



# MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

---

Warszawa, dnia 19 lutego 2021 r.

Poz. 201

**OBWIESZCZENIE  
MINISTRA CYFRYZACJI<sup>1)</sup>**

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*

---

<sup>1)</sup> 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**

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.

|   |  |
|---|--|
| <b>Zestaw 1. Postępowanie się wiedzą z obszaru cyberbezpieczeństwa</b>  |  |
| <b>Poszczególne efekty uczenia się</b>  | <b>Kryteria weryfikacji ich osiągnięcia</b>  |
| 01. Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa  | <ul style="list-style-type: none"> <li>– omawia bezpieczeństwo komputerowe;</li> <li>– omawia cele bezpieczeństwa informacji;</li> <li>– charakteryzuje terminologię z obszaru bezpieczeństwa informacji (np. cyberatak, incydent, wirus);</li> <li>– omawia pojęcia: cyberbezpieczeństwo, cyberprzestrzeń i cyberprzestrzeń RP, bezpieczeństwo i ochrona cyberprzestrzeni, bezpieczeństwo sieci i systemów informatycznych;</li> <li>– charakteryzuje zagrożenia teleinformatyczne (np. cyberprzestępczość, haking, haktywizm, haktywizm patriotyczny, cyberterrorizm, cyberspieszostwo, militarne wykorzystanie cyberprzestrzeni);</li> <li>– rozróżnia zagrożenia, ataki i aktywa;</li> <li>– omawia funkcjonalne wymagania bezpieczeństwa;</li> <li>– klasyfikuje szkodliwe oprogramowanie ze względu na rodzaj i metodę działania.</li> </ul>   |
| 02. Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa   | <ul style="list-style-type: none"> <li>– 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;</li> <li>– omawia opracowania dotyczące cyberbezpieczeństwa RP, w tym: plany, doktryny, koncepcje, wizje, ramy, strategie, programy, uchwały dotyczące ochrony cyberprzestrzeni;</li> <li>– omawia wyniki kontroli organów państwowych w obszarze zarządzania cyberbezpieczeństwem;</li> <li>– omawia analizy i rekomendacje eksperckie i naukowe dotyczące cyberbezpieczeństwa w Polsce i na świecie;</li> <li>– omawia przepisy prawne oraz opracowania Unii Europejskiej dotyczące cyberbezpieczeństwa (np. obowiązujące konwencje, dyrektywy, strategie, rozporządzenia, analizy);</li> <li>– omawia kodeksy etyki i postępowania sformułowane przez ACM, IEEE oraz AITP.</li> </ul> |
| <b>Zestaw 2. Podstawy zarządzania cyberbezpieczeństwem</b>  |  |
| <b>Poszczególne efekty uczenia się</b>  | <b>Kryteria weryfikacji ich osiągnięcia</b>  |
| 01. Omawia standardy i organizacje standardyzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT | <ul style="list-style-type: none"> <li>– charakteryzuje standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standaryzacyjne, takie jak NIST, ITU-T, ISO, IEEE, ISACA;</li> <li>– omawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji według rodziny norm ISO/IEC 27000;</li> <li>– identyfikuje i opisuje zbiór najlepszych praktyk zarządzania usługami IT w odniesieniu do cyberbezpieczeństwa zgodnie z kodeksem postępowania dla działań informatyki określanym jako ITIL (ang. Information Technology Infrastructure Library);</li> <li>– omawia standardy opisujące procesy oceny ryzyka bezpieczeństwa informatycznego, w tym: ISO 13335, ISO 27005, ISO 31000, NIST SP 800-30;</li> <li>– omawia proces przeprowadzania analizy ryzyka.</li> </ul>   |

|   |                                       |
|---|---------------------------------------|
| <ul style="list-style-type: none"> <li>- wymienia standardy oraz regulacje formalno-prawne związane z obsługą incydentów bezpieczeństwa;</li> <li>- omawia zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji;</li> <li>- charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSIRT).</li> </ul> | 02. Obsługa incydentów bezpieczeństwa |
|---|---------------------------------------|

|   |   |
|---|---|
| <b>Zestaw 3.</b> Bezpieczeństwo środowiskowe, techniczne i związane z działalnością człowieka |   |
| <b>Poszczególne efekty uczenia się</b>  |   |
| 01. Charakteryzuje zagrożenia dotyczące bezpieczeństwa infrastruktury teleinformatycznej      | <ul style="list-style-type: none"> <li>- identyfikuje zagrożenia środowiskowe;</li> <li>- wskazuje zagrożenia techniczne;</li> <li>- rozróżnia zagrożenia związane z działalnością człowieka.</li> </ul>  |
| 02. Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej                 | <ul style="list-style-type: none"> <li>- omawia techniki zapobiegania zagrożeniom środowiskowym, technicznym i związanym z działalnością człowieka;</li> <li>- omawia metody odtwarzania po naruszeniach bezpieczeństwa środowiskowego, technicznego i związanych z działalnością człowieka.</li> </ul> |

|  |   |
|--|---|
| <b>Zestaw 4.</b> Elementy informatyki śledczej                   |   |
| <b>Poszczególne efekty uczenia się</b>                           |   |
| 01. Charakteryzuje zasady zabezpieczania dowodów elektronicznych | <ul style="list-style-type: none"> <li>- charakteryzuje stosowane wytyczne dotyczące aspektów technicznych i najlepszych praktyk informatyki śledczej;</li> <li>- charakteryzuje sposoby prawidłowego zabezpieczania materiału dowodowego na potrzeby dochodzenia wewnętrznego, jak również na potrzeby procesowe;</li> <li>- omawia zasady postępowania z cyfrowymi śladami dowodowymi.</li> </ul> |

## 6. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację

|                             |  |
|-----------------------------|--|
| <b>1. Etap weryfikacji.</b> | <p>1.1. Metody. Do weryfikacji efektów uczenia się stosuje się wyłącznie test teoretyczny (pisemny) lub analizę dowodów i deklaracji opcjonalnie uzupełnioną wywiadem swobodnym.</p> <p>1.2. Zasoby kadrowe.</p> <p>Komisja walidacyjna musi składać się z co najmniej dwóch członków, w tym przewodniczącego. Przewodniczący komisji musi spełniać następujące warunki:</p> <ul style="list-style-type: none"> <li>- posiada kwalifikację pełną z 7 poziomem PRK (dyplom ukończenia studiów II stopnia);</li> <li>- legitymuje się co najmniej 5-letnim doświadczeniem w przeprowadzaniu egzaminów, osiągnięciem w okresie ostatnich 6 lat;</li> <li>- 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).</li> </ul> |
|-----------------------------|--|

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-video 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 informacyjną 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](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 zachowania), posiadać cechy umożliwiającej jednoznaczny 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 umyślnie przestępstwo skarbowe

## 8. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat