Związek Pracodawców Edukacji

12.03.2026 r.

Dotyczy: opinii Związku Pracodawców Edukacji w sprawie planowanego wprowadzenia zawodu „Technik cyberbezpieczeństwa” do klasyfikacji szkolnictwa branżowego

W związku z prowadzonymi konsultacjami dotyczącymi planowanego wprowadzenia do klasyfikacji szkolnictwa branżowego nowego zawodu „Technik cyberbezpieczeństwa”, Związek Pracodawców Edukacji przekazuje **opinię ekspercką przygotowaną przez jednego z członków Związku – Fundację Infotech.**

Opinia została opracowana przez **Adama Kamińskiego, Prezesa Zarządu Fundacji Infotech**, na podstawie doświadczeń wynikających z prowadzenia kształcenia w obszarze technologii informatycznych, w tym specjalizacji z zakresu cyberbezpieczeństwa, a także w oparciu o współpracę z przedstawicielami sektora bezpieczeństwa oraz środowiska technologicznego.

Zdaniem Związku Pracodawców Edukacji przedstawione stanowisko stanowi istotny głos praktyków rynku technologicznego oraz podmiotów bezpośrednio zaangażowanych w kształcenie przyszłych kadr dla sektora cyberbezpieczeństwa. Z tego względu przekazujemy je jako wkład środowiska pracodawców w proces projektowania nowego zawodu w systemie szkolnictwa branżowego.

Poniżej przekazujemy pełną treść opinii.

Związek Pracodawców Edukacji
ul. J. Gorczyczewskiego 2/7
60-554 Poznań
tel. 536 215 233
biuro@pracodawcy.edu.pl
www.pracodawcy.edu.pl

Stanowisko członka Związku Pracodawców Edukacji - Fundacja Infotech

W odpowiedzi na pismo z dnia 16 lutego 2026 r., Fundacja Infotech wyraża zdecydowane poparcie dla inicjatywy wprowadzenia zawodu „Technik cyberbezpieczeństwa". Jest to krok strategicznie niezbędny dla zniwelowania luki kompetencyjnej oraz wzmocnienia cyfrowego bezpieczeństwa kraju w dobie dyrektywy NIS 2.

Z perspektywy Fundacji Infotech, która od ponad dwóch lat z sukcesem prowadzi w Białymstoku specjalizację z cyberbezpieczeństwa (na podbudowie zawodu Technik programista) oraz autoryzowane centrum egzaminacyjne Pearson VUE, nowy zawód nie odniesie jednak sukcesu bez fundamentalnych zmian prawnych. Nasze stanowisko opieramy również na najnowszej diagnozie kadr "Dual-Use" dla Podlasia, przeprowadzonej z udziałem 35 dowódców jednostek wojskowych i cywilnych służb mundurowych.

Z perspektywy praktyki edukacyjnej i współpracy z rynkiem cyberbezpieczeństwa wskazujemy poniżej kluczowe uwarunkowania, które powinny zostać uwzględnione przy projektowaniu nowego zawodu:

1. Bariera prawna: Niewydolność obecnego systemu zatrudniania ekspertów

Zapotrzebowanie dotyczy inżynierów i operatorów bezpieczeństwa (SOC). Szkoły nie posiadają takiej kadry. Teoretycznie istniejące rozwiązania, takie jak art. 15 Prawa oświatowego (zatrudnienie bez przygotowania pedagogicznego za zgodą kuratora) czy limitowane możliwości stosowania umów cywilnoprawnych, są całkowicie niekompatybilne z rynkiem IT. Ekspert z branży cyberbezpieczeństwa lub oddelegowany oficer służb nie podpisze umowy o pracę w reżimie szkolnym za ułamek stawki rynkowej, ani nie będzie funkcjonował w biurokratycznym gorsecie zgód kuratoryjnych. Dodatkowo nowe rygory (od 2026 r.) dotyczące kontroli umów B2B skutecznie zniechęcają dyrektorów do elastycznego kontraktowania specjalistów.

Rekomendacja: Ministerstwo Cyfryzacji, we współpracy z MEN, musi wypracować specustawę lub radykalną nowelizację Prawa oświatowego dla zawodów kluczowych technologicznie. Niezbędne jest wprowadzenie nielimitowanych, elastycznych form kontraktowania (B2B) praktyków z rynku oraz ekspertów służb mundurowych, wyłączonych spod reżimu Karty Nauczyciela i standardowych ograniczeń art. 15.

2. Model "Dual-Use" – priorytet dla kompetencji miękkich i postaw

Z przeprowadzonej przez nas diagnozy z 35 dowódcami jednostek na Podlasiu wynika jednoznacznie: kluczową cechą mentalną operatora technologii w sytuacji kryzysowej nie jest sama wiedza inżynieryjna, lecz "odporność na stres", "opanowanie", "decyzyjność" oraz "chłodna kalkulacja". Aż 25 lokalnych jednostek zadeklarowało gotowość delegowania ekspertów na zajęcia praktyczne do naszej szkoły.

Rekomendacja: Podstawa programowa musi zawierać obowiązkowy moduł zarządzania kryzysowego i psychologii działań pod presją. Rozwiązanie wskazane w pkt 1 (uelastycznienie prawa) jest warunkiem sine qua non, aby szkoły mogły legalnie wpuszczać ekspertów mundurowych w celu hartowania tych postaw.

Związek Pracodawców Edukacji
ul. J. Gorczyczewskiego 2/7
60-554 Poznań
tel. 536 215 233
biuro@pracodawcy.edu.pl
www.pracodawcy.edu.pl

3. Infrastruktura chmurowa zamiast tradycyjnej infrastruktury sprzętowej

Zwykła pracownia informatyczna jest bezużyteczna do symulacji ataków czy analizy logów w czasie rzeczywistym.

Rekomendacja: Podstawa programowa musi formalnie opierać się na laboratoriach chmurowych (Cloud Labs). Państwo powinno zagwarantować celowe subwencje (vouchery) na dostęp do takich, stale aktualizowanych środowisk wirtualnych.

4. Rynkowa certyfikacja ponad państwowe egzaminy

Wiedza teoretyczna w cyberbezpieczeństwie dezaktualizuje się błyskawicznie. Wraz ze wzrostem zagrożeń, rynek oczekuje weryfikacji przez globalne standardy (co widzimy codziennie w naszym centrum Pearson VUE).

Rekomendacja: Zdobycie przez ucznia uznanego komercyjnego certyfikatu (np. CompTIA, Cisco) powinno automatycznie zwalniać z części państwowego egzaminu zawodowego i być z nim prawnie zrównane.

Związek Pracodawców Edukacji pozostaje otwarty na dalszy dialog dotyczący rozwoju szkolnictwa branżowego oraz kształtowania rozwiązań wspierających współpracę systemu oświaty z rynkiem pracy. Deklarujemy gotowość do przekazywania doświadczeń i perspektywy naszych członków w zakresie kształcenia kadr dla nowoczesnej gospodarki oraz funkcjonowania całego środowiska oświatowego.

Z wyrazami szacunku,

Mateusz Krajewski

Prezes

Związek Pracodawców Edukacji

Związek Pracodawców Edukacji
ul. J. Gorczyczewskiego 2/7
60-554 Poznań

tel. 536 215 233
biuro@pracodawcy.edu.pl
www.pracodawcy.edu.pl