Caltechu obiegł media jako „największy komputer kwantowy". Samo osiągnięcie jest prawdziwe i ważne, ale opis był mylący.

Zespół wykazał, że da się jednocześnie utrzymać ponad sześć tysięcy atomów, nie tracąc przy tym jakości sterowania pojedynczym atomem – dotąd sądzono, że jedno wyklucza drugie. To rekord skali, nie rekord mocy obliczeniowej.

Do komputera brakuje dwóch rzeczy: splątania tych atomów ze sobą w kontrolowany sposób oraz kompletu bramek, którymi dałoby się wykonać dowolne obliczenie. W układzie z Caltechu nie wykonywano operacji dwukubitowych. **Macierz 6100 atomów jest zatem bardzo dobrą pamięcią kwantową, a nie procesorem.**

skala i swoboda: atomy można przenosić w trakcie obliczenia, więc siatka połączeń nie jest zamrożona w krzemie. We wrześniu 2025 roku zespół z Caltechu opublikował w czasopiśmie „Nature" macierz 6100 atomów cezu, w której stan pojedynczego atomu utrzymywał się przez trzynaście sekund, a sterowanie udawało się z wiernością 99,98 procent. Trzynaście sekund to w tej dziedzinie bardzo dużo – nadprzewodnikowy kubit fizyczny traci swój stan po kilkudziesięciu mikrosekundach. Słabszym punktem są operacje na parach: ich wierność, rzędu 99,5 procent, wciąż ustępuje jonom.

Fotonika. Kubitem fizycznym jest pojedynczy foton biegnący przez falowody wytrawione w układzie scalonym. Informację zapisuje się w jego polaryzacji albo w tym, którą z dwóch dostępnych ścieżek foton wybrał. Największą zaletą jest wytwarzanie: takie układy powstają w zwykłych fabrykach półprzewodników, na tych samych liniach produkcyjnych co procesory krzemowe, co daje dostęp do dojrzałej technologii i dużych wolumenów.

Fotony nie mają temperatury w sensie, w jakim mają ją jony czy obwody nadprzewodzące, ale chłodzenia wymagają detektory pojedynczych fotonów, pracujące w temperaturze od jednego do czterech kelwinów. Zasadniczą trudnością jest to, że fotony niemal nie oddziałują ze sobą, więc bramki dwukubitowe udają się tylko z pewnym prawdopodobieństwem i wymagają natychmiastowej korekty na podstawie wyniku pomiaru pomocniczego. Firma PsiQuantum zbudowała na tym założeniu strategię pomijającą etap maszyn pośrednich: buduje od razu instalację docelową, licząc, że skala wytwarzania zrekompensuje zawodność pojedynczej operacji.

Kubity topologiczne. Pomysł najdalej idący i najsłabiej udokumentowany. Informacja miałaby być zapisana nie w stanie pojedynczej cząstki, lecz w zbiorowej właściwości całego układu – w konfiguracji nadprzewodnika połączonego z półprzewodnikowym nanoprzewodem. Zaburzenie działające lokalnie nie sięgałoby takiej informacji, więc odporność na błędy byłaby wbudowana w samą fizykę,

Tabela 2.1. Parametry pięciu technologii – rzędy wielkości, stan na połowę 2026 roku

Technologia	Temperatura układu kubitowego	Czas bramki dwukubitowej	Wierność bramki dwukubitowej	Największy zbudowany układ (kubity fizyczne)
Nadprzewodniki	10…20 mK	25…100 ns	ok. 99,7%	1121 (IBM Condor, 2023); w użyciu 156 (Heron)
Jony w pułapkach	jon: ok. 1 μK	10…100 μs	do 99,9%	ok. 100 (Quantinuum Helios)
Atomy neutralne	atom: ok. 1 μK	setki ns	ok. 99,5%	6100 (macierz Caltech – bez bramek dwukubitowych)
Fotonika	detektory: 1…4 K	bramki probabilistyczne	trudna do porównania	brak porównywalnej miary
Kubity topologiczne	poniżej 100 mK	niezmierzony	niezmierzona	8 zapowiedzianych (Majorana 1)

Wartości różnią się między poszczególnymi egzemplarzami maszyn i bywają podawane w warunkach optymalnych. Należy je czytać jako rzędy wielkości, nie jako dane katalogowe

a nie dokładana kodem korekcyjnym. Microsoft ogłosił w lutym 2025 roku układ Majorana 1, jednak część środowiska naukowego kwestionuje, czy przedstawione pomiary dowodzą tego, co deklarowano. Traktujemy to jako kierunek badań, nie jako wynik.

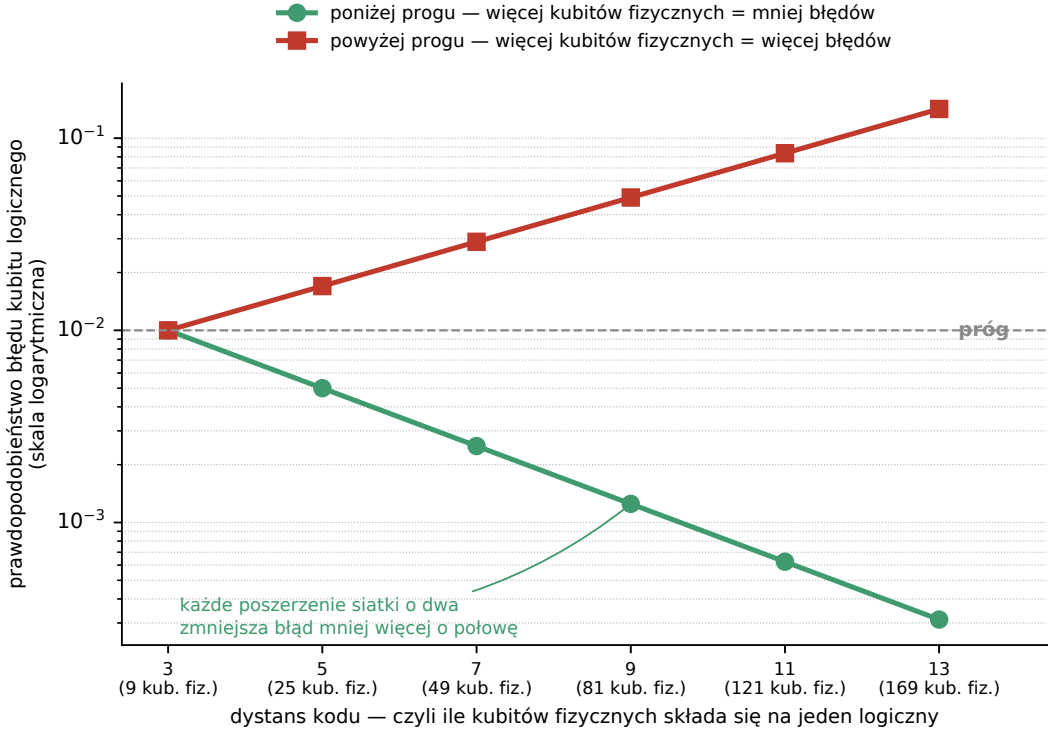
2.2. Od kubitu fizycznego do logicznego

Wyścig o liczbę kubitów fizycznych jest tym, o czym pisze prasa. Rywalizacja rozstrzygająca toczy się gdzie indziej: o to, czy dokładanie kubitów fizycznych poprawia jakość obliczenia, czy ją pogarsza.

Pytanie brzmi paradoksalnie tylko do chwili, gdy uwzględni się jedną okoliczność. W kodzie korekcyjnym część kubitów fizycznych przechowuje informację, a część nieustannie mierzy swoich sąsiadów, sygnalizując miejsca, w których coś poszło nie tak. Te kontrolujące kubity fizyczne również są zawodne i same wprowadzają błędy. Dokładając kolejne kubity fizyczne, zwiększamy więc jednocześnie zdolność wykrywania błędów i liczbę ich źródeł. Który efekt przeważy, zależy od wierności pojedynczej bramki.

Istnieje graniczna wartość tej wierności, nazywana **progiem korekcji błędów**. Jeżeli bramki są gorsze niż próg, rozbudowa kodu pogarsza wynik. Jeżeli lepsze – poprawia go wykładniczo: każde poszerzenie siatki kubitów fizycznych o dwa zmniejsza prawdopodobieństwo błędu kubitu logicznego mniej więcej o połowę.

Przez dwadzieścia lat próg pozostawał wielkością teoretyczną: wiadomo było, że istnieje, ale żadna maszyna nie znalazła się po właściwej jego stronie. W grudniu 2024 roku Google przedstawił układ Willow, w którym poszerzanie kodu powierzchniowego z dystansu trzy na pięć, a następnie na siedem, za każdym razem zmniejszało błąd kubitu logicznego mniej więcej o połowę. Wynik opublikowano w „Nature" na początku 2025 roku. Od tego momentu budowa dużej maszyny odpornej na błędy przestała być pytaniem z zakresu fizyki podstawowej, a stała się pytaniem o inżynierię, wytwarzanie i pieniądze.



Rysunek 2.2. Dlaczego próg jest ważniejszy od liczby kubitów fizycznych. Powyżej progu każde powiększenie kodu pogarsza wynik. Poniżej progu ta sama rozbudowa poprawia go wykładniczo. Liczby w nawiasach pod osią podają, ile kubitów fizycznych zajmuje kod o danym dystansie

Pozostały jednak dwie poważne przeszkody, o których w komunikatach prasowych mówi się mniej.

Pierwsza dotyczy zestawu dostępnych operacji. Kod powierzchniowy chroni informację sprawnie, ale pozwala wykonywać niewielkim kosztem tylko część potrzebnych bramek. Brakującą – potocznie zwaną bramką T, a w wersji trójkubitowej bramką Toffoliego – trzeba dostarczyć z zewnątrz w postaci specjalnie przygotowanych stanów kwantowych, nazywanych **stanami magicznymi**. Wytwarza się je w wydzielonej części układu w procesie przypominającym wzbogacanie rudy: z wielu egzemplarzy niskiej jakości powstaje jeden dostatecznie dobry. W projektach dużych maszyn taka „fabryka" zajmuje większość powierzchni procesora, a liczba potrzebnych stanów magicznych jest wprost proporcjonalna do liczby bramek Toffoliego w obwodzie. Dlatego szacunki ataków kryptograficznych podaje się właśnie w bramkach Toffoliego, a nie w bramkach dowolnego rodzaju. IBM planuje uruchomić wytwarzanie stanów magicznych około 2028 roku.

Druga przeszkoda to koszt samego kodu powierzchniowego, w którym na jeden kubit logiczny przypada od kilkudziesięciu do kilkuset kubitów fizycznych. Stąd rosnące zainteresowanie nowszą rodziną kodów oznaczaną skrótem qLDPC (quantum low-density parity-check – kwantowe kody o rzadkiej macierzy kontrolnej). Wymagają one wyraźnie mniej kubitów fizycznych na jeden logiczny, ale potrzebują połączeń między kubitami odległymi od siebie na płytce, co przy płaskiej siatce jest trudne do wykonania. Zespół IBM opublikował w 2024 roku w „Nature" konstrukcję takiego kodu i wpisał ją do swojej mapy drogowej. Na kodach qLDPC oparty jest również szacunek mówiący o stu tysiącach kubitów fizycznych potrzebnych do złamania RSA – **z tym, że pochodzi on z pracy, która nie przeszła recenzji naukowej**, i traktujemy go jako zapowiedź kierunku, a nie ustalenie.

2.3. Rachunek zasobów: trzy piętra

Zestawmy teraz wszystkie wielkości, które pojawiają się w doniesieniach o zagrożeniu kryptograficznym, i sprawdźmy, co dokładnie każda z nich opisuje. Weźmiemy za przykład atak na 256-bitowy klucz na krzywej eliptycznej – ten sam, którym zabezpieczone są portfele kryptowalutowe i większość dzisiejszych podpisów cyfrowych.

Piętro pierwsze – algorytm. Obwód opisany przez zespół Google w marcu 2026 roku wymaga 1200 kubitów logicznych i około 90 milionów bramek Toffoliego. Obie te liczby są cechą samego algorytmu i nie zależą od tego, na jakim sprzęcie zostanie uruchomiony. Druga z nich mówi, **ile operacji zawiera obwód od początku do końca** – a nie ile operacji maszyna wykonuje w ciągu sekundy.

Piętro drugie – korekcja błędów. Aby uzyskać jeden kubit logiczny o wierności wystarczającej

Trzy piętra rachunku: co trzeba mieć, żeby złamać 256-bitowy klucz na krzywej eliptycznej

Dwie wielkości, które najczęściej się myli: liczba kubitów podana bez określenia, czy chodzi o logiczne, czy fizyczne — oraz liczba operacji podana bez określenia, czy opisuje rozmiar obwodu, czy szybkość maszyny. Pierwsza różnica bywa stukrotna, druga zmienia sens zdania.

Rysunek 2.3. Trzy piętra rachunku. Pierwsze piętro opisuje algorytm i jest niezależne od sprzętu. Drugie mówi, ile sprzętu kosztuje jeden kubit logiczny. Dopiero trzecie przekłada to na liczbę kubitów fizycznych i czas pracy maszyny

„Sto milionów operacji" – czego ta liczba nie mówi

Zapowiedź, że maszyna wykona sto milionów operacji, bywa czytana jak parametr wydajności procesora klasycznego, podawany w operacjach na sekundę. To błędne odczytanie i prowadzi do zupełnie fałszywych wniosków.

Liczba bramek w obwodzie mówi, jak długie obliczenie maszyna zdoła doprowadzić do końca, zanim błędy je zniszczą. Jest to więc miara wytrzymałości, nie prędkości. Maszyna wykonująca sto milionów operacji może potrzebować na to sekundy albo tygodnia – zależnie od czasu jednej bramki i od narzutu korekcji błędów.

Do oszacowania czasu pracy potrzebne są trzy liczby jednocześnie: liczba bramek w obwodzie, czas wykonania jednej bramki oraz liczba cykli korekcji przypadających na jedną bramkę logiczną. Podanie tylko pierwszej z nich nie pozwala powiedzieć nic o tym, jak szybko maszyna złamie szyfr.

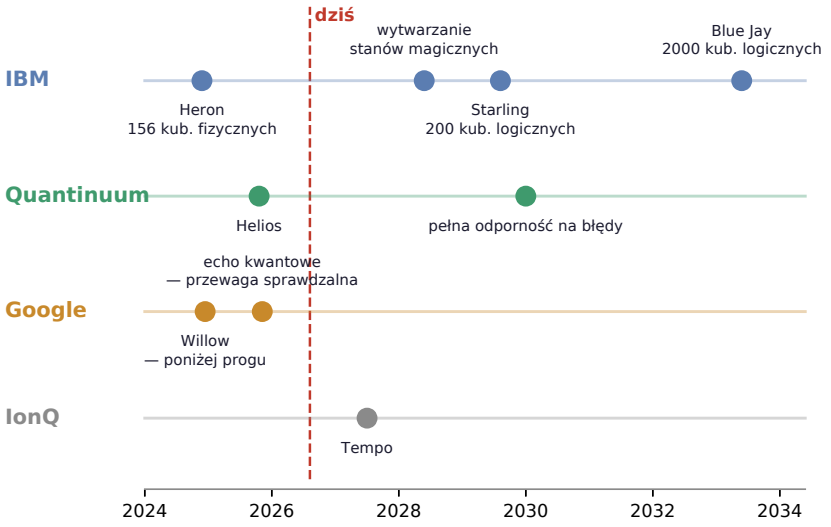
do przeprowadzenia obwodu tej długości, trzeba przeznaczyć kilkaset kubitów fizycznych. Do tego dochodzi fabryka stanów magicznych, zasilająca obwód w bramki Toffoliego. Narzut zależy od wierności bramek: im lepsze bramki fizyczne, tym mniejszy kod wystarcza.

Piętro trzecie – czas. Dopiero teraz pojawia się sprzęt. Przy założeniach przyjętych przez zespół Google – jedna bramka na tysiąc kończąca się błędem, cykl kodu powierzchniowego trwający mikrosekundę, reakcja układu sterującego w dziesięć mikrosekund – całość mieści się w mniej niż 500 tysiącach kubitów fizycznych i zajmuje około dziewięciu minut pracy maszyny. Zmiana któregokolwiek z tych założeń zmienia wynik. Gdyby te same 90 milionów bramek wykonywać na maszynie jonowej, z bramką trwającą pięćdziesiąt mikrosekund, obliczenie ciągnęłoby się tygodniami.

2.4. Mapy drogowe, czyli obietnice z datami

Producenci publikują harmonogramy sięgające początku lat trzydziestych. Warto je znać, pamiętając zarazem, czym są: deklaracjami przedsiębiorstw konkurujących o kapitał inwestycyjny i o kontrakty publiczne.

IBM ma harmonogram najbardziej szczegółowy. Maszyna Starling ma w 2029 roku dysponować 200 kubitami logicznymi i wykonywać obwody liczące do 100 milionów bramek. Kolejna, Blue Jay, około 2033 roku ma osiągnąć 2000 kubitów logicznych i obwody miliardowe. Pośrednim krokiem jest uruchomienie wytwarzania



Wszystkie daty po roku 2026 to deklaracje producentów, nie fakty. Skrót „kub." oznacza kubity — przy każdym kamieniu milowym podano, które.

Rysunek 2.4. Zapowiedzi czterech głównych producentów. Wszystko na lewo od czerwonej linii jest faktem, wszystko na prawo – planem. Przy każdym kamieniu milowym zaznaczono, czy podana liczba dotyczy kubitów fizycznych, czy logicznych

W układzie bez zakłóceń ewolucja wstecz przywróciłaby stan początkowy. Zaburzenie wprowadzone w kroku 2 to uniemożliwia, a odległość stanu końcowego od punktu wyjścia zależy od tego, jak informacja rozeszła się po układzie. Wynikiem pomiaru jest pojedyncza wielkość liczbowa, możliwa do zmierzenia niezależnie na innej maszynie — i na tym polega różnica wobec eksperymentu z 2019 roku.

Rysunek 2.5. Echo kwantowe w czterech krokach. Metoda jest dalekim krewnym echa spinowego stosowanego od dziesięcioleci w rezonansie magnetycznym: układ puszcza się do przodu, delikatnie zaburza, puszcza wstecz i mierzy, jak daleko od punktu wyjścia się znalazł

stanów magicznych w architekturze modułowej, zapowiadane na 2028 rok.

Quantinuum ogłosiło 22 lipca 2026 roku przyspieszony harmonogram, zakładający osiągnięcie pełnej, uniwersalnej odporności na błędy do 2030 roku. Firma opiera się na architekturze pułapek jonowych, w której jony są przemieszczane między strefami pułapki. Wysoka wierność bramek pozwala tam na kody korekcyjne o mniejszym narzucie, ale liczby podawane przez producenta nie zostały dotąd niezależnie zweryfikowane.

Zestawmy teraz zapowiedź IBM z rachunkiem z poprzedniego podrozdziału, pilnując, by porównywać wielkości tego samego rodzaju. Atak na klucz eliptyczny wymaga 1200 kubitów logicznych i obwodu liczącego około 90 milionów bramek Toffoliego. Starling z 2029 roku ma mieć 200 kubitów logicznych i obsługiwać obwody do 100 milionów bramek. Pod względem długości obwodu maszyna byłaby więc mniej więcej wystarczająca. Pod względem liczby kubitów logicznych brakowałoby jej sześciokrotnie.

Warto dodać zastrzeżenie, którego to porównanie samo nie zawiera: 100 milionów bramek w zapowiedzi IBM to bramki dowolnego rodzaju, podczas gdy 90 milionów w szacunku ataku to wyłącznie bramki Toffoliego, każda wymagająca stanu magicznego. Rzeczywisty obwód ataku zawiera ich znacznie więcej. Zestawienie należy więc czytać jako orientacyjne, a nie jako rachunek.

Historia map drogowych w tej dziedzinie zaleca ostrożność w obie strony. Terminy bywały przesuwane, ale zdarzały się też postępy szybsze od zapowiadanych. Szacunek liczby kubitów fizycznych potrzebnych do złamania RSA-2048 spadł z dwudziestu milionów w 2019 roku do niecałego miliona w 2025 – i nikt tej redukcji sześć lat wcześniej nie przewidywał. Nie wynikała ona z postępu sprzętowego, lecz z ulepszenia samego algorytmu i sposobu gospodarowania kubitami logicznymi w trakcie obliczenia.

2.5. Echo kwantowe: pierwsza przewaga, którą da się sprawdzić

W październiku 2025 roku Google ogłosił wynik, który w dłuższej perspektywie może okazać się ważniejszy od układu Willow. Chodzi o eksperyment nazwany echem kwantowym.

Aby zrozumieć jego znaczenie, trzeba wrócić do roku 2019. Google ogłosił wtedy pierwszą „przewagę kwantową": maszyna wykonała w kilka minut zadanie, na które superkomputer miał potrzebować tysięcy lat. Zarzut, który padł natychmiast i nigdy nie został do końca odparty, brzmiał: skoro nikt nie potrafi tego obliczenia powtórzyć, to na jakiej podstawie uznajemy wynik za poprawny? Zadanie polegało na wygenerowaniu rozkładu losowych ciągów bitów, a takiego wyniku nie da się bezpośrednio zweryfikować.

Echo kwantowe różni się tym, że jego wynikiem jest pojedyncza wielkość liczbowa, którą inna maszyna kwantowa może zmierzyć niezależnie i porównać. Wynik daje się potwierdzić albo obalić, a to jest różnica między eksperymentem a pokazem. Obliczenie wykonane na układzie Willow było według Google około trzynaście tysięcy razy szybsze niż najlepszy znany algorytm klasyczny uruchomiony na superkomputerze Frontier. Praca ukazała się w „Nature" 22 października 2025 roku.

Mierzoną wielkością jest tak zwany korelator poza porządkiem czasowym. Opisuje on, jak szybko informacja umieszczona w jednym

miejscu układu rozprzestrzenia się na całą resztę. Zespół Google wskazuje jako możliwe zastosowanie jądrowy rezonans magnetyczny: metoda mogłaby pomagać w ustalaniu odległości między atomami w cząsteczce, a więc w odczytywaniu struktury związków chemicznych. Od demonstracji do użytecznego narzędzia droga jest jednak daleka.

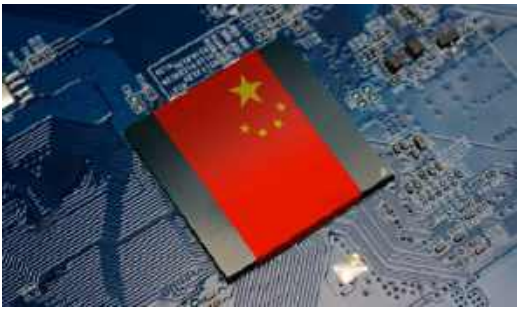
Należy przy tym odnotować zastrzeżenie, którego w komunikatach prasowych zabrakło: zadanie zostało dobrane pod możliwości maszyny, a nie wzięte z listy problemów, na których rozwiązanie ktoś czeka. Postęp polega na tym, że wynik po raz pierwszy daje się sprawdzić – nie na tym, że okazał się komuś potrzebny.

2.6. Chiny, czyli brakująca kolumna w każdej tabeli

Wszystko, co opisaliśmy dotąd, pochodzi z laboratoriów amerykańskich i europejskich. W wyścigu uczestniczy jeszcze jeden gracz, o którym wiadomo znacznie mniej – i sama ta niewiedza jest istotną informacją.

Chiński Uniwersytet Nauki i Technologii w Hefei rozwija linię procesorów nadprzewodnikowych Zuchongzhi: 62 kubity fizyczne w 2021 roku, 105 w wersji 3.0 z grudnia 2024, 107 w roku 2025. Przedsiębiorstwo Origin Quantum dysponuje maszyną Wukong o 72 kubitach fizycznych, a operator China Telecom układem Tianyan-504. Udostępniona publicznie platforma chmurowa Tianyan odnotowała, według danych cytowanych przez amerykański ośrodek CSIS, ponad 37 milionów wejść z ponad sześćdziesięciu krajów.

Istotniejszy od liczby kubitów fizycznych jest jednak łańcuch dostaw. Chiny rozpoczęły produkcję własnych kriostatów rozcieńczalnikowych



– urządzeń schładzających procesor do kilkunastu milikelwinów, dotąd sprowadzanych z Finlandii i Wielkiej Brytanii. Piętnasty plan pięcioletni, obejmujący lata 2026–2030, wymienia technologie kwantowe wśród nowych punktów wzrostu gospodarczego, co zapowiada finansowanie na poziomie porównywalnym z programami półprzewodnikowymi.

I tu pojawia się kłopot przewijający się przez cały ten numer. Parametry chińskich maszyn nie zostały niezależnie zweryfikowane – zaznacza to sam CSIS w raporcie z maja 2026 roku, oceniając zarazem, że Chiny mogą dorównać Ameryce Północnej w ciągu pięciu lat. **Ankieta ekspercka, o której pisaliśmy w rozdziale pierwszym – ta z prognozą 28…49 procent na dziesięć lat – nie zawiera ani jednego respondenta z Chin.** Jeżeli więc w powszechnych szacunkach tkwi błąd systematyczny, to najprawdopodobniej właśnie tam.

W następnym rozdziale odwrócimy perspektywę. Ta sama maszyna, która niepokoi kryptografów, jest od czterdziestu lat wymarzonym narzędziem chemików – i to oni, a nie włamywacze, są powodem, dla którego rządy i przedsiębiorstwa finansują te kriostaty. ■

Bibliografia

[18] Google Quantum AI, Quantum Error Correction Below the Surface Code Threshold, „Nature” 2025, t. 638, s. 920–926. DOI: 10.1038/s41586-024-08449-y.

[19] Manetsch H. J., Nomura G., Bataille E. i in., A Tweezer Array with 6100 Highly Coherent Atomic Qubits, „Nature” 2025. DOI: 10.1038/s41586-025-09641-4. Komunikat: California Institute of Technology, Pasadena, 24 września 2025.

[20] Google Quantum AI, A Verifiable Quantum Advantage, blog Google Research, 22 października 2025; praca towarzysząca opublikowana w „Nature” tego samego dnia. https://research.google/blog/a-verifiable-quantum-advantage/ [dostęp: 5.08.2026].

[21] Bravyi S., Cross A. W., Gambetta J. M. i in., High-Threshold and Low-Overhead Fault-Tolerant Quantum Memory, „Nature” 2024, t. 627, s. 778–782. DOI: 10.1038/s41586-024-07107-7.

[22] Bravyi S., Kitaev A., Universal Quantum Computation with Ideal Clifford Gates and Noisy Ancillas, „Physical Review A” 2005, t. 71, 022316. DOI: 10.1103/PhysRevA.71.022316. Praca wprowadzająca destylację stanów magicznych.

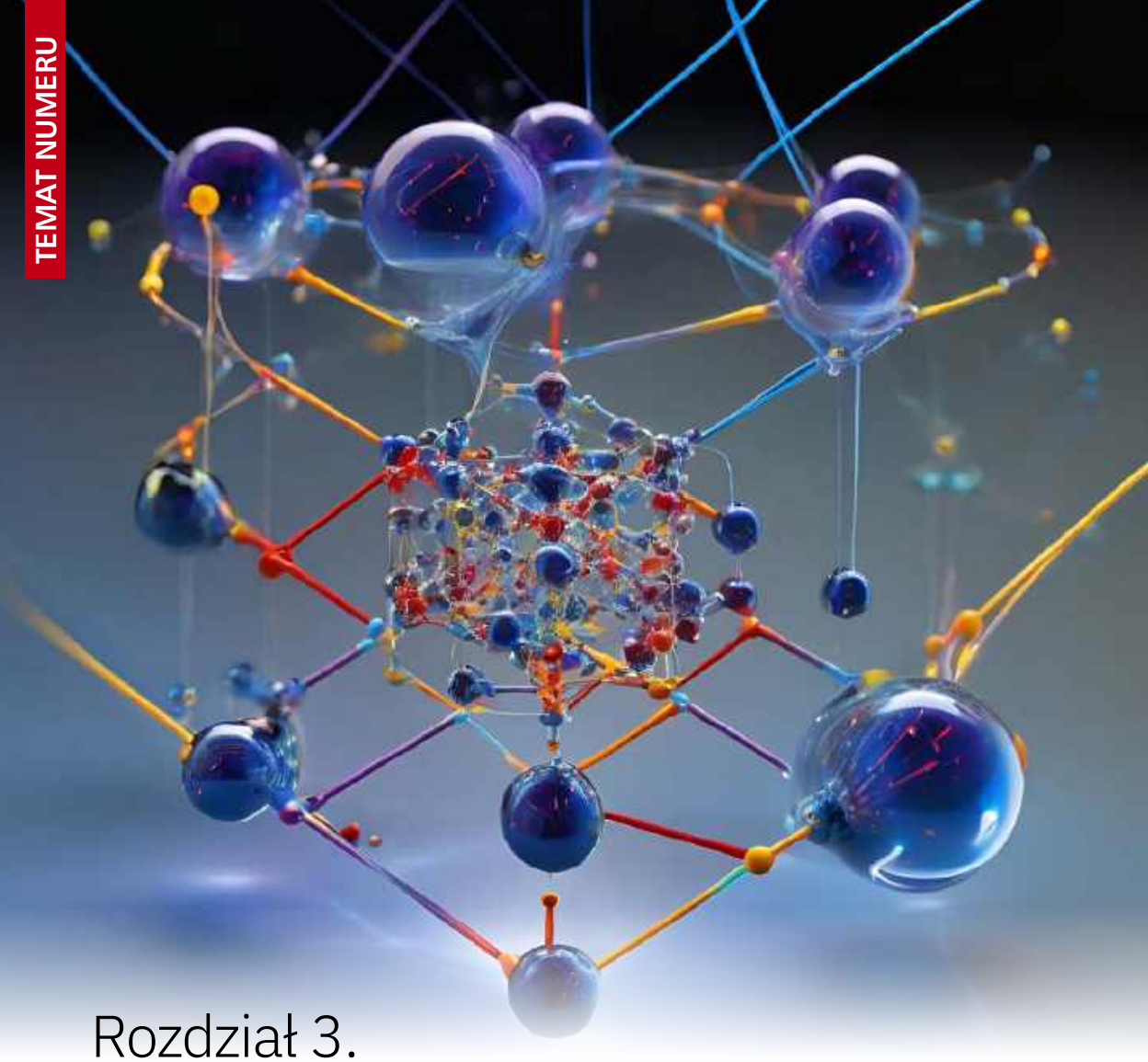
[23] Quantinuum, Quantinuum Unveils Accelerated Roadmap to Achieve Universal, Fully Fault-Tolerant Quantum Computing by 2030, komunikat prasowy, Broomfield, 22 lipca 2026.

[24] Gao D., Fan D., Zha C. i in., Establishing a New Benchmark in Quantum Computational Advantage with 105-Qubit Zuchongzhi 3.0 Processor, preprint arXiv:2412.11924 [quant-ph], grudzień 2024.

[25] Center for Strategic and International Studies, Understanding China’s Quest for Quantum Advancement, CSIS, Waszyngton, maj 2026. https://www.csis.org/analysis/understanding-chinas-quest-quantum-advancement [dostęp: 5.08.2026].

[26] Microsoft, Microsoft’s Majorana 1 Chip Carves New Path for Quantum Computing, komunikat prasowy, Redmond, 19 lutego 2025.

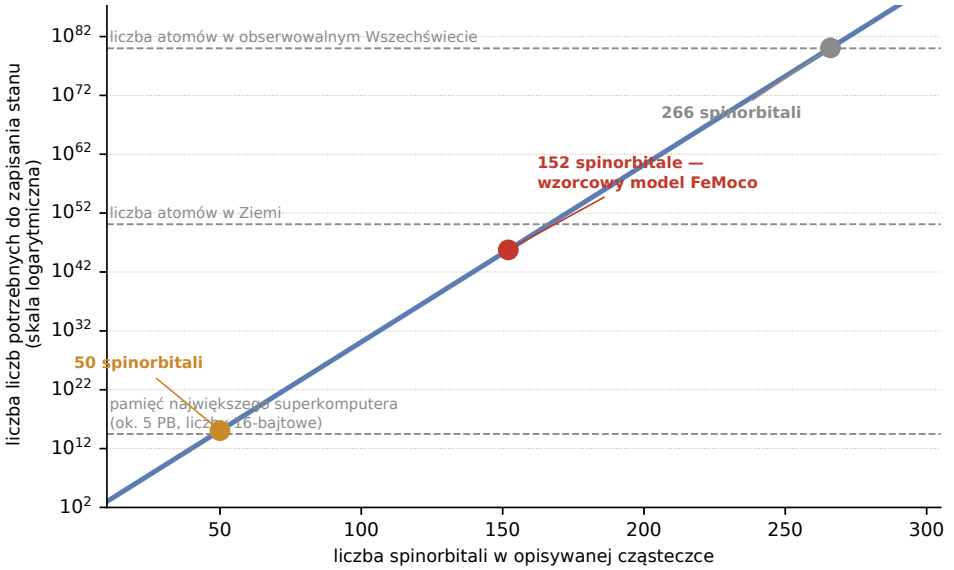
Ponadto w rozdziale przywołano pozycje [4], [6], [7] i [8] z bibliografii rozdziału 1 (Preskill 2018; Gidney 2025; Iceberg Quantum 2026; mapa drogowa IBM Quantum) oraz pozycję [3] (szacunek zasobów ataku na krzywą eliptyczną).



Rozdział 3.

Kto czeka na Q-DAY z nadzieją

Komputer kwantowy nie powstał po to, żeby łamać szyfry. Powstał – najpierw jako pomysł, potem jako program badawczy – po to, żeby symulować przyrodę. Kryptografia znalazła się na tej liście przypadkiem, dziesięć lat po sformułowaniu pierwotnego zamysłu, i to ona zapewniła całej dziedzinie finansowanie ze środków publicznych. Ale gdyby zapytać, kto naprawdę czeka na te maszyny, odpowiedź brzmiałaby: chemicy. Ten rozdział opisuje, na co dokładnie czekają, i sprawdza, ile z tych obietnic wytrzymuje bliższe sprawdzenie



Dokładny opis stanu kwantowego układu N cząstek wymaga 2 do potęgi N liczb. Już przy pięćdziesięciu spinorbitalach przekracza to pamięć największego superkomputera, przy stu pięćdziesięciu dwóch — liczbę atomów w Ziemi, a przy dwustu sześćdziesięciu sześciu liczbę atomów w obserwowalnym Wszechświecie. To właśnie ta ściana skłoniła Richarda Feynmana do zaproponowania w 1981 roku komputera opartego na tej samej fizyce co badany układ.

Rysunek 3.1. Wzrost wykładniczy w praktyce. Oś pionowa jest logarytmiczna, więc każda podziałka oznacza dziesięć rzędów wielkości. Krzywa nie zakręca ani nie zwalnia – po prostu przebija kolejne granice fizycznej możliwości zapisania czegokolwiek

3.1. Ściana wykładnicza

W maju 1981 roku, na konferencji zorganizowanej wspólnie przez MIT i firmę IBM, Richard Feynman wygłosił wykład zatytułowany „Symulowanie fizyki komputerami". Postawił w nim pytanie pozornie techniczne: czy zwykły komputer potrafi wiernie odtworzyć zachowanie układu kwantowego? Odpowiedź, do której doszedł, brzmiała: nie, i to nie z powodu niedostatecznej mocy obliczeniowej, lecz z powodów zasadniczych. Skoro tak, ciągnął Feynman, to trzeba zbudować maszynę, która sama podlega prawom mechaniki kwantowej.

Aby zrozumieć, skąd bierze się ta przeszkoda, warto prześledzić prosty rachunek.

Zwykły komputer opisuje cząstkę, podając jej położenie i pęd. Cząstka kwantowa nie ma jednego określonego stanu – ma rozkład możliwości. Gdy cząstek jest kilka i wzajemnie na siebie oddziałują, ich możliwości nie sumują się, lecz mnożą. Dokładny opis układu N cząstek wymaga **2 do potęgi N liczb**, a nie N liczb. Dla dziesięciu cząstek to tysiąc liczb – drobiazg. Dla pięćdziesięciu to już ponad tysiąc bilionów, czyli więcej niż mieści pamięć największego superkomputera świata.

To jest właśnie ściana wykładnicza. Nie da się jej obejść szybszym procesorem, bo dołożenie jednej cząstki podwaja zapotrzebowanie na pamięć. Postęp technologiczny, który co dwa lata podwaja moc komputerów, pozwala w tym tempie dołożyć do symulacji jedną cząstkę na dwa lata. Chemik potrzebuje kilkudziesięciu naraz.

Chemia obliczeniowa radzi sobie z tym od pół wieku przez przybliżenia. Najpopularniejsza metoda, teoria funkcjonału gęstości, zamiast śledzić wszystkie elektrony opisuje ich uśrednioną gęstość. Działa zaskakująco dobrze i to na niej opiera się większość dzisiejszego projektowania materiałów. Ma jednak klasę przypadków, w których zawodzi: układy z wieloma niesparowanymi elektronami, w których żaden pojedynczy sposób ich rozmieszczenia nie dominuje nad innymi. Fachowo mówi się o silnych korelacjach. Praktycznie chodzi o metale przejściowe – żelazo, mangan, kobalt, molibden – czyli o pierwiastki, na których opiera się większość interesujących katalizatorów.

Pomysł Feynmana polegał na tym, żeby przestać z tym walczyć. Skoro opis układu kwantowego rośnie wykładniczo, a układ kwantowy sam siebie „opisuje" bez trudu, to zbudujmy

Dlaczego akurat 2 do potęgi N

Rzućmy dziesięcioma monetami. Wynik da się zapisać dziesięcioma symbolami: orzeł albo reszka dla każdej z nich. Ale zanim spojrzymy, każda moneta ma dwie możliwości, a wszystkich kombinacji jest 2 do potęgi 10, czyli 1024.

W świecie klasycznym te 1024 kombinacje są tylko wyliczeniem możliwości – rzeczywistość realizuje jedną z nich. W świecie kwantowym układ może znajdować się we wszystkich naraz, a **każdej z nich odpowiada osobna liczba** opisująca jej udział. Żeby wiernie zapisać stan, trzeba przechować wszystkie te liczby.

Stąd bierze się cała trudność i cała nadzieja. Trudność – bo zwykły komputer musi te liczby trzymać w pamięci. Nadzieja – bo komputer kwantowy o N kubitach ma dokładnie tyle samo możliwości co opisywany układ, więc nie musi ich wypisywać. Utrzymuje je w sposób, w jaki robi to sama przyroda.

urządzenie z tego samego materiału co badany problem. **Komputer kwantowy jest w tym ujęciu nie tyle szybszym kalkulatorem, ile fizycznym modelem badanego układu.**

Analogia, która to porządkuje, pochodzi z lotnictwa. Konstruktor samolotu może próbować rozwiązać równania opisujące opływ powietrza wokół skrzydła – i szybko napotyka trudność podobną do tej, o której mowa wyżej. Może też postąpić inaczej: zbudować pomniejszony model skrzydła, umieścić go w tunelu aerodynamicznym i włączyć dmuchawę. **Rachunku nie wykonuje wtedy nikt – wykonuje go samo powietrze**, a inżynier jedynie odczytuje wynik z przyrządów. Model w tunelu nie jest szybszym komputerem; jest fizycznym zastępnikiem obliczenia.

Komputer kwantowy działa według tej samej zasady, tylko badanym zjawiskiem nie jest przepływ powietrza, lecz zachowanie elektronów. Zamiast wypisywać w pamięci wszystkie 2 do potęgi N liczb opisujących cząsteczkę, buduje się sterowany układ kwantowy – z jonów, atomów albo obwodów nadprzewodzących – i nastawia go tak, aby podlegał tym samym prawom co badana cząsteczka. Potem pozwala mu się dojść do stanu o najniższej energii i odczytuje, jaka to energia. **Wykładnicza liczba możliwości nigdzie nie zostaje zapisana; istnieje w samym układzie, tak jak istnieje w rzeczywistej cząsteczce.**

3.2. Azotaza: sztandarowy przykład, który się skomplikował

Jeśli w tej dziedzinie istnieje jedna cząsteczka-symbol, jest nią kofaktor żelazowo-molibdenowy azotazy, w skrócie FeMoco. Warto poświęcić mu chwilę, bo jego historia w miniaturze opowiada całą historię obietnic komputerów kwantowych – łącznie z niespodzianką z początku 2026 roku.

Azotaza to enzym bakterii glebowych, który potrafi rozerwać wiązanie potrójne w cząsteczce

Ten sam produkt, dwie zupełnie różne drogi

azot z powietrza → amoniak

PROCES HABERA I BOSCHA		AZOTAZA — ENZYM BAKTERII	
temperatura	**ok. 450 °C**	temperatura	**otoczenia**
ciśnienie	**ok. 200 atmosfer**	ciśnienie	**atmosferyczne**
katalizator	**żelazo**	katalizator	**kofaktor FeMo**
zużycie energii	**1–2% energii świata**	zużycie energii	**z metabolizmu**
emisja CO_2	**1,2–3% emisji świata**	emisja CO_2	**brak**

Dlaczego nie potrafimy naśladować bakterii? Bo nie wiemy dokładnie, jak działa jej katalizator. Osiem jonów metali przejściowych z wieloma niesparowanymi elektronami to układ, którego stanu podstawowego przez dziesięciolecia nie umiano policzyć.

Rysunek 3.2. Ta sama reakcja chemiczna przeprowadzana dwiema drogami. Proces przemysłowy odpowiada za wyżywienie mniej więcej połowy ludzkości i zarazem za kilka procent światowej emisji dwutlenku węgla. Bakteria robi to samo bez ogrzewania i bez sprężania

azotu i przerobić azot z powietrza na amoniak, czyli na formę przyswajalną dla roślin. Robi to w temperaturze otoczenia i pod ciśnieniem atmosferycznym. Ludzkość opanowała tę samą reakcję sto lat temu, w procesie Habera i Boscha, ale za cenę temperatury 450 stopni i ciśnienia dwustu atmosfer.

Skala tej różnicy jest trudna do przecenienia. Produkcja nawozów azotowych pochłania **od jednego do dwóch procent światowej produkcji energii** i odpowiada za około jeden do trzech procent globalnej emisji dwutlenku węgla. Gdyby udało się zaprojektować katalizator naśladujący bakterię, byłaby to zmiana porównywalna z wynalezieniem samego procesu Habera. To dlatego FeMoco stał się wzorcowym zadaniem, na którym mierzy się postęp algorytmów kwantowych.

Przeszkodą jest to, że nie wiemy dokładnie, jak ten katalizator działa. Ma osiem jonów metali przejściowych, siedem żelaza i jeden molibdenu, spiętych siarką i węglem. Elektrony w takim układzie są rozmieszczone na wiele sposobów naraz i żaden nie dominuje – to modelowy przypadek silnych korelacji, przed którym teoria funkcjonału gęstości kapituluje.

Historia szacunków, ile kosztowałoby policzenie tego układu na komputerze kwantowym, jest sama w sobie pouczająca. W 2017 roku Markus Reiher wraz ze współpracownikami opublikował pierwszy poważny rachunek: około 111 kubitów logicznych, ale rzędu 10 do potęgi 14 najdroższych bramek, co przy realistycznych założeniach dawało czas pracy liczony w latach. W 2021 roku zespół Joonho Lee zamienił czas na sprzęt: 2142 kubity logiczne i 5,3 miliarda bramek Toffoliego, czyli niecałe cztery doby obliczeń przy czterech milionach kubitów fizycznych. Najnowsze szacunki

Mikrofotografia (barwienie H&E) brodawki zwykłej (verruca vulgaris) ukazująca charakterystyczne cechy (hiperkeratozę, akantozę, hipergranulozy, wydłużenie grzbietu siateczki i duże naczynia krwionośne na połączeniu skórno-naskórkowym) (Fot. Nephron – Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=16247974)

mówią o 1137 kubitach logicznych i 340 milionach bramek.

Zwróćmy uwagę na to, co się tu wydarzyło: **w ciągu ośmiu lat zapotrzebowanie spadło o sześć rzędów wielkości**, i to bez najmniejszego postępu w sprzęcie. Zmieniły się algorytmy i sposób zapisu problemu. Dokładnie ta sama rzecz przydarzyła się szacunkom ataku na kryptografię, o czym pisaliśmy w rozdziale drugim – i nie jest to przypadek. W obu przypadkach chodzi o ten sam typ obliczenia, wykonywany tą samą metodą.

A teraz niespodzianka. W styczniu 2026 roku zespół Garneta Chana z Caltechu opublikował pracę, w której policzył stan podstawowy wzorcowego modelu FeMoco z dokładnością chemiczną – na zwykłych komputerach. Użyto sieci tensorowych i metod sprzężonych klastrów, a więc narzędzi klasycznych, tyle że zastosowanych z lepszym zrozumieniem struktury problemu.

Jak czytać deklaracje o przewadze kwantowej w zastosowaniach

Komunikaty o „przewadze kwantowej w chemii" albo „w materiałoznawstwie" pojawiają się co kilka miesięcy. Trzy pytania pozwalają szybko ocenić ich wagę.

Z czym porównano wynik? Jeżeli z metodą klasyczną dobraną przez zespół promujący maszynę kwantową, wynik znaczy niewiele. Historia tej dziedziny zna wiele przypadków, w których deklarowaną przewagę unieważniał lepszy algorytm klasyczny opublikowany kilka miesięcy później.

Czy zadanie było potrzebne komukolwiek poza autorami? Zadania dobierane pod możliwości sprzętu są uprawnionym etapem badań, ale nie są zastosowaniem. Różnica jest taka jak między testem silnika na hamowni a przejazdem z ładunkiem.

Czy podano liczbę kubitów logicznych, czy fizycznych? Wracamy do słowniczka zamykającego rozdział pierwszy. Bez tego rozróżnienia żadna deklaracja nie daje się zweryfikować.

Wniosek, który się z tego narzuca, jest prosty i zarazem mylący, więc warto go sformułować ostrożnie. **Nie oznacza to, że chemia kwantowa nie potrzebuje komputerów kwantowych.** Chan sam wystąpił potem z komentarzem prostującym takie odczytanie. Oznacza natomiast dwie rzeczy. Po pierwsze, granica możliwości metod klasycznych przesuwa się równolegle do postępu kwantowego, i to szybciej, niż zakładano. Po drugie, wszystkie szacunki przewagi kwantowej trzeba porównywać z najlepszą znaną metodą klasyczną, a nie z metodą podręcznikową – bo inaczej mierzy się przewagę nad przeciwnikiem, którego nikt nie wystawia do walki.

Chan zwraca też uwagę na rzecz, o której w tej dyskusji łatwo zapomnieć: chemia nie oferuje nieskończonego zapasu coraz większych problemów. FeMoco jest jednym z największych układów tego typu, jakie w ogóle występują w przyrodzie. Jeśli metody klasyczne sięgnęły już tego poziomu, to obszar, w którym komputer kwantowy miałby przewagę bezsporną, jest węższy, niż wynikałoby z entuzjastycznych zapowiedzi.

3.3. Leki, materiały i akumulatory

Poza azotazą lista oczekiwanych zastosowań jest długa, a każde z nich sprowadza się do tego samego: policzyć, jak zachowują się elektrony w układzie, którego nie da się policzyć klasycznie.

Projektowanie leków bywa przedstawiane jako sztandarowe zastosowanie, ale wymaga tu największej ostrożności. Komputer kwantowy nie zaprojektuje leku – projektowanie leku to wieloletni proces, w którym obliczenia kwantowochemiczne są jednym z wielu etapów, i to nie najdłuższym. To, co maszyna kwantowa mogłaby wnieść, to dokładniejsze policzenie energii wiązania cząsteczki z białkiem oraz mechanizmów reakcji enzymatycznych, w których uczestniczą metale – na przykład w rodzinie enzymów cytochromu P450, odpowiadających za metabolizowanie większości leków w ludzkiej wątrobie.

Skala problemu jest jednak inna niż w przypadku pojedynczej cząsteczki. Konkurs Q4Bio, prowadzony w Wielkiej Brytanii, wskazuje jako cel symulacje kompleksów białkowych liczących ponad dwanaście tysięcy atomów. Żaden dzisiejszy szacunek zasobów nie obejmuje układów tej wielkości i nikt nie twierdzi, że da się je policzyć w całości metodami kwantowymi. Realistyczny scenariusz zakłada podejście mieszane: klasyczny komputer opisuje całe białko, a kwantowy – tylko to niewielkie centrum aktywne, przed którym metody klasyczne kapitulują.

Materiały i energetyka to obszar mniej efektowny medialnie, lecz prawdopodobnie bliższy praktyce. Chodzi o elektrolity i materiały elektrodowe w akumulatorach, o katalizatory do rozkładu wody na wodór i tlen, o nadprzewodniki wysokotemperaturowe, o warstwy fotowoltaiczne. Wszystkie te przypadki łączy jedno: struktura elektronowa decyduje o właściwości użytkowej, a dzisiejsze metody dają wynik z niepewnością zbyt dużą, by na jej podstawie projektować.

Warto przy tym znać kontekst gospodarczy, bo wyjaśnia on, dlaczego akurat te zastosowania przyciągają pieniądze. Znacząca część czasu obliczeniowego światowych superkomputerów – według różnych szacunków rzędu jednej trzeciej – jest zajęta obliczeniami z zakresu chemii i materiałoznawstwa. Nie chodzi więc o rynek, który trzeba dopiero stworzyć, lecz o rynek istniejący, na którym klienci już dziś płacą za czas obliczeniowy.

W maju 2026 roku firma Q-CTRL ogłosiła wynik dotyczący poszukiwania materiałów dla sektora energetycznego: obliczenie wykonane na sprzęcie IBM w dwie minuty miało zająć narzędziom klasycznym ponad sto godzin. Deklarację tę należy czytać przez pryzmat pytań z ramki: pochodzi od dostawcy oprogramowania sterującego, nie od niezależnego zespołu, i nie została dotąd potwierdzona przez stronę trzecią.

3.4. Optymalizacja: rozdział o studzeniu entuzjazmu

Jeśli w tym rozdziale jest miejsce, w którym rozdźwięk między obietnicą a stanem wiedzy jest największy, to właśnie tutaj.

Optymalizacja to problemy typu: jak ułożyć trasy dla floty pojazdów, jak rozłożyć portfel inwestycyjny, jak zaplanować grafik na dwustu stanowiskach. Ich wspólną cechą jest to, że liczba możliwych rozwiązań rośnie wykładniczo z rozmiarem zadania – a więc pozornie mamy do czynienia z tym samym rodzajem trudności, który komputer kwantowy ma pokonywać.

Podobieństwo jest jednak mylące. Ściana wykładnicza w chemii wynika z tego, że opisywany układ jest kwantowy – komputer kwantowy

pasuje do niego jak klucz do zamka. W optymalizacji nic kwantowego nie ma. Problem jest zwyczajnie duży, a jedynym znanym narzędziem ogólnym pozostaje algorytm Grovera z jego przyspieszeniem pierwiastkowym.

A przyspieszenie pierwiastkowe jest w praktyce znacznie mniej warte, niż się wydaje. Trzeba je bowiem opłacić narzutem korekcji błędów, opisanym w rozdziale drugim: każda operacja logiczna kosztuje setki operacji fizycznych i cykle sprawdzania siatki. Zysk z pierwiastka bywa zjadany przez ten narzut w całości, i to zanim jeszcze porównamy się z konkurencją.

Konkurencja zaś jest bezlitosna. Firmy logistyczne dopracowują swoje algorytmy od czterdziestu lat. Rzecz, którą łatwo przeoczyć: **pokonanie algorytmu podręcznikowego nie jest tym samym co pokonanie działającego systemu**. Rozwiązania stosowane w przemyśle to nie czyste algorytmy, lecz zestawy reguł dopasowanych do konkretnej firmy, testowanych na rzeczywistych danych przez dekady. Publikacja pokazująca, że maszyna kwantowa znalazła lepszą trasę niż prosty algorytm , nie mówi nic o tym, czy pokonałaby system używany w przedsiębiorstwie kurierskim.

Do tego dochodzi zjawisko nazywane dekwantyzacją. Kilkakrotnie w ostatnich latach algorytm kwantowy zapowiadany jako dający wykładniczą przewagę okazywał się możliwy do naśladowania klasycznie, gdy tylko ktoś przyjrzał się bliżej strukturze problemu. Najgłośniejszy taki przypadek dotyczył systemów rekomendacji i został pokazany przez studentkę. To samo dotyczy większości propozycji z zakresu kwantowego uczenia maszynowego: dla danych klasycznych przewaga jest dziś nieudowodniona, a w kilku przypadkach obalona.

Trzeźwy wniosek brzmi więc tak: optymalizacja i uczenie maszynowe pozostają otwartym obszarem badań, ale nie należą do tych, w których na Q-Day czeka się z konkretnym planem. Wyjątkiem jest uczenie maszynowe stosowane do danych, które same są kwantowe – na przykład do wyników pomiarów z sensorów opisanych za chwilę albo z symulacji chemicznych. Tam przewaga bierze się z natury danych, a nie z samego algorytmu.

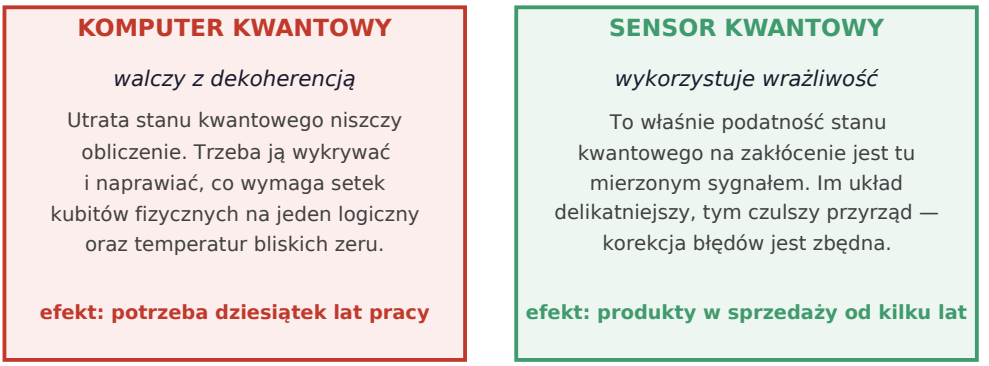
3.5. Sensory kwantowe: jedyna gałąź, która wygrywa już dziś

Cały ten numer opowiada o czekaniu – na maszynę, na standard, na termin. Jest jednak gałąź technologii kwantowych, w której czekanie się skończyło, a produkty są w sprzedaży. Nie mówi się o niej wiele, bo nie ma w niej żadnego dnia „Q".

Powód, dla którego sensory kwantowe wyprzedziły komputery o dwie dekady, jest elegancki i wart zapamiętania.

Komputer kwantowy musi chronić swój stan przed otoczeniem – każde zakłócenie niszczy obliczenie, więc buduje się kriostaty, ekrany i kody korekcyjne. Sensor kwantowy robi coś odwrotnego: **zakłócenie jest jego sygnałem**. Chcemy zmierzyć pole magnetyczne, więc wystawiamy delikatny układ kwantowy na jego działanie i patrzymy, jak bardzo się zmienił. Im układ wrażliwszy, tym przyrząd czulszy. Korekcja błędów jest tu nie tylko zbędna – byłaby przeciwskuteczna.

Dlatego sensor kwantowy potrzebuje od kilkunastu do kilkuset atomów, a nie milionów kubitów fizycznych i dlatego działa dziś, a nie za dziesięć lat.



Rysunek 3.3. Ta sama właściwość fizyczna w dwóch rolach. Skrajna wrażliwość układów kwantowych na otoczenie jest przekleństwem konstruktora komputera i zasadą działania konstruktora przyrządu pomiarowego

Trzy poziomy gotowości w jednej dziedzinie

Zegary atomowe – poziom 7…8. Wyroby sprzedawane i eksploatowane w warunkach polowych. Rynek istnieje.

Magnetometry – poziom 6…7. Prototypy w ograniczonym użyciu, pierwsze zastosowania medyczne i wojskowe.

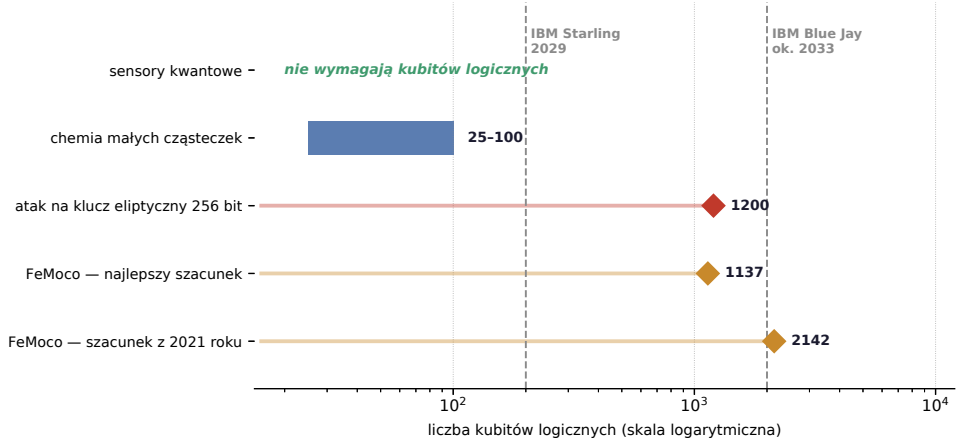
Grawimetry – poziom 5…6. Próby przedkomercyjne; docelowa czułość osiągalna, ale nie w obudowie znoszącej warunki terenowe.

Skala gotowości technologicznej, opracowana pierwotnie przez NASA, ma dziewięć stopni: od pomysłu (1) po sprawdzone działanie w warunkach docelowych (9). Komputery kwantowe ogólnego przeznaczenia mieszczą się w niej na poziomie 3…4.

Zegary atomowe są najbardziej dojrzałym przedstawicielem tej rodziny – w skali gotowości technologicznej stoją na poziomie 7…8, co oznacza gotowe wyroby sprzedawane odbiorcom. W październiku 2025 roku pierwszy kwantowy zegar optyczny zainstalowano na okręcie podwodnym Royal Navy. Zastosowanie jest bezpośrednie: okręt pod wodą nie odbiera sygnału satelitarnego, a nawigacja bezwładnościowa wymaga bardzo dokładnego odmierzania czasu. Te same zegary synchronizują sieci telekomunikacyjne, energetyczne i systemy transakcyjne giełd.

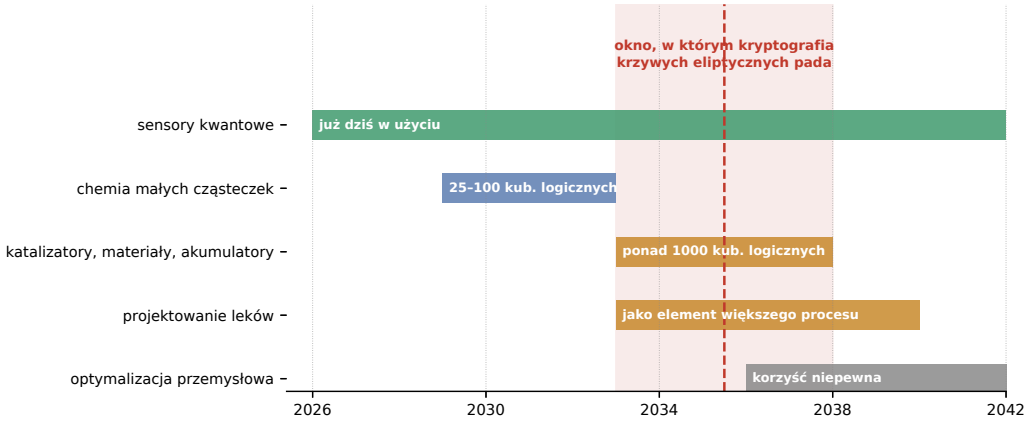
Magnetometry – na centrach barwnych w diamencie albo na parach metali alkalicznych – stoją o szczebel niżej, na poziomie 6…7. Mierzą pola miliardy razy słabsze od ziemskiego, i to bez chłodzenia ciekłym helem, którego wymagały poprzednie rozwiązania. Otwiera to dwa zastosowania: obrazowanie pracy serca i mózgu z czułością dotąd zarezerwowaną dla dużych ośrodków oraz wykrywanie obiektów podziemnych – rur, pustek, niewybuchów.

Nawigacja bez sygnału satelitarnego jest zastosowaniem, które napędza dziś większość finansowania. W sierpniu 2024 roku Boeing przeprowadził pierwszy lot z nawigacją opartą wyłącznie na kwantowej jednostce bezwładnościowej, bez odbiornika satelitarnego. Rozwijane są też układy porównujące zmierzone pole magnetyczne Ziemi z mapą anomalii magnetycznych – przyrząd wie, gdzie jest, bo rozpoznaje magnetyczny „odcisk palca" terenu. Grawimetry kwantowe, mierzące zmiany przyspieszenia ziemskiego, pozostają na wcześniejszym etapie, ale pozwalają wykrywać pustki i złoża bez wiercenia.



Najważniejszy wniosek tego rozdziału mieści się w jednym spostrzeżeniu: sztandarowy problem chemii kwantowej i atak na kryptografię krzywych eliptycznych wymagają maszyny tej samej wielkości. Dzień, w którym chemia dostanie swoje narzędzie, będzie tym samym dniem, w którym kryptografia straci swoje zabezpieczenie.

Rysunek 3.4. Ile kubitów logicznych potrzebuje która dziedzina. Zestawienie ujawnia fakt, który w osobnych doniesieniach zwykle umyka: sztandarowy problem chemii kwantowej i atak na kryptografię krzywych eliptycznych wymagają maszyny tej samej wielkości



Wszystkie przedziały są orientacyjne i opierają się na dzisiejszych szacunkach zapotrzebowania na kubity logiczne oraz na zapowiedziach producentów sprzętu. Nie są prognozą — są zestawieniem tego, co z czego wynika, jeśli obecne mapy drogowe zostaną dotrzymane.

Rysunek 3.5. Przełożenie zapotrzebowania na kubity logiczne na kalendarz, przy założeniu, że zapowiedzi producentów sprzętu zostaną dotrzymane. Czerwony pas oznacza okno, w którym według tych samych zapowiedzi kryptografia krzywych eliptycznych przestaje być bezpieczna

Trzeba przy tym powiedzieć wprost, skąd biorą się na to pieniądze. Dominującym odbiorcą jest wojsko, a bezpośrednim powodem – założenie, że w konflikcie sygnał nawigacji satelitarnej będzie zagłuszony lub podrobiony. Prognozy wielkości rynku różnią się kilkukrotnie, od kilkuset milionów do dwóch miliardów dolarów w 2030 roku, co samo w sobie mówi, jak wczesna jest to faza.

3.6. Kiedy? Drabina i kalendarz

Zbierzmy teraz to wszystko w jedną odpowiedź na pytanie, które w tym rozdziale jest najważniejsze: kiedy poszczególne dziedziny dostaną to, na co czekają. Miarą nie jest data, lecz liczba kubitów logicznych – bo to ona przekłada się na kalendarz przez mapy drogowe producentów, opisane w rozdziale drugim.

To jest kluczowe spostrzeżenie całego numeru i warto je wypowiedzieć wprost. Wzorcowe zadanie chemii kwantowej wymaga od 1137 do 2142 kubitów logicznych. Atak na 256-bitowy klucz eliptyczny wymaga około 1200. **Są to te same maszyny.** Nie istnieje scenariusz, w którym chemia dostaje swoje narzędzie, a kryptografia zachowuje bezpieczeństwo

Tabela 3.1. Kto na czym skorzysta i czego do tego potrzebuje

Dziedzina	Co dokładnie zyska	Potrzebne kubity logiczne	Ocena
Sensory kwantowe	pomiar czasu, pola magnetycznego, grawitacji; nawigacja bez satelitów	zero	DZIAŁA DZIŚ
Chemia małych cząsteczek	dokładna energia i mechanizm reakcji dla układów kilkudziesięcioatomowych	25…100	prawdopodobne
Katalizatory i materiały	projektowanie katalizatorów, elektrolitów, nadprzewodników	ponad 1000	prawdopodobne
Leki	energia wiązania z białkiem, mechanizmy enzymów metalicznych	ponad 1000, jako etap procesu	częściowe
Optymalizacja przemysłowa	trasy, portfele, harmonogramy	nieustalone	WĄTPLIWE
Uczenie maszynowe na danych klasycznych	przyspieszenie uczenia	nieustalone	WĄTPLIWE
Fizyka podstawowa	symulacja układów niedostępnych eksperymentowi	od kilkudziesięciu wzwyż	prawdopodobne

– chyba że zdąży się przezbroić wcześniej, o czym mówi rozdział szósty.

Wyjątkiem od tej reguły są dwa końce skali. Sensory kwantowe działają już teraz, bo nie potrzebują kubitów logicznych w ogóle. Chemia małych cząsteczek – dwadzieścia pięć do stu kubitów logicznych – mieści się poniżej progu kryptograficznego i mogłaby przynieść pierwsze wyniki użytkowe jeszcze przed nim. Na drugim końcu stoi optymalizacja przemysłowa, w której nie wiadomo nawet, czy korzyść w ogóle wystąpi.

Na koniec warto wrócić do Feynmana. Jego wykład z 1981 roku nie zapowiadał łamania szyfrów ani projektowania leków. Zapowiadał urządzenie, którym fizyk mógłby badać układy kwantowe niedostępne eksperymentowi – materię w ekstremalnych warunkach, zachowanie pól kwantowych, procesy zachodzące w ułamkach sekundy po Wielkim Wybuchu. Ta część obietnicy jest realizowana najciszej i najkonsekwentniej, bo nie potrzebuje uzasadnienia gospodarczego.

W następnym rozdziale przechodzimy na drugą stronę bilansu. Zobaczymy, kto na Q-Day straci – i przekonamy się, że lista ta jest znacznie dłuższa od listy beneficjentów, a przede wszystkim **znacznie bardziej konkretna**. Nadzieje z tego rozdziału są warunkowe i rozłożone na dekadę. Zagrożenia z następnego dotyczą urządzeń, które już dziś schodzą z linii produkcyjnych. ■

Bibliografia

[27] Feynman R. P., Simulating Physics with Computers, „International Journal of Theoretical Physics" 1982, t. 21, s. 467–488. DOI: 10.1007/BF02650179. Wykład wygłoszony w maju 1981 roku na konferencji MIT–IBM.
[28] Reiher M., Wiebe N., Svore K. M., Wecker D., Troyer M., Elucidating Reaction Mechanisms on Quantum Computers, „Proceedings of the National Academy of Sciences" 2017, t. 114, nr 29, s. 7555–7560. DOI: 10.1073/pnas.1619152114.
[29] Lee J., Berry D. W., Gidney C. i in., Even More Efficient Quantum Computations of Chemistry through Tensor Hypercontraction, „PRX Quantum" 2021, t. 2, 030305. DOI: 10.1103/PRXQuantum.2.030305.
[30] Zhai H., Li C., Zhang X., Li Z., Lee S., Chan G. K.-L., Classical Solution of the FeMo-Cofactor Model to Chemical Accuracy and Its Implications, preprint arXiv:2601.04621, styczeń 2026.
[31] Chan G. K.-L., The FeMo-Cofactor and Classical and Quantum Computing, blog Quantum Frontiers, 12 marca 2026 – komentarz autora prostujący rozpowszechnione interpretacje pracy [30]. https://quantumfrontiers.com/2026/03/12/the-femo-cofactor-and-classical-and-quantum-computing/ [dostęp: 5.08.2026].
[32] Alexeev Y., Batista V. S., Bauman N. i in., A Perspective on Quantum Computing Applications in Quantum Chemistry Using 25–100 Logical Qubits, „Journal of Chemical Theory and Computation" 2025, t. 21, s. 11335–11357.
[33] Quantum Computing in Transition, „Nature Biotechnology" 2026. DOI: 10.1038/s41587-026-03233-x.
[34] Q-CTRL, Q-CTRL Delivers 3,000× Speedup in Materials Discovery for the Energy Sector, komunikat prasowy, Sydney, 6 maja 2026 – deklaracja producenta, bez niezależnego potwierdzenia.
[35] Tang E., A Quantum-Inspired Classical Algorithm for Recommendation Systems, [w:] Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, ACM, 2019, s. 217–228. DOI: 10.1145/3313276.3316310. Praca zapoczątkowująca nurt dekwantyzacji.
[36] Quantum Sensing Technology Landscape 2026, PatSnap, kwiecień 2026 – zestawienie poziomów gotowości technologicznej dla zegarów atomowych, magnetometrów i grawimetrów.
[37] Quantum Sensors Market 2026–2046: Technology, Trends, Players, Forecasts, IDTechEx, 2026.

Ponadto w rozdziale przywołano pozycje [3] i [6] z bibliografii rozdziału 1 oraz mapy drogowe producentów sprzętu, pozycje [8], [21] i [23] z bibliografii rozdziałów 1 i 2.

Rozdział 4.

Kto ma powód do niepokoju

Nadzieje z poprzedniego rozdziału były warunkowe i rozłożone na dekadę. Zagrożenia natomiast są konkretne i dotyczą urządzeń, które właśnie schodzą z linii produkcyjnych. Zanim jednak przejdziemy do listy zagrożeń, trzeba wprowadzić istotne rozróżnienie. Q-Day nie jest jednym zagrożeniem. Są dwa rodzaje zagrożeń o zupełnie różnych zegarach.

4.1. Dwa zegary

Kryptografia klucza publicznego pełni w dzisiejszych systemach dwie osobne funkcje. Bywają realizowane tymi samymi algorytmami, więc łatwo je pomylić – a różnią się wszystkim, co dla planowania istotne.

Funkcja pierwsza to poufność. Dwie strony, które nigdy się nie spotkały, muszą uzgodnić wspólny sekret przez otwartą sieć, żeby dalej rozmawiać już szyfrem symetrycznym. Do tego służą mechanizmy uzgadniania klucza, opisane w rozdziale pierwszym.

Funkcja druga to autentyczność. Odbiorca musi mieć pewność, że wiadomość pochodzi od tego, kto się pod nią podpisał, i że po drodze jej nie zmieniono. Do tego służy podpis cyfrowy.

Teraz kluczowa różnica. Aby złamać poufność, napastnik nie musi mieć komputera kwantowego w chwili rozmowy. Wystarczy, że zapisze zaszyfrowany ruch i poczeka. Aby podrobić podpis, musi mieć działającą maszynę dokładnie wtedy, kiedy próbuje kogoś oszukać – sfałszowanie podpisu pod dokumentem, który wysłano dziesięć lat temu, nie ma sensu, bo dokument już dawno przyjęto albo odrzucono.

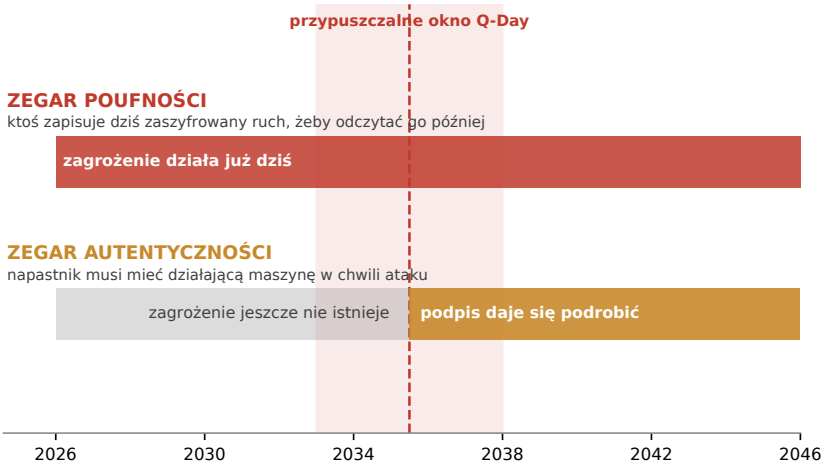
Praktyczna konsekwencja jest jednoznaczna: **wymianę mechanizmów uzgadniania klucza trzeba przeprowadzić najszybciej jak tylko można, a wymianę podpisów można odłożyć w czasie**. Tak właśnie zbudowane są wszystkie oficjalne harmonogramy – amerykańskie rozporządzenie wykonawcze wyznacza koniec 2030 roku dla kluczy i koniec 2031 dla podpisów. Tak też postąpił internet: ponad dwie trzecie ruchu w sieci Cloudflare korzysta już z postkwantowego uzgadniania klucza, podczas gdy postkwantowe certyfikaty pozostają w fazie prac normalizacyjnych.

Od tej reguły istnieje jednak wyjątek i to on tworzy najtrudniejsze przypadki w całym rozdziale. Dotyczy podpisów, które mają zachować moc dowodową przez dziesięciolecia: aktu notarialnego, wpisu do księgi wieczystej, podpisanego cyfrowo oprogramowania sterującego urządzeniem, które przepracuje dwadzieścia lat. W tych przypadkach zegar autentyczności zachowuje się jak zegar poufności – bo dokument podpisany dziś musi pozostać wiarygodny długo po Q-Day.

4.2. Infrastruktura zaufania: co dokładnie pęka

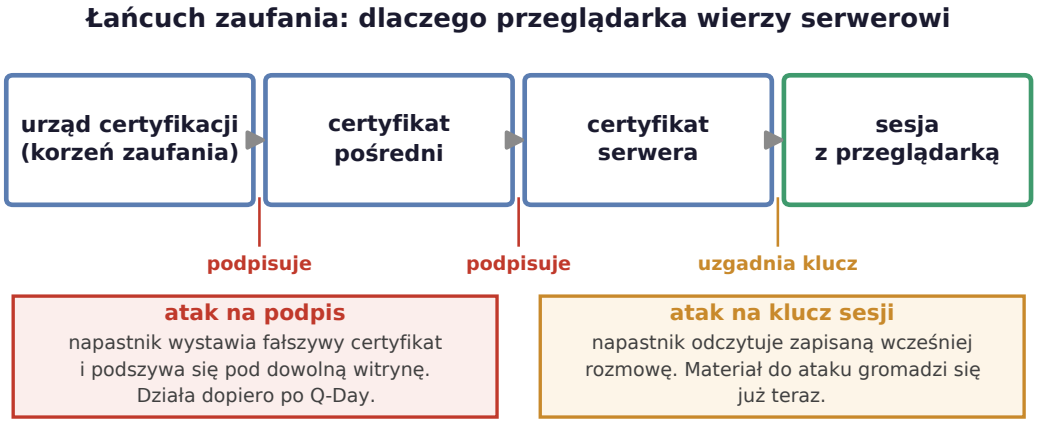
Zacznijmy od mechanizmu, który jest niewidoczny, a od którego zależy wszystko inne. Kiedy w pasku przeglądarki pojawia się kłódka, znaczy to, że zadziałał łańcuch certyfikatów.

W przeglądarce i w systemie operacyjnym zapisano listę kilkudziesięciu urzędów certyfikacji, którym producent oprogramowania postanowił ufać. Urząd taki podpisuje certyfikaty pośrednie, te podpisują certyfikaty poszczególnych serwerów, a serwer przedstawia swój certyfikat przy każdym połączeniu. Przeglądarka



Z tego rozróżnienia wynika kolejność prac. Wymiana kluczy szyfrujących jest pilna teraz, bo przechwycony dziś ruch da się odczytać za piętnaście lat. Podpisy cyfrowe wolno wymienić później, bo podrobić je można dopiero wtedy, gdy maszyna faktycznie zadziała — ale dotyczy to wyłącznie podpisów składanych na bieżąco, nie tych, które mają zachować moc dowodową przez dziesięciolecia.

Rysunek 4.1. Dwa zegary o różnych momentach startu. Zegar poufności ruszył już; zegar autentyczności zacznie chodzić dopiero w dniu Q. To rozróżnienie wyznacza kolejność prac migracyjnych w każdej organizacji na świecie



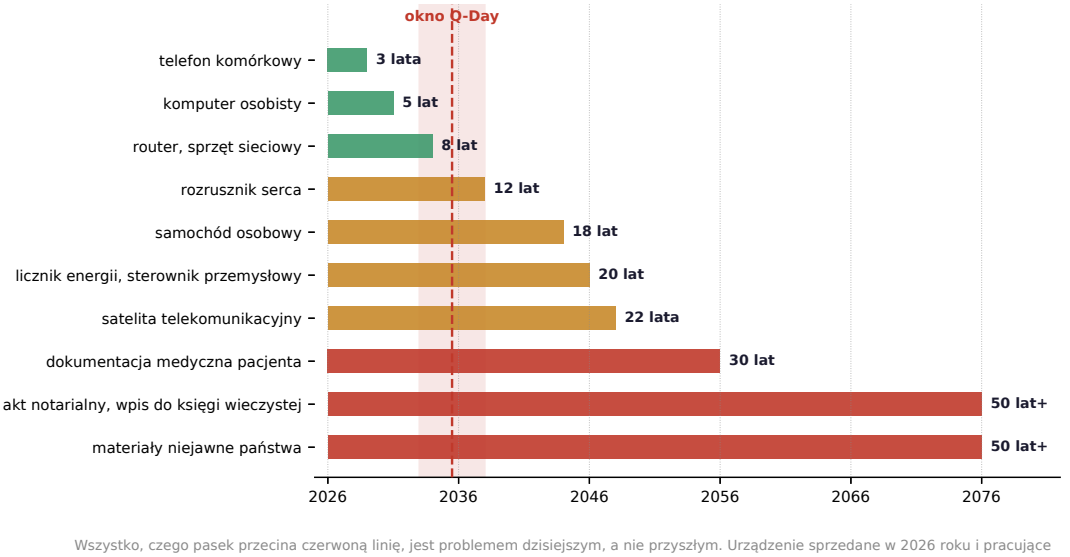
Rysunek 4.2. Uproszczony łańcuch zaufania w internecie. Czerwone ogniwa to podpisy cyfrowe, złote – uzgadnianie klucza sesji. Każde z nich pada na inny sposób i w innym momencie

sprawdza podpisy wstecz aż do korzenia, a jeśli wszystkie się zgadzają – uznaje, że rozmawia z tym, z kim chciała.

Cały ten łańcuch trzyma się na podpisach cyfrowych, czyli na kryptografii krzywych eliptycznych albo na RSA. Po Q-Day napastnik dysponujący kluczem prywatnym dowolnego urzędu certyfikacji mógłby wystawić poprawny certyfikat na dowolną domenę. **Skutek: nie da się już odróżnić prawdziwego banku od podrobionego**, a mechanizm, który miał to rozstrzygać, sam potwierdza fałszywkę.

Osobno pada uzgadnianie klucza sesji. Tu, jak wiemy z pierwszego rozdziału, zagrożenie jest cofnięte w czasie: rozmowa przechwycona dziś zostaje odczytana wtedy, gdy maszyna wreszcie powstanie.

Ten sam mechanizm łańcucha zaufania pracuje w wielu miejscach, o których na co dzień się nie myśli: w połączeniach VPN, w zdalnym dostępie do serwerów, w uwierzytelnianiu abonenta w sieci komórkowej, w kartach płatniczych, w podpisywaniu aktualizacji systemu operacyjnego. Nie są to osobne



Rysunek 4.3. Czas życia wybranych danych i urządzeń, odmierzany od 2026 roku. Pasek, który przecina czerwoną linię, oznacza problem istniejący dzisiaj – niezależnie od tego, kiedy dokładnie wypadnie Q-Day

Polski przykład: notariusz, księga wieczysta i archiwum

Od 2018 roku polscy notariusze umieszczają elektroniczne wypisy aktów notarialnych w Centralnym Repozytorium Elektronicznych Wypisów Aktów Notarialnych, podpisując je podpisem kwalifikowanym. Nowelizacja obowiązująca od 17 marca 2026 roku rozszerzyła zakres czynności prowadzonych w tej formie.

Powstaje z tego pytanie, na które nie ma jeszcze dobrej odpowiedzi. Akt notarialny dotyczący nieruchomości bywa podstawą roszczeń przez dziesięciolecia. Co się stanie, jeśli w 2040 roku okaże się, że **podpis pod dokumentem z 2026 roku da się podrobić z mocą wsteczną?** Formalnie dokument pozostaje ważny, praktycznie zaś przestaje być dowodem, bo nie da się odróżnić oryginału od fałszerstwa wytworzonego później.

Rozwiązaniem jest zaświadczanie czasu: kwalifikowany znacznik czasu potwierdza, że podpis istniał przed dniem, w którym algorytm przestał być bezpieczny. Unijne rozporządzenie w wersji z 2024 roku wprowadza usługę kwalifikowanej archiwizacji elektronicznej właśnie po to, by moc dowodowa dokumentów przetrwała zmianę algorytmów. Warunek jest jeden: znacznik musi zostać nałożony przed Q-Day, a nie po nim. Dokumenty podpisywane dziś, bez takiego zabezpieczenia, będą wymagały późniejszego przepodpisania – o ile ktokolwiek się tym zajmie.

problemy – to jeden problem widziany z kilkunastu stron.

4.3. Dane, które muszą przetrwać dekady

Reguła Mosca z rozdziału pierwszego mówiła, że o pilności decyduje suma czasu migracji i horyzontu tajności danych. Przyjrzyjmy się teraz temu drugiemu składnikowi.

Dokumentacja medyczna jest przypadkiem podręcznikowym. Wynik badania genetycznego pozostaje prawdziwy przez całe życie pacjenta i przez połowę życia jego dzieci; rozpoznanie choroby psychicznej sprzed dwudziestu lat wciąż może zaważyć na zatrudnieniu albo na składce ubezpieczeniowej. Przepisy nakazują przechowywać dokumentację przez dwadzieścia lat, a w niektórych przypadkach dłużej – ale wrażliwość danych nie wygasa razem z obowiązkiem archiwizacji.

Akta państwowe i materiały niejawne mają horyzont jeszcze dłuższy. Klauzule tajności zdejmuje się zwykle po trzydziestu, pięćdziesięciu albo więcej latach; do tego czasu zawartość ma pozostać nieznana. Dla służb wywiadowczych oznacza to, że ruch przechwycony przez obcą służbę w 2026 roku jest realnym zagrożeniem operacyjnym – i że decyzja o zabezpieczeniu tej komunikacji powinna zapaść wczoraj.

Dokumenty o mocy prawnej tworzą kategorię odrębną, bo tu zagrożona jest nie poufność, lecz sama możliwość udowodnienia, że dokument jest autentyczny. Podpis kwalifikowany ma na gruncie prawa unijnego skutek równy podpisowi własnoręcznemu, a opiera się na tej samej kryptografii co reszta.

Tajemnice przedsiębiorstw bywają w tym zestawieniu pomijane, choć ich horyzont bywa równie długi. Dokumentacja konstrukcyjna silnika lotniczego, receptura, wyniki badań klinicznych, warunki wieloletniego kontraktu – wszystko to ma wartość handlową przez dziesięciolecia. Wywiad gospodarczy jest w tym obszarze zjawiskiem opisanym i dobrze udokumentowanym, a koszt zapisania przechwyconego ruchu jest dziś bliski zeru.

4.4. Pieniądze: sektor finansowy

Bankowość jest szczególnym przypadkiem nie dlatego, że kryptografia jest tam inna, lecz dlatego, że systemy są stare, wzajemnie połączone i nie da się ich wyłączyć nawet na godzinę.

Najlepszym dostępnym świadectwem tego, jak trudna jest ta migracja, jest druga faza projektu Leap, prowadzonego przez Bank Rozrachunków Międzynarodowych wspólnie z bankami centralnymi Włoch, Francji i Niemiec oraz z operatorem sieci Swift. Zespół podmienił mechanizm podpisów cyfrowych na postkwantowy w działającym systemie rozliczeń Target2 – czyli w infrastrukturze, przez którą przechodzą płatności międzybankowe strefy euro.

Wynik ogłoszony w grudniu 2025 roku jest umiarkowanie optymistyczny i bardzo pouczający. Podmiana okazała się wykonalna, ale wymagała zmian w wielu komponentach naraz, ujawniła istotne różnice w wydajności i wykazała, że **największe trudności nie mają charakteru technicznego**. Były nimi: ustalenie, gdzie w ogóle w systemie używa się

kryptografii, brak kompetencji w zespołach utrzymaniowych i koordynacja między instytucjami, które muszą wykonać zmianę jednocześnie.

Ta ostatnia obserwacja jest ogólna i wróci w rozdziale szóstym. Migracja kryptograficzna nie jest projektem informatycznym – jest projektem organizacyjnym, w którym część zadania polega na sporządzeniu spisu tego, czego nikt nigdy nie spisywał.

Do tego dochodzą przepisy. Unijne rozporządzenie o odporności cyfrowej sektora finansowego, znane jako DORA, wymaga od instytucji finansowych zarządzania ryzykiem teleinformatycznym w sposób udokumentowany. Ryzyko kwantowe mieści się w tej definicji, choć nie zostało w niej wymienione z nazwy – co oznacza, że nadzór może go wymagać, a instytucja nie ma jak się zasłonić brakiem wyraźnego przepisu.

4.5. Urządzenia, których nie da się zaktualizować

Tu dochodzimy do przypadku najtrudniejszego w całym numerze – trudniejszego nawet niż kryptowaluty z następnego rozdziału, bo tam przynajmniej wiadomo, kto miałby podjąć decyzję.

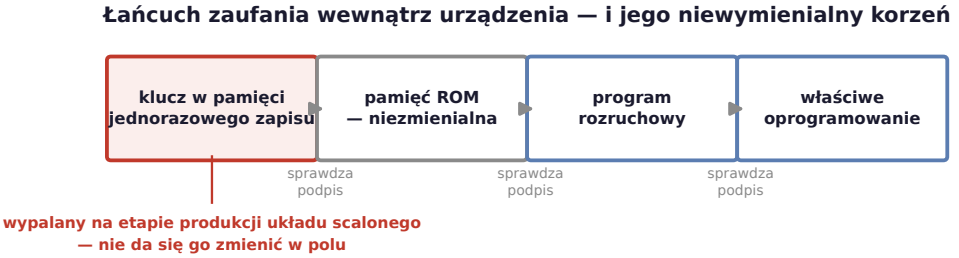
Aby zrozumieć, na czym polega kłopot, trzeba zajrzeć do środka dowolnego urządzenia z oprogramowaniem układowym – sterownika w samochodzie, licznika energii, routera, rozrusznika serca.

Aby urządzenie nie dało się przejąć przez podmianę oprogramowania, stosuje się bezpieczny rozruch. Niezmienialna pamięć ROM sprawdza podpis programu rozruchowego, ten sprawdza podpis kolejnego etapu, ten – podpis właściwego oprogramowania. Ciąg zaczyna się

od klucza publicznego wypalonego w pamięci jednorazowego zapisu, zwanej OTP, na etapie produkcji układu. Wypalenie jest nieodwracalne: taka pamięć zmienia stan tylko raz i celowo nie przewidziano sposobu, by go cofnąć. Właśnie ta nieodwracalność jest jej zaletą – dzięki niej napastnik nie podmieni korzenia zaufania.

I tu tkwi pułapka. Jeżeli w tym korzeniu zapisano klucz oparty na krzywej eliptycznej, to po Q-Day napastnik może wyprowadzić odpowiadający mu klucz prywatny i podpisać własne oprogramowanie, które urządzenie przyjmie jako prawdziwe. **Aktualizacja oprogramowania nie pomoże, bo to właśnie ten klucz rozstrzyga, czy aktualizacja zostanie w ogóle przyjęta.** Urządzenie pozostaje podatne do końca swojego życia, a jedynym lekarstwem jest wymiana sprzętu.

Amerykańska agencja bezpieczeństwa narodowego uznała z tego powodu podpisywanie oprogramowania układowego za zadanie o najwyższym priorytecie w całej migracji postkwantowej – wyżej niż szyfrowanie komunikacji. Zalecane rozwiązania są dostępne od kilku lat: podpisy oparte na funkcjach skrótu, oznaczane



Jeżeli w tym korzeniu zapisano klucz oparty na krzywej eliptycznej, urządzenie pozostaje podatne do końca swojego życia. Nie pomoże aktualizacja oprogramowania: to właśnie ten klucz decyduje, czy aktualizacja zostanie w ogóle przyjęta.

Rysunek 4.4. Bezpieczny rozruch w czterech etapach. Każdy sprawdza podpis następnego, a cały ciąg zaczyna się od klucza wypalonego w pamięci jednorazowego zapisu na etapie produkcji układu scalonego

Motoryzacja: przepisy, które zderzą się z Q-Day

Samochód sprzedany w 2026 roku będzie jeździł przeciętnie osiemnaście lat, a więc do połowy lat czterdziestych. W tym czasie musi przyjmować aktualizacje oprogramowania – i to nie z uprzejmości producenta, lecz z mocy przepisów.

Regulaminy Europejskiej Komisji Gospodarczej ONZ o numerach 155 i 156, obowiązujące w Unii dla nowych typów pojazdów, wymagają od producenta systemu zarządzania cyberbezpieczeństwem oraz zdolności do bezpiecznego aktualizowania oprogramowania przez cały cykl życia pojazdu. Norma ISO/SAE 21434 rozpisuje to na wymagania techniczne. **Producent ma więc prawny obowiązek zapewnienia bezpiecznych aktualizacji przez osiemnaście lat, a mechanizm, którym je zabezpiecza, ma przestać być bezpieczny mniej więcej w połowie tego okresu.**

Rozwiązanie jest znane i nie jest tajemnicą: nowe pojazdy powinny mieć w korzeniu zaufania podpisy oparte na funkcjach skrótu albo przynajmniej możliwość wymiany algorytmu. Zderzenie polega na tym, że decyzja o architekturze układu scalonego zapada trzy lata przed pierwszym egzemplarzem z taśmy, a układy projektowane w 2026 roku trafią do samochodów sprzedawanych w latach trzydziestych.

skrótami LMS i XMSS, opisane w normie NIST SP 800-208, oraz ich bezstanowy odpowiednik SLH-DSA. Ich zaletą jest to, że opierają się wyłącznie na funkcjach skrótu, a więc na jedynym mechanizmie, który po Q-Day pozostaje nienaruszony.

Problemem jest rozmiar. Podpis w standardzie ML-DSA na poziomie średnim zajmuje 3309 bajtów, podczas gdy dotychczasowy podpis na krzywej eliptycznej mieści się w sześćdziesięciu czterech. Dla urządzenia komunikującego się przez wąskie łącze radiowe oznacza to konieczność dzielenia komunikatu na kilkadziesiąt części, co wydłuża transmisję i zużywa baterię. Dla układu z kilkudziesięcioma kilobajtami pamięci oznacza to czasem, że podpis nie mieści się w ogóle.

Podobnie wygląda sytuacja satelitów, z jedną różnicą na niekorzyść: do satelity nie da się podejść. Komercyjne satelity geostacjonarne pracują od piętnastu do dwudziestu pięciu lat, a satelita wyniesiony w 2026 roku będzie na orbicie w latach czterdziestych. Najbardziej wrażliwym elementem jest łącze telekomend, czyli kanał, którym wysyła się polecenia sterujące – podrobienie podpisu na takim poleceniu oznacza przejęcie kontroli nad pojazdem. Branża wskazuje ten kanał jako zadanie migracyjne o najwyższym priorytecie i podkreśla zasadę, którą warto zapamiętać: doposażenie

Tabela 4.1. Przegląd sektorów

Sektor	Co dokładnie jest zagrożone	Który zegar	Trudność migracji
Internet, usługi sieciowe	certyfikaty, uzgadnianie klucza sesji	oba	niska – trwa
Ochrona zdrowia	archiwa, systemy obrazowania, wymiana danych między placówkami	poufności	średnia
Administracja publiczna	podpis kwalifikowany, rejestry, archiwa niejawne	oba	wysoka
Finanse	rozliczenia międzybankowe, karty płatnicze, podpisy transakcji	oba	wysoka
Telekomunikacja	uwierzytelnianie abonenta, karty SIM, sieci szkieletowe	oba	średnia
Motoryzacja	korzeń zaufania w sterownikach, aktualizacje zdalne	autentyczności	**BARDZO WYSOKA**
Kosmonautyka	łącze telekomend, telemetria	autentyczności	**BARDZO WYSOKA**
Energetyka i przemysł	sterowniki, liczniki, systemy nadzoru	autentyczności	**BARDZO WYSOKA**
Urządzenia medyczne	oprogramowanie implantów i aparatury	autentyczności	**BARDZO WYSOKA**

po starcie nie jest możliwe, a jedyną drogą wyjścia jest wymiana algorytmu przez aktualizację oprogramowania w granicach zasobów, które zaprojektowano wcześniej.

Do tej samej rodziny należą sterowniki przemysłowe w elektrowniach i wodociągach, liczniki energii i wody instalowane na dwadzieścia lat, urządzenia medyczne wszczepiane pacjentom oraz cała infrastruktura, którą wymienia się nie wtedy, gdy wygasa jej kryptografia, lecz wtedy, gdy się zepsuje.

4.6. Czego Q-Day nie dotknie

Dla higieny tego rozdziału trzeba wyraźnie powiedzieć, co pozostaje bezpieczne – bo doniesienia prasowe zwykle sugerują, że pada wszystko.

Szyfrowanie danych szyfrem symetrycznym pozostaje bezpieczne, o ile klucz ma 256 bitów. Funkcje skrótu pozostają bezpieczne. Kody uwierzytelniające wiadomość, oparte na funkcjach skrótu, pozostają bezpieczne. Hasła przechowywane w poprawnie zaprojektowanym systemie pozostają bezpieczne, bo chroni je funkcja skrótu, a nie kryptografia klucza publicznego. Kopie zapasowe na taśmach, zaszyfrowane szyfrem symetrycznym i przechowywane w sejfie, są w tym zestawieniu jednym z najbezpieczniejszych rozwiązań, jakie istnieją.

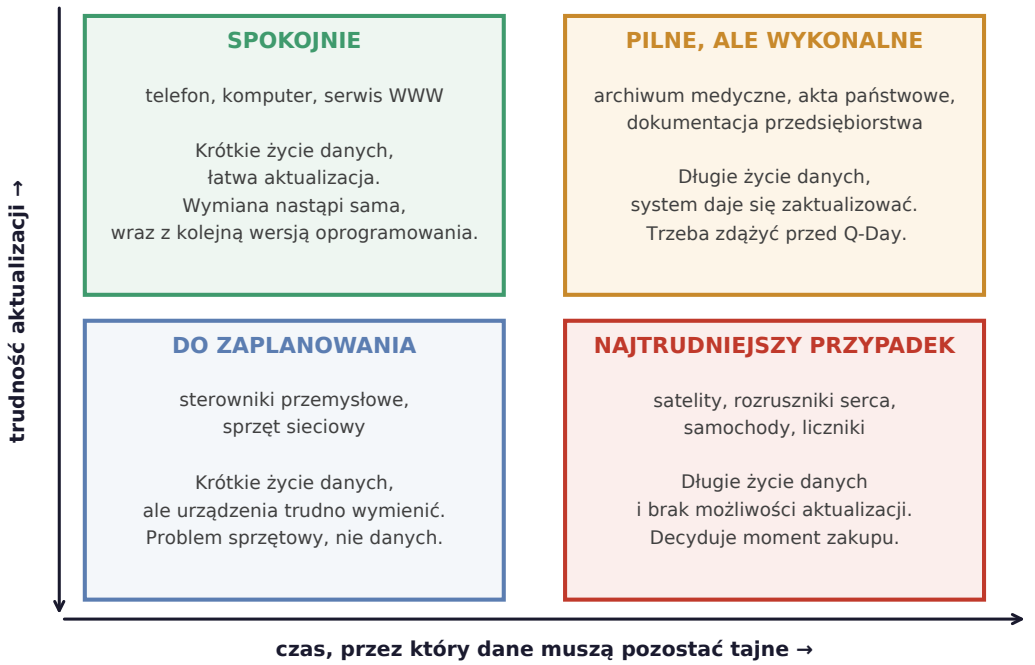
Warto tę listę czytać uważnie, bo wynika z niej praktyczna wskazówka: **problemem nie jest szyfrowanie danych w spoczynku, lecz wszystko, co wymaga porozumienia między dwiema stronami**. Dysk zaszyfrowany w laptopie przetrwa Q-Day bez zmian. Rozmowa, w której ten laptop uzgadniał klucz z serwerem, już nie.

4.7. Jak ustawić kolejność

Z całego tego przeglądu da się wyprowadzić prostą regułę porządkującą. Nie zależy ona od branży ani od wielkości organizacji, tylko od dwóch pytań: jak długo dane muszą pozostać tajne i czy system da się zaktualizować.

Ćwiartka lewa górna – krótkie życie danych, łatwa aktualizacja – rozwiąże się sama. Telefon kupiony w tym roku dostanie postkwantową kryptografię wraz z kolejną aktualizacją systemu i właściciel się o tym nie dowie. **Prawa górna** – długie życie danych, system da się zaktualizować – jest tym, o czym mówią wszystkie rozporządzenia: trzeba zdążyć, ale da się zdążyć.

Ćwiartka prawa dolna jest jedyną, w której samo zdążenie nie wystarcza, bo problemu nie



Rysunek 4.5. Cztery ćwiartki i cztery różne strategie. Największej uwagi wymaga prawy dolny róg – nie dlatego, że zagrożenie jest tam większe, lecz dlatego, że jest to jedyna ćwiartka, w której decyzja musi zapaść przed zakupem sprzętu

da się rozwiązać po fakcie. **Jeżeli kupujesz dziś urządzenie, które ma pracować do lat czterdziestych, decyzja o jego bezpieczeństwie kwantowym zapada w chwili zakupu i później już nie podlega korekcie.** Właśnie dlatego amerykańskie i unijne dokumenty zaczęły wpisywać odporność kwantową do wymagań przetargowych – jest to jedyny moment, w którym cokolwiek da się jeszcze zmienić.

W następnym rozdziale przyjrzymy się przypadkowi, w którym wszystkie te rachunki dają się przeprowadzić do końca – bo dotyczą systemu, którego zawartość jest w całości jawna. ■

Bibliografia

[38] Bank for International Settlements, Project Leap Phase 2: Quantum-Proofing Payment Systems, BIS Innovation Hub, Bazylea, 11 grudnia 2025. https://www.bis.org/publ/othp107.htm [dostęp: 5.08.2026].
[39] National Institute of Standards and Technology, Recommendation for Stateful Hash-Based Signature Schemes, NIST SP 800-208, Gaithersburg, październik 2020. DOI: 10.6028/NIST.SP.800-208.
[40] National Security Agency, Commercial National Security Algorithm Suite 2.0, CNSA 2.0 – dokument wskazujący podpisywanie oprogramowania układowego jako zadanie o najwyższym priorytecie w migracji postkwantowej.
[41] Europejska Komisja Gospodarcza ONZ, Regulamin nr 155 – jednolite przepisy dotyczące homologacji pojazdów w odniesieniu do cyberbezpieczeństwa oraz Regulamin nr 156 – aktualizacje oprogramowania, Genewa 2021.
[42] ISO/SAE 21434:2021 – Road Vehicles: Cybersecurity Engineering, Międzynarodowa Organizacja Normalizacyjna, Genewa 2021.
[43] Post-Quantum Cryptography for Space Systems: Algorithms, Implementation, and Design Constraints – A Systematic Survey, „Acta Astronautica" 2026. DOI: 10.1016/j.actaastro.2026.04.043.
[44] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS), wraz z rozporządzeniem zmieniającym (UE) 2024/1183 wprowadzającym usługę kwalifikowanej archiwizacji elektronicznej.
[45] Ustawa z dnia 21 listopada 2025 r. o zmianie ustawy – Prawo o notariacie oraz ustawy o księgach wieczystych i hipotece, Dz.U. 2025, poz. 1793, obowiązująca od 17 marca 2026 r.
[46] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA), Bruksela 2022.
[47] Post-Quantum Cryptographic Expiration Date on Every Satellite You're Launching, SpaceComputer, kwiecień 2026 – analiza branżowa dotycząca łącza telekomend.

Ponadto w rozdziale przywołano pozycje [14], [16], [17] i [33] z bibliografii rozdziałów 1 i 2 (Executive Order 14412; wytyczne NCSC; Strategia Cyberbezpieczeństwa RP; dane Cloudflare o udziale ruchu postkwantowego).

Rozdział 5.

Kryptowaluty: najtrudniejszy przypadek

W poprzednim rozdziale opisaliśmy dziedziny, które mają powód do niepokoju. Bitcoin jest wśród nich przypadkiem osobnym z trzech powodów. Po pierwsze, zagrożoną wartość da się policzyć co do monety – wystarczy przejrzeć łańcuch bloków, który jest jawny. Po drugie, nie ma tu zarządu, regulatora ani ministerstwa, które mogłoby zarządzić migrację; decyzję musi podjąć zbiorowo sieć, która z założenia miała nie podlegać niczyjej decyzji. Po trzecie, i najciekawsze: dostępne lekarstwo może okazać się równie dotkliwe jak choroba. Zacznijmy jednak od obalenia nieporozumienia, które w tej sprawie powtarza się najczęściej. (Temat kryptowalut nie należy do szczególnie łatwych, dlatego przed lekturą tego rozdziału polecamy temat numeru w MT 06/2026 – dostępny w ulubionykiosk.pl)

5.1. Kopalnia jest bezpieczna

Pytanie, które pada niemal zawsze, brzmi: co się stanie, kiedy komputer kwantowy wykopie wszystkie bitcoiny? Odpowiedź brzmi: nic, i to z kilku niezależnych powodów naraz. Aby je zrozumieć, trzeba zauważyć, że Bitcoin opiera się na dwóch zupełnie różnych narzędziach kryptograficznych, o odmiennej odporności na atak kwantowy.

Wydobycie, czyli dopisywanie nowych bloków do łańcucha, polega na zgadywaniu. Górnik dobiera liczbę zwaną nonce tak, aby skrót całego bloku, obliczony funkcją SHA-256, okazał się mniejszy od zadanej wartości progowej. Funkcja skrótu nie daje żadnej wskazówki, w którą stronę szukać – każda próba jest tak samo prawdopodobna jak poprzednia. Jedyną metodą jest sprawdzanie po kolei, a jedyną przewagą jest szybkość.

Jak pisaliśmy w rozdziale pierwszym, **algorytm Grovera przyspiesza takie przeszukiwanie pierwiastkowo**: zamiast 2 do potęgi 256 prób wystarczy 2 do potęgi 128. Brzmi to jak połowa pracy, lecz nią nie jest – chodzi o połowę wykładnika, a to nadal liczba astronomiczna. Dokładniejsze analizy pokazują, że atak na SHA-256 prowadzony na maszynie odpornej na błędy kosztowałby rzędu 2 do potęgi 166 cykli pracy kubitów logicznych, czyli setki miliardów razy więcej, niż wynikałoby z samego zliczania zapytań.

To jednak dopiero pierwszy z powodów. Drugi jest znacznie mniej znany, a rozstrzygający.

Algorytm Grovera prawie nie daje się zrównoleglić. Klasyczna kopalnia skaluje się liniowo: dwa razy więcej układów ASIC to dwa razy większa moc obliczeniowa. W przypadku Grovera K maszyn pracujących równolegle daje przyspieszenie zaledwie pierwiastkowe – czyli sto maszyn przyspiesza pracę dziesięciokrotnie, a nie stokrotnie. Cała przewaga algorytmu bierze się z tego, że jedna maszyna wykonuje długi, nieprzerwany ciąg operacji; dzielenie tego ciągu między urządzenia niszczy efekt. Ta sama właściwość ogranicza przydatność algorytmu Grovera w optymalizacji przemysłowej, o czym pisaliśmy w rozdziale trzecim – i z tego samego powodu.

Trzeci powód odpowiada wprost na pytanie, które w tym miejscu nasuwa się każdemu: dlaczego zwykły układ krzemowy za kilka tysięcy złotych bije maszynę kwantową za kilkaset milionów. Chodzi o szybkość – ale nie o szybkość zegara. Chodzi o to, **ile kosztuje jedno obliczenie skrótu w każdej z tych dwóch maszyn**.

Jak liczy układ ASIC. Nie jest to procesor. Nie wykonuje programu, nie ma pamięci operacyjnej ani systemu operacyjnego. Funkcja SHA-256 jest w nim wytrawiona w krzemie jako nieruchomy układ bramek logicznych – dosłownie ścieżka, którą sygnał elektryczny przebiega od wejścia do wyjścia. Takich ścieżek jest w jednym układzie kilkaset i pracują niezależnie od siebie. Co więcej, każda z nich jest potokowa: zanim jedna wartość dobiegnie do końca, na wejście wchodzi już następna, tak jak kolejne samochody wjeżdżają na taśmę montażową, nie czekając, aż poprzedni zjedzie. Efekt jest taki, że układ kończy jeden skrót na każdej ze ścieżek co takt zegara. Stąd bierze się 110 bilionów skrótów na sekundę z jednej kostki wielkości znaczka pocztowego.

Jest jeszcze druga właściwość, o której łatwo zapomnieć: **układowi ASIC wolno się mylić**. Źle policzony skrót po prostu nie trafi w cel i zostanie wyrzucony razem z miliardami innych nietrafionych. Gdyby przypadkiem trafił mimo błędu, sieć odrzuci nieprawidłowy blok. Dlatego kopalnie projektuje się na granicy stabilności – podkręcone, gorące, z niezerowym odsetkiem pomyłek. Błąd nic tu nie kosztuje.

Jak liczy komputer kwantowy. Każdy z tych warunków jest odwrócony. Po pierwsze, funkcję SHA-256 trzeba zbudować od nowa z bramek kwantowych, i to w postaci odwracalnej – obliczenie kwantowe nie może po drodze niczego zapomnieć ani nadpisać, bo zniszczyłoby to stan, na którym pracuje. Taki obwód liczy setki tysięcy bramek logicznych, a znaczna ich część wymaga stanów magicznych, o których pisaliśmy w rozdziale drugim. Wytworzenie jednego takiego stanu zajmuje osobną część układu i wiele cykli korekcji błędów, a pojedynczy cykl trwa około mikrosekundy. W rezultacie jeden skrót SHA-256 policzony kwantowo zajmuje – zależnie od architektury – nie nanosekundy, lecz ułamki sekundy albo i całe sekundy.

Po drugie, **komputerowi kwantowemu nie wolno się pomylić**. Niezauważony błąd nie psuje jednego skrótu, tylko rujnuje całe poszukiwanie Grovera, które trzeba zacząć od początku. Stąd bierze się narzut korekcji błędów opisany w rozdziale drugim: setki kubitów fizycznych na jeden logiczny, nieustanne sprawdzanie siatki, kriostat.

Cała ta machineria istnieje po to, żeby jedno obliczenie dobiegło końca w całości – i ona właśnie jest powodem, dla którego pojedynczy krok jest tak kosztowny.

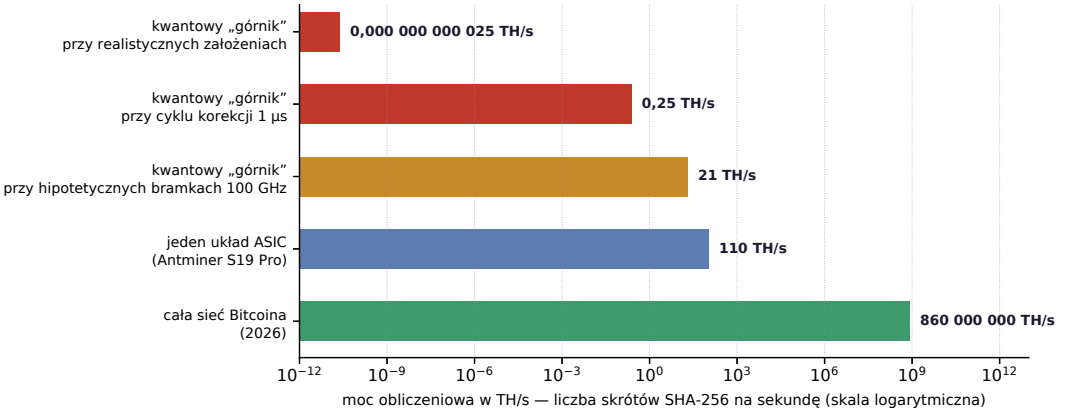
Po trzecie wreszcie – i tu wraca powód drugi – **tej pracy nie da się rozdzielić**. Kopalnia zwiększa moc, dokładając kolejne układy: dwa razy więcej sprzętu to dwa razy więcej prób na sekundę. Poszukiwanie Grovera jest jednym długim, nieprzerwanym ciągiem operacji, którego nie można pociąć na kawałki bez utraty przewagi.

Najprostsza analogia wygląda tak. Klasyczna kopalnia to stadion pełen ludzi, z których każdy niezależnie zgaduje liczby i wykrzykuje wynik. Ilu ich jest, tyle prób pada w każdej sekundzie – **dwa razy więcej zgadujących to dwa razy szybsze poszukiwanie**. To, że część z nich się myli, nikomu nie przeszkadza: błędna odpowiedź po prostu nie trafia w cel i ginie wśród miliardów innych nietrafionych.

Algorytm Grovera działa inaczej. **To jedna osoba idąca bardzo długą, precyzyjnie wyznaczoną ścieżką.** Ścieżka jest istotnie krótsza niż sprawdzanie wszystkich możliwości po kolei – na tym polega przewaga kwantowa. Ale przejść nią może tylko jeden wędrowiec: jedno potknięcie oznacza powrót na start, a dostawienie drugiego nie dzieli drogi na pół. Wędrowcy mogą co najwyżej ruszyć różnymi ścieżkami, a wtedy zysk jest już tylko pierwiastkowy. **Żeby podwoić tempo, potrzeba nie dwóch maszyn, lecz czterech; żeby przyspieszyć dziesięciokrotnie – stu.**

Liczby pochodzą z dwóch niezależnych analiz. Zespół Google przyjął skrajnie optymistyczne założenie, że komputer kwantowy zdoła policzyć jeden skrót SHA-256 w ciągu jednego cyklu korekcji błędów trwającego mikrosekundę. Przy takim założeniu uzyskałby moc 0,25 TH/s – ponad czterysta razy mniej niż popularny układ ASIC Antminer S19 Pro, osiągający około 110 TH/s. Przy założeniach realistycznych wynik spada o ponad dziesięć rzędów wielkości. Niezależna analiza z czerwca 2026 roku sprawdziła wariant jeszcze bardziej życzliwy dla maszyny kwantowej – bramki stukrotnie szybsze niż cokolwiek dziś istniejącego – i otrzymała 21 TH/s, czyli około jednej piątej jednego układu ASIC. Cała sieć Bitcoina pracowała w 2026 roku z mocą około 860 EH/s, co odpowiada mniej więcej 4,3 miliona takich układów. Aby przejąć nad nią kontrolę, trzeba by rzędu 10 do potęgi 13 maszyn kwantowych.

Jest wreszcie powód czwarty, który sam wystarczyłby za wszystkie: **trudność wydobycia dostosowuje się automatycznie**. Co 2016 bloków sieć porównuje rzeczywiste tempo ich powstawania z zakładanym i przelicza próg tak, by średni odstęp znów wynosił dziesięć minut. Gdyby więc ktoś rzeczywiście zbudował szybszego górnika, stałby się po prostu kolejnym uczestnikiem rynku, a nie łamaczem systemu.



Dwa górne słupki to szacunki z pracy zespołu Google. Trzeci pochodzi z niezależnej analizy przy założeniu bramek stukrotnie szybszych niż jakiekolwiek dziś istniejące. Algorytm Grovera prawie się nie zrównolegla: K maszyn daje przyspieszenie tylko pierwiastkowe, podczas gdy farma układów ASIC skaluje się liniowo.

Rysunek 5.1. Wydajność hipotetycznego „górnika kwantowego” w zestawieniu z jednym układem ASIC i z całą siecią. Skala jest logarytmiczna, więc każda podziałka oznacza tysiąckrotność. Nawet przy założeniach, które sami autorzy szacunku nazywają fantastycznymi, maszyna kwantowa przegrywa z pojedynczym układem scalonym za kilka tysięcy złotych

Dwie różne kryptografie w jednym łańcuchu

Zamieszanie wokół kryptowalut bierze się z tego, że Bitcoin używa dwóch rodzajów kryptografii jednocześnie, a atak kwantowy dotyczy tylko jednego z nich.

Funkcje skrótu – SHA-256 w wydobyciu, SHA-256 i RIPEMD-160 przy tworzeniu adresu, zamki skrótowe w kanałach Lightning. Podatne wyłącznie na algorytm Grovera, czyli tracące połowę wykładnika. Pozostają bezpieczne.

Kryptografia krzywych eliptycznych – podpisy ECDSA i Schnorra, którymi posiadacz dowodzi prawa do wydania środków. Podatne na algorytm Shora, czyli łamane całkowicie.

Cała różnica między spokojnym a alarmującym tonem doniesień o kryptowalutach zależy od tego, czy autor rozróżnia te dwa mechanizmy. Zagrożone są podpisy, nie wydobycie.

5.2. Gdzie naprawdę jest luka

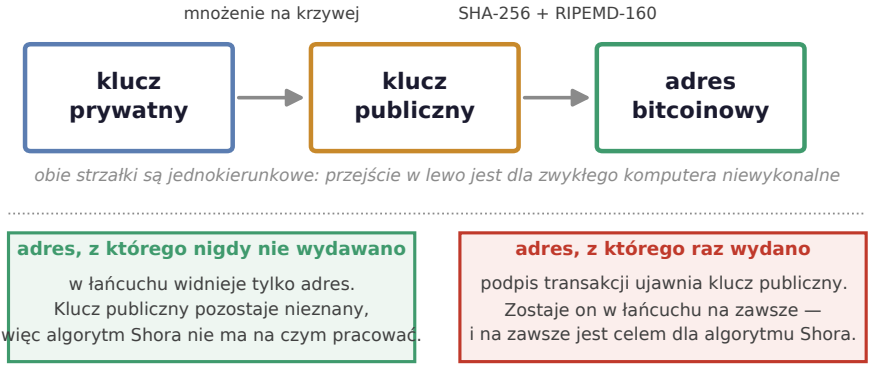
Aby zobaczyć, na czym polega problem, trzeba prześledzić drogę od klucza prywatnego do adresu, na który przyjmujemy przelew.

Klucz prywatny to po prostu bardzo duża liczba losowa – 256 bitów, czyli mniej więcej tyle możliwości, ile jest atomów w obserwowalnym Wszechświecie. Klucz publiczny powstaje z niego przez operację na krzywej eliptycznej o nazwie secp256k1: punkt początkowy krzywej dodaje się do siebie tyle razy, ile wynosi klucz prywatny. Działanie jest łatwe do wykonania i praktycznie niemożliwe do odwrócenia – mając wynik, nie da się ustalić, ile razy wykonano dodawanie. To właśnie problem logarytmu dyskretnego, z rozdziału pierwszego.

Adres bitcoinowy powstaje w kolejnym kroku: klucz publiczny przepuszcza się przez dwie funkcje skrótu, SHA-256 i RIPEMD-160, otrzymując 160-bitowy ciąg. To druga ściana jednokierunkowa. Z adresu nie da się odzyskać klucza publicznego.

I tu pojawia się sedno sprawy. Aby wydać środki, trzeba podpisać transakcję – a podpis ECDSA jest weryfikowalny tylko wtedy, gdy sieć zna klucz publiczny. Klucz trafia więc do łańcucha razem z transakcją. **Od tej chwili jest publiczny na zawsze**, bo łańcuch bloków niczego nie zapomina. Adres, z którego wydano choć raz, jest chroniony już tylko trudnością logarytmu dyskretnego – czyli dokładnie tym, co algorytm Shora rozwiązuje.

Z tego wynika reguła, którą warto zapamiętać: nowy, nigdy nieużywany adres jest chroniony podwójnie, a adres używany ponownie – tylko pojedynczo. Dlatego wszystkie podręczniki bezpieczeństwa zalecają, by każdą wpłatę przyjmować na świeży adres. Zalecenie to powtarzano od lat z powodów związanych z prywatnością; teraz doszedł powód drugi.



Wyjątek najstarszy i najgroźniejszy: w formacie P2PK, używanym w latach 2009–2010, klucz publiczny zapisywano wprost w łańcuchu, bez przeliczania na adres. Monety z tamtego okresu — w tym przypisywane Satoshiemu Nakamoto — są odsłonięte od chwili powstania i nigdy nie były chronione skrótem.

Rysunek 5.2. Dwie ściany jednokierunkowe chroniące środki oraz moment, w którym jedna z nich znika. Dopóki z adresu nie wydano ani razu, klucz publiczny nie jest znany nikomu poza właścicielem. Po pierwszym wydaniu zostaje w łańcuchu na zawsze

Są jednak przypadki, w których ochrona skrótem nigdy nie działała.

Format P2PK, używany w latach 2009–2010, zapisywał klucz publiczny wprost w treści transakcji, bez przeliczania go na adres. Wszystkie monety z tamtego okresu – w tym około miliona bitcoinów przypisywanych Satoshiemu Nakamoto – są odsłonięte od chwili powstania i nigdy nie były chronione skrótem.

Format P2TR, wprowadzony wraz z aktualizacją Taproot w 2021 roku, również umieszcza klucz publiczny bezpośrednio w wyjściu transakcji – taka jest cena wydajności i prywatności, jakie Taproot oferuje. Z punktu widzenia zagrożenia kwantowego oznacza to, że jedna z najnowocześniejszych funkcji Bitcoina jest zarazem jedną z najbardziej odsłoniętych. To dlatego proponowany następca, opisany w dalszej części rozdziału, jest w istocie Taprootem pozbawionym tej właśnie ścieżki.

Warto jeszcze odnotować jeden szczegół, który przewija się w analizach technicznych. Skrót adresu ma 160 bitów, a nie 256. Algorytm Grovera obniża jego odporność do około 80 bitów – to najcieńszy margines w całym systemie. Osiemdziesiąt bitów wciąż pozostaje poza zasięgiem czegokolwiek, co da się zbudować, więc nie jest to zagrożenie praktyczne. Jest to natomiast dobry przykład tego, że w kryptografii bezpieczeństwo wyznacza najsłabsze ogniwo, a nie średnia.

5.3. Ile monet jest już odsłoniętych

Skoro klucz publiczny ujawnia się przy pierwszym wydaniu, a łańcuch bloków jest jawny, to odsetek zagrożonych środków da się po prostu policzyć. Zrobili to autorzy propozycji BIP-361, o której będzie mowa dalej.

Na dzień 1 marca 2026 roku **ponad 34 procent wszystkich wydobytych bitcoinów miało klucz publiczny ujawniony w łańcuchu**. To mniej więcej 6,8 miliona monet, z czego około miliona przypada na adresy z ery P2PK wiązane z twórcą protokołu. Reszta to skutek zwykłego użytkowania: każdy, kto kiedykolwiek wydał środki z danego adresu i zostawił na nim resztę, dołożył się do tej puli.

Cechą tej liczby, którą trzeba podkreślić, jest jej jednokierunkowość. Odsetek może tylko rosnąć. Nie istnieje operacja, która cofnęłaby ujawnienie klucza publicznego – jedynym sposobem ochrony jest przeniesienie środków na adres nowego typu, a to wymaga wykonania transakcji, czyli ponownego ujawnienia klucza starego. Migracja jest więc wyścigiem: każda moneta musi zostać przeniesiona, zanim powstanie maszyna zdolna odczytać jej klucz.

5.4. Dwa rodzaje ataku

Zagrożenie dzieli się na dwa scenariusze o zupełnie różnej dynamice.

Atak długodystansowy dotyczy owych 34 procent. Napastnik nie ma tu żadnej presji czasu: klucz publiczny leży w łańcuchu od lat i będzie leżał dalej. Może spokojnie policzyć klucz prywatny, a potem wybrać moment.

Najbardziej niepokojący wariant tego scenariusza opisali sami autorzy propozycji BIP-361 i warto go przytoczyć, bo zmienia sposób myślenia o całej sprawie. Napastnik, który zdobył zdolność łamania kluczy, nie ma powodu ogłaszać tego światu. Przeciwnie: opłaca mu się wyprowadzać środki powoli, po trochu, przez tygodnie albo miesiące, z wielu różnych adresów, tak aby wyglądało to na zwykły ruch. Serwisy analizujące

Stan na 1 marca 2026 roku, według danych zebranych przez autorów propozycji BIP-361. Odsetek rośnie z każdą transakcją, bo każde wydanie środków ujawnia klucz publiczny adresu.

Rysunek 5.3. Podział podaży bitcoina według stopnia odsłonięcia. Udział monet z ujawnionym kluczem publicznym rośnie z każdą transakcją i nie da się go cofnąć – raz zapisanej informacji nie można z łańcucha usunąć

Średni odstęp między blokami w sieci Bitcoina wynosi dziesięć minut. Szacunek zespołu Google mówi o około dziewięciu minutach potrzebnych na wyprowadzenie klucza prywatnego. To zestawienie, a nie pomiar: dziewięć minut dotyczy hipotetycznej maszyny o mniej niż 500 tysiącach kubitów fizycznych, przy ściśle określonych założeniach o jakości bramek.

Rysunek 5.4. Przebieg ataku krótkodystansowego. Klucz publiczny ujawnia się w chwili nadania transakcji do sieci, a napastnik ma na wszystko tyle czasu, ile zostało do zamknięcia bloku

łańcuch nie zauważyłyby wzorca. W takim scenariuszu Q-Day nie byłby wydarzeniem ogłoszonym – zostałby rozpoznany dopiero po fakcie, długo po tym, jak się wydarzył.

Atak krótkodystansowy jest technicznie trudniejszy, ale dotyczy wszystkich, także tych, którzy nigdy nie używali adresu ponownie. Rozgrywa się w kilkuminutowym oknie między nadaniem transakcji a jej potwierdzeniem.

Mechanizm wygląda następująco. Nadana transakcja trafia najpierw do mempoola – poczekalni, w której czeka na włączenie do bloku. Jest już w niej podpis, a więc i klucz publiczny. Napastnik odczytuje go, wyprowadza klucz prywatny i tworzy własną transakcję, przenoszącą te same środki pod swój adres, ale z wyższą opłatą dla górnika. Zasada zastępowania transakcji wyższą opłatą, znana jako replace-by-fee, jest normalną częścią protokołu i sprawia, że to wersja napastnika trafi do bloku.

Ile czasu ma napastnik? Średni odstęp między blokami wynosi w Bitcoinie dziesięć minut. Szacunek zespołu Google z marca 2026 roku mówi o około dziewięciu minutach potrzebnych na wyprowadzenie klucza prywatnego z 256-bitowej krzywej. Zestawienie tych dwóch liczb robi wrażenie i słusznie – **trzeba jednak pamiętać, że dziewięć minut to nie pomiar, lecz szacunek zasobów** dla hipotetycznej maszyny o mniej niż 500 tysiącach kubitów fizycznych, przy ściśle określonych założeniach o jakości bramek, które omawialiśmy w rozdziale drugim. Żadna taka maszyna nie istnieje.

5.5. Pierwszy realny wyłom

Wszystko powyższe dotyczy maszyn, które jeszcze nie powstały. W kwietniu 2026 roku pojawił się jednak wynik, który po raz pierwszy przeniósł sprawę z rozważań teoretycznych do eksperymentu.

Firma Project Eleven ogłosiła w kwietniu 2025 roku konkurs z nagrodą jednego bitcoina dla tego, kto złamie algorytmem kwantowym najdłuższy klucz na krzywej eliptycznej. Nagrodę przyznano 24 kwietnia 2026 roku. Zwycięzca, Giancarlo Lelli, złamał klucz 15-bitowy, korzystając z ogólnodostępnego sprzętu kwantowego w chmurze. Przestrzeń przeszukiwana w tym zadaniu liczyła 32 767 możliwości.

Dlaczego Q-Day może przejść niezauważony

Wyobrażamy sobie Q-Day jako moment ogłoszenia: konferencja prasowa, komunikat, gwałtowna reakcja rynków. W przypadku kryptowalut najbardziej prawdopodobny przebieg jest odwrotny.

Napastnik dysponujący komputerem łamiącym szyfry ma silny interes w ukryciu tego faktu. Ujawnienie natychmiast obniżyłoby wartość zdobyczy i uruchomiło obronę całego ekosystemu. Racjonalne postępowanie polega więc na cichym, rozłożonym w czasie wyprowadzaniu środków z wielu adresów naraz.

Konsekwencja jest niewygodna: **brak widocznych ataków nie dowodzi, że atak nie trwa**. Ten sam argument dotyczy zresztą całej reszty tego numeru – gromadzenie zaszyfrowanych danych z zamiarem odczytania ich w przyszłości, opisane w rozdziale pierwszym, jest z definicji niewidoczne dla ofiary.

Poprzedni rekord, ustanowiony we wrześniu 2025 roku, wynosił 6 bitów.

Skok jest pięćsetkrotny i dokonał się w siedem miesięcy. Kusi, by wyciągnąć z tego wniosek o tempie – ale zrobienie tego wprost byłoby błędem, i to podwójnym.

Po pierwsze, odległość do klucza 256-bitowego nie wynosi „siedemnaście razy". Przestrzeń kluczy rośnie wykładniczo, więc między 15 a 256 bitami mieści się czynnik 2 do potęgi 241 – liczba, dla której nie ma sensownego porównania. Z drugiej strony trudność samego ataku **nie rośnie tak szybko jak przestrzeń kluczy**: liczba potrzebnych kubitów logicznych rośnie z długością klucza mniej więcej liniowo, a długość obwodu – wielomianowo. To właśnie dlatego atak jest w ogóle wyobrażalny. Właściwą miarą postępu jest więc krzywa zapotrzebowania na zasoby, a nie stosunek długości kluczy.

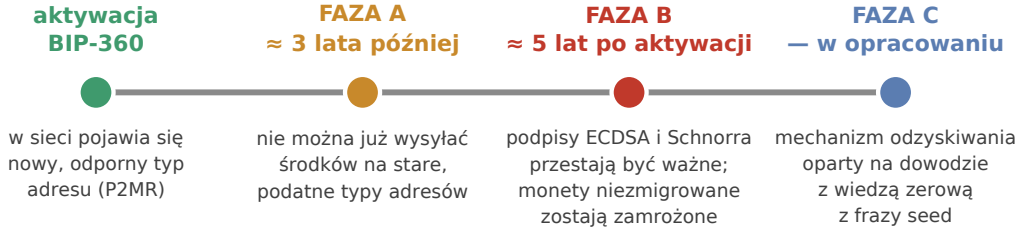
Po drugie, drobne demonstracje algorytmów typu Shora bywały w przeszłości krytykowane z konkretnego powodu: obwód kwantowy przygotowywano, **znając z góry odpowiedź**, co pozwalało uprościć go do postaci, która nie wykonuje już właściwej pracy obliczeniowej. Zarzut ten padał wobec słynnych „faktoryzacji liczby 15". Nie wiadomo, w jakim stopniu dotyczy on omawianego rekordu i dlatego pojedynczy wynik tego rodzaju należy traktować jako sygnał, a nie dowód.

Wiadomością jest tu kierunek i to, że próg wejścia obniżył się: rekord ustanowiono nie w laboratorium narodowym, lecz na sprzęcie dostępnym publicznie, za pośrednictwem chmury obliczeniowej.

5.6. Odpowiedź Bitcoina: dwie propozycje i jeden trylemat

Środowisko deweloperów Bitcoina odpowiedziało dwiema propozycjami, które trzeba czytać razem, bo dotyczą dwóch różnych części problemu.

BIP-360, opublikowany w lutym 2026 roku, tworzy nowy typ wyjścia transakcji, nazwany



Wszystkie terminy liczone są od aktywacji BIP-360, do której dotąd nie doszło. Na sierpień 2026 roku BIP-361 pozostaje projektem bez ustalonych parametrów aktywacji i bez mechanizmu głosowania. Osiągnięcie zgody sieci jest warunkiem, nie formalnością.

Rysunek 5.5. Trzyfazowy harmonogram proponowany w BIP-361. Terminy liczone są od aktywacji BIP-360, do której dotąd nie doszło; sam BIP-361 pozostaje projektem bez ustalonych parametrów aktywacji

Trylemat: trzy możliwe odpowiedzi i cena każdej

Pozwolić kraść wszystkim. Nie robimy nic; kto pierwszy zbuduje odpowiednią maszynę, ten przejmuje 6,8 miliona monet. Nagrodą za lata inwestycji w komputery kwantowe byłby największy transfer majątku w historii, dokonany poza jakąkolwiek kontrolą.

Pozwolić kraść w sposób ograniczony. Wprowadzamy mechanizm spowalniający przejmowanie środków, licząc, że prawowici właściciele zdążą zareagować. Autorzy wskazują, że skończyłoby się to licytacją opłat między napastnikiem a właścicielem, a górnicy zaczęliby czerpać dochód z monet odzyskiwanych kwantowo – czyli zyskaliby interes w tym, by proceder trwał.

Nie pozwolić kraść nikomu. Wyłączamy stare podpisy. Monety niezmigrowane zostają zamrożone. Cena: sieć po raz pierwszy w historii unieważnia środki, które są kryptograficznie poprawne i formalnie niczyjej winy nie stanowią.

BIP-361 wybiera trzecią drogę. Spór nie dotyczy tego, czy wybór jest logiczny – dotyczy tego, czy sieć, której obietnicą było „twoje klucze, twoje monety", ma prawo taki wybór podjąć.

pay-to-Merkle-root, w skrócie P2MR. Jest to w istocie konstrukcja Taproota pozbawiona ścieżki kluczowej, czyli tej właśnie, która umieszczała klucz publiczny wprost w łańcuchu. Podpisy w nowym formacie wykorzystują ML-DSA – standard postkwantowy zatwierdzony przez NIST, opisany w rozdziale szóstym. Propozycja zachowuje zgodność z siecią Lightning, z konstrukcjami wielopodpisowymi i z BitVM, a osobną uwagę poświęca rozmiarowi: podpisy postkwantowe są znacznie większe od dotychczasowych, co przy ograniczonej pojemności bloku ma bezpośrednie przełożenie na opłaty. Rozwiązanie działa już na testowej sieci kwantowej uruchomionej przez firmę BTQ Technologies.

BIP-360 chroni jednak wyłącznie monety nowe. Dla tych 34 procent, których klucze są już w łańcuchu, nie robi nic. Tym zajmuje się propozycja druga.

BIP-361, zatytułowany „Post Quantum Migration and Legacy Signature Sunset", trafił do oficjalnego repozytorium 14 kwietnia 2026 roku. Podpisało go sześciu autorów, wśród nich Jameson Lopp, współzałożyciel firmy Casa. Propozycja zakłada wygaszenie starych podpisów w trzech fazach.

W fazie A, około trzech lat po aktywacji nowego typu adresu, sieć przestaje przyjmować przelewy na adresy starego typu. Środki już tam zgromadzone można nadal wydawać, ale nie można ich powiększać. W fazie B, około dwóch lat później, węzły przestają uznawać podpisy ECDSA i Schnorra – monety, których nie zmigrowano, pozostają w rejestrze, lecz nie da się ich ruszyć. Faza C, wciąż w opracowaniu, ma dać prawowitym właścicielom sposób odzyskania zamrożonych środków przy użyciu dowodu z wiedzą zerową, wyprowadzonego z frazy seed – czyli z zapasowej listy słów, którą użytkownik zapisuje przy zakładaniu portfela.

Aby zrozumieć, dlaczego propozycja wywołała spór, trzeba przyjrzeć się rozumowaniu jej autorów. Wyliczają oni, że możliwe odpowiedzi na problem odsłoniętych kluczy są tylko trzy, i każda ma cenę.

Przyjęcie propozycji było w środowisku zdecydowanie chłodne. Argument przeciwników jest prosty i trudny do zbicia: jeżeli reguły można zmienić raz, dla dobrego powodu, to przestają być regułami. Zwolennicy odpowiadają, że alternatywa – sześć i osiem dziesiątych miliona monet przechodzących w nieznane ręce w sposób niemożliwy do zauważenia – zniszczyłaby zaufanie do sieci równie skutecznie, tyle że bez debaty.

Na sierpień 2026 roku BIP-361 pozostaje projektem: nie ma ustalonych parametrów aktywacji ani mechanizmu głosowania. Ethan Heilman, badacz zajmujący się tą migracją, oszacował, że pełne przeprowadzenie zmiany zajęłoby siedem lat licząc od dnia, w którym sieć osiągnie zgodę – a zgody nie ma. Równolegle rozważane są rozwiązania alternatywne; w czerwcu 2026 roku zespół Blockstream przedstawił szkic instrukcji OP_CHECKSHRINCS wraz z propozycją parametrów, które pozwoliłyby zmieścić podpisy postkwantowe w mniejszej liczbie bajtów.

5.7. Ethereum i pozostałe sieci

Porównanie z Ethereum jest pouczające, bo pokazuje, że trudność Bitcoina nie jest trudnością techniczną.

Ethereum przeprowadziło w swojej historii kilkanaście zmian protokołu wymagających zgodnego przejścia całej sieci, łącznie ze zmianą mechanizmu konsensusu w 2022 roku. Zdolność

Tabela 5.1. Co w ekosystemie kryptowalut jest zagrożone, a co nie

Mechanizm	Gdzie występuje	Los po Q-Day
SHA-256 w dowodzie pracy	wydobycie bitcoina	**BEZPIECZNY**
Skrót adresu (SHA-256 + RIPEMD-160)	adresy bitcoinowe	osłabiony do ok. 80 bitów – wciąż poza zasięgiem
Podpis ECDSA/Schnorr	autoryzacja transakcji w Bitcoinie	**ZŁAMANY**
Zamki skrótowe (HTLC)	kanały płatnicze sieci Lightning	**BEZPIECZNE**
Podpisy BLS	głosowanie walidatorów w Ethereum	**ZŁAMANE**
Dowody oparte na funkcjach skrótu (STARK)	rozwiązania skalujące, dowody obliczeń	**BEZPIECZNE**
Dowody oparte na parowaniach krzywych (SNARK)	część rozwiązań skalujących i prywatnościowych	**ZŁAMANE**

do skoordynowanej zmiany jest tam częścią kultury technicznej, a nie wyjątkiem od niej. W styczniu 2026 roku Fundacja Ethereum powołała osobny zespół do spraw bezpieczeństwa postkwantowego, w lutym Vitalik Buterin opublikował mapę drogową wskazującą cztery obszary wymagające wymiany kryptografii, a w marcu uruchomiono poświęcony temu serwis pq.ethereum.org. Ponad dziesięć zespołów utrzymujących oprogramowanie klienckie prowadzi cotygodniowe testy zgodności.

Zakres prac jest rozległy, bo Ethereum używa krzywych eliptycznych w kilku miejscach naraz. W warstwie konsensusu podpisy BLS, pozwalające scalić głosy setek tysięcy walidatorów w jeden podpis, mają zostać zastąpione podpisami opartymi na funkcjach skrótu. Powstaje jednak nowy problem: podpisy postkwantowe nie dają się scalać w naturalny sposób, więc trzeba to nadrobić dowodami kryptograficznymi generowanymi przez wyspecjalizowaną maszynę wirtualną. W warstwie wykonawczej planowane jest wbudowanie weryfikacji podpisów postkwantowych wprost w protokół, tak aby użytkownicy mogli przechodzić na nowe konta stopniowo, bez jednego dnia granicznego.

Docelowy termin to okolice 2029 roku – ten sam, który Google wyznaczył sobie na przestawienie własnej infrastruktury. Fundacja ufundowała dwie nagrody po milionie dolarów za wzmocnienie funkcji skrótu używanych w dowodach kryptograficznych oraz za wydajniejsze podpisy postkwantowe.

Inne sieci idą podobną drogą: XRP Ledger testuje podpisy ML-DSA na sieci eksperymentalnej z zamiarem wdrożenia około 2028 roku, a sieć Tron ogłosiła własną inicjatywę postkwantową. Giełda Coinbase powołała niezależną radę doradczą do oceny zagrożenia. Trzeba jednak zaznaczyć rzecz podstawową: na sierpień 2026 roku żadna znacząca sieć nie działa w pełni na kryptografii postkwantowej. Wszystko, co opisaliśmy, to plany, testy i projekty na różnym etapie zaawansowania.

5.8. Co z tego wynika

Dla posiadacza kryptowalut praktyczne wnioski są krótkie i nie wymagają żadnej wiedzy o fizyce kwantowej. Nie należy używać tego samego adresu wielokrotnie. Warto sprawdzić, czy posiadane środki znajdują się na adresach, z których już kiedyś wydawano. Monety przechowywane od lat w starych formatach wymagają decyzji – przy czym samo ich przeniesienie jest operacją, którą trzeba dobrze przygotować, bo błąd kosztuje więcej niż odległe zagrożenie. Producenci

portfeli sprzętowych będą musieli dodać obsługę podpisów postkwantowych, i to jest moment, na który warto poczekać.

Dla czytelnika śledzącego całą tę historię istotniejszy jest jednak inny wniosek. W pozostałych dziedzinach opisywanych w tym numerze zawsze istnieje ktoś, kto może wydać polecenie: ministerstwo, regulator, zarząd, komisja standaryzacyjna. Rozdział szósty opisuje właśnie taką machinę – terminy, rozporządzenia, normy.

W Bitcoinie tego kogoś nie ma i nigdy nie miało być. Sieć zbudowano tak, aby żadna instytucja nie mogła zmienić jej reguł – i właśnie ta cecha, przez piętnaście lat uważana za jej największą zaletę, okazuje się teraz największą trudnością. **Zagrożenie kwantowe jest dla kryptowalut nie tyle problemem kryptograficznym, ile pierwszym prawdziwym testem zdolności podejmowania decyzji.** Czy sieć bez władzy potrafi w ogóle uzgodnić coś, co dla części uczestników oznacza stratę? Odpowiedź poznamy najprawdopodobniej wcześniej niż odpowiedź na pytanie, kiedy powstanie komputer zdolny łamać szyfry. ■

Bibliografia

[48] Aggarwal D., Brennen G. K., Lee T., Santha M., Tomamichel M., Quantum Attacks on Bitcoin, and How to Protect Against Them, „Ledger” 2018, t. 3. DOI: 10.5195/ledger.2018.127. Preprint: arXiv:1710.10377.
[49] Quantum Horizon: An Evaluation of Quantum Computing as a Threat to Bitcoin and Ethereum, preprint arXiv:2606.14484 [quant-ph], czerwiec 2026.
[50] Lopp J., Papathanasiou C., Smith I., Ross J., Vaile S., Dallaire-Demers P.-L., BIP-361: Post Quantum Migration and Legacy Signature Sunset, Bitcoin Improvement Proposals, 14 kwietnia 2026, status: projekt. https://github.com/bitcoin/bips/blob/master/bip-0361.mediawiki [dostęp: 5.08.2026].
[51] BIP-360: Pay to Quantum Resistant Hash/Pay-to-Merkle-Root (P2MR), Bitcoin Improvement Proposals, luty 2026, status: projekt.
[52] Project Eleven, Q-Day Prize Awarded: 15-bit Elliptic Curve Key Broken on Quantum Hardware, komunikat, 24 kwietnia 2026.
[53] Buterin V., How to Make Ethereum Quantum-Resistant, mapa drogowa opublikowana w lutym 2026; materiały towarzyszące: Ethereum Foundation, pq.ethereum.org, uruchomiony 25 marca 2026.
[54] Ethereum Foundation, Post-Quantum Cryptography on Ethereum, ethereum.org/roadmap/future-proofing/quantum-resistance [dostęp: 5.08.2026].
[55] Bitcoin’s Quantum Migration Plan Forces the Network to Choose Between Frozen and Stolen Coins, CryptoSlate, 16 kwietnia 2026.

Ponadto w rozdziale przywołano pozycje [1], [3] i [6] z bibliografii rozdziału 1 (Shor 1994; szacunek zasobów ataku na krzywą eliptyczną, Google Quantum AI/Ethereum Foundation/Boneh 2026; Gidney 2025).

Rozdział 6.

Wyścig: kryptografia postkwantowa

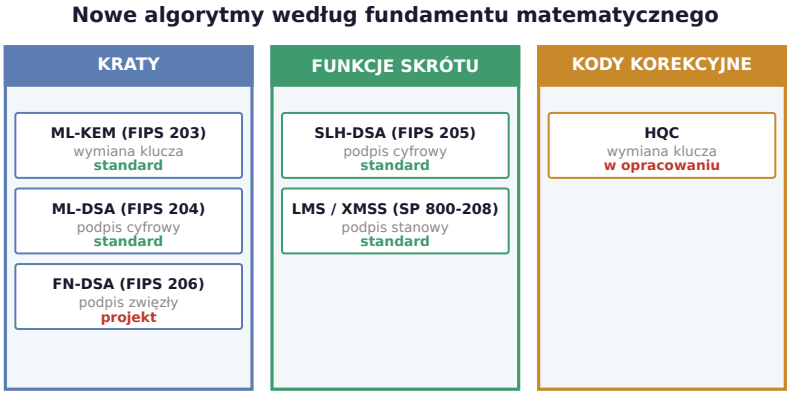
Pięć poprzednich rozdziałów opisywało zagrożenie. Ten opisuje odpowiedź – i zaczyna się od stwierdzenia, które w tym kontekście brzmi zaskakująco: odpowiedź jest gotowa od 2024 roku. Nowe szyfry istnieją, są znormalizowane i można je pobrać za darmo. Wbrew intuicji nie potrzeba do nich żadnego sprzętu kwantowego; działają na zwykłych komputerach, telefonach i sterownikach. Cały wyścig, o którym mowa w tytule tego numeru, nie polega więc na wymyśleniu lekarstwa. Polega na podaniu go kilkunastu miliardom urządzeń, z których część nie wie nawet, że jest chora.

6.1. Trzy różne fundamenty

Kryptografia postkwantowa – w skrócie PQC, od angielskiego post-quantum cryptography – to zbiór algorytmów opartych na zadaniach matematycznych, których nie rozwiązuje ani algorytm Shora, ani żaden inny znany algorytm kwantowy. Amerykański instytut NIST ogłosił w 2016 roku otwarty konkurs, na który zgłoszono osiemdziesiąt dwie propozycje z całego świata. Po ośmiu latach analiz i publicznego łamania nawzajem swoich prac wyłoniono zwycięzców.

Kraty. Wyobraźmy sobie regularną siatkę punktów rozpiętą w przestrzeni o kilkuset wymiarach. Zadanie brzmi: mając wskazany punkt gdzieś pomiędzy węzłami, znaleźć najbliższy węzeł siatki. W dwóch czy trzech wymiarach jest to trywialne. W pięciuset wymiarach nie znamy metody istotnie lepszej niż sprawdzanie po kolei – ani klasycznej, ani kwantowej. Na tym opierają się trzy z sześciu znormalizowanych algorytmów: ML-KEM do uzgadniania klucza oraz ML-DSA i FN-DSA do podpisów.

Funkcje skrótu. Tu nie ma żadnej nowej matematyki – jest tylko sprytne użycie tego, co i tak mamy. Skoro funkcje skrótu przeżywają Q-Day, o czym pisaliśmy w rozdziale czwartym, to da się z nich zbudować podpis cyfrowy. Zaletą jest bezpieczeństwo oparte na najlepiej przebadanym mechanizmie w całej kryptografii. Wadą – rozmiar i, w wariancie stanowym, konieczność pamiętania, których kluczy jednorazowych już użyto. Powtórzenie takiego klucza kompromituje cały schemat, co czyni te podpisy znakomitymi



Trzy różne fundamenty to nie nadmiar, lecz ubezpieczenie. Gdyby ktoś złamał matematykę krat, padłyby jednocześnie trzy algorytmy z lewej kolumny — i dlatego dwie pozostałe kolumny muszą istnieć, choć są wolniejsze albo dają większe podpisy.

Rysunek 6.1. Rodzina nowych algorytmów. Podział przebiega według rodzaju matematyki, na której opiera się bezpieczeństwo, a nie według zastosowania – i to właśnie ten podział jest w całej konstrukcji najważniejszy

Tabela 6.1. Nowe algorytmy i ich stan na sierpień 2026 roku

Algorytm	Norma	Do czego służy	Fundament	Stan
ML-KEM	FIPS 203	uzgadnianie klucza	kraty	standard od 2024
ML-DSA	FIPS 204	podpis cyfrowy	kraty	standard od 2024
SLH-DSA	FIPS 205	podpis cyfrowy	funkcje skrótu	standard od 2024
LMS, XMSS	SP 800-208	podpis stanowy, oprogramowanie układowe	funkcje skrótu	standard od 2020
FN-DSA	FIPS 206	podpis o małym rozmiarze	kraty	projekt; finał 2026/27
HQC	w opracowaniu	uzgadnianie klucza – rezerwa	kody korekcyjne	wybrany 2025

W maju 2026 roku NIST skierował do trzeciej rundy oceny dziewięć kolejnych propozycji podpisów cyfrowych. Żadna z nich nie staje się przez to standardem – ale sam fakt prowadzenia dalszych prac jest częścią odpowiedzi na pytanie z następnego podrozdziału.

Dwie porażki z 2022 roku, o których warto pamiętać

SIKE był jednym z kandydatów, który przeszedł do czwartej rundy konkursu NIST. Opierał się na eleganckiej matematyce izogenii krzywych eliptycznych i dawał wyjątkowo małe klucze. W lipcu 2022 roku dwaj belgijscy matematycy, Wouter Castryck i Thomas Decru, opublikowali atak, który **łamał go na jednym rdzeniu zwykłego komputera w około godzinę**. Nie chodziło o słabą implementację ani o dobór parametrów – pękła sama podstawa matematyczna, przeoczona przez pięć lat publicznych analiz.

Rainbow, kandydat na podpis cyfrowy, padł kilka miesięcy wcześniej z rąk Warda Beullensa – jego atak sprowadzał złamanie do weekendu obliczeń na laptopie.

Oba algorytmy przeszły wieloletnią, otwartą ocenę środowiska naukowego. Wniosek nie brzmi, że konkurs zawiódł – przeciwnie, konkurs zadziałał dokładnie tak, jak miał zadziałać, bo obie prace powstały właśnie dlatego, że specyfikacje były jawne. Wniosek brzmi: nie wiadomo, czego jeszcze nie wiemy.

do oprogramowania układowego, a kłopotliwymi w serwerowni.

Kody korekcyjne. Trzeci fundament wywodzi się z techniki, którą znamy z płyt kompaktowych i transmisji satelitarnej: do wiadomości dokłada się nadmiarowe bity, żeby odbiorca mógł naprawić przekłamania. Jeżeli natomiast ktoś nie zna struktury kodu, odróżnienie zamierzonych błędów od przypadkowych okazuje się bardzo trudne. Pomysł ma pięćdziesiąt lat i nikt go dotąd nie złamał. Reprezentuje go algorytm HQC, wybrany w marcu 2025 roku.

6.2. Dlaczego nie jeden algorytm

Skoro kraty dają najlepszy stosunek bezpieczeństwa do rozmiaru, dlaczego nie oprzeć wszystkiego na nich i nie zamknąć sprawy? Odpowiedź brzmi: bo już raz omal nie skończyło się to katastrofą.

Stąd bierze się zasada, którą warto zapamiętać: **monokultura kryptograficzna jest ryzykiem samym w sobie**. Gdyby cała światowa infrastruktura oparła się wyłącznie na kratach, jedno odkrycie matematyczne unieważniłoby ją w całości – jednocześnie i wszędzie. Dlatego NIST znormalizował podpisy oparte na funkcjach skrótu, mimo że są większe, i wybrał HQC jako rezerwowy mechanizm wymiany klucza, mimo że jest wolniejszy od ML-KEM. Płaci się za to wydajnością, a kupuje niezależność fundamentów.

6.3. Hybryda, czyli pas i szelki

Ta sama ostrożność stoi za rozwiązaniem, które dziś dominuje w praktyce. Nazywa się hybrydą i polega na tym, że **dwie strony uzgadniają klucz dwoma algorytmami naraz** – starym, opartym na krzywej eliptycznej, i nowym, postkwantowym – a następnie łączą oba wyniki w jeden klucz sesji. Napastnik musi złamać oba, żeby cokolwiek odczytać.

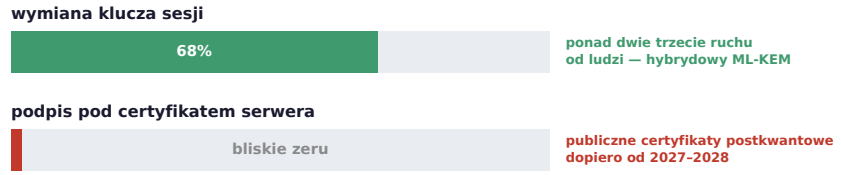
Zysk jest podwójny. Jeżeli w nowym algorytmie znajdzie się luka w rodzaju tej, która pogrążyła SIKE, chroni nas stary. Jeżeli powstanie komputer kwantowy, chroni nas nowy. Ceną jest niewielki narzut obliczeniowy i większy rozmiar przesyłanych danych.

Francuska agencja ANSSI uczyniła z hybrydy wymóg formalny: dopuszcza kryptografię postkwantową wyłącznie w połączeniu z klasyczną, argumentując, że nowe algorytmy nie mają za sobą dostatecznie długiej historii publicznych ataków. Niemiecki urząd BSI zajmuje stanowisko zbliżone. Amerykańska NSA w wytycznych CNSA 2.0 poszła w drugą stronę – dopuszcza czyste rozwiązania postkwantowe, uznając hybrydę za niepotrzebną komplikację. Spór ten nie został rozstrzygnięty i przebiega dokładnie tam, gdzie przebiega różnica temperamentów między instytucjami: między kosztem złożoności a kosztem pomyłki.

6.4. Co już działa, a co jeszcze nie

Przejdźmy do rzeczy najciekawszej: jak daleko zaszło wdrożenie. Odpowiedź jest dwuczłonowa i to właśnie ta dwuczłonowość jest cechą charakterystyczną roku 2026.

Wymiana klucza sesji jest w znacznej mierze załatwiona. **Ponad dwie trzecie ruchu generowanego przez ludzi w sieci Cloudflare korzysta z hybrydowego ML-KEM.** Przeglądarka Chrome włączyła to domyślnie w kwietniu 2024 roku, pozostałe poszły w jej ślady. Biblioteka OpenSSL od wersji 3.5, wydanej w kwietniu 2025 roku, obsługuje nowe algorytmy natywnie. Czytelnik, który odwiedził dziś jakąkolwiek większą witrynę, najprawdopodobniej użył kryptografii postkwantowej i nie miał o tym pojęcia.



Rysunek 6.2. Dwie połowy tego samego połączenia. Wracamy tu do rozróżnienia z rozdziału czwartego: pilne było to, co dotyczy poufności, i to właśnie zostało zrobione najpierw

Podpisy cyfrowe to zupełnie inna historia. Publiczne certyfikaty postkwantowe praktycznie nie istnieją i nie będą powszechnie dostępne przed 2027 albo 2028 rokiem. Powstaje z tego sytuacja, którą warto sobie uświadomić: gdy przeglądarka łączy się dziś z bankiem, klucz sesji jest już odporny na przyszły atak kwantowy, ale certyfikat potwierdzający, że to naprawdę bank, wciąż podpisano algorytmem ECDSA albo RSA.

Powodów opóźnienia jest kilka i pierwszy z nich jest przyziemny.

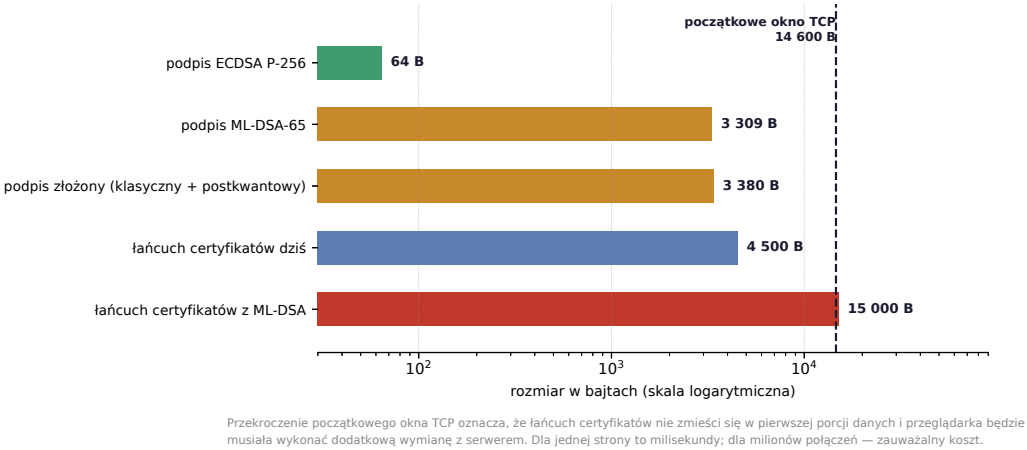
Podpis ECDSA zajmuje sześćdziesiąt cztery bajty. Podpis ML-DSA-65 – **3309 bajtów**, czyli pięćdziesiąt razy więcej. Cały łańcuch certyfikatów rośnie z około czterech i pół kilobajta do piętnastu, a to przekracza początkowe okno przeciążenia protokołu TCP wynoszące 14 600 bajtów. W praktyce oznacza to, że dane uwierzytelniające nie zmieszczą się w pierwszej porcji przesyłanej przez sieć i połączenie będzie wymagało dodatkowej wymiany komunikatów.

Drugim powodem jest niedokończona normalizacja. Grupa robocza LAMPS w organizacji IETF osiągnęła w marcu 2026 roku ostatni etap uzgodnień w sprawie podpisów złożonych, z docelowym dokumentem planowanym na koniec tego roku. Forum CA/Browser, ustalające reguły dla publicznych urzędów certyfikacji, ma zaktualizować swoje wymagania na przełomie lat 2026 i 2027.

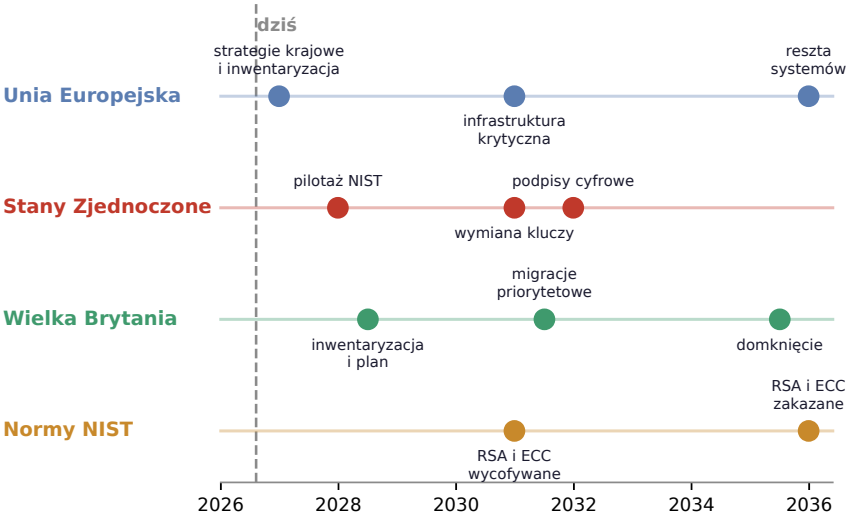
Trzeci powód jest najbardziej podstępny. Certyfikaty korzeni zaufania mają okres ważności rzędu dwudziestu do trzydziestu lat, więc korzenie wystawione dzisiaj – algorytmem klasycznym – będą siedziały w przeglądarkach i systemach operacyjnych przez całą erę postkwantową. Google testuje wspólnie z Cloudflare rozwiązanie nazwane certyfikatami drzewa Merkle, pozwalające zmniejszyć objętość danych uwierzytelniających i zapowiada osobny magazyn korzeni odpornych kwantowo do końca 2027 roku.

6.5. Kalendarz prawny

Skoro rozwiązania techniczne istnieją, a wdrożenie idzie nierówno, do gry wchodzi przymus



Rysunek 6.3. Dlaczego podpisy są trudniejsze od wymiany klucza. Wartości dotyczą typowego łańcucha certyfikatów dla witryny internetowej; przy podpisach złożonych, zawierających wersję klasyczną i postkwantową jednocześnie, narzut jest jeszcze większy



Terminy oznaczają koniec wskazanego roku. Pierwszy z nich wypada pięć miesięcy po ukazaniu się tego numeru.

Rysunek 6.4. Terminy obowiązujące w czterech porządkach prawnych. Zbieżność dat nie jest przypadkowa: rok 2030 wynika z tych samych szacunków zagrożenia, które opisywaliśmy w rozdziale pierwszym

administracyjny. Ostatnie dwa lata przyniosły więcej wiążących terminów niż cała poprzednia dekada.

Unia Europejska opublikowała 23 czerwca 2025 roku skoordynowaną mapę drogową, przygotowaną przez Grupę Współpracy powołaną dyrektywą NIS2. Wyznacza ona trzy kamienie milowe: do końca 2026 roku wszystkie państwa członkowskie mają mieć krajowe strategie przejścia i rozpocząć inwentaryzację kryptografii; do końca 2030 zabezpieczona ma być infrastruktura krytyczna i zastosowania wysokiego ryzyka; do końca 2035 – reszta. Projekt nowelizacji dyrektywy NIS2 z stycznia 2026 roku przekształca to zalecenie w obowiązek prawny.

Stany Zjednoczone przyspieszyły najbardziej. Rozporządzenie wykonawcze numer 14412, podpisane 22 czerwca 2026 roku, przesunęło termin federalny z 2035 na **31 grudnia 2030 dla wymiany kluczy i 31 grudnia 2031 dla podpisów cyfrowych**. Nakazuje też każdej agencji wyznaczyć osobę odpowiedzialną za migrację i sporządzić spis używanej kryptografii, a osobna procedura ma rozciągnąć te wymagania na wykonawców rządowych.

Wielka Brytania przyjęła harmonogram trójstopniowy: do 2028 roku inwentaryzacja i plan, w latach 2028–2031 migracje priorytetowe, do 2035 domknięcie. Normy amerykańskiego NIST wyznaczają zaś ramę, w której poruszają się wszyscy: po 2030 roku RSA i krzywe eliptyczne mają status wycofywanych, a po 2035 – zakazanych.

6.6. A może po prostu QKD?

W tym miejscu pojawia się zwykle pytanie o rozwiązanie, które brzmi znacznie efektowniej: skoro problem stworzyła fizyka kwantowa, może fizyka kwantowa go rozwiąże?

Kwantowa dystrybucja klucza, w skrócie QKD, wykorzystuje właściwość pojedynczych fotonów: nie da się ich zmierzyć, nie zmieniając ich stanu. Dwie strony przesyłają światłowodem ciąg fotonów i porównują wyniki pomiarów. Jeżeli ktoś podsłuchiwał, zostawił ślad – i to nie dlatego, że sprzęt był kiepski, lecz dlatego, że nie pozwala na to fizyka. Bezpieczeństwo nie zależy tu od trudności żadnego zadania matematycznego, a więc żaden postęp algorytmiczny go nie unieważni.

Brzmi to nieodparcie i dlatego trzeba od razu powiedzieć, czego QKD nie potrafi. Wymaga dedykowanego łącza światłowodowego między dwiema stronami i osobnych urządzeń na obu końcach. Nie działa przez zwykły internet, bo każdy wzmacniacz sygnału niszczyłby fotony, które ma przekazać. Zasięg bez pośredników wynosi kilkaset kilometrów. Nie rozwiązuje problemu podpisu cyfrowego – służy wyłącznie do uzgadniania klucza. I nie ma odpowiedzi na pytanie, skąd wiadomo, że urządzenie po drugiej stronie należy do tego, za kogo się podaje.

Dlatego zachodnie agencje bezpieczeństwa – amerykańska NSA, brytyjska NCSC, francuska ANSSI – zalecają jednoznacznie kryptografię postkwantową, a QKD traktują jako uzupełnienie do zastosowań szczególnych. Amerykańskie rozporządzenie z czerwca 2026 roku świadomie tę technologię pomija. Odmiennie postępują Chiny, które zbudowały rozległą sieć QKD i traktują ją jako element strategii państwowej.

Różnicę można ująć krótko: **QKD chroni jedno łącze, PQC chroni internet**. Pierwsze rozwiązanie wymaga położenia kabla, drugie – aktualizacji oprogramowania.

6.7. Pięć kroków i najczęstszy błąd

Zejdźmy wreszcie na poziom praktyczny. Jak organizacja – bank, szpital, zakład produkcyjny, urząd – ma się do tego zabrać?

Najczęstszy błąd polega na rozpoczynaniu od kroku trzeciego, czyli od zakupu rozwiązania hybrydowego. Doświadczenie drugiej fazy projektu Leap, opisanej w rozdziale czwartym, mówi coś przeciwnego: **największą trudnością nie jest wdrożenie nowych algorytmów, lecz ustalenie, gdzie w ogóle używa się starych.** W dużej organizacji kryptografia bywa jak instalacja elektryczna w starym budynku – wszyscy z niej korzystają, a dopiero remont ujawnia, jak dziwnie poprowadzono przewody.

Krok piąty – krypto-zwinność – jest w tym wszystkim celem właściwym i zarazem najczęściej pomijanym. Chodzi o zaprojektowanie systemów tak, aby wymiana algorytmu była zmianą konfiguracji, a nie przebudową. **Migracja postkwantowa nie jest bowiem ostatnią w historii.** Jeżeli po niej zostanie infrastruktura równie sztywna jak dotychczasowa, następne pokolenie przejdzie przez dokładnie to samo – i będzie musiało przeczytać podobny numer tego pisma.

6.8. Polska

Polska jest w tej sprawie w punkcie, który wymaga jasnego nazwania.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029, przyjęta przez Radę Ministrów 10 marca 2026 roku, wymienia wprost plan migracji do kryptografii postkwantowej oraz rozwój krajowej kryptografii i technologii kwantowych. Dokument istnieje, kierunek jest wskazany, a Instytut Łączności prowadzi prace analityczne i publikuje raporty o stanie przygotowań na świecie.

Pozostaje kwestia tempa. Unijny termin – krajowa strategia przejścia wraz z rozpoczętą inwentaryzacją kryptografii – wypada **31 grudnia 2026 roku**, czyli pięć miesięcy po ukazaniu się tego numeru. Dotyczy on nie tylko administracji, ale wszystkich podmiotów objętych dyrektywą NIS2: banków, szpitali, operatorów energetycznych, dostawców usług cyfrowych. Dla większości z nich oznacza to rozpoczęcie od kroku pierwszego – od spisu, którego nikt dotąd nie sporządzał.

Warto przy tym zauważyć rzecz, która w tej dyskusji rzadko pada. Polska nie musi opracowywać własnych algorytmów ani budować własnych komputerów kwantowych, żeby być przygotowana. Standardy są jawne i darmowe, biblioteki otwarte, a najtrudniejsza część pracy – inwentaryzacja i uporządkowanie własnych systemów – nie wymaga niczego poza decyzją i ludźmi. To zadanie organizacyjne, nie technologiczne, i to jest w nim zarazem dobra i zła wiadomość.

Najczęstszy błąd polega na rozpoczynaniu od kroku trzeciego. Bez spisu nie wiadomo, czego szukać, a doświadczenie instytucji finansowych pokazuje, że właśnie sporządzenie spisu pochłania większość czasu całego przedsięwzięcia.

Rysunek 6.5. Kolejność, która wynika z doświadczeń pierwszych migracji. Krok piąty nie jest ozdobnikiem – to on decyduje, ile będzie kosztowała następna wymiana algorytmu

CBOM, czyli spis kryptografii

Od kilku lat przy oprogramowaniu mówi się o SBOM – wykazie wszystkich komponentów, z których zbudowano program. Migracja postkwantowa wymusiła powstanie odpowiednika dla kryptografii, nazwanego CBOM.

Jest to maszynowo czytelny spis wszystkiego, co w danym systemie szyfruje albo podpisuje: algorytmów wraz z długościami kluczy, bibliotek, certyfikatów, protokołów oraz powiązań między nimi. Format opiera się na tym samym standardzie co SBOM, więc mieści się w narzędziach, które organizacje już mają.

Znaczenie CBOM przestało być czysto techniczne. Unijna mapa drogowa z czerwca 2025 roku wymienia go z nazwy jako zalecany format inwentaryzacji, a amerykańskie rozporządzenie z czerwca 2026 nakazuje agencjom CISA i NIST opublikować minimalne wymagania dla takiego spisu **w ciągu 270 dni, czyli mniej więcej do marca 2027 roku**. Spis kryptografii przestaje być dobrą praktyką, a staje się obowiązkiem.

6.9. Co z tego wynika

Zamknijmy sześć rozdziałów jednym zestawieniem.

Komputer kwantowy zdolny łamać dzisiejsze szyfry nie istnieje i nie powstanie w tej dekadzie. Szacunki jego rozmiaru kurczą się jednak szybciej, niż ktokolwiek zakładał, a te same maszyny, które go umożliwią, są od czterdziestu lat wymarzonym narzędziem chemików. Nie da się zbudować jednego bez drugiego.

Zagrożenie nie zacznie się w dniu Q. Zaczęło się w chwili, gdy pamięć masowa stopniała do ceny, przy której opłaca się zapisywać cudzy zaszyfrowany ruch na piętnaście lat. Dlatego pilne jest to, co dotyczy poufności, a nie to, co dotyczy podpisu – z wyjątkiem podpisów, które mają zachować moc dowodową przez dziesięciolecia, i urządzeń, których nie da się zaktualizować.

Lekarstwo istnieje, jest znormalizowane i darmowe. Trudność leży gdzie indziej: w tym, że trzeba je podać systemom, o których nikt nie prowadzi ewidencji. I w tym, że **w części przypadków – jak w Bitcoinie – nie ma nikogo, kto mógłby wydać takie polecenie**.

Zegar, o którym pisaliśmy w rozdziale pierwszym, nie odmierza czasu do katastrofy. Odmierza czas, jaki został na przygotowanie – a to jest zupełnie inna rzecz i wymaga zupełnie innych reakcji. Pierwszy termin wypada za pięć miesięcy. ■

Paul Bavarian

O Autorze
Paul Bavarian jest wnukiem mojego bułgarskiego przyjaciela z czasów studenckich w Politechnice Kijowskiej. Pasjonują go nowe technologie, które obserwuje z perspektywy kalifornijskiej. The last but not least – odziedziczył po swoim dziadku fascynację Polską.

Prof. Wiesław Marciniak

Bibliografia

[56] National Institute of Standards and Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203, Gaithersburg, 13 sierpnia 2024. DOI: 10.6028/NIST.FIPS.203.
[57] National Institute of Standards and Technology, Module-Lattice-Based Digital Signature Standard, FIPS 204, Gaithersburg, 13 sierpnia 2024. DOI: 10.6028/NIST.FIPS.204.
[58] National Institute of Standards and Technology, Stateless Hash-Based Digital Signature Standard, FIPS 205, Gaithersburg, 13 sierpnia 2024. DOI: 10.6028/NIST.FIPS.205.
[59] National Institute of Standards and Technology, HQC Announced as a Fourth-Round Selection, komunikat, 11 marca 2025. https://csrc.nist.gov/news/2025/hqc-announced-as-a-4th-round-selection [dostęp: 6.08.2026].
[60] Castryck W., Decru T., An Efficient Key Recovery Attack on SIDH, [w:] Advances in Cryptology – EUROCRYPT 2023, Springer, s. 423–447. Preprint: IACR ePrint 2022/975, lipiec 2022.
[61] Beullens W., Breaking Rainbow Takes a Weekend on a Laptop, [w:] Advances in Cryptology – CRYPTO 2022, Springer, s. 464–479. Preprint: IACR ePrint 2022/214.
[62] Cloudflare, Post-Quantum Encryption for Cloudflare IPsec Is Generally Available, blog Cloudflare, kwiecień 2026. https://blog.cloudflare.com/post-quantum-ipsec/ [dostęp: 6.08.2026].
[63] Internet Engineering Task Force, grupa robocza LAMPS, Composite ML-DSA for Use in X.509 Public Key Infrastructure, draft-ietf-lamps-pq-composite-sigs; ostatnie uzgodnienia grupy roboczej – marzec 2026.
[64] Securing Cryptography in the Age of Quantum Computing and AI: Threats, Implementations, and Strategic Response, preprint arXiv:2603.06969, marzec 2026 – źródło danych o rozmiarach łańcuchów certyfikatów.
[65] OWASP CycloneDX, Cryptography Bill of Materials (CBOM), specyfikacja CycloneDX 1.6, opublikowana jako norma ECMA-424. https://cyclonedx.org/capabilities/cbom/ [dostęp: 6.08.2026].
[66] Waszkiewicz D. i in., Q-Day coraz bliżej – Polska musi przyspieszyć przygotowania do ery komputerów kwantowych, ITwiz, maj 2026 – omówienie zapisów Strategii Cyberbezpieczeństwa RP dotyczących migracji do PQC.

Ponadto w rozdziale przywołano pozycje [12], [13], [14], [15], [16], [17] i [40] z bibliografii rozdziałów 1 i 4 (stanowiska ANSSI i BSI; mapa drogowa NIS CG; Executive Order 14412; NIST IR 8547; wytyczne NCSC; Strategia Cyberbezpieczeństwa RP; CNSA 2.0).

AI w podróży

Planowanie wymarzonej podróży od lat wiąże się z dużą ilością przygotowań. W końcu wymarzony czas wolny nie może zostać zmarnowany. Gdy nadchodzi moment wyjazdu, większość osób chce wykorzystać go jak najlepiej. Z tego powodu przygotowania do wypoczynku od dawna oznaczają długie godziny poświęcone na zakup biletów, wybór atrakcji, organizację transportu oraz rezerwację noclegów.

Wszystkie te czynności sprowadzają się w dużej mierze do przeszukiwania zasobów internetowych i porównywania dostępnych informacji. Skoro modele językowe miały zrewolucjonizować również ten aspekt codziennego życia, warto sprawdzić, czy rzeczywiście potrafią zaplanować wyjazd od początku do końca. Spróbujmy więc przygotować całą podróż z poziomu interfejsu Chata GPT.

Wybór terminu podróży

Darujmy sobie pytania AI o to, dokąd chcemy pojechać. Załóżmy konkretny scenariusz: tygodniową wycieczkę do Japonii – kraju popularnego, dobrze skomunikowanego i niezwykle bogatego w atrakcje. Przyjmijmy również kilka założeń. Chcemy ograniczyć koszty, jedziemy tam po raz pierwszy i zależy nam na zobaczeniu jak największej liczby miejsc. W takiej sytuacji warto unikać najdroższego sezonu turystycznego, zwłaszcza okresu kwitnienia wiśni, kiedy ceny lotów i noclegów gwałtownie rosną, a najpopularniejsze atrakcje są bardzo zatłoczone.

Zacznijmy więc od wyboru miesiąca podróży i poprośmy ChatGPT o przygotowanie tabeli porównawczej. Już po pierwszym spojrzeniu widać, że najtańsze miesiące – szczególnie luty oraz pierwsza połowa grudnia – oferują bardzo korzystne ceny lotów. Luty wyróżnia się dodatkowo dużą liczbą słonecznych dni i niewielkimi kolejkami do atrakcji, ceną najniższych temperatur. Po przeanalizowaniu kosztów, pogody i liczby turystów najlepszym kompromisem okazał się listopad. Jest to jeden z tańszych okresów na podróż do Japonii, przypada po porze deszczowej i pozwala zwiedzać w komfortowej temperaturze około 13–14°C. Dodatkowym atutem są jesienne kolory, które w wielu regionach Japonii stanowią atrakcję porównywaną popularnością do wiosennej „sakury". To właśnie listopad stanie się terminem naszej podróży.

Atrakcje i plan wycieczki

W następnym kroku opisałem ChatGPT moje osobiste zainteresowania oraz cele podróży. Poprosiłem o znalezienie 50 interesujących miejsc w całej Japonii, z uwzględnieniem moich preferencji. Największy nacisk położyłem na buddyzm, historię i shintō, a w mniejszym stopniu na anime, gry wideo oraz sztukę. Jednocześnie zależało mi na tym, aby nie pomijać najbardziej ikonicznych atrakcji Japonii i zwrócić szczególną uwagę na wydarzenia odbywające się w wybranym miesiącu podróży. Do zapytania dodałem również prośbę, aby model opierał się przede wszystkim na opiniach z forów podróżniczych i relacjach turystów, traktując blogi oraz treści marketingowe jako źródła mniej wiarygodne.

Listopad okazał się miesiącem stosunkowo ubogim w duże festiwale. Jednocześnie jest to jeden z najlepszych okresów na podziwianie japońskiej jesieni. Wiele świątyń udostępnia wtedy nocne

Specjalna noc w świątyni Kiyomizu-dera jest największym wydarzeniem w czwartym najtańszym miesiącu Japonii

Miesiąc	Śr. temp.	cena lotu Google Flights	Uwagi dla turysty
Styczeń	5…6°C	2 900…3 700 zł	Mało turystów, suche powietrze, krótszy dzień; po 10 stycznia zwykle wyraźnie taniej.
Luty	6…7°C	2 700…3 500 zł	Najlepszy budżetowo; dużo słońca, małe kolejki, dobre na intensywne zwiedzanie piesze.
Marzec	10…11°C	3 400…4 800 zł	Początek sakury pod koniec miesiąca; ceny i tłumy szybko rosną.
Kwiecień	15…16°C	4 200…6 000 zł	Szczyt kwitnienia wiśni; najładniej, ale też najdrożej i najbardziej tłoczno.
Maj	19…20°C	3 600…4 800 zł	Bardzo przyjemna pogoda; unikaj Golden Week (ok. 29 IV – 5 V).
Czerwiec	22…23°C	3 200…4 200 zł	Pora deszczowa, wysoka wilgotność, mniej turystów i tańsze hotele.
Lipiec	26…27°C	4 600…6 200 zł	Bardzo gorąco i wilgotno; możliwe fale upałów, męczące zwiedzanie w dzień.
Sierpień	27…28°C	4 200…5 800 zł	Najbardziej duszno; okres Obon zwiększa ceny i ruch krajowy.
Wrzesień	24…26°C	3 300…4 300 zł	Często jedna z tańszych opcji; nadal gorąco, możliwe tajfuny i ulewy.
Październik	18…20°C	3 700…4 900 zł	Świetna pogoda, mało deszczu, bardzo popularny miesiąc turystycznie.
Listopad	13…14°C	3 000…3 900 zł	Sucho, komfortowo, jesienne kolory, mniej tłumów niż w październiku.
Grudzień	8…9°C	2 900…3 800 zł	Pierwsza połowa miesiąca bywa tania; świąteczne iluminacje, chłodno wieczorami.

zwiedzanie ogrodów, które w tym czasie przybierają intensywne odcienie pomarańczy i czerwieni. Takie iluminacje zostały wskazane przez ChatGPT jako najlepsze wydarzenia w miesiącu.

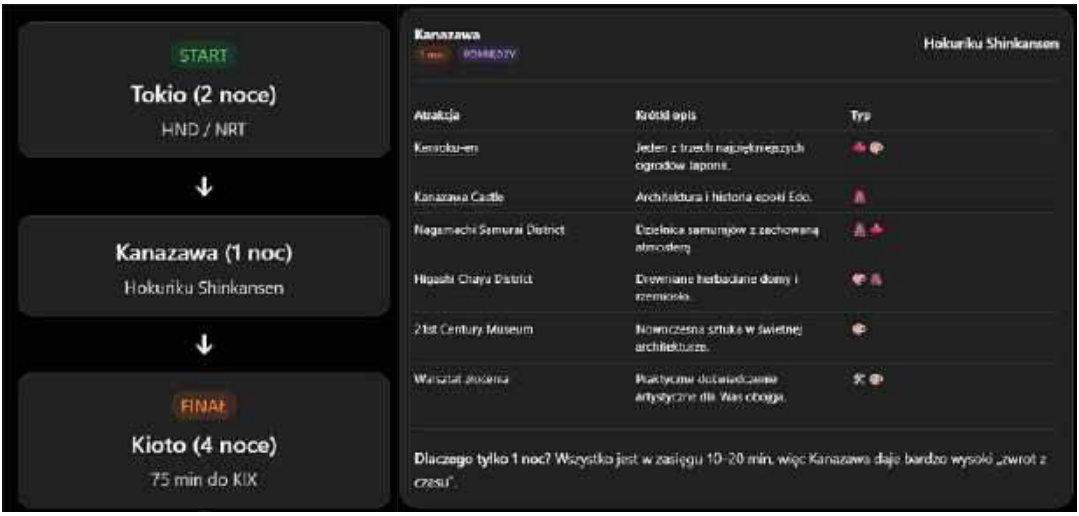
Po wybraniu atrakcji model zaproponował pięć najlepszych miast noclegowych oraz przygotował wstępny plan podróży obejmujący aż 17 dni. W tym momencie mogłem samodzielnie wybrać interesujące mnie miejsca, jednak ChatGPT dodatkowo zasugerował najbardziej oczywiste miasta i atrakcje dla krótszej, siedmiodniowej wycieczki. Dalsze planowanie warto już dostosować do własnych preferencji. Można rozpisać każdy dzień z góry albo zachować jedynie listę atrakcji wraz z najlepszymi porami ich odwiedzenia i podejmować decyzje na miejscu. Ostatecznie naszą podróż rozpoczniemy od dwóch noclegów w Tokio. Następnie spędzimy jedną noc w historycznej Kanazawie, a pozostałą część wycieczki przeznaczymy na Kioto.

Transport i szczegóły wycieczki

Japonia słynie z wyjątkowo sprawnej komunikacji publicznej, jednak na potrzeby bardziej uniwersalnego poradnika poprosiłem ChatGPT o porównanie wszystkich głównych opcji podróżowania po kraju. Analiza potwierdziła, że wszystkie wybrane przez nas atrakcje znajdują się w zasięgu pociągów, metra i autobusów, dzięki czemu wynajem samochodu nie był konieczny.

W kolejnym kroku model samodzielnie porównał dostępne bilety okresowe, bilety turystyczne oraz różnego rodzaju passy autobusowe i kolejowe. W naszym przypadku opłacalny okazał się jedynie 48godzinny bilet na metro w Tokio. Pozostałe przejazdy zostały policzone indywidualnie. Według wyliczeń ChatGPT łączny koszt komunikacji miejskiej dla jednej osoby podczas całego tygodnia wyniósł około 260 zł.

Obecnie ChatGPT posiada integrację z Google Maps, dzięki czemu może pomagać również w wyborze bardziej konkretnych miejsc, takich jak restauracje, kawiarnie czy punkty usługowe znajdujące się w pobliżu. Należy jednak zwrócić uwagę, że funkcja ta znajduje się we wczesnej fazie rozwoju i nie działa prawidłowo we wszystkich krajach (np. w Korei Południowej). Podobnie jak przy wyborze atrakcji, warto opisać swoje oczekiwania, poprosić o kilka propozycji i samodzielnie podjąć ostateczną decyzję.

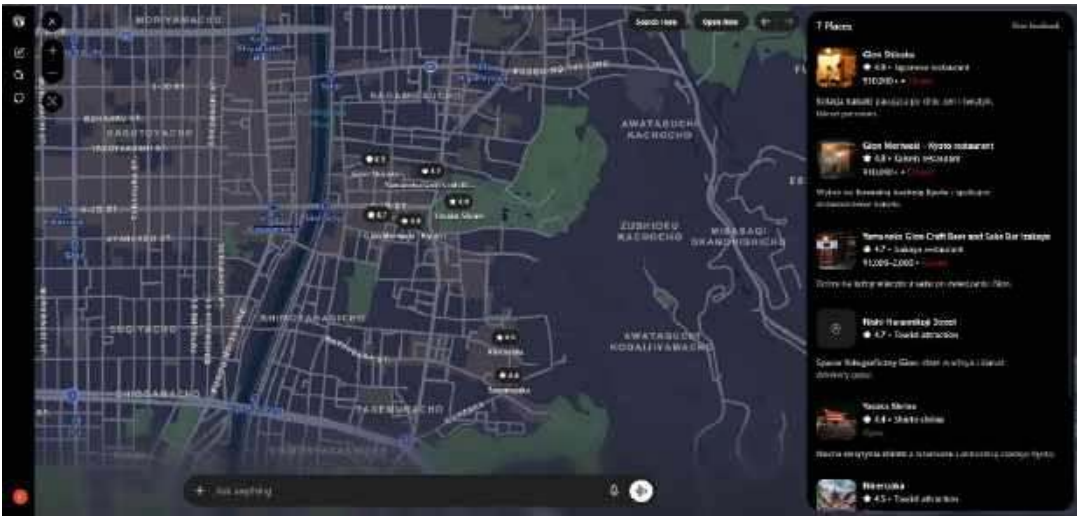


W podobny sposób model może pomóc w doborze hoteli, przygotowaniu listy bagażu oraz sprawdzeniu wymaganych dokumentów podróżnych. Warto również spytać Czat o bardziej ogólne aspekty wyjazdu, takie jak podstawowe zwroty grzecznościowe, różnice kulturowe czy praktyczne wskazówki, którymi podróżnicy dzielą się na forach internetowych.

ChatGPT może być przydatny także w trakcie samej podróży. Potrafi tłumaczyć napisy, menu, komunikaty oraz krótkie rozmowy w obcym języku. Jest bardzo użyteczny również na zakupach, szczególnie w krajach posługujących się innym alfabetem. Nie eliminuje całkowicie bariery językowej, ale w wielu sytuacjach pozwala ją znacząco ograniczyć i ułatwia poruszanie się po nieznanym kraju. W przeciwieństwie do tradycyjnych translatorów potrafi rozpoznawać i oddawać intencje oraz kontekst wypowiedzi, zamiast tłumaczyć ją dosłownie.

Podsumowanie

Z pomocą modeli językowych staranne przygotowanie spersonalizowanego i spójnego planu wycieczki może zająć jedno popołudnie zamiast wielu dni. ChatGPT potrafi dostosować się do naszych wymagań i w bardzo krótkim czasie wyszukać, uporządkować oraz porównać dużą liczbę



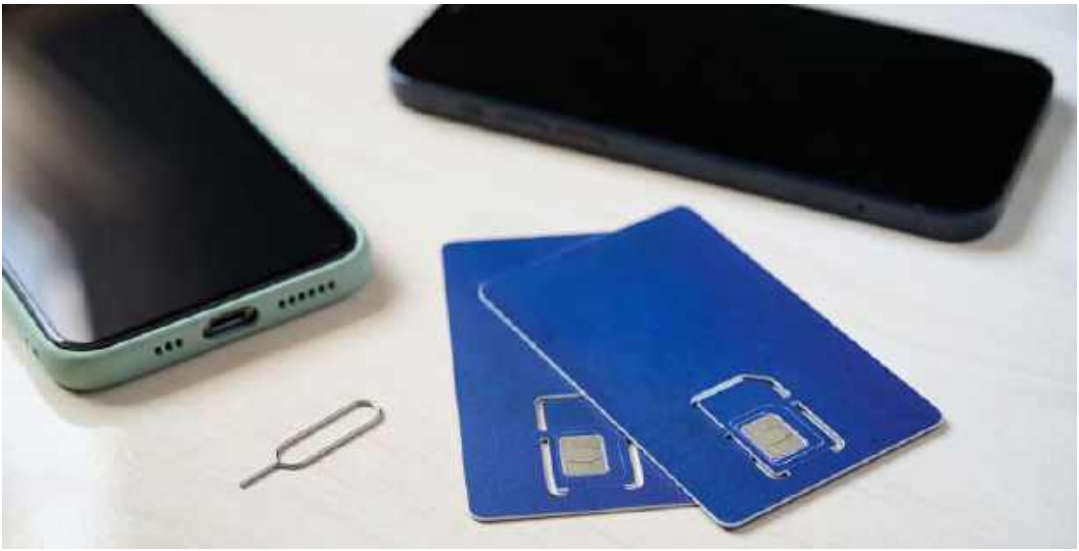
ChatGPT posiada obecnie wczesną wersję integracji z Mapami Google. Potrafi wyszukiwać i porównywać dowolne obiekty

Listopadowa 7 dniowa wycieczka do Japonii dla jednej osoby			
	Ekonomicznie	**Normalnie**	**Luksus**
Lot	2200 zł Promocje, gorsze godziny, 1 przesiadka. Możliwy Tokio wlot + Osaka wylot przy dobrej cenie.	2300 zł Realny zakup kilka miesięcy wcześniej. Lepsze godziny, normalne linie.	4500 zł Lepsze linie, krótsze przesiadki, wygodne godziny, mniejsza strata czasu.
Nocleg	700 zł Business hotel/mały pokój. Tokio poza centrum, Kioto poza Gion.	1500 zł Tokio: Ueno/Asakusa/ Shinjuku Kioto: Higashiyama/ Gion okolice.	3500 zł+ Lepsze pokoje, ryokan, nocleg jako część doświadczenia.
Transport między miastami	450...600 zł Podróż głównie autobusami nocnymi Minus: 8...10h w autobusach.	800...900 zł Japońskie superszybkie pociągi międzymiastowe nie są tanie.	1300...1800 zł Green Car, taxi przy bagażu/deszczu, brak kompromisów czasowych. Prywatne transfery.
Transport lokalny	150 zł COCA/Suica, dużo chodzenia. Metro tylko gdy potrzebne.	200...250 zł Metro Tokio Autobusy KiotoKanazawa bus pass Eizan Railway/ Kurama-Kibune.	600 zł Taksówki
Jedzenie	700 zł Konbini + ramen + curry + tanie bary.	1400 zł Restauracje + kawa/deser. Ramen, sushi, izakaya, matcha	3300 zł Kaiseki, omakase sushi, bary premium.
Atrakcje	130 zł Fushimi Inari, Meiji, Senso-ji, wiele chramów.	350 zł Eikando iluminacja, Kiyomizu-dera, Tofuku-ji Kenroku-en, Tokyo National Museum, Byodo-in	1000 zł+ Prywatni przewodnicy, premium tea ceremony, warsztaty rzemiosła.
Internet + drobne wydatki	100 zł eSIM/SIM + podstawowe rzeczy.	250 zł eSIM, kawy, desery, automaty, drobne zakupy.	600 zł Premium SIM, więcej kawiarni, spontaniczne wydatki.
Pamiątki	150 zł Omiyage, magnesy, słodycze.	350 zł Matcha, ceramika, rękodzieło, rzeczy z Kanazawy.	1200 zł Rękodzieło premium, ceramika artystyczna, luksusowe produkty.
SUMA	**~4 500...5 000 zł**	**~7 500 zł**	**~15 000...16 000 zł**

informacji. W przedstawionym przykładzie udało się przygotować siedmiodniową wycieczkę do Japonii bogatą w dopasowane do zainteresowań atrakcje, a jednocześnie mieszczącą się komfortowo w budżecie do 10 000 zł.

Podczas korzystania z AI trzeba jednak pamiętać o jej ograniczeniach. Model może ulegać wpływowi treści marketingowych oraz popełniać błędy takie jak halucynacje, szczególnie w przypadku cen, godzin przejazdów czy dostępności usług. Dlatego każdą istotną informację warto potwierdzić w oficjalnych źródłach lub niezależnych serwisach.

Ostateczne decyzje zawsze należą do użytkownika. To on wybiera, w których aspektach planowania chce skorzystać z pomocy AI – zarówno przed wyjazdem, jak i w trakcie samej podróży. Sztuczna inteligencja nie zastępuje zdrowego rozsądku ani samodzielnej weryfikacji informacji, ale może znacząco przyspieszyć planowanie, ułatwić organizację i pomóc sprawniej poruszać się po świecie. ■ **Karol Chruzik**



Koniec karty SIM

Plastikowa karta znika z telefonów. Co ją zastępuje i co to zmienia dla użytkownika

Od 2022 roku telefony bez szufladki na kartę SIM sprzedawano wyłącznie na rynku amerykańskim. iPhone 17 Air jest pierwszym modelem, który nie ma jej niezależnie od kraju sprzedaży. Według GSMA Intelligence na koniec 2025 roku eSIM obsługiwało 5 procent połączeń smartfonowych na świecie, a na koniec 2026 roku ma to być 10 procent. Karta, którą przekładaliśmy między telefonami przez trzydzieści pięć lat, jest zastępowana przez oprogramowanie. Warto wiedzieć, co dokładnie się zmienia – bo zmienia się więcej niż sposób montażu.

Czym jest karta SIM

Karta SIM nie jest pamięcią na numer telefonu. Jest to karta mikroprocesorowa: ma własny procesor, pamięć trwałą i system operacyjny, a od czasu wprowadzenia standardu Java Card także możliwość uruchamiania niewielkich programów. W terminologii technicznej nośnik nazywa się UICC, a SIM lub USIM to aplikacja działająca na tym nośniku.

Karta przechowuje dwie rzeczy o zasadniczym znaczeniu. Pierwsza to numer IMSI, czyli międzynarodowy identyfikator abonenta – inny niż numer telefonu, który jest tylko etykietą przypisaną do IMSI w bazie operatora. Druga to klucz Ki: liczba o długości 128 bitów, znana wyłącznie karcie i rejestrowi abonentów operatora.

Sposób, w jaki sieć sprawdza kartę, jest wart wyjaśnienia, bo tłumaczy całą resztę artykułu.

Rysunek 1. Uwierzytelnianie w sieci komórkowej. Klucz nigdy nie opuszcza karty

Sieć nie pyta karty o klucz. Wysyła do niej liczbę losową, oznaczaną RAND. Karta wykonuje na niej działanie z użyciem klucza Ki i odsyła wynik: odpowiedź SRES oraz klucz szyfrowania Kc, którym będzie zaszyfrowana transmisja. Operator wykonuje to samo obliczenie u siebie i porównuje wyniki. Zgodność oznacza, że karta zna Ki, choć klucz ani razu nie został przesłany. W sieciach 2G służył do tego algorytm A3/A8 w wersji COMP128, w sieciach trzeciej generacji i nowszych – Milenage, dodatkowo pozwalający karcie sprawdzić, czy rozmawia z prawdziwą siecią.

Karta jest zatem elementem bezpieczeństwa. Jej sensem nie jest przechowywanie danych, tylko wykonywanie obliczenia kryptograficznego w miejscu, z którego klucz nie może wyciec. To rozróżnienie będzie potrzebne przy ocenie eSIM.

Trzydzieści pięć lat skracania plastiku

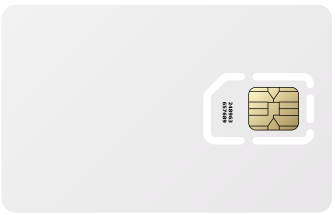
Pierwszą kartę SIM wyprodukowała w 1991 roku monachijska firma Giesecke+Devrient, dostarczając 300 sztuk fińskiemu operatorowi Radiolinja. Rok później Radiolinja sprzedawał pierwsze telefony GSM z kartą – Nokia 1101. Karta miała wtedy wymiary karty płatniczej: 85,6 na 53,98 milimetra. Format nazwano później 1FF.

Kolejne formaty nie zmieniały układu scalonego, tylko usuwały plastik wokół niego. Mini-SIM (2FF) o wymiarach 25 na 15 milimetrów pojawił się w 1996 roku, micro-SIM (3FF) o wymiarach 15 na 12 milimetrów w 2003, a nano-SIM (4FF) o wymiarach 12,3 na 8,8 milimetra w 2012 – pierwszym telefonem z tym formatem był iPhone 5. Kto pamięta docinanie karty nożyczkami do mniejszego gniazda, ten robił dokładnie to, co producenci: usuwał obudowę, nie ruszając modułu.

Ostatnim krokiem tej samej drogi jest format MFF2 – układ przeznaczony do przylutowania do płyty głównej. To jest właśnie eSIM w sensie sprzętowym: nie inna technologia, tylko ta sama karta bez obudowy i bez gniazda.

eSIM: co dokładnie się zmienia

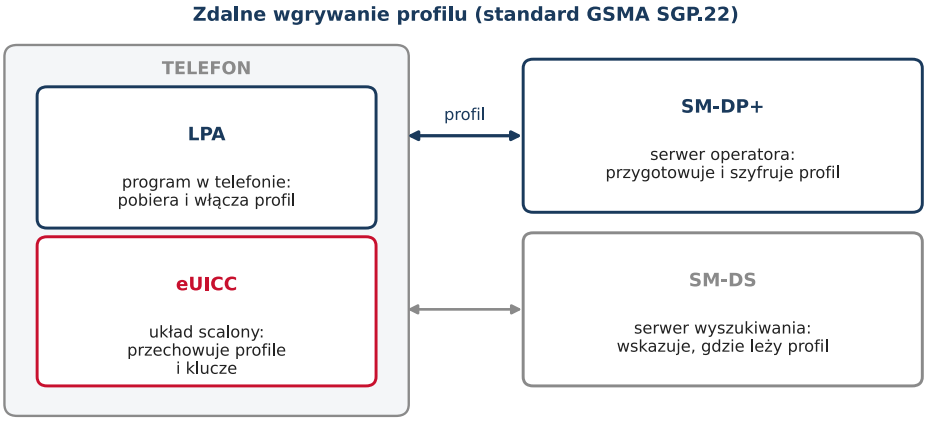
Nazwa eSIM opisuje dwie rzeczy naraz, co bywa źródłem nieporozumień. Pierwsza to sprzęt: układ eUICC wlutowany w płytę. Druga i ważniejsza to sposób dostarczania



1FF (1991 r.)	2FF (1996 r.)	3FF (2003 r.)	4FF (2012 r.)	MFF2 (2013 r.)
pełnowymiarowa	mini-SIM	micro-SIM	nano-SIM	wlutowany
85,36×53,98 mm	25×15 mm	15×12 mm	12,3×8,8 mm	~5×6 mm

Złotym kolorem zaznaczono pole styków. Wymiary według norm ETSI; MFF2 podano w przybliżeniu — jest to obudowa do lutowania, nie karta.

Rysunek 2. Kolejne formaty w skali. Malała powierzchnia karty, nie układ scalony



Kod QR podawany przez operatora zawiera adres serwera SM-DP+ i kod aktywacyjny. Profil jest szyfrowany dla konkretnego układu eUICC.

Rysunek 3. Elementy biorące udział w pobraniu profilu do telefonu

danych abonenta. W karcie tradycyjnej IMSI i klucz Ki zapisywano fabrycznie, w zakładzie personalizacji, i nie dawało się ich zmienić. W eUICC te dane tworzą profil, który można pobrać przez sieć, wyłączyć i usunąć. Procedurę nazwano zdalnym wgrywaniem profilu (remote SIM provisioning) i opisano w specyfikacjach GSMA.

W wariancie konsumenckim, opisanym w dokumentach SGP.21 i SGP.22, biorą udział trzy elementy. W telefonie działa program zwany LPA, odpowiedzialny za pobranie i włączenie profilu. Po stronie operatora pracuje serwer SM-DP+, który przygotowuje profil i szyfruje go dla konkretnego egzemplarza układu eUICC. Trzeci element, SM-DS, to serwer wyszukiwania – pozwala telefonowi znaleźć czekający na niego profil bez skanowania kodu. Kod QR, który dostaje klient, zawiera adres serwera i jednorazowy kod aktywacyjny.

W układzie eUICC może być zapisanych kilka profili, ale zwykle tylko jeden bywa aktywny; specyfikacja Samsunga w wersji 3.0 dopuszcza więcej niż jeden profil włączony jednocześnie. To odpowiada na częste pytanie, czy eSIM zastępuje telefon dwusimowy: zastępuje, o ile producent zaimplementował obsługę wielu profili.

Dla urządzeń bez ekranu i klawiatury – liczników energii, alarmów, czujników – wariant konsumencki się nie nadaje, bo zakłada, że ktoś zeskanuje kod. Do 2023 roku używano do tego starszej specyfikacji SGP.02, wymagającej wysyłania technicznych SMS-ów. Zastąpiła ją para dokumentów SGP.31 i SGP.32, w której rolę użytkownika przejmuje serwer zarządzający, a wgrywanie profilu odbywa się przez zwykłe połączenie internetowe. Zaplecze pozostało to samo – ten sam serwer SM-DP+ obsługuje telefony i czujniki.

iSIM: układ, którego nie ma na płycie

Następny krok jest już wdrażany. iSIM to funkcja karty przeniesiona do wnętrza głównego procesora urządzenia, do wydzielonego, odizolowanego obszaru. Nie ma osobnego układu ani osobnej powierzchni na płycie. Pierwszy iSIM z certyfikatem bezpieczeństwa GSMA opracowały wspólnie firmy Thales i Qualcomm, uruchamiając go na platformie Snapdragon; rozwiązanie spełnia te same wymagania zdalnego wgrywania profili co eSIM.

Prognozy różnią się co do tempa. Kaleido Intelligence szacuje 300 milionów układów iSIM w 2027 roku, co odpowiadałoby 19 procentom wszystkich dostaw eSIM. Juniper Research podaje wzrost z 800 tysięcy sztuk w 2024 roku do 210 milionów w 2028. Obie liczby wskazują ten sam kierunek: najpierw urządzenia przemysłowe i samochody, potem telefony.

Co użytkownik zyskuje, a co traci

Po stronie zysków jest przede wszystkim czas. Uruchomienie numeru zajmuje kilkanaście minut zamiast oczekiwania na kuriera, a pakiet danych na wyjazd zagraniczny kupuje się w aplikacji przed wylotem. Znika też cała kategoria awarii: karta się nie utleni, nie pęknie i nie wypadnie z tacki. Znika odpad – plastikowa karta z opakowaniem to kilka gramów tworzywa na każdą aktywację.

Jest jeszcze korzyść mniej oczywista, warta odnotowania przy okazji kradzieży telefonu. Pierwszą czynnością złodzieja bywa wyjęcie karty, żeby odciąć urządzenie od sieci i uniemożliwić lokalizowanie. Profilu eSIM nie da się wyjąć – trzeba go usunąć z poziomu systemu, a do tego potrzebne jest odblokowanie ekranu.

Po stronie strat jest utrata niezależności od urządzenia. Kartę można było w dziesięć sekund przełożyć do zapasowego telefonu – cudzego, starego, pożyczonego. Profil eSIM jest związany z konkretnym układem eUICC i przeniesienie go wymaga albo narzędzia producenta, albo nowego kodu od operatora. Producenci mają własne mechanizmy – Apple eSIM Quick Transfer, Google eSIM Transfer Tool – ale działają one najlepiej w obrębie jednego ekosystemu. Przy przenosinach z Androida na iPhone lub odwrotnie zwykle trzeba zalogować się do aplikacji operatora albo skontaktować się z obsługą klienta po nowy kod QR.

Drobiazg, o którym warto uprzedzić czytelnika, bo bywa przykrą niespodzianką: kontakty i wiadomości zapisane w pamięci fizycznej karty przepadają przy wymianie na eSIM. Orange ostrzega o tym wprost w opisie usługi. Trzeba je skopiować wcześniej.

Bezpieczeństwo: co się zmienia, a co nie

W tej sprawie krąży uproszczenie warte sprostowania. eSIM bywa reklamowany jako zabezpieczenie przed przejęciem numeru, czyli atakiem znanym jako SIM swap. To nieporozumienie wynikające z pomylenia dwóch różnych zagrożeń.

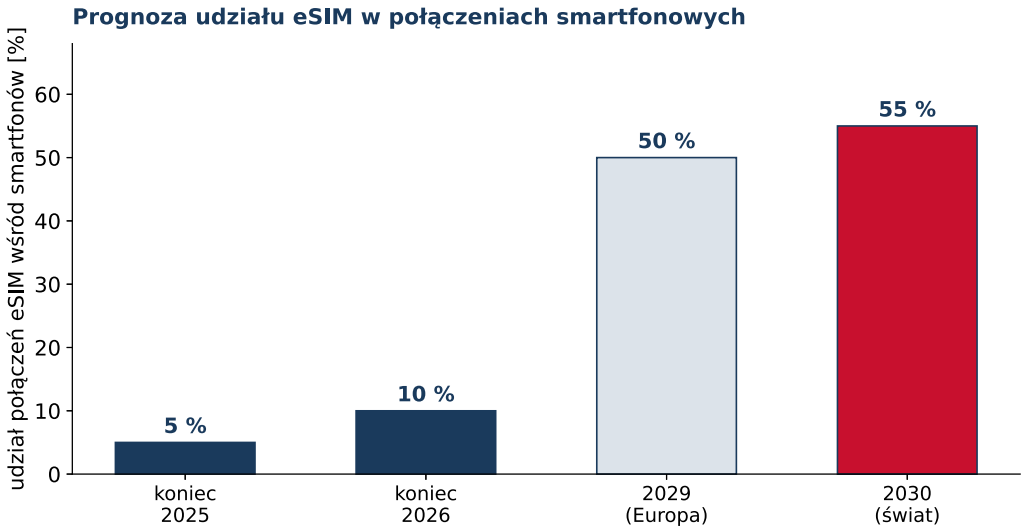
Przejęcie numeru nie polega na kradzieży karty. Polega na przekonaniu operatora, że dzwoni właściciel numeru, który zgubił kartę i prosi o wydanie nowej. Napastnik zbiera wcześniej dane osobowe z wycieków i mediów społecznościowych, żeby przejść weryfikację. Jeżeli się uda, na jego urządzeniu zaczynają działać połączenia i SMS-y ofiary – w tym kody jednorazowe do bankowości.

Ten atak działa na eSIM dokładnie tak samo, a bywa nawet szybszy, bo nie wymaga wysyłania niczego pocztą: wystarczy nowy kod aktywacyjny przesłany na adres e-mail. Atakujący zamiast prosić o kartę, prosi o wgranie profilu na swoje urządzenie. Zjawisko jest udokumentowane co najmniej od jesieni 2023 roku, gdy analitycy odnotowali ponad sto prób przejęcia kont klientów w jednej tylko instytucji finansowej. Słabym punktem jest procedura weryfikacji po stronie operatora, nie postać nośnika.

Wniosek praktyczny jest taki sam jak przy artykule o hasłach: numer telefonu nie powinien być podstawą zabezpieczenia konta. Do uwierzytelniania dwuskładnikowego lepiej służy aplikacja generująca kody lub klucz sprzętowy, a konto w serwisie operatora warto zabezpieczyć osobnym, mocnym hasłem i dodatkowym składnikiem. Warto też sprawdzić, czy operator oferuje blokadę zmiany karty i przeniesienia numeru – kilku dużych operatorów udostępnia taką opcję, ale trzeba ją włączyć samodzielnie.

Polska: eSIM jest, telefonów bez tacki nie ma

Wszyscy czterej operatorzy sieci komórkowych w Polsce oferują eSIM, choć na różnych zasadach. Play udostępnia go także w ofercie na kartę, co nie jest regułą na rynku. Plus wprowadził usługę dodatkowej karty eSIM za 10 złotych miesięcznie, pozwalającą aktywować do pięciu wirtualnych kopii jednego numeru na różnych urządzeniach; przy uruchomieniu obsługiwane były wyłącznie urządzenia z Androidem, a pierwszych pięć wymian karty fizycznej na eSIM jest bezpłatnych. Play oferuje analogiczne rozwiązanie w ramach usługi Multi SIM za 9 złotych miesięcznie. Orange wymaga abonamentu do aktywacji dodatkowej karty eSIM.



Dane: GSMA Intelligence, prognoza z 2026 r. Wartość dla 2030 r. odpowiada 4,9 mld połączeń.
Dwa pierwsze słupki to stan zmierzony i prognoza bieżącego roku, dwa kolejne — progi przekroczenia połowy rynku.

Rysunek 4. Prognozowany udział eSIM w połączeniach smartfonowych

Czego w Polsce nie ma, to telefonów wyłącznie na eSIM. Operatorzy przyznają to wprost: takie modele wchodzą na rynek powoli i u nas nie są dostępne. Powód nie jest techniczny, tylko handlowy. Polski rynek prepaid opiera się na sprzedaży starterów w kioskach, sklepach sieciowych i na stacjach paliw, a każdą kartę trzeba zarejestrować na dane osobowe. Cała ta ścieżka zakłada, że klient wychodzi ze sklepu z fizycznym przedmiotem. Zmiana wymaga przebudowy procesu sprzedaży, nie wymiany sprzętu.

Jest jeszcze skutek uboczny dotyczący telefonów z importu. Egzemplarze produkowane na rynek amerykański od modelu iPhone 14 nie mają gniazda karty, podobnie część modeli Samsunga. Kupując taki telefon w Polsce, trzeba wcześniej sprawdzić, czy operator wyda profil eSIM na wybraną ofertę.

Słowniczek

UICC – nośnik, czyli sama karta mikroprocesorowa. SIM i USIM to aplikacje działające na tym nośniku; USIM to wersja dla sieci trzeciej generacji i nowszych.

eUICC – układ scalony przystosowany do przechowywania wielu profili i ich zdalnej wymiany. Sprzętowa podstawa eSIM.

Profil – zestaw danych abonenta: numer IMSI, klucz Ki, ustawienia operatora. To, co dawniej zapisywano w karcie fabrycznie, a dziś pobiera się przez sieć.

IMSI – międzynarodowy identyfikator abonenta, do 15 cyfr. Numer telefonu jest tylko przypisaną do niego etykietą.

Ki – klucz o długości 128 bitów, wspólny dla karty i rejestru operatora. Nigdy nie jest przesyłany.

LPA – program w telefonie zarządzający pobieraniem i przełączaniem profili.

SM-DP+ – serwer przygotowujący i szyfrujący profil dla konkretnego układu eUICC.

MFF2 – format obudowy do lutowania na płycie głównej, stosowany w eSIM.

Co dalej?

Kierunek jest przesądzony, tempo – nie. GSMA Intelligence przewiduje, że w 2030 roku połączeń eSIM w telefonach będzie 4,9 miliarda, czyli około 55 procent wszystkich; próg połowy rynku Ameryka Północna ma przekroczyć w 2027 roku, a Europa w 2029. Dwa wydarzenia z końca 2025 roku przyspieszyły ten proces: rozszerzenie przez Apple modelu bez gniazda karty na rynki poza Stanami oraz uruchomienie eSIM dla telefonów przez operatorów chińskich, którzy wcześniej dopuszczali go tylko w urządzeniach ubieralnych i przemysłowych.

Otwarte pozostają trzy kwestie i to one zdecydują, czy zmiana wyjdzie użytkownikowi na dobre. Pierwsza to swoboda zmiany operatora. Przy

karcie fizycznej przeniesienie numeru wymagało wizyty i podpisu, ale nikt nie mógł zablokować użytkownikowi wyjęcia karty. Przy profilu pobieranym z serwera więcej zależy od procedur – łatwiej to uprościć, ale też łatwiej obwarować warunkami.

Druga to rynek urządzeń używanych. Telefon bez gniazda karty jest wart tyle, ile wart jest dostęp do profilu – jeśli poprzedni właściciel nie usunie swojego, kupujący ma problem, którego przy karcie nie było, bo wystarczyło ją wyjąć.

Trzecia to grupy, które zostają z tyłu: użytkownicy starszych telefonów, klienci prepaid bez konta w aplikacji, osoby kupujące starter w kiosku. Dopóki operator ma dwie ścieżki obsługi, problemu nie ma. Pytanie brzmi, co się stanie, gdy jedna z nich przestanie się opłacać.

Karta SIM przetrwała trzydzieści pięć lat, cztery generacje sieci i pięć zmian formatu, bo rozwiązywała konkretny problem: pozwalała oddzielić tożsamość abonenta od urządzenia. Ta funkcja zostaje. Znika tylko przedmiot, który ją nosił – razem ze szpilką do wysuwania tacki, która w wielu domach przetrwa pewnie dłużej niż same karty.

(red.)

Bibliografia

Wszystkie źródła sprawdzone 10 sierpnia 2026 r.

1. GSMA (2026). SGP.21 i SGP.22 – architektura i specyfikacja techniczna zdalnego wgrywania profili dla urządzeń konsumenckich. gsma.com
2. GSMA (2023, aktualizacja 2026). SGP.31 i SGP.32 – specyfikacje eSIM dla internetu rzeczy; zastąpienie architektury SGP.02, rezygnacja z technicznych SMS-ów.
3. droam.news (25.05.2026). New eSIM standards explained: SGP.22, SGP.32, eIM, discovery service – omówienie ról LPA, SM-DP+ i SM-DS.
4. velocityiot.io (13.06.2026). GSMA eSIM standards: SGP.02, SGP.22 and SGP.32 – porównanie modeli wgrywania profilu.
5. Spenza (18.02.2026). What is remote SIM provisioning – stan wdrożeń zdalnego wgrywania profili w 2026 r.
6. GSMA (01.05.2026). eSIM mass market deployment moves from forecast to fact – dane GSMA Intelligence: 5 % penetracji na koniec 2025 r., 10 % na koniec 2026 r., przewaga eSIM nad kartami wyjmowanymi do 2030 r.; uruchomienie eSIM przez operatorów chińskich.
7. Cellesim (16.06.2026). eSIM statistics 2026 – zestawienie prognoz: 4,9 mld połączeń eSIM w 2030 r., progi 50 % dla Ameryki Północnej i Europy.
8. Thales / Qualcomm (komunikat prasowy, aktualizacja 2026). Pierwszy iSIM z certyfikatem bezpieczeństwa GSMA na platformie Snapdragon; prognoza Kaleido Intelligence: 300 mln układów iSIM w 2027 r.
9. Mordor Intelligence (26.02.2026). Embedded SIM market – prognoza Juniper Research dla iSIM: 800 tys. sztuk w 2024 r. i 210 mln w 2028 r.; specyfikacja Samsung eSIM 3.0.
10. Grokipedia (28.03.2026). SIM card – historia standaryzacji formatów pod egidą ETSI i 3GPP, wymiary 1FF–4FF, funkcja elementu bezpieczeństwa.
11. Giesecke+Devrient – dane historyczne: pierwsza partia 300 kart dla operatora Radiolinja (1991) i pierwszy telefon GSM z kartą, Nokia 1101 (1992).
12. Intel 471 (20.08.2025). A look at eSIMs and number hijacking – mechanizm przejmowania numeru przy zdalnym wydawaniu profilu.
13. BleepingComputer (2024, materiał źródłowy). SIM swappers hijacking phone numbers in eSIM attacks – ponad sto prób przejęcia kont klientów jednej instytucji finansowej od jesieni 2023 r.
14. Deepstrike (09.09.2025). SIM swap scam statistics – analiza, dlaczego postać nośnika nie chroni przed atakiem na procedurę weryfikacji operatora.
15. Spy-Fy (12.06.2026). SIM swap attack: how to stop number hijacking – zalecenia dotyczące blokady zmiany karty i przeniesienia numeru.
16. spidersweb.pl (29.01.2026). Ranking kart eSIM 2026 – warunki usług operatorów w Polsce, w tym dodatkowa karta eSIM w Plusie (10 zł miesięcznie, do pięciu kopii numeru, pierwsze pięć wymian bezpłatnie).
17. Saily (17.04.2026). eSIM Play – usługa Multi SIM (9 zł miesięcznie) i tryb aktywacji.
18. Orange Polska. Opis usługi eSIM – wymóg abonamentu przy dodatkowej karcie, ostrzeżenie o utracie kontaktów i SMS-ów zapisanych na karcie fizycznej. orange.pl
19. Play (materiał informacyjny). Które telefony nie mają slotu na kartę SIM – brak dostępności modeli wyłącznie na eSIM na rynku polskim.
20. holafly.com (18.05.2026). Telefony z eSIM – zestawienie modeli; iPhone 17 Air jako pierwszy pozbawiony tacki niezależnie od kraju produkcji.
21. T-Mobile Polska (12.06.2026). Karta SIM prepaid w Polsce – dostępność eSIM w ofertach na kartę u wszystkich czterech operatorów.

O tych, co przekuli innowacyjne wizje w biznesowy sukces
W polskim życiu publicznym coraz częściej używanym słowem jest odmieniany na wszystkie sposoby wyraz „innowacje". I tak powinno być przez najbliższe lata, bo ambicją naszego kraju jest spektakularny awans do grona państw o gospodarce kreatywnej, tworzącej własne produkty i marki, znane i szanowane w świecie.
To Wy, młodzi Czytelnicy MT, macie tego dokonać! Żeby Was natchnąć dobrymi przykładami, co miesiąc przedstawiamy reprezentantów czołówki światowych liderów innowacji. Najczęściej byli oni jeszcze w wieku szkolnym lub studenckim, gdy w ich głowach rodziły się śmiałe pomysły skutkujące później powstaniem superproduktów, wielkich brandów i fantastycznych fortun.
To oni kształtują cywilizację technologiczną.
To bohaterowie naszych czasów.

1. Seymour Cray, źródło: Wikimedia Commons

Człowiek, który budował maszyny jak rzeźbiarz

Seymour Cray

Przez ponad trzy dekady każdy najszybszy komputer na świecie był jego dziełem. Projektował je sam, w małych zespołach, z dala od korporacyjnych zebrań i raportów. Kiedy pracodawca dał mu więcej pracowników, odszedł i założył własną firmę. Seymour Cray nie chciał zarządzać. Chciał budować.

CV: Seymour Roger Cray

Urodzony:	28 września 1925, Chippewa Falls, Wisconsin, USA
Zmarł:	5 października 1996, Colorado Springs, Colorado (wypadek samochodowy)
Edukacja:	University of Minnesota – inżynieria elektryczna (1950), matematyka (1951)
Kariera:	Engineering Research Associates (1951–1957) → Control Data Corporation (1957–1972) → założyciel Cray Research (1972–1989) → założyciel Cray Computer Corporation (1989–1996)
Główne projekty:	CDC 1604 (1958), CDC 6600 (1964), Cray-1 (1976), Cray-2 (1985)
Zainteresowania:	narciarstwo, ogrodnictwo, kopanie tunelów pod domem

Chłopiec od radia

Seymour Roger Cray urodził się 28 września 1925 roku w Chippewa Falls w Wisconsin, małym miasteczku przy granicy z Minnesotą. Ojciec George był inżynierem miejskim. Dom miał warsztat. Seymour spędzał w nim godziny, składając radioodbiorniki, lutując układy elektroniczne i czytając książki o elektronice. W szkole średniej zbudował mechaniczny komputer analogowy z resztek sprzętu elektrycznego.

Wojsko wzięło go do działań szyfrowych i wywiadu. Przez dwa lata przetwarzał zaszyfrowane depesze, rozbijając japońskie kody na dużych maszynach elektromechanicznych. Kiedy wrócił z frontu, wiedział, co chce robić: budować maszyny szybsze niż te, na których pracował. Ukończył elektrotechnikę na University of Minnesota i poszedł do pracy.

ERA i początek

Pierwsza praca była idealna: Engineering Research Associates w Minneapolis budowało komputery dla marynarki wojennej USA. Cray szybko okazał się kimś wyjątkowym – nie tylko rozumiał elektronikę, ale czuł ją. Potrafił zaprojektować układ, który będzie działał szybciej, zużywał mniej mocy i był prostszy w budowie jednocześnie. To bardzo trudna kombinacja.

Kiedy ERA zostało wchłonięte przez Remington Rand, a potem przez Sperry, Cray poczuł ciężar biurokracji. W 1957 roku razem z Williamem Norrisem założył Control Data Corporation. Była to jedna z pierwszych firm technologicznych, którą założyli inżynierowie, nie finansiści. Cray dostał jedno żądanie: wolność projektową. Odpowiedział CDC 1604 – pierwszym komercyjnym komputerem tranzystorowym.

CDC 6600 – najszybszy komputer świata

W 1964 roku Cray zaprezentował CDC 6600 – maszynę, która była trzy razy szybsza od czegokolwiek, co istniało. IBM, który wtedy dominował na rynku komputerów, dowiedział się o tych wynikach i prezes Thomas Watson Jr. napisał wewnętrzną notatkę: „CDC 6600 jest budowany przez trzydziestu czterech ludzi. My mamy 34 000 i jesteśmy daleko za nimi. Proszę o wyjaśnienie”.

2. CDC 6600 – najszybszy komputer świata w latach 1964–69. Fot. Autorstwa Hullie – Praca własna, Domena publiczna, https://commons.wikimedia.org/w/index.php?curid=2514283

Odpowiedź była prosta: Cray pracował w grupie, którą sam zrekrutował i która nie miała kolegiów, recenzji ani hierarchii zatwierdzeń. Każda decyzja projektowa leżała po jego stronie. Każdy kompromis – też. CDC 6600 miał 3 MFLOPS (*Millions Floating Point Operations per Second* – miliony operacji zmiennoprzecinkowych na sekundę) i stał się podstawowym narzędziem fizyków jądrowych w CERN oraz inżynierów w NASA. To od CDC 6600 pochodzi słowo „superkomputer”.

Ucieczka do lasu

Kiedy CDC rosło, rosła i biurokracja. Zebrania. Raporty. Kolegia projektowe. Cray nie znosił zebrań. Wynegocjował z Norrisem jedyną w swoim rodzaju umowę: przeniesie swoje laboratorium do rodzinnego Chippewa Falls, tysiąc

Jak mierzymy szybkość komputerów?

FLOPS – *Floating Point Operations Per Second* – to jednostka wydajności obliczeniowej. Mierzy, ile działań na liczbach zmiennoprzecinkowych (takich jak 3,14159) komputer wykonuje w ciągu sekundy. Nauka potrzebuje takich działań do symulacji fizycznych, prognozowania pogody i obliczeń jądrowych.

CDC 6600 (1964): 3 megaFLOPS – 3 miliony działań na sekundę. Cray-1 (1976): 160 megaFLOPS. Cray-2 (1985): 1 900 megaFLOPS. Dziś najszybsze superkomputery osiągają ponad 1 000 000 000 megaFLOPS, czyli 1 eksaFLOPS. iPhone 15 ma ok. 2 000 megaFLOPS – czyli jest mocniejszy niż Cray-1, który kosztował 8,86 miliona dolarów.

3. Cray-1 w Computer History Museum, Mountain View, Kalifornia. Źródło: FlyAkwa – Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=69936769

kilometrów od Minneapolis. Będzie pracował z zespołem maksymalnie kilkudziesięciu osób i nie będzie musiał przyjeżdżać na zebrania. CDC płaci rachunki. Cray buduje.

Z Chippewa Falls wyjechał Cray-1 w 1976 roku. Był rewolucyjny nie tylko technicznie, ale i estetycznie. Miał kształt litery C – siedzenie wokół centralnej kolumny przetwarzającej. Los Alamos National Laboratory kupiło pierwszą sztukę za 8,86 miliona dolarów. Cray-1 wykonywał 160 megaflopsów. Nic na świecie nie było szybsze.

Samotnik, tunel i elfy

Kiedy odwiedzali go dziennikarze i pytali, jak wypoczywa, Cray mówił bez ironii, że kopie w ogrodzie tunel. Nie metaforycznie – fizyczny tunel pod swoim domem, kilka metrów długi, który co kilka lat zaczynał od nowa. Mówił, że elfy pomagają mu przy kopaniu i podszeptują pomysły. Nie zawsze było jasne, czy żartuje.

Nikt nigdy nie był pewien. Pracownicy Cray Research wspominali, że kiedy projekt utknął w martwym punkcie, Cray znikał na kilka dni. Potem wracał z gotowym rozwiązaniem. Nie wyjaśniał, skąd je wziął. Być może rzeczywiście pytał elfów.

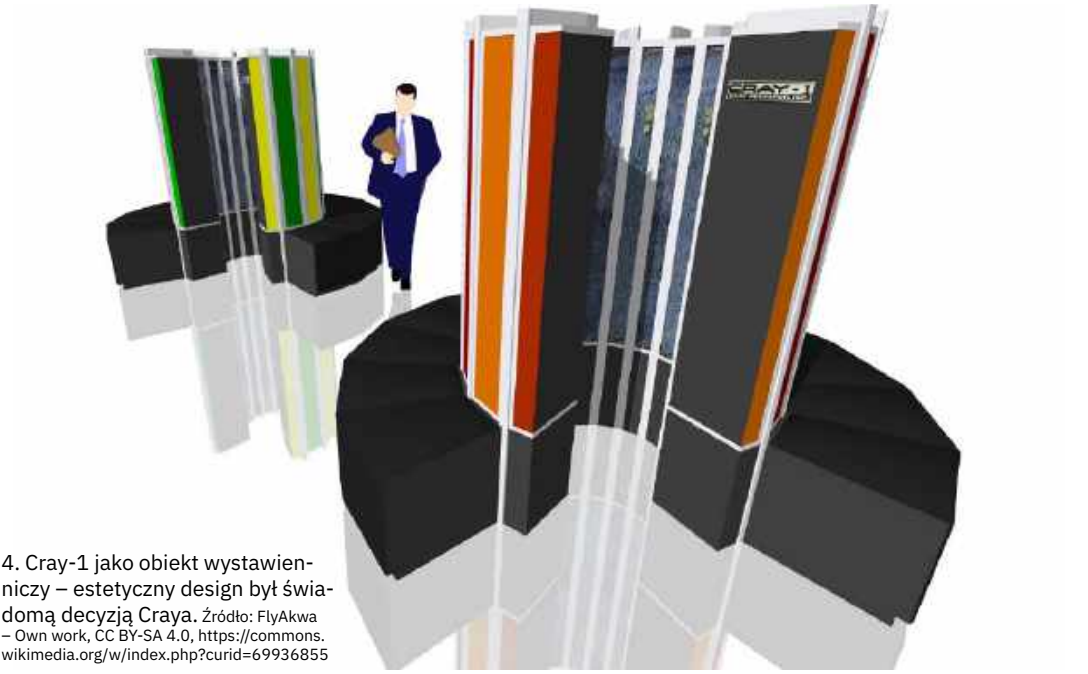
Cray-2 (1985) był 12 razy szybszy od Craya-1. Projekty Cray-3 i Cray-4 napotkały problemy z arsenkiem galu zamiast krzemu. W 1989 roku Cray Research wstrzymało finansowanie projektu. Cray odszedł i założył Cray Computer Corporation.

Bankructwo i wypadek

5 października 1996 roku Seymour Cray miał wypadek samochodowy w Colorado Springs. Ciężko ranny, zmarł w szpitalu pięć dni później. Miał 71 lat. Pracował nad Crayem-4 do końca. W jego laboratorium były kartki z obliczeniami, części zamienne i lista pytań do rozstrzygnięcia.

Cray Computer Corporation zbankrutowała rok przed jego śmiercią. Rynek superkomputerów zmieniał się: klastry z tanich procesorów biły drogą elektronikę szytą na miarę. Model Craya – jeden genialny inżynier, mały zespół, bezkompromisowa architektura – zderzył się ze światem, w którym wystarczyło połączyć tysiąc serwerów Della.

Wydajność komputerów Seymour Craya na tle epoki – w MFLOPS



4. Cray-1 jako obiekt wystawienniczy – estetyczny design był świadomą decyzją Craya. Źródło: FlyAkwa – Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=69936855

Co zostało po Crayu

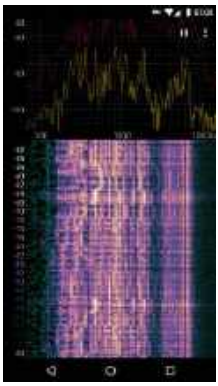
Firma Cray Inc. – kontynuacja Cray Research – produkowała superkomputery do 2019 roku, gdy przejęło ją HPE.

Ale prawdziwe dziedzictwo Craya jest gdzie indziej. Pokazał, że jeden dobry inżynier z małym zespołem może pokonać korporację. Ta myśl jest fundamentem kultury startupowej. Każdy założyciel firmy technologicznej, który wierzy, że jakość wynika z koncentracji, a nie ze skali, jest choć trochę Crayem.

Steve Jobs powiedział kiedyś, że Cray był artystą. Projektował superkomputer jak rzeźbiarz – z myślą o formie, która powinna być piękna, bo tylko piękna forma jest naprawdę wydajna. Cray-1 stał się eksponatem muzealnym i po trzech dekadach nadal wygląda jak obiekt z wystawy designu. To niemałe osiągnięcie dla maszyny, która miała tylko liczyć. ■

Paweł Biernacki

Tym razem zestaw dla tych, którzy traktują telefon jak przyrząd. Analizator widma, symulator układów elektronicznych, diagnostyka sieci, skaner trójwymiarowy, pełne środowisko wiersza poleceń i sposób na dane za granicą bez wymiany karty. Wszystkie pozycje sprawdzone w sierpniu 2026 roku.



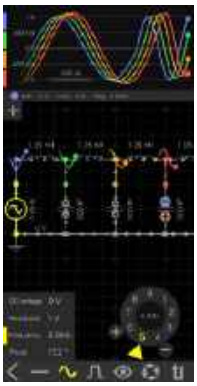
Spectroid

Analizator widma akustycznego w kieszeni

Spectroid zamienia mikrofon telefonu w analizator widma pracujący w czasie rzeczywistym. Na ekranie widać dwa wykresy: bieżące widmo częstotliwości oraz tak zwany wodospad, czyli mapę pokazującą, jak widmo zmieniało się w ostatnich sekundach. Zakres obejmuje całe pasmo słyszalne, a rozdzielczość można ustawić kosztem szybkości odświeżania. Program korzysta z banku filtrów o stałej dobroci, co daje rozdzielczość proporcjonalną do częstotliwości – dokładniejszą w niskich tonach, zgrubną w wysokich. To rozwiązanie bliższe temu, jak słyszy ucho niż klasyczna transformata o stałym kroku. W praktyce oznacza to, że łatwo znaleźć częstotliwość buczenia w zasilaczu, sprawdzić strojenie instrumentu albo zobaczyć, gdzie leży rezonans pomieszczenia.

Ograniczeniem jest mikrofon telefonu: jego charakterystyka nie jest płaska, a układ redukcji szumów w systemie potrafi zniekształcić pomiar. Do porównań względnych – który dźwięk jest głośniejszy, gdzie leży składowa – to nie przeszkadza. Do pomiarów bezwzględnych trzeba mikrofonu pomiarowego z kalibracją.

Producent: Carl Reinke
Platformy: Android (na iOS podobne funkcje oferują inne programy, np. SpectrumView)
Cena: bezpłatna, z reklamami
Możliwości: 8,5/10
Łatwość obsługi: 8,0/10
Ocena ogólna: 8,5/10



EveryCircuit

Symulator układów elektronicznych z animacją

EveryCircuit pozwala narysować palcem schemat i natychmiast zobaczyć, jak układ działa. Wyróżnia go sposób prezentacji: ładunek płynący przewodami jest animowany, napięcia zmieniają kolor elementów, a wbudowany oscyloskop rysuje przebiegi w tym samym oknie. Wartości elementów zmienia się pokrętłem podczas trwającej symulacji, więc od razu widać skutek.

Biblioteka obejmuje elementy bierne, diody, tranzystory bipolarne i polowe, wzmacniacze operacyjne, źródła i podstawowe układy cyfrowe. To wystarcza do nauki: dzielnika napięcia, filtru RC, prostownika, multiwibratora czy wzmacniacza w układzie wspólnego emitera. Program jest przy tym rzeczywistym symulatorem, a nie animacją poglądową – liczy równania węzłowe, więc błędny układ zachowa się błędnie, tak jak na stole laboratoryjnym.

Do zastosowań profesjonalnych to za mało: nie ma analizy szumowej, modeli SPICE producentów ani projektowania płytki. Jako narzędzie do zrozumienia, dlaczego coś działa, sprawdza się jednak lepiej niż niejeden program na komputer, bo pętla „zmień wartość i patrz” trwa sekundę.

Producent: MuseMaze
Platformy: Android, iOS, przeglądarka
Cena: wersja bezpłatna z ograniczoną liczbą elementów, wersja płatna
Możliwości: 8,5/10
Łatwość obsługi: 9,5/10
Ocena ogólna: 9,0/10

WiFiman

Diagnostyka sieci bezprzewodowej i lokalnej

WiFiman pokazuje wszystkie widoczne sieci bezprzewodowe wraz z siłą sygnału, standardem, szerokością kanału i pasmem. Najbardziej przydatny jest wykres zajętości kanałów: widać na nim, które kanały są zatłoczone przez sąsiadów i gdzie warto przestawić własny router. Przy typowym problemie „internet zwalnia wieczorami” to zwykle pierwsza rzecz do sprawdzenia.

Druga część programu skanuje sieć lokalną i wypisuje wszystkie podłączone urządzenia z adresami i nazwami producentów. To dobry sposób, żeby sprawdzić, co właściwie jest podłączone do domowej sieci – i czy nie ma tam czegoś, czego nie rozpoznajemy. Jest też test przepustowości oraz pomiar opóźnień.

Program pochodzi od producenta sprzętu sieciowego i jest bezpłatny bez ograniczeń funkcjonalnych. Warto pamiętać o ograniczeniu systemowym: nowsze wersje Androida i iOS udostępniają aplikacjom mniej danych o sieciach niż dawniej, więc część informacji może być niedostępna zależnie od modelu telefonu.

Producent: Ubiquiti
Platformy: Android, iOS, komputer
Cena: bezpłatna
Możliwości: 9,0/10
Łatwość obsługi: 9,0/10
Ocena ogólna: 9,0/10

Scaniverse

Skaner trójwymiarowy z telefonu

Scaniverse buduje trójwymiarowy model przedmiotu lub pomieszczenia na podstawie zdjęć albo pomiaru dalmierzem laserowym, jeżeli telefon go ma. Obchodzi się wokół obiektu, program wyświetla na bieżąco, które fragmenty ma już pokryte, a przetwarzanie odbywa się na urządzeniu – bez wysyłania danych do chmury i bez czekania w kolejce. Wynik można obejrzeć, przyciąć, zmierzyć i wyeksportować w formatach przyjmowanych przez programy do modelowania i druku trójwymiarowego. Program obsługuje też metodę zwaną Gaussian Splats, dającą wyjątkowo realistyczny obraz sceny, choć trudniejszą do dalszej obróbki niż klasyczna siatka trójkątów. Jakość zależy przede wszystkim od oświetlenia i cierpliwości. Przedmioty błyszczące, przezroczyste i jednolicie gładkie wychodzą źle, bo algorytm nie ma czego dopasować. Podstawowe skanowanie na urządzeniu pozostaje bezpłatne; płatne plany dotyczą przetwarzania w chmurze i zastosowań komercyjnych. Głównym konkurentem jest Polycam, wygodniejszy, ale z wyraźnie kosztowniejszym abonamentem.

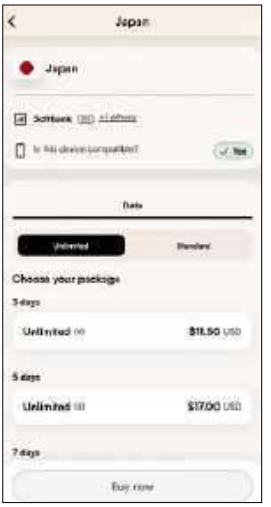
Producent: Niantic Spatial
Platformy: Android, iOS
Cena: bezpłatna w podstawowym zakresie; plany płatne dla funkcji chmurowych
Możliwości: 9,0/10
Łatwość obsługi: 8,5/10
Ocena ogólna: 8,5/10

Termux

Środowisko wiersza poleceń na Androidzie

Termux to emulator terminala z własnym menedżerem pakietów, dający dostęp do kilku tysięcy programów znanych z Linuksa. Nie wymaga odblokowania telefonu ani uprawnień administratora. Po instalacji dostajemy powłokę, a poleceniem pkg install dokładamy to, czego potrzebujemy: Pythona, git, ffmpeg, serwer SSH, edytory tekstu.
Dla czytelnika, który uczy się programować, to najtańsza droga do prawdziwego środowiska pracy: skrypt napisany w telefonie działa tak samo jak na komputerze. Zestaw dodatkowy Termux:API daje dostęp do czujników, aparatu, powiadomień i schowka, więc z poziomu skryptu można na przykład zapisać odczyt akcelerometru do pliku. Jedna rzecz wymaga wyjaśnienia, bo bywa źródłem kłopotów. Wersja publikowana w sklepie Google jest osobnym wydaniem, odbiegającym od głównego projektu; twórcy wskazują jako oficjalne źródła katalog F-Droid oraz repozytorium na GitHubie. Wersji z różnych źródeł nie da się aktualizować wzajemnie, bo mają inne podpisy cyfrowe – trzeba wybrać jedną i przy niej zostać.

Producent: projekt społecznościowy Termux
Platformy: Android
Cena: bezpłatna, otwarte źródła
Możliwości: 9,5/10
Łatwość obsługi: 6,5/10
Ocena ogólna: 8,5/10



Airalo

Pakiet danych na wyjazd bez wymiany karty

Airalo sprzedaje pakiety transmisji danych w postaci profili eSIM. Wybiera się kraj lub region, kupuje pakiet, a aplikacja instaluje profil w telefonie – bez kodu QR, bez wizyty w salonie i bez wyjmowania własnej karty. Numer krajowy pozostaje aktywny do połączeń i wiadomości, a dane idą przez profil zagraniczny.
Oferta obejmuje ponad dwieście krajów. Pakiety krajowe zaczynają się od kilku dolarów za jeden do dwóch gigabajtów, większe kosztują kilkanaście do kilkudziesięciu; od 2026 roku dostępne są też pakiety bez limitu danych. To zwykle wyraźnie taniej niż roaming poza Unią Europejską, gdzie polskie taryfy przestają działać na dotychczasowych zasadach.
Trzy zastrzeżenia. Po pierwsze, telefon musi obsługiwać eSIM i nie może być zablokowany na jednego operatora. Po drugie, większość pakietów nie daje lokalnego numeru, więc do potwierdzeń logowania nadal służy numer krajowy. Po trzecie, po przekroczeniu progu określonego w pakiecie prędkość bywa ograniczana. Aplikacja jest przy okazji najprostszym sposobem, żeby zobaczyć w praktyce mechanizm opisany w tym numerze w artykule o końcu karty SIM.

Producent: Airalo
Platformy: Android, iOS
Cena: aplikacja bezpłatna, pakiety danych płatne
Możliwości: 8,5/10
Łatwość obsługi: 9,0/10
Ocena ogólna: 8,5/10

Algorytm cię odrzucił. Wyjaśnienie dostaniesz za szesnaście miesięcy

Unia miała od 2 sierpnia wymagać, by maszyna oceniająca kandydata była sprawdzalna. Sześć dni wcześniej przesunęła ten termin.
2 sierpnia 2026 roku miał być dniem, w którym w Unii Europejskiej przestaje być obojętne, jak działa program odrzucający twoje podanie o pracę. Nie przestał. Rozporządzenie opublikowane 24 lipca przesunęło ten obowiązek na 2 grudnia 2027 roku. Szesnaście miesięcy różnicy, decyzja podjęta na sześć dni przed terminem, na który firmy przygotowywały się przez dwa lata.

Zacznijmy od tego, czego dotyczy spór, bo w doniesieniach prasowych ginie to pod skrótami. Unijne rozporządzenie o sztucznej inteligencji dzieli systemy na kategorie według ryzyka. Do kategorii wysokiego ryzyka trafiło wszystko, co ocenia ludzi w zatrudnieniu: programy przesiewające życiorysy, systemy punktujące kandydatów, narzędzia analizujące nagrania rozmów kwalifikacyjnych, oprogramowanie rozdzielające zadania i oceniające pracowników. Nie

ma progu wielkości firmy – dziesięcioosobowa agencja rekrutacyjna podlega tym samym zasadom co korporacja.

Obowiązki nie są symboliczne. Dostawca systemu musi prowadzić dokumentację techniczną, zarządzać ryzykiem i testować narzędzie pod kątem stronniczości. Pracodawca, który go używa, ma własny zestaw powinności: stosować system zgodnie z instrukcją, zapewnić rzeczywisty nadzór człowieka, poinformować kandydatów i przedstawicieli załogi, prowadzić rejestr decyzji. Zapisano wprost, że kupienie „zgodnego z przepisami" narzędzia nie zdejmuje z pracodawcy odpowiedzialności. Nadzór ma być prawdziwy – osoba z uprawnieniem do zmiany decyzji maszyny, nie ktoś, kto przystawia pieczątkę.

Dlaczego termin przesunięto

Powód podany oficjalnie jest techniczny i – trzeba to przyznać – niegłupi. Do wykazania zgodności potrzebne są zharmonizowane normy, czyli dokumenty opisujące, jak konkretnie zmierzyć stronniczość modelu albo udokumentować nadzór. Tych norm nie zdążono opracować. Firma, która chciałaby wykazać zgodność 2 sierpnia, nie miałaby według czego. Prawo wymagałoby czegoś, czego nie da się wykonać.

Chronologia jest jednak pouczająca. Komisja Europejska zgłosiła projekt zmian 19 listopada 2025 roku. Pierwsza runda negocjacji, 28 kwietnia 2026, zakończyła się bez porozumienia. Porozumienie polityczne osiągnięto 7 maja, Parlament zatwierdził je 16 czerwca, Rada 29 czerwca. Publikacja w dzienniku urzędowym – 24 lipca. Wejście w życie – 27 lipca. Sześć dni zapasu przy przepisie, którego data obowiązywania była znana od 2024 roku.

Nie wszystko zostało odsunięte, i to warto zapamiętać, bo w komentarzach zdarza się skrót „Unia odpuściła". Nieprawda. Zakazy wprowadzone w lutym 2025 roku obowiązują: nie wolno rozpoznawać emocji pracowników w miejscu pracy ani prowadzić państwowego oceniania obywateli. Od 2 sierpnia 2026 obowiązuje wymóg oznaczania treści generowanych przez maszynę i informowania człowieka, że rozmawia z systemem, a nie z człowiekiem. Od 2 grudnia 2026 dochodzą nowe zakazy, w tym dla programów generujących fałszywą nagość i materiały z udziałem dzieci. Kary też zostały bez zmian: do 35 milionów euro lub 7 procent światowego obrotu za praktyki zakazane.

Co ma z tego kandydat

Tu dochodzimy do sedna. Przesunięcie dotyczy obowiązków po stronie firm, nie praw po stronie człowieka – a te wynikają także z innego przepisu, o którym w tej dyskusji mówi się za mało. Artykuł 22 rozporządzenia o ochronie danych

Rysunek 1. Co obowiązuje, co dopiero wejdzie i co zostało przesunięte

osobowych, obowiązujący od 2018 roku, zakazuje podejmowania decyzji wywołujących istotne skutki wyłącznie w sposób zautomatyzowany, poza trzema wąskimi wyjątkami. Odrzucenie podania o pracę mieści się w tej definicji.

W praktyce oznacza to, że kandydat już dziś ma prawo żądać, by jego odrzucenie przejrzał człowiek. Problem polega na czym innym: żeby skorzystać z tego prawa, trzeba wiedzieć, że program w ogóle brał udział w decyzji. A obowiązek informowania kandydata o tym, że podlega systemowi wysokiego ryzyka, właśnie przesunięto o szesnaście miesięcy.

To jest ta luka, o której warto mówić głośno. Nie brak przepisów – one są. Brak informacji, bez której przepisy pozostają martwe. Człowiek, który dostaje wiadomość „dziękujemy za zainteresowanie, wybraliśmy innego kandydata", nie ma jak ustalić, czy odrzucił go rekruter, czy próg punktowy w programie.

Argument drugiej strony

Trzeba przyznać, że przeciwnicy szybkiego wdrożenia nie mówią rzeczy absurdalnych. Po pierwsze, przepis bez norm to zaproszenie do fikcji – firmy wypełniłyby dokumentację, jak umiały, urzędy nie miałyby czego sprawdzać, a wszyscy udawaliby zgodność. Po drugie, ciężar obowiązków rzeczywiście spada nieproporcjonalnie na małe firmy, bo dokumentacja i testy kosztują tyle samo niezależnie od skali. Po trzecie, część narzędzi zniknęłaby z europejskiego rynku, co też jest kosztem – dla kandydatów również, bo dobrze zaprojektowany algorytm bywa mniej stronniczy niż zmęczony rekruter przeglądający dwusetne życiorysy tego dnia.

Ten ostatni argument jest najmocniejszy i nie należy go lekceważyć. Badania nad rekrutacją pokazują wpływ nazwiska, zdjęcia, adresu i pory dnia na decyzje ludzi. Maszyna, którą da się przetestować, jest pod tym względem lepsza od człowieka, którego przetestować się nie da. Cała wartość przepisu polega jednak na słowie „da się" – a właśnie obowiązek umożliwiający sprawdzenie odsunięto.

Co z tego wynika

Mam do tej decyzji stosunek mieszany i nie zamierzam tego ukrywać. Rozumiem argument o brakujących normach. Nie rozumiem, dlaczego przez dwa lata ich nie przygotowano, skoro data była zapisana w ustawie. Rozumiem, że firmy potrzebują czasu. Nie rozumiem, dlaczego czas dostały wyłącznie one, a kandydat nie dostał nic – ani jednego dodatkowego uprawnienia, które obowiązywałoby w okresie przejściowym.

Rzecz jest poważniejsza niż jeden termin. Rozporządzenie o sztucznej inteligencji reklamowano jako pierwsze na świecie kompleksowe prawo w tej dziedzinie i jako dowód, że Europa potrafi uregulować technologię, zanim ta ureguluje ludzi. Pierwsza poważna próba tego prawa polegała na tym, że nie weszło ono w życie w terminie. Trudno o gorszy początek dla przepisu, którego cała siła miała polegać na tym, że jest wiążący.

Do 2 grudnia 2027 roku pozostaje więc stan, który warto nazwać po imieniu: program może ocenić człowieka, a człowiek nie musi się o tym dowiedzieć. Jeżeli szukasz w tym czasie pracy, masz jedno praktyczne uprawnienie – możesz zapytać pracodawcę wprost, czy w procesie rekrutacji użyto systemu zautomatyzowanego, i zażądać przeglądu decyzji przez człowieka. To prawo działa od 2018 roku i nikt go nie przesunął. Trzeba tylko wiedzieć, że się je ma. ■

De Coder

Trzy pytania, które warto zadać pracodawcy

1. Czy w ocenie mojego zgłoszenia brał udział system zautomatyzowany? Pytanie jest zgodne z prawem i pracodawca powinien na nie odpowiedzieć.
2. Jeżeli tak – czy decyzję o odrzuceniu przejrzał człowiek? Artykuł 22 rozporządzenia o ochronie danych daje prawo żądać takiego przeglądu.
3. Na jakich kryteriach opierała się ocena? Pełnego opisu działania modelu nikt nie ma obowiązku ujawniać, ale kryteriów oceny kandydata – tak.

Przyszłość rodzi się z wyobraźni. VI Kongres Futurologiczny już we wrześniu w Krakowie!

W dniach 11–13 września 2026 roku w Pałacu Potockich w Krakowie odbędzie się VI Kongres Futurologiczny – interdyscyplinarna konferencja, która od 2021 roku łączy środowiska nauki, kultury, technologii i sztuki, tworząc unikalną przestrzeń dialogu o nadchodzących przemianach cywilizacyjnych. Wydarzenie, inspirowane literackim oraz filozoficznym dziedzictwem Stanisława Lema, realizowane jest przez Polską Fundację Fantastyki Naukowej we współpracy z Krakowskim Biurem Festiwalowym oraz Wydawnictwem IX.

W programie tegorocznej edycji – tradycyjnie podzielonym na Blok Kultury i Blok Nauki – znajdą się debaty, panele dyskusyjne, wykłady, warsztaty oraz spotkania autorskie. Swój udział zapowiedzieli wybitni naukowcy reprezentujący m.in. Instytut Fizyki Jądrowej PAN, Akademię Górniczo-Hutniczą oraz Uniwersytet Jagielloński. Kongres zgromadzi również nagradzanych pisarzy science fiction, krytyków literackich, artystów wizualnych, ekspertów sektora kosmicznego i sztucznej inteligencji, a także delegatów Ministerstwa Obrony Narodowej oraz działaczy organizacji klimatycznych. Obecność tak szerokiego grona gości podkreśla interdyscyplinarny charakter wydarzenia, w ramach którego poruszone zostaną tematy eksploracji kosmosu, energetyki, cyberbezpieczeństwa, etyki technologicznej, prawa autorskiego w dobie AI oraz wpływu literatury na kształtowanie myślenia o przyszłości. Podczas konferencji ogłoszone zostaną także wyniki plebiscytu na 10 najważniejszych polskich książek science fiction, zorganizowanego z okazji 250-lecia narodzin polskiej fantastyki, które obchodzimy w tym roku.

Kongres niezmiennie promuje dialog między wyobraźnią a nauką, akcentując szczególną rolę naukowej fikcji spekulatywnej jako narzędzia do śledzenia oraz prognozowania przemian cywilizacyjnych. Szczególna uwaga poświęcona zostanie pracy z młodym pokoleniem – w części edukacyjnej przygotowano dedykowane zajęcia dla studentów i nauczycieli, koncentrujące się na popularyzacji nauk ścisłych i humanistycznych, nowoczesnych metodach nauczania oraz rozwijaniu kompetencji przyszłości.

Gospodarzem Kongresu Futurologicznego po raz kolejny będzie Kraków – Miasto Literatury UNESCO, z którym nierozerwalnie związane było życie i twórczość Stanisława Lema. Konferencja odbywa się pod honorowym patronatem Ministra Obrony Narodowej, Urzędu Komunikacji Elektronicznej, Centrum Badań Kosmicznych Polskiej Akademii Nauk oraz Polskiego Towarzystwa Informatycznego.

Udział w konferencji jest bezpłatny. Wstęp tylko dla osób pełnoletnich. Szczegółowy program znajduje się na stronie www.kongres.pffn.org.pl ■

Entropia

Mgławica była oszałamiająca. Wyglądała jak gigantyczny, zatrzymany w czasie wybuch fioletowego atramentu, przetykany świetlistymi żyłkami w odcieniach seledynu i miedzi. Adam opierał dłonie o chłodny metal barierki w pokoju widokowym i po prostu chłonął wspaniały obraz. Czuł błogi i rozleniwiający spokój. Fraktalne wzory gazu i pyłu pulsowały w próżni niemal niezauważalnie, a może to po prostu statek badawczy Entropia kontynuował swój nieprzerwany lot, powoli zmieniając perspektywę.

Lecieli z ogromną prędkością. Wiedział, że za kilka dni ten kosmiczny kalejdoskop zniknie za rufą, stając się jedynie kolejnym zapisanym terabajtem w dzienniku pokładowym. Na razie jednak mgławica wypełniała całe panoramiczne okno, całkowicie go hipnotyzując.

Wziął głęboki oddech. Powietrze z systemów recyrkulacji, mimo że pachniało sterylnością i chłodnym metalem, wydało mu się orzeźwiające. Sztuczna grawitacja, generowana przez powolny, miarowy obrót głównego pierścienia statku, ciążyła mu w nogach w znajomy, uspokajający sposób. Rozpoczął się piętnasty dzień jego samotnej warty. Równo połowa cyklu. Pozostała jedenastka załogi była w fazie kriosnu w komorach hibernacyjnych, powierzając mu swoje życie i bezpieczeństwo okrętu. Przez te dwa tygodnie izolacji zdążył polubić tę absolutną, zawieszoną w czasie ciszę, zakłócaną jedynie niskim mruczeniem reaktora.

– Dobra, koniec tego dobrego – mruknął do siebie. Jego własny głos zabrzmiał nieco obco w pustym pomieszczeniu.

Oderwał wzrok od pulsujących, fioletowych obłoków. Kiedy tylko odwrócił się plecami do szyby, poczuł w skroniach ledwie dostrzegalne ukłucie – jakby nagły spadek ciśnienia, ulotny cień znużenia. Zignorował to, zrzucając winę na samotność i monotonię. Czas było zacząć poranny obchód.

Wyprostował się i ruszył w stronę wyjścia. Automatyczne drzwi rozsunęły się z cichym sykiem, wpuszczając go do głównego korytarza. Światła jarzeniowe zapalały się sekwencyjnie nad jego głową w miarę, jak szedł łagodnie zakrzywionym pokładem pierścienia w stronę sekcji kriogenicznej. Piętnasty dzień zapowiadał się idealnie.

Korytarz głównego pierścienia wyginał się łagodnie ku górze, sprawiając wrażenie, jakby człowiek wiecznie wspinał się na niewidzialne wzniesienie. Taka była natura rotacyjnych statków kosmicznych – perspektywa zawsze urywała się zaledwie kilkadziesiąt metrów dalej, zablokowana przez stalową podłogę, która zaginała się ku górze i znikała za sufitem. Oświetlenie budziło się do życia z cichym, elektrycznym pstryknięciem dokładnie w chwili, gdy mijał kolejne czujniki ruchu, by po kilkunastu sekundach znów zgasnąć w ciemności za jego plecami. Entropia oszczędzała energię, gdzie tylko mogła.

Drzwi do sekcji kriogenicznej rozsunęły się gładko. Uderzyło go zimne, przefiltrowane powietrze, pachnące ozonem i medycznym polimerem. W półmroku obszernego pomieszczenia jarzyły się jedynie blade, błękitne diody modułów podtrzymywania życia. Jedenaście cylindrycznych kapsuł stało w idealnym, geometrycznym rzędzie.

Adam podszedł do pierwszej z brzegu, należącej do kapitan Lask. Jej twarz, widoczna zza warstwy oszronionego szkła syntetycznego, wydawała się woskowa, pozbawiona wyrazu i nienaturalnie spokojna. Przeszedł wzdłuż komór, muskając palcami główny panel diagnostyczny. Wyświetlacz

posłusznie wyrzucał kolumny zielonych danych. Temperatura w normie. Fale mózgowe uśpione. Zużycie ciekłego azotu na poziomie bazowym. Byli tu tylko oni – jedenastu zahibernowanych członków załogi i on, samotny strażnik. Z zadowoleniem wypowiedział standardową formułkę:

– Komputer, autoryzacja. Zapisz, że wszystkie odczyty prawidłowe.

Kiedy zakończył, znowu to poczuł. Tępy, narastający ból u podstawy czaszki, zupełnie jakby ktoś założył mu na głowę o numer za ciasny hełm próżniowy. Zacisnął zęby i mocno przetarł skronie.

– Za dużo filtrowanego powietrza, za mało słońca – mruknął pod nosem. Dźwięk jego głosu natychmiast utonął w jednostajnym szumie chłodziw. Zdecydował, że jak tylko skończy obchód, pójdzie do ambulatorium i weźmie coś mocniejszego z apteczki.

Opuścił sekcję hibernacyjną. Grodzie zatrzasnęły się z głuchym tąpnięciem, odcinając go od śpiącej załogi. Ruszył dalej łukiem głównego korytarza. Rytm jego własnych kroków dudnił o metalowe kratownice pokładu, przypominając mu o absolutnej izolacji. Następnym, standardowym punktem harmonogramu był mostek. Miał tylko zweryfikować odczyty nawigacyjne, zrobić kopię zapasową dziennika systemowego i wrócić do swojej kajuty.

Podchodząc do ciężkich, opancerzonych drzwi centrum dowodzenia, zwolnił kroku. Czujniki zareagowały na jego obecność, a zamki puściły z głośnym szczęknięciem. Skrzydła drzwi rozsunęły się na boki.

Wzdrygnął się i zamarł w progu. Zmarszczył brwi, a resztki sennej rutyny wyparowały z niego w ułamku sekundy. Coś było nie tak.

Mostek tonął w świetle. Zamiast standardowego, przyćmionego oświetlenia awaryjnego, główne konsole nawigacyjne i panele taktyczne jarzyły się pełną mocą. Ekrany rzucały na ściany ostre, błękitne i pomarańczowe refleksy, a w chłodnym powietrzu unosił się wyższy niż zazwyczaj, elektryczny szum procesorów pracujących na podwyższonych obrotach.

Stał w progu i czuł, jak żołądek zaciska mu się w lodowaty supeł. Zgodnie z żelaznymi protokołami Entropii, centrum dowodzenia przechodziło w stan całkowitego uśpienia dokładnie godzinę po wylogowaniu ostatniego użytkownika. Wiedział z absolutną, niepodważalną pewnością, że nie było go tutaj od wczorajszego obchodu.

Serce zabiło mu mocniej, uderzając o żebra z głuchym łomotem. Pasażer na gapę? Awaria systemu kriogenicznego, która kogoś wybudziła? Nie, to niemożliwe. Przecież zaledwie pięć minut temu osobiście sprawdził sekcję hibernacyjną. Widział twarze wszystkich członków załogi. Widział odczyty. Wszyscy spali. Nikt nie opuścił kapsuły.

Zrobił ostrożny krok w przód. Grodzie zamknęły się za nim, odcinając go od korytarza. Ból u podstawy czaszki nagle przybrał na sile, pulsując jakby w reakcji na ostre światło monitorów. Zignorował go, kierowany wyrzutem adrenaliny. Podszedł do stanowiska dowodzenia. Ktoś przed chwilą tu był. Ktoś przeglądał zapisy z kamer bezpieczeństwa – otwarta aplikacja wciąż wisiała na wirtualnym pulpicie.

Opadł na fotel, a jego palce instynktownie zawisły nad klawiaturą.

– Komputer, autoryzacja – rzucił w przestrzeń. – Pokaż zapis z kamer bezpieczeństwa na mostku. Odfiltruj pusty obraz.

Główny ekran zamigotał. Pojawiła się oś czasu i po chwili umieszczony na niej znacznik zatrzymał się na „T -00:30:17". Zaledwie trzydzieści minut temu system odnotował ruch. Wstrzymał oddech i kliknął ikonę odtwarzania. Spodziewał się zobaczyć obcą sylwetkę, intruza przemykającego w cieniach, a w najgorszym razie zdezorientowanego członka załogi, obudzonego przez usterkę komputera pokładowego.

Zamiast tego zobaczył, jak ciężkie, opancerzone drzwi na nagraniu rozsuwają się. W progu stanął mężczyzna w szarym kombinezonie technicznym Entropii. Miał ciemne, zmierzwione włosy i lekki zarost.

Poczuł, jak krew odpływa mu z twarzy. Zrobiło mu się słabo.

To był on sam.

Z niedowierzaniem patrzył, jak „on" z nagrania wzdryga się i zastyga w progu – dokładnie tak samo, jak zrobił to przed chwilą. Jak z wyrazem absolutnego szoku i zagubienia na twarzy powoli podchodzi do głównej konsoli. Jak opada na ten sam fotel, w którym właśnie siedział, i wypowiada komendę wywołania zapisów kamer bezpieczeństwa.

Kliknął pauzę. Z ekranu patrzyła na niego jego własna twarz, zniekształcona grymasem i oświetlona blaskiem wyświetlacza. Twarz człowieka całkowicie zszokowanego tym, co właśnie odkrył. Zimny pot spłynął mu po karku.

– Komputer, śledź obiekt na wszystkich kamerach – wykrztusił. Głos łamał mu się w gardle. – Przyspiesz odtwarzanie.

Śledził samego siebie z fascynacją graniczącą z obłędem. Widział, jak jego odpowiednik zrywa się z fotela, w którym on sam właśnie siedział, i wybiega z mostka. Kamera w głównym korytarzu uchwyciła go, gdy szybkim, nerwowym krokiem przemierzał zakrzywiony pokład, aż w końcu zniknął za drzwiami laboratorium naukowego.

Po kilku minutach czasu rzeczywistego postać na ekranie opuściła laboratorium. Jednak coś się zmieniło. Tamten Adam nie biegł. Szedł wolniej, chwiejnie. Wyglądał jak człowiek wybudzony z głębokiego, nienaturalnego snu, zataczając się lekko w stronę zewnętrznej ściany pierścienia.

Kolejna kamera. Pokój widokowy. Nagranie ukazywało, jak mężczyzna wchodzi do środka, podchodzi do panoramicznej szyby i zastyga. Stoi tak przez kilkanaście minut, niemal w bezruchu, po prostu wpatrując się w pulsującą mgławicę. A potem... odwraca się. Przeciąga się leniwie i spokojnym krokiem rusza do sekcji hibernacyjnej, sprawdza kapsuły z załogą i kieruje się prosto na mostek.

Zimny dreszcz przebiegł mu wzdłuż kręgosłupa. – Przecież ja to właśnie przed chwilą zrobiłem – pomyślał z czystym, wręcz zwierzęcym przerażeniem. – Podziwiałem mgławicę. Poszedłem do komór. Przyszedłem tutaj.

Jego mózg pracował na najwyższych obrotach, próbując znaleźć jakiekolwiek logiczne wytłumaczenie. Zespół stresu izolacyjnego? Mikroudar?

Ból głowy, który do tej pory był zaledwie irytującym uciskiem, uderzył nagle ze zdwojoną siłą. Wbił się w jego czaszkę niczym rozgrzany pręt, zaburzając ostrość widzenia. Zasyczał przez zaciśnięte zęby.

Z trudem podniósł się z fotela. Nogi miał jak z ołowiu, a błędnik zdawał się wariować od obrotowego ruchu statku. Wybiegł z mostka, kierując się łukiem korytarza w stronę laboratoriów.

Laboratorium znajdowało się na końcu kolejnego segmentu pierścienia. Automatyczne drzwi rozsunęły się, a Adam wpadł do środka, opierając się ciężko o futrynę. Ból głowy pulsował w rytm uderzeń serca, spłycając mu oddech.

Podobnie jak na mostku, główne konsole analityczne jarzyły się zimnym światłem. Podszedł do centralnego terminala badawczego. Na monitorach widniały zamrożone wykresy ze spektrometru zewnętrznego. Ktoś – on sam w jakiejś zapomnianej przeszłości – analizował tu widmo emisyjne mgławicy.

Pochylił się nad blatem, mrużąc oczy, by wyostrzyć rozmazujący się z bólu obraz. Skupił wzrok na podświetlonych na czerwono anomaliach. Mgławica za burtą nie była zwykłym obłokiem zjonizowanego gazu i pyłu. Pomiary wskazywały potężne, ukierunkowane promieniowanie. To nie była jedna, stała fala. Wykresy szalały, rejestrując nieustanne zmiany fazy i dynamiczną modulację częstotliwości.

Wywołał raport osłon. System meldował 100% skuteczności przeciwko promieniowaniu kosmicznemu. A jednak czerwone wskaźniki na ekranie medycznym nie kłamały – promieniowanie z mgławicy było tak chaotyczne, że dosłownie prześlizgiwało się poprzez skomplikowaną konstrukcję osłon Entropii.

Jego wzrok padł na okno symulacji medycznej otwarte w prawym rogu ekranu. Wykres fal z mgławicy nakładał się tam na model ludzkiego mózgu. Zmienność częstotliwości idealnie rezonowała z falami w płacie czołowym i hipokampie.

Wszystko złożyło się w jedną, przerażającą całość. Mgławica dosłownie wypalała mu wspomnienia. Promieniowanie kumulowało się w jego organizmie, a gdy osiągało punkt krytyczny, kasowało kilka ostatnich godzin, wywołując przy tym euforyczne, hipnotyczne otępienie. Resetowało jego świadomość do momentu, w którym czuł się spokojny i bezpieczny. Krążył po statku od kilku lub kilkunastu godzin.

Musiał natychmiast działać. Nie zdąży napisać programu przestrajającego osłony. Nie ma szans. Czuł, że jego umysł już zaczyna się wyłączać, a myśli rwą się i blakną. Było tylko jedno wyjście: przeczekać to. Uśpić się na kilkadziesiąt godzin, żeby nie umrzeć z wyczerpania, błąkając się w kółko po statku. Sen... Przecież sen zmienia częstotliwość fal mózgowych! Ta myśl uderzyła go jak nagłe

olśnienie. Jeśli jego mózg zwolni, zniknie rezonans. Promieniowanie straci punkt zaczepienia. To była jego jedyna szansa.

Plan był prosty. Musiał dobiec do ambulatorium, napisać na ścianie grubymi literami wiadomość: „Jesteśmy w strefie radiacji. Wstrzyknij sobie kolejną dawkę i śpij dalej", a potem podać sobie potężny środek nasenny.

Oderwał się od konsoli. Zebrał resztki sił i wybiegł z laboratorium, kierując się łukiem korytarza w stronę pokładowego szpitala.

I wtedy świat zawirował.

Ból w skroniach przestał być uciskiem, a stał się ogłuszającym, białym szumem. Jęknął, zataczając się na ścianę. Spróbował chwycić się metalowej poręczy, ale palce odmówiły mu posłuszeństwa. Obraz przed oczami zaczął drżeć, a myśli – jeszcze przed ułamkiem sekundy ostre i logiczne – zaczęły tonąć w gęstej, nieprzeniknionej mgle.

Zwolnił krok. Potknął się o własne nogi.

Co ja miałem... Ambulatorium. Strzykawka. Muszę... zostawić wiadomość...

Spróbował utrzymać tę myśl, powtórzyć ją jak mantrę, ale napotkał tylko pustkę. Słowa uciekały, tracąc swoje znaczenie. Zdezorientowany, zatrzymał się na środku korytarza. Ciężko dyszał. Czego on tu właściwie szukał? Gdzie biegł?

Przerażenie powoli, acz nieubłaganie ustępowało miejsca łagodnemu, obezwładniającemu otępieniu. Nogi stały się dziwnie lekkie. Instynktownie ruszył przed siebie, wzdłuż zakrzywionego pokładu. Szukał światła. Szukał spokoju.

Drzwi przed nim rozsunęły się z cichym sykiem.

Adam wszedł do pokoju widokowego. Gdy tylko jego oczy napotkały pulsującą, fioletową mgławicę, resztki bólu głowy zniknęły jak ręką odjął. Jego myśli stały się czyste, pozbawione trosk. Z uśmiechem podszedł do szyby i oparł dłonie o chłodny metal barierki.

Patrzył na fraktalne, przepiękne wzory kosmicznego pyłu, chłonąc wspaniały obraz. Czuł błogi i rozleniwiający spokój. Wziął głęboki oddech przyjemnie orzeźwiającego powietrza.

Rozpoczął się piętnasty dzień jego samotnej warty. Zapowiadał się idealnie. ■

Tomasz Nowak

Przemijanie cywilizacji

Refleksje nad cyklem „Helikonia” Briana W. Aldissa

Cykl „Helikonia” Briana W. Aldissa to jedno z najbardziej bezkompromisowych i zarazem najsubtelniej skonstruowanych przedsięwzięć w całej literaturze science fiction. Trzytomowa epopeja – *Wiosna Helikonii*, *Lato Helikonii* i *Zima Helikonii* – nie opowiada o losach jednostek ani nawet o losach narodów, lecz o ewolucji całego świata w reżimie astronomicznych prawideł. Helikonia jest planetą, której historia rozgrywa się w rytmie wyznaczanym przez orbitalny taniec dwóch słońc. Aldiss nie tyle kreuje kolejną egzotyczną scenerię, ile przeprowadza kompletny eksperyment myślowy, w którym biologia, kultura, religia i polityka okazują się wtórnymi funkcjami astrofizycznej maszynerii. W centrum tego eksperymentu tkwi pytanie, jak kształtują się losy cywilizacji nie w skali pokoleń, lecz w skali globalnych zmian klimatycznych.

Sercem konstrukcyjnym powieści jest układ podwójny, w którym planeta krąży wokół gwiazdy nazwanej Bataliksą, przypominającej nasze Słońce, a ta z kolei obiega po wydatnie ekscentrycznej orbicie jasnego superolbrzyma Freyra. Właśnie ta podwójna astronomia narzuca helikońską miarę czasu: Wielki Rok, cykl trwający około 2592 ziemskich lat, w trakcie którego planeta przechodzi od skwarnego lata, gdy Freyr dominuje nad niebem niczym milczący,

niebieskawy bóg, do wielowiekowej, surowej zimy, gdy Bataliksa niemal samotnie pełza nisko nad horyzontem. Ponieważ Bataliksa porusza się po elipsie, dawka energii docierająca do atmosfery zmienia się nie o procenty, lecz o rzędy wielkości, a wraz z nią zmianom ulega cała ekologia. W efekcie na kartach powieści science fiction, otrzymujemy konsekwentnie egzekwowaną spekulację astrofizyczną. Aldiss, konsultując się z astronomami, stworzył model, który do dziś pozostaje jednym z najściślej pomyślanych planetarnych laboratoriów w fantastyce. W przeciwieństwie do łagodnego kołysania ziemskich zlodowaceń wywołanych cyklami Milankovicia, na Helikonii różnica między latem a zimą Wielkiego Roku jest cywilizacyjną gilotyną. Całe gatunki oraz formacje kulturowe mają swój początek i koniec w dyktacie orbity Freyra. To właśnie ów astrofizyczny mechanizm czyni z planety nie tło, lecz prawdziwego protagonistę, a historia helikońskich cywilizacji okazuje się odmianą astronomicznego determinizmu, wobec którego nawet dialektyka dziejów jest jedynie powierzchniowym efektem.

Na tym chłodnym, fizycznym fundamencie Aldiss nadbudowuje śmiałą tezę o konwergencji ewolucyjnej. Ludzie Helikonii nie są potomkami ziemskich kolonistów – wyewoluowali niezależnie, w odpowiedzi na te same ciśnienia selekcyjne, które na Ziemi uformowały *Homo sapiens*. Tym samym „człowieczeństwo" przestaje być przywilejem jednej planety, a staje się potencjalnym wzorcem adaptacyjnym, który Wszechświat może realizować wielokrotnie, niczym motyw w muzyce ewolucji. Antagonistami, a także biologicznym kontrapunktem, są fagory, istoty o anatomii minotaurów, przystosowane do permanentnego chłodu. Ich inteligencja jest odmienna, ich czas panowania przypada na epoki lodowcowe, gdy ludzie cofają się do roli przetrzebionej, trwożliwej populacji. Aldiss z precyzją literackiego architekta pokazuje, że nie ma tu trwałej hierarchii gatunków. Sinusoida klimatu rysuje sinusoidę dominacji. Każdy rozumny gatunek jest więc tylko tymczasowym beneficjentem termicznego optimum. Efektem staje się model, który wykracza poza doraźną publicystykę będąc ewolucyjnym realizmem, w którym moralność i polityka są funkcjami gradientu temperatury.

Z tego astronomiczno-biologicznego podglebia wyrastają cywilizacje, które Aldiss opisuje z iście antropologiczną drobiazgowością. W długich zimach zamykają się w sztywnych hierarchiach, religiach surowego ocalenia i hermetycznych strukturach rodowych; w epokach gorąca otwierają na handel, naukę, sztukę i synkretyzm. Każde nowe kulturowe otwarcie jest jednak budowane na ruinach poprzedniego, z resztek mitów, które powoli dryfują w stronę baśni. Ta *cywilizacyjna amnezja* jest szczególnie przejmującą koncepcją cyklu. Działa jak epigenetyczny mechanizm dziedziczenia. W opowieściach i rytuałach kodowane są szczątkowe instrukcje przetrwania, nawet jeśli ich literalny sens dawno wyparował. Kultura staje się zatem biologicznie użyteczną fikcją, zaś Aldiss zdaje się sugerować, że każda pamięć zbiorowa, także nasza, to nie archiwum prawdy, lecz adaptacyjny nawyk.

W tym zimnym laboratorium jedynym ogniwem łączącym planetę z gatunkiem *Homo sapiens* jest stacja Avernus, orbitująca nad Helikonią. Jej załoga, prawdziwi Ziemianie, obserwuje przez tysiąclecia zmagania planety niczym pasażerowie zamkniętego akwarium. Ich transmisje są po trosze dokumentacją naukową, po trosze kosmicznym reality show. I tu Aldiss wpisuje gorzką nutę autorefleksji: stacja dysponuje technologią zdolną do interwencji, lecz decyduje się na wieczną bierność, aż jej misja wyjaławia się w izolacji. Avernus staje się metaforą postawy współczesnej cywilizacji zdolnej do spektakularnego poznania, ale odciętej od odpowiedzialności, która z tego poznania powinna wynikać. Obserwator, który nigdy nie przekracza granicy uczestnictwa, ostatecznie traci sens własnej egzystencji. To chyba najmocniejszy, bo najciszej podany, komentarz etyczny powieści.

Filozoficznie cykl Helikonii zbliża się do kosmicznego pesymizmu, ale nie przechodzi w nihilizm. Przyroda jest bezosobowa, ślepa na kategorie dobra i zła, a jednak ludzie i fagory podejmują nieustający wysiłek odbudowy i transmisji doświadczenia. Nawet jeśli każda cywilizacja prędzej czy później zostanie starta przez nieubłagany postęp orbitalnego mechanizmu, sam gest przekazywania wiedzy – choćby w zdegradowanej, mitycznej formie – nadaje istnieniu swoistą godność. Jawi się jako heroizm bez nagrody, heroizm czystej adaptacji. W tym ujęciu postęp przestaje być liniowym marszem ku oświeceniu, a staje się oscylacją wokół punktu, który nigdy nie zostaje osiągnięty. Podobne tony pobrzmiewają u Olafa Stapledona, który

w *Ostatnich i pierwszych ludziach* kreślił miliardy lat historii, ale w chłodny, niemal abstrakcyjny sposób. Aldiss dodaje do tego biologię, klimatologię i żelazny konkret codziennego życia. W porównaniu z *Diuną* Herberta, gdzie ekologia Arrakis sprzęga się z polityką i religią, Helikonia idzie o krok dalej: tu polityka i religia są nie tyle sprzężone z ekologią, ile są same ekologią wyrażoną w języku symboli.

Narracyjnie Aldiss podejmuje odważną decyzję: żaden pojedynczy bohater nie spina trzech tomów osią swej własnej egzystencji. Powieść stanowi monumentalną kronikę, ale nie antropocentryczną, lecz planeto-centryczną. To posunięcie rzadkie w science fiction, które z reguły kotwiczy sens w indywidualnym losie. Tutaj bowiem Helikonia, ze swoim nieubłaganym rytmem Wielkiego Roku, jest właściwą protagonistką, a ludzie i fagory są jej chwilowymi symbolami. Struktura powieści podąża za tą logiką, gdyż kolejne tomy nie kontynuują indywidualnych narracji, lecz prezentują następne fazy tego samego planetarnego oddechu. Czytelnik zaś stopniowo uczy się myśleć w kategoriach geologicznych i ewolucyjnych, a nie biograficznych.

W ostatecznym rozrachunku cykl Aldissa jest czymś więcej niż monumentalną space operą, stanowiąc w rzeczywistości traktat o biologiczno-astrofizycznej kołysce, która decyduje o tym, co w ogóle może zaistnieć jako kultura. Autor rozciąga pojęcie ewolucji daleko poza biologię, stosując je do religii, nauki i struktur społecznych, oraz konsekwentnie wskazuje, że każde osiągnięcie umysłu jest formą adaptacji do zmieniającego się termodynamicznego budżetu planety. Dziś, w epoce antropocenu i świadomości planetarnych granic, Helikonia przestaje być jedynie egzotyczną fikcją, a staje się gorzkim memento. Nasze miasta i imperia również są zaledwie chwilowym zapisem w rytmie kosmicznych cyklów, a każda próba dominacji nad naturą jest aktem krótkowzrocznej pychy. Aldiss nie odbiera nadziei, ale umieszcza ją tam, gdzie jej prawdziwe miejsce – nie w triumfalnych wizjach wiecznego postępu, lecz w zdolności do dostrojenia się do rytmów znacznie od nas potężniejszych. Bo historia, biologia i astrofizyka są ostatecznie trzema językami opowiadającymi tę samą historię – historię chwilowego, kruchego istnienia rozumnych gatunków. ■

Łukasz Marek Fiema

Wieża radiowa w Berlinie

3 września poświęcono w Berlinie nową wieżę radiową o wysokości 146,7 metra, wzniesioną na terenach wystawowych przy okazji trzeciej Wielkiej Niemieckiej Wystawy Radiowej. Konstrukcja jest stalowa, kratowa i z daleka przypomina wieżę paryską. Służy jednocześnie celom nadawczym i wystawienniczym: zwiedzającym udostępniono platformę widokową oraz restaurację umieszczoną kilkadziesiąt metrów nad ziemią. Wieża jest widomym znakiem tempa, w jakim radiofonia zdobywa sobie miejsce wśród urządzeń użyteczności publicznej.

Najdłuższy tunel kolejowy świata

13 września otwarto dla ruchu przedłużenie linii Northern kolei podziemnej w Londynie, prowadzące od stacji Morden do East Finchley. Łączna długość przebiegu pod ziemią wynosi 27,841 kilometra, co czyni go najdłuższym tunelem kolejowym na świecie. Roboty prowadzono metodą tarczową w gruntach ilastych, a obudowę stanowią pierścienie żeliwne. Pierwsze pociągi jechały w ścisku, publiczność bowiem tłumnie stawiła się, żeby odbyć przejazd najdłuższym tunelem.

Edison: radio to przedsięwzięcie chybione

Thomas Edison oświadczył 22 września, że radiofonia zawiodła jako interes handlowy. Jego zdaniem zainteresowanie odbiornikami stanowi zaledwie ułamek tego, co obserwowano rok wcześniej, aparat jest zbyt zawiły dla ludzi, którzy nie mają o nim pojęcia, a sprzedawcy nic na nim nie zarobili. Publiczność, twierdzi wynalazca, wraca do fonografu, bo chce dobrej muzyki. Warto pamiętać, że mówi to konstruktor fonografu z 1877 roku, którego sprzedaż wyraźnie spadła, odkąd upowszechniły się odbiorniki radiowe. Sąd wypowiedziany w miesiącu, w którym Berlin poświęcił wieżę radiową, a Finlandia uruchomiła stałe nadawanie, wypada uznać za przedwczesny.

Radiofonia w Finlandii

9 września rozpoczęła regularne nadawanie fińska rozgłośnia Yleisradio w Helsinkach. Pierwszy program obejmował wiadomości, odczytane przez spikera Alexisa af Enehjelma. Finlandia dołącza tym samym do grona państw, które w ciągu ostatnich trzech lat uruchomiły stałą służbę radiofoniczną.

Zmarł Léon Thévenin

21 września zmarł w wieku pięćdziesięciu dziewięciu lat Léon Charles Thévenin, inżynier telegrafii francuskiej. Ogłoszone przez niego w 1883 roku twierdzenie pozwala zastąpić dowolnie zawiłą sieć źródeł i oporów jednym źródłem zastępczym, o odpowiednio dobranej sile elektromotorycznej i oporze wewnętrznym. Reguła ta, przyjęta początkowo z niedowierzaniem, weszła na stałe do praktyki obliczeniowej i oszczędza dziś rachmistrzom niezliczonych godzin mozołu.

Katastrofa przy próbie lotu przez Atlantyk

21 września na lotnisku Roosevelt Field pod Nowym Jorkiem uległ zniszczeniu trójsilnikowy samolot Sikorsky S-35, przygotowany przez kapitana René Foncka do lotu bez lądowania do Paryża. Podczas rozbiegu, przy pełnym obciążeniu paliwem i czteroosobowej załodze, załamało się pomocnicze podwozie. Maszyna wypadła poza koniec pasa i stanęła w płomieniach. Kapitan Fonck i porucznik Curtin zdołali wyskoczyć, natomiast radiotelegrafista i mechanik, zamknięci w kabinie, ponieśli śmierć. Nagroda Orteiga, wyznaczona za pierwszy lot bez lądowania między Nowym Jorkiem a Paryżem, pozostaje nieodebrana.

Porozumienie stalowe weszło w życie

30 września weszło w życie międzynarodowe porozumienie stalowe, ustanawiające jednolite ceny wyrobów hutniczych między wytwórcami z Niemiec, Francji i Wielkiej Brytanii. Rzecz ma znaczenie nie tylko handlowe. Wspólna cena oznacza podział rynków, a więc pośrednio także podział zamówień na urządzenia hutnicze, walcownie i koksownie, o które ubiegają się biura konstrukcyjne całej Europy. Kraje pozostające poza porozumieniem, a do nich należy Polska, staną wobec konkurentów działających w uzgodnieniu. Skutki tego układu dla naszego hutnictwa warto śledzić uważnie.

Ratunek czterdziestu trzech górników

W kopalni rudy żelaza towarzystwa Pabst w Ironwood w stanie Michigan runął szyb, odcinając od świata czterdziestu trzech ludzi. Trzej elektromonterzy, którzy znajdowali się w klatce, ponieśli śmierć na miejscu. Uwięzieni przebywali na głębokości 727 stóp, to jest przeszło dwustu dwudziestu metrów. Prace ratunkowe prowadzono bez przerwy przez pięć dób i zakończyły się wydobyciem wszystkich żywych po stu dwudziestu dziewięciu godzinach. Wypadek raz jeszcze dowodzi, jak wielkie znaczenie ma utrzymanie drugiego, niezależnego wyjścia z wyrobiska. ■

Chemiczne bliźniaki (2)

O podobieństwach pierwiastków przedstawionych w ubiegłym miesiącu wspomina się nawet w szkole. W drugim odcinku artykułu poznasz te, o których wiedzą tylko chemicy interesujący się tymi zagadnieniami. Przed Tobą kolejne chemiczne bliźniaki, oczywiście wraz z porcją eksperymentów.

Krótka forma układu okresowego ujawnia...

...kolejne pierwiastkowe pokrewieństwa. Były one dobrze znane XIX-wiecznym chemikom, ale w kolejnym stuleciu, wraz z rozpowszechnieniem się długiej postaci tablicy Mendelejewa (z grupami oznaczonymi od 1 do 18), poszły w zapomnienie. Grupy krótkiej formy tablicy układu okresowego (oznaczone liczbami rzymskimi od I do VIII) łączą ze sobą grupy formy długiej: 1 z 11, 2 z 12, itd. Wyjątkowo grupa VIII składa się aż z czterech rodzin: 8, 9, 10 i 18. Choć postać ta jest mniej przejrzysta niż forma długa, pozwala dostrzec znacznie więcej pokrewieństw między pierwiastkami. W naturalny sposób widoczne jest w niej chociażby podobieństwo diagonalne z poprzedniego odcinka (**1**).

Przygotuj roztwory rozpuszczalnych soli ołowiu (azotan $Pb(NO_3)_2$ lub octan $(CH_3COO)_2Pb$) oraz baru (chlorek $BaCl_2$ lub azotan $Ba(NO_3)_2$). **Zachowaj ostrożność podczas doświadczeń z tymi związkami, ponieważ są one toksyczne: noś ochronne rękawice, nie jedz i nie pij podczas pracy.** Potrzebne będą także roztwory chromianu potasu K_2CrO_4 (też jest toksyczny) i rozpuszczalnego siarczanu, np. Na_2SO_4 (**2**). Przeprowadź reakcje soli ołowiu z chromianem i siarczanem oraz te same próby z solą baru. Reakcje wykonaj w probówkach lub na płytce porcelanowej z wgłębieniami (wymagają dosłownie kropli odczynników). Gdy nie masz takiej płytki, zastąpi ją blister po tabletkach lub folia, na której zmieszasz krople roztworów. W każdym z przypadków powstają osady: białej barwy $PbSO_4$ i $BaSO_4$ oraz żółty $PbCrO_4$ i jasnożółty $BaCrO_4$ (**3**). Zachowanie obu anionów i wzory tworzonych przez nie soli są analogiczne; można jeszcze dodać, że wszystkie one były (sole ołowiu) lub nadal

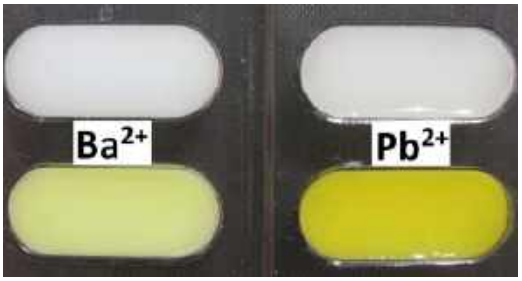
	I A	I B	II A	II B	III B	III A	IV B	IV A	V B	V A	VI B	VI A	VII B	VII A	VIIIB			VIIIA
1	H																	He
2	Li		Be		B		C		N		O		F					Ne
3	Na		Mg		Al		Si		P		Si		Cl					Ar
4	K		Ca		Sc		Ti		V		Cr		Mn		Fe	Co	Ni	
		Cu		Zn		Ga		Ge		As		Se		Br				Kr
5	Rb		Sr		Y		Zr		Nb		Mo		Tc		Ru	Rh	Pd	
		Ag		Cd		In		Sn		Sb		Te		I				Xe
6	Cs		Ba		La		Hf		Ta		W		Re		Os	Ir	Pt	
		Au		Hg		Tl		Pb		Bi		Po		At				Rn
7	Fr		Ra		Ac		Rf		Db		Sg		Bh		Hs	Mt	Ds	
		Rg		Cn		Nh		Fl		Mc		Lv		Ts				Og

1. Krótka forma tablicy układu okresowego wyraźnie pokazuje pokrewieństwo pomiędzy pierwiastkami grup głównych i pobocznych

2. Odczynniki do twojego doświadczenia: azotany ołowiu i baru oraz chromian potasu

są (sole baru) używane jako pigmenty. Pokrewieństwo chromu i siarki nie jest przypadkowe – pierwiastki te leżą w grupach 6 i 16 układu okresowego, co oznacza, że w formie krótkiej znajdują się razem w grupie VI. Molibden i wolfram, pozostałe pierwiastki z grupy 6, również wykazują podobieństwo do siarki: znane są molibdenian $BaMoO_4$ i wolframian baru $BaWO_4$. Wszystkie te metale tworzą również sole o bardziej złożonej strukturze, np. często używany w laboratoriach dichromian potasu $K_2Cr_2O_7$. A siarka? Grono tworzonych przez nią kwasów i soli także jest liczne, przykładem jest pirosiarczan potasu $K_2S_2O_7$, analog dichromianu.

A co z innymi grupami? Wanadowce tworzą sole kwasów podobnych do wywodzących się z fosforu (H_3PO_4, HPO_3), np. wanadany Na_3VO_4 lub NH_4VO_3. W grupie VII (7 i 17 w formie długiej) analogia jest jeszcze wyraźniejsza. Dwa popularne związki potasu – nadmanganian $KMnO_4$ i nadchloran $KClO_4$ – tak się do siebie upodobniły, że powstają nawet kryształy mieszane w dowolnych proporcjach. Oba związki są utleniaczami i oba stosunkowo słabo rozpuszczają się w wodzie (jak na sole potasu). W innych grupach również można dostrzec podobieństwo: skandowce (grupa 3) zbliżają się właściwościami do glinu, a tytanowce (grupa 4) do cyny. Cynk i kadm (grupa 12) to pierwiastki reagujące podobnie do magnezu (z tym że ten ostatni nie jest amfoteryczny). Nawet gazy szlachetne mają coś wspólnego z grupą 8 – maksymalna wartościowość ksenonu w otrzymanych związkach wynosi VIII, tak jak osmu czy rutenu. Jedynie grupa 11 (miedź, srebro i złoto) nie wykazuje podobieństw do litowców z grupy 1. Cóż, widocznie metale szlachetne chcą zachować swoją odrębność.



3. Barwy osadów soli baru i ołowiu: u góry siarczanów, u dołu chromianów

Wartościowość mniejsza o dwa

Wykonane doświadczenie dowiodło podobieństwa chromianów i siarczanów, a co za tym idzie, także chromu i siarki, czyli pierwiastków grup 6 i 16. Jednak eksperyment jest również potwierdzeniem podobieństwa reakcji jonów baru i ołowiu (grupy 2 i 14). Podczas analizy chemicznej kationów ołów często jest wykrywany wraz z wapniem, strontem i barem na podstawie tworzenia trudno rozpuszczalnych siarczanów.

Za takie zachowanie szarego metalu odpowiada... teoria względności. Zaskakujące, prawda? Elektrony w ciężkich atomach osiągają prędkości zbliżające się do prędkości światła, to zaś pociąga za sobą występowanie efektów relatywistycznych. Odpowiadają one m.in. za barwę złota i ciekły stan skupienia rtęci. W przypadku ołowiu, który, jako pierwiastek grupy 14, powinien być IV-wartościowy, efekty relatywistyczne powodują, że najwyższy stopień utlenienia jest nietrwały i w konsekwencji ołów jest przeważnie II-wartościowy. Stąd też jego reakcje są podobne

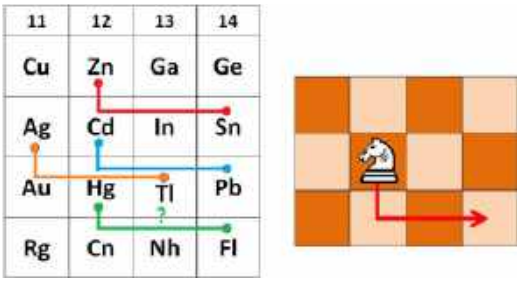
do obserwowanych dla pierwiastków grupy 2. Zauważ, że w krótkiej formie układu okresowego jest to „cofnięcie" się o dwie kolumny.

Podobnie zachowuje się leżący obok ołowiu tal (grupa 13) z najtrwalszą wartościowością wynoszącą I, bizmut (grupa 15) tworzący trwałe związki na III stopniu utlenienia oraz zwykle IV-wartościowy polon z grupy 16. Tal upodabnia się do litowców, a zwłaszcza potasu (np. tworzy mocną zasadę) oraz srebra, z którym jest razem wykrywany podczas analizy kationów (oba tworzą trudno rozpuszczalne chlorki rozkładające się pod wpływem światła) (**4**). Zauważ, że w krótkiej formie tablicy litowce i srebro znajdują się razem w grupie I, więc i w tym przypadku widoczny jest efekt „cofnięcia".

4. Po dodaniu chlorków do roztworu soli srebra(I) wytrąca się biały osad, analogicznie reagują jony talu(I)

Chemiczne szachy

Podobieństwo srebra i talu jest fragmentem jeszcze innego zjawiska, widocznego, gdy potraktujesz tablicę układu okresowego w formie długiej jak szachownicę. To nie żart, takie podobieństwo zauważono stosunkowo niedawno, ale jest ono opisywane w literaturze chemicznej i powiązane z ruchem konika szachowego (ściślej jednym z możliwych ruchów skoczka – o jedno pole w dół i dwa w prawo). W takim samym położeniu względem siebie znajdują się kadm i ołów – toksyczne metale służące do produkcji akumulatorów, stopów łożyskowych oraz wykorzystywane w technice jądrowej. Inny przykład to cyna i cynk – przyjazne organizmom żywym (w przeciwieństwie do wielu metali leżących w ich pobliżu), stosowane jako powłoki antykorozyjne i od wieków będące składnikami ważnych stopów z miedzią: brązu (cyna) i mosiądzu (cynk). Dodatkowym potwierdzeniem zjawiska jest fakt, że bardzo wiele związków metali związanych ruchem skoczka ma podobne właściwości fizykochemiczne (temperatury topnienia, struktury krystaliczne). Obecnie nie istnieje wytłumaczenie tego zaskakującego zjawiska.



5. Kilka par pierwiastków połączonych ruchem skoczka szachowego

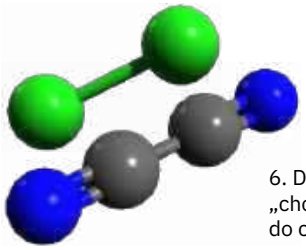
Na podstawie zaobserwowanego podobieństwa próbowano przewidzieć właściwości pierwiastka 114 (flerow), leżącego pod ołowiem. Otrzymane pojedyncze jądra atomów Fl nie pozwalają przy obecnym stanie techniki na dokładniejsze zbadanie jego właściwości fizykochemicznych, jednak ruch konika szachowego wiąże rtęć z tym pierwiastkiem. Można zatem przypuszczać, że będzie miał on dość niską temperaturę topnienia (czyżby kolejny ciekły metal?) (**5**).

Przedstawiona zależność pokazuje także, że nie ma „jedynie słusznej" wersji tablicy układu okresowego – jedne podobieństwa pierwiastków są lepiej widoczne w formie długiej, inne w krótkiej.

Pierwiastki na niby

Nie tylko jedne pierwiastki udają inne, ale także niektóre jony. Mowa tu oczywiście o jonach złożonych, czyli takich, które składają się z kilku atomów; jony proste podobne do innych jonów już znasz (np. Ba^{2+} i Pb^{2+}). Przykładem są **pseudohalogeny**, czyli aniony udające fluorowce, zwane halogenami (z gr. „tworzące sole"). Przedstawiciele tej licznej grupy to np. jon cyjankowy CN^- i rodankowy SCN^-. Reagują one podobnie do jonu chlorkowego i tworzą z kationami srebra białe osady nierozpuszczalne w rozcieńczonych kwasach. Nie powinno zatem dziwić wykrywanie pseudohalogenów w toku analizy razem z anionem Cl^-. Jon cyjankowy tak bardzo „chce" upodobnić się do fluorowców, że tworzy nawet analog ich dwuatomowych cząsteczek – dicyjan $(CN)_2$, zupełnie jak np. chlor Cl_2 (**6**).

Do cyjanków z oczywistych względów nie masz dostępu, ale możesz porównać zachowanie rodanków i chlorków. Sporządź roztwory azotanu srebra $AgNO_3$, chlorku sodu NaCl i rodanku potasu KSCN. Użyj wody destylowanej, ponieważ chlorki

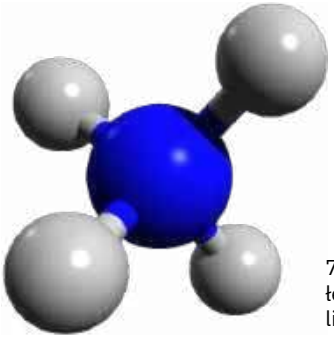


6. Dicyjan (u dołu) bardzo „chce" upodobnić się do chloru (u góry)

i inne sole obecne w „kranówce" zafałszują wyniki (w roztworze soli srebra od razu zauważysz zmętnienie). Do roztworów chlorków i rodanków dodaj porcje roztworu $AgNO_3$. W obu przypadkach powstaną białe osady. Po opadnięciu zawiesin na dno, zlej ciecz znad osadów i do każdego z nich dodaj niewielką ilość wody amoniakalnej. Osady rozpuszczają się w tym odczynniku (rodanek nieco słabiej niż chlorek). Dodatek kwasu azotowego wywoła ponowne wytrącenie osadów. Jak zatem widać, anion rodankowy rzeczywiście jest bliźniakiem jonu chlorkowego.

Kationy nie są gorsze i również mają swojego sobowtóra – jon amonowy NH_4^+. Ten z kolei upodobnił się do jonów litowców, a zwłaszcza jonu potasu (**7**). Oba kationy posiadają zbliżone rozmiary, tworzą szereg związków o podobnej rozpuszczalności, a ponadto mogą się wzajemnie zastępować w krystalicznych solach. Podobnie jak anion cyjankowy, jon amonowy również bardzo „chce" upodobnić się do swojego bliźniaka. Podczas elektrolizy prowadzonej na katodzie rtęciowej rozpuszcza się w niej (podobnie jak litowce i inne reaktywne metale) w postaci egzotycznego tworu o wzorze NH_4. Ten ostatni jest jednak nietrwały i szybko rozpada się na amoniak i wodór.

Ponieważ wszystkie popularne związki potasu są dobrze rozpuszczalne w wodzie, do porównania ich właściwości z jonem amonowym trzeba użyć specjalnego odczynnika. Sporządź roztwory chlorku kobaltu $CoCl_2$ i azotynu sodu



7. Amon, jon z tytułem „honorowego" litowca

8. Zarówno jony potasu, jak i amonu dają identyczną reakcję

$NaNO_2$ (inaczej azotanu(III)). Potrzebny będzie również spożywczy ocet o stężeniu 6...10% oraz sole potasu (np. KCl) i amonu (NH_4Cl). Do dwóch probówek wlej po kilka cm^3 roztworu soli kobaltu, po 1 cm^3 octu i po kilka cm^3 roztworu azotynu sodu. Zamieszaj zawartość i do jednej z probówek dodaj roztwór KCl, a do drugiej – NH_4Cl. W obu naczyniach powstanie żółtawe zabarwienie, w przypadku zaś większego stężenia soli – takiego samego koloru osad (**8**). Pomijając skomplikowany wzór powstającego związku i reakcje, które doprowadziły do jego utworzenia, masz zidentyfikowaną kolejną parę „bliźniaków".

W dwóch częściach artykułu przedstawione zostały podobieństwa pierwiastków: te znane Ci z nauki szkolnej i te, o których nie każdy, nawet chemik, słyszał. Nie są to oczywiście wszystkie poznane dotychczas „chemiczne bliźniaki", a wraz z rozwojem wiedzy z pewnością pojawią się i inne. Chemia jest znacznie bardziej skomplikowana niż jej, z konieczności, uproszczony szkolny obraz. Czytając jednak artykuły działu chemicznego w „Młodym Techniku", dobrze o tym fakcie wiesz. ■

Krzysztof Orliński

Transport

W 1965 roku student Yale o nazwisku Fred Smith napisał pracę semestralną, w której opisał system dostarczania przesyłek na terenie całych Stanów Zjednoczonych w ciągu jednej nocy. Profesor wystawił mu ocenę dostateczną i zasugerował, żeby skupił się na czymś bardziej realistycznym. Smith skupił się na swoim pomyśle. W 1971 roku założył FedEx. Dziś firma obsługuje ponad 16 milionów przesyłek dziennie, zatrudnia ponad 500 tysięcy ludzi i działa w ponad 220 krajach. Cały ten mechanizm – samoloty, ciężarówki, magazyny, harmonogramy, trasy, systemy śledzenia – nie działa sam z siebie. Ktoś musi go zaprojektować, zorganizować i utrzymać w ruchu. I właśnie tym zajmują się absolwenci kierunku, na który zapraszamy. Zapraszamy na Transport.

Załadunek

Transport to kierunek, który można studiować dziennie, wieczorowo i zaocznie, a uczelni oferujących tę dziedzinę w Polsce jest naprawdę sporo, bo ponad dwadzieścia. Politechniki, uniwersytety techniczne, akademie morskie i szkoły prywatne – wszystkie one przekonują kandydatów, że właśnie u nich transport wygląda najciekawiej. Wybierając szkołę prywatną, można liczyć na to, że z chwilą złożenia dokumentów zostanie się studentem. Wybierając uczelnię publiczną, trzeba być przygotowanym na postępowanie rekrutacyjne oparte na wynikach maturalnych. Konkurencja jest realna: Politechnika Krakowska odnotowała w ostatnich latach nawet czterech kandydatów na jedno miejsce na kierunku Transport.

Zanim jednak kandydat wybierze uczelnię, warto sprawdzić, jak ocenia ją środowisko akademickie. W najnowszym Rankingu Kierunków Studiów Perspektywy 2026 Politechnika Warszawska utrzymała pozycję lidera w dziedzinie transportu i robi to już od dziesięciu lat z rzędu, nie dając się zepchnąć z tronu żadnej konkurencji. Tuż za nią Politechnika Krakowska, która awansowała na drugie miejsce. Prowadzi co prawda kierunek pod nazwą Środki Transportu i Logistyka, ale to wciąż transport w pełnym wymiarze. Trzecia jest Politechnika Morska w Szczecinie, czwarta Politechnika Śląska, a w pierwszej dziesiątce mieszczą się jeszcze Politechniki Poznańska, Lubelska, Gdańska i Wrocławska. Dla tych, którzy nie celują w czołówkę albo szukają mniejszego ośrodka, opcji też nie brakuje. Swoją ofertę mają politechniki: Rzeszowska, Częstochowska, Świętokrzyska czy Bydgoska. Mniejsze miasto często oznacza niższe koszty życia i bardziej kameralne warunki nauki, a traci się jedynie nieco na prestiżu dyplomu. To rachunek, który każdy musi sobie zrobić sam.

Uczelnie oferują bogaty wachlarz specjalizacji, spośród których student może po trzecim semestrze wybrać tę, która jest mu najbliższa. Politechnika Warszawska daje do wyboru między innymi Sterowanie ruchem drogowym, kolejowym i lotniczym, Telematykę transportu, Logistykę i technologię transportu kolejowego lub samochodowego, a nawet Pojazdy autonomiczne i systemy transportu autonomicznego. Politechnika Krakowska proponuje Transport lotniczy, miejski i kolejowy, Spedycję czy Inteligentne zintegrowane systemy transportowe i logistyczne. Gdańsk daje możliwość pójścia zarówno przez Wydział Inżynierii Lądowej, jak i przez Wydział Oceanotechniki i Okrętownictwa. To dla tych, których ciągnie morze. Nowością ostatnich lat jest specjalność Transport w przemyśle 4.0, dostępna między innymi na AGH na studiach drugiego stopnia, łącząca klasyczne kształcenie z automatyzacją, robotyzacją i intralogistyką. Można by tak wymieniać bez końca, bo uczelnie mają do zaoferowania jeszcze więcej, dlatego przed złożeniem dokumentów warto upewnić się, że wybrana szkoła ma tę specjalizację, z którą chcemy związać swoją przyszłość.

Trasa

Studia na Transporcie to podróż przez kilka dziedzin naraz, i to dosłownie, bo program kształcenia łączy inżynierię, ekonomię, zarządzanie i coraz częściej informatykę. W treściach podstawowych pojawia się królowa nauk. Na inżynierce jej wymiar to zazwyczaj 120 godzin,

a do kompletu dochodzi 60 godzin fizyki, 75 godzin mechaniki technicznej, 45 godzin informatyki i porcja ekonomii. Reszta to przedmioty kierunkowe, wśród których znajdziemy: logistykę, inżynierię ruchu, telematykę, systemy transportowe i rysunek techniczny. Jedno jest pewne: studentowi Transportu nie powinno się nudzić.

Poziom trudności oceniany jest przez studentów jako umiarkowany, choć zdania bywają podzielone, a zależy to mocno od uczelni. Faktem jest, że nasi rozmówcy mówią niemalże jednym głosem: najtrudniejszy jest pierwszy rok. Świeżo upieczeni maturzyści nie zawsze spodziewają się tempa, w jakim zostają zagonieni do pracy, i bywa, że zbyt dużo czasu poświęcają na budowanie relacji towarzyskich. Sporo problemów przysparzają fizyka i grafika inżynierska. Te dwa przedmioty potrafią skrócić wakacje i przyprawić o kilka siwych włosów. Potem już jest z górki. Absolwenci doceniają, że ich wiedza inżynieryjna jest rozległa i są w stanie wypowiedzieć się na wiele tematów, ale zwracają też uwagę na pewną lukę między teorią a praktyką. Studia kształcą szeroko i ogólnie, a konkretnych kwalifikacji potrzebnych od pierwszego dnia w zawodzie trzeba szukać samemu. Pomagają w tym praktyki i staże, które są obowiązkowym elementem programu, jednak warto potraktować je jako wstęp, a nie zakończenie budowania doświadczenia.

Najlepiej w tej sytuacji wychodzą studenci zaoczni, którzy już w trakcie nauki mogą pracować. Spedytorem czy logistykiem można zostać nawet bez dyplomu wyższej uczelni, więc wejście do branży nie wymaga otwierania wielu drzwi naraz. Doświadczenie zdobyte przy okazji procentuje potem przy staraniu się o wyższe stanowiska, a znajomości nawiązane w firmie bywają cenniejsze niż niejeden egzamin. Nie obejdzie się również bez języków obcych. Angielski to absolutne minimum, ale w transporcie przyda się też niemiecki. Branża silnie operuje na osi wschód–zachód, a codzienny kontakt z partnerami z Niemiec czy Austrii to standard w wielu firmach. Kto dorzuci jeszcze rosyjski albo chiński, ten otworzy sobie drzwi, o których inni nawet nie wiedzą, że istnieją.

Rozładunek

Koniec studiów. Minęło pięć, może sześć lat. I co dalej? Czas poszukać pracy na miarę możliwości i umiejętności absolwenta Transportu. Do dyspozycji są między innymi stanowiska kierownika do spraw dystrybucji, kierownika do spraw planowania transportu, spedytora, dyrektora logistyki lub specjalisty tego działu. Pracy można szukać w przedsiębiorstwach transportu drogowego, kolejowego, lotniczego i morskiego, firmach logistycznych i spedycyjnych, biurach projektowych infrastruktury transportowej, a także w urzędach i instytucjach zajmujących się planowaniem mobilności na poziomie miasta i regionu.

Rzeczywistość wygląda natomiast tak, że na wiele z tych stanowisk mogą aplikować również absolwenci innych kierunków technicznych. Studia logistyczne, a nawet matematyczne bywają mile widziane u kandydatów na transportowca. Czasami wystarczy, by przyszły menedżer skończył ekonomię i znał się na zarządzaniu. Bardzo to utrudnia życie absolwentowi Transportu, ale nie powinien się poddawać, bo praca jest i czeka na najlepszych. Branża boryka się przy tym z poważnym niedoborem kadr. Szacunki mówią o od kilkudziesięciu do nawet dwustu tysiącach wakatów w różnych segmentach rynku, co wyraźnie wzmacnia pozycję negocjacyjną kandydata z dyplomem.

Zarobki wyglądają dziś znacznie lepiej niż jeszcze kilka lat temu. Świeżo upieczony absolwent zaczynający pracę jako specjalista może liczyć na wynagrodzenie w okolicach od 6000 do 8000 złotych brutto miesięcznie. Z kilkuletnim doświadczeniem widełki przesuwają się w okolice od 8000 do 11 000 złotych. Kierownik do spraw transportu lub logistyki zarabia przeciętnie od 11 000 do 16 000 złotych brutto, a dyrektorzy w dużych strukturach liczą już w dziesiątkach tysięcy, i to bez uwzględniania premii, które w tej branży potrafią być całkiem pokaźne. Wyraźne różnice regionalne sprawiają, że Warszawa i duże ośrodki płacą lepiej.

Transport to kierunek dla osób, które charakteryzują się analitycznym umysłem i zdolnościami organizacyjnymi. To miejsce dla ludzi, którzy są odporni na stres, potrafią podejmować szybkie decyzje i starają się rozwiązywać problemy, zamiast rozkładać ręce, mówiąc: nie da się. Jeśli ktoś ma te cechy i interesuje go to, co dzieje się między producentem a konsumentem, między lotniskiem a dworcem, między autonomicznym pojazdem a sygnalizacją świetlną, to koniecznie powinien postawić na Transport. ■

Michał Pacholski

Promienie Roentgena
– od rury Crookesa do pierścienia synchrotronu

Rentgen – słowo to weszło do współczesnej polszczyzny jako rzeczownik pospolity. Mówimy: pójść do rentgena, rentgen pokazał... Właśnie mija 130. rocznica odkrycia przez Roentgena przenikliwych promieni nazwanych jego imieniem. Było to jedno z wielkich odkryć fizyki przełomu XIX i XX wieku, które wpłynęły na całe następne stulecie. Historia tego odkrycia jest fascynująca; chcemy ją tu przypomnieć.

Na początek kilka encyklopedycznych informacji o samym odkrywcy. Wilhelm Conrad Roentgen (w oryginalnym zapisie Röntgen) był synem Niemca i Holenderki [1]. Studiuje na słynnej Politechnice w Zurychu, gdzie uzyskuje dyplom inżyniera mechanika i zostaje asystentem sławnego profesora fizyki Augusta Kundta. Od tej pory zajmuje się wyłącznie badaniami naukowymi i nauczaniem, pracując kolejno na kilku niemieckich uniwersytetach. W roku 1894 zostaje rektorem bawarskiego Uniwersytetu Juliusza i Maksymiliana w Würzburgu. Kieruje tam znakomicie wyposażonym Instytutem Fizyki, gdzie dokonuje największego odkrycia swojego życia.

W tym czasie fizycy pasjonowali się zjawiskami elektrycznymi występującymi w bańkach szklanych, z których częściowo wypompowano powietrze. Bańki te miały metalowe elektrody wtopione w szkło, do których przykładano napięcie elektryczne. Eksperymenty z takimi bańkami (zwanymi także lampami lub rurami) doprowadziły do wykrycia promieni katodowych, które później okazały się strumieniem naładowanych

1. Wilhelm Conrad Roentgen (1845–1923), laureat pierwszej Nagrody Nobla z dziedziny fizyki (1901)

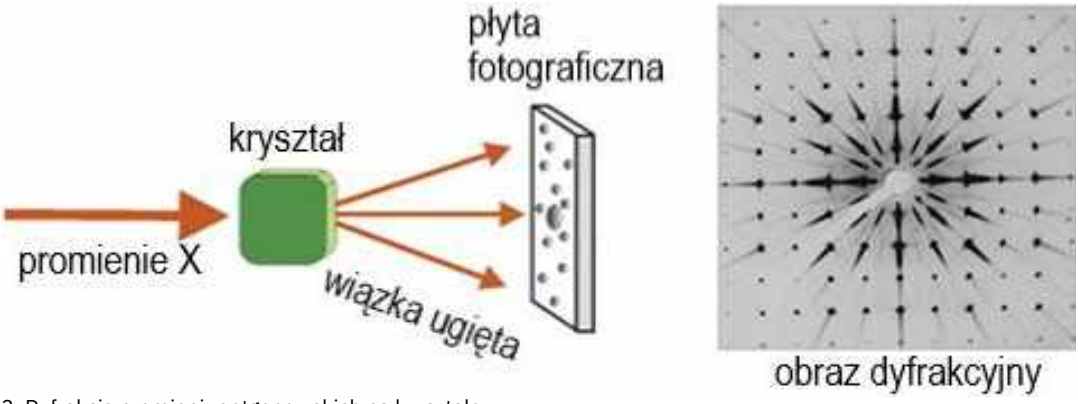
cząstek, elektronów, wysyłanych przez ujemnie spolaryzowaną elektrodę, katodę (patrz: WiŻ nr 10/1991). Zderzenia elektronów powodowały świecenie resztkowego gazu zawartego w lampie, a także szklanej ścianki, w którą uderzały.

Kronika wielkiego odkrycia

Na początku października 1895 roku Roentgen rozpoczął eksperymenty z promieniami katodowymi wytwarzanymi w tzw. rurze Crookesa. Był to rodzaj bańki szklanej, bardzo popularnej w owym czasie, którą zaprojektował angielski uczony sir William Crookes. Promienie katodowe można wyprowadzić na zewnątrz bańki, jeśli ściankę naprzeciw katody zastąpi się cienką blaszką glinową. W powietrzu promienie te są silnie pochłaniane, toteż ich zasięg jest bardzo krótki, rzędu centymetrów, ale można je wykryć, gdyż działają na umieszczoną w ich zasięgu kliszę fotograficzną lub ekran fluorescencyjny.

A oto jak relacjonują historycy nauki samo odkrycie. Wieczorem 8 listopada 1895 roku Roentgen przeprowadza kolejne doświadczenie z promieniami katodowymi. Przypadkowo zauważa, że ekran fluorescencyjny, przygotowany do innego eksperymentu i umieszczony w tak dużej odległości od lampy, że w żadnym wypadku nie mogły do niego docierać promienie katodowe, świeci! Świeci tylko wtedy, gdy do rury Crookesa przyłożone jest wysokie napięcie. Zdumiony tym Roentgen przesłania ekran leżącą w pobliżu książką, ale świecenie nie ustaje. Wkrótce stwierdza, że także inne nieprzezroczyste dla światła materiały, takie jak drewno, ebonit, guma, a nawet niektóre metale, nie wygaszają świecenia. Jedynie blacha ołowiana lub platynowa, umieszczona pomiędzy rurą i ekranem, tłumi całkowicie ten efekt. Zafascynowany nowym zjawiskiem, bada je intensywnie przez kilka tygodni. Stopniowo uświadamia sobie, że rura Crookesa jest źródłem nieznanych dotychczas niewidzialnych promieni, które nazywa promieniami X. W odróżnieniu od promieni katodowych promienie X nie są odchylane polem magnetycznym. Któregoś dnia następuje najbardziej spektakularny moment jego odkrycia. Roentgen dostrzega na fluoryzującym ekranie szkielet własnej ręki! Stwierdza następnie, że promienie X działają na kliszę fotograficzną, nawet owiniętą w ciemny papier, i wobec tego obrazy powstające w wyniku prześwietlenia różnych przedmiotów promieniami X można łatwo rejestrować. Do historii przeszło wykonane przez Roentgena w grudniu 1895 roku

2. Rentgenogram dłoni żony Roentgena



3. Dyfrakcja promieni rentgenowskich na krysztale

zdjęcie ręki jego żony, na której palcu widnieje ślubna obrączka [2]. Jest to pierwszy rentgenogram ludzkiego ciała, pieczołowicie przechowywany w Instytucie Fizyki w Würzburgu. Kontrast występujący na kliszy jest spowodowany tym, że kościec silniej niż mięśnie pochłania promienie X.

W styczniu 1896 r. Roentgen referuje wyniki swoich badań na posiedzeniu miejscowego Towarzystwa Fizyko-Medycznego. Argumentuje, że promienie X wybiegają ze szklanej ścianki rury Crookesa w miejscu, gdzie promienie katodowe (dzisiaj powiedzielibyśmy – elektrony) uderzają w szkło. Zaproponowano wówczas, by promienie X, na cześć odkrywcy, nazywać promieniami Roentgena.

Niezwykłe właściwości promieni Roentgena wywołały natychmiast ogromne zainteresowanie na całym świecie. Ponieważ rura Crookesa była wówczas popularnym rekwizytem w laboratoriach fizycznych, setki uczonych stały się od razu „ekspertami" od promieni X. Rentgenowskie zdjęcie kośćca dłoni ludzkiej w ciągu kilku dni obiegło cały świat. Gazety zapełniły się budzącymi grozę fotografiami szkieletów dłoni i stóp oraz sensacyjnymi informacjami, rysunkami i dowcipami na temat promieni Roentgena. Dzięki temu możemy dziś śledzić ówczesną fascynację nowo odkrytymi promieniami.

Pewna londyńska firma konfekcyjna zachęcała klientki do kupna swoich wyrobów, twierdząc, że produkowana przez nią bielizna damska jest wykonywana z materiałów nieprzezroczystych dla promieni X. Tytuł ogłoszenia tej firmy brzmiał: „X-ray proof underwear – no lady safe without it", co znaczy: bielizna odporna na promienie X – żadna dama nie jest bez niej bezpieczna. Z dnia na dzień Roentgen stał się bohaterem narodowym. Gwoli gorzkiej prawdy trzeba jednak dodać, że pod koniec życia wegetował na granicy nędzy.

Świat lekarski szybko zaczął stosować promienie Roentgena w celach diagnostycznych. Później odkryto, że promienie te wywołują szkodliwe działanie biologiczne: porażają i niszczą żywe komórki. Zostało to zresztą wykorzystane jako narzędzie terapeutyczne – do niszczenia nowotworów. Tak więc odkrycie Roentgena stało się bardzo szybko powszechnie znanym i cenionym osiągnięciem naukowym. Nic też dziwnego, że gdy w roku 1901 zaczęto przyznawać Nagrody Nobla, pierwszym laureatem tej nagrody w dziedzinie fizyki został właśnie Roentgen.

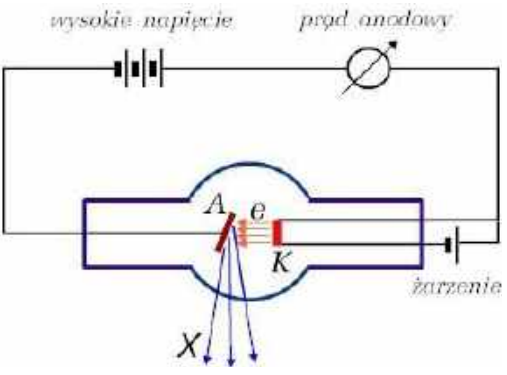
Promienie X w świecie kryształów

Natura promieni Roentgena przez wiele lat pozostawała niewyjaśniona, choć sam Roentgen przypuszczał, że jest ona raczej falowa niż korpuskularna. Gdy w roku 1910 zaczął pracować na Uniwersytecie Ludwika i Maksymiliana w Monachium, spotkał tam wielu wybitnych fizyków, między innymi Maxa von Laue. W tym czasie domyślano się już, że kryształy są ciałami zbudowanymi z regularnie rozmieszczonych atomów, ale nie było na to żadnego dowodu eksperymentalnego. Co więcej, nie wszyscy fizycy byli przekonani, że atomy naprawdę istnieją. Laue podejrzewał, że hipotetyczna długość fali promieni Roentgena może być tego samego rzędu co odległości między atomami w kryształach. Gdyby to było prawdą, to promienie Roentgena powinny ulegać ugięciu (dyfrakcji) na kryształach, podobnie jak światło ulega ugięciu na siatce dyfrakcyjnej

wykonanej np. przez nacięcie równoodległych rys na płytce szklanej, między którymi odstęp jest rzędu długości fali padającej. Ugięcie fali świetlnej przez siatkę prowadzi do powstania na ekranie umieszczonym poza nią obrazu dyfrakcyjnego złożonego z układu na przemian jasnych i ciemnych prążków.

Przypuszczenie Lauego okazało się prawdziwe! Jego dwaj asystenci uzyskali pierwsze obrazy dyfrakcyjne promieni Roentgena ugiętych na krysztale siarczanu miedzi. Kryształ stanowił tu trójwymiarową siatkę dyfrakcyjną, a otrzymane obrazy składały się z odosobnionych plamek (refleksów) rozłożonych w sposób symetryczny na kliszy fotograficznej [3]. Z symetrii obrazu dyfrakcyjnego można było wnioskować wprost o symetrii samego kryształu. To historyczne doświadczenie było podwójnym sukcesem. Po pierwsze, udowadniało ono, że promienie Roentgena mają naturę elektromagnetyczną, podobnie jak światło. Po drugie, pokazywało, że kryształy są rzeczywiście zbudowane z regularnie rozmieszczonych w przestrzeni atomów. Laue został za to doświadczenie uhonorowany Nagrodą Nobla w 1914 roku.

Badaniami Lauego zainteresowali się dwaj inni uczeni pracujący w Anglii: sir William Henry Bragg i William Lawrence Bragg, ojciec i syn. Doprowadzili oni dzieło rozpoczęte przez Lauego do końca. Pokazali, jak za pomocą dyfrakcji można zmierzyć długość fali promieni rentgenowskich i równocześnie określić strukturę kryształu, to znaczy rozszyfrować sposób, w jaki są rozmieszczone atomy w krysztale. Były to doniosłe wyniki, które w rezultacie pokazały, że większość ciał stałych występujących w przyrodzie ma budowę krystaliczną. Uczeni uzyskali odtąd wspaniałe narzędzie badawcze pozwalające badać strukturę krystaliczną różnych substancji. Zapoczątkowało to rozwój nowej gałęzi fizyki: krystalografii strukturalnej. Za prace nad badaniami struktury kryształów za pomocą promieni Roentgena Braggowie otrzymali w roku 1915 Nagrodę Nobla z fizyki. Była to więc już trzecia Nagroda Nobla przyznana za odkrycia związane z promieniami X.



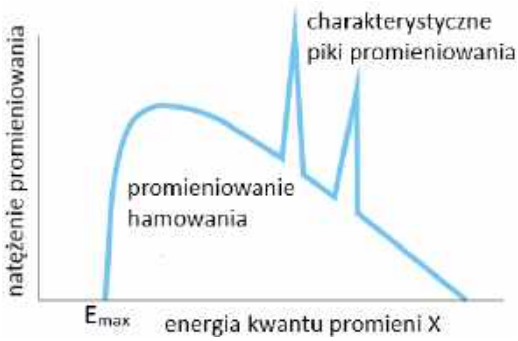
4. Schemat klasycznej lampy rentgenowskiej

Dzisiaj dyfraktometry rentgenowskie, a także inne urządzenia wykorzystujące promienie Roentgena, stanowią standardowe wyposażenie laboratoriów naukowych i przemysłowych. W medycynie wielkim sukcesem było opracowanie w latach 80. ubiegłego stulecia techniki zwanej tomografią komputerową. W metodzie tej badany obiekt (np. głowa pacjenta) znajduje się pomiędzy ruchomym źródłem promieniowania a zsynchronizowanym z nim detektorem. W ten sposób wiązka promieni X penetruje całe wnętrze obiektu, a detektor rejestruje intensywność transmisji dla różnych konfiguracji. Zebrane w ten sposób dane są potem przetwarzane przez komputer i przedstawiane w postaci graficznej. Pozwala to na zlokalizowanie i zidentyfikowanie występującego urazu.

Od rury do pierścienia

Przełomem w zastosowaniu promieniowania rentgenowskiego w nauce i przemyśle było zbudowanie w latach 40. ubiegłego stulecia synchrotronu, źródła promieniowania o bardzo dużej mocy. W synchrotronie elektrony krążą wewnątrz toroidalnej komory próżniowej, nazywanej pierścieniem. Są one przyspieszane, gdy przechodzą przez obszary pola elektrycznego wytwarzanego przez specjalne generatory. Odpowiednio dobrane pole magnetyczne, skierowane prostopadle do płaszczyzny pierścienia, utrzymuje poruszające się elektrony na orbitach kołowych wewnątrz pierścienia, zapobiegając ich uderzeniom w ścianki. Jeśli rozpędzony elektron zostanie, za pomocą specjalnego urządzenia, wyprowadzony z pierścienia, a następnie wyhamowany, to emituje on promieniowanie elektromagnetyczne, którego długość fali rozciąga się od podczerwieni do promieniowania rentgenowskiego. Moc takiego promieniowania synchrotronowego przewyższa o rzędy wielkości moce wysyłane przez konwencjonalne lampy rentgenowskie. Stwarza to zupełnie nowe możliwości zastosowań

Promienie Roentgena (w literaturze francuskiej i anglojęzycznej używa się terminu – promienie X) stanowią wycinek promieniowania elektromagnetycznego o długości fal w zakresie od 0,0001 do 10 nm. Fale te, ze względu na swą krótkość, mają zdolność łatwego przenikania przez większość substancji, co zadecydowało o ich zastosowaniach w medycynie. Promieniowanie rentgenowskie powstaje bądź w wyniku hamowania naładowanej cząstki, elektronu, przez materię (tzw. promieniowanie hamowania), bądź w wyniku przejścia elektronu w atomie z poziomu o wyższej energii na poziom o niższej energii. Ten drugi proces, będący następstwem jonizacji wewnętrznej powłoki elektronowej atomu spowodowanej bombardowaniem elektronami, prowadzi do emisji tzw. promieniowania charakterystycznego, którego długość fali zależy od rodzaju pierwiastka emitującego to promieniowanie. Wytwarzane są najczęściej w lampie rentgenowskiej, tj. próżniowej bańce szklanej lub metalowej, zawierającej wewnątrz dwie elektrody: anodę i katodę [4]. Elektrony, emitowane termicznie przez katodę, są przyspieszane polem elektrycznym wytworzonym przez przyłożone między anodą i katodą wysokie napięcie. Bombardują one anodę, która staje się źródłem promieniowania rentgenowskiego [5].



5. Przykładowy kształt widma promieniowania emitowanego z lampy rentgenowskiej

promieni rentgenowskich, nieosiągalne za pomocą źródeł konwencjonalnych.

Pierwszy synchrotron elektronowy zbudowany na Uniwersytecie Cornella (USA) miał średnicę kilku metrów i mieścił się wewnątrz pokoju laboratoryjnego. Współcześnie budowane synchrotrony mają średnicę rzędu kilometra, a ich pierścienie umieszczone są w specjalnie wybudowanych podziemnych tunelach. Pierścień dużego synchrotronu Europejskiego Ośrodka Badań Jądrowych (CERN-u) przecina granicę Francji i Szwajcarii.

W Polsce obchodziliśmy właśnie jubileusz związany z dziesiątą rocznicą uruchomienia synchrotronu „Solaris" w Narodowym Centrum Promieniowania Synchrotronowego działającym przy Uniwersytecie Jagiellońskim [6]. Jest to jedyny synchrotron w Europie Środkowo-Wschodniej. Obwód pierścienia Solarisa wynosi 96 m, a energia przyspieszanych elektronów 1,5 GeV. Urządzenie jest wykorzystywane do badań w wielu różnorodnych dziedzinach, takich jak inżynieria materiałowa, fizyka ciała stałego, medycyna i farmacja itp. ■

Tadeusz Figielski

6. Kraków, Narodowe Centrum Promieniowania Synchrotronowego „Solaris"

Z „Młodym Technikiem” jestem związany od półwiecza. Wtedy w naszym kraju można było jeszcze spotkać dinozaura. W 1976 roku opublikowałem w MT artykuł o poszukiwaniu liczb pierwszych – w przededniu eksplozji tej tematyki związanej z metodami szyfrowania wiadomości za pomocą niesamowitych własności tych liczb. Potem przyszła bliższa współpraca. Od 1978 roku pisuję co miesiąc o mojej pięknej matematyce. Chcę i muszę tu podziękować mojemu nauczycielowi matematyki z liceum. Był nim inż. Wacław Chyra (1904–1970) – dowódca kompanii w Powstaniu Warszawskim. Kilkakrotnie podrywał kompanię do straceńczego ataku. Sam przeżył przypadkiem. Kłaniam się nisko, Panie Profesorze.
Na pytanie, jakie mam hobby, odpowiadam, że trzy: 1) matematyka, 2) matematyka, 3) matematyka. Na pytanie o szczęśliwe liczby odpowiadam: 1, 41, 116. Autobusem warszawskiej linii 116 dojeżdżałem do mojej szkoły: warszawskiego Liceum nr 41 im. Joachima Lelewela. Gdy jechałem na egzamin maturalny, podjechał autobus z numerem bocznym 1. Wtedy „jedynka” nie kojarzyła się z oceną niedostateczną, lecz miała raczej znaczenie: „będziesz pierwszy”. Udało się. Zdałem maturę!
Piszę zatem o matematyce. Przenika ona nasze życie. Uczy myślenia, precyzji i spokoju. Nie rozwiązuje naszych codziennych problemów, ale daje nadzieję na ciekawe życie. Dorastają już Czytelnicy „Młodego Technika”, którzy będą żyć w XXII wieku. Zainteresujcie się matematyką.

Dwie rocznice

Mijają właśnie „okrągłe” rocznice ważnych i związanych ze sobą wydarzeń matematycznych. Pięćdziesiąt lat temu, w 1976 roku, rozwiązano zagadnienie czterech barw, a trzydzieści lat temu w warszawskim szpitalu zmarł Pál Erdős. Ten wakacyjny odcinek poświęcę kolorowankom, a więcej o Erdősie – za miesiąc. Wspomnę tylko krótko, kim był. Z nazwiska można wywnioskować, że był Węgrem, ale od wyjazdu do USA w 1938 roku (a urodził się w 1913) był „obywatelem świata”. Szybko stał się sławnym matematykiem i ta sława pozwalała mu na specyficzny tryb życia. Nie miał rodziny – pozostali w kraju nie przeżyli wojny; nie ożenił się i właściwie nie miał stałego miejsca zamieszkania. Jeździł z uniwersytetu na uniwersytet, z konferencji na konferencję, z małą walizką – a dla każdego uniwersytetu i każdej konferencji goszczenie Erdősa było zaszczytem. Zajmował się wieloma zagadnieniami matematycznymi. Pracował „z każdym”, łącznie miał 514 współautorów. Po jego śmierci powstało pojęcie „liczby Erdősa”. Określa się ją tak. Każdy, kto miał wspólną pracę z nim, ma numer 1. Każdy, kto miał wspólną pracę z numerem 1, ma numer 2. Każdy, kto miał wspólną pracę z numerem 2, ma numer 3... i tak dalej. Piszący te słowa ma liczbę Erdősa 4.

Wspomnę o bardziej poważnym światowym wyróżnieniu, związanym z Erdősem. Od 35 lat przyznawana jest prestiżowa nagroda jego imienia za działalność w olimpiadach matematycznych. W tym roku (2026) otrzymał ją Michał Krych z Uniwersytetu Warszawskiego. Jest on drugim polskim laureatem tej nagrody. Pierwszym był Marcin Kuczma, też z Uniwersytetu Warszawskiego (1992). Dla ścisłości wspomnę, że wtedy nagroda ta funkcjonowała jako „nagroda Hilberta”. Kilka słów o Hilbercie – nieco dalej. Obaj uczeni, Erdős i Hilbert, to filary współczesnej matematyki. Dlatego ranga tych nagród jest bardzo wielka. Gratuluję Michałowi (Marcinowi gratulowałem owe 34 lata temu).

Przejdę do kolorowania grafów – czyli punktów połączonych odcinkami. Co w tym trudnego? Oj, to bywa bardzo trudne. Czy zajmowanie się takimi zadaniami ma sens? Tak, od kilkudziesięciu lat analiza kolorowych grafów ma dużo zastosowań. Po kolei.

***

Czy wiesz, Czytelniku, że pierwszym zagadnieniem matematycznym rozwiązanym za pomocą programu komputerowego było zagadnienie czterech barw? Zaczęło się to 23 października 1852 roku. Pewien student brytyjski, Francis Guthrie, zauważył wtedy, że każdą mapę umie pokolorować czterema kolorami w ten sposób, że obszary mające wspólną granicę są zaznaczone różnymi kolorami. Zapytał znanego matematyka Augustusa De Morgana, czy to jest ogólnie prawdziwe. Ten po dłuższym czasie odpisał, że nie wie i nie umie tego udowodnić. Zagadnienie stało się sławne. Wielu matematyków próbowało rozwiązać ten problem. W 1879 roku dowód opublikował Alfred Kempe i wydawało się, że sprawa się zakończyła. Ale w kilka lat potem znaleziono błąd w tym dowodzie. Dało się tylko uratować „twierdzenie o pięciu barwach" – że pięć kolorów wystarczy. Ten dowód nie jest bardzo skomplikowany, choć też wykracza poza ramy tego kącika.

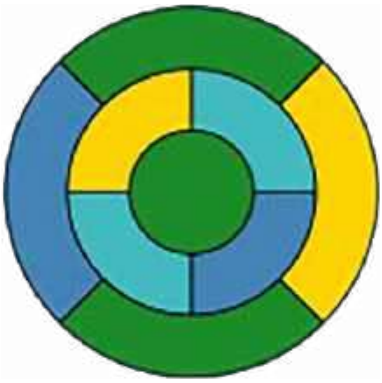
Rysunki 1 i **2** pokazują, o co chodzi. Na pierwszym mamy pięć kolorów i nie możemy zamienić czerwonych obszarów na żadne inne. Wydaje się więc, że tych pięć kolorów jest niezbędnych. Wystarczy jednak inaczej ustawić kolory i widzimy, że cztery istotnie wystarczą.

Zagadnienie przeszło na XX wiek. Należy wspomnieć o tzw. 23 problemach Hilberta. David Hilbert, niekwestionowany lider matematyków owych czasów, w 1900 roku sformułował najważniejsze zagadnienia matematyczne do rozwiązania w nadchodzącym wtedy XX stuleciu. Nie włączył do tej listy zadania o czterech barwach. W oczach współczesnych matematyków miało ono charakter bardziej „łamigłówkowy", a poza tym nie wpisywało się w główne kierunki badań Hilberta. Dopiero potem zadanie to stało się sławne – właśnie przez to, że w 1976 roku rozwiązali je Kenneth Appel i Wolfgang Haken przy użyciu komputerów, co było wtedy czymś przełomowym (i kontrowersyjnym).

Zresztą trochę jest tak, jak czuł Hilbert. Niektóre twierdzenia matematyczne są trudne, a nawet bardzo trudne, ale nie są specjalnie ważne z ogólnego punktu widzenia. Jeżeli porównać matematykę do eksploracji wysokich gór, to można powiedzieć, że są one jak samotnie sterczająca skała na uboczu. Trudna, ale nie zawadza w eksploracji. Istotne jest tylko to, że zagadnienie to wpisuje się w intensywnie rozwijaną od około 50 lat teorię grafów. Grafy okazały się nadzwyczaj ważnym pojęciem matematycznym.

1

2

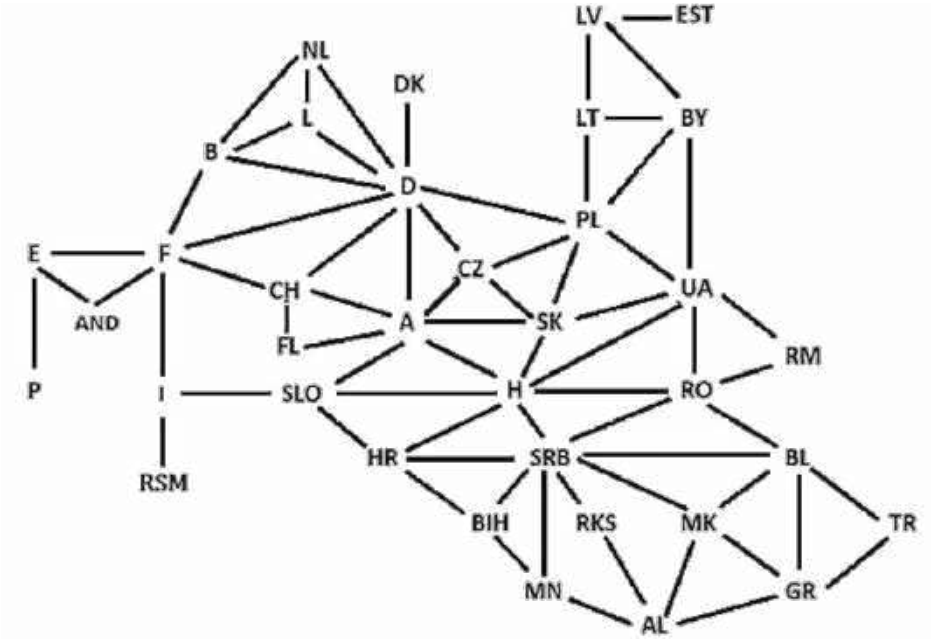


Ważnym dla samej matematyki, ale przede wszystkim dla zastosowań – co pokazują dalsze zadania.

Wspomnijmy jeszcze Francisa Guthrie (1831–1899). W 1861 roku wyjechał na stałe do Afryki Południowej. Został profesorem na Uniwersytecie w Kapsztadzie. Prowadził tam również badania botaniczne. Rozwiązania odkrytego przez siebie problemu, jak widać, nie doczekał.

Zadanie 1. Poniżej widzisz schematyczną mapę sąsiedztwa krajów europejskich (bez państw wyspowych i Skandynawii, ale z Liechtensteinem, Andorrą i San Marino). Czy widzisz, że nie da się jej pokolorować trzema kolorami? Zobacz – wszystko psuje mały Luksemburg! Gdyby nie on, to trzy kolory wystarczyłyby. Pokoloruj czterema.

Zadanie 2 ma sformułowanie jak w filmie akcji, ale po przeczytaniu proszę przetłumaczyć je na całkiem „cywilną" i pokojową sytuację. Mamy ułożyć plan lekcji. Niektóre zajęcia nie mogą się odbywać jednocześnie (na przykład prowadzi je ten sam nauczyciel albo niektórzy uczniowie chodzą na obydwa). W jednej sali nie może być jednocześnie dwóch różnych zajęć. Być może są jeszcze inne uwarankowania, nawet niecałkiem poważne – na przykład prof. X nie chce



3

mieć lekcji po prof. Y, bo uważa, że po lekcji z nim uczniowie są zbyt „rozbrykani". Teraz owo zadanie z wątkiem szpiegowskim.

Zadanie 2. Xylonia i Yxlonia to dwie wyspy na Oceanie Kolorowym. Panuje między nimi wrogość. Xylonia wysłała do Yxlonii szpiegów. Ich dane są oczywiście tajne, a ich pseudonimy operacyjne to: Arbuzy, Brunacy, Czarusia, Drapichrust, Endokrynologia, Falafel i Gradacja. Pracują nad powierzonymi zadaniami, ale niezależnie. Nie znają się nawzajem. To po pierwsze dla bezpieczeństwa, ale również po to, by Centrala mogła ich doniesienia łatwiej weryfikować. Jak to szpiedzy, mają bowiem przekazywać meldunki do centrali. Robią to tak, jak na filmach z Klossem. W określone dni tygodnia o godzinie 11 wrzucają kartkę z meldunkiem do umówionych koszy na śmieci na ulicy. Meldunek wyjmuje o godzinie 12 wysłannik centrali, przebrany za pracownika Zakładu Oczyszczania Miasta. Jak przydzielić kosze na śmieci, żeby szpiedzy, którzy mają te same zadania, nie spotykali się?

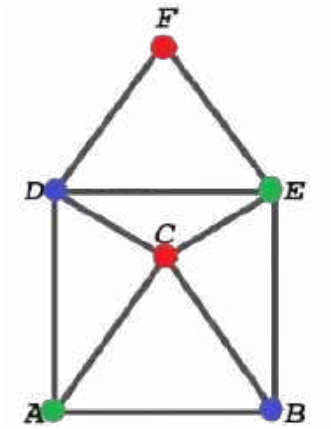
1. Arbuzy pracuje nad tymi samymi tematami co Brunacy, Czarusia i Drapichrust.
2. Brunacy pracuje nad tymi samymi co Arbuzy, Czarusia i Endokrynologia.
3. Czarusia nad tymi samymi co Arbuzy, Brunacy i Drapichrust.
4. Drapichrust ma te same zadania co Arbuzy, Czarusia, Endokrynologia i Falafel.
5. Endokrynologia – to samo co Brunacy, Czarusia, Drapichrust i Falafel.
6. Falafel – to samo co Drapichrust i Endokrynologia.

Jaki to ma związek z kolorowaniem grafu? Oczywisty – trzeba narysować schemat systemu uwarunkowań i pokolorować go zgodnie z przyjętą zasadą (końce każdego odcinka mają różne kolory). To oczywiście łatwe i bez wielkiej matematyki, ale gdy w grę wchodzą dziesiątki osób i dziesiątki ograniczeń, trzeba użyć matematyki.

Jeżeli nie zależy nam na optymalnym rozwiązaniu, można użyć tak zwanego algorytmu zachłannego. Po prostu kolorujemy po kolei. Jeżeli zabraknie koloru, dokładamy następny. I tu właśnie cała trudność. Rozwiązanie będzie – ale może być za skomplikowane. Ułożony plan zajęć będzie nieżyciowy. Potrzebna jest lepsza matematyka.

Zadanie 3. Do obszaru działania naszej siatki z poprzedniego zadania doszła jeszcze jedna ważna sprawa, ale tak tajna, że nikt nie wie, o co chodzi. Tym niemniej przydzielono do niej Czarusię i Falafela. Narysuj graf zależności i przydziel na nowo kosze na śmieci. Czy potrafisz uzasadnić, że naprawdę potrzeba czterech kolorów?

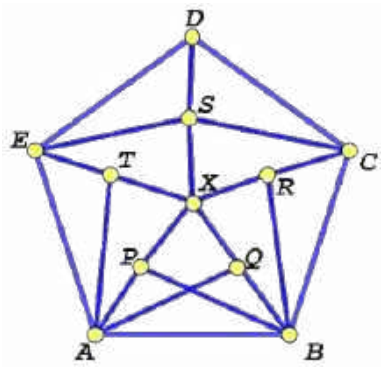
Zadanie 4. W ogródkach działkowych są ujęcia wody do podlewania w punktach A, B, C,



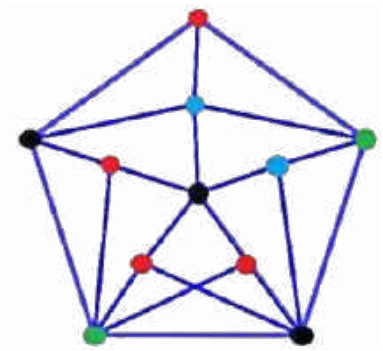
4

D, E, P, Q, R, S, T, X. Niebieskie linie pokazują, dokąd ciągnie się rura z danego punktu. Z powodu długotrwałej suszy wprowadzono nakaz, że żadnego dnia nie mogą być włączone ujęcia z obu stron jednego odcinka. Jak ustawić kolejność podlewania? Jaki to ma związek z kolorowaniem grafu?

Odpowiedź. W kolejne dni włączane są ujęcia: zielone, czarne, czerwone, niebieskie. Na przykład w dniu „czerwonym" woda dostępna jest na odcinkach *SE*, *SD*, *SC*, *SX*, *PA*, *PX*, *PB*.



5



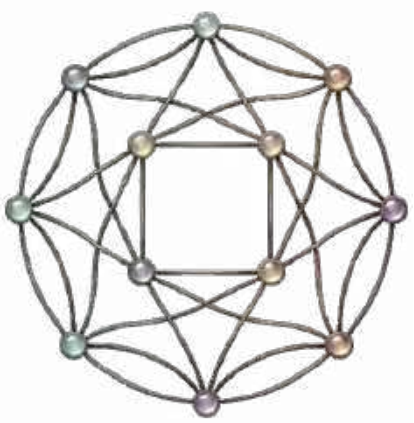
6

Zadanie 5. Najpierw dowiedz się, co to jest mandala – choć nie ma to wiele wspólnego z zadaniem. Pokoloruj widoczną niżej mandalę, zgodnie z regułą, że końce każdego odcinka (łuku) mają mieć różne kolory. Oczywiście chodzi o jak najmniejszą liczbę kolorów.

Zadanie 6. Zarząd amerykańskiej sieci fast food „Eat here" postanowił sprawdzić, czy pewna restauracja w miasteczku Oconomowoc w stanie Wisconsin spełnia ogólne normy tej sieci. W tym celu czworo członków zarządu i ośmioro pracowników niższego szczebla wybrało się do tej restauracji. Zarząd usiadł na miejscach na zewnątrz, pracownicy przy stolikach ustawionych wewnątrz, w kształcie ośmiokąta. Menu restauracji to: 1) kurczak z frytkami i ketchupem, 2) pizza z pieczarkami i ketchupem, 3) cheeseburger z sosem serowym, 4) chińska zupa wonton. Zażądano, by wszyscy, których łączy odcinek na załączonym schemasie (**rysunek 8**), dostali co innego. W ten sposób Zarząd dostałby dwie opinie od dwóch swoich członków i od dwóch pracowników, a każdy z pracowników jedną od członka Zarządu i trzy niezależne od swoich kolegów.

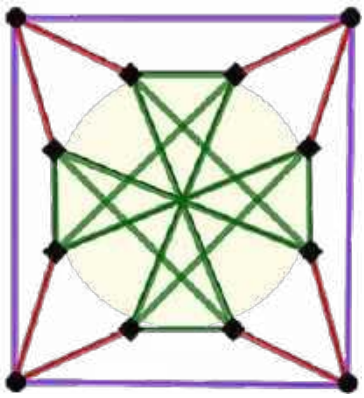
1. Znajdź na mapie USA tę miejscowość.
2. Zaproponuj, co kto ma dostać.
3. Czy da się to tak zrobić, żeby Zarząd nie dostał dania z ketchupem?
4. Postaraj się to zrobić za pomocą **mex**.
5. Wyobraź sobie, że ajent w tej restauracji oświadcza, że jest sorry, ale nie może dziś zrobić pizzy, bo zepsuł się piekarnik. Czy da się spełnić wymagania Zarządu za pomocą dostępnych trzech dań?

Komentarz. Taki graf nosi nazwę grafu Chvátala. Václav Chvátal jest Czechem. Wyjechał

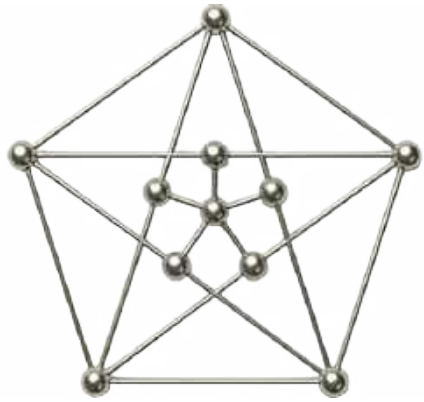


7

8



9



do USA trzy dni po inwazji radzieckiej w 1968 roku. Spotkałem go w Montrealu w 1984 roku; dziwił się, że nie zamierzam zostać na emigracji. W teorii grafów jego nazwisko wiele znaczy.

Zadanie 7. W pięknym i atrakcyjnym turystycznie miasteczku Barwigród Pentagonalny jest uroczy rynek w kształcie pięciokąta (**rysunek 9**). Kilka lat temu zarzucono tam politykę „betonozy" i rynek jest teraz cały w kwiatach i krzewach, a rosną już nowe drzewa. W narożnikach tego rynku jest pięć zabytkowych kamienic, a w centralnej części rynku też pięć malutkich restauracji. Między nimi są alejki spacerowe. W samym środku jest ratusz. Pewnego razu burmistrz Barwigrodu, Gwidon Koloryński, wpadł na pomysł, który jego zdaniem jeszcze podniesie atrakcyjność miasteczka. „Pomalujmy kamieniczki, restauracje i mój ratusz wesołymi kolorami, ale tak, żeby budynki na dwóch końcach każdej alejki były w innym kolorze". Radni zgodzili się i już-już zamówiono jedenaście kolorów, ale burmistrz oburzony zakrzyknął: „Co wy, matematyki nie znacie, chcecie mi tu jakąś pstrokaciznę zrobić, a poza tym stracilibyśmy fundusze unijne za niegospodarność. Cztery podstawowe kolory są po prostu tańsze, no i wykorzysta się je bardziej ekonomicznie. Zaprojektować mi wszystko w czterech kolorach! A jak się da, to może w trzech. Ale wydaje mi się, że trzy to za mało." A zatem pomożecie?

Komentarz. Ten graf jest w matematyce nazywany grafem Mycielskiego M_3. Jan Mycielski (1932–2025) był polskim matematykiem – choć teraz mówi się „polsko-amerykańskim". Wyjechał do USA w 1986 roku jako „visiting professor" na prestiżowy Uniwersytet w Boulder w stanie Kolorado i został tam na stałe. Graf ten nie jest może czymś wyjątkowym, ale jest to początek całej serii grafów Mycielskiego, ważnych w tej dyscyplinie matematyki.

***

Od pewnego czasu przypatruję się felgom samochodowym (bądź plastikowym kołpakom) i odkrywam na nich często interesującą geometrię. Dziś o felgach związanych z zagadnieniem kolorowania.

Na fotografii (**rysunek 10**) widzimy częsty motyw felgi aluminiowej w samochodach Peugeot. Trochę przypomina on graf złożony z dwóch pięciokątów (**rysunek 11**). Po raz pierwszy zwrócił na niego uwagę duński matematyk Julius Petersen (1838–1910). Wtedy teoria grafów wydawała się czystą ciekawostką i układanką – trochę jak dzisiejsze puzzle. W wierzchołkach grafu Petersena można tak umieścić koraliki trzech kolorów, żeby dwa końce każdego odcinka były w różnych kolorach. Więcej kolorów (bo cztery) potrzeba do innego kolorowania. Mianowicie gdy budujemy ten ornament (dygresja: czy wiesz, co to jest makrama?) ze sznurków różnych kolorów. Chcemy, by w każdym węźle mieć trzy różne kolory. Graf Petersena jest przykładem żmirłacza. Czego? Nie słyszałeś tego słowa, Czytelniku? Najpierw: czy wiesz, że Lewis Carroll (ten od „Alicji w Krainie Czarów") był matematykiem? No, to już wiesz. Otóż w 1876 roku napisał on abstrakcyjny poemat „The Hunting of the Snark". Takiego słowa „snark" nie ma w angielszczyźnie – on je utworzył. Było to coś pomiędzy *snake* (wąż) a *shark* (rekin). W 1982 roku Robert Stiller przetłumaczył to (i cały poemat) na polski jako „Wyprawa na żmirłacza", błyskotliwie oddając sens oryginalnego połączenia. A w samej matematyce żmirłaczem (*snark*) nazwano, no cóż, graf stopnia 3 z indeksem chromatycznym

10

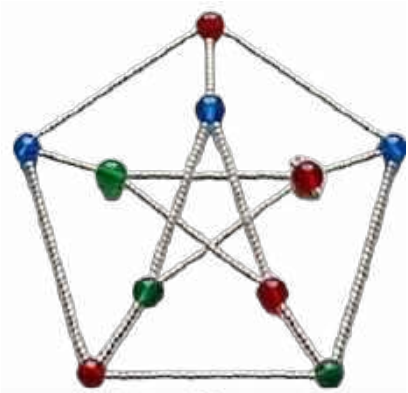
13

4. Chodzi o to, że z każdego wierzchołka wychodzą po trzy krawędzie, wybrane spośród czterech (tak jak na rysunku 12). Ale nie będę się zagłębiał w teorię grafów, bo mam jeszcze wiele ciekawego do opowiedzenia. Może innym razem.

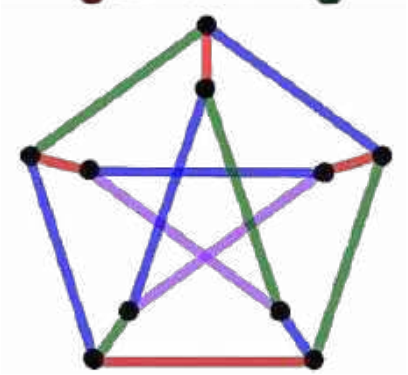
***

Jeden z moich sąsiadów ma dużego, paliwożernego SUV-a, z taką felgą jak na fotografii poniżej po lewej stronie. Obok widzisz wielokąt (*graf*), podobny do tej felgi. Wprawne oko matematyka zobaczy na nim... połowę dwunastościanu. Pokoloruj wierzchołki tego wielokąta zgodnie z regułą z poprzednich zadań.

11



12



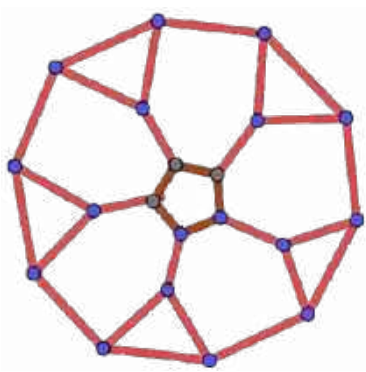
***

I to samo dla innej felgi (**rysunek 15** i **16**). Najpierw odgadnij markę tego samochodu. Poprosiłem AI, żeby poszukała, czy jest to jakiś znany graf. Odpowiedziała bez ładu i składu, byle co, zgodnie z zasadą „będzie pan zadowolony". Nie będę przytaczał tych jej wypowiedzi. Sam poszukam. Ale jedna jej odpowiedź była ciekawa. Poprosiłem: na podstawie zdjęcia (rysunek 15) stwórz sama odpowiedni graf i ładnie go narysuj. „Proszę bardzo", odpowiedziała i pokazała **rysunek 17**. Nie widzę związku, ale rysunek ładny.

***

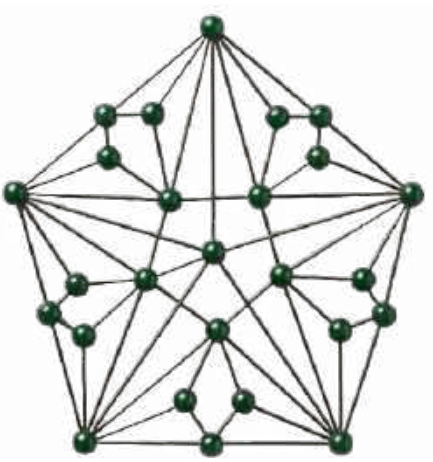
Zachwyć się grafem na **rysunku 18**. Pokoloruj jego wierzchołki (koraliki) zgodnie z zasadą, o której tu cały czas chodzi: koraliki na końcach tego samego odcinka mają mieć różne kolory. Ile najmniej kolorów potrzeba? Pokoloruj krawędzie (odcinki) zgodnie z zasadą przy

14



15

18

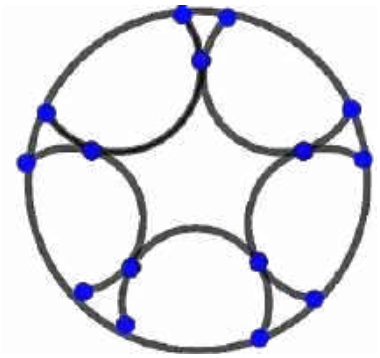


rysunku 12 – wszystkie krawędzie wychodzące z jednego wierzchołka muszą mieć inny kolor. Jeżeli uważasz, że to zbyt żmudne, to tylko odpowiedz: ilu kolorów najmniej potrzeba? To proste: spójrz na wierzchołki dużego pięciokąta.

***

Zacząłem od Pála Erdősa. O jego pracach o kolorowaniu grafów można napisać duży artykuł. Wspomnę jeden z ulubionych jego problemów, za rozwiązanie którego obiecał w 1972 roku nagrodę 500 dolarów. Była to tak zwana hipoteza Erdősa–Fabera–Lovásza. Samo sformułowanie jest dość skomplikowane, ale przytoczę je. Mamy *n* grafów pełnych (czyli takich, gdzie każdy koralik jest połączony z każdym innym). Każdy z tych grafów ma dokładnie *n* wierzchołków. Jeśli te grafy nakładają się na siebie w taki sposób, że każde dwa grafy mają co najwyżej jeden wspólny wierzchołek, to czy cały ten układ da się pokolorować, używając tylko *n* kolorów?

16



17

W 2021 roku piątka matematyków (Dong Yeap Kang, Tom Kelly, Stefan Kühn, Abhishek Methuku i Deryk Osthus) rozwiązała ten problem. Spadkobiercy wypłacili owe pół tysiąca USD, czyli po 100 na głowę; może wystarczyło na średnio wytworną kolację. Ale nie w tym tkwi wartość nagrody. Erdős był znany z tego, że „wyceniał" problemy matematyczne w zależności od ich trudności. Ceny wahały się zazwyczaj od 10 do 3000 dolarów. Za życia wypłacał je z własnej kieszeni. Sam mówił o tym z humorem, twierdząc, że wyznaczenie nagrody to sposób na skupienie uwagi młodych talentów na konkretnym zagadnieniu. Nagrody stały się tak kultowe, że dla matematyka czek podpisany przez niego (lub pośmiertne uznanie nagrody) jest wart wielokrotnie więcej niż wartość nominalna.

To optymistyczne, prawda? ■

Michał Szurek

Źródła ilustracji: rysunki 1 i 2 – Wikipedia, hasło „twierdzenie o czterech barwach". Rysunki 7, 9, 11, 17, 18 – Gemini (według poleceń autora). Pozostałe fotografie i rysunki – autor.

Dlaczego samolot leci?

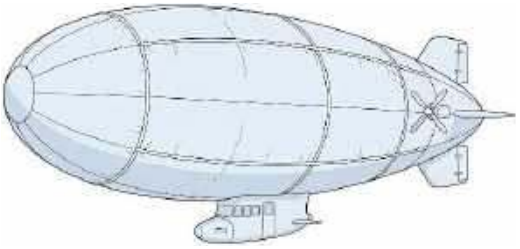
Lot w powietrzu a prawa fizyki

Samolot, jako obiekt o gęstości większej niż gęstość powietrza, nie byłby w stanie latać, gdyby nie silniki. Ale same silniki to ciągle za mało. Obecnie większość pojazdów poruszających się po powierzchni Ziemi również jest wyposażona w napęd. Niemniej pojazdy te nie wzbijają się ku niebu, nawet jeśli mogą osiągać znaczne prędkości. Ktoś może powiedzieć, że różnica wynika z tego, iż samolot ma skrzydła... i w dużej mierze będzie miał rację. To właśnie w konstrukcji skrzydeł tkwi klucz do skutecznego wzniesienia się w powietrze.

Zastanówmy się przez chwilę, jakie warunki muszą być spełnione, aby jakikolwiek obiekt oderwał się od powierzchni Ziemi. Przede wszystkim, zgodnie z zasadami dynamiki Newtona, musiałaby działać na niego siła skierowana przeciwnie do siły grawitacji i co do wartości większa od ciężaru tego ciała. W przypadku balonów wykorzystuje się siłę wyporu. Czasza wypełniona gazem o gęstości mniejszej od gęstości otaczającego ośrodka jest wypychana do góry na tej samej zasadzie, na jakiej bąbelek powietrza jest wypychany z wody.

Aby jednak balon zaczął się poruszać poziomo, musimy wykorzystać jakąś siłę działającą w wybranym kierunku, na przykład wiatr. Rozwiązaniem łączącym start w oparciu o działanie siły wyporu i poziomy ruch kontrolowany za pomocą silników jest sterowiec, którego pierwszy udany lot odbył się w 1852 roku, czyli ponad pół wieku przed pierwszym lotem samolotu.

Jeśli dokładnie przyjrzymy się rysunkowi sterowca, to zauważymy, że podczepiona pod powłoką z gazem gondola przypomina przednią część kadłuba samolotu. Niemniej podobieństwo bierze się głównie z przyczyn praktycznych. Najlepiej, jeśli gondola ma kształt stawiający jak najmniejszy opór powietrzu. Projekty samolotów rozwijały się niezależnie od projektów sterowców.



Rysunek 1. Schematyczny rysunek sterowca. Pojazd łączy cechy balonu z cechami samolotu i był pierwszą maszyną powietrzną pozwalającą na loty załogowe

Rysunek 2. Profil skrzydła samolotu i opływające go strugi powietrza

Odrobina historii

Ludzkość od bardzo dawna zdawała sobie sprawę z tego, że człowiek mógłby wznieść się w powietrze za pomocą skrzydeł. Opis takiego urządzenia znany jest mniej więcej od V wieku przed naszą erą, gdy w micie o Dedalu i Ikarze zamieniono łódź z płóciennymi żaglami (z jego wersji pierwotnej) na sztuczne skrzydła z ptasich piór i wosku.

Z czasów starożytnych pochodzą pierwsze doniesienia o anonimowych śmiałkach, którzy próbowali latać, używając konstrukcji podobnych do tych z mitu o Dedalu i Ikarze. Pierwszy potwierdzony lot człowieka odnotowano jednak dopiero w średniowieczu. W IX wieku arabski uczony i poeta, Abbas Ibn Firnas, podjął się kilku prób skonstruowania maszyny latającej. Ostatni z tych wynalazków (i pierwszy udany) miał formę ramy z drewna obciągniętej jedwabiem. Konstrukcja ta była podobna do współczesnych lotni i pozwoliła mu utrzymać się w kontrolowanym locie przez około 10 minut.

Jednak pierwszy samolot w dzisiejszym rozumieniu tego słowa został skonstruowany przez braci Wright. Był to dwupłatowiec wykonany z drewna obitego tkaniną i wyposażony w silnik. Jego pierwszy lot odbył się w 1903 roku i trwał zaledwie kilka sekund. Bardzo szybko znaleźli się kolejni konstruktorzy maszyn latających.

Siła nośna

Przyjrzyjmy się przez chwilę profilowi skrzydła na **rysunku 2**. Jak można zauważyć, jest on niesymetryczny względem osi zaznaczonej przerywaną linią. Z powodu tej asymetrii występują dwa zjawiska, które zsumowane ze sobą dają największy wkład w powstawanie siły nośnej, pchającej samolot do góry. Siła ta przeciwdziała sile ciężkości spychającej go w dół, a w fazie wznoszenia jest od niej większa co do wartości.

W układzie odniesienia związanym z samolotem powietrze porusza się względem skrzydeł z ogromną prędkością. Początkowo powietrze porusza się poziomo i, napotykając skrzydło, zaczyna je opływać. Skrzydło, ustawione pod pewnym kątem do strumienia powietrza, działa na jego cząsteczki pewną siłą skierowaną w dół. Oczywistą oznaką działania tej siły jest zmiana kierunku ruchu strumienia powietrza. Ale to nie wszystko, ponieważ zgodnie z III zasadą dynamiki Newtona, powietrze oddziałuje na skrzydło z siłą o tej samej wartości, lecz przeciwnym zwrocie, czyli skierowanym do góry.

Kolejne zjawisko wynika z tego, że strugi powietrza opływające samolot zachowują się jak ciecz. Po rozdzieleniu przez skrzydło powietrze, opływając górną powierzchnię, porusza się szybciej niż powietrze opływające stronę dolną. W efekcie powietrze znajdujące się nad skrzydłem zostaje rozrzedzone w stosunku do powietrza znajdującego się pod nim. Dzięki temu po obu stronach skrzydła powstaje różnica ciśnień. Wyższe ciśnienie panujące pod spodem skrzydła „pcha" samolot do góry.

Silniki

Silniki samolotu służą do nadania mu prędkości poziomej. Dlatego też samolot startuje po poziomym pasie i w pierwszej fazie rozpędu porusza się jak każdy inny pojazd naziemny. Opisana powyżej konstrukcja skrzydeł sprawia, że po osiągnięciu odpowiedniej prędkości wystarczy lekko unieść dziób samolotu w górę, aby siła nośna oderwała go od powierzchni Ziemi. Nie wnikając w szczegóły, siła nośna działająca na samolot rośnie wraz z kwadratem jego prędkości i jest proporcjonalna do powierzchni skrzydeł.

W przypadku szybowców, a także innych konstrukcji, takich jak lotnie i niektóre rodzaje

spadochronów, siłę nośną generuje się bez udziału silnika. Wystarczy rozpędzić szybowiec do odpowiedniej prędkości (na przykład na wyciągarce lub holując go za innym samolotem), aby wzbił się w powietrze. Potem już tylko od umiejętności pilota oraz sprzyjających warunków atmosferycznych zależy, jak długo uda mu się utrzymać maszynę w powietrzu.

Warto tutaj zauważyć, że zasada działania samolotu różni się od zasady działania sterowca. W samolocie silnik nadaje prędkość poziomą, ale ze względu na kształt skrzydła i generowaną siłę nośną to od mocy silnika zależy możliwość wznoszenia się lub opadania. W przypadku sterowca silnik odpowiada wyłącznie za ruch postępowy. Wznoszenie lub opadanie takiego pojazdu zależy wyłącznie od wartości siły wyporu, z jaką powietrze działa na wypełnioną gazem czaszę.

Co się stanie, gdy silniki zgasną?

Odpowiedź na to pytanie zależy głównie od typu samolotu i jego wielkości. Im większa powierzchnia skrzydeł samolotu w stosunku do jego masy, tym łatwiej złagodzić skutki takiej awarii. Jak już wspomnieliśmy, siłę nośną generuje ruch samolotu względem powietrza. Jeśli samolot leci z odpowiednio dużą prędkością, to nawet bez pracujących silników siła nośna ciągle jest generowana.

Problem pojawia się dopiero wtedy, gdy na skutek działania oporów ruchu prędkość samolotu maleje. Spadek prędkości przekłada się bowiem na zmniejszenie siły nośnej. W przypadku lekkich szybowców, które w ogóle nie posiadają silników, można wykorzystać wznoszące prądy powietrza, aby samolot nie tracił pułapu praktycznie przez godziny.

Jakkolwiek wydaje się to nieprawdopodobne, również maszyny wyposażone w silniki mogą się poruszać lotem szybowcowym. Znane są przypadki, gdy samoloty pasażerskie o masie kilkudziesięciu ton po awarii wszystkich silników były w stanie dotrzeć bezpiecznie do lotniska. Rekord pobili piloci lotu Air Transat, którzy w 2001 roku pokonali nad Atlantykiem 120 kilometrów, zanim posadzili maszynę w bazie wojskowej na Azorach. Nikt z załogi ani pasażerów nie ucierpiał.

Kolejny spektakularny przypadek to pokonanie 50 kilometrów lotem szybowcowym samolotu linii Air Canada w 1983 roku i wylądowanie na zamkniętym pasie startowym w nieczynnej bazie w Gimli. Pomimo że na pasie odbywał się zlot miłośników motoryzacji, nikt z uczestników zlotu nie ucierpiał. Również pasażerowie nie doznali poważniejszych obrażeń. Tylko maszyna została uszkodzona w trakcie lądowania z powodu niecałkowitego wysunięcia się podwozia oraz niewielkiego pożaru.

Sprawdź, co potrafisz

Nie wszystkie obiekty latające poruszają się na skutek działania siły nośnej. Znajdź i zaznacz te, które unoszą się w powietrzu w oparciu o inne zjawisko.

- ☐ A. balon
- ☐ B. latawiec
- ☐ C. lotnia
- ☐ D. sterowiec
- ☐ E. szybowiec
- ☐ F. śmigłowiec (helikopter)

Dla nauczyciela

Jakkolwiek pojęcie siły nośnej nie jest uwzględnione w obecnej podstawie programowej, temat sam w sobie może zostać wykorzystany zarówno w szkole podstawowej, jak i ponadpodstawowej do realizacji zagadnień związanych z zasadami dynamiki Newtona oraz z pojęciem siły wypadkowej. Lecący samolot jest doskonałym obiektem do analizy działających na niego sił: siły ciężkości i siły nośnej w kierunku pionowym oraz siły ciągu silnika i oporów ruchu w kierunku poziomym. ■

Joanna Borgensztajn

Odpowiedź do zadania: A, D

Szkoła Wynalazców

dozwolone do lat 15

Wakacje jeszcze trwają (wszak studenci mogą jeszcze korzystać), jest to okres, kiedy to szlaki turystyczne pustoszeją, a więc jest to dogodna pora do wypraw, np. w góry. Jak zwykle pojawia się problem kwiatków domowych, których doglądnięcie nie zawsze da się powierzyć zaprzyjaźnionej osobie. A więc: zaproponować system samoczynnego podlewania domowych kwiatków bez automatyki elektronicznej, tak, aby zapewniał podlewanie przez okres ok. 3 tygodni naszej nieobecności w mieszkaniu.

Zadanie należy do grupy „klasycznych", rozwiązywanych już od czasów starożytności. Wtedy też nie było automatyki, prądu i podobnych, zaawansowanych urządzeń. A jednak dawali sobie z tą sprawą radę. Zobaczmy, jak sobie z tym problemem poradzili nasi czytelnicy:

Zbigniew Góralski proponuje sposób zaczerpnięty z przyrody: wykorzystać włoskowatość. Uważa za najlepszy system postawienie sporego zbiornika z wodą nieco wyżej niż poziom doniczek i wyprowadzenie z tego zbiornika kilku knotów, po jednym do każdej doniczki. Żeby – w razie upałów – knoty nie wysychały, proponuje poprowadzić knoty w rurkach polietylenowych i zbiornik z wodą nakryć.

Sposób wydaje się najlepszy. Należy jednak zadbać o to, żeby doniczki nie zostały „przelane". To już można załatwić na kilka sposobów: dławienie knotów lub odprowadzanie nadmiaru wody z doniczek do naczynia położonego niżej. Też knotami.

Jerzy Nowak proponuje ustawienie dużego zbiornika z wodą (trzeba obliczyć zapotrzebowanie na wodę poszczególnych roślin) i na każdej rurce, którą woda spływa grawitacyjnie, zastosować zacisk, np. śrubkę z nakrętką lub inny, podobny w działaniu element.

System również prosty i niezawodny. Trzeba jednak wykonać trochę wstępnej pracy i zbilansować potrzeby roślin z pojemnością zbiornika. No cóż, nie ma nic za darmo!

Wymienionym kolegom gratulujemy i zapraszamy do kolejnych zadań.

Nowe zadanie

Wrzesień to już zapowiedź jesieni, a jednocześnie jest to czas zbierania jesiennych „darów natury". Nasi młodzi wynalazcy nie potrzebują specjalnych narzędzi i sprzętów do zbierania z ziemi różnych owoców. Ale młodzi ludzie mają dziadków, którzy dość chętnie biorą udział w tych zbiorach, ale niestety plecy zaczynają ich boleć. Stąd wasze zadanie: zaproponować proste i lekkie urządzenie do zbierania z ziemi owoców, tak, by nie być zmuszonym do działania w pochyleniu, niewygodnym i na dłuższą metę męczącym.

Chodzi o sprzęt taki, którego ideę widzimy często na ulicach i alejkach, gdy pracownicy MPO zbierają niedopałki i różne śmieci. Idea jest więc prosta, ale jabłka, śliwki, renklody to delikatne owoce; nie można ich traktować zbyt obcesowo. I to będzie główny problem do rozwiązania. Poza tym owoce trzeba gdzieś odłożyć. Jak to zrobić? To już wasz problem. Czekamy na ciekawe propozycje.

Termin nadsyłania rozwiązań – do końca września br.

Klub Wynalazców

bez ograniczeń wieku

Zadaniem waszym było: zaproponować sposób i ewentualnie pojemnik na płyn „po goleniu", taki, żeby nie mógł trafić do oczu, a jednocześnie pozwalał na zwilżenie twarzy, oszczędzając płyn, który nie powinien trafiać na podłogę.

Aż dziwne jest, że producenci większości płynów „po goleniu" zupełnie lekceważą problem ekonomii zużycia płynu, a przede wszystkim sprawę bezpieczeństwa dla oczu – ważne przy butelkach z atomizerem lub płynem w sprayu. Nie życzymy nikomu źle, ale proszę sobie wyobrazić taką oto sytuację: mężczyzna goli się, zmywa twarz wodą, suszy ręcznikiem, po czym zwilża twarz płynem po goleniu z butelki z atomizerem. W pośpiechu trochę płynu trafia do oka. Zmywa twarz i oko, jednak trochę płynu zostaje. Oko pieczе. Idzie do pracy i parę godzin męczy się z tym okiem i po pracy ma zamiar skorzystać z pomocy lekarza okulisty. Okazuje się, że musi mieć skierowanie od lekarza „pierwszego kontaktu". Będzie miał duże szczęście, jeśli uda mu się dostać do lekarza po południu. Dostaje skierowanie i rejestruje się do okulisty – otrzymuje termin: za dwa miesiące (przy ogromnym szczęściu!). To jest sytuacja prawdziwa. Wszystko przez to, że zdaniem „władz od zdrowia", np. inżynier – „nieuk medyczny" nie rozróżnia oka od – pupy! Dlatego wasze zadanie jest naprawdę ważne! Zobaczmy, jak sobie z tym „nierozwiązywalnym" dla producentów kosmetyków poradzili nasi czytelnicy:

Ryszard Bogucki – uważa, że najlepszym rozwiązaniem byłby pojemnik przypominający butelkę do pasty do butów z miękkim aplikatorem gąbkowym na końcu. Podobne rozwiązanie mają niektóre pasty do butów. Dla płynu po goleniu należałoby starannie dobrać rodzaj gąbki, spełniającej warunki kosmetyczne i sanitarne.

Chyba najlepszy i w zasadzie znany pomysł – sprawdzony przy paście do butów. Ważny jest – jak to kolega podkreślił – dobór właściwej gąbki, ale to chyba nie będzie problemem.

Marek Piwowarczyk – proponuje „pędzel po goleniu" z wewnętrznym zbiorniczkiem na płyn. Pędzel mógłby być wielokrotnego użytku, do zbiorniczka wlewałoby się kolejne porcje płynu. Ilość płynu podawanego na syntetyczne włosie regulowałoby się dławikiem, pokręcając pokrętłem lub w innym systemie, np. przesuwając suwak, jak w kroplówkach.

Bardzo dobry pomysł i wygodny dla producentów kosmetyków; nie musieliby nadal nic robić, bo taki pędzel mógłby produkować ktoś inny.

Włodzimierz Zamorski – zobaczył w jednej z audycji reklamowych prosty sprzęt do malowania mieszkań. Sprzęt to rolka z gąbki, pusta wewnątrz, do której wlewa się farbę. Przetaczając rolkę po twarzy, naciskiem na rolkę reguluje się ilość płynu. Nic nie kapie ani nie bryzga!

Również dobry pomysł! – nawiasem mówiąc, jest to przykład tzw. benchmarkingu, czyli przeniesienia idei jednego rozwiązania na inny obiekt spełniający podobną rolę.

Kolegom gratulujemy i zachęcamy do rozwiązywania kolejnych problemów.

Nowe zadanie

Wszyscy wiemy, że segregacja odpadków domowych, biurowych itp. jest konieczna, ale wiemy też, że jest uciążliwa. Może, gdyby pomyśleć, dałoby się opracować pojemnik, do którego wrzucamy odpadki „jak leci", a on sam segreguje i rozdziela na 3...4 komory. Oczywiście natychmiast mamy na oku systemy komputerowe, ale redukując pracę przy segregacji do minimum, może udałoby się opracować pojemnik półsamoczynny, ułatwiający dokuczliwą pracę... A więc: zaproponować konstrukcję domowego lub biurowego kosza, który sam ułatwia segregację odpadów, ogranicza wydobywanie się zapachów i zmniejsza objętość śmieci, ale nie wykorzystuje zasilania elektrycznego.

Sądzę, że można by się zgodzić na zasilanie bateryjne, ale to wszystko. System powinien działać półsamoczynnie i skutecznie. Nie powinien być też gabarytowo wielki, bo większość mieszkań to jednak „mini klitki". Przypominam o terminie nadsyłania propozycji: do końca września br.

Vademecum Młodego Wynalazcy

Jak powstaje wynalazek? Skąd biorą się nowe pomysły i gdzie ich szukać?

Powszechnie powtarza się powiedzenie, że „potrzeba jest matką wynalazku". Jest w nim wiele prawdy, ponieważ ogromna liczba wynalazków rzeczywiście powstała po to, aby rozwiązać konkretny problem. Człowiek zauważa trudność, niedogodność lub stratę czasu i zaczyna szukać lepszego rozwiązania. Tak narodziły się tysiące urządzeń, narzędzi i technologii. Nie jest to jednak jedyna droga prowadząca do wynalazku.

Historia techniki pokazuje, że nowe pomysły pojawiają się z bardzo różnych powodów. Czasami wynalazca chce po prostu zarobić pieniądze i świadomie poszukuje produktu, na który znajdzie się wielu klientów. Innym razem inspiracją jest przypadkowa obserwacja, hobby, marzenie senne, zainteresowanie nauką albo chęć udowodnienia, że coś da się zrobić lepiej niż dotychczas.

Dobrym przykładem jest odkrycie zjawisk naukowych, które początkowo nie miały żadnego praktycznego zastosowania. Kiedy fizycy badali elektryczność czy fale radiowe, niewielu przewidywało, że powstaną telefony komórkowe, internet i nawigacja satelitarna. Najpierw pojawiła się ciekawość poznawcza, a dopiero później zastosowania techniczne.

Wynalazek bardzo rzadko jest efektem nagłego olśnienia. Zwykle poprzedzają go lata obserwacji, doświadczeń i rozmyślań. Nawet jeśli ktoś mówi: „wpadłem na pomysł pod prysznicem" albo „przyśniło mi się rozwiązanie", to taki błysk jest najczęściej końcowym etapem dłuższego procesu zachodzącego w umyśle.

Jak definiować potrzeby?

Pierwszym krokiem jest nauczenie się dostrzegania problemów. Większość ludzi przyzwyczaja się do niedogodności i przestaje je zauważać. Wynalazca postępuje odwrotnie – zadaje pytania.

- Co zajmuje zbyt dużo czasu?
- Co jest niewygodne?
- Co często się psuje?
- Co kosztuje więcej niż powinno?
- Jakie czynności wymagają nadmiernego wysiłku?
- Gdzie użytkownicy najczęściej popełniają błędy?

Jeżeli jakaś czynność wywołuje irytację u milionów ludzi, istnieje duża szansa, że jej usprawnienie może mieć wartość rynkową.

Przykładowo ktoś zauważa, że osoby starsze mają problem z otwieraniem słoików. To jeszcze nie jest wynalazek. Jest to jednak dobrze zdefiniowana potrzeba. Dopiero później rozpoczyna się poszukiwanie rozwiązania: specjalnego uchwytu, mechanizmu wspomagającego lub zupełnie nowego rodzaju zamknięcia.

Gdzie szukać pomysłów?

Najwięcej okazji do wynalazków znajduje się tam, gdzie występuje duża liczba użytkowników i częste problemy.

Do najbardziej obiecujących obszarów należą:

- Zdrowie i rehabilitacja – starzenie się społeczeństw – powoduje wzrost zapotrzebowania na urządzenia wspomagające osoby starsze i niepełnosprawne.
- Konieczność oszczędzania energii – rosnące ceny energii sprawiają, że każda technologia zmniejszająca zużycie prądu, gazu lub paliwa może znaleźć odbiorców.
- Transport i logistyka – nawet niewielkie usprawnienie pozwalające skrócić czas transportu lub zmniejszyć koszty bywa bardzo wartościowe.
- Bezpieczeństwo – ludzie są skłonni płacić za rozwiązania zwiększające bezpieczeństwo domu, samochodu czy miejsca pracy.
- Rolnictwo – nowoczesne rolnictwo coraz bardziej wykorzystuje automatykę, czujniki i sztuczną inteligencję.
- Codzienne przedmioty – nie należy lekceważyć prostych produktów. Czasami niewielka modyfikacja zwykłego narzędzia lub opakowania przynosi większe zyski niż skomplikowane urządzenie elektroniczne.

Jak myśli wynalazca?

Przydatną metodą jest zadawanie sobie pytań typu:

- Co można usunąć?
- Co można połączyć?
- Co można zmniejszyć?
- Co można powiększyć?
- Co można zautomatyzować?
- Czy da się wykorzystać inne zjawisko fizyczne?

Przykładowo, jeśli urządzenie zawiera dziesięć części, warto zastanowić się, czy nie da się zastąpić ich pięcioma. Mniejsza liczba elementów oznacza zwykle niższe koszty produkcji i większą niezawodność.

Czy warto śledzić cudze wynalazki?

Zdecydowanie tak. Wielu początkujących wynalazców popełnia błąd polegający na unikaniu kontaktu z istniejącymi rozwiązaniami z obawy przed „skażeniem pomysłu". Tymczasem znajomość stanu techniki jest konieczna.

Przeglądając patenty i nowe produkty, można zauważyć ich słabe strony. Bardzo wiele wynalazków nie polega na stworzeniu czegoś całkowicie nowego, lecz na znaczącym ulepszeniu istniejących rozwiązań.

Wynalazek a biznes

Technicznie doskonały pomysł nie zawsze odnosi sukces rynkowy. Należy odpowiedzieć na kilka pytań:

- Kto będzie klientem?
- Ile osób ma dany problem?
- Ile są gotowe zapłacić za rozwiązanie?
- Czy produkt można produkować tanio?
- Czy istnieje konkurencja?

Nierzadko prosty produkt rozwiązujący powszechny problem okazuje się bardziej dochodowy niż skomplikowana technologia przeznaczona dla niewielkiej grupy odbiorców.

Znaczenie wytrwałości

Największym sekretem wynalazczości nie jest geniusz, lecz wytrwałość. Pierwsze wersje urządzeń niemal zawsze działają niedoskonale. Konieczne są poprawki, testy i kolejne próby. Wielu znanych wynalazców podkreślało, że sukces był rezultatem setek nieudanych eksperymentów. Dlatego osoba poszukująca wynalazku powinna przede wszystkim nauczyć się obserwować świat. Problemy są wszędzie: w domu, pracy, transporcie, medycynie, rolnictwie i rozrywce. Każda niedogodność może stać się początkiem nowego rozwiązania. Wynalazek rodzi się


1

wtedy, gdy ktoś nie godzi się na istniejący stan rzeczy i zadaje proste pytanie: „Czy nie dałoby się zrobić tego lepiej?". Od takiego pytania zaczyna się większość wielkich i małych odkryć, które później zmieniają codzienne życie milionów ludzi.

Pomysł już jest i co dalej?

Szereg wynalazków powstaje „nie wiadomo po co" i powstaje problem, jak to zrobić i do czego się to przyda itp. Nie ma wyraźnej przyczyny – tej „matki" wynalazków. Czy są takie wynalazki? Oczywiście, że są. Pierwszym z brzegu może być słynna „kostka Rubika". Jest to po prostu zabawka logiczna, której atrakcyjność polega na tym, że jej elementy są przestawiane nie ortogonalnie, lecz biegunowo. A w „te klocki" człowiek jest przeciętnie znacznie gorszy niż w układankach ortogonalnych. Skąd wzięła się idea tej sławnej kostki? W 1974 roku w głowie węgierskiego architekta, Ernő Rubika (**1**), narodził się pomysł, który miał wkrótce opanować cały świat.

Pierwotnie nie była to zabawka. Prototyp zbudowany z drewna, którego elementy były spięte gumkami „recepturkami", miał służyć studentom w zrozumieniu przestrzeni 3D. Kiedy jednak po raz pierwszy pomieszał kolory

swojego wynalazku, zorientował się, że stworzył prawdziwego potwora. Samemu twórcy znalezienie drogi powrotnej do startowego układu zajęło... bity miesiąc!

Wkrótce okazało się, że mimo woli stworzył „matematycznego potwora". Nie wdając się w szczegóły, bo te znaleźć można w Internecie, wystarczy podać jedną liczbę: otóż gdyby ułożyć kostki jedna na drugiej, w ilości odpowiadającej liczbie możliwych kombinacji, to byłaby to „wieża" o wysokości równej ponad 246 lat świetlnych! To 60 razy dalej niż prosto z Ziemi do gwiazdy Proxima Centauri! Ale nie o to nam tutaj chodzi. Potraktujmy kostkę jako wynalazek, czym w istocie jest. Jest to bowiem ideał wynalazków, marzenie wielu wynalazców. Szacuje się, że na całym świecie od początku wyprodukowano ponad 400 milionów egzemplarzy tej kostki. Gdyby jego zarobek na jednej kostce wynosił 1 złotówkę, to zarobiłby 400 mln złotych.

Zasada działania kostki jest od pierwszej chwili jasna, ale jak zrobić ją taką, żeby ściany obracały się dokoła trzech osi i całość nie rozlatywała się przy pierwszej próbie? Jak wiadomo, Rubik te problemy pokonał i zrobił coś, co z miejsca podbiło cały świat.

Innym przykładem wynalazku, który „zdobył świat", może być karabinek AK-47 AKM (2), Michaiła Kałasznikowa. Karabinek ten w wersji podstawowej i zmodernizowanej (AKM) został wyprodukowany w ilości ok. 150 milionów egzemplarzy, licząc szacunkowo egzemplarze produkowane na podstawie licencji i te produkowane nielegalnie. Na tym wynalazku Michaił Kałasznikow nie zarobił prawie nic, nie

2

licząc okazjonalnych nagród i... medali, których władza mu nie szczędziła.

Karabinek ten – oczywiście „służący do obrony" – cieszył się dużym popytem, wymuszanym przez wzajemne obawy potencjalnych stron konfliktów zbrojnych. A tak już na świecie jest, że największe nakłady są kierowane na narzędzia wzajemnego mordowania się ludzi, którzy nie potrafią żyć w pokoju i przyjaźni.

Inne naprawdę masowo produkowane rzeczy to dziś przede wszystkim telefon komórkowy – smartfon. Łącznie, w skali globalnej licząc, komórkek i smartfonów wyprodukowano około 30 miliardów egzemplarzy. Coraz gęstsza sieć połączeniowa, stosunkowo niska cena (z wyłączeniem egzemplarzy luksusowych) i powszechna potrzeba wzajemnego kontaktu ludzi są motorem napędzającym produkcję i sprzedaż tego sprzętu. Należy tu oczywiście dodać, że współczesne smartfony ze swoją ofertą programową daleko wyprzedzają komputery z lat 90.

I zasadniczym pytaniem jest problem: jakie będą smartfony za 25 lat? Może wreszcie będą „prały i prasowały koszule" – jak to przewidują niektórzy futuryści – dowcipnisie? ■

Prezes Klubu Wynalazców
Champion TRIZ
Jan Boratyński

Jak nakarmić świat
Historia i przyszłość żywności
Vaclav Smil

Wydawnictwo: Insignis, stron: 352, sugerowana cena: 54,99 zł

Nigdy wcześniej nie musieliśmy wyżywić tylu ludzi co dziś. Jak globalne potrzeby żywnościowe wpływają na nasze życie? Dlaczego niektórzy z największych producentów żywności na świecie to jednocześnie kraje z największym odsetkiem ludności niedożywionej? Dlaczego marnujemy tak ogromne ilości jedzenia i jak można temu zaradzić? Czy wszyscy moglibyśmy przejść na dietę wegańską i cieszyć się zdrowiem? A co najważniejsze – czy powinniśmy? Wybitny naukowiec Vaclav Smil odpowiada nie tylko na te pytania. Rozprawia się z mitami i objaśnia, skąd naprawdę bierze się żywność. Opisując dzieje globalnej produkcji jedzenia, wyjaśnia, dlaczego hodujemy te, a nie inne gatunki zwierząt, jak doszło do tego, że większość kalorii spożywanych na świecie pochodzi z zaledwie kilku produktów oraz jak może się to zmienić w przyszłości.

Pomysły genialne, zwariowane i takie sobie

Genialne w swej prostocie: **6 innowacyjnych pomysłów Czytelników, które mogą zmienić naszą codzienność**

Prezentujemy najciekawsze propozycje nadesłane do naszej redakcji w ostatnim miesiącu. Od ekologii, przez ogrodnictwo, aż po wsparcie dla seniorów – oto dowód na to, że kreatywność nie zna granic.

Piotr Wojciechowski – inteligentna laska dla seniora i osób niepełnosprawnych, niewidomych i z zaburzeniami równowagi. Piotr uważa, że jedyna specjalna laska dla osób niepełnosprawnych istnieje w wersji biernej, jako biała laska dla osób niewidomych. Uważa, że nowoczesna laska powinna świecić o zmroku, sygnalizować upadek lub puszczenie z dłoni, powinna mieć możliwość porozumienia się z osobami, które mogłyby pomóc.

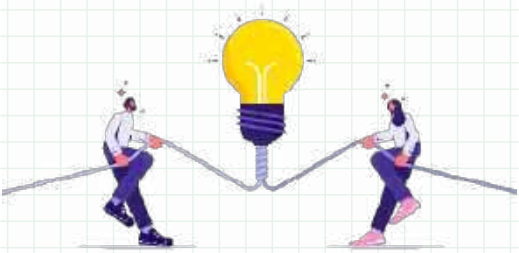
Urządzenia pełniące podobną funkcję już częściowo są. Są to tzw. „opaski bezpieczeństwa", mające formę zegarka na rękę, które sygnalizują stan alarmowy, np. przy upadku, umożliwiają dwukierunkową łączność. Laska z natury rzeczy ma jeszcze jedną funkcję: pozwala utrzymać pewniejszy chód. Dodanie jej funkcji zaproponowanych przez Piotra istotnie poprawiłby jej użyteczność.

Tomasz Rutkowski – biorąc udział w imprezach masowych, np. jak mecz piłkarski, zauważył, że przy wychodzeniu ze stadionu podczas deszczu, gdy kibice i widzowie chodzą pod parasolami, dochodzi do częstych kolizji parasoli, które prowadzą do ich uszkodzeń i często gwałtownych reakcji ich właścicieli. Nowoczesny parasol powinien reagować na taką sytuację i częściowo się składać lub odchylać, powinien też reagować na silne podmuchy wiatru.

Pomysł niemal genialny i pozostaje jedynie zadanie: jak to zrealizować? Być może dałoby się wykorzystać echolokację taką, jaką mają nietoperze. Przestudiowanie osiągnięć bioniki może dałoby jakiś kierunek.

Władysław Solecki – proponuje opracowanie domowej prasy do zgniatania i formowania jesiennych liści w brykiety. Brykiety takie można by wykorzystać jako materiał opałowy, izolacyjny lub do innych potrzeb. Liście „luzem" zazwyczaj trafiają do ogniska lub na kompost, gdzie muszą dość długo leżeć, żeby mogły się całkowicie rozłożyć.

Jeśli to ma być prasa domowa, to warto pomyśleć o wykorzystaniu takich urządzeń jak podnośnik samochodowy. Urządzenie takie w wersji hydraulicznej może wywrzeć znaczną siłę i przez dobudowanie prostej skrzynki stalowej z dnem uruchamianym podnośnikiem, mogłoby taką funkcję pełnić. Pomysł wart rozważenia.



Monika Zawistowska – jest wielbicielką kotów i ma w swoim mieszkaniu dwa koty. Właściwie dobrze zna swoje zwierzaki i na ogół wie, co oznaczają ich zachowania. Jednakże marzy jej się sprzęt, który mógłby dokładniej sygnalizować nastrój kota, np. „nudzi mi się", „daj coś dobrego zamiast zwykłej karmy", „pobaw się ze mną" itd.

Wzruszająca dbałość o komfort, także psychiczny. Taki „tłumacz kociego języka" jest do zrobienia. Kwestią zasadniczą jest rynek: nie może to być drogie urządzenie i nie może być zbyt inwazyjne w stosunku do kotów no i czy jest popyt na takie coś.

Mateusz Brzozowski – wiadomo, że w dziedzinie badania ludzkich marzeń sennych w ostatnich latach nastąpił znaczny postęp. Mateuszowi, który nie pamięta swoich – jak twierdzi – bardzo ciekawych snów – marzy się aparatura, która zapisywałaby treść marzeń sennych i pozwalała na odtworzenie ich już na jawie.

Pewne elementy snów można już dzisiaj zapisać, ale nie bardzo jeszcze oddają one treść marzeń sennych. Wierzymy jednak w potęgę elektroniki i – być moze – za parę lat coś takiego się pojawi.

Zygmunt Sierpiński – uważa, że zimy u nas bywają ostre i w mieszkaniach budowanych jeszcze 30...40 lat temu, mimo nakładania warstwy termoizolacyjnej, sporo ciepła idzie w mur. Częściowo można te straty ograniczyć, podkładając pod grzejnik folię termoizolacyjnyą, ale to tylko półśrodek. Zygmunt proponuje opracowanie urządzenia, które odbierałoby całe ciepło oddane w kierunku ściany i następnie prezkierowałoby je do wnętrza mieszkania.

Koncepcja interesująca, pod warunkiem, że koszt urządzenia nie będzie zaporowy. Wydaje się jednak, że lepsza izolacja grzejnika od całej ściany, mogłaby dać porównywalny efekt.

Peryskopy MT-ZPT 26/09

Dziś „Na warsztacie” stosunkowo nietrudne w realizacji modele dydaktyczne, opracowane i „przetestowane w warunkach trzecioklasowych” ;) specjalnie do zastosowań na zajęciach praktyczno-technicznych, które to zajęcia po dwóch dekadach nieobecności już od najbliższego września powracają do klas od czwartej do szóstej polskich szkół podstawowych!

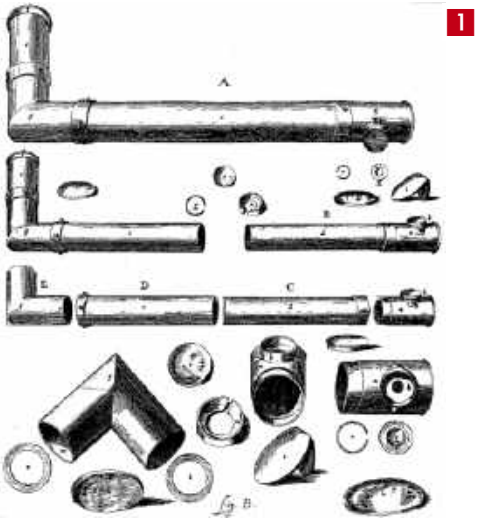
Dwa łuty historii peryskopów

Łut szczęścia najpewniej nie będzie potrzebny do prawidłowego wykonania dzisiejszych modeli, ale warto poznać kilka faktów związanych z wynalezieniem naszych dzisiejszych nawarsztatowych bohaterów.

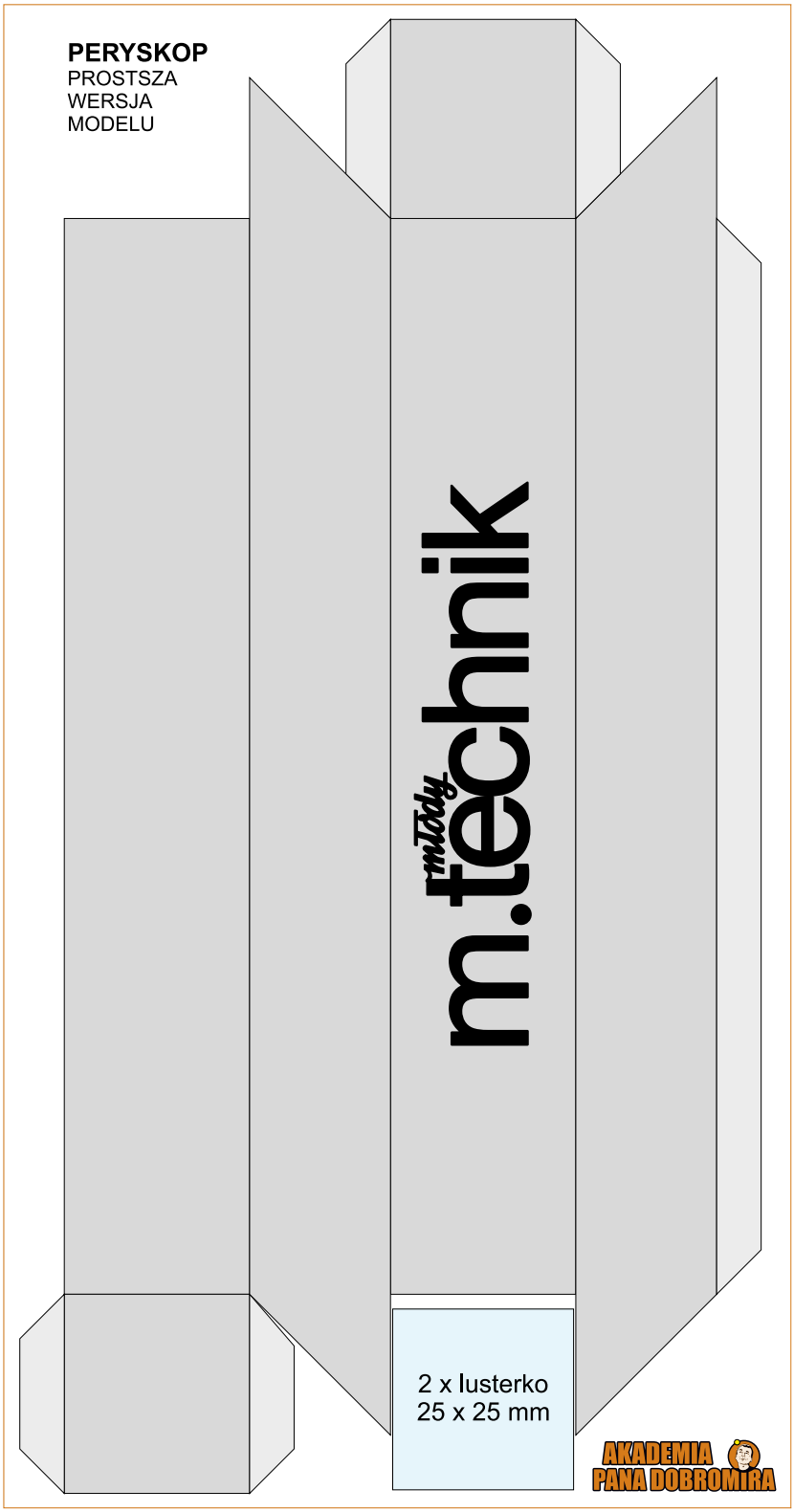
Trudno dziś ustalić, kto pierwszy zauważył, że dwa odpowiednio ustawione lustra pozwalają „widzieć zygzakiem” – bo przecież lustra kamienne znane są od co najmniej 6 tysięcy lat, metalowe od 3 tysięcy, a szklanych używali starożytni Rzymianie już 2 tysiące lat temu.

Łut – dawna jednostka masy używana w Europie od średniowiecza do końca XIX w.
W zależności od miejsca i czasu oznaczało to od **10 do 50 gramów**.
1 łut to **1/16 grzywny** lub **1/32 funta**.
System staropolski: ok. **12,7 g**.
System nowopolski: **12,672 g**.

Po raz pierwszy przyrząd najbliższy dzisiejszemu wyobrażeniu peryskopu opracował w 1637 roku Jan Heweliusz [1] i nazwał go polemoskopem (co znaczyło „dalekowid polowy”).



1



Ciekawostka: swój wynalazek (oraz m.in. lunety i mikroskop) słynny gdański astronom podarował Janowi III Sobieskiemu (wówczas dopiero Marszałkowi Wielkiemu Koronnemu), którego gościł w swoim obserwatorium. Polemoskop Heweliusza był używany do obserwacji pola bitwy zza przeszkód terenowych.

W późniejszym czasie wielokrotnie (często od nowa) wracano do tego pomysłu. W 1854 roku Francuz Marie-Davy opracował tubę obserwacyjną z dwoma lustrami dla okrętów podwodnych. W 1872 roku lustra zastąpione zostały doskonalszymi pryzmatami. Dopiero pod koniec XIX wieku Simon Lake skonstruował w Ameryce peryskop składany, który nazwał omniskopem lub skalomniskopem. Wkrótce potem opracowano konstrukcję peryskopu wysuwanego, który jeszcze lepiej sprawdzał się w okrętach podwodnych. Łącząc dwa peryskopy w zintegrowaną parę, można było uzyskać przyrząd 3 w 1: dalmierz, lornetkę i urządzenie do bezpiecznego podglądu pola walki zza bezpiecznej przegrody.

Mówiąc o peryskopach, które powszechnie używane były także w obydwu wojnach światowych, nie można nie wspomnieć o wynalezionym na początku lat trzydziestych ubiegłego wieku przez polskiego inżyniera Rudolfa Gundlacha peryskopie odwracalnym, który pozwalał w ciasnych wnętrzach czołgów na obserwację w zakresie 360 stopni bez konieczności obracania się wokół osi optycznej. Polski patent został wprawdzie kupiony przez Anglików, ale już przez III Rzeszę oraz ZSRR zwyczajnie wykradziony. Używany był powszechnie w kolejnych czołgach na wszystkich frontach II wojny światowej


3

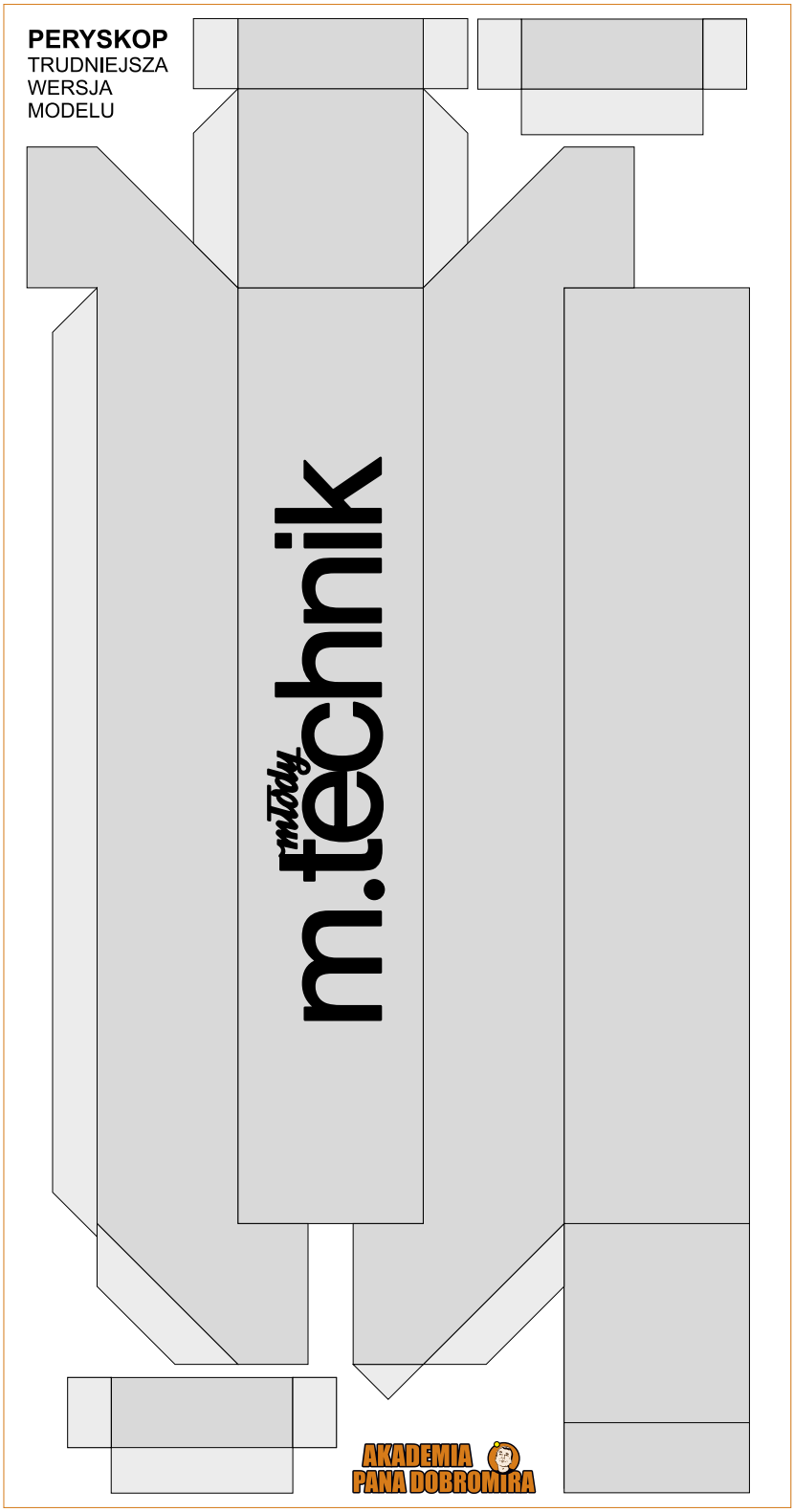
– możemy go zobaczyć np. w kadrze z serialu o „Czterech pancernych" [2].

Choć wciąż udoskonalane peryskopy miały przede wszystkim zastosowanie militarne (z nieporównywalnie bardziej zaawansowaną w stosunku do wyłącznie lustrzanej optyką [3]), a nawet kosmiczne (np. w Sojuzie 19 [4]), i w ostatnich latach zostały praktycznie wyparte przez coraz


2


4

PERYSKOP
TRUDNIEJSZA
WERSJA
MODELU



Podstawa programowa zajęć praktyczno-technicznych na r. szk. 2026/2027
https://www.mac.pl/szkola-podstawowa/zpt-2026

doskonalsze i coraz tańsze kamery cyfrowe, to ich najprostsze wersje używane są do dziś na przykład jako pozwalające patrzeć ponad tłumem gadżety reklamowe na imprezach masowych, zabawki oraz doskonałe środki dydaktyczne z zakresu podstaw optyki.

Zetpetowo-młodotechnikowe peryskopy

Peryskopy pokazane na rysunkach [A] i [B] są opracowane w dwóch wariantach, różniących się stopniem skomplikowania i zewnętrznym wyglądem. Prostszy peryskop nie posiada osłon okularu (na dole) i okienka (na górze), natomiast nieco bardziej skomplikowany zdecydowanie bardziej przypomina użytkowe peryskopy, które kojarzymy choćby z filmów.

Modele te można wykonać w trakcie zajęć praktyczno-technicznych przy użyciu niewielu narzędzi, niedużym kosztem, jednocześnie ucząc się optyki, trenując umiejętności manualne oraz krytyczne spojrzenie na własną pracę, dokładność i staranność jej wykonania.

Materiały i narzędzia

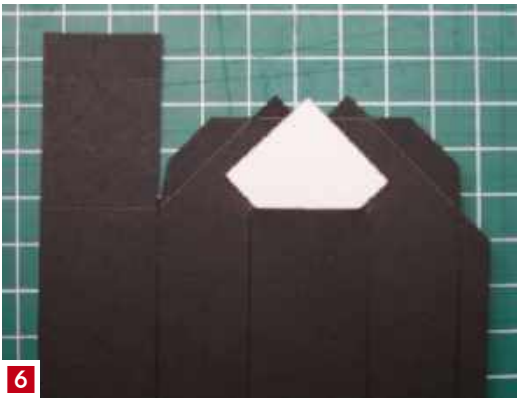
Do zbudowania modeli, które są tematem dzisiejszego „Na warsztacie", potrzebne będą:

- lusterka 25×25 mm z tworzywa sztucznego (można je kupić jako elementy do samodzielnego tworzenia na przykład kul dyskotekowych);
- brystol 160...250 g/m^2,
- nożyczki,
- igła do bigowania,
- linijka min. 30 cm,
- klej PVA (typu wikol, magic itp.);

Przydatna może być również listewka o przekroju około 8×8 mm, ułatwiająca docisk podczas klejenia najdłuższej sklejki.

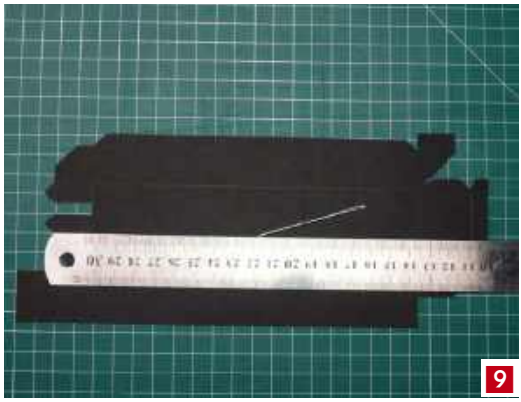
Przygotowania do budowy opisanych poniżej modeli peryskopów warto zacząć od przygotowania wydruków. Można je skopiować bezpośrednio ze stron naszego miesięcznika ew. nieodpłatnie


5


6


7


8


9


10


11


12

uzyskać bezpośrednio od autora (pisząc na adres pandobromir@gmail.com). Dobrze jest wydrukować je na czarnym brystolu (linie i tak będą zupełnie dobrze widoczne), ponieważ czarne wnętrze peryskopu (a ściślej: kolor ten) absorbuje światło, zapobiegając powstawaniu odbić światła i poprawiając komfort użytkowania przyrządu.

Montaż modelu

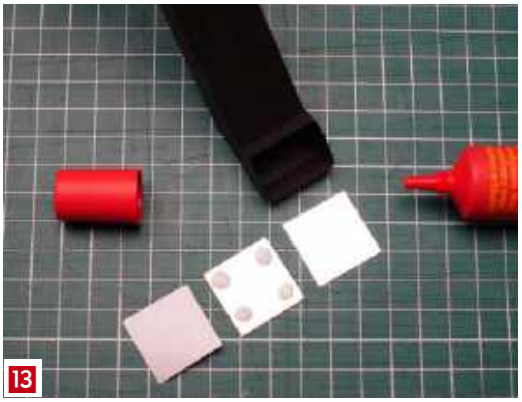
Po wydrukowaniu formatek [5], zadaniem wykonawców jest staranne wycięcie po obrysie elementów modelu. Przy wycinaniu trudniejszego wzoru modelu warto zwrócić uwagę na nacięcia przy okularze [6] oraz okienku peryskopu [7].

Następnym krokiem jest precyzyjne zbigowanie krawędzi, ułatwiające dokładne zagięcie elementów w określonych miejscach. Do zbigowania warto użyć grubych igieł do szycia ręcznego (nie muszą być szczególnie ostre), ewentualnie szydeł lub rzutek do darta z metalowymi końcówkami. Bigowanie należy przeprowadzać przy linijce, prowadząc igłę możliwie płasko, równolegle do krawędzi linijki [9]. Nie wolno tutaj zanadto oszczędzać na precyzji. Zagięte elementy obu wersji peryskopu pokazuje zdjęcie numer [10].

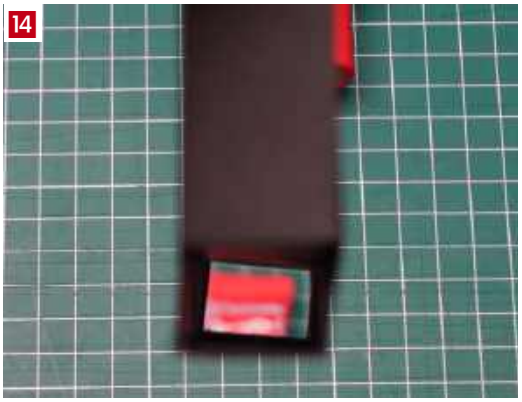
Warto zwrócić uwagę na dodatkowe dwa elementy, które nieco przypominają ławeczki, które następnie będą wypełniać górną i dolną część okularu i okienka w wersji trudniejszej peryskopu [11].

Sklejanie najlepiej rozpocząć od najdłuższej sklejki, stopniowo przechodząc do kolejnych skrajnych sklejek. Ostatnimi elementami, które przykleja się do nieco bardziej skomplikowanej wersji peryskopu, są tak zwane ławeczki [12].

Klejenie luster jest ostatnim krokiem montażu modeli. Polimerowe lusterka użyte do budowy tych modeli mają wymiar 2,5×2,5 cm, z jednej strony chronione są folią, z drugiej papierem zabezpieczającym klej. Mimo zastosowania w nich folii samoprzylepnej, lepsze efekty daje jednak podklejenie luster za pomocą kleju PVA, ponieważ dociskanie luster powoduje ich zabrudzenie oraz wygięcie [13]. O ile pierwsze można usunąć za pomocą wacików kosmetycznych, o tyle deformacja lusterka



13



14

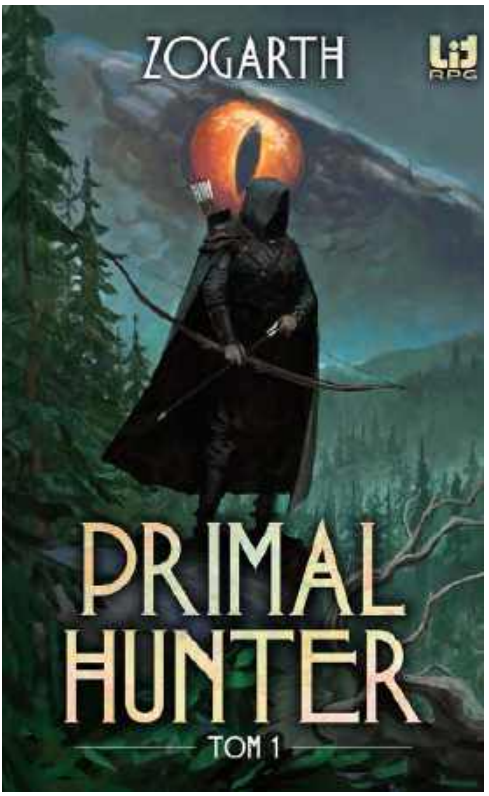
jest trudna do wyeliminowania. Przede wszystkim nieporównywalnie bardziej zniekształca ona obraz widziany przez model peryskopu. Najlepiej jest po nałożeniu kleju, wykorzystując samoprzylepną stronę luster, nanieść je za pomocą igiełki stosowanej do bigowania.

Weryfikacja prawidłowości sklejenia nastąpi już za chwilę. Dobrze sklejony model pozwala na oglądanie niezdeformowanego obrazu przez oba lusterka.

Podsumowanie

Na zakończenie tradycyjnie życzę wszystkim Wykonawcom młodotechnikowych modeli peryskopów satysfakcji ze zrealizowanego własnoręcznie projektu, natomiast Nauczycielkom i Nauczycielom ZPT – udanych zajęć z wykorzystaniem wielu tematów publikowanych w dziale „Na warsztacie" (ich specjalne wersje cyfrowe można nabyć w sklepiku Wydawnictwa AVT). W razie potrzeby wszystkich zachęcam także do dzielenia się swoimi sukcesami w tej materii via e-mail. ■

P. Dobromir



Primal Hunter
Zogarth
Wydawnictwo: Insignis,
Cykl: The Primal Hunter (tom 1),
stron: 768, sugerowana cena: 79,99 zł

„Primal Hunter" – jedna z najpopularniejszych serii LitRPG na świecie – w końcu trafia do Polski!
Wkrocz do niesamowitego uniwersum stworzonego przez tajemniczego Zogartha, który uciekł z korpoświata, by poświęcić się pisaniu! To miał być kolejny zwyczajny dzień w biurze. Nic nie zapowiadało, że to właśnie dziś wydarzy się coś przerażającego... Wszechświat osiągnął próg, o którego istnieniu ludzkość nie miała pojęcia. Oto nadszedł czas integracji z ogromnym multiwersum. Pieniądze, stanowiska i dotychczasowe zasady – to wszystko traci na znaczeniu. Tu liczy się tylko siła. Jake, z pozoru niczym niewyróżniający się pracownik biurowy, trafia do tajemniczego lasu pełnego potworów, pułapek i ludzi, którym coraz trudniej zaufać. Rozpoczyna się gra, ale nie z tych wybaczających błędy. Każde spotkanie może skończyć się śmiercią, a każde podjęte ryzyko może okazać się szansą. Jake powinien się bać. Powinien szukać drogi ucieczki. Tymczasem odkrywa, że w świecie, którym rządzą przemoc, instynkt i obsesja nieustannego rozwoju, odnajduje się lepiej, niż kiedykolwiek przypuszczał.
Może Jake nie został wrzucony do koszmaru.
Może wreszcie trafił tam, gdzie od zawsze było jego miejsce.

Zapis dźwięku

Od rysika kreślącego drgania na sadzy do pliku, który waży mniej niż zdjęcie

Przez całe dzieje ludzkości dźwięk był zjawiskiem nietrwałym: zabrzmiał i przestawał istnieć. Wszystko, co wiemy o muzyce sprzed połowy XIX wieku, wiemy z nut, opisów i instrumentów – nie z brzmienia. Zmieniło się to w ciągu jednego pokolenia, i to nie za sprawą jednego odkrycia, lecz łańcucha pomysłów, z których każdy rozwiązywał inny problem: jak dźwięk zapisać, jak go odtworzyć, jak powielić zapis, jak go zmontować i wreszcie jak go zmniejszyć na tyle, żeby zmieścił się w kieszeni.

Muzyka bez muzyka

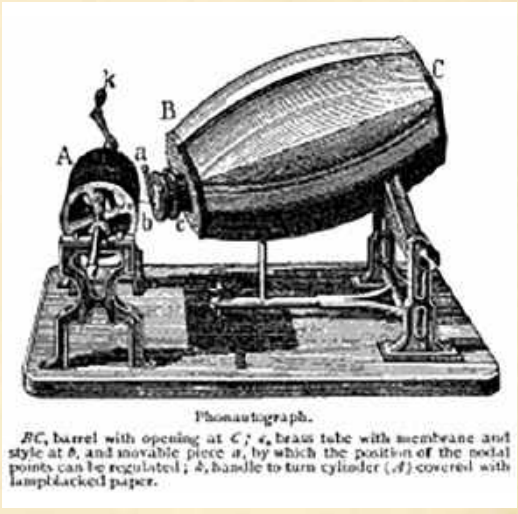
Urządzenia odtwarzające muzykę samodzielnie pojawiły się na długo przed jakimkolwiek zapisem dźwięku, ale nie mają z nim nic wspólnego. Pozytywka z bębenkiem najeżonym kołkami, katarynka z wałkiem sterującym piszczałkami czy kurant w wieży ratusza przechowywały nie dźwięk, lecz instrukcję jego wykonania – dokładnie tak jak nuty. Mechanizm wytwarzał dźwięk od nowa przy każdym uruchomieniu.

Żeby zapisać samo brzmienie, trzeba było wiedzieć, czym ono jest. Fizyka XIX wieku dała odpowiedź: dźwięk to fala zagęszczeń i rozrzedzeń powietrza, więc każdemu dźwiękowi odpowiada określony kształt fali – a kształt można narysować. To spostrzeżenie jest punktem wyjścia dla wszystkiego, co nastąpiło potem, łącznie z odtwarzaczem w telefonie.

Zapis, którego nikt nie umiał odsłuchać

W 1857 roku francuski zecer i księgarz Édouard-Léon Scott de Martinville opatentował fonautograf. Urządzenie było zaskakująco proste: tuba zbierająca dźwięk, zamykająca ją membrana z pergaminu i przymocowana do niej szczecina świńska, która przy drganiach membrany kreśliła ślad na papierze pokrytym sadzą, nawiniętym na obracany korbą walec.

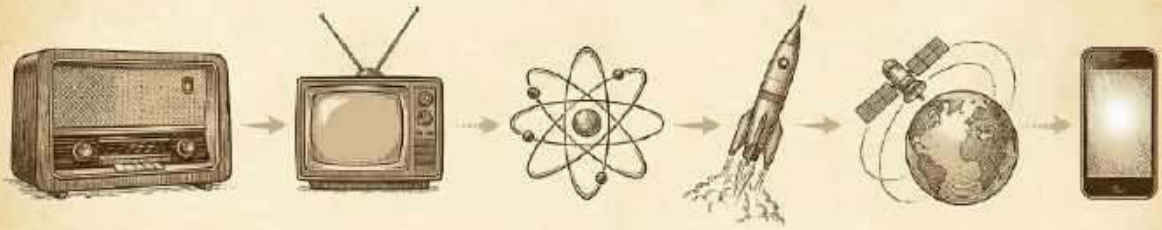
Fonautograf zapisywał dźwięk znakomicie i nie potrafił go odtworzyć – bo nikt tego od niego nie oczekiwał. Scott był człowiekiem od pisma i myślał o swoim wynalazku jak o stenografii doskonałej: mowa miała zapisywać się sama, a odczytywać ją miało wprawione oko. Zamysł okazał się nierealny,



Phonautograph.

BC, barrel with opening at *C*; *a*, brass tube with membrane and style at *b*, and movable piece *a*, by which the position of the nodal points can be regulated; *k*, handle to turn cylinder (*A*) covered with lampblacked paper.

1. Fonautograf Scotta de Martinville – tuba, membrana i walec pokryty sadzą. Źródło: Autorstwa uncredited 19th century engraving – Century Dictionary, Domena publiczna, https://commons.wikimedia.org/w/index.php?curid=2832951



bo z rysunku fali nie da się nauczyć czytać. Wynalazca nigdy nie usłyszał tego, co zarejestrował.

Historia dopisała zakończenie po stu pięćdziesięciu latach. W 2008 roku badacze dawnych nagrań zeskanowali zakopcone kartki Scotta z paryskich archiwów i przetworzyli rysunek fali z powrotem na dźwięk – komputerowo, tak jak igła przetwarza rowek. Z zapisu z 1860 roku odezwał się cienki fragment francuskiej piosenki „Au clair de la lune". Najstarszy słyszalny głos świata czekał na odtworzenie sto czterdzieści osiem lat.

KAMIEŃ MILOWY 1877 – fonograf Edisona

Thomas Edison rozwiązał problem, którego Scott nawet nie postawił: jak przejść tę samą drogę w obie strony. Doszedł do tego, pracując nad urządzeniem powtarzającym sygnały telegraficzne, gdy zauważył, że membrana telefonu drgająca pod wpływem głosu ma dość siły, by poruszać igłą.

W fonografie igła połączona z membraną żłobiła rowek o zmiennej głębokości w cynfolii owiniętej wokół walca obracanego korbą. Przy odtwarzaniu ta sama igła prowadzona po istniejącym rowku unosiła się i opadała, wprawiając membranę w drgania odtwarzające zapis. Pierwszym nagraniem, jakie w ten sposób powstało i zostało odsłuchane, był wierszyk o Mary i jej owieczce, wykrzyczany do tuby przez samego wynalazcę.

Zasada jest tak prosta, że dziś odtwarza się ją na lekcjach fizyki, budując fonograf z kubka po jogurcie i szpilki. W 1877 roku była sensacją: po raz pierwszy głos człowieka mógł przetrwać jego samego. Sam Edison ułożył listę zastosowań, na której muzyka znalazła się dopiero na czwartym miejscu – przed nią były dyktowanie listów, książki dla niewidomych i nauka wymowy.

Wady były jednak zasadnicze. Cynfolia rwała się i wystarczała na kilka odtworzeń, a nagrania nie dawało się powielić inaczej niż przez ponowne wykonanie utworu przed tubą. Poprawę przyniosło zastąpienie folii warstwą wosku, ale wciąż każdy egzemplarz nagrywano osobno – śpiewacy powtarzali ten sam utwór po kilkanaście razy dziennie do zestawu ustawionych obok siebie tub.

KAMIEŃ MILOWY 1887 – gramofon Berlinera i płaska płyta

Emil Berliner, niemiecki wynalazca pracujący w Stanach Zjednoczonych, zmienił dwie rzeczy naraz: zastąpił walec płaskim krążkiem, a rowek żłobił nie w głąb, lecz na boki, jako wężyk o stałej głębokości. Ważniejsze było to drugie.

Zapis boczny pozwalał wykonać z nagrania metalową matrycę, czyli negatyw rowka, i tłoczyć nią kopie z rozgrzanego tworzywa. Od tej chwili nagranie przestało być przedmiotem jednostkowym, a stało się wyrobem przemysłowym, powielanym w tysiącach egzemplarzy z jednego wykonania. Powstał

2. Fonograf Edisona z walcem cynfoliowym, model z 1877 roku. Źródło: Autorstwa Levin C. Handy (per http://hdl.loc.gov/loc.pnp/cwpbh.04326) – Brady-Handy Photograph Collection (Library of Congress) – http://hdl.loc.gov/loc.pnp/cwpbh.04044, Domena publiczna, https://commons.wikimedia.org/w/index.php?curid=1550649

3. Gramofon Berlinera z tubą i płytą szelakową. Źródło: By Science Museum – Science Museum, CC0, https://commons.wikimedia.org/w/index.php?curid=68559258

przemysł płytowy, a wraz z nim zawód, którego wcześniej nie było: artysty znanego z nagrań, a nie z estrady.

Przez pierwsze lata płyty uchodziły za jarmarczną zabawkę wobec poważnych walców. Zmieniły to nagrania wielkiego tenora, zarejestrowane w hotelowym pokoju w Mediolanie w 1902 roku, które dowiodły, że płyta przenosi sztukę, nie tylko kuplety. Spór o format trwał jeszcze dwie dekady i wygrała go płyta – tańsza w tłoczeniu i wygodniejsza w przechowywaniu.

Ustalił się materiał: szelak, krucha żywica z wydzieliny owadów, i prędkość około 78 obrotów na minutę. Wynikło z tego ograniczenie, które kształtowało muzykę przez pół wieku: na jednej stronie mieściły się trzy, najwyżej cztery minuty. Kompozytorzy pisali pod tę długość, a słuchacze przywykli, że utwór tyle właśnie trwa. Standardowa długość piosenki nie wynika z niczego w muzyce – wynika ze średnicy krążka i prędkości obrotu.

Polak, który zapisał dźwięk na taśmie filmowej

Józef Tykociński-Tykociner urodził się w 1877 roku we Włocławku – w tym samym roku, w którym Edison zbudował fonograf. Jako osiemnastolatek wyjechał do Stanów Zjednoczonych, w Nowym Jorku poznał Teslę i zajął się falami krótkimi. Pracował dla Marconiego w Londynie, zakładał łączność radiową dla floty rosyjskiej, a po odzyskaniu przez Polskę niepodległości wrócił do kraju i pracował przy łączności telegraficznej. W 1921 roku przyjął posadę pierwszego profesora badawczego w katedrze elektrotechniki Uniwersytetu Illinois.

Pomysł nosił w sobie od młodości: jako nastolatek zachwycił się fonografem, ale uznał, że brzmi gorzej niż telefon. Rozwiązanie, do którego doszedł, było zaskakujące. Skoro dźwięk da się zamienić na zmienny prąd, a prąd na zmienne światło, to można go zapisać na kliszy jako pasmo o zmiennym zaczernieniu. Przy odtwarzaniu światło przechodzące przez to pasmo pada na fotokomórkę, która zamienia je z powrotem na prąd, a ten na dźwięk.

9 czerwca 1922 roku, niecały rok po przyjeździe na uczelnię, Tykociner pokazał publicznie działający układ. W sali wykładowej fizyki, przed zebraniem miejscowego oddziału stowarzyszenia inżynierów elektryków, wyświetlił film, na którym jego żona Helena dzwoni dzwonkiem, a kierownik katedry odczytuje mowę gettysburską. Obraz i dźwięk pochodziły z tej samej taśmy, więc były zsynchronizowane z natury rzeczy – bez żadnego mechanizmu utrzymującego zgodność. Kluczowym elementem była fotokomórka skonstruowana przez uniwersyteckiego kolegę, Jakoba Kunza.

Dalszy ciąg jest mniej budujący. Spór z uczelnią o prawa patentowe wstrzymał zgłoszenie; patent Tykociner uzyskał dopiero w 1926 roku, a tymczasem inni opatentowali rozwiązania konkurencyjne. Za początek kina dźwiękowego uznano „Śpiewaka jazzbandu" z 1927 roku, w którym dźwięk odtwarzano z płyt zsynchronizowanych z projektorem. Metoda z płytami okazała się jednak ślepą uliczką – gubiła zgodność z obrazem po każdym zerwaniu taśmy i nie dawała się montować. W ciągu kilku lat wyparła ją ścieżka optyczna, czyli dokładnie to, co pokazał Polak, i została w kinie standardem przez pół wieku.

Mikrofon, czyli koniec krzyczenia do tuby

Do połowy lat dwudziestych nagrywano akustycznie: energia dźwięku bezpośrednio poruszała membranę i igłę. Wymuszało to sposób pracy, który dziś wygląda niedorzecznie. Orkiestrę ustawiano w ciasnej gromadzie wokół wlotu tuby, a instrumenty za ciche, by poruszyć igłę, zastępowano donośniejszymi. Śpiewak musiał krzyczeć, a przy cichych fragmentach podchodzić bliżej.

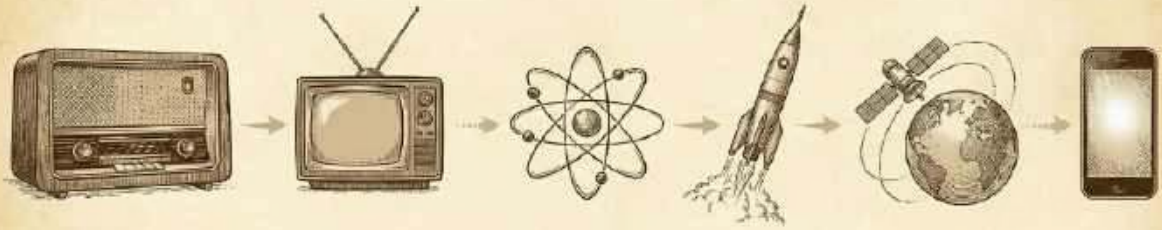
W 1925 roku wprowadzono zapis elektryczny. Między dźwiękiem a igłą stanęły trzy nowe elementy: mikrofon, wzmacniacz lampowy i głowica elektromagnetyczna żłobiąca rowek na podstawie wzmocnionego sygnału. Pasmo przenoszonych częstotliwości wzrosło ponad dwukrotnie.

Najciekawsze skutki nie były jednak techniczne. Skoro za głośność odpowiadał wzmacniacz, śpiewak przestał konkurować siłą płuc z orkiestrą – mógł śpiewać cicho, niemal szeptem, i tak narodził się nowy sposób śpiewania, oparty na intymności zamiast na donośności. Muzycy przestali też tłoczyć się przy tubie, a brzmienie dobierał odtąd inżynier, przesuwając mikrofon. Zawód realizatora dźwięku powstał właśnie wtedy.

Taśma magnetyczna i narodziny montażu

Duński inżynier Valdemar Poulsen pokazał na wystawie w Paryżu w 1900 roku telegrafon, zapisujący dźwięk na namagnesowanym stalowym drucie. Zasada była poprawna, ale drut plątał się i rwał, a jakość ustępowała płycie. Przez trzydzieści lat zapis magnetyczny pozostawał ciekawostką.

W latach trzydziestych w Niemczech połączono dwa wynalazki: magnetofon zbudowany przez zakłady elektrotechniczne oraz taśmę z tworzywa



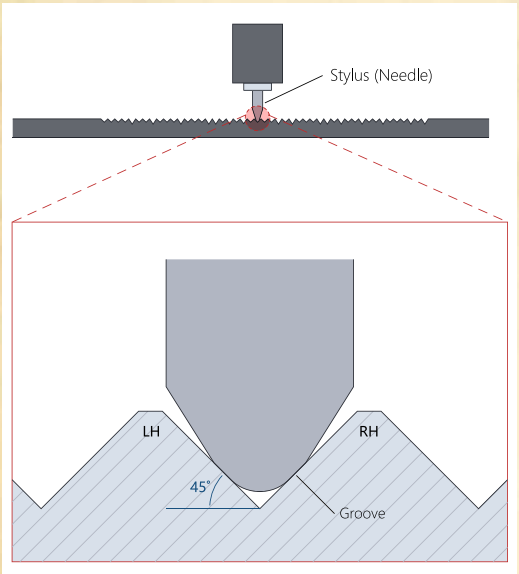
pokrytą sproszkowanym materiałem magnetycznym. Taśma była lekka, tania i mieściła się w szpuli. W 1940 roku dołożono rozwiązanie, które przesądziło o jakości: podkład wielkiej częstotliwości. Do nagrywanego sygnału dodaje się drgania o częstotliwości znacznie wyższej od słyszalnych, co usuwa zniekształcenia wynikające z nieliniowości nośnika. Brzmienia nie odróżniano już od transmisji na żywo.

Najważniejsza była jednak możliwość, o której początkowo nikt nie myślał: taśmę można przeciąć nożyczkami i skleić. Nagranie przestało być zapisem jednego wykonania, a stało się materiałem, który wolno porządkować i składać z kawałków. Wkrótce dołożono nagrywanie kolejnych ścieżek na jednej taśmie, tak by muzyk mógł zagrać sam ze sobą. Całe dzisiejsze studio wywodzi się z tego jednego cięcia nożyczkami.

KAMIEŃ MILOWY 1948 – płyta długogrająca

Krążek z winylu obracany z prędkością 33⅓ obrotu na minutę, z rowkiem znacznie węższym niż w płycie szelakowej, pomieścił ponad dwadzieścia minut na stronę. Winyl był przy tym mniej kruchy i cichszy od szelaku, który szumiał z powodu ziarnistej struktury.

Skutki znów sięgnęły poza technikę. Muzyka poważna przestała być rozcinana na trzyminutowe kawałki, a w muzyce rozrywkowej pojawiło się pojęcie albumu jako całości zaplanowanej przez artystę. Konkurencyjna wytwórnia odpowiedziała mniejszym krążkiem na 45 obrotów, mieszczącym jeden utwór – i tak przez czterdzieści lat rynek dzielił się na albumy i single.



4. Przekrój rowka płyty stereofonicznej – dwie ścianki, dwa kanały. Źródło: Adobe Stock

Dziesięć lat później wprowadzono zapis stereofoniczny, oparty na pomyśle opatentowanym w 1931 roku przez Alana Blumleina. Jeden rowek niesie dwa sygnały, bo igła odchyla się w dwóch prostopadłych kierunkach – po jednym na kanał. Płytę stereofoniczną dawało się przy tym odtworzyć igłą monofoniczną i to przesądziło o przyjęciu formatu.

Dźwięk wychodzi z domu

W sierpniu 1963 roku, na berlińskiej wystawie radiowej – tej samej, przy okazji której trzydzieści siedem lat wcześniej poświęcono tamtejszą wieżę radiową – firma Philips pokazała kasetę kompaktową: dwie szpulki taśmy w plastikowym pudełku, którego nie trzeba było nawlekać.

Miał to być nośnik do dyktafonów, a stał się nośnikiem muzyki. Zadecydowała decyzja handlowa: producent udostępnił konstrukcję innym wytwórniom bez opłat licencyjnych, pod warunkiem zachowania wymiarów. Format przyjął się na całym świecie, a początkowo słabą jakość podniosły lepsze taśmy oraz układy redukcji szumów.

Kaseta dała słuchaczowi dwie rzeczy, których nie miał wcześniej. Pierwszą był kieszonkowy odtwarzacz ze słuchawkami, wprowadzony w 1979 roku: muzykę można było wreszcie zabrać na ulicę. Drugą – możliwość nagrywania własnych składanek, czyli robienia z cudzych nagrań czegoś swojego. Wytwórnie uznały to za kradzież i przekonywały, że domowe nagrywanie zabija muzykę.

W Polsce kaseta miała jeszcze jedno znaczenie. Przy ubogiej ofercie oficjalnych wydawnictw i wysokiej cenie płyt to na kasetach krążyły kopie przegrywane z pożyczonych płyt i z audycji radiowych. Pokolenie, które dziś ma pięćdziesiąt lat, poznawało muzykę głównie z kopii kopii – ze słyszalnym szumem, który dla wielu pozostał częścią wspomnienia.

KAMIEŃ MILOWY 1982 – płyta kompaktowa i koniec zapisu ciągłego

Wszystkie wcześniejsze techniki były analogowe: rowek, namagnesowanie taśmy i zaczernienie kliszy odwzorowywały kształt fali w sposób ciągły. Płyta kompaktowa zerwała z tym całkowicie – zamiast odwzorowywać falę, opisała ją liczbami.

Sygnał mierzy się 44 100 razy na sekundę, każdy pomiar zapisuje jako liczbę szesnastobitową, a liczby – jako mikroskopijne wgłębienia w warstwie tworzywa, odczytywane wiązką lasera. Dobór tych wartości nie jest przypadkowy. Twierdzenie o próbkowaniu mówi, że falę trzeba mierzyć częściej niż dwa razy na okres najwyższej zachowywanej częstotliwości; skoro granica słyszalności to około 20 tysięcy drgań na sekundę, próbkowanie musiało przekroczyć 40 tysięcy. Szesnaście bitów daje zaś zakres dynamiki większy niż różnica między szeptem a orkiestrą w sali koncertowej.

Zapis cyfrowy ma cechę, której żaden analogowy nie miał: kopia jest identyczna z oryginałem, a odczyt niczego nie zużywa, bo laser nie dotyka nośnika. Zniknęły trzaski, szum i pogarszanie się nagrania przy kolejnych odtworzeniach. Zniknęła też część charakteru, o którą miłośnicy winylu spierają się do dziś – spór nie jest wyłącznie sentymentalny, bo dotyczy tego, co dzieje się na granicach zakresu.

Kompresja, czyli jak zmieścić muzykę w kieszeni

W czasach, gdy dysk twardy miał kilkaset megabajtów, a łącze telefoniczne przesyłało kilka kilobajtów na sekundę, przesłanie jednego utworu było przedsięwzięciem na całe popołudnie. Rozwiązanie przyszło nie z elektroniki, lecz z psychoakustyki – badań nad tym, czego ucho w istocie nie słyszy.

Okazuje się, że nie słyszy zaskakująco wiele. Dźwięk cichy tuż po głośnym jest maskowany i nie dociera do świadomości; tak samo ginie dźwięk cichy o częstotliwości bliskiej głośnemu – na przykład trójkąt uderzony podczas fortissimo orkiestry. Skoro te składowe i tak nie są słyszane, można ich nie zapisywać.

Na tej zasadzie zespół z niemieckiego instytutu badawczego opracował format kompresji stratnej, zatwierdzony jako norma międzynarodowa na początku lat dziewięćdziesiątych. Plik zmniejszał się mniej więcej dziesięciokrotnie przy brzmieniu, którego większość słuchaczy nie odróżniała od oryginału. Algorytm strojono na nagraniu głosu bez akompaniamentu – bo w nim każdy błąd słychać najwyraźniej.

Skutki wykroczyły poza wygodę. Plik dziesięciokrotnie mniejszy dawał się przesłać siecią, co podważyło cały handel muzyką oparty na sprzedaży krążków i zapoczątkowało dekadę sporów sądowych. Przełom nie polegał przy tym na lepszym brzmieniu – przeciwnie. Polegał na tym, że muzyka przestała mieć wagę i rozmiar.

Jak to działa: od fali do liczby

Zamiana dźwięku na liczby ma dwa etapy, które łatwo pomylić:

Próbkowanie – to pomiar wartości sygnału w równych odstępach czasu; decyduje o tym, jak wysokie tony da się zapisać. Zbyt rzadkie próbkowanie zamienia wysoki ton w niższy – tak jak koło wozu w filmie zdaje się kręcić wstecz, gdy klatki padają zbyt rzadko.

Kwantowanie – to zaokrąglenie każdego pomiaru do najbliższej dostępnej wartości. Decyduje o tym, jak ciche dźwięki da się odróżnić od szumu. Im więcej bitów, tym drobniejsza podziałka i większy zakres dynamiki.

Płyta kompaktowa: 44 100 pomiarów na sekundę, 16 bitów na pomiar, dwa kanały. Stąd około dziesięciu megabajtów na minutę muzyki – liczba, która w latach dziewięćdziesiątych była problemem nie do przeskoczenia.

Dziś: dostęp zamiast posiadania

Obecnie większość słuchaczy nie ma nagrań ani na półce, ani w postaci plików. Muzyka jest przesyłana strumieniowo w chwili odtwarzania, a użytkownik nie kupuje nagrania, tylko dostęp do zbioru. Ograniczenia, które przez sto lat kształtowały muzykę – trzy minuty szelaku, dwadzieścia minut winylu, siedemdziesiąt kilka minut płyty kompaktowej – przestały obowiązywać. Zastąpiły je nowe, wynikające nie z fizyki nośnika, lecz ze sposobu rozliczania odtworzeń.

Równolegle wróciła płyta winylowa, kupowana dziś głównie przez ludzi, którzy i tak słuchają muzyki z sieci. Przestała być nośnikiem, a stała się przedmiotem – gdy nośnik przegrywa jako narzędzie, bywa, że wygrywa jako rzecz.

Cały ten łańcuch, od szczeciny Scotta po serwer strumieniowy, opiera się na jednym pomyśle: drganie powietrza da się przedstawić jako fala, a falę zapisać czymkolwiek, co zmienia się w podobny sposób. Sadzą, głębokością rowka, namagnesowaniem taśmy, zaczernieniem kliszy, wgłębieniem w tworzywie i wreszcie ciągiem liczb. Zmieniał się nośnik i sposób odczytu – zasada nie zmieniła się od 1857 roku.

Leksykon: dwadzieścia pojęć z historii zapisu dźwięku

- **Fala dźwiękowa** – rozchodzące się w powietrzu zagęszczenia i rozrzedzenia; wszystko, co opisano niżej, służy zapisaniu jej kształtu.
- **Fonautograf** – urządzenie Scotta z 1857 roku, zapisujące kształt fali na sadzy bez możliwości odtworzenia.
- **Fonograf** – urządzenie Edisona z 1877 roku, zapisujące i odtwarzające dźwięk z rowka o zmiennej głębokości wyżłobionego na walcu.
- **Gramofon** – urządzenie Berlinera z 1887 roku, odtwarzające zapis boczny z płaskiej płyty.
- **Zapis wgłębny i boczny** – dwa sposoby żłobienia rowka: zmienną głębokością albo zmiennym odchyleniem na boki. Ten drugi umożliwił tłoczenie kopii.
- **Matryca** – metalowy negatyw rowka, służący do tłoczenia płyt. Podstawa przemysłu płytowego.
- **Szelak** – krucha żywica pochodzenia owadziego, materiał płyt do połowy XX wieku. Stąd nazwa płyt siedemdziesięcioośmioobrotowych.
- **Zapis akustyczny** – nagrywanie bez mikrofonu, wyłącznie energią dźwięku poruszającą membranę i igłę.
- **Zapis elektryczny** – nagrywanie z mikrofonem i wzmacniaczem, wprowadzone w 1925 roku; podniosło pasmo i zmieniło sposób śpiewania.
- **Ścieżka optyczna** – zapis dźwięku na taśmie filmowej w postaci zmiennego zaczernienia, odczytywany fotokomórką. Pokazany publicznie przez Tykocinera w 1922 roku.
- **Fotokomórka** – element zamieniający padające światło na prąd elektryczny; warunek działania ścieżki optycznej.
- **Telegrafon** – urządzenie Poulsena z przełomu wieków, zapisujące dźwięk na namagnesowanym drucie stalowym.
- **Podkład wielkiej częstotliwości** – drgania o częstotliwości ponadsłyszalnej dodawane do sygnału przy nagraniu na taśmę; usuwają zniekształcenia nośnika.
- **Wielośladowość** – nagrywanie kolejnych partii na osobnych ścieżkach tej samej taśmy, z możliwością ich późniejszego zmieszania.
- **Stereofonia** – zapis dwóch kanałów odtwarzających położenie źródeł dźwięku w przestrzeni; pomysł opatentowany przez Blumleina w 1931 roku.
- **Redukcja szumów** – układ wzmacniający ciche tony wysokie przy nagraniu i tłumiący je przy odtwarzaniu wraz z szumem nośnika.
- **Próbkowanie** – pomiar wartości sygnału w równych odstępach czasu; dla płyty kompaktowej 44 100 razy na sekundę.
- **Kwantowanie** – zaokrąglenie każdego pomiaru do najbliższej dostępnej wartości; liczba bitów decyduje o zakresie dynamiki.
- **Twierdzenie o próbkowaniu** – zasada mówiąca, że sygnał trzeba mierzyć częściej niż dwa razy na okres najwyższej zapisywanej częstotliwości.
- **Kompresja stratna** – zmniejszenie pliku przez usunięcie składowych, których ucho i tak nie usłyszy.
- **Maskowanie** – zjawisko polegające na tym, że dźwięk głośny czyni niesłyszalnym dźwięk cichy sąsiadujący z nim w czasie lub częstotliwości. Podstawa kompresji stratnej.

KURS PRAKTYCZNY AI

Praktyczne podejście. Zero marketingowej mgły!

Zyskaj **15%** rabatu

W prenumeracie tylko

~~116,00 zł~~

98,60 zł

prenumerata drukowana 4 kolejnych wydań

(zima 2026, wiosna, lato, jesień 2027)

Zamów na www.UlubionyKiosk.pl

lub zeskanuj kod QR i zaprenumeruj w 1 minutę

Wydania archiwalne (wiosna, lato, jesień 2026)
są dostępne na www.UlubionyKiosk.pl