

STANOWISKO

na temat Założeń do Polityki Technologii Kwantowych

Niniejsza opinia dotyczy dokumentu udostępnionego do konsultacji przez Ministerstwo Cyfryzacji w sierpniu 2025.

Przedstawione założenia w wielu obszarach determinują odpowiedzi na kluczowe strategiczne pytania. Naszym zdaniem jest to przedwczesne ze względu na niejasną sytuację przynajmniej z punktu widzenia bezpieczeństwa w obszarze IT.

- Większość technologii kwantowych (wyjątkiem jest kwantowa dystrybucja klucza) należy traktować w kategorii potencjalnych zagrożeń bezpieczeństwa teleinformatycznego a nie obrony. Z tego względu należy podjąć decyzję, czy strategicznym celem jest rozwijanie agresywnych technologii przeciw współczesnym technologiom bezpieczeństwa czy skoncentrowanie się na defensywie. W drugim przypadku prace powinny być skoncentrowane na technikach PQC, które w Strategii potraktowane są marginalnie a proponowane działania ograniczają się do pasywnego przyjmowania rozwiązań narzucanych z zagranicy i przez korporacje.
- W przypadku technologii QKD, nie jest do końca jasne jaka jest finalna rola tej technologii w ekosystemie informacyjnym. Traktowanie QKD jako technologii automatycznie zapewniającej bezpieczeństwo komunikacji przed przyszłymi atakami jest nieuzasadnione. QKD obejmuje tylko niewielki wycinek (uzgadnianie klucza) i jest to stosunkowo droga i wrażliwa na ataki fizyczne/ akty terroru itp. alternatywa dla technik stosowanych dzisiaj.
- Decyzje pod względem strategicznych kierunków działań w obszarze cyberbezpieczeństwa powinny brać pod uwagę najślabesze ogniwa systemu. W szczególności, należy zidentyfikować te obszary gospodarki kluczami, które w rzeczywistości mają największe przełożenie na realny poziom odporności.
- Wiele informacji dotyczących perspektyw technologii kwantowych może okazać się mieć charakter informacji marketingowych luźno związanych w realiami technologicznymi i ekonomicznymi. Udokumentowane w literaturze nierzetelne dokumentowanie postępów w faktoryzacji liczb RSA wskazuje, że problem ma poważny charakter.

W sytuacji tej kluczową składową strategii powinna być budowa mechanizmów i instytucji, które mogłyby podjąć decyzje w tym bardzo trudnym obszarze przy zachowaniu niezależności i transparentności.

- (2) Niezwykle ostrożnie należy podchodzić do działań w zakresie edukacyjnym. Uruchomienie kształcenia na proponowaną skalę niesie ze sobą niebezpieczeństwo wykształcenia kadr, które mogą okazać się niepotrzebne na polskim rynku pracy. Niebezpieczeństwo to istnieje nawet w przypadku sukcesu technologii kwantowych – nie jest wcale jasne, że Polska jest w stanie kadry te wykorzystać na miejscu – najbardziej prawdopodobnym scenariuszem jest lokalizacja tego typu przemysłu w obszarach o wyższym poziomie stabilności i bezpieczeństwa, a w konsekwencji emigracja kadr.
- (3) Szanse budowy znaczącego przemysłu hardware’u kwantowego w Polsce wydają się nikłe, być może z wyjątkiem jednostkowych niszowych rozwiązań. Problemem jest kolosalna różnica w realistycznej skali nakładów, jakie mogą być i jakie ponoszone są przez Polskę oraz przez wiodących graczy. Zdobycie znaczącej pozycji może być tak samo trudne jak obecnie rywalizacja w obszarze produkcji mikroprocesorów. Doświadczenie uczy, że nawet dobra znajomość know-how w tym specyficznym obszarze nie jest decydująca—problemem może okazać się dostęp do kluczowych technologii znajdujących się w obcych dla nas rękach.
- (4) Należy zdecydować, jaka część przewidywanych nakładów finansowych powinna być przeznaczona na badania naukowe (badania podstawowe) związane z technikami kwantowymi, a jaka część powinna finansować praktyczne wdrożenia, jeśli takie w wyniku badań będą realne. Istotą tego obszaru jest niezbędna współpraca międzynarodowa w zakresie nauki, na którą lepiej przeznaczyć środki niż na budowę rozwiązań hardware’y kwantowego, który jest w stanie skonsumować większość środków, bez oczekiwanego efektu.

Mirostaw Kutylowski

Józef Pieprzyk

Wiesław Paluszyński

Stanowisko wyraża poglądy Sekcji Bezpieczeństwa Komitetu Informatyki PAN i nie powinno być utożsamiane ze stanowiskiem Polskiej Akademii Nauk.