MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 30 grudnia 2020 r.

Poz. 1214

OBWIESZCZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 14 grudnia 2020 r.

w sprawie włączenia kwalifikacji rynkowej „Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych” 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 przemyśle w zakresie zasobów ludzkich i proceduralnych” 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. 1214)

INFORMACJE O WŁĄCZENIU KWALIFIKACJI RYNKOWEJ „ZARZĄDZANIE NIEZAWODNOŚCIĄ I CYBERBEZPIECZEŃSTWEM W PRZEMYŚLE W ZAKRESIE ZASOBÓW LUDZKICH I PROCEDURALNYCH" DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

1. Nazwa kwalifikacji rynkowej

Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych

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 przemyśle w zakresie zasobów ludzkich i proceduralnych" samodzielnie realizuje plan zapobiegania zagrożeniom w zakresie zasobów ludzkich. 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. Lokalizuje wektory ataku w sieci OT/IT. Tworzy scenariusze działań naprawczych po skutecznym cyberataku. Analizuje koszty strat i przygotowuje schemat odtworzenia pracy instalacji. Zarządza pracą podległego zespołu oraz współpracuje z innymi specjalistami.

Zestaw 1. Posługiwanie się wiedzą z zakresu niezawodności i cyberbezpieczeństwa	
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; – omawia cyberzagrożenia pochodzące z cyberprzestrzeni np. ransomware, trojany, wirusy, robaki, bots, DDoS (Distributed Denial of Service);

	– podaje przykłady dostępnego sprzętu i technologii sieciowych służących do zapobiegania zagrożeniom, np. Firewall Intrusion Detection System, Intrusion Prevention System, Deep Packet Inspection, diody jednokierunkowe; – omawia wyznaczanie strefy bezpieczeństwa poprzez właściwą segregację i segmentację sieci.
02. Charakteryzuje techniki analityczne w odniesieniu do zasobów sprzętowych	– 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; – omawia definicję „efektu domino”; – podaje przykład „efektu domino” w przedsiębiorstwie.
03. Charakteryzuje zagadnienia prawne związane z niezawodnością i cyberbezpieczeństwem	– omawia przepisy regulujące krajowy system cyberbezpieczeństwa; – omawia europejskie normy dotyczące systemów zarządzania ciągłością działania; – omawia regulacje w zakresie bezpieczeństwa wydane przez NIST, ENISA; – podaje przykłady dobrych praktyk rozwiązań prawno-normatywnych w zakresie niezawodności i cyberbezpieczeństwa, stosowanych w krajach Unii Europejskiej i USA; – wymienia aktualne regulacje prawne dotyczące bezpieczeństwa funkcjonalnego elektrycznych, elektronicznych i programowalnych elektronicznych systemów związanych z bezpieczeństwem.

Zestaw 2. Realizowanie polityki zapobiegania zagrożeniom w zakresie zasobów ludzkich i proceduralnych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Zarządza pracą zespołu	– określa zadania członków zespołu; – określa czas i kolejność realizacji zadań; – wskazuje kompetencje członków zespołu niezbędne do realizacji zadań; – określa sposoby monitorowania realizacji zadań; – wskazuje działy, z którymi musi podjąć współpracę w celu realizacji zadań.
02. Analizuje opracowany plan zapobiegania zagrożeniom w zakresie zasobów ludzkich	– weryfikuje strefy zagrożeń newralgiczne dla niezawodności i ciągłości działania na określonym obszarze/obiekcie; – zbiera dane niezbędne do uaktualnienia matrycy ryzyk; – aktualizuje schemat IT/OT (technologia informatyczna / sterowanie przemysłowe); – wskazuje mocne i słabe punkty zaproponowanych rozwiązań IT/OT; – formułuje informację zwrotną dotyczącą planu monitorowania i zapobiegania zagrożeniom; – aktualizuje dokumentację dotyczącą schematu IT/OT; – określa urządzenia oraz technologie sieciowe służące do przeciwdziałania zagrożeniom, takie jak: Firewall, Intrusion Detection/Prevention System, Deep Packet Inspection.

03. Dostosowuje i wdraża plan zapobiegania zagrożeniom	– analizuje zapisy w rejestrze incydentów; – formułuje wnioski dla zarządu; – formułuje zalecenia dla działu sterowania procesami technologicznymi.

Zestaw 3. Postępowanie po skutecznym cyberataku w zakresie zasobów ludzkich i proceduralnych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Wykonuje czynności wstępne po skutecznym cyberataku	– lokalizuje miejsce wejścia (wektory ataku) do obszaru IT/OT; – omawia procedury postępowania po incydencie, m.in. w zakresie informatyki śledczej; – sporządza protokół z postępowania.
02. Prowadzi działania osłabiające skutki cyberataku	– tworzy scenariusze działań naprawczych; – wskazuje i uzasadnia wybór optymalnego scenariusza dla danej sytuacji; – opisuje kroki, jakie należy podjąć w celu uruchomienia działań naprawczych.
03. Analizuje koszty możliwych strat	– rozróżnia obszary strat; – sporządza rejestr skutków cyberataku w technologii; – tworzy scenariusz odtworzenia pracy instalacji.

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.