MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 7 grudnia 2023 r.

Poz. 1353

OBWIESZCZENIE MINISTRA CYFRYZACJI[1)]

z dnia 27 października 2023 r.

w sprawie włączenia kwalifikacji rynkowej „Przetwarzanie danych cyfrowych w środowisku zawodowym z wykorzystaniem technologii informacyjno-komunikacyjnych” 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 oraz z 2023 r. poz. 2005) ogłasza się w załączniku do niniejszego obwieszczenia informacje o włączeniu kwalifikacji rynkowej „Przetwarzanie danych cyfrowych w środowisku zawodowym z wykorzystaniem technologii informacyjno-komunikacyjnych” do Zintegrowanego Systemu Kwalifikacji.

Minister Cyfryzacji: *J. Cieszyński*

1) Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 792).

Załącznik do obwieszczenia Ministra Cyfryzacji
z dnia 27 października 2023 r. (M.P. poz. 1353)

INFORMACJE O WŁĄCZENIU KWALIFIKACJI RYNKOWEJ „PRZETWARZANIE DANYCH CYFROWYCH W ŚRODOWISKU ZAWODOWYM Z WYKORZYSTANIEM TECHNOLOGII INFORMACYJNO-KOMUNIKACYJNYCH” DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

1. Nazwa kwalifikacji rynkowej

Przetwarzanie danych cyfrowych w środowisku zawodowym z wykorzystaniem technologii informacyjno-komunikacyjnych

2. Nazwa dokumentu potwierdzającego nadanie kwalifikacji rynkowej

Certyfikat

3. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji rynkowej i warunki przedłużenia jego ważności

5 lat. Po upływie 5 lat ponowne przystąpienie do walidacji.

4. Poziom Polskiej Ramy Kwalifikacji przypisany do kwalifikacji rynkowej

4 poziom Polskiej Ramy Kwalifikacji

5. Efekty uczenia się wymagane dla kwalifikacji rynkowej

Syntetyczna charakterystyka efektów uczenia się

Osoba, która posiada kwalifikację rynkową, potrafi wyszukiwać niezbędne w trakcie pracy zawodowej informacje z wykorzystaniem filtrów i botów wyszukiwarek, odróżniając przy tym informacje prawdziwe od tzw. fake newsów oraz rozpoznając zjawiska agresji w Internecie. W tworzonych i edytowanych plikach tekstowych oraz arkuszach kalkulacyjnych korzysta z wielu różnych narzędzi i filtrów poprawiających ich czytelność i wygląd, a także zwiększających produktywność. Potrafi również nagrywać pulpit oraz umieszczać nagrania na platformach streamingowych. Rozpoznaje najpopularniejsze formaty kompresji plików, potrafi samodzielnie znaleźć, pobrać i zainstalować sterowniki i aplikacje firm trzecich według potrzeb, rozróżnia nośniki wielokrotnego i jednokrotnego zapisu, a także łączy się z zewnętrznymi zasobami sieciowymi w firmie (mapuje dyski do NAS). Podczas komunikacji z innymi uczestnikami wykorzystuje bezpieczne, szyfrowane kanały informacji, przesyłając posiadane pliki również w formie spakowanych i zabezpieczonych archiwów danych. Osoba posiadająca kwalifikację rynkową korzysta z mechanizmów zabezpieczających w postaci 2FA, wskazuje dobre praktyki cyberbezpieczeństwa, rozumie potrzebę używania kopii bezpieczeństwa, omawia i przeciwdziała zagrożeniom bezpieczeństwa oraz potrafi usuwać większość prostych problemów z oprogramowaniem i sprzętem komputerowym. W przypadku poważniejszych problemów łączy się za pomocą narzędzi zdalnych (pulpit zdalny) ze wsparciem technicznym.

Zestaw 1. Przetwarzanie danych cyfrowych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Charakteryzuje systemy operacyjne	– omawia zagadnienia związane z zarządzaniem danymi zlokalizowanymi na lokalnych lub zewnętrznych nośnikach danych (np. hierarchiczny schemat organizacji dysków, folderów i plików, poziomy dostępu do zasobów komputera, sortowanie, grupowanie, filtrowanie danych, zmiana układu folderów, modyfikacja opcji folderów, formatowanie, defragmentacja, zerowanie nośników), – wskazuje najpopularniejsze formaty kompresji plików (np. *.zip, *.rar, *.7z), – omawia otoczenie sieciowe, funkcję mapowania dysków sieciowych lub zewnętrzne urządzenia do przechowywania plików (np. NAS, DAS), – rozróżnia nośniki wielokrotnego zapisu od nośników jednorazowego zapisu (np. CD-R, DVD-R, DVD-RW), – opisuje procedurę instalacji sterowników (np. weryfikacja modelu, pobranie najnowszej wersji, instalacja).

Administruje systemami operacyjnymi	– przetwarza archiwa plików z wykorzystaniem aplikacji firm trzecich, zabezpieczając je hasłami (np. winzip, winrar, 7-zip, unarchiver), – sprawdza listę zainstalowanych w systemie czcionek systemowych, – tworzy skrót do lokalizacji sieciowej.
Przetwarza pliki tekstowe w formie offline i online	– tworzy pliki tekstowe (przechowywane lokalnie lub na zewnętrznym nośniku, np. dysku sieciowym), – charakteryzuje typy kodowania plików (UTF-8, Windows-1256), – edytuje pliki tekstowe (np. tworzy korespondencję seryjną, dodaje znak wodny, ustawia niestandardowe marginesy, tworzy zautomatyzowany spis treści, sprawdza pisownię i gramatykę w dokumencie tekstowym).
Przetwarza arkusze kalkulacyjne w formie offline i online	– tworzy arkusze kalkulacyjne (przechowywane lokalnie lub na zewnętrznym zasobie, np. dysku sieciowym), – edytuje arkusze kalkulacyjne (np. wstawia tabele przestawne, korzysta z funkcji „szukaj i zamień" w trybie zaawansowanym, blokuje przewijanie wierszy i kolumn, dostosowuje szerokość wierszy i wysokość kolumn), – korzysta z funkcji arytmetyczno-logicznych, których konstruktor składa się z kilku zmiennych.
Przetwarza multimedialne treści cyfrowe	– charakteryzuje stosowane narzędzia do publikacji materiałów audiowizualnych (np. Twitch, YouTube) lub formaty plików multimedialnych (np. *.mp4, *.wav, *.flac, *.aac, *.tiff, *.heic), – nagrywa pulpit z wykorzystaniem wbudowanych mechanizmów systemowych, – umieszcza na platformie streamingowej krótki materiał wideo (dostęp prywatny).
Omawia prawo autorskie i licencje	– wskazuje najważniejsze zasady autorskich praw majątkowych w kontekście zasobów cyfrowych, – omawia założenie licencji Creative Commons.

Zestaw 2. Bezpieczna wymiana informacji	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Charakteryzuje funkcje narzędzi do komunikacji indywidualnej lub grupowej	– omawia filtry wyszukiwania z wykorzystaniem operatorów (np. AND, OR, FILETYPE, SITE), – identyfikuje rodzaje komunikatorów z wbudowanym szyfrowaniem danych, wskazując różnice pomiędzy komunikacją szyfrowaną i nieszyfrowaną, – omawia elementy przeglądarek (np. rolę wtyczek i dodatków, menedżery haseł, tryb incognito), – porównuje narzędzia do wideokonferencji (np. Zoom, Skype, Teams), – omawia pojęcie danych telemetrycznych i cel ich gromadzenia przez usługodawców, – identyfikuje spam, spim i inne formy niechcianych wiadomości.
Przetwarza dane z użyciem narzędzi cyfrowych	– wyszukuje treści cyfrowe z wykorzystaniem operatorów wyszukiwania (np. AND, OR, FILETYPE, SITE), – używa narzędzi do szyfrowania załączników wysyłanych pocztą e-mail lub komunikatorem (np. za pomocą aplikacji 7-zip, funkcji nadawania haseł w dokumentach Office), – współdzieli pliki zabezpieczone hasłem zapisane na dyskach internetowych z wykorzystaniem dodatkowych opcji (np. Google Drive, One Drive, iCloud), – modyfikuje dane przeglądarki (np. zapisuje stronę www do pliku za pomocą funkcji zapisz stronę w przeglądarce, usuwa dane przeglądarki, tj. cache, hasła, historię przeglądania, ciasteczka), – wykorzystuje funkcje poczty e-mail (np. przekierowania poczty, automatycznej odpowiedzi zwrotnej, wymuszenia potwierdzenia odczytania wiadomości, grup dyskusyjnych, tożsamości, oznaczania niechcianych wiadomość i przenoszenie ich do SPAMu).

Charakteryzuje zasady cyberbezpieczeństwa	– identyfikuje metody bezpiecznego logowania (np. 2FA z wykorzystaniem smsa, aplikacji autentyfikujących, fizycznych kluczy kryptograficznych), – omawia potencjalne źródła zagrożeń dla cyberbezpieczeństwa (np. strony ze złośliwym oprogramowaniem, zainfekowane załączniki w wiadomości e-mail, brak aktualizacji dla systemu operacyjnego, luki sprzętowe), – wskazuje rozwiązania poprawiające cyberbezpieczeństwo (np. wykorzystanie silnych haseł, korzystanie z komunikacji szyfrowanej, nieklikanie w linki od nieznanych odbiorców, zasady tworzenia i przechowywania kopii bezpieczeństwa wraz z ich wersjonowaniem, stosowanie i wykorzystanie mechanizmu CAPTCHA, itp.), – omawia socjotechniczne formy zagrożeń dla użytkowników Internetu (np. patostreamy, agresja w Internecie, phising, stalking, fake newsy) i omawia przykłady przeciwdziałania im.
Stosuje narzędzia zapewniające cyberbezpieczeństwo	– wykorzystuje narzędzia firm trzecich do wykonania kopii zapasowej (np. EaseUS Todo Backup Free, Paragon Backup & Recovery, Bvckup 2), – weryfikuje certyfikat bezpieczeństwa strony www (np. SSL 3.1, TLS 1.0), – przeprowadza skanowanie pliku za pomocą narzędzi offline lub online pod kątem zidentyfikowania zagrożeń, – weryfikuje, czy wskazany adres e-mail został upubliczniony w ramach wykrytego wycieku danych.

Zestaw 3. Metody rozwiązań problemów technicznych dotyczących komputerów klasy PC	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Opisuje sposoby rozwiązywania problemów technicznych	– charakteryzuje narzędzia do podłączania pulpitu zdalnego (np. Team Viewer) zarówno w kontekście uzyskania wsparcia technicznego, jak i jego świadczenia współpracownikom, – identyfikuje problemy ze sprzętem lub oprogramowaniem (np. problem ze sterownikiem weryfikowalny z poziomu menedżera urządzeń, artefakty obrazu, zawieszona aplikacja, krytyczne błędy systemu), – omawia procedurę usuwania lub przywracania danych (np. formatowania nośników danych, tworzenia, przywracania kopii zapasowej systemu).
Diagnozuje problemy techniczne	– sprawdza informacje o systemie lub stanie funkcjonowania sieci LAN, korzystając z wbudowanych narzędzi (np. Menedżera urządzeń, MSINFO, funkcji PING) lub z wykorzystaniem linii komend, – weryfikuje zainstalowane sterowniki i w razie potrzeby aktualizuje je do najnowszej wersji; – wyszukuje rozwiązania zdiagnozowanych problemów technicznych.

6. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację

1. Etap weryfikacji

1.1. Metody

Możliwe do stosowania metody walidacji to:

– obserwacja w warunkach symulowanych,

– obserwacja w warunkach rzeczywistych,

– wywiad swobodny,

– test teoretyczny.

Weryfikacja efektów uczenia się składa się z części praktycznej (np. obserwacji w warunkach symulowanych lub rzeczywistych, wywiadu swobodnego) oraz części teoretycznej (np. pisemnego testu teoretycznego) zgodnych z efektami uczenia się dla kwalifikacji.

1.2. Zasoby kadrowe

Komisja walidacyjna składa się minimum z 2 osób spełniających następujące warunki:

asesor – ukończone studia kierunkowe na kierunku informatyka lub pokrewnym (akceptowane są również uprawnienia trenera szkoleń z zakresu technologii informacyjno-komunikacyjnych (ICT), kursy/szkolenia z zakresu TIK i/lub równoważne szkolenia specjalistyczne (np. z cyberbezpieczeństwa, OSINTu, CCNA od poziomu 4 wzwyż)) posiadający minimum 2 lata doświadczenia w nauczaniu osób dorosłych

oraz

przewodniczący komisji walidacyjnej z decydującym głosem w sprawie wyniku walidacji (podejmuje decyzję o wyniku walidacji po weryfikacji dokumentacji przeprowadzonej walidacji przez asesora) – ukończone studia kierunkowe na kierunku informatyka lub pokrewnym, minimum 5 lat doświadczenia w uczeniu osób dorosłych oraz minimum 3 lata doświadczenia w przeprowadzaniu walidacji i/lub tworzeniu testów.

1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne

Czas trwania walidacji jest określony przez instytucję certyfikującą i jest dostosowany do liczby zadań praktycznych i teoretycznych przeznaczonych do walidacji.

Walidacja odbywa się stacjonarnie albo zdalnie pod nadzorem asesora zgodnie z wytycznymi instytucji certyfikującej, gdzie minimum wytycznych określono poniżej.

Instytucja certyfikująca zapewnia udogodnienia dla osób z niepełnosprawnościami i posiada wytyczne ich zastosowania. Udogodnienia są dostosowane do rodzaju niepełnosprawności kandydata. Instytucja certyfikująca przeprowadzająca walidację zapewnia lokal o odpowiednich warunkach do przeprowadzenia walidacji, z uwzględnieniem potrzeb osób z niepełnosprawnościami (w przypadku walidowania takich osób). Bezwzględnie powinny być spełnione warunki związane z zapewnieniem samodzielności pracy zdającego. W sali podczas trwania walidacji mogą znajdować się wyłącznie osoby autoryzowane.

Instytucja certyfikująca odpowiada za poprawność identyfikacji zdającego (weryfikacja tożsamości na podstawie dokumentu tożsamości ze zdjęciem).

2. Etap identyfikowania i dokumentowania efektów uczenia się

Instytucja certyfikująca może zapewniać wsparcie dla kandydatów prowadzone przez doradcę walidacyjnego w zakresie identyfikowania posiadanych efektów uczenia się. Korzystanie z tego wsparcia nie jest obowiązkowe.

2.1. Metody

Etap identyfikowania i dokumentowania może być realizowany w oparciu o dowolne metody służące zidentyfikowaniu posiadanych efektów uczenia się.

2.2. Zasoby kadrowe

Doradca walidacyjny.

Funkcję doradcy walidacyjnego może pełnić osoba, która posiada:

– doświadczenie w weryfikowaniu efektów uczenia się lub ocenie kompetencji,

– umiejętność stosowania metod i narzędzi wykorzystywanych przy identyfikowaniu i dokumentowaniu kompetencji,

– wiedzę dotyczącą kwalifikacji dotyczących posługiwania umiejętnościami ICT.

2.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne etapu identyfikowania i dokumentowania

Instytucja certyfikująca, która zdecyduje się na wsparcie osób w procesie identyfikowania i dokumentowania, zapewnia warunki umożliwiające im indywidualną rozmowę z doradcą walidacyjnym.

7. Warunki, jakie musi spełniać osoba przystępująca do walidacji

Nie dotyczy

8. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat