Zintegrowany Rejestr Kwalifikacji

Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji*

Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle

Skrót nazwy

Rodzaj kwalifikacji*

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji*

6

Krótka charakterystyka kwalifikacji, obejmująca informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikacje oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji*

Osoba posiadająca kwalifikacje „Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń i 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. Wykorzystuje systemy IT (information technology) i OT (operational technology) w procesach biznesowych i operacyjnych przedsiębiorstwa. Opracowuje elementy schematu IT/OT. Lokalizuje miejsce naruszenia bezpieczeństwa w obszarze technologicznym po skutecznym cyberataku. Sporządza rejestr skutków cyberataku w sprzęcie. Tworzy scenariusze działań naprawczych i odtworzenia pracy sprzętu. Osoba posiadająca kwalifikację może znaleźć zatrudnienie między innymi w spółkach prawa handlowego, jednostkach samorządu terytorialnego lub przedsiębiorstwach przemysłu procesowego. Orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie kwalifikacji wynosi: 4000 zł

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]*

240

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Kwalifikacją mogą być zainteresowani: kierownicy działów IT / OT w spółkach kapitałowych małych i średnich przedsiębiorstw; kierownicy działów IT / OT w spółkach przemysłu

procesowego (wodociągi, ciepłownictwo, systemy sterowania ruchem ulicznym, itp.) podległych pod samorządy terytorialne; kierownicy działów urzędów miast i gmin.

Wymagane kwalifikacje poprzedzające

Opis

Kwalifikacja pełna z 6 poziomem PRK

Lista

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

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

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) Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w odniesieniu do zasobów ludzkich i technicznych oraz 2) Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych), które wzajemnie się uzupełniają. Wnioskowana kwalifikacja pozwala potwierdzić efekty uczenia się, które umożliwiają ukierunkowanie działań osoby odpowiedzialnej za bezpieczeństwo IT w myśl zdefiniowanych przez szczebel dyrektorski i menedżerski planów. Jednocześnie odpowiednio parametryzuje niezbędną wiedzę techniczną oraz proceduralną z zakresu cyberbezpieczeństwa, tak aby działania były skoordynowane z całością działań przedsiębiorstwa. Z uwagi na to, że nie jest możliwe określenie właściwej polityki cyberbezpieczeństwa bez wkładu techników oraz inżynierów, którzy tworzą sieć przemysłową, kluczowym aspektem tej kwalifikacji są także umiejętności dotyczące przekazywania informacji zwrotnej zarządowi. Kwalifikacja pozwala potwierdzić kompetencje zdobywane m.in. w ramach takich stanowisk pracy, jak np. administrator sieci IT, serwisant sieci OT. 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.

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.

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 w sprawie wykazu certyfikatów uprawniających do przeprowadzania audytu z dnia 12 października 2018; - 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.

Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy)

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się*

Osoba posiadająca kwalifikacje „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.

Zestawy efektów uczenia się

Numer zestawu w kwalifikacji*

1

Nazwa zestawu*

Posługiwanie się wiedzą z zakresu niezawodności i cyberbezpieczeństwa w zakresie urządzeń

kontrolno-pomiarowych

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

80

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

1. Posługuje się pojęciami normatywnymi z obszaru niezawodności i cyberbezpieczeństwa

Kryteria weryfikacji*

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 Servise). - omawia urządzenia oraz technologie sieciowe służące do przeciwdziałania zagrożeniom takie jak: Firewall, Intrusion Detection/Prevention System, Deep Packet Inspection,

Efekt uczenia się

2. Charakteryzuje normatywne techniki analityczne w odniesieniu do urządzeń kontrolno-pomiarowych

Kryteria weryfikacji*

omawia techniki analityczne (np. wstępna analiza zagrożeń (PHA), badania zagrożeń i zdolności do działania (HAZOP), procedura 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).

Efekt uczenia się

3. Charakteryzuje zagadnienia prawne związane z niezawodnością i cyberbezpieczeństwem

Kryteria weryfikacji*

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.

Numer zestawu w kwalifikacji*

2

Nazwa zestawu*

Realizowanie polityki zapobiegania zagrożeniom w zakresie urządzeń kontrolno-pomiarowych

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

80

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

1. Analizuje opracowany plan zapobiegania w zakresie urządzeń kontrolno pomiarowych

Kryteria weryfikacji*

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 służącym 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.

Efekt uczenia się

2. Dostosowuje i wdraża plan zapobiegania zagrożeniom

Kryteria weryfikacji*

omawia elementy rejestru incydentów; omawia elementy rejestru serwisu sprzętu i aktualizacji oprogramowania; określa wymagania dla dostawców rozwiązań technicznych; formułuje wnioski dla kadry zarządzającej.

Numer zestawu w kwalifikacji*

3

Nazwa zestawu*

Postępowanie po skutecznym cyberataku w zakresie urządzeń kontrolno-pomiarowych

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

80

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

1. Wykonuje czynności wstępne po skutecznym cyberataku

Kryteria weryfikacji*

sprawdza poprawność ustawień parametrów systemowych; lokalizuje miejsce naruszenia bezpieczeństwa w obszarze technologicznym; omawia procedury postępowania awaryjnego w zlokalizowanym obszarze naruszenia cyberbezpieczeństwa.

Efekt uczenia się

2. Prowadzi działania osłabiające skutki cyberataku

Kryteria weryfikacji*

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.

Efekt uczenia się

3. Analizuje koszty możliwych strat

Kryteria weryfikacji*

rozróżnia obszary strat; sporządza rejestr skutków cyberataku w sprzęcie; tworzy scenariusz odtworzenia pracy sprzętu.

Informacje o instytucjach uprawnionych do nadawania kwalifikacji

Wnioskodawca*

Intchem sp. z o.o.

Minister właściwy*

Ministerstwo Cyfryzacji

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.

Nazwa dokumentu potwierdzającego nadanie kwalifikacji*

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji*

Brak

Kod dziedziny kształcenia*

523 - Elektronika i automatyzacja

Kod PKD*

62.03 - Działalność związana z zarządzaniem urządzeniami informatycznymi

Status

Dokumenty

#	Tytuł dokumentu
1	Pismo rekomendujące kwalifikację - GRUPA LOTOS
2	Potwierdzenie płatności
3	ZRK_FKU_Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle
4	ZRK_FKU_Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle
5	ZRK_FKU_Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle

☐

Oświadczam, że dane zawarte we wniosku o włączenie kwalifikacji rynkowej do Zintegrowanego Systemu Kwalifikacji są zgodne z prawdą. Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.*

Dane o podmiocie, który złożył wniosek

Intchem sp. z o.o.
Siedziba i adres: Leszno 8/1, 01-192 Warszawa
NIP: 5272704870
REGON: 146975895
Numer KRS: 0000484765
Reprezentacja: Adam Paturej

Adres elektroniczny osoby wnoszącej wniosek: a.paturej@iccss.eu