

Zintegrowany Rejestr Kwalifikacji

Kwalifikacja - podgląd

Nazwa kwalifikacji

Zarządzanie cyberbezpieczeństwem - menedżer

Skrót nazwy

Certyfikowany menedżer cyberbezpieczeństwa (CMCB)

Rodzaj kwalifikacji

kwalifikacja cząstkowa

Poziom PRK/ERK

6

Krótką charakterystyka kwalifikacji, obejmująca informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikację

Osoba z kwalifikacją "Zarządzanie cyberbezpieczeństwem - menedżer" posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi krajowymi i UE z obszaru cyberbezpieczeństwa. Posiada również wiedzę dotyczącą opracowywania strategii cyberbezpieczeństwa w organizacji, wdrażania środków, planów i procedur bezpieczeństwa IT, zarządzania ryzykiem, ciągłości działania oraz incydentami cyberbezpieczeństwa i audytu bezpieczeństwa. Jest przygotowana do zarządzania zespołami reagowania na incydenty bezpieczeństwa komputerowego. Dysponuje również wiedzą w obszarze bezpieczeństwa infrastruktury teleinformatycznej i zasobów ludzkich. Posiada przygotowanie merytoryczne w obszarze zastosowań informatyki śledczej. Osoby posiadające kwalifikację mogą podjąć zatrudnienie m.in.: w naczelnych, centralnych i terenowych organach administracji państwowej (w tym jednostkach samorządu terytorialnego), u operatorów usług kluczowych (UOK), w służbach mundurowych i specjalnych, w przedsiębiorstwach i organizacjach, w których konieczne jest utrzymywanie właściwego poziomu bezpieczeństwa informacji, przetwarzanej za pomocą systemów teleinformatycznych.

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]

240

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji

Uzyskaniem kwalifikacji mogą być zainteresowani: - kierownicy komórek organizacyjnych odpowiedzialni w organizacjach za ochronę informacji i cyberbezpieczeństwo oraz kształtowanie polityki bezpieczeństwa; - menedżerowie IT z doświadczeniem w zarządzaniu zespołem i doświadczeniem w obszarze technologicznym; - osoby posiadające kwalifikację CSCB, CECB; - osoby posiadające wiedzę, umiejętności i kompetencje wskazane w efektach uczenia się, chcące formalnie je potwierdzić.

Wymagane kwalifikacje poprzedzające

Opis

Kwalifikacja pełna z 6 poziomem PRK

Lista

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

- kwalifikacja pełna z 6 poziomem PRK; - udokumentowane 3-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa w ciągu ostatnich 6 lat; - oświadczenie o niekaralności za przestępstwo popełnione umyślnie ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe.

Zapotrzebowanie na kwalifikację

W przestrzeni publicznej funkcjonuje powszechny pogląd o braku dostatecznej liczby specjalistów z zakresu cyberbezpieczeństwa w Europie i na świecie. Problem ten dotyczy również rynek polskich pracodawców, zarówno w sektorze prywatnym jak i państwowym. Istnieje szereg opracowań analitycznych wskazujących na pogłębiający się problem z rekrutacją odpowiednio przygotowanych specjalistów z dziedziny cyberbezpieczeństwa. Z szacunków CISCO wynika, że na chwilę obecną w Polsce brakuje 5 tysięcy specjalistów ds. cyberbezpieczeństwa w firmach, za rok deficyt tych specjalistów podwoi się do 10 tysięcy[1], a połowa alertów o incydentach bezpieczeństwa w organizacjach pozostaje bez odpowiedzi z powodu braku odpowiednio wykwalifikowanych kadr. Na dramatyczny brak specjalistów do spraw cyberbezpieczeństwa wskazuje wiele innych opracowań. Raporty dowodzą, że zwrócenie uwagi na lukę w umiejętnościach i kompetencjach w zakresie cyberbezpieczeństwa, stało się niezbędne i priorytetowe w obliczu realnych zagrożeń cybernetycznych. Szczegółową analizę w przedmiotowym zakresie zawiera opracowanie Tommaso De Zan z Uniwersytetu w Oksfordzie pod nazwą „Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions” (luty 2019). Autor szeroko odnosi się w dokumencie do problemów edukacji oraz walidacji kompetencji w zakresie cyberbezpieczeństwa. Z lektury publikacji jednoznacznie wynika, że problem niedoborów specjalistów z obszaru bezpieczeństwa cybernetycznego istnieje i będzie się nasilać. Autor przytacza dane z raportów, np. ISACA (2018) stwierdza, że prawie 60% firm ma wakaty. CSIS-IS (2016) sugeruje, że 15% stanowisk w zakresie cyberbezpieczeństwa w przedsiębiorstwach pozostanie pustych do 2020 roku. (ISC)² (2018) uważa, że istnieje niedobór ok. 2,93 mln specjalistów ds. cyberbezpieczeństwa na rynku pracy, podczas gdy Cybersecurity Ventures-Herjavec Group przewiduje 3,5 mln otwarć miejsc pracy w cyberbezpieczeństwie/ niewypełnionych stanowisk w zakresie cyberbezpieczeństwa do 2021 roku (CV-HG, 2017). ISACA (2018) stwierdza, że 54% organizacji zajmuje od 3 do 6 miesięcy na obsadzenie wakatu lub nie może obsadzić wolnych stanowisk, podczas gdy Burningglass (2015) konstatuje, że firmy średnio 8% dłużej znajdują i wynajmują cyberspecjalistów. Z kolei w publikacji „Top cybersecurity concerns for every board of directors, part two: people” opracowanej przez John Reed Stark Consulting LLC (2018) 55% ankietowanych specjalistów w dziedzinie cyberbezpieczeństwa uważa, że „niedobór umiejętności w zakresie cyberbezpieczeństwa jest znacznie większym problemem niż jest przekazywane”. Według raportu McAfee przytoczonego przez autorów publikacji „Hacking the Skills Shortage” (2017) 82% respondentów zgodziło się, że istnieje duży niedobór w ich własnej organizacji, a także w całym kraju. Najwyższa Izba Kontroli po przeprowadzonych w latach 2015-2019 kontrolach w administracji państwowej w obszarze bezpieczeństwa elektronicznych zasobów informacyjnych i cyberprzestrzeni, uznaje za najważniejsze wyzwania edukację oraz pozyskanie i utrzymanie profesjonalnej kadry[2]. To tylko

część z wielu opracowań powstałych w ostatnich latach. W ramach prac Komisji Europejskiej w 2018 roku powstał dokument analityczny opracowany przez Europejską Organizację ds. Cyberbezpieczeństwa (ECISO), zawierający informacje o systemach certyfikacji w zakresie cyberbezpieczeństwa w Europie („Information and Cyber Security Professional Certification”). Raport opracowano w ramach prac grupy roboczej WG5, podgrupy EHR5CYBER, która koncentruje się w szczególności na zagadnieniach analizy europejskiej sieci zasobów ludzkich w obszarze cyberprzestrzeni. Autorzy publikacji odwołują się między innymi do badania opublikowanego w lutym 2017 roku pod nazwą „Global Information Security Workforce - Benchmarking Workforce Capacity and Response to Cyber Risk”[3]. W wyżej wymienionym opracowaniu autorzy[4] zaprezentowali wyniki ósmej edycji badania na próbie 19 641 respondentów (specjalistów od cyberbezpieczeństwa) reprezentujących 170 krajów. Dwie trzecie tych specjalistów wskazało, że w ich organizacjach nie ma wystarczającej liczby pracowników zajmujących się cyberbezpieczeństwem, aby sprostać wyzwaniom, przed którymi obecnie stoją. Badania wskazują również, że luka w zatrudnieniu w sektorze cyberbezpieczeństwa wyniesie 1,8 miliona specjalistów do roku 2022, co stanowi wzrost o 20% w stosunku do prognozy z 2015 roku. Pozytywną informacją płynącą z tego badania jest fakt, że w Europie 38% pracodawców planuje zwiększyć ilość zatrudnionych specjalistów z zakresu cyberbezpieczeństwa (największy wskaźnik regionalny). Menedżerowie muszą zacząć odkrywać nowe kanały rekrutacji i znajdować niekonwencjonalne strategie i techniki, aby wypełnić lukę pracowniczą w tym obszarze. Co istotne autorzy opracowania podkreślają, że ważne, o ile nie niezbędne, będzie rozważenie odpowiednich podstaw edukacyjnych, szkoleń i możliwości rozwoju zawodowego, które będą wspierać rynek w celu wypełnienia niedoboru pracowników. Innym opracowaniem analitycznym związanym z rynkiem specjalistów z obszaru cyberbezpieczeństwa, do którego odwołują się autorzy „Information and Cyber Security Professional Certification” jest dokument oryginalnie zatytułowany „H4CKER5 WANTED - An Examination of the Cybersecurity Labor Market”[5]. Publikacja odnosi się do rynku amerykańskiego, ale z powodzeniem można potraktować badania jako globalne zagadnienie (na co zresztą autorzy zwracają uwagę). Jeden z kluczowych wniosków tego raportu odnosi się do rosnącego popytu na specjalistów z zakresu cyberbezpieczeństwa. Istotną rekomendacją wynikającą z treści raportu jest udoskonalenie metod identyfikacji kandydatów, którzy mogą odnieść sukces w obszarze cyberbezpieczeństwa (np. poprzez oficjalnie uznaną kwalifikację zawodową, potwierdzoną stosownym certyfikatem). W publikacji przytoczono również analizę opracowaną w Uniwersytecie w Lejdzie w Holandii[6], pod kątem popytu i podaży specjalistów z zakresu cyberbezpieczeństwa (CSP[7]). Innym ze stwierdzeń jest teza, że firmy i organizacje publiczne są coraz bardziej świadome faktu, że cyberbezpieczeństwo to nie tylko kwestia IT. Niezależnie od przygotowania zawodowego oczekuje się, że popyt na specjalistów z obszaru cyberbezpieczeństwa wzrośnie. Dotyczy to głównie osób o wyższych kwalifikacjach. Autorzy dokumentu podkreślają, że certyfikacja umiejętności w zakresie cyberbezpieczeństwa jest coraz bardziej niezbędna zarówno wewnątrz dla samego pracodawcy, jak i dla jego zewnętrznych klientów pod względem jakości usług. Wiele kursów i szkoleń od różnych dostawców, w tym uniwersytetów i szkół wyższych niekoniecznie prowadzi do ujednoliconego programu nauczania, który byłby wymagany dla specjalistów cyberbezpieczeństwa. Zależność między popytem na specjalistów od bezpieczeństwa cybernetycznego, a podażą tych specjalistów jest zakłócona przez jakościowe rozbieżności i brak przejrzystości. To sprawia, że trudno jest ocenić, czy kandydaci spełniają wymagania. Na rynku europejskim i światowym istnieje wiele certyfikatów z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa dla osób fizycznych. Lista znajdująca się w serwisie Wikipedia obejmuje 107 pozycji[8]. Certyfikaty wydawane są przez szereg różnych organizacji w wielu krajach, jednak żaden z tych certyfikatów nie jest wydawany przez polski podmiot. Ich jakość i poziom akceptacji różnią się na całym świecie, od znanych i wysokiej jakości przykładów, po kontrowersyjną listę wielu dziesiątek mniej znanych organizacji. W Polsce popularność certyfikatów takich organizacji

jak ISACA czy (ISC)2 nie jest wysoka. Świadczyć może o tym niewielka liczba osób, które te certyfikaty posiadają[9]. Istnieją również kwestie problematyczne, na przykład: - większość certyfikatów, chociaż mają uznanie globalne, są ukierunkowane na amerykański rynek i specyfikę, zwłaszcza aspekty, takie jak ustawy i regulacje, ale także różnice kulturowe między narodami, - bariera językowa - zarówno kursy jak i egzaminy prowadzone są z użyciem trudnego, specjalistycznego słownictwa co zmniejsza motywację do ich zdobywania, - wysoki koszt uzyskania certyfikatów. W opinii krajowego środowiska branżowego, istnieje zapotrzebowanie na wdrożenie systemu certyfikacji narodowej, uznawanej przez Państwo, społeczności korporacyjne, środowiska naukowe, edukacyjne i organizacje pozarządowe. To przekonanie potwierdzono w procesie szeregu konsultacji zrealizowanych przez Polskie Towarzystwo Informatyczne m.in. z kluczowymi interesariuszami z sektorów rządowego, telekomunikacyjnego, naukowego czy prawniczego. Zapotrzebowanie na wnioskowaną kwalifikację jest bezsporne. Wraz z przedmiotową kwalifikacją zostały złożone dwa inne wnioski na kwalifikacje „Zarządzanie cyberbezpieczeństwem – specjalista” (CSCB) oraz „Zarządzanie cyberbezpieczeństwem – ekspert” (CECB). Należy zwrócić uwagę, że wszystkie trzy kwalifikacje są merytorycznie zróżnicowane. Niniejsza kwalifikacja „Zarządzanie cyberbezpieczeństwem – menedżer” koncentruje się na zagadnieniach związanych z zarządzaniem w obszarze cyberbezpieczeństwa, dedykowanym dla osób przygotowujących się do pełnienia roli kierowniczej w zespole lub organizacji („team leader”), odpowiedzialnych w szczególności za kształtowanie i nadzorowanie realizacji polityki bezpieczeństwa IT. Osoby te nie muszą być „techniczne”. Tymczasem kwalifikacja CECB (ekspert) jest kierowana przede wszystkim do osób o pogłębionych umiejętnościach technicznych w obszarze bezpieczeństwa systemów teleinformatycznych. Osoby te najczęściej będą posiadały wiedzę i praktyczne przygotowanie do realizacji funkcji administratorów systemów zorientowanych w szczególności na ich bezpieczeństwo. Z kolei kwalifikacja CSCB (specjalista) przeznaczona jest dla początkujących pracowników komórek odpowiedzialnych za cyberbezpieczeństwo w organizacji. Osoby te będą odpowiedzialne głównie za realizowanie powtarzalnych, rutynowych zadań na podstawie opracowanych już procedur.

Przypisy: [1] <http://next.gazeta.pl/next/7,151243,24551696,specjalisci-od-cyberbezpieczenstwa-pilnie-potrzebni-juz-dzis.html> [2] Wystąpienie przedstawiciela NIK na XII Forum Bezpieczeństwa i Audytu IT SEMAFOR, marzec 2019 [3] <https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf> [4] Center for Cyber Safety and Education, (ISC)2, Booz Allen Hamilton (Presenting sponsor), Alta Associates (Gold sponsor), and Frost & Sullivan [5] Autor: RAND Corporation [6] https://www.wodc.nl/binaries/2486-summary_tcm28-73678.pdf [7] ang. Cyber Security Professionals [8] https://en.wikipedia.org/wiki/List_of_computer_security_certifications [9] Na przykład: <https://www.isc2.org/en/About/Member-Counts>

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

Ministerstwo Cyfryzacji proceduje następujące wnioski o włączenie kwalifikacji rynkowych z obszaru cyberbezpieczeństwa: - „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”. Po przeprowadzeniu analizy przedmiotowych wniosków nie zidentyfikowano wspólnych zestawów uczenia się dla żadnej z kwalifikacji. Należy podkreślić, że złożone wnioski odnoszą się do dedykowanego stosowania kwalifikacji w przemyśle, ze szczególnym zorientowaniem na systemy informatyczne nadzorujące przebiegi 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 obszarze szkolnictwa wyższego prowadzone są kierunki i studia podyplomowe związane z bezpieczeństwem informacji i cyberbezpieczeństwem, niemniej zakres merytoryczny poszczególnych kierunków jest zróżnicowany i nie odnosi się bezpośrednio do przedmiotowej kwalifikacji. Z niniejszą kwalifikacją zostały złożone dwa inne wnioski na kwalifikacje „Zarządzanie cyberbezpieczeństwem – specjalista” (CSCB) oraz „Zarządzanie cyberbezpieczeństwem – ekspert” (CECB). W wyżej wymienionych kwalifikacjach występują zestawy lub komponenty zestawów (zarówno umiejętności jak i kryteria weryfikacji) o zbliżonym znaczeniu i opisie, lecz w każdym przypadku dotyczą innych zadań realizowanych przez osoby posiadające każdą z wymienionych kwalifikacji. Zestaw efektów uczenia się o nazwie „Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa” jest wspólny dla wszystkich trzech kwalifikacji, ale dla kwalifikacji CSCB został rozszerzony o jedno kryterium. Również obszar związany z informatyką śledczą występuje we wszystkich trzech kwalifikacjach. Przedmiotowa kwalifikacja, inaczej niż pozostałe, dotyczy w szczególności zarządzania cyberbezpieczeństwem. Dodatkowo obejmuje następujące obszary: zarządzanie ryzykiem, bezpieczeństwo IT i zarządzanie ciągłością działania, zarządzanie incydentami, audyt bezpieczeństwa oraz bezpieczeństwo zasobów ludzkich.

Streszczenie opinii uzyskanych podczas konsultacji projektu kwalifikacji

Informacje zawarte we wniosku, jak również opinie otrzymane w ramach konsultacji, wykazały zgodność kwalifikacji z potrzebami społecznymi oraz z zapotrzebowaniem na rynku pracy.

Typowe możliwości wykorzystania kwalifikacji

Osoby posiadające kwalifikację mogą podjąć zatrudnienie m.in.: - w naczelnych, centralnych i terenowych organach administracji państwowej (w tym jednostkach samorządu terytorialnego), - u operatorów usług kluczowych (UOK), - w służbach mundurowych i specjalnych, - w przedsiębiorstwach i organizacjach, w których konieczne jest utrzymywanie właściwego poziomu bezpieczeństwa informacji, przetwarzanej za pomocą systemów teleinformatycznych. Kwalifikacja w szczególności może być wykorzystana w zespołach reagowania na incydenty komputerowe CERT/CSIRT (ang. Computer Emergency Response Team/Computer Security Incident Response Team) oraz operacyjnych centrach bezpieczeństwa SOC (ang. Security Operations Center) – utworzenie SOC to obowiązek ustawy dla UOK.

Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację

1. Etap weryfikacji. 1.1. Metody. Do weryfikacji efektów uczenia się stosuje się wyłącznie: test teoretyczny (pisemny) lub analizę dowodów i deklaracji opcjonalnie uzupełnioną wywiadem swobodnym. 1.2. Zasoby kadrowe. 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 3-letnim doświadczeniem w przeprowadzaniu egzaminów, osiągniętym w okresie ostatnich 6 lat, - legitymuje się co najmniej jednym ważnym certyfikatem CISA, CISM, CRISC, CGEIT, CISSP, wymienionym między innymi w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.poz. 1999). 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 technologii

cyfrowej, osiągniętych 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. Test teoretyczny przeprowadzany jest w ośrodku egzaminacyjnym przy pomocy 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). Warunki dodatkowe: - instytucja certyfikująca nie może kształcić oraz prowadzić szkoleń, kursów, itp. z zakresu wiedzy ujętej w przedmiotowej kwalifikacji; - walidacja prowadzona jest zgodnie z procedurami instytucji certyfikującej we własnym zakresie lub w akredytowanych laboratoriach przez certyfikowanych egzaminatorów; - każdy asesór walidacyjny oraz obserwator zobowiązany jest do złożenia oświadczenia o braku okoliczności stanowiących podstawę wyłączenia z czynności egzaminacyjnych (np. konflikt interesów). 2. Etapy identyfikowania i dokumentowania. Instytucja certyfikująca musi zapewnić wsparcie doradcy walidacyjnego. Doradca walidacyjny musi spełnić następujące warunki: - zgodność z profilem kompetencyjnym doradcy walidacyjnego określonym w podręczniku "WALIDACJA – nowe możliwości zdobywania kwalifikacji" opracowanym przez Instytut Badań Edukacyjnych, Warszawa 2016 (link: http://www.kwalifikacje.gov.pl/download/Publikacje/Walidacja_nowe_mozliwosci_zdobywania_kwalifikacji_z_wkladka.pdf); - min. 5 lat doświadczenia zawodowego w branży teleinformatycznej. Dokumentacja dowodowa z przeprowadzonej walidacji przechowywana jest przez minimum 5 lat. Ponadto instytucja certyfikująca jest zobowiązana do bezterminowego prowadzenia rejestru wydanych certyfikatów. Certyfikaty muszą być niepowtarzalne (w rozumieniu druku ścisłego zarachowania), posiadać cechy umożliwiające jednoznaczną identyfikację instytucji certyfikującej oraz jedno z wybranych zabezpieczeń - optyczne (np. hologram, kinegram) lub inne.

Odniesienie do poziomu sektorowych ram kwalifikacji (o ile dotyczy)

Nie dotyczy

Data włączenia kwalifikacji do ZSK

2021-02-17

Podstawa prawna

Obwieszczenie Ministra Cyfryzacji z dnia 8 lutego 2021 r. w sprawie włączenia kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem - menedżer” do Zintegrowanego Systemu Kwalifikacji (Monitor Polski z dnia 17 lutego 2021 r, poz. 189).

Syntetyczna charakterystyka efektów uczenia się

Osoba z kwalifikacją „Zarządzanie cyberbezpieczeństwem – menedżer” posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi

krajowymi i UE z obszaru cyberbezpieczeństwa. Posiada wiedzę dotyczącą opracowywania strategii cyberbezpieczeństwa w organizacji, wdrażania środków, planów i procedur bezpieczeństwa IT, zarządzania ryzykiem, ciągłości działania oraz incydentami cyberbezpieczeństwa i audytu bezpieczeństwa. Posiada wiedzę w zakresie funkcjonowania zespołów reagowania na incydenty bezpieczeństwa komputerowego. Dysponuje również wiedzą w obszarze bezpieczeństwa infrastruktury teleinformatycznej. Posiada również przygotowanie merytoryczne w obszarze zastosowań informatyki śledczej.

Zestawy efektów uczenia się

Numer zestawu w kwalifikacji

1

Nazwa zestawu

Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa

Poziom

4

Orientacyjny nakład pracy [godz.]

40

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. Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa

Kryteria weryfikacji

- omawia bezpieczeństwo komputerowe; - omawia cele bezpieczeństwa informacji; - charakteryzuje terminologię z obszaru bezpieczeństwa informacji (np. cyberatak, incydent, wirus); - omawia pojęcia: cyberbezpieczeństwo, cyberprzestrzeń i cyberprzestrzeń RP, bezpieczeństwo i ochrona cyberprzestrzeni, bezpieczeństwo sieci i systemów informatycznych; charakteryzuje zagrożenia teleinformatyczne (np. cyberprzestępczość, haking, haktywizm, haktywizm patriotyczny, cyberterrorizm, cyberszpiegostwo, militarne wykorzystanie cyberprzestrzeni); - rozróżnia zagrożenia, ataki i aktywa; - omawia funkcjonalne wymagania bezpieczeństwa.

Efekt uczenia się

2. Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa

Kryteria weryfikacji

- omawia krajowe przepisy prawne dotyczące cyberbezpieczeństwa, w tym: kodeks karny w obszarze cyberprzestępczości, ustawa o krajowym systemie cyberbezpieczeństwa, ustawa o działaniach antyterrorystycznych w obszarze cyberbezpieczeństwa, ustawa o usługach zaufania oraz identyfikacji elektronicznej, ustawa o ochronie danych osobowych, przepisy o

własności intelektualnej; - omawia opracowania dotyczące cyberbezpieczeństwa RP, w tym: plany, doktryny, koncepcje, wizje, ramy, strategie, programy, uchwały dotyczące ochrony cyberprzestrzeni; - omawia wyniki kontroli organów państwowych w obszarze zarządzania cyberbezpieczeństwem; - omawia analizy i rekomendacje eksperckie i naukowe dotyczące cyberbezpieczeństwa w Polsce i na świecie; - omawia przepisy prawne oraz opracowania Unii Europejskiej dotyczące cyberbezpieczeństwa (np. obowiązujące konwencje, dyrektywy, strategie, rozporządzenia, analizy); - omawia kodeksy etyki i postępowania sformułowane przez ACM, IEEE oraz AITP.

Numer zestawu w kwalifikacji

2

Nazwa zestawu

Zarządzanie cyberbezpieczeństwem

Poziom

6

Orientacyjny nakład pracy [godz.]

40

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. Omawia standardy i organizacje standaryzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT

Kryteria weryfikacji

- charakteryzuje standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standaryzacyjne, takie jak NIST, ITU-T, ISO, IEEE, ISACA; - omawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji według rodziny norm ISO/IEC 27000; - identyfikuje i opisuje zbiór najlepszych praktyk zarządzania usługami IT w odniesieniu do cyberbezpieczeństwa zgodnie z kodeksem postępowania dla działów informatyki określanym jako ITIL (ang. Information Technology Infrastructure Library); - omawia standard COBIT (ang. Control Objectives for Information and related Technology) opracowany przez ISACA oraz IT Governance Institute stanowiący zbiór dobrych praktyk z zakresu IT Governance.

Efekt uczenia się

2. Omawia strategię cyberbezpieczeństwa w organizacji

Kryteria weryfikacji

- omawia zasady projektowania cyberbezpieczeństwa; - określa role i przypisuje odpowiedzialności poszczególnych osób w procesie zarządzania cyberbezpieczeństwem; - wymienia i wartościuje zagrożenia i ataki oraz techniki wykorzystywania słabości bezpieczeństwa; - omawia architekturę bezpieczeństwa informacji w organizacji; - wymienia przykłady implementacji strategii w odniesieniu do obowiązujących norm i standardów; - różnicuje sposoby diagnozy i walidacji skuteczności procesu zarządzania cyberbezpieczeństwem.

Numer zestawu w kwalifikacji

3

Nazwa zestawu

Zarządzanie ryzykiem

Poziom

6

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. Charakteryzuje standardy i metody oceny ryzyka bezpieczeństwa informacji

Kryteria weryfikacji

- omawia i analizuje standardy opisujące procesy oceny ryzyka bezpieczeństwa informatycznego, w tym: ISO 13335, ISO 27005, ISO 31000, NIST SP 800-30; - charakteryzuje inne metodyki szacowania ryzyka, w tym: EBIOS, MAGERIT, CRAMM, MEHARI, MIGRA, OCTAVE.

Efekt uczenia się

2. Charakteryzuje ryzyko bezpieczeństwa informacji w organizacji

Kryteria weryfikacji

- opisuje proces zarządzania ryzykiem; - identyfikuje i grupuje wartości aktywów w organizacji; - kategoryzuje zagrożenia i podatności (ryzyka) dla tych aktywów; - omawia podejścia do oceny ryzyka bezpieczeństwa (podstawowe, nieformalne, szczegółowe, łączone); - wybiera i uzasadnia optymalne podejście do oceny ryzyka bezpieczeństwa.

Numer zestawu w kwalifikacji

4

Nazwa zestawu

Bezpieczeństwo IT i zarządzanie ciągłością działania

Poziom

6

Orientacyjny nakład pracy [godz.]

40

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. Charakteryzuje środki, plany i procedury bezpieczeństwa IT

Kryteria weryfikacji

- porównuje rodzaje środków bezpieczeństwa (organizacyjne, operacyjne, techniczne) w oparciu o standardy, w tym ISO 27002, ISO 13335, FIPS 200, NIST SP 800-53; - omawia budowę oraz etapy tworzenia i wdrażania planu bezpieczeństwa IT w organizacji; - opisuje aspekty monitorowania zagrożeń w procesie zarządzania bezpieczeństwem IT.

Efekt uczenia się

2. Charakteryzuje regulacje formalno-prawne i standardy związane z zarządzaniem ciągłością działania

Kryteria weryfikacji

- omawia zawarte w krajowych aktach prawnych zapisy dotyczące wymagań w zakresie zapewnienia ciągłości działania; - charakteryzuje normy ISO 22301 oraz ISO 22313; - opisuje zasady ustanawiania strategii zarządzania i polityki ciągłości działania w organizacji.

Numer zestawu w kwalifikacji

5

Nazwa zestawu

Zarządzanie incydentami

Poziom

6

Orientacyjny nakład pracy [godz.]

20

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. Charakteryzuje obszar zarządzania zespołami reagowania na incydenty bezpieczeństwa komputerowego

Kryteria weryfikacji

- charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSIRT); - wskazuje korzyści związane z posiadaniem procedur reagowania na incydenty; - omawia zasady działania krajowego systemu cyberbezpieczeństwa.

Efekt uczenia się

2. Omawia regulacje formalno-prawne, standardy, procedury i dobre praktyki związane z zarządzaniem incydentami

Kryteria weryfikacji

- opisuje standardy oraz regulacje formalno-prawne związane z zarządzaniem incydentami; - dobiera i uzasadnia metody zapewnienia usystematyzowanego podejścia do zarządzania i obsługi incydentów bezpieczeństwa informacji; - omawia zasady klasyfikacji i kwalifikacji zdarzeń jako incydentów bezpieczeństwa; - analizuje zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji.

Numer zestawu w kwalifikacji

6

Nazwa zestawu

Audyt bezpieczeństwa w obszarze cyberbezpieczeństwa

Poziom

6

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. Charakteryzuje obszar audytu bezpieczeństwa

Kryteria weryfikacji

- omawia terminy stosowane w obszarze audytu bezpieczeństwa; - opisuje cele i zakres audytu bezpieczeństwa; - omawia zasady opracowywania wymagań dotyczących audytu bezpieczeństwa; - porównuje standardy audytowania bezpieczeństwa; - omawia przebieg procesu audytu bezpieczeństwa; - opisuje narzędzia wykorzystywane w trakcie audytu bezpieczeństwa; - charakteryzuje zasady raportowania wyników bezpieczeństwa.

Numer zestawu w kwalifikacji

7

Nazwa zestawu

Bezpieczeństwo fizyczne i bezpieczeństwo zasobów ludzkich w obszarze cyberbezpieczeństwa

Poziom

6

Orientacyjny nakład pracy [godz.]

20

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. Charakteryzuje zagadnienia dotyczące bezpieczeństwa fizycznego infrastruktury teleinformatycznej

Kryteria weryfikacji

- charakteryzuje zagrożenia środowiskowe; - charakteryzuje zagrożenia techniczne; - charakteryzuje zagrożenia związane z działalnością człowieka.

Efekt uczenia się

2. Omawia dobre praktyki i zasady zatrudniania pracowników w obszarze cyberbezpieczeństwa

Kryteria weryfikacji

- wymienia cele bezpieczeństwa procesu rekrutacji; - opisuje wytyczne dotyczące sprawdzania kandydatów na kluczowe stanowiska w organizacji związane z zarządzaniem cyberbezpieczeństwem; - wylicza i wartościuje korzyści związane z motywowaniem pracowników do podnoszenia wiedzy z zakresu cyberbezpieczeństwa i stosowania się do procedur w tym zakresie; - charakteryzuje zagadnienia dotyczące obszaru podnoszenia

świadomości bezpieczeństwa, szkoleń i programów edukacyjnych; - omawia zagadnienia etyki zawodowej w obszarze cyberbezpieczeństwa i aspekty własności intelektualnej.

Numer zestawu w kwalifikacji

8

Nazwa zestawu

Informatyka śledcza

Poziom

6

Orientacyjny nakład pracy [godz.]

20

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. Charakteryzuje zagadnienia dotyczące norm, standardów i dobrych praktyk informatyki śledczej

Kryteria weryfikacji

- charakteryzuje wytyczne dotyczące aspektów technicznych i najlepszych praktyk informatyki śledczej, w tym SWGDE (ang. The Scientific Working Group on Digital Evidence), SWGIT (ang. The Scientific Working Group on Imaging Technology); - omawia standardy ANSI (ang. American National Standards Institute), NIST (ang. National Institute of Standard and Technology) oraz normy międzynarodowe ISO/IEC z rodziny norm ISO/IEC 27000 w obszarze informatyki śledczej.

Efekt uczenia się

2. Charakteryzuje zasady zabezpieczania i metody analizy dowodów elektronicznych

Kryteria weryfikacji

- charakteryzuje sposoby prawidłowego zabezpieczania materiału dowodowego na potrzeby dochodzenia wewnętrznego, jak również na potrzeby procesowe; - omawia zasady postępowania z cyfrowymi śladami dowodowymi; - wymienia metody analizy zawartości komputerów i urządzeń mobilnych za pomocą specjalistycznych narzędzi oraz oprogramowania dedykowanego do prowadzenia analiz; - opisuje prawa i obowiązki podmiotów w zakresie realizacji czynności procesowych prowadzonych w ramach postępowań przygotowawczych przez służby bezpieczeństwa i porządku publicznego.

Informacje o instytucjach uprawnionych do nadawania kwalifikacji

Instytucja uprawniona do nadawania kwalifikacji

Polskie Towarzystwo Informatyczne

Data uzyskania uprawnień do nadawania kwalifikacji

2021-04-06

Termin wykonania ewaluacji zewnętrznej

Instytucja prowadząca ewaluację zewnętrzną

Grupa Gumułka Euroedukacja Spółka z o.o.

Data zawarcia umowy na pełnienie funkcji zewnętrznego zapewniania jakości wobec instytucji certyfikującej

2021-08-24

Status

aktywny

Wnioskodawca

Polskie Towarzystwo Informatyczne

Minister właściwy

Minister Cyfryzacji

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności

Certyfikat jest ważny 5 lat. Przedłużenie następuje na podstawie przedłożenia dokumentów potwierdzających: - zatrudnienie przez minimum 3 lata w okresie ostatnich 5 lat poprzedzających przedłużenie certyfikatu w charakterze osoby odpowiedzialnej za realizację zadań tożsamy z uzyskaną kwalifikacją; - ustawiczne doskonalenie kompetencji poprzez między innymi udział w konferencjach, szkoleniach, warsztatach o tematyce tożsamej z uzyskaną kwalifikacją w wymiarze minimum 200 godzin w okresie ostatnich 5 lat poprzedzających przedłużenie certyfikatu.

Termin dokonywania przeglądów kwalifikacji (dotyczy kwalifikacji rynkowych)

2030-02-17

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 DORADZTWEW W ZAKRESIE INFORMATYKI ORAZ DZIAŁALNOŚĆ POWIĄZANA

Kod kwalifikacji w ZRK

6C482100009

Status

Włączona