Możliwość dofinansowania

Społeczna Akademia Nauk z siedzibą w Łodzi

4,6 / 5

21 ocen

Cyberbezpieczeństwo z elementami metodyki zwalczania przestępczości w cyberprzestrzeni- studia podyplomowe

Numer usługi 2026/02/03/14038/3303736

Łódź

Studia podyplomowe

mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

180:00 h

17.10.2026 do 30.06.2027

7 500,00 PLN brutto

7 500,00 PLN netto

41,67 PLN brutto/h

41,67 PLN netto/h

Informacje podstawowe

Kategoria	Inne / Edukacja
Grupa docelowa usługi	Osoby z dyplomem magistra lub licencjata, absolwenci kierunków: bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, informatyka, prawo, administracja, zarządzanie i inne. Osoby zainteresowane bezpieczeństwem cyfrowym, pracujące lub wykonujące zadania w środowisku wirtualnym, urzędnicy państwowi lub samorządowi, osoby gromadzące lub przetwarzające dane osobowe lub inne dane istotne, osoby odpowiadające za bezpieczeństwo obiektów, żołnierze i funkcjonariusze, osoby zainteresowane służbą w formacjach mundurowych, wszyscy zainteresowani bezpieczeństwem osobistym, bezpieczeństwem organizacji i państwa. Kandydat powinien posiadać przygotowanie wykraczające poza standardową obsługę komputera, winien znać podstawy zachowania sieciowego i przechowywania danych, mieć wiedzę i umiejętności na poziomie systemów operacyjnych, znać budowę sieci komputerowych i podstaw konfiguracji.
Minimalna liczba uczestników	20
Maksymalna liczba uczestników	40
Data zakończenia rekrutacji	12-10-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	180

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

Kierunek ten pozwala zdobyć praktyczne i aktualne kompetencje z zakresu bezpieczeństwa cyfrowego, ochrony informacji oraz przeciwdziałania cyberprzestępczości. Absolwent studiów zyskuje wiedzę i umiejętności niezbędne do skutecznego działania w środowisku zawodowym i prywatnym – zwiększając swoją atrakcyjność na rynku pracy oraz realne szanse na awans zawodowy w sektorach IT, administracji publicznej, służbach mundurowych czy firmach technologicznych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
posiada wiedzę z podstaw funkcjonowania systemów cyberbezpieczeństwa oraz kluczowych przepisów prawa i zasad bezpieczeństwa cyfrowego: - zrozumienie krajowego i europejskiego systemu cyberbezpieczeństwa; - znajomość przepisów prawa dotyczących cyberprzestępczości, ochrony danych i reagowania na incydenty; - umiejętność rozpoznawania zagrożeń oraz reagowania na incydenty w środowisku cyfrowym, - świadomość zagrożeń dla użytkowników i organizacji – od ataków phishingowych po ransomware.	Wiedza weryfikowana jest podczas wykonywania studiów przypadków, a umiejętności utrwalane w trakcie wykonywania zleconych zadań. Zasady zaliczenia studiów: - zaliczenie przedmiotów przewidzianych w programie studiów, - zaliczenie egzaminu teoretycznego i praktycznego.	Test teoretyczny
		Prezentacja
		Debata swobodna
posiada praktyczne umiejętności techniczne niezbędne w pracy specjalisty ds. cyberbezpieczeństwa: - konfiguracja i zarządzanie zaporami sieciowymi (firewall), - obsługa urządzeń odpowiadających za bezpieczeństwo sieci IT, - przeprowadzanie testów bezpieczeństwa (penetracyjnych) sieci i aplikacji, - analiza logów i identyfikacja śladów ataków, - rozpoznawanie podatności w systemach lokalnych i chmurowych.	Wiedza weryfikowana jest podczas wykonywania studiów przypadków, a umiejętności utrwalane w trakcie wykonywania zleconych zadań. Zasady zaliczenia studiów: - zaliczenie przedmiotów przewidzianych w programie studiów, - zaliczenie egzaminu teoretycznego i praktycznego.	Test teoretyczny
		Prezentacja
		Debata swobodna

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
potrafi korzystać z profesjonalnych narzędzi i środowisk pracy wykorzystywanych w branży: - obsługa systemów Microsoft Security, Cisco, Palo Alto oraz innych rozwiązań ochrony, - analiza ryzyka, projektowanie i wdrażanie zabezpieczeń infrastruktury IT, - rozwiązywanie rzeczywistych problemów z zakresu bezpieczeństwa danych i systemów, - prowadzenie podstawowych dochodzeń wewnętrznych w organizacji (incident response, dokumentacja, rekomendacje).	Wiedza weryfikowana jest podczas wykonywania studiów przypadków, a umiejętności utrwalane w trakcie wykonywania zleconych zadań. Zasady zaliczenia studiów: - zaliczenie przedmiotów przewidzianych w programie studiów, - zaliczenie egzaminu teoretycznego i praktycznego.	Test teoretyczny
		Prezentacja
		Debata swobodna

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

Efekty kształcenia – konkretna wiedza i realne umiejętności zawodowe:

Kompetencje ogólne

Poznasz podstawy funkcjonowania systemów cyberbezpieczeństwa oraz kluczowe przepisy prawa i zasady bezpieczeństwa cyfrowego:

- zrozumienie krajowego i europejskiego systemu cyberbezpieczeństwa,
- znajomość przepisów prawa dotyczących cyberprzestępczości, ochrony danych i reagowania na incydenty,
- umiejętność rozpoznawania zagrożeń oraz reagowania na incydenty w środowisku cyfrowym,
- świadomość zagrożeń dla użytkowników i organizacji – od ataków phishingowych po ransomware.

Kompetencje techniczne

Zdobędziesz praktyczne umiejętności techniczne niezbędne w pracy specjalisty ds. cyberbezpieczeństwa:

- konfiguracja i zarządzanie zaporami sieciowymi (firewall),
- obsługa urządzeń odpowiadających za bezpieczeństwo sieci IT,
- przeprowadzanie testów bezpieczeństwa (penetracyjnych) sieci i aplikacji,
- analiza logów i identyfikacja śladów ataków,
- rozpoznawanie podatności w systemach lokalnych i chmurowych.

Umiejętności praktyczne

Nauczysz się korzystać z profesjonalnych narzędzi i środowisk pracy wykorzystywanych w branży:

- obsługa systemów Microsoft Security, Cisco, Palo Alto oraz innych rozwiązań ochrony,
- analiza ryzyka, projektowanie i wdrażanie zabezpieczeń infrastruktury IT,
- rozwiązywanie rzeczywistych problemów z zakresu bezpieczeństwa danych i systemów,
- prowadzenie podstawowych dochodzeń wewnętrznych w organizacji (incident response, dokumentacja, rekomendacje).

Uczelnia zastrzega sobie prawo do zmian w programie oraz harmonogramie usługi.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	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	7 500,00 PLN
Koszt przypadający na 1 uczestnika netto	7 500,00 PLN
Koszt osobogodziny brutto	41,67 PLN
Koszt osobogodziny netto	41,67 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

dr Anna Rycaj- Pilipczuk

funkcjonariusz Policji, specjalista zagadnień prawnych i administracyjnych

2 z 2

mgr Andrzej Kokociński

informatyk, specjalista bezpieczeństwa chmurowego, trener Microsoft Security Academy, Cisco Networking Academy , Palo Alto Network Cybersecurity Academy

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy studiów podyplomowych Cyberbezpieczeństwo z elementami metodyki zwalczania przestępczości w cyberprzestrzeni otrzymają dostęp do materiałów przygotowanych przez specjalistyczne platformy szkoleniowe: Microsoft Security Academy, Cisco Networking Academy , Palo Alto Network Cybersecurity Academy.

Warunki uczestnictwa

Rekrutacji na studia podyplomowe Cyberbezpieczeństwo z elementami metodyki zwalczania przestępczości w cyberprzestrzeni dokonuje się poprzez założenie konta w systemie rekrutacyjnym na stronie www.e-rekrutacja.san.edu.pl.

System rekrutacyjny Uczelni zostanie uruchomiony od 01.05.2026 r.

Po założeniu i zalogowaniu się do swojego konta kandydata należy:

- uzupełnić swoje dane,
- wybrać kierunek studiów podyplomowych,
- dodać zdjęcie w formacie dowodowym- 35 mm x 45 mm (szerokość x wysokość),
- uiścić opłatę wpisową w wysokości 100 zł,
- dodać dokumenty i podpisać umowę.

W terminie 7 dni od daty rekrutacji należy dostarczyć oryginały wymaganych dokumentów do Biura Rekrutacji w Łodzi lub Warszawie.

Warunki techniczne

Zajęcia odbywają się przez aplikację Microsoft TEAMS.

WYMAGANIA SPRZĘTOWE DLA ZESPOŁÓW NA KOMPUTERZE Z SYSTEMEM WINDOWS

Wymagania dotyczące komponentów

Komputer i procesor Minimum 1,1 GHz lub szybszy, 2 rdzenie Uwaga: w przypadku procesorów Intel należy wziąć pod uwagę maksymalną prędkość osiągniętą przy użyciu technologii Intel Turbo Boost (maksymalna częstotliwość Turbo)

Pamięć 4,0 GB RAM (zespoły wymagają dedykowanych 4 GB pamięci RAM ponad wszelkie inne wymagania systemowe)

Dysk twardy 3,0 GB dostępnego miejsca na dysku

Wyświetl rozdzielczość ekranu 1024 x 768

Sprzęt graficzny System operacyjny Windows: Przyspieszenie sprzętowe grafiki wymaga DirectX 9 lub nowszego, z WDDM 2.0 lub nowszym dla Windows 10 (lub WDDM 1.3 lub nowszym dla Windows 10 Fall Creators Update)

System operacyjny Windows 10 (z wyłączeniem Windows 10 LTSC), Windows 10 na ARM, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2. Uwaga: zalecamy korzystanie z najnowszej wersji systemu Windows i dostępnych poprawek zabezpieczeń.

Wersja .NET Wymaga środowiska CLR .NET 4.5 lub nowszego

Wideo Kamera wideo USB 2.0

Urządzenia Standardowa kamera laptopa, mikrofon i głośniki

Rozmowy wideo i spotkania Wymaga procesora 2-rdzeniowego. Aby uzyskać wyższą rozdzielczość wideo/współdzielenia ekranu i liczbę klatek na sekundę, zalecany jest procesor 4-rdzeniowy lub lepszy.

Efekty wideo w tle wymagają systemu Windows 10 lub procesora z zestawem instrukcji AVX2.

Zobacz Zalecenia dotyczące dekodera sprzętowego i sterownika kodera, aby uzyskać listę nieobsługiwanych dekoderów i koderów.

Dołączanie do spotkania przy użyciu wykrywania bliskości w Microsoft Teams Room wymaga Bluetooth LE, który wymaga włączenia Bluetooth na urządzeniu klienckim, a w przypadku klientów Windows wymaga również 64-bitowego klienta Teams. Ta funkcja nie jest dostępna w 32-bitowych klientach usługi Teams.

Wydarzenia Teams na żywo Jeśli tworzysz wydarzenie Teams na żywo, zalecamy użycie komputera z procesorem Core i5 Kaby Lake, 4,0 GB pamięci RAM (lub nowszej) i koderem sprzętowym. Zobacz Zalecenia dotyczące dekodera sprzętowego i sterownika kodera, aby uzyskać listę nieobsługiwanych dekoderów i koderów.

Wymagania dla aplikacji Teams na urządzeniach mobilnych

Z usługi Teams możesz korzystać na tych platformach mobilnych:

Android: kompatybilny z telefonami i tabletami z Androidem.

Wsparcie jest ograniczone do czterech ostatnich głównych wersji Androida. Na przykład po wydaniu nowej, głównej wersji systemu Android wymaganiem systemu Android jest nowa wersja i trzy najnowsze wersje, które ją poprzedzają.

iOS: kompatybilny z iPhonem, iPadem i iPodem touch.

Wsparcie jest ograniczone do dwóch najnowszych głównych wersji systemu iOS. Na przykład po wydaniu nowej, głównej wersji systemu iOS wymaganiem systemu iOS jest nowa wersja i najnowsze wersje, które ją poprzedzały. Opcjonalny efekt wideo Rozmyj moje tło w systemie iOS wymaga systemu operacyjnego iOS 12 lub nowszego, zgodnego z następującymi urządzeniami: iPhone 7 lub nowszy, iPad 2018 (6. generacji) lub nowszy oraz iPod touch 2019 (7. generacji).

WYMAGANIA SPRZĘTOWE DLA ZESPOŁÓW NA MAC

Wymagania dotyczące komponentów Komputer i procesor Procesor Intel Core Duo

Pamięć 4,0 GB RAM (zespoły wymagają dedykowanych 4 GB pamięci RAM ponad wszelkie inne wymagania systemowe)

Dysk twardy 1,5 GB wolnego miejsca na dysku

Wyświetlacz o rozdzielczości 1280 x 800 lub wyższej

System operacyjny Jedna z trzech najnowszych wersji systemu macOS.

Kamera internetowa kompatybilna z wideo

Mikrofon i głośniki zgodne z funkcją Voice, zestaw słuchawkowy z mikrofonem lub równoważne urządzenie

Rozmowy wideo i spotkania Wymaga procesora 2-rdzeniowego. Aby uzyskać wyższą rozdzielczość wideo/współdzielenia ekranu i liczbę klatek na sekundę, zalecany jest procesor 4-rdzeniowy lub lepszy.

Dołączanie do spotkania przy użyciu wykrywania zbliżenia w pokoju Microsoft Teams nie jest dostępne w systemie macOS.

Adres

ul. Jana Kilińskiego 98
90-011 Łódź
woj. łódzkie

Kontakt

Mirosław Olszewski

E-mail molszewski@san.edu.pl

Telefon (+48) 447 884 622