LEWIATAN

Warszawa, 6 marca 2026 r.
KL/164/46/SSz/2026

Dot. pisma: DC.WSiPP.5541.7.2025

opinia na temat planowanego wprowadzenia nowego zawodu do klasyfikacji szkolnictwa branżowego – „Technik cyberbezpieczeństwa”

Pan
Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

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 stoi na stanowisku, że zmiany w obszarze szkolnictwa zawodowego są nieodzowne, a tempo wprowadzanych zmian w zakresie dostosowywania podstaw programowych kształcenia zawodowego, aktualizacji klasyfikacji szkolnictwa branżowego, a także wprowadzania nowych zawodów do klasyfikacji szkolnictwa branżowego powinno być wysokie i dopasowane do przemian technologicznych wpływających na rynkek pracy.

Z zadowoleniem przyjmujemy, że Ministerstwo Cyfryzacji dostrzega potrzebę uzupełnienia nieodoboru specjalistów w obszarze cyberbezpieczeństwa i kształcenia kadr już na poziomie szkolnictwa branżowego. Jesteśmy przekonani, że wprowadzenie zawodu technik cyberbezpieczeństwa umożliwi przygotowanie absolwentów do pracy w zespołach IT i SOC, a także wpłynie na wzmocnienie bezpieczeństwa cyfrowego przedsiębiorstw oraz zmniejszenie luki kompetencyjnej na rynku pracy.

W opinii Konfederacji Lewiatan, absolwent programu kształcenia w zakresie cyberbezpieczeństwa powinien opanować efekty kształcenia umożliwiające rozpoczęcie pracy na stanowiskach juniorskich w obszarze cyberbezpieczeństwa. Ważne jest, aby absolwent rozumiał podstawowe zasady cyberbezpieczeństwa, w tym znaczenie poufności, integralności i dostępności informacji (CIA), a także potrafił identyfikować zagrożenia, podatności oraz ryzyka związane z funkcjonowaniem systemów informatycznych. Znajomość najczęstszych technik stosowanych w cyberatakach, takich jak złośliwe oprogramowanie, phishing, ataki typu denial-of-service czy socjotechnika,

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

oraz posługiwanie się wiedzą z zakresu bezpieczeństwa sieci komputerowych, w szczególności dotyczącego protokołów TCP/IP, adresacji sieciowej oraz architektury infrastruktury IT – należy do podstawowych wymagań pracodawców zatrudniających osoby odpowiedzialne za obszar cyberbezpieczeństwa. Absolwent powinien umieć konfigurować i stosować podstawowe mechanizmy ochrony sieci, takie jak zapory sieciowe, listy kontroli dostępu (ACL), wirtualne sieci prywatne (VPN) czy zabezpieczenia sieci bezprzewodowych.

Do innych kluczowych kompetencji należy zaliczyć również kompetencje w zakresie zabezpieczania systemów końcowych, w tym systemów Windows, Linux i macOS; korzystanie z narzędzi administracyjnych i diagnostycznych; analiza logów systemowych i sieciowych oraz wykrywanie anomalii oraz wspieranie procesów usuwania złośliwego oprogramowania. Nie bez znaczenia są umiejętności takie jak: podstawowe metody zarządzania podatnościami i ryzykiem, korzystanie ze źródeł informacji o zagrożeniach (threat intelligence) oraz wspieranie działań związanych z oceną bezpieczeństwa systemów informatycznych, znajomość zasad monitorowania zdarzeń bezpieczeństwa oraz podstaw reagowania na incydenty, w tym elementy informatyki śledczej i analizy powłamaniowej.

Pracodawcy zrzeszeni w Konfederacji Lewiatan wskazują także na potrzebę rozumienia znaczenia regulacji i standardów dotyczących ochrony danych i bezpieczeństwa informacji (np. GDPR, PCI-DSS) oraz znajomość podstawowych zasad zapewnienia ciągłości działania organizacji i odtwarzania systemów po awarii.

Uzyskane kompetencje pozwalają absolwentowi na podjęcie pracy na stanowiskach takich jak: młodszy specjalista ds. cyberbezpieczeństwa, technik bezpieczeństwa IT, analityk SOC (poziom podstawowy) lub administrator systemów i sieci z elementami bezpieczeństwa. Taki program stanowi również przygotowanie do dalszego rozwoju zawodowego i zdobywania kolejnych certyfikacji w obszarze cyberbezpieczeństwa.

Kluczowe efekty kształcenia

Absolwent kształcenia w zawodzie technik cyberbezpieczeństwa:

- rozumie najczęstsze zagrożenia cybernetyczne oraz metody działania cyberprzestępców,
- zna podstawowe zasady bezpieczeństwa sieci i protokołów TCP/IP,
- potrafi identyfikować podatności oraz proponować działania ograniczające ryzyko,
- diagnozuje i rozwiązuje problemy bezpieczeństwa sieci przewodowych i bezprzewodowych,

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

- korzysta z narzędzi administracyjnych systemów Windows i Linux w kontekście bezpieczeństwa,
- wdraża podstawowe mechanizmy ochrony systemów, sieci i stacji końcowych,
- konfiguruje kontrolę dostępu, listy ACL oraz zapory sieciowe,
- stosuje podstawowe techniki kryptograficzne w celu ochrony danych,
- analizuje logi, alerty i zdarzenia bezpieczeństwa,
- wykorzystuje narzędzia do testowania bezpieczeństwa oraz źródła threat intelligence,
- uczestniczy w procesach zarządzania podatnościami i oceną ryzyka,
- zna podstawy reagowania na incydenty oraz informatyki śledczej,
- stosuje dobre praktyki zapewniające poufność, integralność i dostępność informacji.

Rekomendujemy uwzględnienie powyższych efektów kształcenia w programie nauczania technikum. Zakres ten odpowiada aktualnym potrzebom rynku pracy, a także przygotowuje uczniów do podjęcia pracy na stanowiskach juniorskich lub dalszego kształcenia i specjalizacji oraz zdobywania certyfikacji branżowych. Włączenie wskazanych efektów kształcenia do programu nauczania zapewni użyteczność kwalifikacji absolwentów technikum oraz ich konkurencyjność na rynku pracy. Podkreślamy, że ważnym elementem kształcenia jest możliwość zewnętrznej weryfikacji umiejętności zgodnej ze standardami rynkowymi (przygotowanie do certyfikacji np. CCST Cybersecurity).

Drugim równie ważnym elementem jest zapewnienie elastyczności i modularności programu kształcenia tak, by uwzględniał on rozwój technologii i konieczność ewentualnych modyfikacji treści kształcenia w trakcie 5-letniego cyklu kształcenia. Zwracamy też uwagę na kompetencje społeczne, obejmujące umiejętność komunikacji, pracy zespołowej oraz wspierania użytkowników i zespołów nietechnicznych w zakresie podnoszenia świadomości bezpieczeństwa i stosowania dobrych praktyk w obszarze cyberbezpieczeństwa.

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 wyrazami szacunku

Marek Górski
Prezydent Konfederacji Lewiatan