Możliwość dofinansowania

Zarządzanie cyberbezpieczeństwem - online

Numer usługi 2024/04/19/8729/2129509

7 500,00 PLN brutto
7 500,00 PLN netto
45,18 PLN brutto/h
45,18 PLN netto/h

Akademia WSB

★★★★½

zdalna w czasie rzeczywistym
Studia podyplomowe
166 h
19.10.2024 do 30.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Studia adresowane są do osób zainteresowanych **rozwijaniem ścieżki kariery w branży Cyber Security**, np. menedżerów i specjalistów ds. cyberbezpieczeństwa w firmach i instytucjach sektora publicznego, osób odpowiedzialnych za wdrożenie systemu cyberbezpieczeństwa w organizacji, pełnomocników zarządu ds. cyberbezpieczeństwa, specjalistów i konsultantów ds. cyberbezpieczeństwa, ochrony danych osobowych i zarzadzania bezpieczeństwem informacji, adwokatów i prawników, którzy mogą procesować projekty czy sprawy sądowe w zakresie cyberbezpieczeństwa.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	12-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Słuchacz studiów podyplomowych zdobędzie wiedzę w zakresie określania zasobów informatycznych, które podlegać muszą ochronie, projektowania bezpieczeństwa sytemów IT, prewencji przed atakami komputerowymi. Posiadać będzie świadomość w zakresie scenariuszy nowoczesnych przestępstw komputerowych wymierzonych w informacje przechowywane cyfrowo. Zdobędzie wiedzę i umiejętności w zakresie przeprowadzania wstępnej analizy powłamaniowej systemu komputerowego oraz zabezpieczania dowodu cyfrowego

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Ma uporządkowaną wiedzę z zakresu projektowania i zarządzania bezpieczeństwem systemów informatycznych, przeciwdziałania, wykrywania i zwalczania cyberprzestępczości. Posiada wiedzę w zakresie określania zasobów informatycznych, które podlegać muszą ochronie, projektowania bezpieczeństwa systemów IT, prewencji przed atakami komputerowymi.	egzamin po każdym semestrze	Test teoretyczny
UMIEJĘTNOŚCI: Potrafi przeprowadzać wstępną analizę powłamaniową systemu komputerowego oraz zabezpieczać dowody cyfrowe. Potrafi przeprowadzać audyt bezpieczeństwa sieci komputerowych. Potrafi przeprowadzić analizę zagrożeń bezpieczeństwa danych.	egzamin po każdym semestrze	Test teoretyczny
KOMPETENCJE SPOŁECZNE: Dba o rozwój wiedzy o cyberbezpieczeństwie oraz świadomym zastosowaniu w organizacji, dąży do ciągłego doskonalenia i aktualizacji wiedzy z zakresu cyberbezpieczeństwa.	egzamin po każdym semestrze	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

Lp.	Nazwa przedmiotu	Liczba godzin zajęć teoretycznych	Liczba godzin zajęć praktycznych	Liczba punktów ECTS
1.	Technologie informacyjne	-	12	3
2.	Biały wywiad internetowy	6	14	4
3.	Prawne aspekty przestępstw komputerowych z elementami kryminalistyki	8	8	3
4.	Techniczne aspekty ataków komputerowych	8	8	3
5.	Zarządzanie i audytowanie bezpieczeństwa informacji zgodnie z normą ISO 27001	18	6	4
6.	Elementy informatyki śledczej	8	16	2
7.	Prawno-karna ochrona zasobów IT	12	-	3
8.	Projektowanie bezpieczeństwa w chmurze	8	8	4
9.	Audyt bezpieczeństwa sieci komputerowych	7	7	2

10.	Strategie i technologie IT w służbie ciągłości usług biznesowych	12	-	2
	Razem:	87	79	30

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 500,00 PLN
Koszt przypadający na 1 uczestnika netto	7 500,00 PLN
Koszt osobogodziny brutto	45,18 PLN
Koszt osobogodziny netto	45,18 PLN

Prowadzący

Liczba prowadzących: 5

1 z 5

dr inż. Karol Jędrasiak

Pracownik naukowo-dydaktyczny Akademii WSB, zastępca Dyrektora Centrum Transferu Technologii AWSB. Ekspert RPO WSL 2014-2012, członek Komitetu Sterującego Programu Sektorowego GameINN oraz Towarzystwa Przetwarzania Obrazów. Obecnie sprawuje funkcję Prezesa Zarządu spółki VRTechnology, zajmującej się komercjalizacją innowacyjnych rozwiązań z zakresu technologii wirtualnej rzeczywistości oraz profesjonalnych systemów symulacyjnych i trenażerowych. Autor 67 publikacji naukowych, w tym dwóch monografii naukowych. W ostatnich latach uhonorowany 10

nagrodami przyznawanymi przez instytucje krajowe oraz międzynarodowe za osiągnięcia naukowe i organizacyjne.

2 z 5

Wojciech Muras (net-o-logy)

Absolwent studiów doktoranckich w zakresie telekomunikacji. W branży IT od 14 lat. Związany ze spółką net-o-logy od 2003 roku jako Dyrektor ds. Rozwoju. Od 2010 roku pełnił funkcję Wiceprezesa Zarządu. W styczniu 2013 roku powołany przez Radę Nadzorczą na Prezesa Zarządu. Jest wykładowcą w Akademii WSB oraz członkiem Rady Programowej kierunku Informatyka. Specjalizuje się w procesach zarządzania usługami IT, zarządzania bezpieczeństwem informacji oraz aplikacjach wspierających procesy biznesowe. Rzeczoznawca IR Polskiego Towarzystwa Informatycznego.

3 z 5

Przemysław Szczurek

Senior Manager ds. Bezpieczeństwa Informacji. Z branżą IT związany od ponad 12 lat. Obecnie pełni funkcję Senior Managera ds. Bezpieczeństwa Informacji w TUV NORD Polska, gdzie odpowiada za rozwój i sprzedaż usług związanych z normami: ISO 27001, ISO 20000, ISO 22301 oraz tematyką Ochrony Danych Osobowych i Cyberbezpieczeństwa. Posiada certyfikaty: Audytora Wiodącego ISO 27001, ISO 20000, Audytora Wewnętrznego ISO 22301, Incident Response Managera i Inspektora Ochrony Danych. Jest egzaminatorem w zakresie Systemu Zarządzania Bezpieczeństwem Informacji z ramienia TUV NORD Polska. Jako trener TUV NORD i wykładowca akademicki duży nacisk stawia na świadomość kadry.

4 z 5

Dominik Rozdziałowski

Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Obrony Narodowej, wcześniej: Funkcjonariusz pionu do walki z przestępczością gospodarczą, Dyrektor Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Naczelnik Wydziału dw. Z Cyberprzestępczością Komendy Wojewódzkiej Policji w Kielcach. Specjalizuje się w teleinformatyce. Biegły Sądowy z pięciu dziedzin przy Sądzie Okręgowym w Kielcach.

5 z 5

dr inż. Krystian Mączka

Biegły sądowy z zakresu informatyki śledczej przy Sądzie Okręgowym w Katowicach, wykładowca akademicki, adiunkt w Akademii WSB w Dąbrowie Górniczej, wykładowca Krajowej Szkoły Sądownictwa i Prokuratury, specjalista z zakresu przestępstw komputerowych. Od lat zajmujący się m.in. problemami bezpieczeństwa sieci i systemów teleinformatycznych, zabezpieczaniem i odzyskiem danych, analizą nośników, problemami szyfrowania, monitoringiem. Autor wielu publikacji z zakresu zastosowań metod sztucznej inteligencji. Posiada Certyfikat X-Ways Forensic, Certyfikowany Informatyk Śledczy, Microsoft Certified Professional oraz Auditora Systemów Zarządzania Bezpieczeństwem Informacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują materiały z wytypowanych zajęć po ich realizacji.

Warunki uczestnictwa

Kandydaci powinni posiadać co najmniej wyższe wykształcenie.

Warunkiem uczestnictwa w usłudze jest dokonanie wpłaty oplaty wpisowej w kwocie 300 zł, która jest dodatkową opłatą poza kosztem wskazanym w usłudze.

Informacje dodatkowe

- Kandydaci powinni posiadać co najmniej wyższe wykształcenie.
- Czas trwania: 2 semestry.
- Podstawa zaliczenia: studia kończą się 2 egzaminami po każdym semestrze studiów.
- Dni odbywania się zajęć: dwa razy w miesiącu: soboty, niedziele.

Organizator studiów zastrzega sobie możliwość wprowadzenia zmian w programie studiów.

Zawarto umowę z WUP Kraków w ramach projektu Kierunek Kariera Zawodowa.

Warunki techniczne

Usługa realizowana zdalnie poprzez platformy ClickMeeting oraz Zoom

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: •Komputer stacjonarny/laptop z dostępem do Internetu
•Sprawny mikrofon i kamera internetowa (lub zintegrowane z laptopem)

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: download 8 mb/s, upload 8 mb/s, ping 15 ms

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Zalecamy wykorzystanie aktualnej wersji przeglądarki CHROME (zarówno na komputerach z systemem operacyjnym Windows jak i Apple

Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line: 7,5 h

Kontakt

Sandra Szczygieł

E-mail sszczygiel@wsb.edu.pl
Telefon (+48) 321 110 101