Możliwość dofinansowania

Cyberbezpieczeństwo - Studia podyplomowe - Collegium Da Vinci

Numer usługi 2025/06/13/9743/2814704

8 650,00 PLN brutto
8 650,00 PLN netto
43,25 PLN brutto/h
43,25 PLN netto/h

Collegium Da Vinci z siedzibą w Poznaniu

★★★★½

zdalna w czasie rzeczywistym
Studia podyplomowe
200 h
25.10.2025 do 31.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Studia adresowane są dla: • absolwentów i absolwentek różnych kierunków studiów wyższych, szczególnie informatycznych i pokrewnych • pracowników i pracowniczek branży IT, chcących specjalizować się w obszarze cyberbezpieczeństwa • administratorów i administratorek systemów, programistów i programistek oraz analityków i analityczek IT • kadry zarządzającej oraz specjalistów i specjalistek bezpieczeństwa • przedstawicieli i przedstawicielek firm i organizacji odpowiedzialnych za zgodność z regulacjami (np. RODO) oraz ochronę infrastruktury cyfrowej • osób z podstawową wiedzą informatyczną (systemy operacyjne, sieci, analiza danych, chmura obliczeniowa, programowanie; znajomość platformy Azure, Microsoft 365 i Windows 10/11)
Minimalna liczba uczestników	25
Maksymalna liczba uczestników	27
Data zakończenia rekrutacji	30-09-2025
Forma prowadzenia usługi	zdalna 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 2023 r. poz. 742, z późn. zm.)

Zakres uprawnień	Studia podyplomowe

Cel

Cel edukacyjny

Celem studiów podyplomowych na kierunku Cyberbezpieczeństwo jest projektowanie strategii bezpieczeństwa IT dla organizacji, monitorować ruchy sieciowe i wykrywać zagrożenia w czasie rzeczywistym, analizować incydenty bezpieczeństwa i reagować na nie oraz przygotowywać raporty z audytów bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętność przygotowania raportów z audytów bezpieczeństwa	Raportuje jasny opis stanu zabezpieczeń, identyfikuje lukę oraz ocenia ryzyko	Obserwacja w warunkach symulowanych
Projektowanie strategii bezpieczeństwa IT dla organizacji	Opracowuje rozwiązania, które są spójne, jasne, realistyczne i możliwe do wdrożenia	Obserwacja w warunkach symulowanych
Monitorowanie ruchu sieciowego i wykrywanie zagrożeń w czasie rzeczywistym	Identyfikuje anomalie w ruchu sieciowym oraz rozpoznaje typowe wzorce ataków	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Dokument potwierdzający uzyskanie kompetencji, czyli świadectwo ukończenia studiów podyplomowych zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Studia podyplomowe

Studia podyplomowe trwają 9 miesięcy (200 godzin dydaktycznych po 45 min.). Zajęcia są realizowane w trakcie 10 zjazdów, w trybie sobota – niedziela (w godz. 8.30 – 17.00).

Zastrzegamy sobie możliwość zmiany formy zajęć 24 h przed rozpoczęciem danego spotkania.

W harmonogramie studiów uwzględniono przerwy między zajęciami, które trwają od 5 do 30 minut.

Program

Cyberbezpieczeństwo - dziś i jutro (20 godz.)

- Wstęp. Definicja cyberprzestrzeni i cyberbezpieczeństwa, aktualne trebdy na świecie
- Typy ataków hakerskich - demonstracje wraz z objaśnieniem metody ochrony
- Dobre praktyki, formy obrony przed atakami
- Rozwój kompetencji z zakresu bezpieczeństwa
- Dlaczego bezpieczeństwo to nie tylko departament

Cyberbezpieczeństwo w systemach operacyjnych (10 godz.)

- Wprowadzenie do bezpieczeństwa systemów operacyjnych
- Bezpieczeństwo systemu Windows
- Bezpieczeństwo systemu Linux
- Bezpieczeństwo w systemie MacOS
- Dobre praktyki bezpieczeństwa

Informatyka śledcza (30 godz.)

- Teoria (podstawy i proces informacji śledczej)
- Przegląd aktów prawnych i standardów dotyczących informacji śledczej
- Proces informatyki śledczej
- Zabezpieczanie dowodów cyfrowych
- Analiza danych cyfrowych
- Analiza sieciowa
- Analiza malware
- Informatyka śledcza w chmurze
- Śledztwa w mediach społecznościowych - OSINT
- Warsztaty - symulacja zabezpieczenia miejsca zdarzenia
- Warsztaty - analiza danych cyfrowych
- Warsztaty - analiza sieciowa i malware
- Analiza rzeczywistych przypadków śledczych

Warsztaty z CompTIA Security+ (40 godz.)

- Podstawowe koncepcje bezpieczeństwa
- Porównanie różnych typów zagrożeń
- Omówienie podstawowych pojęć kryptografii
- Wdrażanie zarządzania tożsamością i kontrola dostępu
- Zabezpieczanie architektury sieci korporacyjnej
- Zabezpieczanie architektury sieci w usługach chmurowych
- Omówienie koncepcji odporności
- Zarządzanie podatności
- Bezpieczeństwo sieciowe
- Ocena bezpieczeństwa punktóww końcowych
- Wdrażanie zabezpieczeńs aplikacji
- Zarządzanie incydentem i monitorowanie środowiska
- Po czym rozpoznać atak - wskaźnik kompromitacji
- Zarządzani bezpieczeństwem w organizacji poprzez polityki, standardy i procedury
- Podstawowe pojęcia związane zarządzania ryzykiem
- Ochrona danych i dbałość o ich zgodność w organizacji

Microsoft Security, Compliance and Identity Fundamentals. Przygotowanie do egzaminu (30 godz.)

- Podstawowe pojęcia dotyczące bezpieczeństwa, zgodność i tożsamości
- Koncepcje i możliwości rozwiązań firmy Microsoft do zarządzania tożsamością i dostępem
- Możliwości rozwiązań zabezpieczających firmy Microsoft
- Możliwości rozwiązań Microsoft zapewniających zgodność
- Warsztat przygotowujący do egzaminu

Microsoft Security Operations Analyst (30 godz.)

- Ograniczanie zagrożenia za pomocą usługi Microsoft 365 Defender
- Ograniczanie zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych
- Ograniczanie zagrożenia za pomocą usługi Microsoft Defender for Cloud
- Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language
- Konfiguracja środowiska Microsoft Sentinel
- Łączenie dzienników z Microsoft Sentinel
- Wykrywanie i prowadzenie dochodzenia przy użyciu probgramu Microsoft Sentinel
- Polowanie na zagrożenia w Microsoft Sentinel

RODO (10 godz.)

- Wprowadzenie do RODO (GDPR) i gejo znaczenie w cyberbezpieczeństwie
- [Przetwarzanie danych osobowych i odpowiedzialność w kontekście technologicznym
- Zabezpieczenia techniczne i organizacyjne zgodnie z RODO
- Zarządzanie incydentami naruszenia danych i informatyka śledcza
- Zgodność z RODO w systemach AI i automatyzacji procesów
- Podsumowanie, sesja pytań i odpowiedzi oraz quiz sprawdzający

Bezpieczeństwo aplikacji webowych (20 godz.)

- Wprowadzanie do bezpieczeństwa aplikacji webowych
- Bezpieczeństwo ruchu sieciowego (TLS.SSL, nagłówki HTTP, Same-Origin Policy i Cross-Origin Resource Sharing)
- Narzędzia (analiza ruchu sieciowego, manipulacja zapytaniami HHTP, tworzenie własnych skryptów, skanery podatności)
- Analiza podatności (atak, obrona, przykład)
  - Bezpieczeństwo API
  - Czarnoskrzynkowy test penetracyjny (CTF)

Bezpieczeństwo Copilot (10 godz.)

- Badanie projektu Copilot dla Microsoft 365
- Wdrażanie Copilot dla Microsoft 365
- Badanie bezpieczeństwa danych i zgodność w Copilot dla Microsoft 365
- Zarządzanie bezpiecznych dostępem użytkowników w Microsoft 365
- Zarządzanie rolami i grupami ról w Microsoft 365
- Eksploracja wywiadu zagrożeń w Microsoft Defender XDR

Zaliczenie

Warunkiem ukończenia studiów podyplomowych Cyberbezpieczeństwo jest uzyskane pozytywnego wyniku z dwóch egzaminów semestralnych. Egzaminy przewidziano na koniec każdego semestru w formie testu wyboru.

Absolwenci uzyskują, zgodne z wymogami ustawy, świadectwo ukończenia studiów podyplomowych w Collegium Da Vinci.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 650,00 PLN
Koszt przypadający na 1 uczestnika netto	8 650,00 PLN
Koszt osobogodziny brutto	43,25 PLN
Koszt osobogodziny netto	43,25 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

Piotr Wichrań

Doświadczony, wieloletni trener z zakresu Cybersecurity oraz Bezpieczeństwa Informacji.
Brał udział w wielu audytach bezpieczeństwa IT, szacowaniu ryzyka w dużych i średnich firmach, co pretenduje go do przekazywania wiedzy z obszaru Normy ISO 27000. Działa jako biegły sadowy z zakresu informatyki śledczej (wydanych ponad 2000 opinii sądowych), jest licencjonowanym detektywem.

Podczas swojej pracy spotyka się z ciekawymi przypadkami, złożonymi problemami, którymi dzieli się podczas szkoleń z Informatyki Śledczej Forensics. Najbardziej ceni sobie projekty szkoleniowe oparte o przykłady wzięte z życia z zakresu Cybersecurity, jednocześnie ściśle związane z rozwojem niezbędnych na co dzień umiejętności.

2 z 2

Rafał Wójcik

Pasjonat bezpieczeństwa, którą stara się realizować w każdej wolnej chwili. Po pracy można znaleźć go na różnych CTF-ach, Hackthebox, Tryhackme albo siedzącego przy książkach. Posiada doświadczenie niekomercyjne jak i komercyjne: – TryHackMe z wysokim miejscem (Top 15 w Polsce) – HackTheBox – Top 6 w Polsce – Proving Grounds od Offensive Security – 3 miejsce na świecie – Dodatkowo wiele platform takich jak PentesterLab, PortSwigger niema rankingu, a w których mam zrobione większość ćwiczeń. Rozwiązuje CTF jako członek zespołu Unicorns of Security,

Interesuje się cyberbezpieczeństwem. W szczególności bezpieczeństwem aplikacji webowych oraz mobilnych. Gram CTFy, a wolnym czasie jestem też Bug Hunterem.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne zamieszczane są przez wykładowców w Wirtualnej Uczelni w formie prezentacji, materiałów PDF, zdjęć oraz linków.

Warunki uczestnictwa

Warunkiem uczestnictwa jest:

- **podsiadanie dyplomu ukończonych studiów wyższych I lub II stopnia.**
- zapisanie się na studia poprzez formularz rekrutacyjny **rekrutacja.cdv.pl** (UWAGA: wypełnienie samego formularza rekrutacyjnego nie jest równoznaczne z zapisaniem się na studia)
- podpisanie umowy online oraz załączenie skanu dyplomu ukończenia studiów wyższych (lic., inż., mgr)
- **przed zapisaniem się na studia podyplomowe proszę o kontakt telefoniczny/mailowy podyplomowe@cdv.pl tel. 697 230 138.**

Informacje dodatkowe

Przed zapisaniem się na studia podyplomowe proszę o kontakt telefoniczny/mailowy **podyplomowe@cdv.pl tel. 697 230 138**.

Zapraszam na stronę internetową https://cdv.pl/studia-podyplomowe/it/akademia-programowania-w-pythonie/ ,gdzie szczegółowo przedstawiamy KADRĘ, PARTNERÓW oraz PROGRAM.

Warunki techniczne

Zajęcia realizowane zdalnie, to usługi odbywające się z wykorzystaniem połączeń on-line, realizowane w czasie rzeczywistym, w formie umożliwiającej zrealizowanie opisanego zakresu usługi, jej celów i zadeklarowanych rezultatów. Zajęcia realizowane w formie zdalnej odbywają się przy użyciu platformy GOOGLE MEET, TEAMS lub ZOOM. Link umożliwiającego uczestnictwo w spotkaniu on-line jest ważny tylko w trakcie zaplanowanych zajęć i przesyłany za pomocą wewnętrznego systemu (Wirtualna Uczelnia) do komunikacji pomiędzy Słuchaczem studiów podyplomowych, a Collegium Da Vinci.

1. Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie (np. Smartphone) do zdalnej komunikacji: Dwurdzeniowy procesor Intel Core i5 2,5 GHz i wyższy. Sprzęt komputerowy powinien być wyposażony w głośnik, kamerę i mikrofon.

2. Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: pobieranie: 10 Mb/s, wysyłanie: 5 Mb/s)

3. Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: informacje przekażemy na pierwszych zajęciach. Aby wziąć udział w szkoleniu online potrzebny jest komputer, laptop.

Kontakt

Izabella Bekas-Kwaśniewska

E-mail izabella.bekas-kwasniewska@cdv.pl

Telefon (+48) 697 230 138