Warszawa, 24.03.2020

30.03.2020

08.04.2020

14.04.2020

23.04.2020

Opisywanie kwalifikacji rynkowej – formularz

Opis kwalifikacji rynkowej (nazwa kwalifikacji)
Zarządzanie bezpieczeństwem informacji cyfrowej w lotnictwie.

Materiał roboczy opracowany przy wsparciu Instytutu Badań Edukacyjnych w ramach projektu systemowego „Wspieranie realizacji II etapu wdrażania Zintegrowanego Systemu Kwalifikacji na poziomie administracji centralnej oraz instytucji nadających kwalifikacje i zapewniających jakość nadawania kwalifikacji" współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach programu Operacyjnego Wiedza, Edukacja, Rozwój, Priorytet II: Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji, Działanie 2.13 Przejrzysty i spójny Krajowy System Kwalifikacji. Zadanie 2: Wspieranie podmiotów zainteresowanych włączeniem do ZSK kwalifikacji nadawanych poza systemami oświaty i szkolnictwa wyższego, w tym kwalifikacji rynkowych..

Typ wniosku
Wniosek o włączenie kwalifikacji do ZSK
Nazwa kwalifikacji (300 znaków) *Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. a). Pełna nazwa kwalifikacji, która ma być widoczna w ZRK i być umieszczana na dokumencie potwierdzającym jej uzyskanie.* *Nazwa kwalifikacji (na ile to możliwe) powinna:* – *jednoznacznie identyfikować kwalifikację,* – *różnić się od nazw innych kwalifikacji,* – *różnić się od nazwy zawodu, stanowiska pracy lub tytułu zawodowego, uprawnienia,* – *być możliwie krótka,* – *nie zawierać skrótów,* – *być oparta na rzeczowniku odczasownikowym, np. „gromadzenie", „przechowywanie", „szycie".*

Zarządzanie bezpieczeństwem informacji cyfrowej w lotnictwie.

Skrót nazwy (150 znaków)

Pole nieobowiązkowe.

Certyfikowany menedżer cyberbezpieczeństwa informacji lotniczych (CMCBIL)

Rodzaj kwalifikacji

Wskazanie, czy kwalifikacja jest: kwalifikacją pełną, czy kwalifikacją cząstkową.

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji

Pole obowiązkowe (art. 15 ust. 1 pkt 4). Proponowany poziom Polskiej Ramy Kwalifikacji.

6 poziom Polskiej Ramy Kwalifikacji

Krótka charakterystyka kwalifikacji oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji (4000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. d). Wybrane informacje o kwalifikacji skierowane do osób zainteresowanych uzyskaniem kwalifikacji oraz do pracodawców, które pozwolą im szybko ocenić, czy dana kwalifikacja jest właśnie tą, której poszukują.

Krótka charakterystyka może odpowiadać na pytanie: „Jakie działania lub zadania jest w stanie podejmować osoba posiadająca daną kwalifikację?".

Osoba z kwalifikacją potrafi realizować zadania stojące przed podmiotem z branży lotniczej w zakresie realizacji celów cyberbezpieczeństwa oraz wymagań odpowiednich norm prawnych, w tym ustawy o krajowym systemie cyberbezpieczeństwa. Osoba taka potrafi zarządzać bezpieczeństwem informacji w lotnictwie oraz zna sposoby pozyskiwania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty, zgodnie z definicjami wyżej wymienionej ustawy. Do wykonywania zadań wykorzystuje znajomość integracji systemów wymiany danych lotniczych, również w skali międzynarodowej. Dysponuje wiedzą na temat regulacji formalno-prawnych, standardów, procedur i dobrych praktyk związanych z zarządzaniem incydentami w lotnictwie. Dokonuje analizy bezpieczeństwa przetwarzania i wymiany informacji lotniczych. Przygotowuje plan ciągłości działania.

Osoba posiadająca kwalifikację może znaleźć zatrudnienie m.in. u operatorów usług kluczowych, w tym zwłaszcza w zakresie transportu lotniczego, w organach administracji publicznej, zwłaszcza PAŻP, ULC oraz w podmiotach, w których konieczne jest utrzymanie wysokiego poziomu bezpieczeństwa w procesach przetwarzania i wymiany informacji lotniczych.

Orientacyjny koszt uzyskania kwalifikacji na jedną osobą wynosi 1800 zł.

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. c). Przeciętna liczba godzin, które trzeba poświęcić na osiągnięcie efektów uczenia się wymaganych dla danej kwalifikacji oraz na ich walidację (1 godzina =

60 minut).

W pierwszej kolejności warto ustalić orientacyjny nakład pracy dla poszczególnych zestawów efektów uczenia się. orientacyjny nakład pracy dla kwalifikacji odpowiada sumie nakładu pracy potrzebnego do uzyskania wyodrębnionych w niej zestawów efektów uczenia się.

320 godzin

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji (2000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. f). Informacja na temat grup osób, które mogą być szczególnie zainteresowane uzyskaniem danej kwalifikacji, np. osoby zarządzające nieruchomościami, specjaliści z zakresu telekomunikacji, kobiety powracające na rynek pracy.

Uzyskaniem kwalifikacji mogą być zainteresowani:

- specjaliści z branży IT którzy chcą poszerzyć swoje kompetencje w kierunku cyberbezpieczeństwa;
- absolwenci kierunków związanych z cyberbezpieczeństwem, informatyką, bezpieczeństwem narodowym, bezpieczeństwem wewnętrznym, lotnictwem, inżynierią bezpieczeństwa, kryptologią;
- analitycy bezpieczeństwa;
- pracownicy przedsiębiorstw i organizacji lotniczych w szczególności:pracownicy służb technicznych, operacyjnych oraz administracyjnych;
- osoby zatrudnione u operatorów usług kluczowych w zakresie zarządzania bezpieczeństwem lub obszarem IT lub branży lotniczej.

Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 01.09.2019 r.)

x Kwalifikacja może być przydatna dla uczniów szkół branżowych lub techników kształcących się w określonych zawodach

Rozporządzenie MEN z dnia 16 maja 2019 r.

W szkole prowadzącej kształcenie zawodowe kształcenie odbywa się w oparciu o podstawy programowe określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego (Dz. U. poz. 991).

Część godzin zajęć może zostać przeznaczona na realizację obowiązkowych zajęć edukacyjnych przygotowujących uczniów do uzyskania kwalifikacji rynkowej funkcjonującej w ZSK, związanej z nauczanym zawodem (§ 4 ust 5 pkt 2 rozporządzenia Ministra Edukacji Narodowej z dnia 3 kwietnia 2019 r. w sprawie ramowych planów nauczania dla publicznych szkół (Dz. U. poz. 639)).

Należy wskazać zawody (zgodnie z klasyfikacją zawodów szkolnictwa branżowego określoną w załączniku nr 2 do rozporządzenia Ministra Edukacji Narodowej z dnia 15 lutego 2019 r. w sprawie ogólnych celów i zadań kształcenia w zawodach szkolnictwa branżowego oraz klasyfikacji zawodów szkolnictwa branżowego (Dz. U. poz. 316)), w przypadku których zasadne jest przygotowywanie uczniów do uzyskania kwalifikacji rynkowej objętej wnioskiem.

Wskazanie zawodów szkolnictwa zawodowego, z którymi związana jest kwalifikacja

Jeżeli w punkcie 7a wskazano przydatność kwalifikacji, to z rozwijanej listy branż i zawodów należy wybrać te zawody, z którymi związana jest wnioskowana kwalifikacja

TECHNIK LOTNISKOWYCH SŁUŻB OPERACYJNYCH 315406

Wymagane kwalifikacje poprzedzające (2000 znaków)

Pole nieobowiązkowe. Kwalifikacje pełne i cząstkowe, które musi posiadać osoba ubiegająca się o kwalifikację, by przystąpić do procesu weryfikacji osiągnięcia efektów uczenia się wymaganych dla kwalifikacji.

kwalifikacja pełna z IV poziomem PRK

W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji (2000 znaków)

Pole obowiązkowe (art. 15 ust.1 pkt 2) lit. g). Określenie (w razie potrzeby) warunków, które musi spełniać osoba, aby przystąpić do walidacji i móc uzyskać kwalifikację (np. wymagany poziom wykształcenia).

Podczas określania tych warunków warto mieć na uwadze, że nie są one tożsame z warunkami zatrudnienia (np. ważnymi badaniami lekarskimi). Doświadczenie zawodowe powinno być wskazywane jako warunek jedynie w uzasadnionych przypadkach – kompetencje wynikające z praktyki zawodowej powinny być odzwierciedlone przede wszystkim w efektach uczenia się wymaganych dla kwalifikacji.

Wskazane warunki przystąpienia do walidacji powinny być możliwe do zweryfikowania.

- kwalifikacja pełna z IV poziomem PRK;
- udokumentowane 3-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa, obszarze IT lub audytach związanych z bezpieczeństwem informacji (w tym ISO 27001) w ciągu ostatnich 6 lat lub posiadanie jednego z certyfikatów branżowych m.in. Security+, CISSP, SICA, CISM, CPTE, OSCP, Audytor Wiodący ISO 27001;
-

Zapotrzebowanie na kwalifikację (10000 znaków)

Pole obowiązkowe (art. 15 ust.1 pkt 2) lit. i). Wykazanie, że kwalifikacja odpowiada na aktualne oraz przewidywane potrzeby społeczne i gospodarcze (regionalne, krajowe, europejskie).

Możliwe jest odwołanie się do opinii organizacji gospodarczych, trendów na rynku pracy, prognoz dotyczących rozwoju technologii, a także strategii rozwoju kraju lub regionu.

Zgodnie z *Krajowymi Ramami Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, przyjętymi uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r., zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych stanowi aktualnie warunek konieczny dla możliwości realizacji funkcji państwa i umożliwia na pełne wykorzystanie gospodarki cyfrowej. Osiągnięcie tego celu możliwe będzie poprzez osiągnięcie zdolności służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizowaniu skutków incydentów, które naruszają bezpieczeństwo systemów teleinformatycznych, wzmocnienie

zdolności do przeciwdziałania cyberzagrożeniom, a także zwiększania potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.

Wraz z rozwojem oraz zwiększającym się wykorzystaniem technologii informacyjno-komunikacyjnych w różnych dziedzinach wzrasta również liczba zagrożeń w cyberprzestrzeni oraz poziom ich złożoności. Zagrożenia powyższe mogą prowadzić nie tylko do znacznych strat biznesowych, ale także stać się przyczyną utraty ciągłości działania usług kluczowych, dlatego też właściwe przygotowanie systemów przetwarzania informacji lotniczych na odparcie ewentualnych ataków może zagwarantować bezpieczeństwo. Jak wynika z badań firmy SITA, zajmującej się dostarczaniem m.in. systemów teleinformatycznych dla branży lotniczej, aż 95 proc. linii lotniczych i 96 proc. lotnisk uważa cyberbezpieczeństwo za jeden z priorytetów inwestycyjnych w najbliższych trzech latach. (https://www.pasazer.com/news/36607/cyberbezpieczenstwo,coraz,wazniejsze,w,lotnictwie.html). Zapotrzebowanie na kwalifikacje wynika więc z aktualnego zagrożenia infrastruktury krytycznej ze strony ataków cybernetycznych.

Zarówno podmioty świadczące usługi kluczowe, jak również podmioty świadczące usługi na ich rzecz zobligowani zostali do posiadania wykwalifikowanego personelu, który zapewni wypełnienie obowiązków narzuconych przez przepisy prawa powszechnie obowiązującego. Obowiązki te wynikają przede wszystkim z Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii [Dz.Urz. UE L 194/1, 19.7.2016] oraz implementującej jej Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [Dz.U. z 2018 r., poz. 1560 z późn. zm.] wraz z towarzyszącymi jej rozporządzeniami, w szczególności: rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu [Dz.U. z 2018 r., poz. 1999], rozporządzeniem Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych [Dz.U. z 2018 r., poz. 1806], rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo [Dz.U. z 2019 r., poz. 2479]. Do podmiotów świadczących usługi kluczowe z zakresu transportu lotniczego zaliczeni zostali przewoźnicy lotniczy, zarządzający lotniskami, przedsiębiorcy wykonujący wybrane usługi dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług kluczowych oraz przedsiębiorcy wykonujący dla przewoźników lotniczych zadania związane z kontrolą bezpieczeństwa. Wymagania określone w przepisach wskazanych powyżej dotyczą podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo na rzecz podmiotów świadczących usługi kluczowe w zakresie transportu lotniczego. Ponadto konieczność zapewnienia cyberbezpieczeństwa informacjom lotniczym wynika z przepisów dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Tekst mający znaczenie dla EOG) (*Dz.U. L 345 z 23.12.2008)*; ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2019 r., poz.

1398 z późn. zm.) oraz rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. z 2010 r. Nr 83, poz. 542). Mowa tu o konieczności zapewnienia bezpieczeństwa systemom infrastruktury krytycznej, czyli systemom oraz wchodzącym w ich skład powiązanym ze sobą funkcjonalnie obiektom, w tym obiektom budowlanym, urządzeniom, instalacjom, usługom kluczowym dla bezpieczeństwa państwa i jego obywateli oraz służącym zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucjom i przedsiębiorcom, w tym europejskiej infrastruktury krytycznej. W przypadku terenów obsługi lotniczej ważne w tym przypadku są zarówno systemy transportowe, jak też systemy sieci teleinformatycznych.

Kwalifikacja pozwoli zapewnić specjalistyczne kadry dla podmiotów z branży lotniczej do realizowania zadań z obszaru cyberbezpieczeństwa podmiotów, w tym realizację zadań wynikających z uwarunkowań prawnych (ustawy i rozporządzenia z zakresu cyberbezpieczeństwa oraz zarządzania kryzysowego)

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się (3000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2 lit. k). Wyjaśnienie, czym kwalifikacja różni się od wybranych kwalifikacji o zbliżonym charakterze. Punktem odniesienia powinny być kwalifikacje funkcjonujące w ZSK. Ponadto wskazanie kwalifikacji wpisanych do ZRK, które zawierają co najmniej jeden taki sam zestaw efektów.

TECHNIK LOTNISKOWYCH SŁUŻB OPERACYJNYCH 315406 KWALIFIKACJA WYODRĘBNIONA W ZAWODZIE TLO.02. Obsługa operacyjna portu lotniczego i współpraca ze służbami żeglugi powietrznej

Powyższa kwalifikacja posiada niektóre efekty kształcenia, które są zbliżone i mogą być przydatne w celu uzyskania kwalifikacji.

Umiejętności w zakresie - Obsługa operacyjna portu lotniczego i współpraca ze służbami żeglugi powietrznej posiada następujące zbliżone efekty:

TLO.02.2. Podstawy działania lotniskowych służb operacyjnych

efekt nr 6 - stosuje programy komputerowe wspomagające wykonywanie zadań zawodowych

TLO.02.3. Organizacja działań związanych z funkcjonowaniem portu lotniczego

efekt nr 10 - charakteryzuje rodzaje informacji dotyczących działań operacyjnych związanych z funkcjonowaniem portów lotniczych

efekt nr 11 - charakteryzuje rodzaje zagrożeń związanych z obsługą portów lotniczych

TLO.02.4. Prowadzenie działań związanych z obsługą operacyjną w porcie lotniczym

efekt nr 1 - posługuje się lotniskową dokumentacją operacyjną, mapami lotniczymi i planami lotnisk

efekt nr 4 - stosuje procedury operacyjne obowiązujące w portach lotniczych

efekt nr 5 - korzysta z systemów informacji stosowanych w lotnictwie

efekt nr 17 - wykorzystuje technologie informatyczne podczas eksploatacji portów lotniczych

Inne kwalifikacje o zbliżonym charakterze:

- kierunki kształcenia na uczelniach wyższych związane z kryptologią i cyberbezpieczeństwem - brak szczegółowych odniesień do cyberbezpieczeństwa specyficznego rodzaju informacji, jakimi są informacje lotnicze;
- kierunki kształcenia na uczelniach wyższych związane z lotnictwem i organizacją lotniczych procesów transportowych;
- procedowane przez Ministerstwo Cyfryzacji kwalifikacje: "Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych", "Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle", "Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych" - odnoszą się do obszaru cyberbezpieczeństwa, jednak w odniesieniu do przemysłu. Koncentrują się więc na zagadnieniach bezpieczeństwa w zakresie przemysłu procesowego w środowiskach systemów sterowania przemysłowego;
- procedowane przez Ministerstwo Cyfryzacji kwalifikacje: "Zarządzanie cyberbezpieczeństwem - specjalista", "Zarządzanie cyberbezpieczeństwem - ekspert", "Zarządzanie cyberbezpieczeństwem - menedżer" - zawierają efekty kształcenia o zbliżonym charakterze, jednak odnoszą się do zagadnień ogólnych z zakresu cyberbezpieczeństwa, jednak o różnym poziomie szczegółowości.

Proponowana kwalifikacja, w odróżnieniu od wyżej wskazanych, uszczegóławia zagadnienia, jakim są cyberbezpieczeństwo przetwarzania i wymiany informacji lotniczych.

Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)

X Kwalifikacja zawiera wspólne lub zbliżone zestawy efektów kształcenia z „dodatkowymi umiejętnościami zawodowymi" w zakresie wybranych zawodów szkolnictwa branżowego

Dodatkowe umiejętności zawodowe

Należy wybrać z listy „dodatkowe umiejętności zawodowe" (określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego, załącznik Nr 33) zawierające wspólne lub zbliżone zestawy efektów kształcenia z zestawami efektów uczenia się określonymi w kwalifikacji rynkowej.

Wskazanie „dodatkowych umiejętności zawodowych" w zakresie wybranych zawodów szkolnictwa branżowego zawierających wspólne lub zbliżone zestawy efektów kształcenia

(Branża – Zawód – Umiejętność)

Jeżeli w punkcie 11a udzielono pozytywnej odpowiedzi, to z rozwijanej listy branż, zawodów i dodatkowych umiejętności zawodowych należy wybrać te umiejętności, które zawierają wspólne lub

zbliżone zestawy efektów kształcenia z wnioskowaną kwalifikacją

BRANŻA TELEINFORMATYCZNA (INF) Bezpieczeństwo sieci komputerowych - technik informatyk, technik szerokopasmowej komunikacji elektronicznej

Wymienione zawody posiadają niektóre efekty kształcenia, które są zbliżone i mogą być przydatne w kwalifikacji.

Umiejętności w zakresie - *Bezpieczeństwo sieci komputerowych* posiadają następujące zbliżone efekty:

1) Charakteryzuje pojęcia związane z bezpieczeństwem sieci lokalnych.

2)Rozpoznaje przestępstwa w lokalnych sieciach komputerowych i systemach komputerowych.

3) Rozpoznaje rodzaje ataków sieciowych.

Typowe możliwości wykorzystania kwalifikacji (4000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. j). Omówienie perspektyw zatrudnienia i dalszego uczenia się, najistotniejszych z punktu widzenia rozwoju osobistego i zawodowego osób zainteresowanych uzyskaniem kwalifikacji.

Możliwe jest wskazanie przykładowych stanowisk pracy, na które będzie mogła aplikować osoba posiadająca daną kwalifikację.

Osoba posiadająca kwalifikację może znaleźć zatrudnienie m.in. u operatorów usług kluczowych, w tym zwłaszcza w zakresie transportu lotniczego, w organach administracji publicznej, zwłaszcza PAŻP, ULC oraz w podmiotach, w których konieczne jest utrzymanie wysokiego poziomu bezpieczeństwa w procesach przetwarzania i wymiany informacji lotniczych. Kwalifikacja może być wykorzystana w operacyjnych centrach bezpieczeństwa - SOC (Security Operations Center), których utworzenie jest obowiązkiem operatorów usług kluczowych oraz wynika z dobrych praktyk rynkowych. Niniejsza kwalifikacja może być wykorzystana w podmiotach świadczących usługi lotnicze oraz usługi cyberbezpieczeństwa w lotnictwie lub audyty w podmiotach branży lotniczej.

Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację (10000 znaków)

Pole obowiązkowe (art. 15 ust.1 pkt 2) lit. h). Określenie wymagań stanowiących podstawę do przeprowadzania walidacji w różnych instytucjach. Wymagania powinny dotyczyć:

- *metod stosowanych w walidacji – służących weryfikacji efektów uczenia się wymaganych dla kwalifikacji, ale także (o ile to potrzebne) identyfikowaniu i dokumentowaniu efektów uczenia się;*
- *osób projektujących i przeprowadzających walidację;*
- *sposobu prowadzenia walidacji oraz warunków organizacyjnych i materialnych, niezbędnych do prawidłowego prowadzenia walidacji.*

Wymagania dotyczące walidacji mogą być wskazane dla pojedynczych zestawów efektów uczenia się lub dla całej kwalifikacji.

Wymagania mogą być uzupełnione o dodatkowe wskazówki dla instytucji oraz osób projektujących i przeprowadzających walidację, a także dla osób ubiegających się o uzyskanie kwalifikacji.

1. Etap weryfikacji.

1.1. Metody

Do weryfikacji efektów uczenia się stosuje się: test teoretyczny, studium przypadku, rozmowę z komisją, analizę dowodów i deklaracji.

Weryfikacja prowadzona jest za pomocą testu teoretycznego oraz studium przypadku. Możliwe jest zastosowanie wywiadu swobodnego lub analizy dowodów i deklaracji jako uzupełnienie powyższych metod.

1.2. Zasoby kadrowe:

Komisja walidacyjna musi składać się z co najmniej trzech członków, w tym przewodniczącego.

Przewodniczący komisji walidacyjnej musi spełniać następujące warunki:

- posiada kwalifikację pełną z VII poziomem PRK (dyplom ukończenia studiów II stopnia na kierunkach technicznych);

- legitymuje się co najmniej 3-letnim doświadczeniem w przeprowadzaniu egzaminów,

- 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).

Pozostali członkowie komisji walidacyjnej muszą spełniać następujące warunki:

- posiada kwalifikację pełną z VI PRK (dyplom ukończenia studiów I stopnia na kierunkach technicznych);

- legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze technologii cyfrowej.

Ponadto, co najmniej jeden z członków komisji musi posiadać udokumentowane minimum 5-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa, przetwarzania i wymiany informacji lotniczych.

1.3. Warunki organizacyjne i materialne

Instytucja certyfikująca musi zapewnić:

- salę z wyposażeniem multimedialnym i możliwością rejestracji audio-wideo przebiegu walidacji;

- stanowiska egzaminacyjne wyposażone w komputer z dostępem do internetu umożliwiające samodzielną pracę każdej osobie przystępującej do walidacji lub platformę tele-edukacyjną do zdalnego przeprowadzenia walidacji.

2. Etapy identyfikowania i dokumentowania.

Nie określa się warunków identyfikowania i dokumentowania.

Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy) (1000 znaków)

Jeśli ustanowiono w danym sektorze lub branży Sektorową Ramę Kwalifikacji, to wypełnienie tego pola jest obowiązkowe (art. 15 ust. 1 pkt 4). Podaj propozycję odniesienia do poziomu odpowiednich Sektorowych Ram Kwalifikacji, jeśli są one włączone do ZSK.

nie dotyczy

Syntetyczna charakterystyka efektów uczenia się (2000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1) lit. a). Zwięzła, ogólna charakterystyka wiedzy, umiejętności i kompetencji społecznych poprzez określenie działań, do których podjęcia będzie przygotowana osoba posiadająca daną kwalifikację.

Syntetyczna charakterystyka efektów uczenia się powinna nawiązywać do charakterystyki odpowiedniego poziomu PRK, w szczególności odpowiadać na pytania o przygotowanie osoby posiadającej kwalifikację do samodzielnego działania w warunkach mniej lub bardziej przewidywalnych, wykonywania działania o różnym poziomie złożoności, podejmowania określonych ról w grupie, ponoszenia odpowiedzialności za jakość i skutki działań (własnych lub kierowanego zespołu).

Osoba z kwalifikacją potrafi realizować zadania stojące przed podmiotem z branży lotniczej w zakresie realizacji celów cyberbezpieczeństwa oraz wymagań odpowiednich norm prawnych, w tym ustawy o krajowym systemie cyberbezpieczeństwa. Osoba taka potrafi zarządzać bezpieczeństwem informacji w lotnictwie oraz zna sposoby pozyskiwania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty. Do wykonywania zadań wykorzystuje znajomość integracji systemów wymiany danych lotniczych, również w skali międzynarodowej. Dysponuje wiedzą na temat regulacji formalno-prawnych, standardów, procedur i dobrych praktyk związanych z zarządzaniem incydentami w lotnictwie. Dokonuje analizy bezpieczeństwa przetwarzania i wymiany informacji lotniczych. Przygotowuje plan ciągłości działania. Osoba posiadająca kwalifikację jest gotowa do samodzielnego wykonywania zadań w zmieniających się, nieprzewidzianych warunkach.

Wyodrębnione zestawy efektów uczenia się

Wykaz zestawów efektów uczenia się wymaganych dla kwalifikacji, zawierający: numer porządkowy (1, 2, …), nazwy zestawów, orientacyjne odniesienie każdego zestawu do poziomu PRK oraz orientacyjny nakład pracy potrzebny do osiągnięcia efektów uczenia w każdym zestawie.

Nazwa zestawu powinna:

- *nawiązywać do efektów uczenia się wchodzących w skład danego zestawu lub odpowiadać specyfice wchodzących w jego skład efektów uczenia się,*
- *być możliwie krótka,*

- *nie zawierać skrótów,*

gdy jest to możliwe, być oparta na rzeczowniku odczasownikowym, np. „gromadzenie", „przechowywanie", „szycie".

1. Podstawy cyberbezpieczeństwa w lotnictwie (120 h, 6 PRK)
2. Zarządzanie cyberbezpieczeństwem w lotnictwie (200 h, 6 PRK)

Poszczególne efekty uczenia się w zestawach

Zestaw efektów uczenia się to wyodrębniona część efektów uczenia się wymaganych dla danej kwalifikacji. Poszczególne efekty uczenia się powinny być wzajemnie ze sobą powiązane, uzupełniające się oraz przedstawione w sposób uporządkowany (np. od prostych do bardziej złożonych).

Poszczególne efekty uczenia się są opisywane za pomocą: umiejętności (tj. zdolności wykonywania zadań i rozwiązywania problemów) oraz kryteriów weryfikacji, które doprecyzowują ich zakres oraz określają niezbędną wiedzę i kompetencje społeczne.

Poszczególne efekty uczenia się powinny być:

- *jednoznaczne – niebudzące wątpliwości, pozwalające na zaplanowanie i przeprowadzenie walidacji, których wyniki będą porównywalne, oraz dające możliwość odniesienia do poziomu PRK,*
- *realne – możliwe do osiągnięcia przez osoby, dla których dana kwalifikacja jest przewidziana,*
- *możliwe do zweryfikowania podczas walidacji,*
- *zrozumiałe dla osób potencjalnie zainteresowanych kwalifikacją.*

Podczas opisywania poszczególnych efektów uczenia się korzystne jest stosowanie czasowników operacyjnych (np. „rozróżnia", „uzasadnia", „montuje").

Zestaw efektów uczenia się:	01. Podstawy cyberbezpieczeństwa w lotnictwie
Umiejętności	**Kryteria weryfikacji**
1.1. Charakteryzuje sposoby pozyskiwania informacji o zagrożeniach cyberbezpieczeństwa oraz podatnościach systemów	- omawia źródła pozyskiwania informacji o zagrożeniach dla bezpieczeństwa informacji lotniczych; - omawia źródła pozyskania informacji o podatnościach systemów przetwarzania informacji stosowanych w branży lotniczej.

przetwarzania informacji	
1.2. Charakteryzuje proces reagowania na incydenty bezpieczeństwa komputerowego	- nazywa i omawia kategorie incydentów bezpieczeństwa komputerowego; - wyjaśnia pojęcia np. incydent krytyczny, poważny, istotny; - wymienia etapy procesu zarządzania incydentami bezpieczeństwa komputerowego; - omawia zadania zespołów reagowania na incydenty bezpieczeństwa komputerowego; - omawia czynności wykonywane w czasie poszczególnych etapów reagowania na incydenty bezpieczeństwa komputerowego; - odróżnia incydenty cyberbezpieczeństwa niemające wpływu na bezpieczeństwo ruchu lotniczego od incydentów mających wpływ na bezpieczeństwo ruchu lotniczego; - omawia proces zarządzania aspektami cyberbezpieczeństwa mającymi wpływ na bezpieczeczeństwo ruchu lotniczego.
1.3. Charakteryzuje mechanizmy zapewniające poufność, integralność, dostępność i autentyczność informacji lotniczych.	- omawia czynniki warunkujące poufność, integralność, dostępność i autentyczność informacji lotniczych; - charakteryzuje różnice pomiędzy zasadami poufności, integralności, dostępności i autentyczności informacji; - charakteryzuje źródła informacji lotniczych.
1.4. Omawia zasady i potrzeby aktualizacji oprogramowania.	- omawia zasady związane z aktualizacją oprogramowania; - omawia sposoby i rozwiązania techniczne zapewniające aktualizację oprogramowania.
1.5.	- opisuje różnice pomiędzy szyfrowaniem informacji (poufność) a podpisywaniem informacji (niezaprzeczalność);

Charakteryzuje technologie bezpiecznej komunikacji	- opisuje wymagania dotyczące bezpiecznego przesyłania informacji oraz dostępnych algorytmów szyfrowania; - opisuje elementy i zasady funkcjonowania infrastruktury klucza publicznego.
1.6. Charakteryzuje wymagania bezpieczeństwa w lotnictwie	- charakteryzuje Safety Management System (SMS); - omawia wymagania bezpieczeństwa w lotnictwie według odpowiedniego aneksu ICAO (International Civil Aviation Organization).
1.7. Charakteryzuje procesy przetwarzania danych lotniczych i architektury systemów wykorzystywanych w lotnictwie	- wymienia obszary przetwarzania danych lotniczych; - charakteryzuje podmioty zaangażowane w procesy wymiany i przetwarzania danych lotniczych; - wymienia klasy systemów informatycznych wykorzystywanych w lotnictwie; - wymienia technologie i systemy telekomunikacji wykorzystywane w lotnictwie; - omawia proces przepływu danych w kontekście określonego obszaru przetwarzania danych lotniczych.
1.8. Charakteryzuje zagadnienia integracji systemów wymiany danych lotniczych lokalnie i w skali międzynarodowej	- omawia sieci m.in. Aeronautical Fixed Telecommunication Network (AFTN), Société Internationale de Télécommunications Aéronautiques (SITA), Pan-European Network Service (PENS); - omawia procesy integracji systemów informacyjnych wymieniających i przetwarzających dane lotnicze lokalnie i w skali międzynarodowej; - omawia obszary danych podlegających integracji lokalnie i w skali międzynarodowej; - omawia koncepcję System Wide Information Management (SWIM).
1.9. Omawia zagadnienia integracji systemów zarządzania ruchem Bezzałogowych Statków Powietrznych (BSP) z systemami Air Traffic	- charakteryzuje systemy klasy Unmanned Traffic Management (UTM); - omawia zagadnienia związane z wymianą danych lotniczych w zakresie ruchu BSP; - omawia obszary wymiany danych między systemami.

Management	
1.10. Charakteryzuje zagadnienia związane z ryzykiem w lotnictwie	- rozróżnia pojęcia prawdopodobieństwa, wpływu (skutku) oraz istotności ryzyka; - omawia metody szacowania ryzyka np. Failure Mode and Effects Analysis (FMEA); - omawia wpływ incydentów bezpieczeństwa informatycznego na zagrożenia w lotnictwie.
Zestaw efektów uczenia się:	02. Zarządzanie cyberbezpieczeństwem w lotnictwie
Umiejętności	**Kryteria weryfikacji**
2.1. Dokonuje analizy bezpieczeństwa informacji lotniczych	- szacuje ryzyko w określonym obszarze; - wskazuje sposoby mitygacji ryzyka; - identyfikuje newralgiczne strefy/obszary zagrożeń dla bezpieczeństwa informacji lotniczych; - identyfikuje zagrożenia bezpieczeństwa informacji lotniczych; - wykonuje analizę bezpieczeństwa zgodną z wymaganiami Safety Management System (SMS); - tworzy dokumentację procesów zarządzania bezpieczeństwem informacji lotniczych (np. dokumentację procedur).
2.2. Przygotowuje plan ciągłości działania dla usług kluczowych w lotnictwie	- identyfikuje usługi kluczowe u określonego dostawcy usług; - identyfikuje elementy strategii bezpieczeństwa zapewnienia ciągłości działania; - określa politykę bezpieczeństwa w zakresie zarządzania informacjami lotniczymi określonego podmiotu; - projektuje architekturę infrastruktury zapewnienia ciągłości usług kluczowych; - tworzy procedury “contingency”.
2.3. Kieruje procesem zarządzania bezpieczeństwem informacji	- podaje przykłady dobrych praktyk w zarządzaniu bezpieczeństwem informacji; - określa kryteria doboru członków zespołu zarządzania bezpieczeństwem informacji w kontekście określonego podmiotu; - przypisuje obszary odpowiedzialności poszczególnym członkom zespołu.
2.4. Zarządza podatnościami w bezpieczeństw	- identyfikuje podatności; - określa ryzyko dla zidentyfikowanej podatności; - wskazuje sposoby postępowania z podatnością; - wymienia instytucje i podmioty mogące okazać wsparcie przy usuwaniu podatności lub zagrożeń.

ie informacji.	

Wnioskodawca

Pole obowiązkowe (art. 83 ust. 1 pkt 7).Z listy rozwijanej w formularzu w ZRK należy wybrać podmiot wnioskodawcy.

Minister właściwy

Pole obowiązkowe (art. 16 ust. 1). Należy wskazać odpowiedniego ministra, który zdaniem wnioskodawcy jest właściwy do rozpatrzenia wniosku i po włączeniu kwalifikacji do ZSK powinien odpowiadać za kwalifikację.

Minister Cyfryzacji

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności (2000 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. b). W przypadku kwalifikacji nadawanej na czas określony wskaż, po jakim czasie konieczne jest odnowienie ważności kwalifikacji oraz określ warunki, jakie muszą być spełnione, aby ważność dokumentu została przedłużona.

Certyfikat jest ważny 5 lat. W celu odnowienia ważności certyfikatu potwierdzającego kwalifikację ”Cyberbezpieczeństwo przetwarzania i wymiany informacji lotniczych” należy

1. Dostarczyć aktualne zaświadczenie o niekaralności za przestępstwa popełnione umyślnie, ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe.
2. Uczestniczyć co najmniej dwa razy w roku w seminariach, konferencjach lub szkoleniach branżowych w obszarze zagadnień obejmowanych przez niniejszą kwalifikację.
3. Zaliczyć egzamin (przedłużający lub wznawiający) w zakresie następujących efektów uczenia się:
    - sposobów pozyskiwania informacji o zagrożeniach cyberbezpieczeństwa oraz podatnościach systemów przetwarzania informacji (1.1)
    - nowych technologii bezpieczeństwa w komunikacji (1.5)
    - zarządzanie ryzykiem i procedur bezpieczeństwa w lotnictwie (1.10, 2.1)
    - integracja systemów zarządzania w lotnictwie (1.9)

Nazwa dokumentu potwierdzającego nadanie kwalifikacji

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. b). Np. dyplom, świadectwo, certyfikat, zaświadczenie.

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji (2500 znaków)

Pole obowiązkowe (art. 15 ust. 1 pkt 2) lit. e). Podaj, o jakie uprawnienia może się ubiegać osoba po uzyskaniu kwalifikacji. Jeśli z uzyskaniem kwalifikacji nie wiąże się uzyskanie uprawnień, należy

wpisać "Nie dotyczy".
brak
Kod dziedziny kształcenia *Pole obowiązkowe (art. 15 ust. 1 pkt. 7). Kod dziedziny kształcenia, o którym mowa w przepisach wydanych na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2012 r. poz. 591, z późn. zm.).*
481 informatyka
Kod PKD *Pole obowiązkowe (art. 15 ust. 1 pkt 7). Kod Polskiej Klasyfikacji Działalności (PKD).*
51 Transport lotniczy