Miejscowość (forma spotkania), data

Opisywanie kwalifikacji rynkowej – formularz

Opis kwalifikacji rynkowej (nazwa kwalifikacji)

Zapewnianie cyberbezpieczeństwa sieci elektroenergetycznej

Materiał roboczy opracowany przy wsparciu Instytutu Badań Edukacyjnych w ramach projektu systemowego „Wspieranie funkcjonowania i doskonalenie ZSK na rzecz wykorzystania oferowanych w nim rozwiązań do realizacji celów strategii rozwoju kraju" współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach programu Operacyjnego Wiedza, Edukacja, Rozwój, Priorytet II: Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji, Działanie 2.13 Przejrzysty i spójny Krajowy System Kwalifikacji.
Zadanie 1: Wspieranie podmiotów zainteresowanych rozwojem oferty kwalifikacji funkcjonujących w ZSK i wspierających uczenie się przez całe życie.

Typ wniosku
Wniosek o włączenie kwalifikacji do ZSK
Nazwa kwalifikacji (300 znaków) *Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. a). Pełna nazwa kwalifikacji, która ma być widoczna w ZRK i być umieszczana na dokumencie potwierdzającym jej uzyskanie.* *Nazwa kwalifikacji (na ile to możliwe) powinna:* – *jednoznacznie identyfikować kwalifikację,* – *różnić się od nazw innych kwalifikacji,* – *różnić się od nazwy zawodu, stanowiska pracy lub tytułu zawodowego, uprawnienia,* – *być możliwie krótka,* – *nie zawierać skrótów,* – *być oparta na rzeczowniku odczasownikowym, np. „gromadzenie", „przechowywanie", „szycie".*
Zapewnianie cyberbezpieczeństwa sieci elektroenergetycznej
Skrót nazwy (150 znaków) *Pole nieobowiązkowe.*
nie dotyczy
Rodzaj kwalifikacji

Wskazanie, czy kwalifikacja jest: kwalifikacją pełną, czy kwalifikacją cząstkową.

cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji

Pole obowiązkowe (art. 15 ust. 1 pkt 4). Proponowany poziom Polskiej Ramy Kwalifikacji.

5 PRK

Krótka charakterystyka kwalifikacji oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji (4000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. d). Wybrane informacje o kwalifikacji skierowane do osób zainteresowanych uzyskaniem kwalifikacji oraz do pracodawców, które pozwolą im szybko ocenić, czy dana kwalifikacja jest właśnie tą, której poszukują.

Krótka charakterystyka może odpowiadać na pytanie: „Jakie działania lub zadania jest w stanie podejmować osoba posiadająca daną kwalifikację?”.

Osoba posiadająca kwalifikację jest przygotowana do wykonywania zadań związanych z zapewnieniem cyberbezpieczeństwa sieci elektroenergetycznych. Analizuje system zabezpieczeń danej sieci elektroenergetycznej pod kątem cyberbezpieczeństwa, wskazuje potencjalne zagrożenia dla sieci oraz danych związanych z jej funkcjonowaniem. Na podstawie modelu danej sieci i dokumentacji dotyczącej zabezpieczeń identyfikuje potencjalne miejsca wystąpienia zagrożenia. Przeprowadza testy bezpieczeństwa systemu, analizuje możliwe do zastosowania rozwiązania oraz rekomenduje podjęcie działań w celu zapewnienia cyberbezpieczeństwa sieci elektroenergetycznej . Ocenia zaproponowane rozwiązania zapewniające cyberbezpieczeństwo pod kątem możliwości ich wdrożenia i stosowania oraz zasadności wprowadzenia.

Posiadacz kwalifikacji nadzoruje działanie systemów cyberbezpieczeństwa sieci elektroenergetycznej. Zabezpiecza oprogramowanie wykorzystywane w sieci elektroenergetycznej, analizuje zabezpieczenia urządzeń współpracujących z siecią oraz monitoruje punkty dostępowe do sieci.

Identyfikuje i analizuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej. Wskazuje możliwe przyczyny zaistnienia incydentów oraz wskazuje incydenty wymagające natychmiastowej reakcji. Określa typ incydentu w obszarze cyberbezpieczeństwa sieci elektroenergetycznej, sporządza jego opis oraz dokonuje jego zgłoszenia, zgodnie z obowiązującymi przepisami prawa.

Osoba posiadająca kwalifikację może podjąć zatrudnienie:

- w podmiotach będących operatorami sieci przesyłowej i dystrybucyjnej, zakładach przemysłowych oraz w klastrach energetycznych na stanowiskach związanych m.in. z związanych z eksploatacją oraz ochroną inteligentnych sieci elektroenergetycznych przed zróżnicowanymi zagrożeniami cybernetycznymi,

- w podmiotach świadczących usługi związanych z ochroną inteligentnych sieci elektroenergetycznych przed zróżnicowanymi zagrożeniami cybernetycznymi na rzecz podmiotów zajmujących się wytwarzaniem, przesyłem i dystrybucją energii,
- w podmiotach dostarczających na rynek rozwiązania związane z zapewnianiem cyberbezpieczeństwa, przeznaczone dla branży energetycznej, np. jako konsultant, doradca klienta,
- w przedsiębiorstwach administrujących inteligentnymi budynkami,
- w firmach ubezpieczeniowych oferujących ubezpieczenia na wypadek naruszenia cyberbezpieczeństwa sieci elektroenergetycznej, jako specjalista ds. wyceny ryzyka i szacowania szkód.

Orientacyjna wysokość opłaty za przeprowadzenie walidacji i wystawienie dokumentu potwierdzającego otrzymanie kwalifikacji: 3.000,00 zł (trzy tysiące złotych).

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. c). Przeciętna liczba godzin, które trzeba poświęcić na osiągnięcie efektów uczenia się wymaganych dla danej kwalifikacji oraz na ich walidację (1 godzina = 60 minut).

W pierwszej kolejności warto ustalić orientacyjny nakład pracy dla poszczególnych zestawów efektów uczenia się. orientacyjny nakład pracy dla kwalifikacji odpowiada sumie nakładu pracy potrzebnego do uzyskania wyodrębnionych w niej zestawów efektów uczenia się.

240 godzin

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji (4000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. f). Informacja na temat grup osób, które mogą być szczególnie zainteresowane uzyskaniem danej kwalifikacji, np. osoby zarządzające nieruchomościami, specjaliści z zakresu telekomunikacji, kobiety powracające na rynek pracy.

Zainteresowane uzyskaniem kwalifikacji mogą być:

- osoby pracujące lub planujące pracę w zakresie zarządzania systemami zapewniającymi cyberbezpieczeństwo sieci elektroenergetycznych,
- osoby odpowiedzialne za sieci i systemy informatyczne w energetyce, zarówno zajmujące się ich eksploatacją, jak i dokonujące zakupów pozwalających na funkcjonowanie i rozwój tych systemów, które uzupełnią swoje kompetencje o zagadnienia związane z zapewnianiem cyberbezpieczeństwa,
- osoby zajmujące się utrzymaniem ruchu linii elektroenergetycznych,
- osoby odpowiedzialne za rozwój sieci elektroenergetycznych, biorące udział w podejmowaniu decyzji związanych z wyborem technologii i stosowanych rozwiązań,
- osoby będące użytkownikami i właścicielami systemów AMI (Advanced Metering Infrastructure),
- osoby odpowiedzialne za eksploatację sieci elektroenergetycznych w zakładach przemysłowych, klastrach energetycznych, podmiotach wytwarzających energię ze źródeł odnawialnych,
- osoby zajmujące się wdrażaniem i utrzymaniem systemów przemysłowego Internetu Rzeczy,
- osoby odpowiedzialne za zarządzanie inteligentnymi budynkami, zwłaszcza posiadającymi własne systemy wytwarzania energii,

- specjaliści ds. cyberbezpieczeństwa chcący rozwijać się w zakresie rozwiązań stosowanych w celu zapewniania bezpieczeństwa sieci elektroenergetycznych,
- osoby związane z branżą ubezpieczeniową, dokonujące oceny ryzyka cyberbezpieczeństwa sieci i instalacji elektroenergetycznych oraz szacujące szkody związane z wystąpieniem w sieciach elektroenergetycznych incydentów cyberbezpieczeństwa,
- osoby będące na początku ścieżki zawodowej, studiujące na kierunkach związanych z informatyką, energetyką i budownictwem oraz uczące się w zawodach szkolnictwa branżowego w branży teleinformatycznej (INF) i elektroenergetycznej (ELE).

Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)

☐ **Kwalifikacja może być przydatna dla uczniów szkół branżowych lub techników kształcących się w określonych zawodach**
Rozporządzenie MEN z dnia 16 maja 2019 r.

W szkole prowadzącej kształcenie zawodowe kształcenie odbywa się w oparciu o podstawy programowe określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego (Dz. U. poz. 991).

Część godzin zajęć może zostać przeznaczona na realizację obowiązkowych zajęć edukacyjnych przygotowujących uczniów do uzyskania kwalifikacji rynkowej funkcjonującej w ZSK, związanej z nauczanym zawodem (§ 4 ust 5 pkt 2 rozporządzenia Ministra Edukacji Narodowej z dnia 3 kwietnia 2019 r. w sprawie ramowych planów nauczania dla publicznych szkół (Dz. U. poz. 639)).

Należy wskazać zawody (zgodnie z klasyfikacją zawodów szkolnictwa branżowego określoną w załączniku nr 2 do rozporządzenia Ministra Edukacji Narodowej z dnia 15 lutego 2019 r. w sprawie ogólnych celów i zadań kształcenia w zawodach szkolnictwa branżowego oraz klasyfikacji zawodów szkolnictwa branżowego (Dz. U. poz. 316)), w przypadku których zasadne jest przygotowywanie uczniów do uzyskania kwalifikacji rynkowej objętej wnioskiem.

Wskazanie zawodów szkolnictwa zawodowego, z którymi związana jest kwalifikacja

Jeżeli w punkcie 7a wskazano przydatność kwalifikacji, to z rozwijanej listy branż i zawodów należy wybrać te zawody, z którymi związana jest wnioskowana kwalifikacja

Nie dotyczy

W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji (25000 znaków)

Pole obowiązkowe (Art. 15 ust.1 pkt 2g)

O ile dotyczy, należy podać warunki, które musi spełniać osoba, żeby przystąpić do walidacji i móc uzyskać kwalifikację (np. wymagany poziom wykształcenia – wyższe, podstawowe itp.; wymagana konkretna kwalifikacja poprzedzająca - np. dyplom ukończenia studiów medycznych albo dyplom potwierdzający kwalifikacje zawodowe w zawodzie np. „technik rachunkowości" itp.; zaświadczenie o niekaralności; orzeczenie lekarskie o braku przeciwwskazań itp.;).

Warunki przystąpienia do walidacji określone w opisie kwalifikacji powinny być możliwe do zweryfikowania (warunki te nie są tożsame z warunkami zatrudnienia).

Kompetencje wynikające z doświadczenia zawodowego powinny być odzwierciedlone przede wszystkim w opisie efektów uczenia się wymaganych dla kwalifikacji. Dlatego doświadczenie zawodowe powinno być wskazywane jako warunek przystąpienia do walidacji, jedynie w szczególnie uzasadnionych przypadkach.

Jeżeli nie ma takich warunków należy wpisać: „Brak warunków".

Brak warunków

Zapotrzebowanie na kwalifikację (25000 znaków)

Pole obowiązkowe (art. 15 ust.1 pkt 2) lit. i). Wykazanie, że kwalifikacja odpowiada na aktualne oraz przewidywane potrzeby społeczne i gospodarcze (regionalne, krajowe, europejskie).

Możliwe jest odwołanie się do opinii organizacji gospodarczych, trendów na rynku pracy, prognoz dotyczących rozwoju technologii, a także strategii rozwoju kraju lub regionu.

Cyberbezpieczeństwo jest kluczowym aspektem, który musi zostać uwzględniony przy projektowaniu, budowie i eksploatowaniu inteligentnych sieci elektroenergetycznych (Smart Grid). Sieci tego typu pozwalają na operowanie miksem różnych źródeł energii, od bloków energetycznych wykorzystujących paliwa kopalne, przez źródła odnawialne aż po energię jądrową, wytwarzaną przez zróżnicowanych producentów, zarówno wielkoskalowe firmy państwowe i prywatne, jak też niewielkich wytwórców indywidualnych. Są one niezbędne do kontrolowania produkcji energii z różnych, często rozproszonych i niestabilnych, źródeł, jej przesyłu, dystrybucji i magazynowania w ramach jednego spójnego systemu. Inteligentne sieci energetyczne umożliwiają podejmowanie, na podstawie zmieniających się czynników zewnętrznych i wewnętrznych, złożonych decyzji, optymalizujących proces wytwarzania, dostarczania i wykorzystywania energii elektrycznej. [1]

Zgodnie z założeniami Unii Energetycznej, do 2030 roku UE będzie musiała pozyskiwać 32% swojej energii ze źródeł odnawialnych i osiągnąć cel w postaci poprawy efektywności energetycznej o 32,5%. Realizacja tej strategii jest uznawana za kluczową również dla przyszłości energetycznej Polski i ma swoje odzwierciedlenie w Polskim Krajowym Planie na rzecz energii i klimatu na lata 2021-2030. [2] [3]

Konieczność realizacji tych strategii wiąże się z budową licznych rozproszonych źródeł energii odnawialnej oraz niekonwencjonalnej o zróżnicowanej mocy i trybach funkcjonowania. Konieczność spójnego zarządzania produkowaną w taki sposób energią, w tym do efektywnego wykorzystywania odnawialnych źródeł energii, zmusza do transformacji systemu energetycznego i tworzenia inteligentnych sieci energetycznych. Wymaga to budowy szeregu węzłów sieci, łączących nie zawsze spójne pod względem stosowanych rozwiązań, podsystemy zróżnicowanych wytwórców energii. Wielość i różnorodność punktów dostępowych, rozmaitość odbiorców, złożoność procedowanych danych oraz konieczność elastycznego łączenia różnych podsystemów, w poważny sposób podnoszą poziom zagrożenia cyberbezpieczeństwa w inteligentnej sieci energetycznej. Skuteczne ataki na takie sieci mogą spowodować istotne przerwy w dostawach energii, utrudniające funkcjonowanie gospodarki państwa oraz zagrażające bezpieczeństwu i zdrowiu ludzi.

Dlatego zapewnianie cyberbezpieczeństwa sieci elektroenergetycznej jest jednym z najważniejszych warunków utworzenia i działania inteligentnej sieci energetycznej.

Zagrożenia cyberbezpieczeństwa sieci elektroenergetycznych już obecnie jest bardzo wysokie. Według raportu z działalności CERT w roku 2021 liczba incydentów cyberbezpieczeństwa zgłoszonych w sektorze energetycznym wynosiła aż 4084, co stanowiło 13,85% wszystkich zgłoszeń. W żadnym innym sektorze gospodarki nie odnotowano tak wysokiej liczby incydentów cyberbezpieczeństwa. [5]

Rozwój inteligentnych sieci energetycznych, opartych na rozbudowanych technologiach informatycznych, podatnych na ataki spowoduje, że systemy elektroenergetyczne będą jeszcze bardziej narażone na takie ataki. Rozwój sieci energetycznych poprzez zwiększenie liczby użytkowników systemów, obsługujących te sieci, przyczynia się również do zwiększenia ryzyka związanego z czynnikiem ludzkim. Z tego powodu skuteczny rozwój inteligentnych sieci energetycznych wymaga tworzenia nowych i bardziej wydajnych rozwiązań z zakresu cyberbezpieczeństwa. Powoduje to potrzebę zatrudnienia dużej liczby wykwalifikowanych specjalistów, gotowych do zapewnienia cyberbezpieczeństwa przyszłej inteligentnej sieci elektroenergetycznej. Łącząc alternatywne i tradycyjne źródła energii w jeden system, będzie stanowić o skutecznej zielonej transformacji całej gospodarki.

Wiesław Paluszyński, Prezes Polskiego Towarzystwa Informatycznego i Przewodniczący Sektorowej Rady ds. Kompetencji Telekomunikacji i Cyberbezpieczeństwa, zauważa, że głównym problemem w obszarze cyberbezpieczeństwa nie jest brak rozwiązań technicznych, ale specjalistów cyberbezpieczeństwa. Jednocześnie, według publikacji „Raportu z badania społeczności IT 2021" w 2021 roku jedynie 2,2% uczestniczących w badaniu informatyków deklarowało zatrudnienie w sektorze energetycznym, przy czym badaniu nie wyróżniano specjalistów od zapewniania cyberbezpieczeństwa. [4] [6]

Tymczasem cyberbezpieczeństwo jest kluczowym aspektem dla działania inteligentnych sieci energetycznych. Musi ono zostać uwzględnione nie tylko przy ich projektowaniu, ale też w trakcie ich eksploatacji. Zakłócenie działania takiej sieci przez cyberatak może zagrozić funkcjonowaniu wszystkich elementów gospodarki i państwa. Tym samym kwalifikacja zapewnianie cyberbezpieczeństwa sieci elektroenergetycznej stanowi najważniejszy element prowadzący do skutecznego i bezpiecznego wdrożenia zielonej transformacji w systemie produkcji i dystrybucji energii, a przez to w całej gospodarce. Zadanie to wymaga zatrudnienia dużej liczby specjalistów, których potwierdzone kompetencje będą gwarantowały wysoki poziom obsługi w zakresie ochrony systemów sterowania i monitoringu, wsparcia systemów awaryjnych oraz bezpiecznej wymiany danych z podsystemami. Ich umiejętności będą dotyczyć zarówno zagadnień cyberbezpieczeństwa związanych z projektowaniem i funkcjonowaniem sieci energetycznych oraz innych aspektów, takich jak np. ochrona danych wrażliwych konsumentów i prosumentów energii.

Specjaliści do spraw zapewniania cyberbezpieczeństwa sieci elektroenergetycznej są obecnie bardzo poszukiwani na rynku pracy. Sytuacja ta wynika ze splotu kilku ważnych czynników

natury prawnej, społecznopolitycznej, ekonomicznej i związanych z bezpieczeństwem państwa.

Fundamentalne znaczenie zapewnienia cyberbezpieczeństwa infrastruktury i systemów kluczowych dla funkcjonowania państwa, w tym działania sieci elektroenergetycznych, znajduje swoje odzwierciedlenie w licznych aktach prawnych poziomu unijnego i krajowego, które nakładają na operatorów energetycznych szereg obowiązków i zadań w jego zakresie. [11]

Głównym aktem prawnym ustanawiającym w Polsce system cyberbezpieczeństwa jest Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U.2020.1369 t.j.), która wdraża w Polsce dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1). Na podstawie tej Ustawy powstał w Polsce system umożliwiający sprawne działania w zakresie wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo. Obejmuje on samorządy, dostawców usług cyfrowych i większość firm będących operatorami tak zwanych usług kluczowych dla funkcjonowania społeczeństwa. Wszystkie te podmioty, zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa, mają obowiązek raportować incydenty do właściwego zespołu CSIRT (Computer Security Incident Response Team). [10] [12] [13] [14]

W grudniu 2020 r. Komisja Europejska przedstawiła nowy pakiet przepisów określających cyberbezpieczeństwo, tzw. NIS2. W jego skład weszła propozycja działań na rzecz zapewnienia wysokiego poziomu cyberbezpieczeństwa w całej UE. NIS2 wprowadza nowe zasady odnoszące się do wielkości podmiotów objętych obowiązkiem jej stosowania, który zostaje rozciągnięty na wszystkie duże i średnie przedsiębiorstwa z sektora energetyki, a nie, jak do tej pory, jedynie na wskazanych przez krajowe organy cyberbezpieczeństwa operatorów usług kluczowych. Wprowadzony zostaje również obowiązek zgłaszania nie tylko, jak dotychczas, incydentów, ale również zagrożeń, co stawia przed podmiotami SOC (ang. Security Operations Center) oferującymi usługi w zakresie cyberbezpieczeństwa szereg nowych wyzwań. Dyrektywa NIS2 została przyjęta w grudniu 2022 roku i od tego czasu państwa członkowskie UE mają 21 miesięcy na włączenie nowych przepisów do prawa krajowego. Zaś w 18 miesięcy od przyjęcia dyrektywy wszystkie objęte Dyrektywą podmioty muszą być w stanie się do niej dostosować. Za niedostosowanie się do NIS2 grozi kara grzywny w wysokości do 10 milionów euro lub 2% całkowitego rocznego światowego obrotu firmy. [7]

Konieczność dostosowania się do wskazanych zmian w prawie powoduje na rynku pracy wszystkich państwach UE olbrzymi wzrost zainteresowania wykwalifikowanymi pracownikami do zajmujących się zapewnianiem cyberbezpieczeństwa sieci elektroenergetycznych. Wzrost ten jest potęgowany nie tylko poważnym zwiększeniem wolumenu przedsiębiorstw objętych przepisami i poszerzeniem obowiązków w zakresie zgłaszania incydentów i zagrożeń. Dodatkowo, w Polsce, popyt na pracowników posiadających kwalifikacje w zakresie zapewniania cyberbezpieczeństwa sieci elektroenergetycznej jest generowany przez działania na rzecz zielonej transformacji źródeł

energii, w tym budowę licznych niewielkich siłowni wiatrowych, wodnych i solarnych oraz małych reaktorów jądrowych (SMR). [8]

Obecnie, usługi świadczone przez specjalistów zapewniania cyberbezpieczeństwa sieci elektroenergetycznej są bardzo poszukiwane, ze względu na rosnące zapotrzebowanie na coraz bardziej opłacalną produkcję energii ze źródeł odnawialnych i paliw alternatywnych. Podłączane do krajowej sieci elektroenergetycznej farmy wiatrowe i fotowoltaiczne oraz elektrownie wodne, a wkrótce też reaktory SMR, będą, zgodnie z Dyrektywą NIS2, wymagać stałego zapewniania cyberbezpieczeństwa. Ponadto po 2022 roku stało się jasne, że działania takie są również istotne z uwagi na możliwość cyberataków na te sieci ze strony wrogich państw, co może być przejawem tak zwanej wojny hybrydowej. [9]

Wraz z rozwojem technologii Smart Grid oraz rosnącą liczbą nowych źródeł energii i odbiorników podłączanych do sieci energetycznych, ryzyko ataków cybernetycznych zwiększa się i staje się coraz bardziej złożone. Firmy energetyczne i podmioty SOC, oferujące rynkowe usługi zapewnienia cyberbezpieczeństwa sieci elektroenergetycznej, są gotowe przyjąć dużą liczbę pracowników. Jednak rosnące ryzyko związane z cyberatakami powoduje, że najbardziej poszukiwani będą pracownicy, którzy nie tylko odbyli odpowiednie szkolenie, ale posiadają certyfikat potwierdzający ich kompetencje.

Włączenie do Zintegrowanego Systemu Kwalifikacji kwalifikacji „Zapewnianie cyberbezpieczeństwa sieci elektroenergetycznej" pozwoli na obiektywną walidację kompetencji i uzyskanie przez zainteresowane osoby potwierdzenia posiadanych umiejętności.

Ostatnie lata zweryfikowały stan cyberbezpieczeństwa polskich instytucji oraz działających w kraju przedsiębiorstw, szczególnie operujących w obszarze tak zwanych przemysłów strategicznych i infrastruktury krytycznej, w tym administrującymi sieciami elektroenergetycznymi. W związku ze zwiększeniem się liczby incydentów zapotrzebowanie na specjalistów cyberbezpieczeństwa zdecydowanie wzrosło. Według raportu Hays „Tackling the Cyber Skills Gap. Global Cyber Security Report 2023" na całym świecie występuje olbrzymi niedobór specjalistów cyberbezpieczeństwa, sięgający około 2,3 miliona osób. Przygotowany przez PARP raport "Zastosowania sztucznej inteligencji w gospodarce, przegląd wybranych inicjatyw i technologii", powołując się na opracowanie „Cybersecurity. Raport o rynku pracy w Polsce", przygotowanym przez HackerU Polska i HRK ICT, w Polsce braki specjalistów cyberbezpieczeństwa sięgają nawet 17,5 tys. osób i przy obecnych trendach zatrudnienia będą się one stale powiększać. Braki kadrowe powodują, że niektóre z przedsiębiorstw korzystają w zakresie cyberbezpieczeństwa z usług podmiotów zewnętrznych, co nie daje jednak pewności co do kompetencji osób realizujących zadania. Według raportu, część firm albo nie ma w swoich zespołach IT osoby odpowiedzialnej za cyberbezpieczeństwo, albo zatrudnia osoby, które posiadają pewną wiedzę i umiejętności w tym obszarze, które nie są jednak potwierdzone żadnym certyfikatem. Według globalnego raportu Fortinet, z marca 2023, w przypadku branży cyberbezpieczeństwa aż 95% badanych liderów firm uważało, że certyfikaty mają pozytywny wpływ na zespół, a 81% woli zatrudniać osoby z certyfikatami. Włączenie opisywanej kwalifikacji do Zintegrowanego Systemu Kwalifikacji przyniesie korzyści w postaci spełnienia oczekiwań pracodawców, co do

możliwości zatrudnienia osób posiadających potwierdzone wiarygodnym certyfikatem kompetencje w zakresie zapewniania cyberbezpieczeństwa sieci elektroenergetycznych. Możliwość zdobycia poszukiwanego przez pracodawców certyfikatu zwiększy szanse pracowników na rozwój zawodowy, ułatwi przekwalifikowywanie się i aktywne kreowanie własnej ścieżki zawodowej. Ponadto przełoży się na wyższą jakość świadczonych usług w zakresie cyberbezpieczeństwa, czym przyczyni się do zwiększenia poziomu bezpieczeństwa w strategicznym z punktu widzenia polityki państwa sektorze. [15] [16] [17] [18]

Źródła danych (wybrane):

[1] S. Bielecki, Smart grid – elementy, korzyści i funkcjonalności dostępnych rozwiązań https://www.energetyka.plus/smart-grid-elementy-korzysci-i-funkcjonalnosci-dostepnych-rozwiazan/

[2] Unia energetyczna https://www.consilium.europa.eu/pl/policies/energy-union/

[3] Krajowy plan na rzecz energii i klimatu na lata 2021-2030 https://www.gov.pl/web/klimat/krajowy-plan-na-rzecz-energii-i-klimatu

[4] Potrzeby kompetencyjne w kontekście skutków pandemii koronawirusa. Raport zbiorczy z badania dotyczącego działań antyCOVIDowych w sektorach: Informatyka oraz Telekomunikacja i Cyberbezpieczeństwo, Warszawa 2021

[5] Raport roczny z działalności Cert Polska 2021, Warszawa 2022 https://cert.pl/uploads/docs/Raport_CP_2021.pdf

[6] Raport z badania społeczności IT 2021 https://bulldogjob.pl/it-report/2021

[7] L. Mróz, M. Wrzosek, Cyberbezpieczeństwo w energetyce – Dyrektywa NIS2, czyli wyzwania dla branży https://www.energetyka.plus/cyberbezpieczenstwo-w-energetyce-dyrektywa-nis2-czyli-wyzwania-dla-sektora-energetycznego/

[8] Małe reaktory jądrowe w Polsce. Podpisano ważne porozumienie https://tvn24.pl/biznes/z-kraju/male-reaktory-modulowe-w-polsce-podpisano-porozumienie-z-usa-i-kanada-6858427

[9] P. Łuczuk, Cyberwojna już się toczy. Co nam grozi? https://www.rp.pl/opinie-polityczno-spoleczne/art35753041-cyberwojna-juz-sie-toczy-co-nam-grozi

[10] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS)

[11] Zalecenie Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym

[12] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

[13] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych

[14] Rozporządzenie z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

[15] https://www.hays.co.uk/market-insights/global-cyber-security-report

[16] https://www.parp.gov.pl/storage/publications/pdf/Raport-tematyczny_zastosowania_sztucznej_inteligencji_w_gospodarce_20230616.pdf

[17] https://hackeru.pl/raport-o-pracy-w-cybersecurity/

[18] https://www.fortinet.com/blog/industry-trends/skills-gap-report-untap-talent

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się (6000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2 lit. k). Wyjaśnienie, czym kwalifikacja różni się od wybranych kwalifikacji o zbliżonym charakterze. Punktem odniesienia powinny być kwalifikacje funkcjonujące w ZSK. Ponadto wskazanie kwalifikacji wpisanych do ZRK, które zawierają co najmniej jeden taki sam zestaw efektów.

W Zintegrowanym Systemie Kwalifikacji znajdują się kwalifikacje o podobnym charakterze, takie jak:

- Zarządzanie cyberbezpieczeństwem – specjalista
- Zarządzanie cyberbezpieczeństwem – menedżer
- Zarządzanie cyberbezpieczeństwem - ekspert

Wymienione kwalifikacje obejmują umiejętności pozwalające na kompleksowe zarządzanie cyberbezpieczeństwem. Przeznaczone są one przede wszystkim dla specjalistów w zakresie cyberbezpieczeństwa odpowiedzialnych za ochronę informacji, bezpieczeństwo infrastruktury teleinformatycznej oraz kształtowanie polityki bezpieczeństwa, na różnych szczeblach organizacji. Niniejsza kwalifikacja koncentruje się natomiast na umiejętnościach związanych z zabezpieczeniem sieci elektroenergetycznych. Ujęte w niej efekty uczenia się dotyczą znajomości specyfiki zagrożeń związanych z funkcjonowaniem sieci elektroenergetycznych oraz umiejętności doboru mechanizmów zapewniających im bezpieczeństwo.

Ponadto w ZRK ujęto następujące kwalifikacje:

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

- Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych
- Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle.

Wymienione kwalifikacje dedykowane są do stosowania w przemyśle, ze szczególnym zorientowaniem na systemy informatyczne nadzorujące przebieg procesów technologicznych lub produkcyjnych SCADA (ang. Supervisory Control And Data Acquisition). Wymienione kwalifikacje koncentrują się na zagadnieniach bezpieczeństwa w środowiskach systemów sterowania przemysłowego w zakresie przemysłu procesowego. Wymienione kwalifikacje nie obejmują efektów uczenia się specyficznych dla zapewniania cyberbezpieczeństwa sieciom elektroenergetycznym.

Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)

☐ **Kwalifikacja zawiera wspólne lub zbliżone zestawy efektów kształcenia z „dodatkowymi umiejętnościami zawodowymi" w zakresie wybranych zawodów szkolnictwa branżowego**

Dodatkowe umiejętności zawodowe

Należy wybrać z listy „dodatkowe umiejętności zawodowe" (określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego, załącznik Nr 33) zawierające wspólne lub zbliżone zestawy efektów kształcenia z zestawami efektów uczenia się określonymi w kwalifikacji rynkowej.

Wskazanie „dodatkowych umiejętności zawodowych" w zakresie wybranych zawodów szkolnictwa branżowego zawierających wspólne lub zbliżone zestawy efektów kształcenia

(Branża – Zawód – Umiejętność)

Jeżeli w punkcie 11a udzielono pozytywnej odpowiedzi, to z rozwijanej listy branż, zawodów i dodatkowych umiejętności zawodowych należy wybrać te umiejętności, które zawierają wspólne lub zbliżone zestawy efektów kształcenia z wnioskowaną kwalifikacją

nie dotyczy

Typowe możliwości wykorzystania kwalifikacji (4000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. j). Omówienie perspektyw zatrudnienia i dalszego uczenia się, najistotniejszych z punktu widzenia rozwoju osobistego i zawodowego osób zainteresowanych uzyskaniem kwalifikacji.

Możliwe jest wskazanie przykładowych stanowisk pracy, na które będzie mogła aplikować osoba posiadająca daną kwalifikację.

Osoba posiadająca kwalifikację może podjąć zatrudnienie:

- w podmiotach będących operatorami sieci przesyłowej i dystrybucyjnej, zakładach przemysłowych oraz w klastrach energetycznych na stanowiskach związanych m.in. z związanych z eksploatacją oraz ochroną inteligentnych sieci elektroenergetycznych przed zróżnicowanymi zagrożeniami cybernetycznymi,

- w podmiotach świadczących usługi związanych z ochroną inteligentnych sieci elektroenergetycznych przed zróżnicowanymi zagrożeniami cybernetycznymi na rzecz podmiotów zajmujących się wytwarzaniem, przesyłem i dystrybucją energii,
- w podmiotach dostarczających na rynek rozwiązania związane z zapewnianiem cyberbezpieczeństwa, przeznaczone dla branży energetycznej, np. jako konsultant, doradca klienta,
- w przedsiębiorstwach administrujących inteligentnymi budynkami,
- w firmach ubezpieczeniowych oferujących ubezpieczenia na wypadek naruszenia cyberbezpieczeństwa sieci elektroenergetycznej, jako specjalista ds. wyceny ryzyka i szacowania szkód.

Posiadacz kwalifikacji może też prowadzić działalność gospodarczą jako niezależny konsultant w zakresie zapewniania cyberbezpieczeństwa sieci elektroenergetycznych.

Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację (25000 znaków)

Pole obowiązkowe (art. 15 ust.1 pkt 2) lit. h). Określenie wymagań stanowiących podstawę do przeprowadzania walidacji w różnych instytucjach. Wymagania powinny dotyczyć:

- *metod stosowanych w walidacji – służących weryfikacji efektów uczenia się wymaganych dla kwalifikacji, ale także (o ile to potrzebne) identyfikowaniu i dokumentowaniu efektów uczenia się;*
- *osób projektujących i przeprowadzających walidację;*
- *sposobu prowadzenia walidacji oraz warunków organizacyjnych i materialnych, niezbędnych do prawidłowego prowadzenia walidacji.*

Wymagania dotyczące walidacji mogą być wskazane dla pojedynczych zestawów efektów uczenia się lub dla całej kwalifikacji.

Wymagania mogą być uzupełnione o dodatkowe wskazówki dla instytucji oraz osób projektujących i przeprowadzających walidacje, a także dla osób ubiegających się o uzyskanie kwalifikacji.

1. Etap weryfikacji.

1.1. Metody:

Podczas weryfikacji efektów uczenia się muszą być wykorzystane metody:

- test teoretyczny
- obserwacja w warunkach symulowanych

1.2 Zasoby kadrowe

Zasoby kadrowe niezbędne do przeprowadzenia walidacji:

<u>Osoby przygotowujące narzędzia walidacyjne</u>

W przygotowanie narzędzi walidacyjnych muszą być zaangażowane co najmniej następujące osoby: ekspert branżowy posiadający minimum 3 lata doświadczenia w wykonywaniu zadań objętych kwalifikacją oraz ekspert metodyczny posiadający doświadczenie w opracowywaniu narzędzi walidacyjnych, które były wykorzystywane w ramach walidacji kwalifikacji rynkowej w rozumieniu ustawy o ZSK i przeszły proces ewaluacji wykonanej przez podmiot

zewnętrznego zapewnienia jakości (udział w przygotowaniu narzędzi walidacyjnych dla co najmniej 5 procesów weryfikacji).

Komisja walidacyjna

Komisja walidacyjna musi składać się co najmniej z 3 osób. Funkcję członka komisji walidacyjnej może pełnić osoba, która posiada udokumentowane, aktualne (nie starsze niż 5 lat przed datą przeprowadzenia walidacji), co najmniej 3-letnie doświadczenie w wykonywaniu zadań związanych z projektowaniem, konfigurowaniem, nadzorowaniem działania rozwiązań w zakresie cyberbepieczeństwa sieci elektroenergetycznych.

Co najmniej jedna osoba w komisji walidacyjnej posiada doświadczenie w weryfikowaniu efektów uczenia się w zakresie niniejszej kwalifikacji lub innych kwalifikacjach związanych z cyberbezpieczeństwem (udział w przeprowadzeniu co najmniej 5 procesów weryfikacji.

1.3. Sposób organizacji i zasoby materialne:

Instytucja Certyfikująca musi zapewnić następujące zasoby materialne do przeprowadzenia walidacji:

- test teoretyczny: sala egzaminacyjna, stanowisko dla każdego Kandydata umożliwiające samodzielną pracę, wyposażone w stół/biurko, krzesło, materiały piśmiennicze

- obserwacja w warunkach symulowanych: sala egzaminacyjna,stanowisko dla kandydata wyposażone w stół/biurko, krzesło, komputer z dostępem do internetu, materiały piśmiennicze, opis przypadku z kompletem informacji (w tym charakterystyka sieci elektroenergetycznej, odczyty z inteligentnych systemów monitorujących, dokumentacja dotycząca zabezpieczeń oraz zastosowanych urządzeń i mediów transmisyjnych, opis sytuacji, opis techniczny incydentu, dokumentacja techniczna systemu informatycznego, którego dotyczy incydent, dziennik zdarzeń systemowych), model sieci elektroenergetycznej oraz oprogramowanie pozwalające na symulację pracy sieci elektroenergetycznej

2. Identyfikowanie i dokumentowanie.

Nie określa się wymagań dla etapu identyfikowania i dokumentowania.

Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy) (1000 znaków)

Jeśli ustanowiono w danym sektorze lub branży Sektorową Ramę Kwalifikacji, to wypełnienie tego pola jest obowiązkowe (art. 15 ust. 1 pkt 4). Podaj propozycję odniesienia do poziomu odpowiednich Sektorowych Ram Kwalifikacji, jeśli są one włączone do ZSK.

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się (9000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1) lit. a). Zwięzła, ogólna charakterystyka wiedzy, umiejętności i kompetencji społecznych poprzez określenie działań, do których podjęcia będzie przygotowana osoba posiadająca daną kwalifikację.

Syntetyczna charakterystyka efektów uczenia się powinna nawiązywać do charakterystyki odpowiedniego poziomu PRK, w szczególności odpowiadać na pytania o przygotowanie osoby posiadającej kwalifikację do samodzielnego działania w warunkach mniej lub bardziej przewidywalnych, wykonywania działania o różnym poziomie złożoności, podejmowania określonych ról w grupie, ponoszenia odpowiedzialności za jakość i skutki działań (własnych lub kierowanego zespołu).

Osoba posiadająca kwalifikację wykonuje zadania związane z zapewnieniem cyberbezpieczeństwa sieci elektroenergetycznej. Dokonuje oceny i analizuje system zabezpieczeń danej sieci elektroenergetycznej pod kątem cyberbezpieczeństwa, wskazuje potencjalne zagrożenia dla sieci oraz danych związanych z jej funkcjonowaniem. Na podstawie modelu danej sieci i dokumentacji dotyczącej zabezpieczeń identyfikuje potencjalne miejsca wystąpienia zagrożenia. Zadanie wykonuje samodzielnie w zmiennych i nie w pełni przewidywalnych warunkach. Posiada wiedzę na temat skuteczności oraz możliwości wdrożenia różnych, dostępnych na rynku, rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznych. Porównuje dostępne rozwiązania, analizuje możliwość ich wdrożenia i stosowania. Planuje działania mające na celu zapewnienie cyberbezpieczeństwa danej sieci elektroenergetycznej i koryguje je adekwatnie do zmieniających się warunków wynikających m.in. z zagrożeń zewnętrznych, zachowań użytkowników i rozwoju sieci elektroenergetycznej.

Posiadacz kwalifikacji nadzoruje działanie systemów cyberbezpieczeństwa sieci elektroenergetycznej. Diagnozuje i rozwiązuje problemy związane z bezpieczeństwem oprogramowania wykorzystywanego w sieci elektroenergetycznej, urządzeń współpracujących z siecią oraz koniecznością monitorowania punktów dostępowych do sieci.

Posiadacz kwalifikacji identyfikuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej. Dokonuje ich analizy, w tym wskazuje możliwe przyczyny zaistnienia incydentów. Uwzględnia wpływ zaistnienia incydentu na działanie sieci elektroenergetycznej oraz bezpieczeństwo danych związanych z jej funkcjonowaniem. Przygotowuje plan działania, szereguje incydenty według priorytetów obsługi oraz wskazuje incydenty wymagające natychmiastowej reakcji.

Wyodrębnione zestawy efektów uczenia się (nazwa zestawu: 500 znaków)

Wykaz zestawów efektów uczenia się wymaganych dla kwalifikacji, zawierający: numer porządkowy (1, 2, ...), nazwy zestawów, orientacyjne odniesienie każdego zestawu do poziomu PRK oraz orientacyjny nakład pracy potrzebny do osiągnięcia efektów uczenia w każdym zestawie.

Nazwa zestawu powinna:

- *nawiązywać do efektów uczenia się wchodzących w skład danego zestawu lub odpowiadać specyfice wchodzących w jego skład efektów uczenia się,*
- *być możliwie krótka,*
- *nie zawierać skrótów,*

gdy jest to możliwe, być oparta na rzeczowniku odczasownikowym, np. „gromadzenie", „przechowywanie", „szycie".

1. Modelowanie i ocena bezpieczeństwa sieci elektroenergetycznej (5 PRK, 100 godzin)
2. Nadzorowanie działania systemów cyberbezpieczeństwa sieci elektroenergetycznej (5 PRK, 80 godzin)
3. Detekcja i śledzenie incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej (4 PRK, 60 godzin)

Poszczególne efekty uczenia się w zestawach (nazwa efektu uczenia się: 2000 znaków, kryteria weryfikacji (dla jednego efektu): 10000 znaków)

Zestaw efektów uczenia się to wyodrębniona część efektów uczenia się wymaganych dla danej kwalifikacji. Poszczególne efekty uczenia się powinny być wzajemnie ze sobą powiązane, uzupełniające się oraz przedstawione w sposób uporządkowany (np. od prostych do bardziej złożonych).

Poszczególne efekty uczenia się są opisywane za pomocą: umiejętności (tj. zdolności wykonywania zadań i rozwiązywania problemów) oraz kryteriów weryfikacji, które doprecyzowują ich zakres oraz określają niezbędną wiedzę i kompetencje społeczne.

Poszczególne efekty uczenia się powinny być:

- *jednoznaczne – niebudzące wątpliwości, pozwalające na zaplanowanie i przeprowadzenie walidacji, których wyniki będą porównywalne, oraz dające możliwość odniesienia do poziomu PRK,*
- *realne – możliwe do osiągniecia przez osoby, dla których dana kwalifikacja jest przewidziana,*
- *możliwe do zweryfikowania podczas walidacji,*
- *zrozumiałe dla osób potencjalnie zainteresowanych kwalifikacją.*

Podczas opisywania poszczególnych efektów uczenia się korzystne jest stosowanie czasowników operacyjnych (np. „rozróżnia", „uzasadnia", „montuje").

Zestaw efektów uczenia się:	01. Modelowanie i ocena bezpieczeństwa sieci elektroenergetycznej
Umiejętności	**Kryteria weryfikacji**
1. omawia zagadnienia cyberbezpieczeń-stwa sieci elektroener-getycznej	A. wskazuje normy i regulacje prawne mające wpływ na zakres i sposób zapewniania cyberbezpieczeństwa sieci elektroenergetycznych B. omawia, na podstawie aktualnych norm i aktów prawnych, wymagania względem zapewnienia cyberbezpieczeństwa sieci elektroenergetycznych C. opisuje wymagania wobec zapewnienia cyberbezpieczeństwa sieci elektroenergetycznej wynikające z regulacji prawnych dotyczących infrastruktury krytycznej D. opisuje skutki prawne wynikające z naruszenia bezpieczeństwa sieci elektroenergetycznej

2. analizuje system zabezpieczeń sieci elektroenergetycznej pod kątem cyberbezpieczeństwa	A. wskazuje, na podstawie modelu sieci, dokumentacji dotyczącej zabezpieczeń oraz zastosowanych urządzeń i mediów transmisyjnych, potencjalne zagrożenia dla cyberbezpieczeństwa sieci elektroenergetycznej B. wskazuje, na podstawie modelu sieci, dokumentacji dotyczącej zabezpieczeń oraz zastosowanych urządzeń i mediów transmisyjnych, potencjalne zagrożenia dla poufności, integralności i dostępności danych związanych z funkcjonowaniem sieci elektroenergetycznej C. identyfikuje w systemie zabezpieczeń sieci elektroenergetycznej, na podstawie modelu sieci, dokumentacji dotyczącej zabezpieczeń oraz zastosowanych urządzeń i mediów transmisyjnych, potencjalne miejsca wystąpienia zagrożenia dla jej bezpieczeństwa D. opisuje konsekwencje techniczne naruszenia cyberbezpieczeństwa danej sieci elektroenergetycznej
3. przeprowadza testy bezpieczeństwa systemu zabezpieczeń sieci elektroenergetycznej	A. opracowuje założenia do testu bezpieczeństwa systemu zabezpieczeń sieci B. przeprowadza symulowane ataki C. opracowuje wnioski z testu bezpieczeństwa systemu zabezpieczeń sieci
4. analizuje rozwiązania zapewniające cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem	A. omawia typy, wady i zalety rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem B. porównuje skuteczność różnych rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem w zależności od zastosowanych urządzeń i mediów do transmisji danych C. omawia warunki wdrożenia i stosowania rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem w zależności od zastosowanych urządzeń i mediów do transmisji danych D. wskazuje rodzaje zabezpieczeń adekwatne do poszczególnych typów sieci elektroenergetycznych (np. przesyłowych i dystrybucyjnych)
5. rekomenduje podjęcie działań w celu zapewnienia cyberbezpieczeństwa sieci	A. przedstawia propozycje zabezpieczenia dla danego zagrożenia dla cyberbezpieczeństwa danej sieci elektroenergetycznej B. ocenia zasadność wprowadzenia poszczególnych rozwiązań w odniesieniu do danego zagrożenia dla cyberbezpieczeństwa sieci elektroenergetycznej

elektroenergetycznej i danych związanych z jej funkcjonowaniem	C. analizuje możliwość wdrożenia i stosowania rozwiązań w danej sieci elektroenergetycznej
Zestaw efektów uczenia się:	02. Nadzorowanie działania systemów cyberbezpieczeństwa sieci elektroenergetycznej
Umiejętności	**Kryteria weryfikacji**
1. analizuje zabezpieczenia oprogramowania sieci elektroenergetycznej	A. omawia wymogi i zasady aktualizowania oprogramowania wykorzystywanego w sieci elektroenergetycznej B. wskazuje oprogramowanie wymagające aktualizacji C. ocenia kompatybilność oprogramowania ze zidentyfikowanymi podatnościami sieci elektroenergetycznej na atak D. wskazuje rodzaje zabezpieczeń oprogramowania wykorzystywanego w sieci elektroenergetycznej E. omawia parametry bezpieczeństwa oprogramowania wykorzystywanego w sieci elektroenergetycznej
2. analizuje zabezpieczenia urządzeń współpracujących z siecią elektroenergetyczną	A. omawia sposoby zapewniania cyberbezpieczeństwa urządzeń współpracujących z siecią elektroenergetyczną (np. sieci czujnikowych) B. analizuje zagrożenia ze strony urządzeń IoT (Internet of Things, Internet Rzeczy) zainstalowanych w danej sieci elektroenergetycznej
3. monitoruje dostęp do sieci elektroenergetycznej i zarządza nim	A. wskazuje punkty dostępu do danej sieci elektroenergetycznej B. dokonuje wyboru optymalnych metod identyfikowania, uwierzytelniania i autoryzacji wykorzystywanych do zapewniania cyberbezpieczeństwa sieci elektroenergetycznej na podstawie ich wad, zalet oraz skuteczności C. dokonuje wyboru optymalnych metod zabezpieczeń na podstawie ich wad, zalet oraz skuteczności D. omawia zasady nadawania i odbierania uprawnień dostępu do systemów i urządzeń współpracujących z siecią elektroenergetyczną
Zestaw efektów uczenia się:	03. Detekcja i śledzenie incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej
Umiejętności	**Kryteria weryfikacji**
1.identyfikuje incydenty w	A. wyjaśnia pojęcie incydentu w obszarze cyberbezpieczeństwa sieci elektroenergetycznej

obszarze cyberbezpieczeństwa sieci elektroenergetycznej	B. omawia typy incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej C. rozpoznaje zdarzenia będące incydentami w obszarze cyberbezpieczeństwa D. określa typ incydentu według wybranej klasyfikacji spośród powszechnie uznawanych, np. klasyfikacji eCSIRT.net
2. analizuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	A. ustala zadania, procesy, zasoby i osoby, na które wpływa incydent w obszarze cyberbezpieczeństwa B. wskazuje możliwe przyczyny zaistnienia incydentu w obszarze cyberbezpieczeństwa C. identyfikuje-skutki wystąpienia określonego incydentu w obszarze cyberbezpieczeństwa D. szereguje incydenty w obszarze cyberbezpieczeństwa według priorytetów obsługi E. wskazuje incydenty krytyczne w obszarze cyberbezpieczeństwa wymagające natychmiastowej reakcji
3. zgłasza incydent w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	A. wskazuje akty prawne regulujące obowiązki w zakresie zgłaszania i obsługi incydentów w obszarze cyberbezpieczeństwa, w tym dotyczące infrastruktury krytycznej B. opisuje, wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz innych regulacji prawnych, obowiązki i procedury w zakresie zgłaszania i obsługi incydentów w obszarze cyberbezpieczeństwa C. sporządza opis incydentu na potrzeby zgłoszenia do podmiotu Krajowego Systemu Cyberbezpieczeństwa D. opisuje zasady postępowania w przypadku zaistnienia incydentów związanych z naruszeniem ochrony danych osobowych

Wnioskodawca

Pole obowiązkowe (art. 83 ust. 1 pkt 7).Z listy rozwijanej w formularzu w ZRK należy wybrać podmiot wnioskodawcy.

Minister właściwy

Pole obowiązkowe (art. 16 ust. 1). Należy wskazać odpowiedniego ministra, który zdaniem wnioskodawcy jest właściwy do rozpatrzenia wniosku i po włączeniu kwalifikacji do ZSK powinien odpowiadać za kwalifikację.

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności (2000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. b). W przypadku kwalifikacji nadawanej na czas określony wskaż, po jakim czasie konieczne jest odnowienie ważności kwalifikacji oraz określ warunki, jakie muszą być spełnione, aby ważność dokumentu została przedłużona.

5 lat.

Warunkiem przedłużenia ważności certyfikatu jest wykazanie się aktywnością zawodową w obszarze objętym kwalifikacji tj. przedstawienie dokumentów potwierdzających wykonywanie przez okres minimum 2 lat w okresie ważności certyfikatu zadań związanych z zapewnianiem cyberbezpieczeństwa sieci elektroenergetycznych.

Nazwa dokumentu potwierdzającego nadanie kwalifikacji

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. b). Np. dyplom, świadectwo, certyfikat, zaświadczenie.

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji (2500 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. e). Podaj, o jakie uprawnienia może się ubiegać osoba po uzyskaniu kwalifikacji. Jeśli z uzyskaniem kwalifikacji nie wiąże się uzyskanie uprawnień, należy wpisać "Nie dotyczy".

Nie dotyczy

Kod dziedziny kształcenia

Pole obowiązkowe (art. 15 ust. 1 pkt. 7). Kod dziedziny kształcenia, o którym mowa w przepisach wydanych na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2012 r. poz. 591, z późn. zm.).

481 - Informatyka

Kod PKD

Pole obowiązkowe (art. 15 ust. 1 pkt 7). Kod Polskiej Klasyfikacji Działalności (PKD).

62 - Działalność związana z oprogramowaniem i doradztwem w zakresie informatyki oraz działalność powiązana