Możliwość dofinansowania

EDU SERVICE

Edu Service
Zdzisław Sikora

4,9 / 5

420 ocen

Zarządzanie cyberbezpieczeństwem - specjalista - szkolenie kończące się egzaminem

Numer usługi 2026/05/04/139923/3536179

5 600,00 PLN brutto
5 600,00 PLN netto
155,56 PLN brutto/h
155,56 PLN netto/h
261,33 PLN cena rynkowa

Rzeszów
Usługa szkoleniowa
stacjonarna
36:00 h
27.08.2026 do 03.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Uzyskaniem kwalifikacji mogą być zainteresowani:** • osoby posiadające wiedzę, umiejętności i kompetencje wskazane w efektach uczenia się, chcące formalnie je potwierdzić. • specjaliści komórek organizacyjnych odpowiedzialni w organizacjach za ochronę informacji i cyberbezpieczeństwo oraz kształtowanie polityki bezpieczeństwa; • specjaliści IT z minimalnym doświadczeniem; • uczniowie i absolwenci szkół branżowych; • studenci i absolwenci kierunków z obszaru IT. **Osoby posiadające kwalifikację mogą podjąć zatrudnienie m.in.:** • w naczelnych, centralnych i terenowych organach administracji państwowej (w tym jednostkach samorządu terytorialnego); • u operatorów usług kluczowych (UOK); • w służbach mundurowych i specjalnych; • w przedsiębiorstwach i organizacjach, w których konieczne jest utrzymywanie właściwego poziomu bezpieczeństwa informacji, przetwarzanej za pomocą systemów teleinformatycznych.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	26-08-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	36

Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

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. Posiada również wiedzę dotyczącą bezpieczeństwa środowiskowego, technicznego i z zakresu informatyki śledczej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa	a)omawia bezpieczeństwo komputerowe	Test teoretyczny
	b)omawia cele bezpieczeństwa informacji	Test teoretyczny
	c)charakteryzuje terminologię z obszaru bezpieczeństwa informacji (np. cyberatak, incydent, wirus)	Test teoretyczny
	d)omawia pojęcia: cyberbezpieczeństwo, cyberprzestrzeń i cyberprzestrzeń RP, bezpieczeństwo i ochrona cyberprzestrzeni, bezpieczeństwo sieci i systemów informatycznych	Test teoretyczny
	e)charakteryzuje zagrożenia teleinformatyczne (np. cyberprzestępczość, haking, haktywizm, haktywizm patriotyczny, cyberterroryzm, cyberszpiegostwo, militarne wykorzystanie cyberprzestrzeni)	Test teoretyczny
	f)rozróżnia zagrożenia, ataki i aktywa	Test teoretyczny
	g)omawia funkcjonalne wymagania bezpieczeństwa	Test teoretyczny
	h)klasyfikuje szkodliwe oprogramowanie ze względu na rodzaj i metodę działania	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
2. Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa	a)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	Test teoretyczny
	b)omawia opracowania dotyczące cyberbezpieczeństwa RP, w tym: plany, doktryny, koncepcje, wizje, ramy, strategie, programy, uchwały dotyczące ochrony cyberprzestrzeni	Test teoretyczny
	c)omawia wyniki kontroli organów państwowych w obszarze zarządzania cyberbezpieczeństwem	Test teoretyczny
	d)omawia analizy i rekomendacje eksperckie i naukowe dotyczące cyberbezpieczeństwa w Polsce i na świecie	Test teoretyczny
	e)omawia przepisy prawne oraz opracowania Unii Europejskiej dotyczące cyberbezpieczeństwa (np. obowiązujące konwencje, dyrektywy, strategie, rozporządzenia, analizy)	Test teoretyczny
	f)omawia kodeksy etyki i postępowania sformułowane przez ACM, IEEE oraz AITP	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
3. Omawia standardy i organizacje standaryzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT	a)charakteryzuje standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standaryzacyjne, takie jak NIST, ITU-T, ISO, IEEE, ISACA	Test teoretyczny
	b)omawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji według rodziny norm ISO/IEC 27000	Test teoretyczny
	c)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)	Test teoretyczny
	d)omawia standardy opisujące procesy oceny ryzyka bezpieczeństwa informatycznego, w tym: ISO 13335, ISO 27005, ISO 31000, NIST SP 800-30	Test teoretyczny
	e)omawia proces przeprowadzania analizy ryzyka	Test teoretyczny
4. Obsługa incydentów bezpieczeństwa	a)wymienia standardy oraz regulacje formalno-prawne związane z obsługą incydentów bezpieczeństwa	Test teoretyczny
	b)omawia zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji	Test teoretyczny
	c)charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSiRT)	Test teoretyczny
5. Charakteryzuje zagadnienia dotyczące bezpieczeństwa infrastruktury teleinformatycznej	a)identyfikuje zagrożenia środowiskowe	Test teoretyczny
	b)wskazuje zagrożenia techniczne	Test teoretyczny
	c)rozróżnia zagrożenia związane z działalnością człowieka	Test teoretyczny

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

Kwalifikacje

Kwalifikacje włączone do Zintegrowanego Systemu Kwalifikacji

Kwalifikacje	Zarządzanie cyberbezpieczeństwem - specjalista
Kod kwalifikacji zarejestrowanej w ZRK	13869
Nazwa Podmiotu prowadzącego walidację	Polskie Towarzystwo Informatyczne
Nazwa Podmiotu certyfikującego	Polskie Towarzystwo Informatyczne

Program

PROGRAM:

1. Wprowadzenie do cyberbezpieczeństwa – pojęcia, cele bezpieczeństwa informacji oraz klasyfikacja zagrożeń i podatności
2. Regulacje prawne cyberbezpieczeństwa w Polsce i UE oraz zasady etyki zawodowej w obszarze IT
3. Standardy zarządzania bezpieczeństwem informacji oraz wymagania norm ISO/IEC 27001 i dobrych praktyk ITIL
4. Identyfikacja aktywów, zagrożeń i podatności oraz przeprowadzanie analizy i oceny ryzyka bezpieczeństwa informacji
5. Zarządzanie incydentami bezpieczeństwa informacji oraz organizacja i funkcjonowanie zespołów reagowania CERT/CSIRT

6. Identyfikacja zagrożeń dla infrastruktury teleinformatycznej: środowiskowych, technicznych oraz wynikających z działalności człowieka
7. Dobór i stosowanie zabezpieczeń infrastruktury IT oraz podstawy zapewnienia ciągłości działania i odtwarzania systemów
8. Podstawy informatyki śledczej oraz zasady zabezpieczania, analizy i przechowywania dowodów cyfrowych

Grupę docelową usługi stanowią m.in.:

- specjaliści komórek organizacyjnych odpowiedzialni w organizacjach za ochronę informacji i cyberbezpieczeństwo oraz kształtowanie polityki bezpieczeństwa;

- specjaliści IT z minimalnym doświadczeniem;

- uczniowie i absolwenci szkół branżowych;

- studenci i absolwenci kierunków z obszaru IT;

- osoby posiadające wiedzę, umiejętności i kompetencje wskazane w efektach uczenia się, chcące formalnie je potwierdzić.

Osoby posiadające kwalifikację mogą podjąć zatrudnienie m.in.:

- w naczelnych, centralnych i terenowych organach administracji państwowej (w tym jednostkach samorządu terytorialnego);

- u operatorów usług kluczowych (UOK);

- w służbach mundurowych i specjalnych;

- w przedsiębiorstwach i organizacjach, w których konieczne jest utrzymywanie właściwego poziomu bezpieczeństwa informacji, przetwarzanej za pomocą systemów teleinformatycznych.

Kwalifikacja w szczególności może być wykorzystana w zespołach reagowania na incydenty komputerowe CERT/CSIRT (ang. Computer Emergency Response Team/Computer Security Incident Response Team) oraz operacyjnych centrach bezpieczeństwa SOC (ang. Security Operations Center) – utworzenie SOC to obowiązek ustawowy dla UOK.

Warunki organizacyjne dla przeprowadzenia usługi szkoleniowej:

a) minimalna liczba Uczestników: 5, maksymalna liczba Uczestników: 16

b) liczba stanowisk pracy: każdy z Uczestników posiada dostęp do własnego stanowiska komputerowego

c) wyposażenie stanowiska warsztatowego:

- komputer wraz z niezbędnym oprogramowaniem oraz dostępem do Internetu

d) wyposażenie sali w której są prowadzone zajęcia warsztatowe:

- samodzielne stanowisko komputerowe dla każdego uczestnika szkolenia

- stoliki, krzesła, itp.

- projektor

Kurs realizowany będzie w formie warsztatowej, zakładającej aktywny udział Uczestników/Uczestniczek wraz z realizacją ćwiczeń praktycznych. Czas trwania szkolenia: 36 godziny dydaktyczne, obejmuje 20 godz. teoretycznych oraz 13 godz. praktycznych, oraz 3 godziny przeznaczone na egzamin.

Obowiązkowe dla każdego uczestnika jest uczestnictwo w zajęciach (dopuszczalne jest 20% nieobecności). Po zakończeniu usługi szkoleniowej zostanie przeprowadzona zewnętrzna walidacja oraz certyfikacja potwierdzająca nabycie kwalifikacji zawodowych o Kodzie 13869 w Zintegrowanym Rejestrze Kwalifikacji. Zachowana będzie rozdzielność procesów kształcenia i szkolenia od walidacji.

Po ukończeniu kursu / szkolenia (z absencją wynoszącą maksymalnie 20%) każdy z uczestników musi przystąpić do Certyfikowanego egzaminu / walidacji.

W przypadku potwierdzenia osiągnięcia wybranych modułów Kandydat otrzyma zaświadczenie z informacją, które efekty uczenia się zostały przez niego uzyskane. W momencie zaliczenia ostatniego z efektów uczenia się Kandydat otrzyma certyfikat.

Do weryfikacji efektów uczenia się stosuje się jedną z metod:

- test teoretyczny (pisemny) z użyciem zautomatyzowanego systemu elektronicznego
- analiza dowodów i deklaracji opcjonalnie uzupełniona wywiadem swobodnym.

Uczestnicy otrzymają materiały szkoleniowe: notes, długopis, teczkę.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 600,00 PLN Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT
Koszt przypadający na 1 uczestnika netto	5 600,00 PLN
Koszt osobogodziny brutto	155,56 PLN
Koszt osobogodziny netto	155,56 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	600,00 PLN
W tym koszt certyfikowania netto	600,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają: notes, długopis, teczka.

Warunki uczestnictwa

Wymagania dotyczące uczestnictwa:

Dana kwalifikacja nie ma założonych kryteriów uczestnictwa oraz wymaganych kwalifikacji poprzedzających udział w usłudze. Nie jest wymagane wylegitymowanie się doświadczeniem.

Informacje dodatkowe

Szkolenie realizowane jest w godzinach dydaktycznych 1 godzina szkoleniowa = 1 godzina dydaktyczna (45 min).

W efekcie ukończenia kursu Uczestnicy uzyskają certyfikat (po uzyskaniu pozytywnego wyniku z walidacji) potwierdzający nabycie kwalifikacji zgodnej z Kodem kwalifikacji 13869 w Zintegrowanym Rejestrze Kwalifikacji.

W przypadku kursów dofinansowanych warunkiem uczestnictwa w kursie jest spełnienie warunków przedstawionych przez danego Operatora, do którego składane będą dokumenty o dofinansowanie usługi rozwojowej.

Realizacja usługi rozwojowej jest zgodna ze Standardami dostępności dla polityki spójności 2021 – 2027 oraz zapisami Ustawy z dnia 19 lipca 2019 roku o zapewnieniu dostępności osobom ze szczególnymi potrzebami. Usługa rozwojowa jest dostępna dla osób ze szczególnymi potrzebami, czyli tych osób, które ze względu na swoje cechy zewnętrze lub wewnętrze lub ze względu na okoliczności, w których się znajdują, muszą podjąć dodatkowe działania lub zastosować dodatkowe środki.

Adres

ul. Stanisława Wyspiańskiego 2

35-111 Rzeszów

woj. podkarpackie

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt

Zdzisław Sikora

E-mail biuro@edu-service.pl

Telefon (+48) 500 403 218