POLSKIE TOWARZYSTWO INFORMATYCZNE

Zarząd Główny, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: + 48 22 838 47 05, tel./fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl, www.pti.org.pl

ZG/257/2017

Warszawa, 29.09.2017 r.

Wydział Edukacji i Współpracy Krajowej
Departament Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

Szanowni Państwo,

Polskie Towarzystwo Informatyczne w odpowiedzi na prośbę o przesłanie uwag dotyczących potrzeb uwzględnienia w "Klasyfikacji zawodów i specjalności" nowych zawodów bądź zrewidowania już istniejących, związanych z branżą IT, w tym w szczególności specjalności związanych z problematyką cyberbezpieczeństwo, przesyła swoją opinię i rekomendacje.

Dziękujemy za możliwość udziału w spotkaniu i dyskusji w sprawie kwalifikacji i zawodów, które odbyło się w maju 2017 w Ministerstwie Cyfryzacji.

Zgadzamy się ze stanowiskiem Ministerstwa Cyfryzacji wyrażonym podczas spotkania, że istnieje potrzeba uwzględnienia w "Klasyfikacji zawodów i specjalności" nowych zawodów oraz zrewidowania już istniejących.

Rosnąca rola bezpieczeństwa teleinformatycznego oraz obserwowany, zarówno w Polsce jak i na świecie, pogłębiający się deficyt pracowników związanych zawodowo z tym obszarem, wymusza podjęcie zdecydowanych działań mających na celu uporządkowanie definicji oraz potwierdzenie kwalifikacji zawodowych pracowników.

Rozpatrując aktualizację zawodów związanych z branżą IT chcielibyśmy zwrócić uwagę na nieobecność zawodu informatyka w aktualnej Klasyfikacji zawodów i specjalności (dalej KZiS), wprowadzonej rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. (Dz. U. z 2014 r. poz. 1145; zm.: Dz. U. z 2016 r. poz. 1876). Jest to o tyle dziwne, że w tejże Klasyfikacji znajdujemy takie zawody i specjalności jak:

- bioinformatyk,
- informatyk medyczny,
- inżynier teleinformatyk,
- technik informatyk.

W Polskim Towarzystwie Informatycznym wyrażane są opinie, że zawód "informatyk" powinien się pojawić w czterocyfrowej grupie 2120 „Matematycy, aktuariusze i statystycy i informatycy" oraz 2152 „Inżynierowie elektronicy" oraz że powinny być poczynione

działania na rzecz utworzenia osobnej grupy, zawierającej różne kategorie zawodu informatyka w zgodzie aktualnymi tendencjami rozwoju tej dziedziny. Ponadto jest też opinia, iż warto zaktualizować niektóre nazwy i rodzaje specjalności w grupie 25 "Specjaliści do spraw technologii informacyjno-komunikacyjnych" lub przemianować ją na "Specjaliści informatycy".

Dowodzi to tego, że kwestia pojęcia "informatyk" jest złożona i wywołuje różne opinie oraz propozycje. W kontekście KZiS pojęcie "informatyk" rodzi problemy też ze względu na odwzorowanie w tej klasyfikacji schematu The International Standard Classification of Occupations 2008 (dalej ISCO-08) Intenational Labour Organization (dostępne na stronie http://www.ilo.org/public/english/bureau/stat/isco/isco08/). Schemat nie wyodrębnia wprost grupy "informatyk" rozumianej jako "IT/ICT specialist", więc konsekwentnie polska KZiS również nie uwzględnia tego. Problem ten był już przedmiotem dyskusji w PTI w związku z prośbą GUS o zaopiniowanie i weryfikację typologii kodów zawodów związanych z ICT. Wynikiem tej dyskusji była opinia dostępna na stronie opinii PTI https://wstoin.pti.org.pl/wiki/15-08.01 . Niewątpliwie kwestia ta wymaga dalszych prac i studiów, które będą prowadzone również w ramach Rady Sektorowej ds. Kompetencji IT (http://radasektorowa.pl/).

Odnosząc się do rozważania dotyczącego zawodów i specjalności związanych z obszarem cyberbezpieczeństwa bądź też bezpieczeństwa teleinformatycznego proponujemy je rozpocząć od uporządkowania terminologii.

Brak zdefiniowanego pojęcia cyberbezpieczeństwo (próba dookreślenia tego terminu została podjęta jedynie w Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015) utrudnia jednoznaczną definicję zawodów i specjalności, w nazwie których występuje to pojęcie. Ubolewamy, że jeden z poważniejszych problemów trapiących rozwój sieci i systemów teleinformatycznych – bezpieczeństwo realizacji usług elektronicznych – jest nazywany medialnym stwierdzeniem cyberbezpieczeństwo, zamiast profesjonalnym pojęciem bezpieczeństwo teleinformatyczne na wzór bezpieczeństwa narodowego, wewnętrznego.

Rekomendujemy, aby konsekwentnie w polskiej terminologii zamiast terminu cyberbezpieczeństwo stosować określenie bezpieczeństwo teleinformatyczne.

Porównanie zapisów KZiS z zestawieniem zawodów i specjalności związanych z obszarem ICT poszukiwanymi obecnie przez pracodawców pokazuje, że istnieje szereg poszukiwanych zawodów/specjalności związanych z obszarem bezpieczeństwa teleinformatycznego, które nie znajdują odzwierciedlenia w przywoływanej tu wielokrotnie Klasyfikacji.

Poszukiwane zawody i specjalności

Analiza ofert zatrudnienia na wiodących portalach (np. LinkedIn, pracuj.pl) zawierających oferty pracy pokazuje, że obecnie poszukiwani są pracownicy na następujące stanowiska związane z szeroko pojętym bezpieczeństwem teleinformatycznym (w zestawieniu została zachowana terminologia podawana w ogłoszeniach):

- Analityk Bezpieczeństwa 2 linii (2L) Security Operation Center (SOC)
- Analityk Śledczy (IT Security)
- Blue Team Security Analyst
- Cloud Security Engineer

- Cyber Security Operator
- Cyber Security Scanning Engineer
- Data Protection Officer
- Ethical Hacker (Penetration tester)
- Information and Data Security Officer
- Information Security Analyst
- Information Security Architect
- Information Security Engineer
- Infrastructure Security Consultant
- IT Application Security Architect
- IT Auditor
- IT Security Engineer
- IT Security Senior Advisor
- IT Security Specialist
- IT Security Specialist – Cyber Security Monitoring
- Network Cyber Security - SOC SIEM Analyst
- Network Security Architect
- Security and Privacy Architect
- Security Architect
- Security Assessment Specialist
- Security Auditor
- Security Consultant
- Security Engineer
- Security Manager
- Security Operations Center (SOC) - Monitoring Specialist
- Security Program Manager
- Security Risk Analyst
- Security Solutions Architect
- Senior Cyber Security Operations Analyst
- Senior Cyber Security Operations Analyst
- Senior Security Engineer
- Software Security Engineer
- Vulnerability Researcher

Jak widać, większość z tych pozycji nie znajduje odzwierciedlenia w obowiązującej "Klasyfikacji zawodów i specjalności". W szczególności zasadnym wydawałoby się dodanie do KZiS takich nowych pozycji jak:

- Architekt bezpieczeństwa teleinformatycznego
- Analityk bezpieczeństwa teleinformatycznego
- Analityk ryzyka bezpieczeństwa teleinformatycznego
- Audytor bezpieczeństwa teleinformatycznego
- Audytor systemów informacyjnych
- Inżynier bezpieczeństwa teleinformatycznego
- Tester penetracyjny
- Analityk śledczy

Może to jednak być skomplikowane ze względu na wspomniane już odwzorowania w KZiS schematu ISCO-08, jak też dość długotrwała procedurę wprowadzania pozycji do KZiS. Możliwym rozwiązaniem byłoby utworzenie rozszerzenia KZiS jako wynik prac Rady Sektorowej i rekomendowanej do stosowania przez zainteresowane resorty.

Certyfikacje zawodowe

Obecnie pracodawcy weryfikują kompetencje dotyczące bezpieczeństwa teleinformatycznego pracowników na podstawie posiadanych przez nich certyfikatów zawodowych. Najczęściej są to certyfikaty branżowe wystawiane przez niezależne organizacje oraz producentów rozwiązań bezpieczeństwa. Pierwsze z wymienionych są certyfikacjami neutralnymi technologicznie a drugie są wprost powiązane z rozwiązaniami technicznymi oferowanymi przez danego producenta.

Najpopularniejsze obecnie certyfikaty branżowe związane z bezpieczeństwem teleinformatycznym to:

- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Control)
- SSCP (Systems Security Certified Practitioner)
- CompTIA Security+
- CEH (EC-Council Certified Ethical Hacker)
- OSCP (Offensive Security Certified Professional)
- OSCP (Offensive Security Certified Professional)
- OSCE (Offensive Security Certified Expert)
- GXPN (GIAC Exploit Researcher and Advanced Penetration Tester)
- OSWP (Offensive Security Wireless Professional)

Bardzo istotne jest, że uzyskanie wielu z ww. certyfikatów wymaga nie tylko zdania stosownych egzaminów, ale również udokumentowania pewnego okresu doświadczenia zawodowego w obszarze związanym z bezpieczeństwem teleinformatycznym.

Co więcej, wiele z najbardziej wartościowych certyfikatów ma określony okres ważności (np. 3 lata) i ich przedłużenia wymaga ciągłej edukacji.

Należy zwrócić uwagę, że wiedza wymagana do uzyskania ww. certyfikatów nie uwzględnia znajomości polskich lub europejskich regulacji prawnych np. (ustawy o ochronie danych osobowych lub RODO, lecz uwzględnia wyłącznie regulacje USA, np. HIPAA, Sarbanes-Oxley, PCI DSS. Z punktu widzenia polskich pracodawców może być to postrzegane jako wada.

System polskich neutralnych technicznie certyfikacji zawodowych związanych z bezpieczeństwem teleinformatycznym praktycznie nie istnieje. Znana jest certyfikacja EUCIP Professional oferowana przez Polskie Towarzystwo Informatyczne, będąca klonem systemu swego czasu opracowanego przez CEPIS. Możliwe są dwie specjalności:

- Doradca ds. Bezpieczeństwa,
- Audytor Systemów Informacyjnych.

Następcą systemu EUCIP były kolejne wydania systemu e-Competence Framewok (e-CF), z których wydane 3 z nieznacznymi zmianami zostało przyjęte jako norma europejska EN 16234 - e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors. Obecnie CEPIS wspiera tę normę. Norma, jak i e-CF

odnosi się do 40-tu uogólnionych obszarów kompetencji informatycznych. Związane z bezpieczeństwem teleinformatycznym są dwa obszary:

- Information Security Strategy Development
- Information Security Management

Również i w tym przypadku możliwym rozwiązaniem byłoby utworzenie rozszerzenia normy jako wynik prac Rady Sektorowej i rekomendowanej do stosowania przez zainteresowane resorty.

W tym kontekście naszym zdaniem należy stworzyć całkowicie polski system certyfikacji zawodowej, zawwierający obszar bezpieczeństwa teleinformatycznego. Taki system certyfikacji zawodowej powinien uwzględniać czołowe certyfikacje oferowane przez takie organizacje jak ISACA (certyfikaty CISA, CISM, CRISC), (ISC)2 (certyfikaty CISSP, SSCP) oraz polskie i europejskie regulacje (np. RODO, dyrektywa NIS, przyszła ustawa o cyberbezpieczeństwie). Utworzenie takiego systemu jest jednym z zamiarów PTI, związanych ze strategią i zadaniami statutowymi, a także z działalnością Rady Sektorowej. Jest to jednak przedsięwzięcie kosztowne i wymaga pozyskania źródeł finansowania.

Naszym zdaniem opracowanie systemu certyfikacji zawodowej obejmującej też obszar bezpieczeństwa teleinformatycznego wymaga szerszej dyskusji i konsultacji Ministerstwa Cyfryzacji ze środowiskiem zainteresowanym podnoszeniem adekwatnego poziomu bezpieczeństwa teleinformatycznego (np. takie organizacje jak PIIT, ISACA Polska, ISSA Polska). Polskie Towarzystwo Informatyczne wyraża gotowość udziału w tym procesie.

Odnosząc się do kolejnej kwestii przedstawienia informacji o oczekiwaniach firm i pracowników dotyczących możliwości podnoszenia kwalifikacji pracowników w obszarze cyberbezpieczeństwa oraz czy rynek spełnia te wymagania przekazujemy, że nie dysponujemy takimi danymi. Jest to oczywiście kluczowa sprawa i znajduje się w obszarze działalności Rady Sektorowej. Deklarujemy, że niezwłocznie po wypracowaniu takiego materiału zostanie on opublikowany i jednocześnie przekazany do ministerstwa.

Opracowanie: dr inż. Janusz Dorożyński, dr inż. Tomasz Klasa, mgr Janusz Żmudziński

DYREKTOR GENERALNY
Polskiego Towarzystwa Informatycznego
K. Pełka-Kamińska
Krystyna Pełka-Kamińska