Możliwość dofinansowania

SPECJALISTA DS. CYBERBEZPIECZEŃSTWA - Studia podyplomowe

Numer usługi 2024/11/22/162125/2426952

5 900,00 PLN brutto
5 900,00 PLN netto
29,50 PLN brutto/h
29,50 PLN netto/h

Wyższa Szkoła Przedsiębiorczości i Administracji w Lublinie

Brak ocen dla tego dostawcy

Lublin / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

Studia podyplomowe

200 h

08.03.2025 do 28.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Usługa adresowana jest do: • osób, które wiążą swoją karierę zawodową z cyberbezpieczeństwem • absolwentów kierunków informatycznych lub pokrewnych (ew. zbliżonych) np. matematyka, telekomunikacja, elektronika • osób mających doświadczenie w pracy w IT, które pragną zbudować lub podnieść swoje kwalifikacje w zakresie cyberbezpieczeństwa • osób mających podstawową wiedzę z zakresu systemów i sieci IT • osób ze znajomością języka angielskiego na poziomie B2 i wyżej
Minimalna liczba uczestników	9
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	07-03-2025
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	200

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

Celem studiów podyplomowych z zakresu cyberbezpieczeństwa jest przekazanie uczestnikom zaawansowanej wiedzę i umiejętności niezbędne do skutecznej ochrony infrastruktury informatycznej, sieci oraz danych przed współczesnymi zagrożeniami cybernetycznymi. Celem studiów jest przygotowanie specjalistów zdolnych do ochrony organizacji przed cyberzagrożeniami oraz adaptacji do dynamicznie zmieniającego się świata technologii.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza	Zna i rozumie współczesne problemy cyberbezpieczeństwa Dysponuje wiedzą pozwalającą zaprojektować i wdrożyć system bezpieczeństwa w sieci informatycznej Posiada wiedzę z zakresu architektury, oraganizacji i bezpieczeństwa systemów operacyjnych Zna podstawowe regulacje prawne i oragnizacyjne związane z zachowaniem cyberbezpieczeńtwa w organizacji Zna typy cyberzagrożeń i cyberprzestępstw oraz wskazuje możliwości przeciwdziałania im Posiada wiedzę w zakresie zarządzania zasobami informacynymi i bazami danych Zna podstawowe wyzwania i trendy rozwojowe w zakresie cyberbezpeiczeństwa Zdobył wiedzę z zakresu bezpieczeństwa w sieciach i systemach	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętność	Stosuje praktyczne rozwiązania w zakresie zasobów informacyjnych i ochrony baz danych Potrafi kierować pracą zespołu w zakresie zapewnienia cyberbezpieczeństwa Identyfikuje przypadki prowadzenia”wojny informacyjnej” i cyberataku Stosuje obowiązujące prepisy prawne w procesach zapewnienia bezpieczeństwa cyfrowego Szacuje ryzyko i wdraża technologie i narzędzia przeciwdziałania zagrożeniom cyberbezpieczeństwa Potrafi wykorzystać wiedzę teoretyczną do analizy i charakterystyki wybranych typów cyberzagrożeń Zabezpiecza sieci www przed atakami cybernetycznymi i im przeciwdziała.	Test teoretyczny
Kompetencje	Poszerza swoja wiedzę w zakresie cyberbezpieczeństwa Pracuje i współdziała w zakresie tworzenia zabezpieczeń w obszarze informatyki Posiada świadomość znaczenia cyberbezpieczeństwa Potrafi działać w sposób przedsiębiorczy w zakresie zapewnienia cyberbezpieczeństwa	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Absolwenci otrzymują przewidziane ustawą świadectwo ukończenia studiów podyplomowych Wyższej Szkoły Przedsiębiorczości i Administracji w Lublinie. Na potrzeby Słuchacza, może zostać wydane odrębne zaświadczenie zawierające efekty kształcenia.

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

Tak. Warunkiem ukończenia studiów jest aktywny udział w zajęciach i uzyskanie wymaganych zaliczeń i egzaminów przewidzianych w programie studiów. Świadectwo zawiera wykaz przedmiotów na danym kierunku wraz z liczbą punktów ECTS oraz liczbą godzin, a także wynik ukończenia studiów podyplomowych.

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

Tak. Warunkiem ukończenia studiów jest obecność i aktywność oraz zaliczenie poszczególnych zajęć w ramach studiów. Świadectwo jest potwierdzeniem uzyskania pozytywnego wyniku z zaliczenia poszczególnych przedmiotów w ramach studiów oraz innych zaliczeń dotyczących danego kierunku.

Program

Program studiów:

Studia podyplomowe „Cyberbezpieczeństwo" to kompleksowy program, który ma na celu przygotowanie specjalistów do pracy w sektorze cyberbezpieczeństwa, zapewniając im zarówno teoretyczne podstawy, jak i praktyczne umiejętności potrzebne w codziennej pracy analityka bezpieczeństwa IT.

Zakres tematyczny studiów obejmuje:

1. **Wprowadzenie do cyberbezpieczeństwa** – Podstawy teoretyczne z zakresu ochrony infrastruktury IT, najnowsze zagrożenia oraz kluczowe zasady zachowania bezpieczeństwa w sieci.
2. **Podstawy sieci komputerowych** – Omówienie fundamentów działania sieci, w tym różnych typów sieci, adresacji IPv4, protokołów, mediów transmisji oraz podstaw usług sieciowych, takich jak DNS czy DHCP.
3. **Konfiguracja urządzeń sieciowych** – Praktyczna nauka konfiguracji urządzeń Cisco, podziału sieci na podsieci (IPv4 Subnetting), projektowania hierarchicznych sieci, wirtualizacji oraz usług chmurowych.
4. **Bezpieczeństwo punktów końcowych** – Ochrona systemów i urządzeń przed atakami poprzez implementację odpowiednich środków zapobiegawczych. Uczestnicy nauczą się, jak wykrywać i łagodzić podatności na poziomie protokołów sieciowych (IP/TCP/UDP), chronić urządzenia mobilne i systemy operacyjne (Windows, Linux), oraz wdrażać zaawansowane techniki ochrony przed złośliwym oprogramowaniem i zagrożeniami aplikacyjnymi.
5. **Obrona sieci** – Zaawansowane techniki zabezpieczeń, takie jak szyfrowanie (hashing), zasady obrony wielowarstwowej (defense-in-depth), utwardzanie sieci i urządzeń, zarządzanie dostępem oraz monitorowanie logów. Kurs obejmuje także kwestie związane z bezpieczeństwem chmurowym i zgodnością z przepisami oraz standardami bezpieczeństwa.
6. **Zarządzanie zagrożeniami cybernetycznymi** – Uczestnicy nauczą się, jak zarządzać incydentami bezpieczeństwa, analizować profile sieci i serwerów, przeprowadzać oceny ryzyka oraz wdrażać odpowiednie środki bezpieczeństwa w celu minimalizacji zagrożeń. Zostaną również zaznajomieni z modelami analizy intruzji oraz narzędziami do testowania penetracyjnego i oceniania podatności (CVSS).
7. **Podstawy programowania w Pythonie** – Programowanie w Pythonie w kontekście cyberbezpieczeństwa.
8. **Ethical Hacking** – Nauka testowania zabezpieczeń sieciowych i aplikacyjnych, skanowania podatności oraz przeprowadzania testów penetracyjnych. Program obejmuje również tematy związane z bezpieczeństwem Internetu Rzeczy (IoT) oraz socjotechniką.
9. **CyberOps Associate** – Kurs skupia się na analizie danych, wykrywaniu zagrożeń, reagowaniu na incydenty oraz analizie śladów i logów systemowych. Studenci poznają procedury działania centrów operacji bezpieczeństwa (SOC), analizę złośliwego oprogramowania oraz podstawy kryptografii.
10. **Bezpieczeństwo w chmurze (Cloud Security)** – Wprowadzenie do ochrony infrastruktury i danych w chmurze z użyciem platformy Microsoft Azure. Studenci zapoznają się z najlepszymi praktykami bezpieczeństwa chmurowego oraz metodami wdrażania zabezpieczeń w środowiskach chmurowych.

1.	Pierwsze kroki z systemem GNU/Linux
2.	Bezpieczeństwo w systemach operacyjnych
3.	Komunikacja i bezpieczeństwo sieci komputerowej
4.	Wprowadzenie do programowania w języku Python
5.	Wprowadzenie do Cyberbezpieczeństwa
6.	Kryptografia stosowana

7.	Blue Team - monitoring i obsługa incydentów bezpieczeństwa
8.	Bezpieczeństwo aplikacji WWW
9.	Inżynieria w cybersecurity
10.	Cyberbezpieczeństwo

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 900,00 PLN
Koszt przypadający na 1 uczestnika netto	5 900,00 PLN
Koszt osobogodziny brutto	29,50 PLN
Koszt osobogodziny netto	29,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

dr Waldemar Suszyński

Absolwent UMCS w Lublinie (1998 – fizyka komputerowa) i Politechniki Śląskiej w Gliwicach (2006 – doktor nauk technicznych w zakresie informatyki). Dwudziestoletnie doświadczenie w pracy dydaktyczno-naukowej. Wykładowca UMCS, KUL, PJATK, WSPA, nauczyciel przedmiotów zawodowych w Zespole Szkół Elektronicznych w Lublinie.

Najważniejsze informacje:

Instruktor Akademii Sieciowej CISCO: CCNA (od 2001), CCNA Security i CCNP (od 2009), Pełen zakres szkoleń Akademii sieciowe CISCO od 2010.
Nagrody: Instructor Recognition „Best of Nation" (Najlepszy Instruktor Akademii Sieciowych CISCO w Polsce) Budapeszt 2011.
Nagroda Akademii Sieciowych CISCO Instructor Excellence Award 2015 i 2017
Certyfikaty zawodowe Enterasys (uczestnictwo w sześcio-tygodniowych szkoleniach w USA – 2013-2014: ECE-Networking, ECE-Network_Security, ECE-Switch_Routing, ECS-Advanced_Routing, ECS-IPv6_Networking, ECS-NAC, ECS-Policy, ECS-Routing ECS-Switching_NMS, ECS-Wireless, ECUI – Enterasys University Instructor.

Współautor skryptów akademickich:

Kuczyński K., Suszyński W., Bezprzewodowe sieci lokalne, Instytut Informatyki UMCS, Lublin, 2012.
Kuczyński K., Suszyński W., Przełączanie w sieciach lokalnych, Instytut Informatyki UMCS, Lublin, 2012

Autor ponad 50 publikacji naukowych.
Promotor ponad 50 prac licencjackich, magisterskich i dyplomowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dla uczestników usługi - pliki dokumentów przygotowanych w dowolnym formacie

oraz materiały VOD.

Warunki techniczne

Usługa będzie prowadzona przez Platformę Zdalnego Nauczania. Platforma działa poprawnie w nowych wersjach przeglądarek: Internet Explorer, Mozilla Firefox, Google Chrome, Opera. W przypadku używania starszych wersji, niektóre funkcjonalności mogą działać nieprawidłowo.Do wyświetlania niektórych treści multimedialnych potrzebny jest Adobe Flash Player.

System dla smartfonów: co najmniej Android 10 lub iOS 14

System dla tabletów: co najmniej Android 10 lub iPadOS 14

System i oprogramowanie dla komputerów: co najmniej Windows 10 wraz z przeglądarką nie starszą niż Chrome 85 lub Frefox 85

System dla urządzeń Mac (Apple): co najmniej macOS Catalina (10.15.7)

Procesor minimum 2GHz oraz pamięć RAM minium 4GB

Łącze internetowe o przepustowości - pobieranie minimum 2 Mb/s, wysyłanie minimum 1Mb/s

Konieczny jest mikrofon i kamera.

Nazwa platformy: Platforma e- learningowa WSPA Lublin - Link do Platformy - https://puw.wspa.pl/

Adres

ul. Bursaki 12
20-150 Lublin
woj. lubelskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe
- Parking, restauracja

Kontakt

Karolina Sobczak

E-mail ka.sobczak@wspa.pl
Telefon (+48) 814 529 474