Kwalifikacja cząstkowa na poziomie szóstym Polskiej Ramy Kwalifikacji i europejskich ram kwalifikacji

Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych

Status: włączona funkcjonująca

Rodzaj: cząstkowa

Kategoria: wolnorynkowe

Data włączenia do ZSK: 2020-12-28

Dokument potwierdzający nadanie kwalifikacji: Certyfikat kwalifikacji wolnorynkowej

Krótka charakterystyka kwalifikacji

Osoba posiadająca kwalifikację "Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych" jest przygotowana do opracowania planu zapobiegania zagrożeniom w organizacji. Posiada pogłębioną wiedzę dotyczącą niezawodności i cyberbezpieczeństwa oraz krajowych i europejskich regulacji prawnych w tych obszarach (m.in. zjawiska z obszaru wojny informacyjnej jak np. "fake news" oraz "deepfake"). Wykorzystuje systemy IT (information technology) i OT (operational technology) w procesach biznesowych i operacyjnych organizacji. Zarządza zespołem analiz incydentów IT/OT. Prowadzi politykę organizacji po skutecznym cyberataku. Analizuje politykę bezpieczeństwa zasobów ludzkich w kontekście najnowszych osiągnięć dotyczących powyższego obszaru.
Osoba posiadająca kwalifikację może znaleźć zatrudnienie między innymi w spółkach prawa handlowego, jednostkach samorządu terytorialnego lub przedsiębiorstwach przemysłu procesowego.

Informacje o kwalifikacji

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji

Kwalifikacją mogą być zainteresowani:
- członkowie i kandydaci na członków zarządów spółek skarbu państwa;
- członkowie zarządów samorządu terytorialnego i wyższy szczebel urzędników

samorządu terytorialnego oraz urzędów wojewódzkich;
- członkowie zarządów spółek prawa handlowego;
- prezesi i dyrektorzy ds. finansów z sektora przemysłu procesowego.

W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji

Osoba przystępująca do walidacji musi legitymować się kwalifikacją pełną z 6 poziomem PRK

Wymagane kwalifikacje poprzedzające

Opis

Kwalifikacja pełna z 6 poziomem PRK

Typowe możliwości wykorzystania kwalifikacji

Osoby posiadające kwalifikację mogą znaleźć zatrudnienie w:
- spółkach prawa handlowego;
- sektorze przemysłu procesowego (chemia, petrochemia, gaz, energetyka konwencjonalna, woda, ścieki, przemysł spożywczy i farmacja);
- jednostkach samorządu terytorialnego.

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności

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.

Zapotrzebowanie na kwalifikację

Z punktu widzenia cyberbezpieczeństwa cyfryzacja i automatyzacja w przemyśle, a także coraz większa integracja sieci przemysłowej (OT) z siecią architektury korporacyjnej (IT) są obecnie wyzwaniem dla przemysłu. Utrzymanie niezawodności, czyli ciągłości i zdolności produkcyjnych, w każdym przedsiębiorstwie staje się nierozerwalnym elementem cyberbezpieczeństwa. Kluczowe jest to zwłaszcza w kontekście przemysłu 4.0, który z jednej strony umożliwia łączenie maszyn i urządzeń przez internet, z drugiej zwiększa zagrożenia związane z cyberatakami. Na cyberataki szczególnie narażone są, z uwagi na ich rozproszenie i odmienne systemy zarządzania, systemy sterowania przemysłowego w obszarze przemysłu procesowego (chemia, petrochemia, gazownictwo, energetyka, przygotowanie i oczyszczanie wody, przemysł spożywczy i farmacja). Analiza danych z czujników sieciowych z 851 organizacji i przedsiębiorstw posiadających systemy produkcyjne na całym świecie pozwoliła sformułować następujące wnioski: * Stwierdzono, że ponad 40% systemów przemysłowych ma bezpośrednie podłączenie do internetu, skutkujące możliwością ingerencji w nią z zewnątrz; * Nieaktualne systemy operacyjne

wystąpiły w ponad 53% zakładach produkcyjnych; * Do 84% urządzeń zapewniony jest dostęp przez zdalne protokoły, możliwe do przełamania [https://cyberx-labs.com/resources/risk-report-2019/]. Stwierdzona skala zaniedbań wiąże się m.in. z problemem niedoskonałości proceduralnych oraz braku systemowego doskonalenia kwalifikacji kadr w organizacjach. Szkodliwe złośliwe oprogramowanie, takie jak WannaCry i NotPetya, oraz ukierunkowane ataki na systemy przemysłowe, takie jak TRITON i Industroyer, ukazały wysokie koszty przerw w produkcji, przywrócenia systemów, incydentów środowiskowych oraz przerw w dostawach usług kluczowych dla społeczeństwa, takich jak prąd, ciepło czy woda [https://www.rp.pl/Telekomunikacja-i-IT/170519335-Atak-ransomware-WannaCry-zainfekowal-ponad-200-tys-komputerow.html]. Rosnące z roku na rok zagrożenie skutkami cyberataków na instalacje przemysłowe wymaga adekwatnej obrony zasobów przemysłowych (za "Allianz Risk Barometer – Top Business Risks 2018", https://www.the-digital-insurer.com/allianz-risk-barometer-top-business-risks-for-2018/). Skuteczna obrona przemysłu powinna być, jak pokazują dobre praktyki wielu krajów, adekwatna do istniejącej architektury korporacyjnej w średnich i dużych organizacjach i przedsiębiorstwach oraz być obroną typu holistycznego, tj. opierać się na trzech filarach: 1. Polityka cyberbezpieczeństwa (szczebel menedżerski, decyzyjny). 2. Zarządzanie niezawodnością i cyberbezpieczeństwem (szczebel wykonawczy). 3. Technologia niezawodności i cyberbezpieczeństwa w przemyśle (szczebel wykonawczy). Realizacja skutecznej obrony przemysłu w zakresie cyberbezpieczeństwa opiera się m.in. na wykwalifikowanych pracownikach organizacji i przedsiębiorstw. Dlatego wyodrębniono 3 kwalifikacje odnoszące się do wskazanych powyżej filarów bezpieczeństwa. Wnioskowana kwalifikacja dotyczy zarządzania niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych. Międzynarodowe Centrum Bezpieczeństwa Chemicznego (ICCSS), które od wielu lat promuje najlepsze praktyki w przemyśle, w tym także dotyczące cyberbezpieczeństwa, widzi coraz większą potrzebę doskonalenia kadr na różnych poziomach z tematu cyberbezpieczeństwa. Rynek, zarówno w Europie, jak i na świecie, dostrzega coraz większe braki kadr, systemowo przygotowanych do wdrażania odporności oraz cyberbezpieczeństwa w przemyśle. Wychodząc naprzeciw tej potrzebie, ICCSS również wspiera rozwój nowej kwalifikacji oraz włączenie jej do ZSK. Obecnie cyberbezpieczeństwo to głównie temat dla techników oraz administratorów sieci, którzy powinni panować nad wieloma zagadnieniami jednocześnie. Ich kompetencje nie są opisane poprzez konkretne zawody, a zwykle są to niepisane praktyki zdobyte poprzez stanowisko administratora sieci. Brak sformalizowanych zasad dotyczących rekrutacji osób z takim wykształceniem powoduje, że jedynym kryterium przy wyborze na stanowiska takich osób jest doświadczenie zawodowe i liczba przepracowanych lat w dziale bezpieczeństwa IT. To jednak powoduje duży niedobór tego typu pracowników (na co wskazuje w liście rekomendacyjnym szef bezpieczeństwa Grupy LOTOS), a także powoduje, że koszty pozyskiwania pracowników są wysokie. Jest to kluczowy problem dla menedżerów, którzy nie dysponują odpowiednimi zasobami do wdrażania polityki cyberbezpieczeństwa. Jednak zgodnie ze światowymi trendami odchodzi się od podejścia, w którym to tylko informatycy dbają o cyberbezpieczeństwo. Cyberbezpieczeństwo staje się tematem całej organizacji, w tym pracowników na różnym szczeblu, od szczebla decyzyjnego po wykonawczy. Dlatego wnioskuje się o wprowadzenie także dwóch innych kwalifikacji: (1) Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle oraz (2) Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych, które wzajemnie się uzupełniają. Wnioskowana kwalifikacja jest odpowiedzią na konieczność doceniania problematyki i wagi cyberbezpieczeństwa przez Zarząd organizacji i przedsiębiorstw, w tym uwzględnianie tych aspektów w planowaniu budżetu, budowaniu dalekosiężnych strategii odporności przedsiębiorstwa, pozyskiwaniu wiedzy dotyczącej tego, jak reagować na incydenty, dbając przy tym o kwestie bezpieczeństwa pracowników oraz wizerunkowe. Ta kwalifikacja, w połączeniu z dwiema innymi, stanie się narzędziem dla zarządu, pozwalającym zdefiniować potrzeby

menedżerów oraz techników, którzy na co dzień zmagają się z kwestiami cyberbezpieczeństwa. Kwalifikacja pozwala potwierdzić kompetencje zdobywane m.in. w ramach takich stanowisk pracy, jak np. dyrektor finansowy, dyrektora ds. bezpieczeństwa. Warto odnotować, że Business Insider Poland wśród najbardziej poszukiwanych 10 zawodów w Polsce w 2019 r. ekspertów z obszaru zapewniania cyberbezpieczeństwa w organizacjach i przedsiębiorstwach wymienia na drugim miejscu [https://businessinsider.com.pl/rozwoj-osobisty/kariera/najbardziej-pozadane-zawody-w-2019-roku/hs2k5wx].

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się

W obszarze szkolnictwa wyższego prowadzone są kierunki związane z cyberbezpieczeństwem i bezpieczeństwem narodowym, ale dotyczą one obszaru wojskowości i bezpieczeństwa państwa. Niniejsza kwalifikacja dotyczy cyberbezpieczeństwa w obszarze cywilnym, przemysłowym.

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 stosowane są 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 weryfikowana jest 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.

Informacje dodatkowe

Podstawa prawna włączenia kwalifikacji do ZSK

Na podstawie Obwieszczenia Ministra Cyfryzacji z dnia 2020-12-14 r. w sprawie włączenia kwalifikacji rynkowej >Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych< do Zintegrowanego Systemu Kwalifikacji (Monitor Polski z dnia 2020-12-28 r., poz. 1208) oraz na podstawie Obwieszczenia Ministra Cyfryzacji z dnia 2021-02-15 r. zmieniającego obwieszczenie w sprawie włączenia kwalifikacji rynkowej >Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych< do Zintegrowanego Systemu Kwalifikacji (Monitor Polski z dnia 2021-02-22 r., poz. 202)

Data rozpoczęcia funkcjonowania kwalifikacji w ZSK

2021-08-24

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji (w godzinach)

240

Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat

Termin następnego przeglądu kwalifikacji

2030-12-28

Kod dziedziny kształcenia

345 - Nauki o zarządzaniu i administracji

Kod PKD (wg klasyfikacji 2007)

62.03 - Działalność związana z zarządzaniem urządzeniami informatycznymi

Kod ISCED

0413 - Zarządzanie i administracja

Kod kwalifikacji (do 2020 roku)

6C342100006

Kod kwalifikacji (od 2020 roku)

13865

Streszczenie opinii uzyskanych podczas konsultacji projektu kwalifikacji

Informacje zawarte we wniosku, jak również opinie otrzymane w ramach konsultacji, wykazały zgodność tych kwalifikacji z potrzebami społecznymi oraz z zapotrzebowaniem na rynku pracy.

Efekty uczenia się

Syntetyczna charakterystyka efektów uczenia się

Osoba posiadająca kwalifikacje "Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych" opracowuje plan zapobiegania zagrożeniom w organizacji. Posiada pogłębioną wiedzą dotyczącą niezawodności i cyberbezpieczeństwa oraz krajowych i europejskich regulacji prawnych w tych obszarach (m.in. zjawiska z obszaru wojny informacyjnej jak np. "fake news" oraz deepfake"). Posługuje się technikami analizy zagrożeń i analizy ryzyka Wykorzystuje systemy IT i OT w procesach biznesowych i operacyjnych organizacji. Wyznacza obszary zagrożeń w organizacji, w tym prawdopodobieństwo wystąpienia "efektu domino". Uzasadnia wybór poziomu zagrożenia, jak również ocenia i weryfikuje szacunki nakładów na cyberbezpieczeństwo i niezawodność. Zarządza zespołem analiz incydentów IT/OT. Prowadzi politykę organizacji po skutecznym cyberataku. Tworzy scenariusze działań biznesowych i strategię upubliczniania informacji po skutecznym cyberataku. Analizuje skutki strat fizycznych lub wizerunkowych oraz przygotowuje scenariusze minimalizacji strat. Analizuje politykę bezpieczeństwa zasobów ludzkich w kontekście najnowszych osiągnięć dotyczących powyższego obszaru.

Zestawy efektów uczenia się

1) Posługiwanie się wiedzą z zakresu niezawodności i cyberbezpieczeństwa w zakresie zasobów ludzkich i technicznych

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

1. Posługuje się pojęciami normatywnymi z obszaru niezawodności i cyberbezpieczeństwa

Kryteria weryfikacji:

a. omawia pojęcia niezawodności i cyberbezpieczeństwa
b. omawia pojęcie cyklu życia (projekt, realizacja, eksploatacja, utylizacja) obiektu w kontekście sprzętu i oprogramowania
c. określa typowe zagrożenia pochodzące z cyberprzestrzeni np. ransomware, trojany, wirusy, robaki, bots, DDoS (Distributed Denial of Servise)

2. Charakteryzuje normatywne techniki analityczne

Kryteria weryfikacji:

a. omawia techniki analityczne (np. wstępna analiza zagrożeń (PHA), badania zagrożeń i zdolności do działania (HAZOP), procedura analizy rodzajów i skutków uszkodzeń (FMEA))

b. omawia definicję "efektu domino"
c. podaje przykład "efektu domino" w przedsiębiorstwie
d. omawia zasady tworzenia i zastosowanie matrycy ryzyk

3. Charakteryzuje zagadnienia związane z kształtowaniem polityki bezpieczeństwa zasobów ludzkich

Kryteria weryfikacji:

a. analizuje politykę bezpieczeństwa zasobów ludzkich w kontekście najnowszych osiągnięć dotyczących powyższego obszaru
b. omawia elementy planu walki z "fake news" i "deep news"
c. podaje przykłady zastosowania planu walki z "fake news" i "deep news"
d. omawia sposoby postępowania w przypadku ujawnienia cybermolestowania i cyberstalkingu
e. omawia sposoby postępowania w przypadku wystąpienia cyberprzemocy, np. wobec kobiet

4. Charakteryzuje zagadnienia prawne związane z niezawodnością i cyberbezpieczeństwem

Kryteria weryfikacji:

a. wymienia nazwy regulacji odnoszące się do krajowego systemu cyberbezpieczeństwa
b. omawia przepisy regulujące krajowy system cyberbezpieczeństwa
c. omawia europejskie normy dotyczące systemów zarządzania ciągłością działania i bezpieczeństwa
d. omawia zasady tworzenia strategii i polityki niezawodności i cyberbezpieczeństwa
e. omawia zasady pracy zespołu ds. analiz incydentów IT/OT

2) Opracowanie planu zapobiegania zagrożeniom w zakresie zasobów ludzkich i technicznych w organizacji

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

1. Analizuje zagrożenia i ryzyka pod kątem niezawodności i cyberbezpieczeństwa

Kryteria weryfikacji:

a. identyfikuje strefy zagrożeń newralgiczne dla niezawodności i ciągłości działania na określonym obszarze/obiekcie
b. ocenia ryzyko na określonym obszarze, posługując się matrycą ryzyka
c. identyfikuje potencjalne społeczne cyberzagrożenia w miejscu pracy (np. cyberstalking, cybermolestowanie)
d. podaje przykłady rozwiązań i środków zapobiegawczych w obszarze społecznych cyberzagrożeń w miejscu pracy

2. Przygotowuje plan zapobiegania zagrożeniom w zakresie zasobów ludzkich i technicznych w organizacji

Kryteria weryfikacji:

a. formułuje wnioski i zalecenia dla organizacji na podstawie analizy zapisów w rejestrze incydentów
b. sporządza plan zapobiegania zagrożeniom (uwzględniający m.in. opis sytuacji, możliwe rozwiązania i scenariusze działania z uwzględnieniem obowiązujących przepisów prawa)

3. Zarządza pracą zespołu IT/OT

Kryteria weryfikacji:

a. określa zadania członków zespołu
b. określa czas i kolejność realizacji zadań
c. wskazuje kompetencje członków zespołu niezbędne do realizacji zadań
d. określa sposoby monitorowania realizacji zadań
e. wskazuje działy z którymi musi podjąć współpracę w celu realizacji zadań

3) Postępowanie po skutecznym cyberataku w zakresie zasobów ludzkich i technicznych w organizacji

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

1. Wykonuje czynności wstępne po skutecznym cyberataku

Kryteria weryfikacji:

a. analizuje dostępne źródła informacji o cyberataku (w tym prasę i media społecznościowe)
b. sporządza wstępną informację dotyczącą szacunkowych strat i skutków wewnętrznych i zewnętrznych, jakie mogą wystąpić po cyberataku

2. Prowadzi działania osłabiające skutki cyberataku

Kryteria weryfikacji:

a. tworzy scenariusze działań biznesowych na podstawie pozyskanych informacji (np. z prasy, od dostawców i odbiorców, partnerów biznesowych)
b. tworzy scenariusze upublicznienia informacji o skutecznym cyberataku
c. wskazuje optymalny scenariusz dla danej sytuacji

3. Analizuje koszty możliwych strat

Kryteria weryfikacji:

a. rozróżnia rodzaje strat
b. sporządza wykaz strat fizycznych lub wizerunkowych oraz omawia ich skutki
c. tworzy scenariusze minimalizacji strat

Instytucje certyfikujące i podmioty powiązane z kwalifikacją

#	Instytucje certyfikujące (IC)	Instytucje walidujące
1	Intchem Sp. z o.o.	

Wnioskodawca:

Intchem Sp. z o.o.

Minister właściwy dla kwalifikacji:

Minister Cyfryzacji