LEWIATAN

Warszawa, 16 marca 2026 r.
KL/182/51/SSz/2026

**Dot. pisma:** DC.WSiPP.5541.7.2025

**Opinia w sprawie wprowadzenia nowego zawodu „technik cyberbezpieczeństwa" do systemu oświaty**

Pani
**Kaja Kondratiuk**
Koordynator Prac Wydziału Szkoleń i Programu Partnerstwa
Departament Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

*Szanowna Pani,*

na podstawie art. 16 ust. 2 ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców, przedstawiam opinię na temat planowanego wprowadzenia nowego zawodu do klasyfikacji szkolnictwa branżowego – „Technik cyberbezpieczeństwa". Konfederacja Lewiatan 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.

Analiza założeń do projektu podstawy programowej kształcenia w zawodzie technik cyberbezpieczeństwa, po konsultacjach z pracodawcami branży informatycznej na Pomorzu, co do zasady jest skonstruowana prawidłowo. Jednak zwartość merytoryczna treści jednostek efektów kształcenia wskazuje na to, iż projekt nie ujmuje trendów przyszłości w zakresie zmieniających się dynamicznie technologii w branży informatycznej. Przedstawiciele pracodawców zrzeszonych w Konfederacji Lewiatan wskazują na uwzględnienie poniższych propozycji do podstawy programowej technik cyberbezpieczeństwa:

Kwalifikacja wyodrębniona w zawodzie: **„Bezpieczeństwo systemów i sieci komputerowych":** wskazane dodanie, przynajmniej na poziomie omówienia, następującej tematyki:

*- Architektura Zero Trust*
To model stricte systemowy. Dotyczy tego, jak projektujemy sieć i dostęp, zakładając, że żadne urządzenie wewnątrz sieci nie jest bezpieczne „z zasady";



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- *Bezpieczeństwo chmurowe*
Konfiguracja bezpiecznych kontenerów (Docker/Kubernetes) oraz zarządzanie tożsamością i uprawnieniami (IAM) jako fundamenty bezpiecznego systemu operacyjnego w chmurze;

- *Kryptografia postkwantowa* (wyłącznie jako zasygnalizowanie ze względu na złożoność tematu)
USA zobowiązuje wszystkie agencje federalne do migracji systemów informatycznych na kryptografię postkwantową. To wyraźny kierunek działań i jeden z ważnych trendów. Ataki typu „Harvest Now, Decrypt Later" dzieją się już teraz. Hakerzy kradną zaszyfrowane dane, których nie potrafią odczytać, licząc na to, że za 5 – 10 lat odszyfrują je za pomocą komputera kwantowego;

- *Sztuczna inteligencja (AIOps) połączona z analizą logów*
Narzędzia AI monitorują cały system, szukając anomalii w ruchu sieciowym lub pracy serwerów, co chroni całe środowisko przed awarią lub włamaniem. Podejście z wykorzystaniem AI staje się już nierozłącznym elementem dbania o bezpieczeństwo;

- *Odporność cyfrowa (Resilience) & NIS 2*
Jako klucz do nowoczesnego zarządzania systemami. Zamiast uczyć tylko "jak naprawić zepsute", uczymy, jak zaprojektować system, który przetrwa atak. Kluczowe pojęcia: Disaster Recovery (odzyskiwanie po awarii), Backup w chmurze, dyrektywa NIS 2.

Kwalifikacja wyodrębniona w zawodzie
**„Bezpieczeństwo aplikacji webowych":**

- *Zagrożenia AI (np. Prompt Injection)*
To specyficzny rodzaj ataku na aplikację korzystającą z modeli językowych. Polega na manipulowaniu „wejściem" aplikacji (np. polem czatu), aby zmusić ją do wykonania niepożądanych akcji;

- *Bezpieczeństwo chmurowe (w aspekcie aplikacji)*
Pisanie aplikacji „cloud-native", które bezpiecznie komunikują się z API i prawidłowo obsługują tokeny autoryzacyjne wewnątrz swojego kodu;

- *Bezpieczeństwo tworzenia kodu z AI*
AI pomaga w szybkim tworzeniu, ale jednocześnie takie podejście zawiera wiele podatności i buduje duże ryzyko. Należałoby pokazać czym jest bezpieczne tworzenie oprogramowania z wykorzystaniem sztucznej inteligencji oraz jakie niesie zagrożenia.



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Jednocześnie sugerujemy do rozważenia następujące zagadnienia w zakresie efektów kształcenia:

- **Rozszerzenie analizy zagrożeń o deepfake, dezinformację i phishing:** Absolwent powinien umieć identyfikować manipulacje audiowizualne (AI-generated) oraz rozumieć wektor ataktu jakim jest phishing, które będą głównym narzędziem ataków na firmy w 2030 roku.

- **Ewolucja z „naprawy systemów" na "odporność cyfrową" (Resilience):** Zamiast skupiać się na samym „naprawianiu systemów", warto położyć także nacisk na procedury Disaster Recovery i Backup w środowiskach rozproszonych, zgodnie z wymogami dyrektywy NIS 2.

- **Kompetencje miękkie w sytuacjach kryzysowych:** Dodanie modułu „Komunikacja w incydencie". Technik musi umieć jasno raportować zagrożenia kadrze zarządzającej, co jest kluczowe przy rosnącej odpowiedzialności prawnej firm za wycieki danych.

Ponadto, wskazujemy kluczowe uwarunkowania, bez których nowy zawód nie będzie mógł odegrać tak dużej w roli w gospodarce, jak pokładane w nim nadzieje.

**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 nieprzystające do rynku IT. Ekspert z branży cybersec (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, powinno 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 UPo.



Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

**2. Model "Dual-Use" – priorytet dla rozwoju 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".

**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 zatrudniać ekspertów mundurowych w celu hartowania tych postaw.

**3. Infrastruktura chmurowa zamiast „martwego" sprzętu**

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.

**Rekomendacja:** Zdobycie przez ucznia uznanego komercyjnego certyfikatu (np. CISCO, CompTIA) powinno automatycznie zwalniać z części państwowego egzaminu zawodowego.

W przypadku pytań dotyczących przedmiotowej kwestii, osobą do kontaktu w Konfederacji Lewiatan jest dr Sławomir Szymczak, ekspert w Departamencie Pracy, e-mail: sszymczak@lewiatan.org , tel. kom. 794 646 999.

Wyrażamy pełną gotowość do współpracy w tym zakresie.

Z poważaniem

Krzysztof Kajda

Krzysztof Kajda
Zastępca Dyrektor Generalnej Konfederacji Lewiatan