

Michał Lenart
MIMUW

Komputer za 10-30 lat

W ciągu ostatnich kilkunastu-kilkudziesięciu lat komputery przeszły bardzo wiele zmian. Biurkowy komputer posiada o kilka rzędów wielkości większą zarówno pamięć jak i moc obliczeniową - pojedynczy dysk twardy pojemności rzędu 100GB jeszcze kilkanaście lat temu był nie do pomyślenia - nawet dzisiejsza przeciętna kość pamięci RAM przewyższa swoją pojemnością ówczesne dyski. Zgodnie z prawem Moore'a pojemność pamięci masowych rośnie w tempie wykładniczym. Słynny cytat sprzed lat (który miał rzekomo wygłosić wypierający się tego Bill Gates) mówi, że nikt nie będzie potrzebował pamięci większej niż... 640kB. Dzisiaj nikt już nie ma złudzeń - każda pamięć kiedyś okaże się niewystarczająca. Płyty DVD, zostaną zastąpione np. przez Blue-Ray oparty na niebieskim (zamiast czerwonego) laserze. Dzięki krótszej długości fali światła niebieskiego możliwe staje się dalsze zwiększenie gęstości zapisu (w porównaniu z DVD)- z niecałych 5GB do 25GB (w przypadku tylko jednej warstwy zapisu). W niedalekiej przyszłości to rozwiązanie będzie pewnie na tyle tanie, by każdy mógł sobie na nie pozwolić.

Z kilkanaście lat być może uda się skonstruować i wykorzystywać komputer kwantowy - teoretycznie umożliwiłby on rozwiązanie pewnych problemów w asymptotycznie lepszym czasie, niż "standardowe" komputery krzemowe. Przykładem jest problem znalezienia rozkładów dużych liczb na czynniki pierwsze - dzisiaj potrafimy je znajdować jedynie w czasie wykładniczym. W praktyce oznacza to, że algorytmy kryptograficzne oparte na tym (jak RSA) mogą być bezpieczne. Komputer kwantowy teoretycznie umożliwiłby rozwiązanie tego problemu w czasie wielomianowym - co w praktyce oznaczałoby, że dzisiaj uznawane za bezpieczne protokoły obsługujące np. korzystanie z banków internetowych stałyby się bezużyteczne. Muszę jednak zaznaczyć, że nie jest przesądzone, iż komputer kwantowy jest do tego niezbędny - matematycy na dzień dzisiejszy nie potrafią udowodnić, że nie da się znaleźć rozkładu liczb na czynniki pierwsze w czasie wielomianowym na "zwykłym" komputerze, więc być może pewnego dnia się to uda..

Zmienia się również nasz sposób komunikacji z komputerem. Tak jak kiedyś rewolucją był "okienkowy" system operacyjny obsługiwany za pomocą myszy, tak w przyszłości zapewne powstanie komputer sterowany falami mózgowymi. Coś takiego mogłoby stanowić doskonałe usprawnienie pracy (brak konieczności klikania czy wydawania komend z klawiatury), ciekawe urozmaicenie dla graczy (umożliwiło by to jeszcze większe "zanurzenie się" w wirtualnym świecie) jak i możliwość normalnej pracy dla osób niepełnosprawnych. Właśnie dla osoby sparaliżowanej skonstruowano system porozumiewania się za pomocą fal mózgowych - jednakowoż czerpanie korzyści z tego wynalazku wiąże się z godzinami treningu. Taki sposób komunikacji nie jest też jeszcze tak szybki jak np. pisanie na klawiaturze. Opracowanie sprawnego interfejsu tego typu stanowi więc ciekawe wyzwanie dla inżynierów jak również neurologów.

W bliższej przyszłości czeka nas zapewne dalsze "upiększanie" istniejących interfejsów graficznych, jak również "innowacje" typu trójwymiarowy interfejs, które może i będą wyglądać ładnie, ale też zmuszą użytkowników starszego sprzętu do jego wymiany, jeśli będą chcieli korzystać z najnowszego oprogramowania.

Inną innowacją na rynku komputerów jest standard Trusted Computing. W skrócie oznacza on, że na płycie głównej każdego komputera znajduje się chip

zawierający (w założeniu niewidoczny dla użytkownika) klucz prywatny, oraz klucz publiczny - służący do szyfrowania danych tak, by mogły być czytane tylko na tym komputerze (tylko klucz prywatny umożliwia ich odszyfrowanie). Takie rozwiązanie umożliwiłoby skuteczną walkę z piractwem komputerowym (pliku zaszyfrowanego dla danego komputera nie można odczytać na żadnym innym), ale także odbierałoby nam-użytkownikom pełną kontrolę nad tym, co mamy we własnym komputerze. Poza tym konieczność szyfrowania transmisji w oczywisty sposób obniża wydajność..

Tak naprawdę jednak naprawdę innowacyjnych pomysłów jakie pojawią się za kilkadziesiąt lat prawdopodobnie nie potrafimy dzisiaj przewidzieć.