Miejscowość (forma spotkania), ... r.

Szczegółowe informacje o sposobie zorganizowania i przeprowadzenia walidacji

Nazwa kwalifikacji rynkowej **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.

1. Warunki przystąpienia do walidacji (Art. 15 pkt. 2g)

1.1 Warunki przystąpienia do walidacji i dowody potwierdzające spełnianie warunków

Jakie warunki wynikające z opisu kwalifikacji musi spełniać osoba przystępująca do walidacji w IC?
Jakiego typu dokumenty będą uznawanym, wiarygodnym dowodem na spełnianie tych wymagań?

Brak wymagań

1.2 Dodatkowe wymogi stawiane przez IC

Jakie dodatkowe wymagania musi spełnić osoba przystępująca do walidacji (np. wniesienie opłaty, wypełnienie ankiety osobowej)?

- wypełnienie formularza zgłoszeniowego w formie elektronicznej lub papierowej
- wniesienie opłaty walidacyjnej

2. Opłaty (Art. 15 pkt. 5)

Ile wynosi opłata za udział w walidacji?
Proszę skalkulować koszt walidacji z uwzględnieniem etapów i elementów walidacji, w tym w szczególności np. kosztów: wynagrodzenia kadry uczestniczącej w walidacji, zapewnienia miejsca walidacji i sprzętów/ materiałów, zapewniania obsługi organizacyjnej walidacji i certyfikacji, przygotowania certyfikatu.
Dodatkowe pytania, na które warto odpowiedzieć:

Czy opłata jest pobierana za cały proces w całości, czy np. osobno za walidację, a osobno za wydanie certyfikatu?
Czy kandydat płaci oddzielnie za możliwość przystąpienia do kolejnych części np. części teoretycznej i praktycznej?
Czy IC przewiduje opłaty za dodatkowe usługi poza opłatą za przystąpienie do walidacji i certyfikacji np. płatna usługa doradcy walidacyjnego? Jeśli tak – w jakiej wysokości?
W jakim sposób wnoszona jest opłata i w którym momencie?

Opłata walidacyjna za przeprowadzenie walidacji i wydanie certyfikatu wynosi: 3.000,00 zł (trzy tysiące złotych). Opłata walidacyjna wnoszona jest przelewem na rachunek wskazany przez Instytucję Certyfikującą.

Opłata walidacyjna wnoszona jest jednorazowo, po zakwalifikowaniu Kandydata do walidacji i jest warunkiem przystąpienia do walidacji. Podstawą zakwalifikowania Kandydata do walidacji jest złożenie przez niego kompletnego i poprawnie wypełnionego formularza zgłoszeniowego.

Walidacja – etapy i metody walidacji

3. Identyfikowanie (proces i wykorzystywane metody)

Czy przewidziano wsparcie na etapie identyfikowania? Jeśli nie, proszę przejść do p. 5, a jeśli tak, to:
Jakiego rodzaju wsparcie przewidziano na etapie identyfikowania (np. doradca walidacyjny, zakres zagadnień, test próbny)? Jak ono będzie zorganizowane (on-line, stacjonarnie, telefonicznie)?
Jakie metody będą wykorzystywane na tym etapie?

Instytucja Certyfikująca nie udziela wsparcia Kandydatom na etapie identyfikowania.

4. Dokumentowanie

Etap dokumentowania posiadanych efektów uczenia się nie jest obowiązkowy, występuje wówczas, gdy podmiot planuje zastosować metodę analizy dowodów i deklaracji w weryfikacji efektów uczenia się. Etap dokumentowania polega na gromadzeniu różnych dowodów świadczących o osiągnięciu konkretnych efektów uczenia się określonych w kwalifikacji. Do dokumentacji można włączyć wszystko, co w opinii IC jest dowodem na osiągnięcie wybranych efektów uczenia się, np. certyfikaty, zaświadczenia, próbki pracy, zdjęcia, nagrania wykonanych prac, opis wykonywanej pracy itp. Dokumentowanie może przebiegać przy wsparciu doradcy walidacyjnego lub może być przeprowadzone samodzielnie.

Dla kogo przeznaczony jest etap dokumentowania?
Jakie dowody i deklaracje będą gromadzone na tym etapie? W jakiej formie będą przygotowane (chodzi o konkretny katalog dopuszczalnych dowodów i deklaracji)?
W jaki sposób dowody zostaną przekazane IC?

Instytucja Certyfikująca nie udziela wsparcia Kandydatom na etapie dokumentowania.

5. Weryfikacja efektów uczenia się

5.1. Metody i narzędzia wykorzystywane podczas weryfikacji efektów uczenia się

Jakie metody weryfikacji efektów uczenia się - zgodnie ze wskazanymi w opisie kwalifikacji - będą wykorzystane przez IC?
Jakie narzędzia przewidziano na etapie weryfikacji dla zastosowania poszczególnych metod? np. dla metody test teoretyczny przewidziano: formularz testu, formę ustną czy pisemną/papierową/elektroniczną/, pytania otwarte/zamknięte, jedno czy wielokrotnego wyboru, aplikację webową itd.?
Jakie narzędzia dla asesorów będzie stosowała IC np. scenariusz i arkusz obserwacji symulacji czy scenariusze rozmów i arkusz oceny?
Prosimy o dopasowanie metod i narzędzi do efektów uczenia się i kryteriów ich weryfikacji (patrz Tabela 1).

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

- test teoretyczny (pisemny lub ustny)
  - wykorzystywane narzędzia: formularz testu (zawierający pytania zamknięte i otwarte), klucz odpowiedzi
- obserwacja w warunkach symulowanych
  - wykorzystywane narzędzia: formularz dla Kandydata (zawierający polecenia do wykonania), wytyczne dla asesorów do przeprowadzenia weryfikacji, arkusz oceny dla asesora

5.2. Przebieg weryfikacji efektów uczenia się i sposób jej organizacji

Zapisy muszą być spójne z opisem kwalifikacji, ale już uszczegółowione w stopniu, w jakim planuje to IC.
Jak będzie przebiegał szczegółowo proces weryfikacji efektów uczenia się?
Czy weryfikacja jest podzielona na części?
Jakie metody będą wykorzystywane w poszczególnych częściach?
Czy części te są od siebie zależne (np. pozytywny wynik jednej warunkuje podejście do kolejnej?
Jaki jest czas trwania weryfikacji efektów uczenia się/ poszczególnych części weryfikacji?
W jakim miejscu/ trybie (np. stacjonarnie, online) odbędzie się weryfikacja efektów uczenia się/ poszczególne części weryfikacji?

Weryfikacja efektów uczenia się składa się z dwóch części:

- test teoretyczny (obejmujący pytania testowe i zadania problemowe)
- obserwacja w warunkach symulowanych.

Kandydat przystępuje do poszczególnych części weryfikacji zgodnie z harmonogramem, opracowywanym przez Instytucję Certyfikującą każdorazowo dla danej sesji walidacyjnej. Części weryfikacji są od siebie niezależne, tj. nie jest wymagane uzyskanie pozytywnego wyniku z pierwszej części w celu przystąpienia do drugiej części weryfikacji.

Weryfikacja przeprowadzana jest w formie stacjonarnej, w siedzibie Instytucji Certyfikującej lub w wynajętej na potrzeby danej sesji walidacyjnej sali egzaminacyjnej.

Czas trwania weryfikacji dla kandydata:

- test teoretyczny: 90 minut
- obserwacja w warunkach symulowanych: 120 minut

5.3. Zasoby potrzebne do przeprowadzenia weryfikacji

Jakie są niezbędne zasoby materialne do przeprowadzenia walidacji wynikające z opisu? Tam gdzie to możliwe, proszę doprecyzować, w jaki sposób podmiot zamierza spełnić te wymogi np. konkretny model urządzeń, marki materiałów itp.

Czy będą zapewnione dodatkowe zasoby ponad te określone w opisie kwalifikacji? Jeśli tak- jakie?

Zasoby niezbędne 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

6. Organizacja walidacji w instytucji certyfikującej

Czy IC zamierza samodzielnie przeprowadzać walidację?

Czy IC będzie zlecać przeprowadzenie walidacji swoim oddziałom/ jednostkom wewnętrznym? Czy IC będzie zlecał walidację podmiotowi zewnętrznemu (instytucji walidującej)?

Jeśli tak, to w jaki sposób wpłynie to na organizację walidacji (np. walidacja będzie odbywała się w różnych miastach lub poza siedzibą IC)?

Instytucja Certyfikująca nie zleca walidacji innym podmiotom.

7. Kadry zaangażowane w walidację - zadania i kompetencje

Jakie osoby / zespoły są zaangażowane w walidację?
Jakie są ich zadania?
Jakie są konieczne kompetencje poszczególnych osób zaangażowanych w walidację?
W jaki sposób te kompetencje będą weryfikowane?

Warto tu wskazać wszystkie możliwe osoby, podmioty, role ważne w organizacji i przeprowadzaniu walidacji, uwzględniając te wskazane w opisie kwalifikacji np. komisję walidacyjną, doradcę walidacyjnego. Można też wskazać osoby zajmujące się informowaniem kandydatów, obsługą administracyjną kandydatów, certyfikowaniem, monitorowaniem i ewaluacją oraz obsługą administracyjną, techniczną, księgową, prawną wszystkich tych procesów.
(tabela pomocnicza: Przypisanie odpowiedzialności personelu do etapów walidacji w IC.xcl)

Zasoby kadrowe niezbędne do przeprowadzenia walidacji:

Kierownik Instytucji Certyfikującej - odpowiada za prawidłowy przebieg procesu walidacji w Instytucji Certyfikującej, powołuje komisję walidacyjną i komisję walidacyjną odwoławczą, podejmuje decyzje dotyczące nadania kwalifikacji i wydania certyfikatu, rozpatruje odwołania

Osoba odpowiedzialna za obsługę administracyjną - odpowiada za przyjmowanie i weryfikację formularzy zgłoszeniowych, zapewnienie prawidłowej organizacji weryfikacji efektów uczenia się (ustalenie harmonogramu, weryfikację przygotowania wyposażenia), przekazywanie informacji Kandydatom, osobom zaangażowanym w przebieg walidacji

Osoby przygotowujące narzędzia walidacyjne - odpowiadają za opracowanie narzędzi walidacyjnych

W przygotowanie narzędzi walidacyjnych muszą być zaangażowane co najmniej następujące osoby: ekspert branżowy posiadający minimum 3 lata doświadczenia w wykonywaniu zadań objętych kwalifikacją, weryfikowane na podstawie dokumentów potwierdzających okres i charakter wykonywanych zadań (np. umów o pracę, świadectw pracy, umów cywilno-prawnych) 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 system zewnętrznego zapewnienia jakości (udział w przygotowaniu narzędzi walidacyjnych dla co najmniej 5 procesów weryfikacji).

Komisja walidacyjna - odpowiada za przeprowadzenie i udokumentowanie weryfikacji efektów uczenia się. Spośród członków komisji walidacyjnej powołuje się przewodniczącego komisji walidacyjnej odpowiedzialnego za prawidłowy przebieg pracy komisji walidacyjnej. Decyzje komisji walidacyjnej podejmowane są większością głosów.

Komisja walidacyjna składa się 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, weryfikowane na podstawie dokumentów potwierdzających okres i charakter wykonywanych zadań (np. umów o pracę, świadectw pracy, umów cywilno-prawnych, kontraktów).

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, weryfikowany na podstawie dokumentów takich jak umowy cywilno-prawne, dokumenty potwierdzające powołanie do składu komisji egzaminacyjnych).

Komisja walidacyjna odwoławcza - odpowiada za przeprowadzenie i udokumentowanie weryfikacji efektów uczenia się w toku rozpatrywania odwołania złożonego przez Kandydata. Spośród członków komisji walidacyjnej odwoławczej powołuje się przewodniczącego odpowiedzialnego za prawidłowy przebieg pracy komisji walidacyjnej odwoławczej. Decyzje komisji walidacyjnej odwoławczej podejmowane są większością głosów.

Komisja walidacyjna odwoławcza składa się z 3 osób. Członkowie komisji walidacyjnej odwoławczej muszą spełniać wymagania dla członków komisji walidacyjnej.

8. Dokumenty wykorzystywane w walidacji i certyfikowaniu

Jakie dokumenty są gromadzone w procesie walidacji i certyfikowania?
Proszę wskazać listę wszystkich dokumentów (np. arkusze testów, protokoły, instrukcje, karty ocen, listy obecności, oświadczenia, regulaminy, kwestionariusze osobowe). Przykładowe dokumenty w linku:
https://docs.google.com/spreadsheets/d/1Blmz5cLB5p5ajchppcMfcKStDnafMC6BArjn8qJn0AE/edit#gid=864057461

- regulamin walidacji
- formularz zgłoszeniowy
- wzór oświadczenia Kandydata dotyczącego RODO

- narzędzia walidacyjne opracowane na potrzeby danej sesji walidacyjnej, tj. wskazane w punkcie 5.1 narzędzia do przeprowadzenia testu teoretycznego oraz narzędzia do przeprowadzenia obserwacji w warunkach symulowanych
- deklaracja bezstronności członka komisji walidacyjnej lub komisji walidacyjnej odwoławczej
- wzory oświadczeń członków komisji walidacyjnych dotyczące RODO
- lista obecności Kandydatów przystępujących do testu teoretycznego
- lista obecności Kandydatów przystępujących do obserwacji w warunkach symulowanych
- protokół z przeprowadzenia weryfikacji za pomocą testu teoretycznego
- protokół z przeprowadzenia weryfikacji za pomocą obserwacji w warunkach symulowanych
- formularz odwołania
- wzór certyfikatu

9. Certyfikowanie

Jakie informacje znajdą się na certyfikacie?
W przypadku certyfikatu lub innego dokumentu poświadczającego posiadanie kwalifikacji, proponujemy, aby zawierał on min. następujące elementy:

- *imię i nazwisko uczestnika (dodatkowo można umieścić miejsce i datę urodzenia),*
- *nazwa instytucji certyfikującej,*
- *pełną nazwę kwalifikacji rynkowej widniejącą w obwieszczeniu o włączeniu kwalifikacji do ZSK,*
- *znak PRK,*
- *numer certyfikatu,*
- *datę wystawienia certyfikatu,*
- *data/okres ważności certyfikatu,*
- *podpis osoby reprezentującej IC oraz przewodniczącego komisji walidacyjnej.*

- dane Kandydata: imię i nazwisko, PESEL
- nazwa Instytucji Certyfikującej
- nazwa kwalifikacji rynkowej
- znak graficzny informujący o poziomie PRK
- numer certyfikatu
- datę wystawienia certyfikatu
- okres ważności certyfikatu
- podpis Kierownika Instytucji Certyfikującej
- w załączeniu do certyfikatu: wykaz efektów uczenia się dla kwalifikacji

10. Informowanie o walidacji (Art. 47 ust. 4)

"Instytucja certyfikująca udostępnia na stronie internetowej szczegółowe informacje o sposobie zorganizowania i przeprowadzania walidacji dla danej kwalifikacji rynkowej" (art. 47 ust. 4). *Jakie informacje będą publikowane na stronie internetowej IC?* *Link ze wskazówkami dotyczącymi informowania: https://kwalifikacje.edu.pl/wp-content/uploads/Rekomendacje-IC-INTERNET-popr..pdf* *Rozdział 6 (str. 57)*
Instytucja Certyfikująca zamieszcza na stronie internetowej: ● informacje o kwalifikacji rynkowej wraz z linkiem do Zintegrowanego Rejestru Kwalifikacji ● podstawowe informacje o Zintegrowanym Systemie Kwalifikacji ● informacje o Instytucji Certyfikującej, w tym dotyczące posiadania uprawnień do certyfikowania kwalifikacji rynkowej ● dane kontaktowe do osoby/osób odpowiedzialnych za obsługę Kandydatów ● informacje o sposobie zorganizowania i przebiegu walidacji, opis formalności związanych z przystąpieniem do walidacji, opis procedury odwoławczej ● regulamin walidacji ● informację o dokumencie potwierdzającym uzyskanie kwalifikacji rynkowej i wzór certyfikatu ● formularze dokumentów do pobrania (formularz zgłoszeniowy, formularz odwołania)
Tabela 1 do p. 5.1.: Metody i narzędzia walidacji przypisane do kryteriów weryfikacji uczenia się

Nazwa zestawu efektów efektów uczenia się	**Modelowanie i ocena bezpieczeństwa sieci elektroenergetycznej**	
Nazwa efektu uczenia się	**Kryteria weryfikacji**	**Metoda walidacji**
omawia zagadnienia cyberbezpieczeństwa sieci elektroenergetycznej	wskazuje normy i regulacje prawne mające wpływ na zakres i sposób zapewniania cyberbezpieczeństwa sieci elektroenergetycznych	test teoretyczny
	omawia, na podstawie aktualnych norm i aktów prawnych, wymagania względem	test teoretyczny

	zapewnienia cyberbezpieczeństwa sieci elektroenergetycznych	
	opisuje wymagania wobec zapewnienia cyberbezpieczeństwa sieci elektroenergetycznej wynikające z regulacji prawnych dotyczących infrastruktury krytycznej	test teoretyczny
	opisuje skutki prawne wynikające z naruszenia bezpieczeństwa sieci elektroenergetycznej	test teoretyczny
analizuje system zabezpieczeń sieci elektroenergetycznej pod kątem cyberbezpieczeństwa	wskazuje, na podstawie modelu sieci, dokumentacji dotyczącej zabezpieczeń oraz zastosowanych urządzeń i mediów transmisyjnych, potencjalne zagrożenia dla cyberbezpieczeństwa sieci elektroenergetycznej	obserwacja w warunkach symulowanych
	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	obserwacja w warunkach symulowanych
	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	obserwacja w warunkach symulowanych

	opisuje konsekwencje techniczne naruszenia cyberbezpieczeństwa danej sieci elektroenergetycznej	obserwacja w warunkach symulowanych
przeprowadza testy bezpieczeństwa systemu zabezpieczeń sieci elektroenergetycznej	opracowuje założenia do testu bezpieczeństwa systemu zabezpieczeń sieci	obserwacja w warunkach symulowanych
	przeprowadza symulowane ataki	obserwacja w warunkach symulowanych
	opracowuje wnioski z testu bezpieczeństwa systemu zabezpieczeń sieci	obserwacja w warunkach symulowanych
analizuje rozwiązania zapewniające cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem	omawia typy, wady i zalety rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem	test teoretyczny
	porównuje skuteczność różnych rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem w zależności od zastosowanych urządzeń i mediów do transmisji danych	test teoretyczny
	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	test teoretyczny
	wskazuje rodzaje zabezpieczeń adekwatne do poszczególnych typów sieci	test teoretyczny

	elektroenergetycznych (np. przesyłowych i dystrybucyjnych)	
rekomenduje podjęcie działań w celu zapewnienia cyberbezpieczeństwa sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem	przedstawia propozycje zabezpieczenia dla danego zagrożenia dla cyberbezpieczeństwa danej sieci elektroenergetycznej	obserwacja w warunkach symulowanych
	ocenia zasadność wprowadzenia poszczególnych rozwiązań w odniesieniu do danego zagrożenia dla cyberbezpieczeństwa sieci elektroenergetycznej	obserwacja w warunkach symulowanych
	analizuje możliwość wdrożenia i stosowania rozwiązań w danej sieci elektroenergetycznej	obserwacja w warunkach symulowanych
Nazwa zestawu efektów efektów uczenia się	**Nadzorowanie działania systemów cyberbezpieczeństwa sieci elektroenergetycznej**	
Nazwa efektu uczenia się	**Kryteria weryfikacji**	**Metoda walidacji**
analizuje zabezpieczenia oprogramowania sieci elektroenergetycznej	omawia wymogi i zasady aktualizowania oprogramowania wykorzystywanego w sieci elektroenergetycznej	test teoretyczny
	wskazuje oprogramowanie wymagające aktualizacji	obserwacja w warunkach symulowanych
	ocenia kompatybilność oprogramowania ze zidentyfikowanymi podatnościami sieci elektroenergetycznej na atak	obserwacja w warunkach symulowanych
	wskazuje rodzaje zabezpieczeń oprogramowania wykorzystywanego w sieci elektroenergetycznej	test teoretyczny

	omawia parametry bezpieczeństwa oprogramowania wykorzystywanego w sieci elektroenergetycznej	test teoretyczny
analizuje zabezpieczenia urządzeń współpracujących z siecią elektroenergetyczną	omawia sposoby zapewniania cyberbezpieczeństwa urządzeń współpracujących z siecią elektroenergetyczną (np. sieci czujnikowych)	test teoretyczny
	analizuje zagrożenia ze strony urządzeń IoT (Internet of Things, Internet Rzeczy) zainstalowanych w danej sieci elektroenergetycznej	obserwacja w warunkach symulowanych
monitoruje dostęp do sieci elektroenergetycznej i zarządza nim	wskazuje punkty dostępu do danej sieci elektroenergetycznej	obserwacja w warunkach symulowanych
	dokonuje wyboru optymalnych metod identyfikowania, uwierzytelniania i autoryzacji wykorzystywanych do zapewniania cyberbezpieczeństwa sieci elektroenergetycznej na podstawie ich wad, zalet oraz skuteczności	obserwacja w warunkach symulowanych
	dokonuje wyboru optymalnych metod zabezpieczeń na podstawie ich wad, zalet oraz skuteczności	obserwacja w warunkach symulowanych
	omawia zasady nadawania i odbierania uprawnień dostępu do systemów i urządzeń współpracujących z siecią elektroenergetyczną	test teoretyczny
Nazwa zestawu efektów efektów uczenia się	**Detekcja i śledzenie incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej**	

Nazwa efektu uczenia się	Kryteria weryfikacji	Metoda walidacji
identyfikuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	wyjaśnia pojęcie incydentu w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	test teoretyczny
	omawia typy incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	test teoretyczny
	rozpoznaje zdarzenia będące incydentami w obszarze cyberbezpieczeństwa	obserwacja w warunkach symulowanych
	określa typ incydentu według wybranej klasyfikacji spośród powszechnie uznawanych, np. klasyfikacji eCSIRT.net	obserwacja w warunkach symulowanych
analizuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	ustala zadania, procesy, zasoby i osoby, na które wpływa incydent w obszarze cyberbezpieczeństwa	obserwacja w warunkach symulowanych
	wskazuje możliwe przyczyny zaistnienia incydentu w obszarze cyberbezpieczeństwa	obserwacja w warunkach symulowanych
	identyfikuje, na podstawie opisu sytuacji, skutki wystąpienia określonego incydentu w obszarze cyberbezpieczeństwa	obserwacja w warunkach symulowanych
	szereguje incydenty w obszarze cyberbezpieczeństwa według priorytetów obsługi	obserwacja w warunkach symulowanych
	wskazuje incydenty krytyczne w obszarze cyberbezpieczeństwa wymagające natychmiastowej reakcji	obserwacja w warunkach symulowanych

zgłasza incydent w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	wskazuje akty prawne regulujące obowiązki w zakresie zgłaszania i obsługi incydentów w obszarze cyberbezpieczeństwa, w tym dotyczące infrastruktury krytycznej	test teoretyczny
	opisuje, wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz innych regulacji prawnych, obowiązki i procedury w zakresie zgłaszania i obsługi incydentów w obszarze cyberbezpieczeństwa	test teoretyczny
	sporządza opis incydentu na potrzeby zgłoszenia do podmiotu Krajowego Systemu Cyberbezpieczeństwa	obserwacja w warunkach symulowanych
	opisuje zasady postępowania w przypadku zaistnienia incydentów związanych z naruszeniem ochrony danych osobowych	test teoretyczny