Tabela zgodności

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.

Nazwa kwalifikacji	Zapewnianie cyberbezpieczeństwa sieci elektroenergetycznej
Rekomendowany poziom PRK dla kwalifikacji	5 PRK
Poziom PRK najlepiej odpowiadający zestawom efektów uczenia się*	Zestaw 1. Modelowanie i ocena bezpieczeństwa sieci elektroenergetycznej (5 PRK) Zestaw 2. Nadzorowanie działania systemów cyberbezpieczeństwa sieci elektroenergetycznej (5 PRK) Zestaw 3. Detekcja i śledzenie incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej (4 PRK)

Zestaw 1		
Modelowanie i ocena bezpieczeństwa sieci elektroenergetycznej		
L.p.	**Poszczególne efekty uczenia się w zestawach***	**Kryteria weryfikacji**
1.	omawia zagadnienia cyberbezpieczeństwa sieci elektroenergetycznej	wskazuje normy i regulacje prawne mające wpływ na zakres i sposób zapewniania cyberbezpieczeństwa sieci elektroenergetycznych
		omawia, na podstawie aktualnych norm i aktów prawnych, wymagania względem zapewnienia cyberbezpieczeństwa sieci elektroenergetycznych
		opisuje wymagania wobec zapewnienia cyberbezpieczeństwa sieci elektroenergetycznej wynikające z regulacji prawnych dotyczących infrastruktury krytycznej
		opisuje skutki prawne wynikające z naruszenia bezpieczeństwa sieci elektroenergetycznej
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P4Z_WO (1, 2), P3Z_KP (1)	

2.	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**
		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
		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
		opisuje konsekwencje techniczne naruszenia cyberbezpieczeństwa danej sieci elektroenergetycznej
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P3Z_UI (1, 2), P4Z_UO (4), P5Z WN, P5Z_UO (2)	
3.	przeprowadza testy bezpieczeństwa systemu zabezpieczeń sieci elektroenergetycznej	**opracowuje założenia do testu bezpieczeństwa systemu zabezpieczeń sieci**
		przeprowadza symulowane ataki
		opracowuje wnioski z testu bezpieczeństwa systemu zabezpieczeń sieci
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P5Z_UO (1, 2)	
4.	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**
		porównuje skuteczność różnych rozwiązań zapewniających cyberbezpieczeństwo sieci elektroenergetycznej i danych związanych z jej funkcjonowaniem w zależności od zastosowanych urządzeń i mediów do transmisji danych
		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
		wskazuje rodzaje zabezpieczeń adekwatne do poszczególnych typów sieci elektroenergetycznych (np. przesyłowych i dystrybucyjnych)
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	

	P5Z_WO (1, 2), P5Z_WN	
5.	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**
		ocenia zasadność wprowadzenia poszczególnych rozwiązań w odniesieniu do danego zagrożenia dla cyberbezpieczeństwa sieci elektroenergetycznej
		analizuje możliwość wdrożenia i stosowania rozwiązań w danej sieci elektroenergetycznej
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P5Z_UN, P5Z_UO (2, 4)	

Zestaw 2.		
Nadzorowanie działania systemów cyberbezpieczeństwa sieci elektroenergetycznej		
L.p.	**Poszczególne efekty uczenia się w zestawach***	**Kryteria weryfikacji**
1.	analizuje zabezpieczenia oprogramowania sieci elektroenergetycznej	omawia wymogi i zasady aktualizowania oprogramowania wykorzystywanego w sieci elektroenergetycznej
		wskazuje oprogramowanie wymagające aktualizacji
		ocenia kompatybilność oprogramowania ze zidentyfikowanymi podatnościami sieci elektroenergetycznej na atak
		wskazuje rodzaje zabezpieczeń oprogramowania wykorzystywanego w sieci elektroenergetycznej
		omawia parametry bezpieczeństwa oprogramowania wykorzystywanego w sieci elektroenergetycznej
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P4Z_WO (1, 2), P5Z_WN, P5Z_UN, P5Z_UO (2, 4)	
2.	analizuje zabezpieczenia urządzeń współpracujących z siecią elektroenergetyczną	**omawia sposoby zapewniania cyberbezpieczeństwa urządzeń współpracujących z siecią elektroenergetyczną (np. sieci czujnikowych)**
		analizuje zagrożenia ze strony urządzeń IoT (Internet of Things, Internet Rzeczy) zainstalowanych w danej sieci elektroenergetycznej
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P5Z_WO (1, 2), P5Z_UO (2, 4)	

3.	monitoruje dostęp do sieci elektroenergetycznej i zarządza nim	wskazuje punkty dostępu do danej sieci elektroenergetycznej
		dokonuje wyboru optymalnych metod identyfikowania, uwierzytelniania i autoryzacji wykorzystywanych do zapewniania cyberbezpieczeństwa sieci elektroenergetycznej na podstawie ich wad, zalet oraz skuteczności
		dokonuje wyboru optymalnych metod zabezpieczeń na podstawie ich wad, zalet oraz skuteczności
		omawia zasady nadawania i odbierania uprawnień dostępu do systemów i urządzeń współpracujących z siecią elektroenergetyczną
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P4Z_WO (1, 2), P4Z_UO (2)	

Zestaw 3.		
Detekcja i śledzenie incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej		
L.p.	**Poszczególne efekty uczenia się w zestawach***	**Kryteria weryfikacji**
1.	identyfikuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	wyjaśnia pojęcie incydentu w obszarze cyberbezpieczeństwa sieci elektroenergetycznej
		omawia typy incydentów w obszarze cyberbezpieczeństwa sieci elektroenergetycznej
		rozpoznaje zdarzenia będące incydentami w obszarze cyberbezpieczeństwa
		określa typ incydentu według wybranej klasyfikacji spośród powszechnie uznawanych, np. klasyfikacji eCSIRT.net
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P3Z_WT (1), P4Z_WO (2), P4Z_UO (2)	
2.	analizuje incydenty w obszarze cyberbezpieczeństwa sieci elektroenergetycznej	ustala zadania, procesy, zasoby i osoby, na które wpływa incydent w obszarze cyberbezpieczeństwa
		wskazuje możliwe przyczyny zaistnienia incydentu w obszarze cyberbezpieczeństwa
		identyfikuje skutki wystąpienia określonego incydentu w obszarze cyberbezpieczeństwa

		szereguje incydenty w obszarze cyberbezpieczeństwa według priorytetów obsługi
		wskazuje incydenty krytyczne w obszarze cyberbezpieczeństwa wymagające natychmiastowej reakcji
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P5Z_UO (2, 4)	
3.	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
		opisuje, wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz innych regulacji prawnych, obowiązki i procedury w zakresie zgłaszania i obsługi incydentów w obszarze cyberbezpieczeństwa
		sporządza opis incydentu na potrzeby zgłoszenia do podmiotu Krajowego Systemu Cyberbezpieczeństwa
		opisuje zasady postępowania w przypadku zaistnienia incydentów związanych z naruszeniem ochrony danych osobowych
	Najlepiej dopasowany(e) składnik(i) opisu poziomów PRK:	
	P3Z_WO (2), P3Z_KP (1), P4Z_UI (4)	

*W tabeli zgodności należy zaznaczyć zestaw/y efektów uczenia się / efekty uczenia się o kluczowym znaczeniu dla kwalifikacji.