Możliwość dofinansowania

Cyberbezpieczeństwo i informatyka śledcza – studia podyplomowe

Numer usługi 2025/10/13/18793/3074358

9 840,00 PLN brutto
9 840,00 PLN netto
61,50 PLN brutto/h
61,50 PLN netto/h

Wyższa Szkoła Turystyki i Ekologii w Suchej Beskidzkiej

4,8 / 5

204 oceny

zdalna w czasie rzeczywistym
Studia podyplomowe
160 h
25.04.2026 do 24.01.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Absolwenci dowolnego kierunku studiów wyższych (I lub II stopnia, lub jednolitych magisterskich). Usługa skierowana jest również do uczestników projektu "Małopolski Pociąg do Kariery - sezon I". Program został zaprojektowany z myślą o: • pracownikach działów bezpieczeństwa informacji, • osobach, odpowiedzialnych za ochronę danych i systemów IT w instytucjach publicznych i prywatnych, • prawnikach i specjalistach compliance, zainteresowanych prawem nowych technologii, • osobach, planujących specjalizację lub zmianę ścieżki zawodowej w obszarze cyberbezpieczeństwa i informatyki śledczej.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	20-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	160
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

Rozpoznawanie zagrożeń i typowych ataków w sieciach IT; zarządzanie systemami bezpieczeństwa informacji i incydentami; podstawy informatyki śledczej i zabezpieczania cyfrowych śladów; wykorzystanie narzędzi, takich jak Autopsy, FTK, Volatility; praca z logami, metadanymi i śladami powłamaniowymi; stosowanie przepisów prawa krajowego i międzynarodowego w zakresie ochrony danych i cyberprzestępczości.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W zakresie wiedzy Słuchacz: ma uporządkowaną wiedzę z zakresu cyberbezpieczeństwa dotyczącą: ochrony i bezpiecznej komunikacji danych, zagrożeń i ataków, testów penetracyjnych, narzędzi administracji systemami i sieciami, OSINT oraz zarządzania zasobami projektu.	Słuchacz: - wymienia pojęcia dotyczące bezpieczeństwa informacji oraz sieci komputerowych - wymienia zasady bezpiecznej komunikacji i zabezpieczania informacji cyfrowych - efektywnie zarządza zasobami – alokowanie zasobów ludzkich, finansowych i materialnych w projekcie. - charakteryzuje typy zagrożeń i ataków na systemy informatyczne i sieci - wymienia metody przeprowadzania testów penetracyjnych - opisuje narzędzia administratora i sieci - wymienia techniki gromadzenia i analizy informacji pochodzących z ogólnodostępnych źródeł (Open Source Intelligence)	Test teoretyczny z wynikiem generowanym automatycznie
W zakresie umiejętności Słuchacz: zapewnia bezpieczeństwo środowiska teleinformatycznego (systemów i sieci) poprzez dobór i zastosowanie adekwatnych metod oraz narzędzi, konfigurację i zabezpieczanie systemów, analizę bezpieczeństwa i ruchu sieciowego oraz koordynację pracy zespołu.	Słuchacz: - dobiera oraz wykorzystuje odpowiednie mechanizmy ochrony informacji cyfrowych - wykonuje analizę bezpieczeństwa systemów teleinformatycznych - efektywnie zarządza zespołem - konfiguruje i zabezpiecza system operacyjny - używa wybranych narzędzi administratora systemów i sieci - przeprowadza analizę ruchu w sieciach	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W zakresie kompetencji społecznych Słuchacz: odpowiedzialnie i etycznie funkcjonuje w środowisku zawodowym, współpracuje i komunikuje się w zespole, dba o kształtowanie kultury projektowej i działanie z uwzględnieniem kwestii ekonomicznych	Słuchacz: - pracuje zespołowo i pod presją czasu - kształtuje kulturę projektową w organizacji - realizuje swoje działania z uwzględnieniem aspektów ekonomicznych	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 1. Czy dokument jest wydany przez podmiot systemu oświaty lub szkolnictwa wyższego na podstawie odrębnych przepisów?

TAK

ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, 1871 i 1897)

Informacje

Nazwa Podmiotu prowadzącego walidację	Wyższa Szkoła Turystyki i Ekologii w Suchej Beskidzkiej
Nazwa Podmiotu certyfikującego	Wyższa Szkoła Turystyki i Ekologii w Suchej Beskidzkiej

Program

Podstawy bezpieczeństwa informacji i ochrona danych osobowych

Klasyfikacja zagrożeń w cyberprzestrzeni

Zarządzanie incydentami i analiza ryzyka

Dyrektywa NIS2 i Krajowy System Cyberbezpieczeństwa

Informatyka śledcza i analiza cyfrowych dowodów

OSINT i SOCMINT - wywiad ze źródeł otwartych

Testy penetracyjne i zabezpieczanie systemów

Przestępstwa komputerowe i odpowiedzialność prawna

Dezinformacja, cyberterroryzm, działania wywiadowcze

Kryptografia, VPN, firewalle i IDS/IPS

Zgodność z RODO, ustawą o KSC i konwencją budapeszteńską

Liczba punktów ECTS - 30

Liczba godzin - 160, w tym:

godziny praktyczne: 24

godziny teoretyczne: 136

Czas trwania - 2 semestry

Przerwy nie wliczane w czas trwania usługi.

Metody walidacji:

Weryfikacja osiągniętych efektów uczenia się prowadzona jest w sposób ciągły oraz końcowy, z wykorzystaniem zróżnicowanych metod oceny wiedzy i umiejętności.

Proces walidacji obejmuje testy zaliczeniowe (testy online z wynikiem generowanym automatycznie) po I i II semestrze, realizowane w formie testów wielokrotnego wyboru, które pozwalają na ocenę stopnia opanowania wiedzy teoretycznej, terminologii oraz podstawowych zasad i procedur z zakresu cyberbezpieczeństwa. Całościową ocenę wiedzy zapewnia egzamin końcowy, również przeprowadzany w formie testu wielokrotnego wyboru (online, z wynikiem generowanym automatycznie), obejmujący pełny zakres treści programowych.

Ocena efektów praktycznych realizowana jest poprzez projekt indywidualny lub zespołowy, polegający na analizie incydentu cyberbezpieczeństwa lub opracowaniu strategii bezpieczeństwa dla wybranego systemu lub organizacji. Uzupełnieniem tej formy walidacji jest prezentacja studium przypadku naruszenia cyberbezpieczeństwa, podczas której oceniane są umiejętności analityczne, trafność zaproponowanych rozwiązań oraz kompetencje komunikacyjne.

Zastosowane metody walidacji umożliwiają kompleksową ocenę wiedzy, umiejętności praktycznych oraz kompetencji społecznych studentów.

Usługodawca zapewnia rozdzielność pomiędzy procesem kształcenia i walidacji.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 840,00 PLN
Koszt przypadający na 1 uczestnika netto	9 840,00 PLN
Koszt osobogodziny brutto	61,50 PLN

Koszt osobogodziny netto	61,50 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały w wersji elektronicznej oraz testy online dostępne na dedykowanej dla uczestników platformie e-learningowej.

Warunki uczestnictwa

Ukończone studia wyższe (I lub II stopnia, jednolite magisterskie) dowolnego kierunku.

Warunkiem koniecznym jest dokonanie opłaty wpisowej (300 zł), zapis przez formularz rekrutacyjny dostępny na stronie www.wste.edu.pl oraz podpisanie umowy z WSTiE o świadczenie usługi edukacyjnej.

Informacje dodatkowe

Wśród kadry dydaktycznej są m.in.:

- dr Karolina Walancik
- Krzysztof Bogusz
- Andrzej Tomasiak
- Specjaliści ds. bezpieczeństwa IT i informatyki śledczej
- Praktycy, współpracujący z organami ścigania

Liczba godzin usługi podana jest w godzinach dydaktycznych (1h dydakt. = 45 minut)

160h dydaktycznych = 120h zegarowych.

godziny praktyczne: 24

godziny teoretyczne: 136

Czas trwania - 2 semestry

Przerwy nie wliczane w czas trwania usługi.

Uczestnik zobligowany jest do dokonania opłaty wpisowej na studia w wysokości 300 zł, która **nie jest** wliczona w cenę usługi

Zaakceptowano regulamin projektu "Małopolski Pociąg do Kariery - sezon I" dla Instytucji Szkoleniowych.

Warunki techniczne

Wymagania techniczne:

komputer / laptop ze stałym dostępem do Internetu (Szybkość pobierania/przesyłania: minimalna

2 Mb/s / 128 kb/s; zalecana 4 Mb/s / 512 kb/s)

przeglądarka internetowa – zalecane: Google Chrome, Mozilla Firefox

słuchawki lub dobrej jakości głośniki

mikrofon

zalecane: kamera (w przypadku komputerów stacjonarnych)

spokojne miejsce, odizolowane od zewnętrznych czynników rozpraszających

Kontakt

Anna Oleksa-Kaźmierczak

E-mail szkola@wste.edu.pl
Telefon (+48) 338 745 425