Możliwość dofinansowania

Specjalista ds. cyberbezpieczeństwa – studia podyplomowe

Numer usługi 2025/12/12/162125/3209050

6 800,00 PLN brutto
6 800,00 PLN netto
34,00 PLN brutto/h
34,00 PLN netto/h

Wyższa Szkoła Przedsiębiorczości i Administracji w Lublinie

4,5 / 5

99 ocen

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

Studia podyplomowe

200 h

21.03.2026 do 28.02.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	20-03-2026
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 2024 r. poz. 1571, 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
Potrafi praktycznie stosować rozwiązania w zakresie zasobów informacyjnych i ochrony baz danych	Identyfikuje rodzaje zasobów informacyjnych i potrafi je sklasyfikować Stosuje podstawowe zasady ochrony danych Posługuje się narzędziami do zarządzania bazami danych worzy, modyfikuje i zabezpiecza proste bazy danych lub zestawy danych Potrafi zidentyfikować zagrożenia i zastosować środki ochrony informacji Stosuje się do procedur bezpieczeństwa i polityki prywatności w organizacji	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Potrafi kierować pracą zespołu w zakresie zapewnienia cyberbezpieczeństwa	Określa role i zadania członków zespołu odpowiedzialnych za bezpieczeństwo systemów informatycznych Dobiera odpowiednie procedury i narzędzia do zarządzania incydentami bezpieczeństwa (np. detekcja, reakcja, raportowanie) Organizuje pracę zespołu w sytuacjach kryzysowych (np. cyberatak, naruszenie danych) Monitoruje realizację zadań i egzekwuje stosowanie się do zasad polityki bezpieczeństwa Komunikuje się skutecznie z członkami zespołu oraz z osobami zarządzającymi organizacją Dokonuje oceny ryzyka i podejmuje decyzje dotyczące poprawy procedur bezpieczeństwa Wdraża dobre praktyki zespołowe w zakresie bezpieczeństwa IT i zgodności z regulacjami (np. RODO, ISO/IEC 27001)	Obserwacja w warunkach symulowanych
Identyfikuje przypadki prowadzenia ”wojny informacyjnej” i cyberataku	Rozróżnia pojęcia: „wojna informacyjna”, dezinformacja, manipulacja informacją, atak socjotechniczny, cyberatak Rozpoznaje cechy charakterystyczne wojny informacyjnej (np. fałszywe narracje, kampanie propagandowe, deepfake’i) Identyfikuje formy cyberataków (np. phishing, DDoS, ransomware, exploit zero-day) Analizuje źródła informacji pod kątem ich wiarygodności i potencjalnego wpływu na odbiorców Wskazuje przykłady historyczne i współczesne przypadków wojny informacyjnej i cyberataków (np. ataki na infrastrukturę krytyczną, kampanie wpływu w mediach społecznościowych) Wykrywa objawy trwającej kampanii dezinformacyjnej lub cyberincydentu w analizowanym środowisku	Wywiad swobodny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje obowiązujące przepisy prawne w procesach zapewnienia bezpieczeństwa cyfrowego	Rozpoznaje podstawowe akty prawne dotyczące bezpieczeństwa cyfrowego Identyfikuje obowiązki prawne administratorów systemów i danych w zakresie ochrony informacji Stosuje odpowiednie przepisy w sytuacjach wymagających reakcji na incydenty Uwzględnia aspekty prawne w procedurach bezpieczeństwa IT Ocenia zgodność działań z obowiązującymi przepisami w zakresie zabezpieczenia danych i systemów Potrafi wskazać skutki prawne naruszenia przepisów dotyczących cyberbezpieczeństwa	Wywiad swobodny
Potrafi oszacować ryzyko i wdrażać technologie i narzędzia przeciwdziałania zagrożeniom cyberbezpieczeństwa	Dokonuje identyfikacji zasobów i zagrożeń w systemach informatycznych Przeprowadza analizę ryzyka zgodnie z wybraną metodyką Ocena poziomu ryzyka – potrafi wskazać najbardziej narażone obszary infrastruktury IT Dobiera i uzasadnia odpowiednie środki techniczne i organizacyjne przeciwdziałania zagrożeniom Potrafi wdrożyć procedury i technologie ograniczające ryzyko oraz monitorować ich skuteczność Potrafi opracować plan reagowania na incydenty i wdrażać działania naprawcze	Wywiad swobodny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Potrafi wykorzystać wiedzę teoretyczną do analizy i charakterystyki wybranych typów cyberzagrożeń	Rozpoznaje i klasyfikuje różne typy cyberzagrożeń pisuje mechanizmy działania zagrożeń oraz ich potencjalne skutki dla organizacji Analizuje konkretne przypadki incydentów i identyfikuje źródła oraz wektory ataku Ocenia ryzyko i podatność systemów w kontekście wybranych zagrożeń Wskazuje sposoby wykrywania i przeciwdziałania konkretnym zagrożeniom w oparciu o aktualną wiedzę technologiczną i normatywną Uwzględnia obowiązujące przepisy	Wywiad swobodny

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

Wprowadzenie do cyberbezpieczeństwa

Podstawy sieci komputerowych

Urządzenia sieciowe

Zabezpieczanie urządzeń końcowych

Ochrona sieci

Zarządzanie zagrożeniami cybernetycznymi - laboratorium

Podstawy programowania w języku Python - laboratorium

Ethical Hacker - kurs

CyberOps Associate

Bezpieczeństwo w chmurze obliczeniowej

Łącznie 200 godzin dydaktycznych

Liczba semestrów: 2

Liczba punktów ECTS: 30

Przerwy są wliczone w czas trwania usługi.

Dokument potwierdzający ukończenie studiów: świadectwo ukończenia studiów podyplomowych.

Zajęcia odbywają się w soboty i niedziele, co dwa, trzy tygodnie w godz.: 8:00- 16:00.

Zajęcia na studiach prowadzone są w formie ćwiczeń, warsztatów, case study oraz multimedialnych wykładów.

Warunkiem otrzymania świadectwa ukończenia studiów podyplomowych jest zaliczenie poszczególnych przedmiotów realizowanych w ramach studiów.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 800,00 PLN
Koszt przypadający na 1 uczestnika netto	6 800,00 PLN
Koszt osobogodziny brutto	34,00 PLN
Koszt osobogodziny netto	34,00 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

Szczegółowy harmonogram zajęć zostanie zamieszczony po decyzji Władz Uczelni WSPA o uruchomieniu kierunku, najpóźniej 6 dni przed planowanym pierwszym zjazdem.

Oświadczenia i zobowiązania Uczestnika Usługi BUR

1. Uczestnik oświadcza, że przed zawarciem umowy z Dostawcą usługi - WSPA zapoznał się oraz akceptuje treść:

1) Zarządzenia Kanclerza Wyższej Szkoły Przedsiębiorczości i Administracji w Lublinie nr 31/K/WSPA/2024-2025 z dnia 13 maja 2025 roku w sprawie wysokości i terminów opłat wpisowego i czesnego dla Słuchaczy studiów podyplomowych w roku akademickim 2025-2026,

2) Zarządzenia Kanclerza Wyższej Szkoły Przedsiębiorczości i Administracji w Lublinie nr 32/K/WSPA/2024-2025 z dnia 13 maja 2025 r. w sprawie innych opłat na studiach podyplomowych w roku akademickim 2025-2026,

3) Zarządzenie Kanclerza Wyższej Szkoły Przedsiębiorczości i Administracji w Lublinie nr 33/K/WSPA/2024-2025 z dnia 13 maja 2025 r. w sprawie zniżek na studia podyplomowe dla kandydatów rozpoczynających studia w roku akademickim 2025-2026,

4) Regulaminu Studiów Podyplomowych.

2. Zarządzenia i Regulamin, o których mowa powyżej zostaną przekazane Uczestnikowi do zapoznania się przed zawarciem Umowy z WSPA, w momencie rejestracji poprzez stronę internetową - https://wspa.pl/rekrutacja/.

3. Zarządzenia i Regulamin, o których mowa powyżej dostępne są także na stronie internetowej Uczelni WSPA – www.https://wspa.pl/

Warunki techniczne

Platforma e-learningowa WSPA Lublin.

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 minimum 4GB

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

Adres

Lublin 12
20-150 Lublin
woj. lubelskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

CENTRUM STUDIÓW PODYPLOMOWYCH I SZKOLEŃ

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