IT Leader Club Polska

Brak ocen dla tego dostawcy

Certyfikat Specjalista Cyberbezpieczeństwa CSCB

Numer usługi 2024/04/19/160892/2129162

zdalna
Egzamin
2 h
24.04.2024 do 19.04.2026

984,00 PLN brutto
800,00 PLN netto
492,00 PLN brutto/h
400,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Uzyskaniem kwalifikacji mogą być zainteresowani: • Specjaliści z branży IT oraz cyberbezpieczeństwa chcący potwierdzić swoje umiejętności. • Osoby pracujące w sektorze ochrony informacji. • Studenci i absolwenci kierunków technicznych poszukujący potwierdzenia swoich kwalifikacji. Osoby posiadające kwalifikację mogą podjąć zatrudnienie m.in. w: • Jednostkach administracji państwowej i samorządu terytorialnego. • Operatorach usług kluczowych i specjalnych. • Firmach wymagających utrzymania wysokiego poziomu bezpieczeństwa informacji.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1000
Data zakończenia rekrutacji	31-12-2024
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	2

Cel

Cel edukacyjny

Osoba z kwalifikacją "Zarządzanie cyberbezpieczeństwem - specjalista" posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Klasyfikuje szkodliwe oprogramowanie. Posługuje się regulacjami formalno-prawnymi

krajowymi i UE z obszaru cyberbezpieczeństwa. Dysponuje wiedzą w zakresie pracy w zespole w obszarach zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa	omawia bezpieczeństwo komputerowe omawia cele bezpieczeństwa informacji	Analiza dowodów i deklaracji
Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa	omawia krajowe przepisy prawne dotyczące cyberbezpieczeństwa, w tym: kodeks karny w obszarze cyberprzestępczości, ustawa o krajowym systemie cyberbezpieczeństwa, ustawa o działaniach antyterrorystycznych w obszarze cyberbezpieczeństwa, ustawa o usługach zaufania oraz identyfikacji elektronicznej, ustawa 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	Analiza dowodów i deklaracji
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	Analiza dowodów i deklaracji
Obsługa incydentów bezpieczeństwa	wymienia standardy oraz regulacje formalno-prawne związane z obsługą 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)	Analiza dowodów i deklaracji
Charakteryzuje zagadnienia dotyczące bezpieczeństwa infrastruktury teleinformatycznej	identyfikuje zagrożenia środowiskowe wskazuje zagrożenia techniczne rozróżnia zagrożenia związane z działalnością człowieka	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej	omawia techniki zapobiegania zagrożeniom środowiskowym, technicznym i związanym z działalnością człowieka omawia metody odtwarzania po naruszeniach bezpieczeństwa środowiskowego, technicznego i związanych z działalnością człowieka	Analiza dowodów i deklaracji
Charakteryzuje zasady zabezpieczania dowodów elektronicznych	charakteryzuje stosowane wytyczne dotyczące aspektów technicznych i najlepszych praktyk informatyki śledczej charakteryzuje sposoby prawidłowego zabezpieczania materiału dowodowego na potrzeby dochodzenia wewnętrznego, jak również na potrzeby procesowe omawia zasady postępowania z cyfrowymi śladami dowodowymi	Analiza dowodów i deklaracji

Kwalifikacje

Kwalifikacje zarejestrowane w Zintegrowanym Systemie Kwalifikacji

Kwalifikacje	Zarządzanie cyberbezpieczeństwem - specjalista
Kod kwalifikacji w Zintegrowanym Systemie Kwalifikacji	13869
Nazwa/Kategoria Podmiotu certyfikującego	Fundacja IT Leader Club Polska - Instytucja Certyfikująca decyzją Ministra Cyfryzacji nr 2/2023 z dnia 17.02.2023
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/ sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

Certyfikacja Cyberbezpieczeństwa Fundacji IT Leader Club Polska uzyskała listy referencyjne z Dell Technologies, KPRM, Palo Alto Networks, Wydziału Zarządzania Politechniki Warszawskiej, Straży Granicznej, KGP oraz Google Cloud Poland

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa/Kategoria Podmiotu certyfikującego	Fundacja IT Leader Club Polska
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Program

Państwowy Certyfikat Kwalifikacji Wolnorynkowej „**Zarządzanie cyberbezpieczeństwem – specjalista**” (wzór ozdobny, wersja drukowana) pn. **Certyfikowany Specjalista Cyberbezpieczeństwa CSCB** to prestiżowe wyróżnienie przyznawane przez naszą fundację w postaci urzędowego certyfikatu elektronicznego z unikalnym kodem QR. Dokument sygnowany jest przez Zintegrowany Rejestr Kwalifikacji (ZRK) w ramach Zintegrowanego Systemu Kwalifikacji (ZSK). Aby go otrzymać, kandydaci muszą wykazać się osiągnięciem kompetencji w czterech głównych obszarach:

- **1. Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa**
  - Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa
  - Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa
- **2. Podstawy zarządzania cyberbezpieczeństwem**
  - Omawia standardy i organizacje standaryzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT
  - Obsługa incydentów bezpieczeństwa
- **3. Bezpieczeństwo środowiskowe, techniczne i związane z działalnością człowieka**
  - Charakteryzuje zagadnienia dotyczące bezpieczeństwa infrastruktury teleinformatycznej
  - Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej
- **4. Elementy informatyki śledczej**
  - Charakteryzuje zasady zabezpieczania dowodów elektronicznych

Każdy certyfikat posiada **unikalny kod QR** (wzór urzędowy, wersja elektroniczna i drukowana) umożliwiający szybką i łatwą weryfikację autentyczności nabytych kwalifikacji. Weryfikacja ta jest przeprowadzana niezależnie przez Instytut Badań Edukacyjnych, podległy Ministerstwu Edukacji Narodowej, co gwarantuje obiektywność i wiarygodność certyfikatu.

Zaliczenie wymogów certyfikatu CSCB umożliwia otrzymanie dodatkowego certyfikatu Certified Cybersecurity Professional: Specialist (CCPS) sygnowanego przez Akademię Zarządzania IT Administracji Publicznej oraz AACSB.

Znaczenie międzynarodowe i Europejska Rama Kwalifikacji (ERK)

Certyfikat jest zintegrowany z Polskimi Ramami Kwalifikacji (PRK) na poziomie 4, co oznacza, że odpowiada zaawansowanym umiejętnościom wymagającym wiedzy teoretycznej i praktycznej na poziomie średnio zaawansowanym. ZSK współgra z Europejską Ramą Kwalifikacji (ERK), ułatwiając porównywanie kwalifikacji między różnymi systemami edukacyjnymi w Unii Europejskiej.

Podstawy prawne

Podstawa prawna włączenia kwalifikacji do ZSK: Obwieszczenie Ministra Cyfryzacji z dnia 8 lutego 2021 r., które włącza kwalifikację „Zarządzanie cyberbezpieczeństwem – specjalista” do **Zintegrowanego Systemu Kwalifikacji**, opublikowane w Monitorze Polskim.

Podstawa prawna uprawnienia do certyfikowania kwalifikacji: Decyzja administracyjna Ministra Cyfryzacji z dnia 17 lutego 2023 r., uprawniająca Fundację IT Leader Club Polska do certyfikowania kwalifikacji, wydana w oparciu o Ustawę o Zintegrowanym Systemie Kwalifikacji.

Proces walidacji i certyfikacji

Proces weryfikacji zgłoszenia jest prosty i przejrzysty. Kandydaci zainteresowani uzyskaniem certyfikatu muszą wypełnić formularz zgłoszeniowy dostępny na naszej stronie internetowej, uiścić opłatę walidacyjną a po pozytywnej walidacji uiścić opłatę certyfikacyjną.

Utrzymanie i odnawianie certyfikatu

Certyfikat jest ważny przez 3 lata. Aby przedłużyć jego ważność, należy przedstawić dowody na ciągłe doskonalenie zawodowe, takie jak udział w szkoleniach czy konferencjach, sumujące się do co najmniej 120 godzin w ciągu ostatnich 3 lat oraz uiścić opłatę administracyjną. Zgłoszenie chęci przedłużenia certyfikatu wysyłamy na adres: przedluzenie@cscb.edu.pl

Koszt walidacji i certyfikacji, zasady (procedura walidacyjna)

Koszt walidacji wynosi 200 zł z VAT a koszt certyfikacji (wydanie certyfikatu) to koszt 784 zł z VAT. Do tej kwoty mogą być dołożone kolejne opłaty (jako opcja, tylko dla chętnych) które są zawarte w treści Formularza Zgłoszeniowego.

Procedura walidacyjna / kroki walidacyjne:

1. **Wysłanie Formularza Zgłoszeniowego przez Kandydatki / Kandydatów. Uruchomienie procesu walidacji który trwa ok. 14 dni.**
2. System zgłoszeniowy wysyła maila z wytycznymi realizacji procesu walidacji (możemy na tym etapie poprosić o wsparcie Doradcy Walidacyjnego). W ramach tego kroku prosimy również o przesłanie: CV, scanów (zdjęć) dyplomu szkół, certyfikatów, suplementów na specjalny adres podany w treści maila po wysłaniu zgłoszenia jak w pkt.1. Jest to ważny element prawidłowej realizacji walidacji. Brak ww. kopii dokumentów do 7 dni od wysłania zgłoszenia zatrzymuje i kończy proces walidacji.
3. **Na tym etapie trzeba uiścić opłatę walidacyjną (rejestracyjną) w kwocie 200 zł na konto Fundacji wg wytycznych zapisanych w treści maila po wysłaniu zgłoszenia. Na opłatę oczekujemy max. 7 dni. Brak wpłaty zatrzymuje i kończy proces walidacji.**
4. Po otrzymaniu wpłaty walidacyjnej, Komisja Walidacyjna w przeciągu 14 dni od daty zgłoszania podejmuje decyzje o przyznaniu bądź nie Certyfikatu CSCB. W przypadku braków kompetencyjnych może być wymagane zaliczenie niezależnego testu kompetencyjnego on-line oferowanwgo przez Fundację (IC - Instytucji Certyfikującej) bądź ukończenia niezależnego od IC szkolenia wyrównujcego wiedzę wg wymogów tego certyfikatu.
5. Po pozytywnym spełnieniu wszystkich wymagań (posiadania wymaganej wiedzy i kompetencji), Komisja Walidacyjna wzywa do uregulowania pozostałych kwot jako ostatniego elementu procesu walidacji. Po uregulowania wszystkich płatności Komisja przyznaje Certyfikat CSCB na 3 lata wg zamówienia z Formularza Zgłoszeniowego. W przypadku braku uregulowania wymganych kwot w przeciągu 7 dni od wezwania do zapłaty, proces walidacji zostaje zatrzymany i zamknięty bez wydania Certyfikatu.
6. Dokumentacja dowodowa z przeprowadzonej walidacji przechowywana jest przez 5 lat od daty wydania Certyfikatu.

Skład Komisji Walidacyjnej Instytucji Certyfikującej CSCB

- Bogusław Bujak, PhD, LL.D., CISA, CIA, ISO 27001 LA - Szef Komisji Walidacyjnej, Walidator / Egzaminator
- Arkadiusz Lefanowicz, DBA, MBA, LL.M, MSc, ISO 27001 IA - z-ca Szefa Komisji Walidacyjnej, Walidator / Egzaminator

Kontakt

Wszelkie pytania i zgłoszenia prosimy kierować na adres e-mail: **kontakt@cscb.edu.pl** lub do doradcy walidacyjnego: **doradcawalidacyjny@cscb.edu.pl**

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	984,00 PLN
Koszt przypadający na 1 uczestnika netto	800,00 PLN
Koszt osobogodziny brutto	492,00 PLN
Koszt osobogodziny netto	400,00 PLN
W tym koszt certyfikowania brutto	200,00 PLN

W tym koszt certyfikowania netto	162,60 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Po rejestracji uczestnik otrzyma przewodnik certyfikacji CSCB

Warunki uczestnictwa

Warunkiem uczestnictwa jest popełnienie formularza zgłoszeniowego: https://cscb.syskonf.pl/rejestracja

Warunki techniczne

Aby móc przystąpić do certyfikacji potrzeba posiadać komputer podłączony do sieci internet z przeglądarką internetową

Kontakt

Arkadiusz Lefanowicz

E-mail arkadiusz.lefanowicz@itleader.org.pl
Telefon (+48) 506 955 942