# Zintegrowany Rejestr Kwalifikacji

## Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji*

Zarządzanie cyberbezpieczeństwem - ekspert

Skrót nazwy

Certyfikowany ekspert cyberbezpieczeństwa (CECB)

Rodzaj kwalifikacji*

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji*

6

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 z kwalifikacją “Zarządzanie cyberbezpieczeństwem - ekspert” posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi krajowymi i UE z obszaru cyberbezpieczeństwa. Posiada umiejętności samodzielnej realizacji zadań w obszarze bezpieczeństwa infrastruktury teleinformatycznej. Rozumie działanie algorytmów kryptograficznych oraz zasady zarządzania kontrolą dostępu do zasobów informacyjnych. Dysponuje wiedzą ekspercką z obszaru bezpieczeństwa sieci, systemów operacyjnych, baz danych, rozwiązań chmurowych i oprogramowania. Zna zagadnienia testowania bezpieczeństwa. Posiada wiedzę z obszarów: bezpieczeństwa, środowiskowego, technicznego i związanego z działalnością człowieka, zarządzania usługami IT, zarządzania incydentami bezpieczeństwa, w tym zasad funkcjonowania zespołów CERT/CSiRT. Posiada również wiedzę z zakresu 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 koszt uzyskania dokumentu potwierdzającego otrzymanie kwalifikacji wynosi 1500 złotych (PLN).

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

300

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Uzyskaniem kwalifikacji mogą być zainteresowani : - kierownicy komórek organizacyjnych odpowiedzialni w organizacjach za ochronę informacji i cyberbezpieczeństwo infrastruktury teleinformatycznej; - inżynierowie IT z doświadczeniem w obszarze technologicznym; - osoby posiadające kwalifikacje CSCB; - 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 dotyka 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 (ECSO), 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 wewnętrznie 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 bezsprzeczne. Wraz z przedmiotową kwalifikacją zostały złożone dwa inne wnioski na kwalifikacje „Zarządzanie cyberbezpieczeństwem – specjalista" (CSCB) oraz „Zarządzanie cyberbezpieczeństwem – menedżer" (CMCB). Należy zwrócić uwagę, że wszystkie trzy kwalifikacje są merytorycznie zróżnicowane. Niniejsza kwalifikacja „Zarządzanie cyberbezpieczeństwem – 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. Tymczasem kwalifikacja CMCB (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". 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 – menedżer” (CMCB). 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 administrowania systemami teleinformatycznymi w tym głównie w zakresie ich bezpieczeństwa. Dodatkowo obejmuje następujące obszary: kryptografia, zarządzanie uprawnieniami dostępu, bezpieczeństwo w sieci systemów operacyjnych, baz danych, rozwiązań chmurowych i oprogramowania a także testowanie bezpieczeństwa. W zestawie efektów “Elementy zarządzania cyberbezpieczeństwem” część kryteriów weryfikacji jest tożsama z kwalifikacją “Zarządzanie cyberbezpieczeństwem - menedżer”, jednak w węższym zakresie.

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 ustawowy 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. 2018 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, 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. 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 asesor 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.

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

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się*

Osoba z kwalifikacją “Zarządzanie cyberbezpieczeństwem - ekspert” posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi krajowymi i UE z obszaru cyberbezpieczeństwa. Posiada umiejętności samodzielnej realizacji zadań w obszarze bezpieczeństwa infrastruktury teleinformatycznej. Rozumie działanie algorytmów kryptograficznych oraz zasady zarządzania kontrolą dostępu do zasobów informacyjnych. Dysponuje wiedzą ekspercką z obszaru bezpieczeństwa sieci, systemów operacyjnych, baz danych, rozwiązań chmurowych i oprogramowania. Zna zagadnienia

testowania bezpieczeństwa. Posiada wiedzę z obszarów: bezpieczeństwa, środowiskowego, technicznego i związanego z działalnością człowieka, zarządzania usługami IT, zarządzania incydentami bezpieczeństwa, w tym zasad funkcjonowania zespołów CERT/CSiRT. Posiada również wiedzę z zakresu informatyki śledczej. Osoba posiadająca kwalifikację jest przygotowana do wykonywania samodzielnie złożonych zadań w zmiennych i nie w pełni przewidywalnych warunkach.

**Zestawy efektów uczenia się**

Numer zestawu w kwalifikacji*

1

Nazwa zestawu*

Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa

Poziom PRK*

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, cyberterroryzm, 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*

Kryptografia

Poziom PRK*

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. Omawia algorytmy kryptograficzne

Kryteria weryfikacji*

- charakteryzuje zasady szyfrów symetrycznych i asymetrycznych; - opisuje pojęcia i terminologię związaną z algorytmami szyfrowania, w tym: szyfry blokowe (DES, 3DES, AES), szyfry strumieniowe i RC4, tryby działania szyfrów blokowych, kryptoanaliza; - opisuje kryptograficzne funkcje skrótu m.in. SHA-1, SHA-2, SHA-3, MD5.

Efekt uczenia się

2. Omawia kryptografię klucza publicznego

Kryteria weryfikacji*

- porównuje działanie algorytmów RSA, krzywych eliptycznych, protokół Diffiego-Hellmana; - omawia podpisy cyfrowe; - omawia Infrastrukturę Klucza Publicznego; - identyfikuje i opisuje zbiory osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego oraz certyfikatów elektronicznych.

Efekt uczenia się

3. Omawia narzędzia kryptograficzne

Kryteria weryfikacji*

- omawia narzędzia do szyfrowania przechowywanych danych; - omawia narzędzia do szyfrowania przesyłanych danych.

---

Numer zestawu w kwalifikacji*

3

Nazwa zestawu*

Zarządzanie uprawnieniami dostępu

Poziom PRK*

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. Omawia procesy zarządzania uprawnieniami dostępu

Kryteria weryfikacji*

- opisuje pojęcia: identyfikacja, uwierzytelnienie, autoryzacja i rozliczalność; - porównuje modele kontroli dostępu do zasobów informacyjnych; - omawia metody uwierzytelniania i autoryzacji użytkowników do zasobów informacyjnych, w tym uwierzytelnianie jedno i wieloskładnikowe; - omawia metodę jednokrotnego uwierzytelniania do systemów informatycznych.

---

Efekt uczenia się

2. Omawia narzędzia wspomagające kontrolę dostępu

Kryteria weryfikacji*

- porównuje narzędzia wspomagające kontrolę dostępu (hasła, techniki biometryczne i behawioralne, tokeny, karty kryptograficzne); - omawia narzędzia monitorujące pracę użytkowników uprzywilejowanych.

---

Numer zestawu w kwalifikacji*

4

Nazwa zestawu*

Bezpieczeństwo sieci

Poziom PRK*

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. Omawia pojęcia związane z budową i zasadą działania sieci komputerowych

Kryteria weryfikacji*

- rozróżnia zasady działania sieci LAN, MAN, WAN, WLAN, VPN; - opisuje zasady działania urządzeń sieciowych, - charakteryzuje współczesne rozwiązania bezpieczeństwa sieciowego, w tym: zapory sieciowe (ang. Firewall), zapory aplikacyjne (ang. Web Application Firewall), IDS/IPS, UTM, DLP (Data Leakage Protection), SIEM (Security Information and Event Management), DAM (Database Activity monitoring), PAM (Identity Access Management), EPP/EDR, IdM, SA (Security Analytics), MDM (Mobile Device Management).

Efekt uczenia się

2. Omawia protokoły i standardy bezpieczeństwa Internetu

Kryteria weryfikacji*

- charakteryzuje warstwy modelu ISO OSI RM; - omawia zasady działania i bezpieczeństwo protokołów IPv4, IPv6; - wymienia i opisuje protokoły i standardy dotyczące bezpieczeństwa internetowego, w tym: MIME, S/MIME, DKIM, SSL/TLS, HTTPS, Kerberos, X.509, SNMP, DNSSEC; - opisuje zasady działania i bezpieczeństwo sieci bezprzewodowych.

Numer zestawu w kwalifikacji*

5

Nazwa zestawu*

Bezpieczeństwo systemów operacyjnych, baz danych i rozwiązań chmurowych

Poziom PRK*

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 bezpieczeństwo systemów operacyjnych

Kryteria weryfikacji*

- opisuje model bezpieczeństwa systemu Linuks/Unix; - opisuje architekturę zabezpieczeń systemu Windows; - wymienia luki w zabezpieczeniach systemów operacyjnych i aplikacji systemowych; - charakteryzuje pojęcia wirtualizacji i bezpieczeństwa infrastruktury zwirtualizowanej.

Efekt uczenia się

2. Omawia pojęcia związane z bazami danych

Kryteria weryfikacji*

- omawia systemy zarządzania bazami danych; - różnicuje systemy zarządzania bazami danych; - charakteryzuje składniki baz danych; - opisuje techniki, drogi i typy ataków na bazy danych.

Efekt uczenia się

3. Omawia bezpieczeństwo rozwiązań chmurowych

Kryteria weryfikacji*

- zestawia i opisuje modele usług chmurowych (IaaS, PaaS, SaaS); - charakteryzuje rolę wirtualizacji w rozwiązaniach chmurowych; - charakteryzuje modele realizacyjne rozwiązań chmurowych; - analizuje analizuje koncepcje i podejścia do bezpieczeństwa chmur; - opisuje pojęcie Internetu Rzeczy (ang. Internet of Things, IoT).

Numer zestawu w kwalifikacji*

6

Nazwa zestawu*

Bezpieczeństwo oprogramowania

Poziom PRK*

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. Opisuje modele cyklu życia oprogramowania

Kryteria weryfikacji*

- charakteryzuje czynności związane z tworzeniem oprogramowania w tym: wymagań i specyfikacji, projektowania, implementacji, testowania i weryfikacji, konserwacji (pielęgnacji) i ich elementów składowych; - omawia modele cyklu życia oprogramowania w tym praktyczne zasady monitorowania podatności oraz typowe błędy oprogramowania.

Efekt uczenia się

2. Opisuje bezpieczeństwo aplikacji dostępowych

Kryteria weryfikacji*

- omawia zagrożenia dla bezpieczeństwa aplikacji desktopowych, webowych i mobilnych; - charakteryzuje techniki ataków na aplikacje desktopowe, webowe i mobilne; - klasyfikuje techniki ataków; - opisuje sposoby zabezpieczania aplikacji desktopowych, webowych i mobilnych.

Numer zestawu w kwalifikacji*

7

Nazwa zestawu*

Testowanie bezpieczeństwa

Poziom PRK*

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. Opisuje zasady przeprowadzania audytów bezpieczeństwa i monitorowania podatności

Kryteria weryfikacji*

- omawia etapy analizy zabezpieczeń systemu teleinformatycznego oraz testów kontrolnych,

podczas których sprawdzana jest poprawność instalacji oraz konfiguracji systemu; - opisuje zagrożenia dla systemów teleinformatycznych, w tym: ataki sieciowe, zagrożenia transmisji danych, zagrożenia aplikacyjne, zagrożenia komunikacyjne, awarie techniczne, ludzkie błędy, zagrożenia fizyczne, zagrożenia kryptograficzne, przecieki poufnych informacji, ulot elektromagnetyczny; - charakteryzuje metodyki audytu bezpieczeństwa systemów teleinformatycznych; - omawia narzędzia i metody wykrywania podatności w systemach teleinformatycznych.

Efekt uczenia się

2. Omawia testy penetracyjne

Kryteria weryfikacji*

- charakteryzuje rodzaje testów penetracyjnych: test penetracyjny z minimalną wiedzą (black box), test penetracyjny z pełną wiedzą (white box lub crystal box), testy penetracyjne grey box będące kompromisem pomiędzy black box i white box, zawierające elementy obu podejść; - opisuje metodyki testów penetracyjnych, w tym: OSSTMM (Open Source Security Testing Methodology Manual), NIST SP 800-42, NIST SP 800-115, ISAAF, P-PEN; - omawia narzędzia stosowane w realizacji testów penetracyjnych.

Numer zestawu w kwalifikacji*

8

Nazwa zestawu*

Bezpieczeństwo środowiskowe, techniczne i związane z działalnością człowieka

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

10

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 infrastruktury teleinformatycznej

Kryteria weryfikacji*

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

Efekt uczenia się

2. Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej

Kryteria weryfikacji*

- omawia techniki zapobiegania zagrożeniom środowiskowym, technicznym i związanym z działalnością człowieka; - opisuje metody odtwarzania po naruszeniach bezpieczeństwa środowiskowego, technicznego i związanych z działalnością człowieka; - omawia i wybiera metody pozwalające na uzyskanie wysokiego poziomu niezawodności urządzeń i systemów, w tym: rozwiązania redundancyjne, zasilanie awaryjne.

Numer zestawu w kwalifikacji*

9

Nazwa zestawu*

Elementy zarządzania cyberbezpieczeństwem

Poziom PRK*

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. Zarządzanie ryzykiem

Kryteria weryfikacji*

- omawia 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; - wymienia etapy procesu zarządzania ryzykiem.

Efekt uczenia się

3. 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; - uzasadnia potrzebę ustanawiania strategii zarządzania i polityki ciągłości działania w organizacji.

Efekt uczenia się

4. Zarządzanie incydentami bezpieczeństwa

Kryteria weryfikacji*

- opisuje standardy oraz regulacje formalno-prawne związane z zarządzaniem incydentami; - wymienia zasady klasyfikacji i kwalifikacji zdarzeń jako incydentów bezpieczeństwa; - omawia zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji; - charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSiRT).

Numer zestawu w kwalifikacji*

10

Nazwa zestawu*

Informatyka śledcza

Poziom PRK*

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*

- wymienia przykłady najlepszych praktyk informatyki śledczej, w tym SWGDE (ang. The Scientific Working Group on Digital Evidence), SWGIT (ang. The Scientific Working Group on Imaging Technology); - opisuje 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**

Wnioskodawca*

Polskie Towarzystwo Informatyczne

Minister właściwy*

Ministerstwo 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 tożsamych z uzyskaną kwalifikację; - potwierdzenie ustawicznego podnoszenia kompetencji, np. poprzez udział w warsztatach, konferencjach, szkoleniach o tematyce tożsamej z uzyskaną kwalifikacją w wymiarze minimum 200 godzin w okresie ostatnich 5 lat poprzedzających przedłużenie certyfikatu.

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 | Pełnomocnictwo dla Marcin Cabak |
| 2 | Skan dowodu potwierdzającego wniesienie opłaty na rachunek bankowy wskazany na portalu ZSK, zgodnie z art. 17 ust. 1 Ustawy o ZSK |
| 3 | ZRK_FKU_Certyfikowany ekspert cyberbezpieczeństwa (CECB) |
| 4 | ZRK_FKU_Certyfikowany ekspert cyberbezpieczeństwa (CECB) |

☒
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
Reprezentacja: Marcin Cabak - pełnomocnictwo Jacek Pulwarski

Adres elektroniczny osoby wnoszącej wniosek: marcin.cabak@pti.org.pl