Zintegrowany Rejestr Kwalifikacji

Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji*

Obsługa incydentów w obszarze cyberbezpieczeństwa

Skrót nazwy

Rodzaj kwalifikacji*

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji*

4

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 „Obsługa incydentów w obszarze cyberbezpieczeństwa” jest przygotowana do wykonywania zadań związanych z obsługą zdarzeń będących incydentami naruszającymi cyberbezpieczeństwo. Osoba posiadająca kwalifikacje rozpoznaje zdarzenia, które są incydentami naruszającymi cyberbezpieczeństwo oraz gromadzi dane dotyczące incydentów, niezbędne do dokonania zgłoszenia do właściwego podmiotu Krajowego Systemu Cyberbezpieczeństwa. W szczególności ustala, na podstawie właściwej dokumentacji, moment wystąpienia incydentu, czas jego trwania, przebieg oraz ustala zadania, procesy, zasoby i osoby, na które ma wpływ zaistniałe naruszenie. Identyfikuje skutki wystąpienia określonego incydentu w obszarze cyberbezpieczeństwa oraz rozpoznaje incydenty krytyczne wymagające natychmiastowej reakcji. Przygotowuje i wysyła zgłoszenie o zaistniałym incydencie w obszarze cyberbezpieczeństwa do właściwego podmiotu. Koordynuje działania związane z obsługą incydentu, w szczególności ustala niezbędne działania oraz zasoby wymagane do ich zrealizowania. Monitoruje stopień realizacji działań związanych z obsługą incydentu przez inne osoby i podmioty, w szczególności ocenia ich skuteczność oraz wskazuje kryteria zakończenia obsługi incydentu. Osoba posiadająca kwalifikację przygotowana jest również do wykonywania zadań związanych z poinformowaniem osób i podmiotów, których dotyczy naruszenie bezpieczeństwa. Orientacyjna wysokość opłaty za przeprowadzenie walidacji i wystawienie dokumentu potwierdzającego otrzymanie danej kwalifikacji: 3.000,00 zł (trzy tysiące złotych).

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

80

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Kwalifikacja kierowana jest do osób odpowiedzialnych za funkcjonowanie systemów informatycznych w organizacjach mających obowiązek zgłaszania, do odpowiedniego podmiotu Krajowego Systemu Cyberbezpieczeństwa, incydentów w obszarze cyberbezpieczeństwa, administratorów sieci i systemów informatycznych oraz osób odpowiedzialnych za komunikowanie się z podmiotami Krajowego Systemu Cyberbezpieczeństwa.

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

☐ Możliwe jest przygotowanie do uzyskania kwalifikacji w ramach obowiązkowych zajęć edukacyjnych z zakresu kształcenia zawodowego (branżowa szkoła I stopnia, technikum, szkoła policealna) Rozporządzenie MEN z dnia 16 maja 2019 r.

Wymagane kwalifikacje poprzedzające

Opis

Nie dotyczy

Lista

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

Nie dotyczy

Zapotrzebowanie na kwalifikację*

„Obsługa incydentów w obszarze cyberbezpieczeństwa” to kwalifikacja, na którą zapotrzebowanie występuje nie tylko w sektorze IT, ale też, z uwagi na powszechność rozwiązań cyfrowych, wśród przedsiębiorstw większości działów gospodarki narodowej. Digitalizacja jest uznawana za jedną z fundamentalnych i najdynamiczniej zachodzących zmian społecznych i ekonomicznych w XXI wieku. Powszechnie rozumiany jest również istotny wpływ digitalizacji na możliwości rozwojowe gospodarki narodowej jako części globalnego obiegu ekonomicznego. Mimo świadomości tego faktu i ciągłego rozwoju potencjału cyfrowego gospodarki, w Polsce od lat utrzymuje się dość duża luka technologiczna. Według opublikowanego w roku 2016 raportu „Cyfrowa Polska”, wiele sektorów gospodarki (m.in. produkcja przemysłowa, transport i logistyka, energetyka oraz usługi komunalne) z powodu niskiego poziomu nasycenia technologiami cyfrowymi nie osiągały swojego całkowitego potencjału, zaś najsilniej scyfryzowany wówczas sektor finansowy odnotowywał aż 13 procentową lukę technologiczną w porównaniu do państw Europy Zachodniej [1]. Obecnie, według raportu „DIGI INDEX 2022 Poziom digitalizacji produkcji w Polsce”, prezentującego wyniki badania wykonanego w okresie pandemii COVID-19, nadal tylko 0,7% firm deklaruje poziom cyfryzacji produkcji przekraczający 81% [2]. Wynik ten jest oparty na uśrednionych wartościach poziomu cyfryzacji dla 4 głównych branż gospodarki (Machinery, Automotive, Chemistry&Pharmacy, Food&Beverages). Największa grupa 28% badanych przedsiębiorstw plasuje się na poziomie 21-40%, zaś najwyższy stopień digitalizacji produkcji wykazują reprezentanci sektora Automotive, gdzie dla 20% badanych firm wynosi on 60-79%. DIGI INDEX podaje wskaźnik podejścia do digitalizacji gospodarki w 4-punktowej skali, przy czym wynik poniżej 2 punktów jest równoznaczny z powiększającą się luką technologiczną. Według autorów raportu, w 2022 roku właściwy dla Polski wskaźnik DIGI INDEX wzrósł z 1,8 w latach ubiegłych do 2,4 punktu. Interpretując ten wynik można uważać go za pozytywny sygnał, świadczący o tym, że większość badanych firm przeszła już przez etap przygotowań do aktywnej

implementacji rozwiązań cyfrowych, głównie w zakresie procesów zarządczych i produkcyjnych. Firmy zwiększają budżety na cyfryzację, gdyż w coraz większym stopniu są przekonane o jej korzyściach. Najczęściej wskazywane są oszczędność kosztów (38,7%), wyższa wydajność (38,0%) oraz większe bezpieczeństwo produkcji i danych (27,3%). Od jakości i szybkości transformacji cyfrowej, czyli inaczej cyfryzacji, zależą możliwości rozwojowe polskich przedsiębiorstw. Dotychczas, pomimo funkcjonowania w warunkach globalnej ekonomii rynkowej, procesy cyfryzacji zachodziły w Polsce dużo wolniej niż w innych krajach. Dotyczyły one przy tym głównie lokalnych oddziałów międzynarodowych korporacji, przedsiębiorstw wytwarzających oprogramowanie i oferujących usługi IT oraz wciąż stosunkowo nielicznych firm przemysłu 4.0 oraz startupów. Pozytywną stroną tej sytuacji jest fakt, że względne opóźnienie procesów cyfryzacji polskiej gospodarki powodowało, że wprowadzane rozwiązania były z reguły najbardziej nowoczesne, przez co analitycy postrzegali Polskę jako potencjalnego cyfrowego rywala zachodnich gospodarek, posiadającego poważny potencjał wzrostu ilościowego procesów transformacji cyfrowej, przy jednoczesnej innowacyjności stosowanych rozwiązań i wysokiej wydajności rezultatów [3]. Wspomniany wyraźny wzrost wskaźnika DIGI INDEX oraz podniesienie przez przedsiębiorstwa nakładów na cyfryzację wynika z wpływu pandemii COVID-19, której przebieg skłonił wiele firm do rozpoczęcia planowania lub realizacji procesów cyfryzacji. Pomimo pozytywnego trendu rozwojowego, wskazane opóźnienia w stosunku do państw Europy Zachodniej powodują, że Polska wciąż zajmuje w zestawieniach jedno z ostatnich miejsc, zarówno w pod względem stopnia cyfryzacji gospodarki, jak też kompetencji cyfrowych pracowników. Poziom cyfryzacji Polski odbiega zarówno od lidera na tym polu, czyli Stanów Zjednoczonych, jak też państw Europy Zachodniej. W Stanach Zjednoczonych procesami transformacji cyfrowej objęte jest ogółem 18% gospodarki, zaś w Europy Zachodniej średnio 12%. Tymczasem w Polsce gospodarka jest scyfryzowana tylko w 8%. Stopień cyfryzacji polskich przedsiębiorstw jest wciąż średnio o około 34% niższy niż w takich państwach jak Francja, Holandia, Niemcy, Szwecja, Wielka Brytania czy Włochy [4]. Według danych Komisji Europejskiej, w 2021 roku, podobnie jak w roku 2020, w zakresie cyfryzacji gospodarki Polska uplasowała się na, 24 miejscu wśród 27 państw członkowskich Unii Europejskiej [4]. Analizy te opierają się na wskaźniku Digital Economy and Society Index (dalej: DESI), stworzonym w celu oceny poziomu ucyfrowienia gospodarek i społeczeństw państw UE. DESI za najbardziej „cyfrowe" państwa europejskie uznaje Finlandię, Szwecję, Holandię i Danię, dla których współczynnik wynosi blisko 70 na 80 możliwych do uzyskania punktów. Państwa te od lat są liderami rankingu europejskiego i jednocześnie znajdują się także w czołówce światowej, tuż za Koreą Południową, Japonią i Stanami Zjednoczonymi. W roku 2021 europejska średnia DESI wynosiła 50,7 pkt, zaś wynik Polski osiągnął 41 punktów i wyprzedzała ona takie kraje jak Grecja, Bułgaria i Rumunia, których DESI plasowały się poniżej 40 punktów. Statystyki wskazują, że mimo ogólnego odbiegania Polski od średniej UE w zakresie cyfryzacji, obecnie dwa kluczowe elementy wskaźnika DESI, łączność i cyfrowe usługi publiczne, osiągnęły już w Polsce poziom średniej. Sytuacja taka rokuje pozytywnie, gdyż wysoka dostępność cyfrowych technologii łączności i wysoki poziom cyfryzacji sektora publicznego są przykładem i motorem dla reszty gospodarki w zakresie cyfryzacji. Polski rząd od roku 2013 dąży do stworzenia spójnego systemu rozwiązań prawno-instytucjonalnych oraz upowszechniania dobrych praktyk wspierających bezpieczeństwo cyfrowej gospodarki. Wtedy to przyjęto strategię Polityki Ochrony Cyberprzestrzeni RP, której celem strategicznym było osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa [5]. W 2017 r. strategia ta została zastąpiona przez Krajowe Ramy Polityki Cyberbezpieczeństwa RP. Z kolei od 2019 r. obowiązującym dokumentem jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 [6]. Jako główny cel Strategii wskazano podniesienie poziomu odporności kraju na cyberzagrożenia, w tym zwłaszcza ochrony w sektorach: publicznym, militarnym i prywatnym oraz promowanie wiedzy i dobrych praktyk wśród obywateli. Najistotniejszym 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). Ustawa ta stworzyła w Polsce system cechujący się jasnym przydziałem zadań i odpowiedzialności, umożliwiający sprawne działania w zakresie wykrywania, zapobiegania i minimalizowania skutków ataków naruszających cyberbezpieczeństwo RP. 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). Zespoły te, to współpracujące ze sobą oraz z organami właściwymi do spraw cyberbezpieczeństwa: CSIRT NASK (Naukowej i Akademickiej Sieci Komputerowej), CSIRT GOV (Agencji Bezpieczeństwa Wewnętrznego) oraz CSIRT MON resortu obrony narodowej. Razem tworzą krajowy system zarządzania ryzykiem w obszarze cyberbezpieczeństwa, który przeciwdziała zagrożeniom o charakterze ponadsektorowym i transgranicznym oraz zapewniają koordynację obsługi zgłoszonych incydentów. Kluczowym i jednocześnie najsłabszym elementem systemu są pracownicy wykazanych w ustawie podmiotów objętych nadzorem Krajowego Systemu Cyberbezpieczeństwa, czyli samorządów, dostawców usług cyfrowych i operatorów usług kluczowych. Ich zadaniem jest obsługa incydentów naruszenia cyberbezpieczeństwa w lokalnych sieciach i systemach informatycznych. Braki kadrowe na rynku pracy IT powodują, że w wymienionych podmiotach, w tym zwłaszcza w mniejszych przedsiębiorstwach i samorządach lokalnych, często pracują osoby nie posiadające odpowiednich kompetencji pozwalających na właściwe identyfikowanie i klasyfikowanie incydentów w obszarze cyberbezpieczeństwa, ocenę ich skali i możliwych skutków, nadawanie priorytetów, koordynowanie obsługi incydentów oraz komunikację z podmiotami Krajowego Systemu Cyberbezpieczeństwa, w tym zgłaszanie incydentów, i z podmiotami zewnętrznymi (np. klientami, dostawcami, regulatorami). Z uwagi na obecne w ostatnich latach napięcia międzynarodowe i związane z nimi wzmożone występowanie możliwości ataków cybernetycznych na krajową infrastrukturę i urzędy, jakość wskazanych kompetencji nabiera niezwykłej istotności dla funkcjonowania społeczeństwa i bezpieczeństwa państwa. Mimo rosnącego zapotrzebowania, wskazane wyżej kompetencje nie są obecne w zakresie szkolnictwa branżowego, kształcącego w zawodach Technik Informatyk i Technik Programista. Efekty kształcenia w tych zawodach zawierają jedynie ogólny zapis „stosuje zasady cyberbezpieczeństwa”, który nie odnosi się do zadań pracowniczych związanych z obsługą incydentów cyberbezpieczeństwa, a jedynie do kwestii prewencji. Zagadnienia te dopiero zaczynają być widoczne w efektach uczenia się studiów kierunków informatycznych jak również dedykowanych studiów podyplomowych. Z kolei w obszarze edukacji pozaformalnej można zaobserwować dużo więcej ofert szkoleń pozwalających na rozwój kompetencji związanych z obsługą incydentów cyberbezpieczeństwa. Rozwój tej formy kształcenia wynika z rosnącego zainteresowania ze strony potencjalnych pracowników i pracodawców chcących pozyskać osoby o właściwych kompetencjach. Realizowane kursy i szkolenia nie zawsze jednak pozwalają na ich rzetelną walidację, zaś ich programy i zakładane efekty uczenia się mogą się bardzo różnić. Powoduje to sytuację, w której uzyskiwane zaświadczenia i certyfikaty w rzeczywistości nie zawsze oddają realny poziom umiejętności, co w negatywny sposób odbija się na jakości pracy przeszkolonych osób i może bezpośrednio wpłynąć na przebieg potencjalnych kryzysów związanych z cyberzagrożeniami. Reasumując można stwierdzić, że braki specjalistów od obsługi incydentów cyberbezpieczeństwa wpływają na bezpieczeństwo kraju, instytucji i społeczeństwa polskiego. Rozwój form szkoleniowych w tym zakresie powinien wiązać się z odpowiednimi procedurami walidacyjnymi, które zapewni kwalifikacja „Obsługa incydentów w obszarze cyberbezpieczeństwa”. Warte podkreślenia jest, że stworzy ona możliwość potwierdzenia posiadanych umiejętności i

kompetencji nie tylko dla osób związanych z IT. Umożliwi ona potwierdzanie kompetencji nabywanych zarówno w drodze edukacji, samokształcenia czy praktyki zawodowej. Uzyskiwany certyfikat będzie atrakcyjny zarówno dla jego posiadaczy jak i dla zatrudniających ich jednostek samorządu, instytucji i podmiotów gospodarczych, gdyż będzie w sposób obiektywny gwarantował wysoki poziom kompetencji. Przypisy: 1. Cyfrowa Polska. Szansa na technologiczny skok do globalnej pierwszej ligi gospodarczej, McKinsey &Company 2016, https://www.mckinsey.com/pl/~/media/mckinsey/locations/europe%20and%20middle%20east/polska/raporty/cyfrowa%20polska/cyfrowa-polska.ashx [dostęp: 24.07.2022]. 2. Digi Index 2022. Poziom digitalizacji produkcji w Polsce, Siemens 2022, https://new.siemens.com/pl/pl/o-firmie/raporty-siemens/digi-index-2022.html#Pobierz [dostęp: 24.07.2022]. 3. J. Novak, M. Purta, T. Marciniak, K. Ignatowicz, K. Rozenbaum, K. Yearwood, The rise of Digital Challengers. How digitization can become the next growth engine for Central and Eastern Europe, raport opracowany przez McKinsey Company, 2018, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Europe/Central%20and%20Eastern%20Europe%20needs%20a%20new%20engine%20for%20growth/The-rise-of-Digital-Challengers.ash [dostęp: 20.07.2022]. 4. Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) na 2021 r. Polska, 2022, https://ec.europa.eu/newsroom/dae/redirection/document/80596 [dostęp: 20.07.2022]. 5. Cyber Policy, NASK, https://cyberpolicy.nask.pl/category/strategia-cyberbezpieczenstwa-rp/ [dostęp: 24.07.2022]. 6. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 24.07.2022].

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się*

Kwalifikacje o zbliżonym charakterze ujęte w ZRK: ● 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. Kwalifikacja “Obsługa incydentów w obszarze cyberbezpieczeństwa” koncentruje się natomiast na wiedzy i umiejętnościach związanych z formalną obsługą incydentu w obszarze cyberbezpieczeństwa. W szczególności kwalifikacja obejmuje efekty uczenia się niezbędne do zidentyfikowania incydentu w obszarze cyberbezpieczeństwa, opisania go zgodnie z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz zgłoszenia do właściwego podmiotu. Kwalifikacja ta jest przeznaczona przede wszystkim dla osób administrujących systemami informatycznymi lub odpowiedzialnych za ich funkcjonowanie w organizacjach, które mają obowiązek zgłaszania naruszeń bezpieczeństwa do podmiotów KSC lub osób, które w tych organizacjach odpowiedzialne są za współpracę z podmiotami Krajowego Systemu Cyberbezpieczeństwa. Kwalifikacja nie posiada wspólnych zestawów efektów uczenia się z wymienionymi powyżej kwalifikacjami o zbliżonym charakterze. 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. W wymienionych kwalifikacjach nie zidentyfikowano zestawów uczenia się wspólnych dla kwalifikacji “Obsługa incydentów w obszarze cyberbezpieczeństwa”.

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

Typowe możliwości wykorzystania kwalifikacji*

Osoba posiadająca kwalifikację może podjąć zatrudnienie w organizacjach posiadających obowiązek zgłaszania incydentów w obszarze cyberbezpieczeństwa do podmiotów Krajowego Systemu Cyberbezpieczeństwa. Może również podjąć zatrudnienie w podmiotach prowadzących zespoły reagowania na incydenty/monitorowania cyberbezpieczeństwa na stanowiskach wymagających kontaktu z podmiotami Krajowego Systemu Cyberbezpieczeństwa oraz w podmiotach Krajowego Systemu Cyberbezpieczeństwa.

Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację*

1. Etap weryfikacji 1.1. Metody Weryfikacja dla każdego zestawu efektów uczenia się musi być przeprowadzona: metodą obserwacji w warunkach symulowanych oraz testem teoretycznym (w formie tradycyjnej lub elektronicznej) albo metodą analizy dowodów i deklaracji opcjonalnie uzupełnioną testem teoretycznym (w formie tradycyjnej lub elektronicznej) lub wywiadem swobodnym. Walidacja musi być przeprowadzana w oparciu o wystandaryzowane narzędzia walidacji. Walidacja metodą obserwacji w warunkach symulowanych może być przeprowadzona przy zastosowaniu techniki zadania praktycznego lub studium przypadku (case study). Weryfikacja tą metodą musi być przeprowadzona w oparciu o przygotowany wcześniej opis przypadku lub scenariusz zadania praktycznego. W przypadku metody analizy dowodów i deklaracji instytucja certyfikująca powinna opracować i udostępnić wykaz dowodów uznawanych za wiarygodne oraz określić warunki, jakie muszą spełniać te dowody (np. okres ważności). Za wiarygodne uznane mogą zostać: ● dokumenty potwierdzające wykonywanie przez kandydata zadań związanych z obsługą incydentów w zakresie cyberbezpieczeństwa (np. referencje, zaświadczenia), ● dokumenty świadczące o potwierdzeniu, w wyniku wiarygodnej weryfikacji, określonych dla kwalifikacji efektów uczenia się. 1.2. Zasoby kadrowe Osoby przygotowujące narzędzia walidacji W procesie przygotowania narzędzi walidacji muszą uczestniczyć co najmniej: • osoba posiadająca aktualne (aktualnie wykonująca lub nadzorująca wykonywanie zadań związanych z kwalifikacją) doświadczenie praktyczne z zakresu objętego kwalifikacją, • osoba posiadająca doświadczenie w przygotowywaniu narzędzi walidacji. Komisja walidacyjna. Komisja walidacyjna musi składać się z co najmniej dwóch członków, w tym przewodniczącego. Przewodniczący komisji musi spełniać następujące warunki: • posiada kwalifikację pełną z 7 poziomem PRK (dyplom ukończenia studiów II stopnia); • legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze cyberbezpieczeństwa osiągniętym w okresie ostatnich 6 lat. Drugi członek komisji walidacyjnej musi spełniać następujące warunki: • posiada kwalifikację pełną z 6 PRK (dyplom ukończenia studiów I stopnia); • legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze cyberbezpieczeństwa osiągniętym w okresie ostatnich 3 lat. Ponadto, co najmniej jeden z

członków komisji musi posiadać udokumentowane minimum 5-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa. 1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne Obserwacja w warunkach symulowanych oraz rozmowa z komisją walidacyjną przeprowadzana jest w ośrodku egzaminacyjnym. Instytucja certyfikująca musi zapewnić: • pracownię wyposażoną w stanowisko komputerowe dla każdego uczestnika walidacji tj. stół, krzesło, komputer z dostępem do Internetu, pakietem programów biurowych i z dostępem do drukarki, • scenariusze zadań praktycznych, opisy przypadków. Test teoretyczny przeprowadzany jest w ośrodku egzaminacyjnym za pomocą zautomatyzowanego systemu elektronicznego (system rejestracji kandydatów i obsługi egzaminów). Wykorzystanie innych narzędzi/aplikacji pomocniczych w tym urządzeń mobilnych oraz dostępu do sieci Internet jest dopuszczalne wyłącznie w sytuacji, w której jest to wymagane specyfiką zadań testowych. Instytucja certyfikująca musi zapewnić: • salę z wyposażeniem multimedialnym i możliwością rejestracji audio-wideo przebiegu walidacji oraz stanowiska egzaminacyjne umożliwiające samodzielną pracę każdej osobie przystępującej do walidacji np. boksy biurowe zapewniające przeprowadzenie testów z zachowaniem bezpieczeństwa i poufności procesu walidacyjnego; • centralnie zarządzaną platformę informatyczną do przeprowadzania testów i przechowywania wyników (system rejestracji kandydatów i obsługi egzaminów) spełniającą wymagania określone w przepisach RODO; - sprzęt komputerowy oraz dostęp do systemu obsługi testów i egzaminów indywidualnie dla każdego uczestnika; • nadzór osobowy w charakterze obserwatora/obserwatorów w celu zapewnienia prawidłowego przebiegu egzaminu (w tym przeciwdziałania nieuczciwym praktykom). 2. Etap identyfikowania i dokumentowania efektów uczenia się Instytucja certyfikująca może zapewniać wsparcie dla kandydatów w zakresie identyfikowania oraz dokumentowania posiadanych efektów uczenia się. Korzystanie z tego wsparcia nie jest obowiązkowe. 2.1 Metody Etapy identyfikowania i dokumentowania mogą być realizowane w oparciu o dowolne metody zapewniające osiągnięcie celów tych etapów walidacji. 2.2 Zasoby kadrowe Doradca walidacyjny. Zadaniem doradcy walidacyjnego jest wsparcie osoby przystępującej do procesu walidacji na każdym etapie tego procesu. Doradca walidacyjny pomaga w zidentyfikowaniu posiadanych efektów uczenia się oraz w ich rzetelnym udokumentowaniu na potrzeby walidacji. Pomaga również w określeniu innych, możliwych do potwierdzenia kwalifikacji oraz perspektyw rozwoju i dalszego uczenia się po uzyskaniu kwalifikacji. Udziela informacji dotyczących przebiegu walidacji, wymagań związanych z przystąpieniem do weryfikacji efektów uczenia się oraz kryteriów i sposobów oceny. Funkcję doradcy walidacyjnego może pełnić osoba, która posiada: ● doświadczenie zawodowe związane z bilansowaniem kompetencji, ● doświadczenie w weryfikowaniu efektów uczenia się lub ocenie kompetencji, ● umiejętność stosowania metod i narzędzi wykorzystywanych przy identyfikowaniu i dokumentowaniu kompetencji, ● wiedzę dotyczącą niniejszej kwalifikacji oraz innych kwalifikacji funkcjonujących w obszarze technologii cyfrowej. 2.3 Sposób organizacji walidacji oraz warunki organizacyjne i materialne etapu identyfikowania i dokumentowania Instytucja certyfikująca może zapewnić osobom przystępującym do walidacji wsparcie na etapie identyfikowania i dokumentowania. Etap ten może być również realizowany przez te osoby samodzielnie. Instytucja certyfikująca, która zdecyduje się na wsparcie osób w procesie identyfikowania i dokumentowania powinna zapewnić warunki umożliwiające im indywidualną rozmowę z doradcą walidacyjnym. Instytucja certyfikująca może również udzielać wsparcia zdalnie tzn. za pośrednictwem telefonu lub Internetu, w warunkach zapewniających poufność rozmowy.

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

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się*

Osoba posiadająca kwalifikację rozpoznaje zdarzenia, które są incydentami naruszającymi bezpieczeństwo oraz podejmuje działania niezbędne do dokonania zgłoszenia incydentu do właściwego podmiotu Krajowego Systemu Cyberbezpieczeństwa. W szczególności ustala, na podstawie dokumentacji, moment wystąpienia incydentu, czas jego trwania, przebieg oraz ustala zadania, procesy, zasoby i osoby, na które ma wpływ zaistniałe naruszenie. Wskazuje incydenty krytyczne wymagające natychmiastowej reakcji, uwzględniając skutki ich wystąpienia. Ponadto koordynuje pracę osób i podmiotów realizujących działania naprawcze oraz minimalizujące następstwa wystąpienia incydentu. Ustala harmonogram działań, niezbędne zasoby oraz kryteria zakończenia obsługi incydentu w obszarze cyberbezpieczeństwa. Przedstawia informacje niezbędne do podjęcia, przez osoby decyzyjne, decyzji o sposobie realizacji działań naprawczych, w tym wymienia utrudnienia, jakie mogą wiązać się z obsługą incydentu oraz analizuje zasadność podjęcia poszczególnych działań. Przekazuje informacje o zaistniałym incydencie osobom i podmiotom, których dotyczy naruszenie.

Zestawy efektów uczenia się

Numer zestawu w kwalifikacji*

1

Nazwa zestawu*

Wykrywanie incydentów w obszarze cyberbezpieczeństwa

Poziom PRK*

4

Orientacyjny nakład pracy [godz.]*

50

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. Identyfikuje incydenty w obszarze cyberbezpieczeństwa

Kryteria weryfikacji*

a. Wyjaśnia pojęcia poufności, integralności i dostępności danych oraz systemów informatycznych; b. Wyjaśnia pojęcie incydentu w obszarze cyberbezpieczeństwa; c. Charakteryzuje typy incydentów w obszarze cyberbezpieczeństwa; d. Rozpoznaje, na podstawie opisu sytuacji, zdarzenia będące incydentami w obszarze cyberbezpieczeństwa; e. Określa, na podstawie opisu technicznego incydentu, jego typ według wybranej klasyfikacji spośród powszechnie uznawanych, np. klasyfikacji eCSIRT.net

Efekt uczenia się

2. Analizuje incydenty w obszarze cyberbezpieczeństwa

Kryteria weryfikacji*

a. Ustala, na podstawie dziennika zdarzeń systemowych (logów), moment wystąpienia incydentu w obszarze cyberbezpieczeństwa oraz czas jego trwania; b. Ustala zadania, procesy, zasoby i osoby, na które wpływa incydent w obszarze cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, dziennika zdarzeń systemowych); c. Opisuje przebieg incydentu w obszarze cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, dziennika zdarzeń systemowych); d. Wskazuje możliwe przyczyny zaistnienia incydentu w obszarze cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, dziennika zdarzeń systemowych).

Efekt uczenia się

3. Klasyfikuje incydenty w obszarze cyberbezpieczeństwa

Kryteria weryfikacji*

a. Identyfikuje, na podstawie opisu sytuacji, skutki wystąpienia określonego incydentu w obszarze cyberbezpieczeństwa; b. Szereguje incydenty w obszarze cyberbezpieczeństwa według priorytetów obsługi; c. Wskazuje incydenty krytyczne w obszarze cyberbezpieczeństwa wymagające natychmiastowej reakcji.

Numer zestawu w kwalifikacji*

2

Nazwa zestawu*

Koordynowanie działań związanych z obsługą incydentów w obszarze cyberbezpieczeństwa

Poziom PRK*

5

Orientacyjny nakład pracy [godz.]*

30

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. Zgłasza incydent w obszarze cyberbezpieczeństwa

Kryteria weryfikacji*

a. Wskazuje akty prawne regulujące obowiązki w zakresie zgłaszania i obsługi incydentów w obszarze cyberbezpieczeństwa; 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 (na

podstawie np. opisu sytuacji, dokumentacji technicznej systemu informatycznego, którego dotyczy incydent, opisu technicznego incydentu, dziennika zdarzeń systemowych); d. Opisuje zasady postępowania w przypadku zaistnienia incydentów związanych z naruszeniem ochrony danych osobowych.

Efekt uczenia się

2. Planuje działania związane z obsługą incydentu w obszarze cyberbezpieczeństwa

Kryteria weryfikacji*

a. Wymienia działania niezbędne do obsługi incydentu w obszarze cyberbezpieczeństwa, w tym działania naprawcze, działania ograniczające szkody; b. Ustala harmonogram działań, w tym określa działania priorytetowe, działania, które mają być wykonane sekwencyjnie i te, które mogą być wykonane równolegle; c. Wskazuje zasoby techniczne i kadrowe niezbędne do obsługi incydentu w obszarze cyberbezpieczeństwa; d. Wskazuje możliwe utrudnienia związane z prowadzeniem działań związanych z obsługą incydentów w obszarze cyberbezpieczeństwa (np. utrudnione korzystanie z systemu, czasowe ograniczenia w funkcjonowaniu systemu); e. Ocenia zasadność podjęcia działań naprawczych z uwzględnieniem ich kosztów, oczekiwanych rezultatów oraz skutków wystąpienia incydentu w obszarze cyberbezpieczeństwa.

Efekt uczenia się

3. Monitoruje działania związane z obsługą incydentu w obszarze cyberbezpieczeństwa

Kryteria weryfikacji*

a. Wskazuje kryteria oceny skuteczności działań związanych z obsługą incydentu w obszarze cyberbezpieczeństwa (na podstawie np. opisu sytuacji, dziennika zdarzeń systemowych); b. Ustala kryteria zamknięcia obsługi danego incydentu w obszarze cyberbezpieczeństwa; c. Formułuje, na podstawie opisu przyczyn wystąpienia incydentu w obszarze cyberbezpieczeństwa, wnioski dotyczące minimalizowania ryzyka jego ponownego wystąpienia.

Efekt uczenia się

4. Informuje o wystąpieniu incydentu w obszarze cyberbezpieczeństwa osoby i podmioty, których incydent dotyczy

Kryteria weryfikacji*

a. Wskazuje grupy osób i podmiotów (np. klientów, pracowników, kontrahentów), które należy poinformować o zaistnieniu danego incydentu w obszarze cyberbezpieczeństwa; b. Opisuje zasady informowania o incydencie w obszarze cyberbezpieczeństwa, w tym związane z terminami, zakresem i stopniem szczegółowości przekazywanych informacji; c. Opisuje zagrożenia związane z przekazywaniem informacji o incydencie w obszarze cyberbezpieczeństwa osobom i podmiotom, których incydent dotyczy (np. związane z wywoływaniem paniki, przekazywaniem niepełnych informacji, stratami wizerunkowymi); d. Formułuje, dla danej grupy odbiorców, informację dotyczącą incydentu w obszarze cyberbezpieczeństwa.

Informacje o instytucjach uprawnionych do nadawania kwalifikacji

Wnioskodawca*

Polskie Towarzystwo Informatyczne

Minister właściwy*

Minister Rozwoju i Technologii

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności*

Certyfikat jest ważny 3 lata. Przedłużenie ważności certyfikatu następuje na podstawie przedłożenia dokumentów potwierdzających wykonywanie, w okresie ważności certyfikatu, zadań związanych z obsługą incydentów w obszarze cyberbezpieczeństwa przez okres co najmniej 12 miesięcy.

Nazwa dokumentu potwierdzającego nadanie kwalifikacji*

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji*

Nie dotyczy

Kod dziedziny kształcenia*

481 - Informatyka

Kod PKD*

Kod	Nazwa
62	DZIAŁALNOŚĆ ZWIĄZANA Z OPROGRAMOWANIEM I DORADZTWEM W ZAKRESIE INFORMATYKI ORAZ DZIALALNOŚĆ POWIĄZANA

Status

Dokumenty

#	Tytuł dokumentu
1	Dowód wniesienia opłaty
2	Pełnomocnictwo
3	ZRK_FKU_nie dotyczy
4	ZRK_FKU_Obsługa incydentów w obszarze cyberbezpieczeństwa

☒

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

Polskie Towarzystwo Informatyczne
Siedziba i adres: Solec 38 lok. 103, 00-394 Warszawa
NIP: 5220002038
REGON: 001236905
Numer KRS: 0000043879