



Szanowna Pani  
Kaja Kondratiuk  
Koordynator Prac Wydziału Szkoleń  
i Programu Partnerstwa  
Departament Cyberbezpieczeństwa

**Dotyczy:**

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

Szanowna Pani,

W odpowiedzi na pismo dotyczące wniosku MRiRW dotyczącego wprowadzenia do systemu oświaty zawodów związanych z cyberbezpieczeństwem „Pracodawcy Pomorza” przekazują opinię w powyższej sprawie.

Analiza założeń do projektu podstawy programowej kształcenia w zawodzie technik cyberbezpieczeństwa po konsultacjach z pracodawcami branży informatycznej zdaniem „Pracodawców Pomorza” co do zasady jest skonstruowany prawidłowo. Jednak zawartość 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 naszej organizacji wskazali 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”;

- *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 skomplikowanie 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*



# Pracodawcy Pomorza

---

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.

Jednocześnie sugerujemy do rozważenia następujące zagadnienia:

- **Rozszerzenie analizy zagrożeń o deepfake, dezinformację i phishing:** Absolwent powinien umieć identyfikować manipulacje audiowizualne (AI-generated) oraz rozumieć wektor ataku 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.

Z poważaniem,

Wiceprezes Zarządu  
Pracodawców Pomorza

  
Wojciech Szczepański

Prezes Zarządu  
Pracodawców Pomorza

  
Tomasz Limon