Warszawa, dnia 19 lutego 2021 r.

Poz. 200

OBWIESZCZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 8 lutego 2021 r.

w sprawie włączenia kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem – ekspert” 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 – ekspert” 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. 200)

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

1. Nazwa kwalifikacji rynkowej

Zarządzanie cyberbezpieczeństwem – ekspert

2. Nazwa dokumentu potwierdzającego nadanie kwalifikacji rynkowej

Certyfikat

3. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji rynkowej

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 kwalifikacją; – ustawiczne podnoszenie 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.

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

6 poziom Polskiej Ramy Kwalifikacji

5. Efekty uczenia się wymagane dla kwalifikacji rynkowej

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 kompetencje do 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.

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; – 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.
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; – 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.

Zestaw 2. Kryptografia	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Omawia algorytmy kryptograficzne	– 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.
02. Omawia kryptografię klucza publicznego	– 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.
03. Omawia narzędzia kryptograficzne	– omawia narzędzia do szyfrowania przechowywanych danych; – omawia narzędzia do szyfrowania przesyłanych danych.

Zestaw 3. Zarządzanie uprawnieniami dostępu	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Omawia procesy zarządzania uprawnieniami dostępu	– 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.
02. Omawia narzędzia wspomagające kontrolę dostępu	– porównuje narzędzia wspomagające kontrolę dostępu (hasła, techniki biometryczne i behawioralne, tokeny, karty kryptograficzne); – omawia narzędzia monitorujące pracę użytkowników uprzywilejowanych.

Zestaw 4. Bezpieczeństwo sieci	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Omawia pojęcia związane z budową i zasadą działania sieci komputerowych	– 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).
Omawia protokoły i standardy bezpieczeństwa Internetu	– 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 bezpieczeństwa sieci bezprzewodowych.

Zestaw 5. Bezpieczeństwo systemów operacyjnych, baz danych i rozwiązań chmurowych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Omawia bezpieczeństwo systemów operacyjnych	– opisuje model bezpieczeństwa systemu Linuks/Unix; – opisuje model bezpieczeństwa systemu Windows; – wymienia luki w zabezpieczeniach systemów operacyjnych i aplikacji systemowych; – charakteryzuje pojęcia wirtualizacji i bezpieczeństwa infrastruktury zwirtualizowanej.
02. Omawia pojęcia związane z bazami danych	– omawia systemy zarządzania bazami danych; – różnicuje systemy zarządzania bazami danych; – charakteryzuje składniki baz danych; – opisuje techniki, drogi i typy ataków na bazy danych.
03. Omawia bezpieczeństwo rozwiązań chmurowych	– zestawia i opisuje modele usług chmurowych (IaaS, PaaS, SaaS); – charakteryzuje rolę wirtualizacji w rozwiązaniach chmurowych; – charakteryzuje modele realizacyjne rozwiązań chmurowych; – charakteryzuje koncepcje i podejścia do bezpieczeństwa chmur; – opisuje pojęcie Internetu Rzeczy (ang. Internet of Things, IoT).

Zestaw 6. Bezpieczeństwo oprogramowania	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Opisuje modele cyklu życia oprogramowania	– 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.
02. Opisuje bezpieczeństwo aplikacji dostępowych	– 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.

Zestaw 7. Testowanie bezpieczeństwa	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Opisuje zasady przeprowadzania	– omawia etapy analizy zabezpieczeń systemu teleinformatycznego oraz testów kontrolnych, podczas których sprawdzana jest poprawność instalacji oraz konfiguracji systemu;

audytów bezpieczeństwa i monitorowania podatności	– 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.
Omawia testy penetracyjne	– 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.

Zestaw 8. Bezpieczeństwo środowiskowe, techniczne i związane z działalnością człowieka	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Charakteryzuje zagadnienia dotyczące bezpieczeństwa infrastruktury teleinformatycznej	– charakteryzuje zagrożenia środowiskowe; – charakteryzuje zagrożenia techniczne; – charakteryzuje zagrożenia związane z działalnością człowieka.
02. Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej	– 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.

Zestaw 9. Elementy 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; – 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.

02. Zarządzanie ryzykiem	– 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.
03 Charakteryzuje regulacje formalno-prawne i standardy związane z zarządzaniem ciągłością działania	– 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.
04. Zarządzanie incydentami bezpieczeństwa	– 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).

Zestaw 10. Informatyka śledcza	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Charakteryzuje zagadnienia dotyczące norm, standardów i dobrych praktyk informatyki śledczej	– 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.
02. Charakteryzuje zasady zabezpieczania i metody analizy dowodów elektronicznych	– 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.

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);
– 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.

7. 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.

8. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat