Możliwość dofinansowania

Informatyka śledcza

Numer usługi 2025/12/23/21519/3228078

9 000,00 PLN brutto
9 000,00 PLN netto
30,00 PLN brutto/h
30,00 PLN netto/h

Politechnika Opolska

4,6 / 5

57 ocen

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

Studia podyplomowe

300 h

10.10.2026 do 27.06.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Dwusemestralne studia podyplomowe adresowane do absolwentów wyższych uczelni, pragnących pogłębić bądź zdobyć umiejętności praktyczne oraz wiedzę teoretyczną z zakresu informatyki śledczej, bezpieczeństwa informacji, testów penetracyjnych oraz narzędzi i metod pracy operacyjnej. Absolwent ma wiedzę w zakresie bezpieczeństwa sieci komputerowych, systemów operacyjnych, ochrony danych i typowych metod ataku komputerowego. Zna zagadnienia w zakresie prawa dowodowego dla dowodów elektronicznych. Posiada umiejętności z zakresu pozyskiwania, magazynowania i przetwarzania informacji, a także zastosowania w zakresie wybranych metod sztucznej inteligencji oraz ich zastosowań w informatyce śledczej. Starannie dobrana tematyka zajęć oraz najlepsi specjaliści z całego kraju umożliwią zdobycie nie tylko teorii, ale i praktyki w zakresie zarówno bezpieczeństwa informacji/systemów/sieci, jak również wyszukiwania informacji, uzyskiwania dostępu do informacji oraz odzyskiwania danych/informacji.
Minimalna liczba uczestników	14
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	03-10-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	300

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

Dwusemestralne studia podyplomowe adresowane do absolwentów wyższych uczelni, pragnących pogłębić bądź zdobyć umiejętności praktyczne oraz wiedzę teoretyczną z zakresu informatyki śledczej, bezpieczeństwa informacji, testów penetracyjnych oraz narzędzi i metod pracy operacyjnej.
Absolwent ma wiedzę w zakresie bezpieczeństwa sieci komputerowych, systemów operacyjnych, ochrony danych i typowych metod ataku komputerowego. Zna zagadnienia w zakresie prawa dowodowego dla dowodów elektronicznych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Ma wiedzę w zakresie bezpieczeństwa sieci komputerowych, systemów operacyjnych, ochrony danych i typowych metod ataku komputerowego. Ma wiedzę w zakresie analizy autentyczności obrazu. Ma wiedzę w zakresie wybranych metod sztucznej inteligencji i ich zastosowań w informatyce śledczej. Ma wiedzę z zakresu pozyskiwania, magazynowania i przetwarzania informacji. Ma wiedzę o trendach rozwojowych i najistotniejszych osiągnięciach z zakresu informatyki śledczej. Rozumie potrzebę i zna możliwości ciągłego dokształcania się poprzez podnoszenie kompetencji zawodowych, osobistych i społecznych. Umie odnosić się krytycznie do pozyskiwanych informacji w kontekście pracy zawodowej. Rozumie konieczność przestrzegania zasad etyki zawodowej, kultury współpracy i konkurencji, jak również poszanowania różnorodności poglądów. Ma świadomość odpowiedzialności za pracę własną oraz zespołu, gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania.	Sposób weryfikacji osiągnięcia efektów uczenia się aktywne uczestnictwo w zajęciach, zaliczenie przedmiotów zgodnie z programem studiów, obrona pracy końcowej.	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Absolwent posiada wiedzę w zakresie prawa dowodowego dla dowodów elektronicznych. Potrafi pozyskiwać informacje z literatury, baz danych oraz innych właściwie dobranych źródeł, także w języku obcym, w zakresie informatyki śledczej. Potrafi integrować uzyskane informacje, dokonywać ich analizy i interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Potrafi zaprojektować sieć komputerową oraz właściwą strategię bezpieczeństwa, stosując właściwe metody. Potrafi posługiwać się narzędziami umożliwiającymi przetwarzanie i analizę obrazów cyfrowych, stosując właściwe metody i techniki. Ma umiejętność samokształcenia się. Potrafi posługiwać się technikami i narzędziami właściwymi do realizacji zadań związanych z ochroną danych. Potrafi dokonać krytycznej analizy sposobu funkcjonowania i ocenić przydatność poznanych metod i narzędzi służących do rozwiązania zadań oraz ma umiejętność wyboru i zastosowania właściwej metody i narzędzi.	Sposób weryfikacji osiągnięcia efektów uczenia się aktywne uczestnictwo w zajęciach, zaliczenie przedmiotów zgodnie z programem studiów, obrona pracy końcowej.	Prezentacja

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

Semestr I:

Lp.	Nazwa przedmiotu	Łączna liczba godzin	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	ECTS
1.	Podstawy sieci komputerowych [lab. CISCO]	**20**	10		10			2
2.	Bezpieczeństwo systemów komputerowych i sieci [pentesty]	**25**	10		15			3
3.	Techniczne aspekty bezpieczeństwa danych [wyciek danych]	**25**	10		15			3
4.	Aspekty prawne informatyki śledczej w Kodeksie Karnym	**16**	8		8			2
5.	Aspekty prawne informatyki śledczej w Kodeksie Cywilnym	**8**	8					1
6.	Informatyka śledcza	**25**	10		15			3
7.	Techniki analizy obrazu	**20**	10			10		2
8.	Techniki gromadzenia informacji z serwisów www [biały wywiad]	**25**	10		10	5		3

Łączna liczba godzin teoretycznych: 76

Łączna liczba godzin praktycznych: 88

ŁĄCZNA LICZBA PUNKT ECTS (SEM I): 19

Semestr II:

Lp.	Nazwa przedmiotu	Łączna liczba godzin	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	ECTS
1.	Techniki odzyskiwania danych	**14**	4		10			2
2.	Zabezpieczenie i analiza danych z urządzeń z urządzeń mobilnych	**24**	4		20			3

3.	Praca operacyjna z urządzeniami firmy Apple	**8**	4		4			1
4.	Kryptografia i steganografia	**20**	10		10			2
5.	Cyberbezpieczeństwo IoT, pozyskiwanie danych z systemów mikroprocesorowych	**14**	8		6			1
6.	Techniki pozyskiwania danych	**18**	8		10			2
7.	Wykrywanie i reagowanie na incydenty bezpieczeństwa	**18**	8		10			2
8.	Praca końcowa	**20**					20	4

Łączna liczba godzin teoretycznych: 46

Łączna liczba godzin praktycznych: 90

ŁĄCZNA LICZBA PUNKT ECTS (SEM II): 17

Harmonogram

Liczba przedmiotów/zajęć: 7

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 7 Bezpieczeństwo systemów komputerowych i sieci [pentesty]	Artur Kalinowski	10-10-2026	12:50	14:20	01:30	Tak
2 z 7 Techniki gromadzenia informacji z serwisów www [biały wywiad]	Tomasz Turba	10-10-2026	14:40	16:55	02:15	Tak
3 z 7 Aspekty prawne informatyki śledczej, KK	Tomasz Turba	11-10-2026	08:20	09:50	01:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
4 z 7 Aspekty prawne informatyki śledczej, KK	Tomasz Turba	11-10-2026	10:05	11:35	01:30	Tak
5 z 7 Techniki analizy obrazu	Tomasz Turba	11-10-2026	12:50	14:20	01:30	Tak
6 z 7 Techniki analizy obrazu	Tomasz Turba	11-10-2026	14:40	16:10	01:30	Tak
7 z 7 Podstawy sieci komputerowych	Tomasz Turba	11-10-2026	16:20	17:50	01:30	Tak

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 000,00 PLN
Koszt przypadający na 1 uczestnika netto	9 000,00 PLN
Koszt osobogodziny brutto	30,00 PLN
Koszt osobogodziny netto	30,00 PLN

Prowadzący

Liczba prowadzących: 4

1 z 4

dr hab. inż. Aleksandra Kawala-Sterniuk

Dawna wykładowczyni na Wydziale Informatyczno-Matematycznym (CMS School) londyńskiego University of Greenwich (2009-2013), a obecnie pracownik Politechniki Opolskiej
Posiada zdobyte w pewnej brytyjskiej firmie bogate praktyczne doświadczenie z zakresu wywiadu gospodarczego i białego wywiadu gospodarczego. Obecne zainteresowania badawcze: Sztuczna

inteligencja, przetwarzanie sygnałów biomedycznych, systemy wydobywania wiedzy (knowledge mining), systemy HCI.

2 z 4

Artur Kalinowski

Znamienity specjalista w zakresie bezpieczeństwa systemów teleinformatycznych, sieci oraz informacji, autor bestseleru „Metody inwigilacji i elementy informatyki śledczej”
Z wykształcenia i z zamiłowania informatyk, od wielu lat ściśle związany z praktycznymi aspektami bezpieczeństwa m.in. ochroną płatności on-line oraz przeprowadzaniem testów penetracyjnych. Były pracownik Izby Skarbowej i Izby Celnej, doświadczony dydaktyk. Początkowa fascynacja pisaniem wirusów i tworzeniem sieci komputerowych z czasem przerodziła się w chęć zabezpieczania systemów oraz analizy ich słabych punktów. Zdobyta wiedza i doświadczenie zaowocowały opracowaniem własnych metod uzyskiwania nieautoryzowanego dostępu do danych, jak również przejmowania kontroli nad systemami i sieciami komputerowymi. Autor wielu szkoleń z zakresu informatyki śledczej, bezpieczeństwa systemów i sieci oraz testów penetracyjnych. Moderator jednego z forów o tematyce IT security.

3 z 4

dr hab. Arkadiusz Lach, prof. UMK

Prodziekan i wykładowca Wydziału Prawa i Administracji UMK, Kierownik Katedry Postępowania Karnego i Centrum Badań nad Cyberprzestępczością Uniwersytetu Mikołaja Kopernika w Toruniu. Niezależny ekspert Komisji Europejskiej. Autor kilkudziesięciu opracowań naukowych, w tym monografii „Dowody elektroniczne w procesie karnym” (pierwszego w Polsce opracowania problematyki dowodowej uwzględniającego aspekty kryminalistyczne oraz informatyczne). W pracy naukowej specjalizuje się w prawnych zagadnieniach nowych technologii, nadużyciach w sieciach informatycznych, ochronie danych osobowych oraz europejskim prawie karnym.

4 z 4

Tomasz Turba

Swoją przygodę z bezpieczeństwem rozpoczynał od hackowania Amigi 500. Z wykształcenia administrator *nix. Autor kilku innowacyjnych szkoleń oraz posiadacz licznych certyfikatów (CCNA, CCNP, CCSP, MCP, MCSA, NSA NSTSSI 4011, JNCIA, Acunetix, Kali, IBM*, CISS). Prowadzi swoją działalność z zakresu przeprowadzania testów penetracyjnych oraz konsultacji zabezpieczeń. Entuzjasta adrenaliny (sporty walki, motocykle, spadochron), prowadzi anarchistycznego bloga pod adresem „tturba.pl”. Korespondent jednego z forów o tematyce IT security.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały przygotowane przez wykładowców w formie prezentacji, ćwiczeń zostaną udostępnione w trakcie zajęć. Podana zostanie również bibliografia do każdego przedmiotu.

Warunki uczestnictwa

Nie jest wymagane ukończenie studiów z informatyki, ale na pewno przyda się wiedza ze sprawnego poruszania się po systemach komputerowych i chęci poznawania komputera i innych urządzeń. Znajomość podstaw programowania, znajomość podstawowych pojęć z zakresu komputerów będzie dużym ułatwieniem.

Elektroniczna rekrutacja w systemie IRK https://irk.po.edu.pl/pl

Informacje dodatkowe

Organizator zastrzega sobie prawo do zmiany harmonogramu zajęć.

Zajęcia realizowane są w godzinach dydaktycznych (tj. po 45 minut), przerwy nie są wliczone w czas trwania usługi rozwojowej.

Zajęcia odbywają się w trybie hybrydowym.

Uczestnik ma obowiązek uczestniczyć w 80% zajęć i uzyskać wymaganych programem zaliczeń.

Studia podyplomowe trwają dwa semestry.

Potwierdzeniem ukończenia studiów podyplomowych jest świadectwo ukończenia studiów podyplomowych.

Szczegółowy plan zostanie podany w terminie późniejszym.

Warunki techniczne

1) komputer z dostępem do internetu, kamerą, mikrofonem;

2) łącze internetowe o przepustowości wystarczającej do wideokonferencji;

3) systemy operacyjne Windows 10 lub nowszy;

4) oprogramowanie: Firefox, Chrome, dowolny pakiet biurowy.

Adres

Opole 76/3
45-758 Opole
woj. opolskie

Zajęcia odbywają się w pracowniach i laboratoriach Wydziału Informatyki Politechniki Opolskiej.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Anna Czabak

E-mail a.czabak@po.edu.pl
Telefon (+48) 774 498 169