Warszawa, dnia 29 grudnia 2020 r.

Poz. 1210

OBWIESZCZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 14 grudnia 2020 r.

w sprawie włączenia kwalifikacji rynkowej „Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle” do Zintegrowanego Systemu Kwalifikacji

Na podstawie art. 25 ust. 1 i 2 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2020 r. poz. 226) ogłasza się w załączniku do niniejszego obwieszczenia informacje o włączeniu kwalifikacji rynkowej „Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle” do Zintegrowanego Systemu Kwalifikacji.

Minister Cyfryzacji: wz. *M. Zagórski*

1) Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716).

Załącznik do obwieszczenia Ministra Cyfryzacji
z dnia 14 grudnia 2020 r. (poz. 1210)

INFORMACJE O WŁĄCZENIU KWALIFIKACJI RYNKOWEJ „ZARZĄDZANIE NIEZAWODNOŚCIĄ I CYBERBEZPIECZEŃSTWEM W ZAKRESIE URZĄDZEŃ ORAZ TECHNOLOGII W PRZEMYŚLE" DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

1. Nazwa kwalifikacji rynkowej

Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle

2. Nazwa dokumentu potwierdzającego nadanie kwalifikacji rynkowej

Certyfikat

3. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji rynkowej

Certyfikat jest ważny 3 lata. Przedłużenie certyfikatu następuje na podstawie dokumentów potwierdzających udział w min. jednym szkoleniu lub konferencji wskazanych przez IC w każdym roku w okresie ostatnich 3 lat. Dokumenty należy przedstawić przed upływem ważności certyfikatu.

4. Poziom Polskiej Ramy Kwalifikacji przypisany do kwalifikacji rynkowej

6 poziom Polskiej Ramy Kwalifikacji

5. Efekty uczenia się wymagane dla kwalifikacji rynkowej

Syntetyczna charakterystyka efektów uczenia się

Osoba posiadająca kwalifikację „Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle" samodzielnie realizuje plan zapobiegania zagrożeniom w zakresie urządzeń oraz technologii w przedsiębiorstwie. Posiada wiedzę dotyczącą niezawodności i cyberbezpieczeństwa oraz krajowych i europejskich regulacji prawnych w tych obszarach. Posługuje się technikami analizy zagrożeń i analizy ryzyka, np. HAZOP (Hazard and Operability Study), FMEA. Wykorzystuje systemy IT i OT w procesach biznesowych i operacyjnych przedsiębiorstwa. Opracowuje elementy schematu IT/OT. Określa wymagania dla dostawców rozwiązań technicznych. Lokalizuje miejsce naruszenia bezpieczeństwa w obszarze technologicznym po skutecznym cyberataku. Sporządza rejestr skutków cyberataku w sprzęcie. Tworzy scenariusze działań naprawczych i odtworzenia pracy sprzętu.

Zestaw 1. Posługiwanie się wiedzą z zakresu niezawodności i cyberbezpieczeństwa w zakresie urządzeń kontrolno-pomiarowych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Posługuje się pojęciami normatywnymi z obszaru niezawodności i cyberbezpieczeństwa	– omawia pojęcia niezawodności i cyberbezpieczeństwa; – omawia pojęcie cyklu życia obiektu w kontekście sprzętu i oprogramowania zgodnie z obowiązującymi normami UE; – charakteryzuje cyberzagrożenia pochodzące z cyberprzestrzeni, np. ransomware, trojany, wirusy, robaki, bots, DDoS (Distributed Denial of Service); – omawia urządzenia oraz technologie sieciowe służące do przeciwdziałania zagrożeniom, takie jak: Firewall, Intrusion Detection/Prevention System, Deep Packet Inspection.

02. Charakteryzuje normatywne techniki analityczne w odniesieniu do urządzeń kontrolno-pomiarowych	– omawia techniki analityczne (np. wstępną analizę zagrożeń (PHA), badania zagrożeń i zdolności do działania (HAZOP), procedurę analizy rodzajów i skutków uszkodzeń (FMEA)); – omawia zasady tworzenia i zastosowanie matrycy ryzyk; – charakteryzuje dostępne na rynku narzędzia programowe do wyznaczania rozkładów uszkodzeń (np. rozkład logarytmiczny, dwuparametrowy rozkład WEIBULL, chi-kwadrat); – omawia dostępne na rynku generyczne bazy o uszkodzeniach (np. OREDA, MILITARY HANDBOOK).
03. Charakteryzuje zagadnienia prawne związane z niezawodnością i cyberbezpieczeństwem	– omawia przepisy regulujące krajowy system cyberbezpieczeństwa; – wymienia europejskie normy dotyczące systemów zarządzania ciągłością działania; – omawia regulacje w zakresie bezpieczeństwa wydane przez NIST, ENISA; – charakteryzuje aktualne regulacje prawne dotyczące bezpieczeństwa funkcjonalnego elektrycznych, elektronicznych i programowalnych elektronicznych systemów związanych z bezpieczeństwem; – charakteryzuje aktualne regulacje prawne dotyczące bezpieczeństwa funkcjonalnego odnoszące się do przyrządowych systemów bezpieczeństwa w sektorze przemysłu procesowego.

Zestaw 2. Realizowanie polityki zapobiegania zagrożeniom w zakresie urządzeń kontrolno-pomiarowych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Analizuje opracowany plan zapobiegania w zakresie urządzeń kontrolno-pomiarowych	– weryfikuje strefy zagrożeń newralgiczne dla niezawodności i ciągłości działania na określonym obszarze/obiekcie; – zbiera dane niezbędne do uaktualnienia matrycy ryzyk; – opracowuje wskazane elementy schematu IT/OT (technologia informatyczna / sterowanie przemysłowe); – posługuje się dostępnym sprzętem i technologiami sieciowymi służącymi do zapobiegania zagrożeniom, np. Firewall, Intrusion Detection System, Intrusion Prevention System, Deep Packet Inspection, buduje strefy bezpieczeństwa poprzez właściwą segregację i segmentację sieci, posługuje się bazami generycznymi danych o uszkodzeniach, np. Military, Handbook.
02. Dostosowuje i wdraża plan zapobiegania zagrożeniom	– omawia elementy rejestru incydentów; – omawia elementy rejestru serwisu sprzętu i aktualizacji oprogramowania; – określa wymagania dla dostawców rozwiązań technicznych; – formułuje wnioski dla kadry zarządzającej.

Zestaw 3. Postępowanie po skutecznym cyberataku w zakresie urządzeń kontrolno-pomiarowych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Wykonuje czynności wstępne po skutecznym cyberataku	– sprawdza poprawność ustawień parametrów systemowych; – lokalizuje miejsce naruszenia bezpieczeństwa w obszarze technologicznym; – omawia procedury postępowania awaryjnego w zlokalizowanym obszarze naruszenia cyberbezpieczeństwa.

02. Prowadzi działania osłabiające skutki cyberataku	– tworzy scenariusze działań naprawczych; – określa minimalne wymagania sprzętowe do uruchomienia procesu naprawczego i serwisu; – opisuje kroki, jakie należy podjąć w celu uruchomienia procesu naprawy i serwisu.
03. Analizuje koszty możliwych strat	– rozróżnia obszary strat; – sporządza rejestr skutków cyberataku w sprzęcie; – tworzy scenariusz odtworzenia pracy sprzętu.

6. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację

1. Weryfikacja

Weryfikacja efektów uczenia się składa się z dwóch części: teoretycznej i praktycznej.

1.1. Metody

Na etapie weryfikacji są stosowane wyłącznie następujące metody: część pierwsza: test teoretyczny, część druga: analiza dowodów i deklaracji, obserwacja w warunkach symulowanych połączona z rozmową z komisją. W części pierwszej do zestawu efektów uczenia się 01 stosuje się wyłącznie test teoretyczny. W części drugiej do zestawu efektów uczenia się 02 i 03 stosuje się wyłącznie analizę dowodów i deklaracji w postaci portfolio oraz obserwację w warunkach symulowanych połączoną z rozmową z komisją. Metodą analizy dowodów i deklaracji jest weryfikowana umiejętność „Analizuje opracowany plan monitorowania i zapobiegania w zakresie zasobów ludzkich" z zestawu efektów uczenia się 02.

1.2. Zasoby kadrowe

Komisja walidacyjna składa się z co najmniej trzech członków, w tym przewodniczącego.

Przewodniczący komisji walidacyjnej musi posiadać:

– certyfikat CRP (Certified Reliability Professional) bądź inny z listy rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;

– stopień naukowy (8 PRK);

– min. 3 lata udokumentowanego doświadczenia w przeprowadzaniu egzaminów zdobytego w okresie ostatnich 5 lat.

Każdy z pozostałych członków komisji walidacyjnej musi spełniać następujące warunki:

– kwalifikacja pełna z 7 PRK;

– min. rok doświadczenia w przeprowadzaniu egzaminów.

Ponadto co najmniej jeden z członków komisji walidacyjnej musi posiadać certyfikat szkolenia międzynarodowego w ośrodku zajmującym się cyberbezpieczeństwem przemysłowym.

1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne

Potwierdzenie efektów uczenia się w części pierwszej pozwala na dopuszczenie do części drugiej weryfikacji. Pozytywny wynik części pierwszej jest ważny przez 3 miesiące od daty jej zaliczenia. Instytucja certyfikująca musi zapewnić: laboratorium symulujące sieć przemysłową (min. 20 komputerów połączonych w sieć imitującą instalację przemysłową klasy SCADA lub DCS); narzędzia programistyczne do obliczeń niezawodnościowych 2- lub 3-parametrycznych.

2. Identyfikowanie i dokumentowanie

Nie określa się wymogów dla etapu identyfikowania i dokumentowania efektów uczenia się.

7. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat.