Zintegrowany Rejestr Kwalifikacji

Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji*

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

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 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. Lokalizuje wektory ataku w sieci IT (information technology)/OT (operational technology). 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. 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: 1. Kierujący samodzielnymi lub wydzielonymi organizmami spółek kapitałowych. 2. Szefowie spółek technologicznych podległych pod samorząd terytorialny (np. wodociągów, spółek grzewczych, itp.). 3. Dyrektorzy działów organizacyjnych np. urzędów miast, gmin, itp.

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 dyrektorski, decyzyjny). 2. Zarządzanie niezawodnością i cyberbezpieczeństwem (szczebel menedżerski). 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) Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w odniesieniu do zasobów ludzkich i technicznych), które wzajemnie się uzupełniają. Wnioskowana kwalifikacja, mimo że w swej istocie nietechniczna, pozwala na lepsze zrozumienie zarówno potrzeb techników, jak i szczebla dyrektorskiego dot. strategii ochrony przedsiębiorstwa. Z jednej strony skupia się na budowaniu metryk, które pozwolą właściwie sprawdzać stan wdrożeń cyberbezpieczeństwa na dolnym poziomie, z drugiej strony pozwoli na odpowiednią implementację planów strategicznych stawianych przez zarząd. Kluczowym aspektem w tej kwalifikacji jest odpowiednie dysponowanie zasobami ludzkimi oraz dostosowywanie i wdrażanie procedur, które pozwolą na skuteczną implementację planu odporności oraz cyberbezpieczeństwa. Kwalifikacja pozwala potwierdzić tak opisane kompetencje, zdobywane m.in. np. w ramach takich stanowisk pracy, jak np. inżynier ds. utrzymania ruchu. 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.

Typowe możliwości wykorzystania kwalifikacji*

Osoby posiadające niniejszą 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 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.

Zestawy efektów uczenia się

Numer zestawu w kwalifikacji*

1

Nazwa zestawu*

Posługiwanie się wiedzą z zakresu niezawodności i cyberbezpieczeństwa

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; omawia cyberzagrożenia pochodzące z cyberprzestrzeni np. ransomware, trojany, wirusy, robaki, bots, DDoS (Distributed Denial of Servise). podaje przykłady dostępnego sprzętu i technologii sieciowych służącym 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

Efekt uczenia się

2. Charakteryzuje techniki analityczne w odniesieniu do zasobów sprzętowych

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; omawia definicję „efektu domino”; podaje przykład “efektu domino” w przedsiębiorstwie.

Efekt uczenia się

3. Charakteryzuje zagadnienia prawne związane z niezawodnością i cyberbezpieczeństwem

Kryteria weryfikacji*

- 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.

Numer zestawu w kwalifikacji*

2

Nazwa zestawu*

Realizowanie polityki zapobiegania zagrożeniom w zakresie zasobów ludzkich i proceduralnych

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. Zarządza pracą zespołu

Kryteria weryfikacji*

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.

Efekt uczenia się

2. Analizuje opracowany plan zapobiegania zagrożeniom w zakresie zasobów ludzkich

Kryteria weryfikacji*

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.

Efekt uczenia się

3. Dostosowuje i wdraża plan zapobiegania zagrożeniom

Kryteria weryfikacji*

analizuje zapisy w rejestrze incydentów; formułuje wnioski dla zarządu; formułuje zalecenia dla działu sterowania procesami technologicznymi.

Numer zestawu w kwalifikacji*

3

Nazwa zestawu*

Postępowanie po skutecznym cyberataku w zakresie zasobów ludzkich i proceduralnych

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*

lokalizuje miejsce wejścia (wektory ataku) do obszaru IT/OT; omawia procedury postępowania po incydencie m.in. w zakresie informatyki śledczej; sporządza protokół z postępowania.

Efekt uczenia się

2. Prowadzi działania osłabiające skutki cyberataku

Kryteria weryfikacji*

tworzy scenariusze działań naprawczych; wskazuje i uzasadnia wybór optymalnego scenariusza dla danej sytuacji; opisuje kroki, jakie należy podjąć w celu uruchomienia działań naprawczych.

Efekt uczenia się

3. Analizuje koszty możliwych strat

Kryteria weryfikacji*

rozróżnia rodzaje strat; sporządza rejestr skutków cyberataku w technologii; tworzy scenariusz odtworzenia pracy instalacji.

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 przemyśle w zakresie zasobów ludzkich i proceduralnych
4	ZRK_FKU_Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych
5	ZRK_FKU_Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych

☐

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