Możliwość dofinansowania

Cyberbezpieczeństwo

Numer usługi 2025/12/15/21559/3213125

4 700,00 PLN brutto
4 700,00 PLN netto
24,74 PLN brutto/h
24,74 PLN netto/h

Lubelska Akademia WSEI

4,6 / 5

4 oceny

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

Studia podyplomowe

190 h

03.04.2026 do 28.02.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Wiedza i umiejętności pozyskane w czasie studiów pozwolą absolwentowi na specjalizację w ramach swojej pracy w organach ścigania, instytucjach państwowych oraz w biznesie w obszarze związanym z cyberbezpieczeństwem. Absolwent uzyska wiedzę i praktyczne umiejętności umożliwiające podjęcie pracy związanej z administracją i bezpieczeństwem systemów komputerowych, opracowywaniem polityk bezpieczeństwa, ich wdrażania, utrzymania oraz rozwoju. Pozna podstawy informatyki śledczej oraz najnowsze metody ataków i zagrożenia dla systemów informatycznych. Będzie potrafił przeciwdziałać ich rozprzestrzenianiu i skutkom. Będzie umiał poszukiwać, gromadzić i zabezpieczać materiał dowodowy. Absolwent pozna podstawy analizy kryminalnej, będzie potrafił analizować dane związane z wystąpieniem incydentu teleinformatycznego, wykrywać i identyfikować związki między nimi, określać przesłanki, wyciągać wnioski i oceniać ich wiarygodność.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-04-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	190
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

Podstawowym celem studiów jest przekazanie specjalistycznej wiedzy z obszaru współczesnego podejścia do bezpieczeństwa informacji w ujęciu prawnym i praktycznym. Poprzez liczne praktyczne ćwiczenia słuchacze uzyskają umiejętności pozwalające na skuteczne i zgodne z prawem lub dobytymi praktykami zarządzanie bezpieczeństwem informacji w organizacji lub świadczenie usług z zakresu cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W zakresie wiedzy absolwent w stopniu zaawansowanym między innymi zna i rozumie: pojęcie cyberbezpieczeństwa w odniesieniu do organizacji, w której pracuje oraz miejsca organizacji w systemie krajowym i europejskim, zasady tworzenia kultury bezpieczeństwa w organizacji, ma zaawansowaną wiedzę na temat współczesnych zagrożeń w sieci Internet, ataków na systemy informatyczne, sposobów obrony i reagowania.	Udział w zajęciach, spełnienie warunków / wykonanie zadań ustalonych przez prowadzącego	Test teoretyczny
W zakresie umiejętności absolwent w stopniu zaawansowanym między innymi potrafi: analizować i wdrażać bieżące regulacje prawne, standardy i dobre praktyki w zakresie bezpieczeństwa IT, funkcjonować w zespole bezpieczeństwa, w tym rozumieć i wdrażać politykę bezpieczeństwa organizacji, opracowywać procedury i wymagania w zakresie bezpieczeństwa procesowego i technologicznego, identyfikować słabe punkty systemu informatycznego, opracowywać i wdrażać działania zaradcze, posługiwać się zaawansowanymi umiejętnościami reagowania na incydent bezpieczeństwa, w tym wdrożyć odpowiedniej procedury i przeprowadzić działania mitygujące ryzyko.	Udział w zajęciach, spełnienie warunków / wykonanie zadań ustalonych przez prowadzącego	Obserwacja w warunkach symulowanych Analiza dowodów i deklaracji Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W zakresie kompetencji absolwent w stopniu zaawansowanym jest między innymi gotów do: profesjonalnej współpracy w zespole bezpieczeństwa teleinformatycznego, propagowania idei bezpieczeństwa komputerowego i bezpieczeństwa funkcjonowania w Internecie, samokształcenia w zakresie IT i bezpieczeństwa informacji.	Udział w zajęciach, spełnienie warunków / wykonanie zadań ustalonych przez prowadzącego	Obserwacja w warunkach symulowanych
		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

I. Wprowadzenie do cyberbezpieczeństwa

- Cyberbezpieczeństwo – praktyczne podejście
- Współczesne podejście do bezpieczeństwa w aspekcie ochrony danych osobowych
- Zagadnienia własności intelektualnej przedsiębiorstwa w aspekcie bezpieczeństwa informacji

II. Bezpieczeństwo organizacyjne

- Współczesne podejście do bezpieczeństwa w aspekcie Ustawy o Krajowym Systemie Cyberbezpieczeństwa
- Kreowanie polityki cyberbezpieczeństwa w organizacji
- Cyberprzestępczość – zagadnienia prawne, zwalczanie
- Zbieranie informacji o ludziach, pracownikach i kontrahentach. Biały wywiad – ćwiczenia praktyczne
- Podejście procesowe oparte na ryzyku w bezpieczeństwie IT – wyzwanie dla biznesu – ćwiczenia
- Audyt informatyczny

III. Bezpieczeństwo technologiczne

- Bezpieczeństwo rozwiązań chmurowych – laboratorium

- Rozwiązania techniczne wspierające cyberbezpieczeństwo – laboratorium
- Cyber Treat Intelligence

IV. Zarządzanie incydentem

- Podejście do zabezpieczania dowodów cyfrowych na potrzeby analiz śledczych
- Postępowanie z incydentem informatycznym w ujęciu prawnym i normatywnym
- Informatyka śledcza – zagadnienia techniczne, zabezpieczanie danych, analiza
- Informatyka śledcza – urządzenia mobilne
- Gra strategiczna – zarządzanie incydentem, kryzysem

V. Seminarium i egzamin

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	4 700,00 PLN
Koszt przypadający na 1 uczestnika netto	4 700,00 PLN
Koszt osobogodziny brutto	24,74 PLN
Koszt osobogodziny netto	24,74 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Połączenie zajęć synchronicznych z zajęciami w bezpośrednim kontakcie w siedzibie Uczelni 50/50. Wybrane zajęcia będą realizowane na platformie online z elementami czatu lub wideokonferencji, z dostępem do materiałów i ćwiczeń.

Warunki uczestnictwa

Ukończone studia I lub II stopnia.

O przyjęciu na studia decyduje kolejność zgłoszeń i poprawność złożonych dokumentów.

Uprzejmie informujemy, że w przypadku zbyt małej liczby kandydatów grupa może nie zostać uruchomiona.

WYMAGANE DOKUMENTY

- dyplom/odpis ukończenia studiów wyższych
- wypełniony kwestionariusz zgłoszeniowy
- wypełnione podanie o przyjęcie na studia
- wypełniona umowa w 2 egzemplarzach
- 1 zdjęcie
- dowód uiszczenia opłaty rekrutacyjnej

Link do pobrania dokumentów: https://podyplomowe.wsei.eu/dokumenty-dla-sluchacza/

Informacje dodatkowe

Aktualna oferta z pełnym opisem oraz niezbędną dokumentacją: https://podyplomowe.wsei.eu/nasza-oferta/

Warunki techniczne

Usługa realizowana zdalnie na platformie Moodle poprzez usługę ClickMeeting.

Minimalne wymagania sprzętowe, jakie musi spełniać komputer użytkownika lub inne urządzenie do zdalnej komunikacji:

- komputer stacjonarny/laptop z dostępem do Internetu,
- sprawny mikrofon i kamera internetowa.

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować użytkownik: download 8 mb/s, upload 8 mb/s, ping 15 ms. Zalecamy wykorzystanie aktualnej wersji przeglądarki CHROME.

Adres

ul. Projektowa 4

20-209 Lublin

woj. lubelskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Edyta Czapska

E-mail podyplomowe@wsei.lublin.pl

Telefon (+48) 817 493 224