# MONITOR POLSKI

## DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 19 lutego 2021 r.

Poz. 201


**OBWIESZCZENIE**
**MINISTRA CYFRYZACJI**[1)]

z dnia 8 lutego 2021 r.

**w sprawie włączenia kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem – specjalista” do Zintegrowanego Systemu Kwalifikacji**

Na podstawie art. 25 ust. 1 i 2 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2020 r. poz. 226) ogłasza się w załączniku do niniejszego obwieszczenia informacje o włączeniu kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem – specjalista” do Zintegrowanego Systemu Kwalifikacji.

Minister Cyfryzacji: wz. *M. Zagórski*

1) Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716).

Załącznik do obwieszczenia Ministra Cyfryzacji
z dnia 8 lutego 2021 r. (poz. 201)

INFORMACJE O WŁĄCZENIU KWALIFIKACJI RYNKOWEJ „ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM – SPECJALISTA”
DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

**1. Nazwa kwalifikacji rynkowej**

| |
|---|
| Zarządzanie cyberbezpieczeństwem – specjalista |

**2. Nazwa dokumentu potwierdzającego nadanie kwalifikacji rynkowej**

| |
|---|
| Certyfikat |

**3. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji rynkowej**

| |
|---|
| Certyfikat jest ważny 3 lata. Przedłużenie następuje na podstawie przedłożenia dokumentów potwierdzających ustawiczne podnoszenie i utrzymywanie kompetencji poprzez np. udział w warsztatach, konferencjach, szkoleniach o tematyce tożsamej z uzyskaną kwalifikacją w wymiarze minimum 120 godzin w okresie ostatnich 3 lat poprzedzających przedłużenie certyfikatu. |

**4. Poziom Polskiej Ramy Kwalifikacji przypisany do kwalifikacji rynkowej (ewentualnie odniesienie do poziomu Sektorowej Ramy Kwalifikacji)**

| |
|---|
| 4 poziom Polskiej Ramy Kwalifikacji |

**5. Efekty uczenia się wymagane dla kwalifikacji rynkowej**

| |
|---|
| **Syntetyczna charakterystyka efektów uczenia się**<br>Osoba z kwalifikacją „Zarządzanie cyberbezpieczeństwem – specjalista” posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi krajowymi i UE z obszaru cyberbezpieczeństwa. Dysponuje wiadomościami w zakresie pracy zespołów w obszarach zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa. Posiada również wiedzę dotyczącą bezpieczeństwa środowiskowego, technicznego i związanego z działalnością człowieka, a także z zakresu informatyki śledczej. |

| **Zestaw 1.** Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa | |
|---|---|
| **Poszczególne efekty uczenia się** | **Kryteria weryfikacji ich osiągnięcia** |
| 01. Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa | – omawia bezpieczeństwo komputerowe;<br>– omawia cele bezpieczeństwa informacji;<br>– charakteryzuje terminologię z obszaru bezpieczeństwa informacji (np. cyberatak, incydent, wirus);<br>– omawia pojęcia: cyberbezpieczeństwo, cyberprzestrzeń i cyberprzestrzeń RP, bezpieczeństwo i ochrona cyberprzestrzeni, bezpieczeństwo sieci i systemów informatycznych;<br>– charakteryzuje zagrożenia teleinformatyczne (np. cyberprzestępczość, haking, haktywizm, haktywizm patriotyczny, cyberterroryzm, cyberszpiegostwo, militarne wykorzystanie cyberprzestrzeni);<br>– rozróżnia zagrożenia, ataki i aktywa;<br>– omawia funkcjonalne wymagania bezpieczeństwa;<br>– klasyfikuje szkodliwe oprogramowanie ze względu na rodzaj i metodę działania. |
| 02. Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa | – omawia krajowe przepisy prawne dotyczące cyberbezpieczeństwa, w tym: kodeks karny w obszarze cyberprzestępczości, ustawę o krajowym systemie cyberbezpieczeństwa, ustawę o działaniach antyterrorystycznych w obszarze cyberbezpieczeństwa, ustawę o usługach zaufania oraz identyfikacji elektronicznej, ustawę o ochronie danych osobowych, przepisy o własności intelektualnej;<br>– omawia opracowania dotyczące cyberbezpieczeństwa RP, w tym: plany, doktryny, koncepcje, wizje, ramy, strategie, programy, uchwały dotyczące ochrony cyberprzestrzeni;<br>– omawia wyniki kontroli organów państwowych w obszarze zarządzania cyberbezpieczeństwem;<br>– omawia analizy i rekomendacje eksperckie i naukowe dotyczące cyberbezpieczeństwa w Polsce i na świecie;<br>– omawia przepisy prawne oraz opracowania Unii Europejskiej dotyczące cyberbezpieczeństwa (np. obowiązujące konwencje, dyrektywy, strategie, rozporządzenia, analizy);<br>– omawia kodeksy etyki i postępowania sformułowane przez ACM, IEEE oraz AITP. |

| **Zestaw 2.** Podstawy zarządzania cyberbezpieczeństwem | |
|---|---|
| **Poszczególne efekty uczenia się** | **Kryteria weryfikacji ich osiągnięcia** |
| 01. Omawia standardy i organizacje standaryzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT | – charakteryzuje standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standaryzacyjne, takie jak NIST, ITU-T, ISO, IEEE, ISACA;<br>– omawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji według rodziny norm ISO/IEC 27000;<br>– 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);<br>– omawia standardy opisujące procesy oceny ryzyka bezpieczeństwa informatycznego, w tym: ISO 13335, ISO 27005, ISO 31000, NIST SP 800-30;<br>– omawia proces przeprowadzania analizy ryzyka. |

| | |
|---|---|
| 02. Obsługa incydentów bezpieczeństwa | – wymienia standardy oraz regulacje formalno-prawne związane z obsługą incydentów bezpieczeństwa;<br>– omawia zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji;<br>– charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSiRT). |

| **Zestaw 3.** Bezpieczeństwo środowiskowe, techniczne i związane z działalnością człowieka | |
|---|---|
| **Poszczególne efekty uczenia się** | **Kryteria weryfikacji ich osiągnięcia** |
| 01. Charakteryzuje zagadnienia dotyczące bezpieczeństwa infrastruktury teleinformatycznej | – identyfikuje zagrożenia środowiskowe;<br>– wskazuje zagrożenia techniczne;<br>– rozróżnia zagrożenia związane z działalnością człowieka. |
| 02. Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej | – omawia techniki zapobiegania zagrożeniom środowiskowym, technicznym i związanym z działalnością człowieka;<br>– omawia metody odtwarzania po naruszeniach bezpieczeństwa środowiskowego, technicznego i związanych z działalnością człowieka. |

| **Zestaw 4.** Elementy informatyki śledczej | |
|---|---|
| **Poszczególne efekty uczenia się** | **Kryteria weryfikacji ich osiągnięcia** |
| 01. Charakteryzuje zasady zabezpieczania dowodów elektronicznych | – charakteryzuje stosowane wytyczne dotyczące aspektów technicznych i najlepszych praktyk informatyki śledczej;<br>– charakteryzuje sposoby prawidłowego zabezpieczania materiału dowodowego na potrzeby dochodzenia wewnętrznego, jak również na potrzeby procesowe;<br>– omawia zasady postępowania z cyfrowymi śladami dowodowymi. |

## 6. 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, 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 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).

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);
– minimum 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.

## 7. Warunki, jakie musi spełniać osoba przystępująca do walidacji

Oświadczenie o niekaralności za przestępstwo popełnione umyślnie ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe

## 8. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat