Możliwość dofinansowania

Cyberbezpieczeństwo

Numer usługi 2024/08/26/9407/2278836

10 000,00 PLN brutto
10 000,00 PLN netto
60,24 PLN brutto/h
60,24 PLN netto/h

Akademia Górnośląska im. Wojciecha Korfantego w Katowicach

★★★★½

zdalna
Studia podyplomowe
166 h
19.10.2024 do 29.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Studia podyplomowe "Cyberbezpieczeństwo" są skierowane do osób pracujących lub planujących pracę w obszarze IT, które chcą pogłębić swoją wiedzę z zakresu bezpieczeństwa informatycznego. Program jest odpowiedni dla administratorów systemów, inżynierów bezpieczeństwa, specjalistów ds. IT, menedżerów projektów oraz wszystkich zainteresowanych tematyką cyberbezpieczeństwa, zarówno w sektorze prywatnym, jak i publicznym.
Minimalna liczba uczestników	18
Maksymalna liczba uczestników	24
Data zakończenia rekrutacji	30-09-2024
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	166
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	studia podyplomowe

Cel

Cel edukacyjny

Studia podyplomowe na kierunku „Cyberbezpieczeństwo” mają na celu przygotowanie specjalistów do ochrony systemów informatycznych przed zagrożeniami cybernetycznymi. Program oferuje kompleksową wiedzę na temat bezpieczeństwa systemów operacyjnych, sieci, aplikacji oraz metod wykrywania i neutralizacji zagrożeń. Uczestnicy zdobędą praktyczne umiejętności niezbędne do skutecznego zabezpieczania infrastruktury IT oraz poznają najnowsze technologie i narzędzia używane w branży.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zna podstawowe pojęcia i atrybuty bezpieczeństwa cybernetycznego oraz informacyjnego.	Poprawne zidentyfikowanie pojęć oraz atrybutów	Test teoretyczny
Rozumie znaczenie bezpieczeństwa danych oraz wdraża dobre praktyki backupu danych.	Przedstawienie przykładów dobrych praktyk związanych z backupem danych oraz omówienie ich w studium przypadku.	Test teoretyczny
Identyfikuje normy prawne i branżowe (RODO, ISO 27001) oraz stosuje je w organizacji.	Rozpoznanie i zastosowanie norm prawnych w praktycznym zadaniu opartym na realnym przykładzie organizacyjnym.	Test teoretyczny
Analizuje zagrożenia w cyberprzestrzeni i stosuje metody ochrony przed atakami.	Przeprowadzenie analizy zagrożeń oraz zastosowanie metod ochrony w symulowanej sytuacji ataku hakerskiego.	Test teoretyczny
Ocenia sytuacje kryzysowe i wdraża strategie zarządzania kryzysowego w organizacji.	Przygotowanie i ocena planu zarządzania kryzysowego na podstawie studium przypadku.	Test teoretyczny
Projektuje i wdraża plany ciągłości działania (Business Continuity Plans) w organizacji.	Opracowanie planu ciągłości działania, który spełnia standardy i procedury związane z BCP.	Test teoretyczny
Oceni ryzyko i przeprowadza jego analizę w celu minimalizacji zagrożeń.	Opracowanie i zaprezentowanie raportu z analizy ryzyka oraz działań naprawczych na podstawie analizy studium przypadku.	Test teoretyczny
Przygotowuje się do uzyskania międzynarodowego certyfikatu CompTIA Security+.	Zaliczenie egzaminu teoretycznego i praktycznego przygotowującego do uzyskania certyfikatu CompTIA Security+.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak

Program

CYBERBEZPIECZEŃSTWO

1. Bezpieczeństwo cybernetyczne - wprowadzenie (8 godzin)

• Wprowadzenie do bezpieczeństwa cybernetycznego

o Pojęcie bezpieczeństwa informacyjnego i cyberbezpieczeństwa

o Znaczenie informacji we współczesnym świecie

o Atrybuty bezpieczeństwa informacyjnego

• Bezpieczeństwo danych

o Znaczenie bezpieczeństwa danych dla organizacji

o Backup danych – dobre i złe praktyki

o Zjawisko szpiegostwa przemysłowego

• Normy prawne i branżowe (RODO, ISO 27001)

o Normalizacja i certyfikacja w bezpieczeństwie

o Ochrona danych osobowych w organizacji

o Zintegrowany System Zarządzania Bezpieczeństwem Informacji

• Cyberbezpieczeństwo w organizacji

o Przegląd najczęściej stosowanych metod i ataków hackerskich

o Metody i narzędzia zapewniania cyberbezpieczeństwa w organizacji

o Świadomość cyberbezpieczeństwa pracowników organizacji

• Sytuacje kryzysowe

o Kryzys i sytuacja kryzysowa

o Przegląd wybranych przykładów sytuacji kryzysowych (case study)

o Zarządzanie kryzysowe w organizacji

• Zachowanie ciągłości biznesowej organizacji

o Pojęcie business continuity

o Business continuity plan – omówienie przykładu (case study)

o Przegląd wybranych przykładów wykorzystania planów ciągłości działania

• Zarządzanie ryzykiem

o Pojęcie ryzyka i jego źródła

o Analiza ryzyka – omówienie przykładowej metody (case study)

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	10 000,00 PLN
Koszt przypadający na 1 uczestnika netto	10 000,00 PLN
Koszt osobogodziny brutto	60,24 PLN
Koszt osobogodziny netto	60,24 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe wysyłane mailem

Warunki uczestnictwa

Rekrutacja na studia podyplomowe odbywa się na zasadzie kolejności zgłoszeń. Na studia przyjmowane są osoby z wyższym wykształceniem.

Warunki techniczne

Urządzenie z dostępem do internetu (telefon, tablet, komputer)

Kontakt

Iwona Zub

E-mail iwona.zub@gwsh.pl

Telefon (+48) 323 570 583