Możliwość dofinansowania

Cyberbezpieczeństwo i informatyka śledcza – studia podyplomowe

Numer usługi 2025/07/23/18793/2898309

10 400,00 PLN brutto
10 400,00 PLN netto
65,00 PLN brutto/h
65,00 PLN netto/h

Wyższa Szkoła Turystyki i Ekologii w Suchej Beskidzkiej

4,8 / 5

204 oceny

zdalna w czasie rzeczywistym
Studia podyplomowe
160 h
18.10.2025 do 27.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Absolwenci dowolnego kierunku studiów wyższych (minimum licencjat). 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	10-10-2025
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 2023 r. poz. 742, 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 Student: a) zna strukturę i funkcjonowanie protokołów oraz mechanizmy bezpieczeństwa (np. kryptografia, IDS/IPS, SIEM); b) rozumie prawne i etyczne aspekty cyberbezpieczeństwa (RODO, KSC); c) zna metodologie informatyki śledczej (chain of custody, forensics); d) zna podstawy analizy malware, zagrożeń i incydentów.	Student: – potrafi opisać mechanizmy bezpieczeństwa i protokoły sieciowe; – wskazuje podstawowe regulacje, etyczne wymogi i procedury prawne; – wyjaśnia zasady i etapy informatyki śledczej; – rozumie sposoby analizy incydentów i malware.	Test teoretyczny z wynikiem generowanym automatycznie
W zakresie umiejętności Student: a) potrafi skonfigurować i zabezpieczyć infrastrukturę sieciową (firewall, VPN, segmentacja); b) przeprowadza analizę i reakcję na incydenty (incident response); c) wykonuje działania z zakresu informatyki śledczej – zbiera, zabezpiecza i analizuje dowody cyfrowe; d) przygotowuje dokumentację techniczną – raporty, polityki bezpieczeństwa.	Student: – poprawnie konfiguruje i testuje zabezpieczenia sieci; – realizuje symulowany incydent z dokumentacją IR; – przeprowadza akcję forensyczną i zachowuje integralność dowodów; – tworzy kompletne polityki i raporty zgodnie ze standardami.	Test teoretyczny z wynikiem generowanym automatycznie
W zakresie kompetencji społecznych Student: a) rozumie potrzebę zachowania etyki, poufności i ochrony prywatności; b) efektywnie komunikuje się z odbiorcami nietechnicznymi; c) potrafi działać w interdyscyplinarnym zespole; d) jest świadomy potrzeby ciągłego rozwoju i samokształcenia.	Student: – wskazuje i uzasadnia aspekty etyczne działań; – przeprowadza prezentację wyników incydentu dla zarządu; – uczestniczy aktywnie w pracy grupowej, przydziela i wykonuje zadania; – dokonuje samooceny i zaplanowania dalszego rozwoju.	Test teoretyczny z wynikiem generowanym automatycznie

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

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

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	10 400,00 PLN
Koszt przypadający na 1 uczestnika netto	10 400,00 PLN
Koszt osobogodziny brutto	65,00 PLN
Koszt osobogodziny netto	65,00 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.

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) 338 744 525