Możliwość dofinansowania

Uniwersytet SWPS

Uniwersytet SWPS

Studia podyplomowe WARSZAWA: Specjalista ds. cyberbezpieczeństwa

Numer usługi 2024/11/05/14313/2396214

10 900,00 PLN brutto
10 900,00 PLN netto
56,77 PLN brutto/h
56,77 PLN netto/h

zdalna w czasie rzeczywistym
Studia podyplomowe
192 h
16.11.2024 do 29.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Studia rekomendowane są dla osób początkujących lub średnio zaawansowanych w obszarze cyberbezpieczeństwa, szczególnie dla tych którzy pracują i zarządzają zespołem w obszarach IT.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	15-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	192
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 jest zdobycie wiedzy i doskonalenie kompetencji w zarządzaniu cyberbezpieczeństwem. Studia mają charakter przekrojowy, obejmujący szerokie spektrum zagadnień cyberbezpieczeństwa. Wszystkie zagadnienia nauczane są od podstaw przygotowując studentów do zarządzania cyberbezpieczeństwem w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Podniesienie kwalifikacji jako specjalista ds. cyberbezpieczeństwa i zdobędziesz kluczowe kompetencje menedżerskie.	Zgodność z celami i standardami: Sprawdzenie, czy osiągnięcia osoby studiującej są zgodne z wcześniej określonymi celami edukacyjnymi i standardami nauczania. Jasność i precyzja: Ocenianie czy osiągnięcia osoby studiującej są jasne, konkretne i precyzyjne, czyli czy pokazują rzeczywiste zrozumienie i opanowanie materiału. Zastosowanie w praktyce: Ocena zdolności osoby studiującej do zastosowania nabytej wiedzy i umiejętności w praktycznych sytuacjach lub zadaniach. Interakcja i komunikacja: Analiza umiejętności osoby studiującej w komunikacji i współpracy z innymi, zarówno w kontekście edukacyjnym, jak i społecznym.	Prezentacja
Poznanie nowoczesnych sposobów zarządzania cyberbezpieczeństwem, metody ataku i obrony infrastruktury IT oraz narzędzia białego wywiadu.	Zgodność z celami i standardami: Sprawdzenie, czy osiągnięcia osoby studiującej są zgodne z wcześniej określonymi celami edukacyjnymi i standardami nauczania. Jasność i precyzja: Ocenianie czy osiągnięcia osoby studiującej są jasne, konkretne i precyzyjne, czyli czy pokazują rzeczywiste zrozumienie i opanowanie materiału. Zastosowanie w praktyce: Ocena zdolności osoby studiującej do zastosowania nabytej wiedzy i umiejętności w praktycznych sytuacjach lub zadaniach. Interakcja i komunikacja: Analiza umiejętności osoby studiującej w komunikacji i współpracy z innymi, zarówno w kontekście edukacyjnym, jak i społecznym.	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętność reagowania na incydenty, przeprowadzanie testów penetracyjnych, rozpoznawanie dezinformacji i manipulacji medialnej.	Zgodność z celami i standardami: Sprawdzenie, czy osiągnięcia osoby studiującej są zgodne z wcześniej określonymi celami edukacyjnymi i standardami nauczania. Jasność i precyzja: Ocenianie czy osiągnięcia osoby studiującej są jasne, konkretne i precyzyjne, czyli czy pokazują rzeczywiste zrozumienie i opanowanie materiału. Zastosowanie w praktyce: Ocena zdolności osoby studiującej do zastosowania nabytej wiedzy i umiejętności w praktycznych sytuacjach lub zadaniach. Interakcja i komunikacja: Analiza umiejętności osoby studiującej w komunikacji i współpracy z innymi, zarówno w kontekście edukacyjnym, jak i społecznym.	Prezentacja
Poznane technologii bezpieczeństwa firmy Microsoft.	Zgodność z celami i standardami: Sprawdzenie, czy osiągnięcia osoby studiującej są zgodne z wcześniej określonymi celami edukacyjnymi i standardami nauczania. Jasność i precyzja: Ocenianie czy osiągnięcia osoby studiującej są jasne, konkretne i precyzyjne, czyli czy pokazują rzeczywiste zrozumienie i opanowanie materiału. Zastosowanie w praktyce: Ocena zdolności osoby studiującej do zastosowania nabytej wiedzy i umiejętności w praktycznych sytuacjach lub zadaniach. Interakcja i komunikacja: Analiza umiejętności osoby studiującej w komunikacji i współpracy z innymi, zarówno w kontekście edukacyjnym, jak i społecznym.	Prezentacja

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętność skutecznego zabezpieczenia systemu Windows i Linux.	Zgodność z celami i standardami: Sprawdzenie, czy osiągnięcia osoby studiującej są zgodne z wcześniej określonymi celami edukacyjnymi i standardami nauczania. Jasność i precyzja: Ocenianie czy osiągnięcia osoby studiującej są jasne, konkretne i precyzyjne, czyli czy pokazują rzeczywiste zrozumienie i opanowanie materiału. Zastosowanie w praktyce: Ocena zdolności osoby studiującej do zastosowania nabytej wiedzy i umiejętności w praktycznych sytuacjach lub zadaniach. Interakcja i komunikacja: Analiza umiejętności osoby studiującej w komunikacji i współpracy z innymi, zarówno w kontekście edukacyjnym, jak i społecznym.	Prezentacja

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 2. Czy dokument został wydany przez organy władz publicznych lub samorządów zawodowych na podstawie ustawy lub rozporządzenia?

Świadectwo ukończenia studiów podyplomowych zgodne z przepisami określonymi w Ustawie z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce.

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnionych do wydawania dokumentów potwierdzających uzyskanie kwalifikacji, w tym w zawodzie
Nazwa/Kategoria Podmiotu prowadzącego walidację	Uniwersytet SWPS
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa/Kategoria Podmiotu certyfikującego	Uniwersytet SWPS
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

PLAN STUDIÓW

Bezpieczeństwo użytkownika w cyberprzestrzeni (metodyka RESILIA)

- RESILIA™ Foundation – szkolenie akredytowane z egzaminem

Normalizacja i certyfikacja w bezpieczeństwie informacyjnym

- Normy i standardy w cyberbezpieczeństwie
- Audyty bezpieczeństwa

Bezpieczeństwo defensywne

- Wprowadzenia do bezpieczeństwa infrastruktury IT
- Inżynieria bezpieczeństwa
- Reakcja na incydenty
- Testy penetracyjne
- Bezpieczeństwo aplikacji internetowych

Systemy serwerowe

- BW10 - Bezpieczeństwo systemu Windows 10
- Bezpieczeństwo w systemach Linux

Certyfikowany egzamin RESILIA™ Foundation jest wliczony w cenę studiów.

Harmonogram

Liczba przedmiotów/zajęć: 26

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 Audyty bezpieczeństwa	16-11-2024	09:00	16:00	07:00
2 z 26 Audyty bezpieczeństwa	17-11-2024	09:00	16:00	07:00
3 z 26 Normy i standardy w cyberbezpieczeństwie	07-12-2024	09:00	16:00	07:00
4 z 26 Microsoft Security, Compliance, and Identity Fundamentals	08-12-2024	09:00	16:00	07:00
5 z 26 Przygotowanie do egzaminu SC-900: Security Fundamentals	18-01-2025	09:00	16:00	07:00

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 26 Microsoft Azure Security Technologies	19-01-2025	09:00	16:00	07:00
7 z 26 Microsoft Azure Security Technologies	01-02-2025	09:00	16:00	07:00
8 z 26 Microsoft Azure Security Technologies	02-02-2025	09:00	16:00	07:00
9 z 26 Microsoft Azure Security Technologies	22-02-2025	09:00	16:00	07:00
10 z 26 Bezpieczeństwo systemu Windows 11	23-02-2025	09:00	16:00	07:00
11 z 26 Bezpieczeństwo systemu Windows 11	08-03-2025	09:00	16:00	07:00
12 z 26 Bezpieczeństwo systemu Windows 11	09-03-2025	09:00	16:00	07:00
13 z 26 Bezpieczeństwo systemu Windows 11	09-03-2025	09:00	16:00	07:00
14 z 26 Bezpieczeństwo w systemach Linux	22-03-2025	09:00	16:00	07:00
15 z 26 Bezpieczeństwo w systemach Linux	23-03-2025	09:00	16:00	07:00
16 z 26 Bezpieczeństwo w systemach Linux	05-04-2025	09:00	16:00	07:00
17 z 26 Bezpieczeństwo w systemach Linux	06-04-2025	09:00	16:00	07:00
18 z 26 Wprowadzenia do bezpieczeństwa infrastruktury IT	27-04-2025	09:00	16:00	07:00

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 26 Inżynieria bezpieczeństwa	10-05-2025	09:00	16:00	07:00
20 z 26 Inżynieria bezpieczeństwa	11-05-2025	09:00	16:00	07:00
21 z 26 Reakcja na incydenty	24-05-2025	09:00	16:00	07:00
22 z 26 Reakcja na incydenty	25-05-2025	09:00	16:00	07:00
23 z 26 Testy penetracyjne sieci	14-06-2025	09:00	16:00	07:00
24 z 26 Testy penetracyjne sieci	15-06-2025	09:00	16:00	07:00
25 z 26 Bezpieczeństwo aplikacji internetowych	28-06-2025	09:00	16:00	07:00
26 z 26 Bezpieczeństwo aplikacji internetowych	29-06-2025	09:00	16:00	07:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	10 900,00 PLN
Koszt przypadający na 1 uczestnika netto	10 900,00 PLN
Koszt osobogodziny brutto	56,77 PLN
Koszt osobogodziny netto	56,77 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: 2

1 z 2

Marcin Wiktorowicz

Trener Altkom Akademii z wieloletnią praktyką w zakresie technologii serwerowych związanych z systemami Linux, specjalista w dziedzinie automatyzacji serwerów z użyciem technologii Ansible. Prowadzi szkolenia z bezpieczeństwa w systemach Linux, Ansible, Enterprise Linux Administration oraz warszaty z cyberbezpieczeństwa. Posiadacz certyfikatów Red Hat.

2 z 2

Dominik Węglarz

Trener z ponad dwudziestoletnim doświadczeniem w branży IT, projektował i wdrażał infrastruktury w wielu firmach i instytucjach. Specjalista w zakresie VMware. Prowadzi szkolenia i warsztaty z bezpieczeństwa IT, Certified Ethical Hacker, Certified Secure Computer User oraz cyber awareness dla pracowników biurowych. Posiadacz licznych certyfikatów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dostępne na Wirtualnej Uczelni.

Warunki uczestnictwa

Rekrutacja na studia podyplomowe wymaga wypełnienia internetowego formularza zgłoszeniowego. Uprzejmie informujemy, że wypełnienie formularza rekrutacyjnego drogą internetową nie jest jednoznaczne z zakwalifikowaniem się na dany kierunek studiów podyplomowych. O przyjęciu na studia decyduje kolejność zgłoszeń.
Centrum Studiów Podyplomowych i Szkoleń zastrzega możliwość zaproszenia kandydata na rozmowę rekrutacyjną.

Warunki techniczne

Warunki techniczne niezbędne do udziału w części usługi realizowanie zdalnie:

1) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa: narzędzie z pakietu Google G-Suite (Google Classroom oraz Google Meet)

2) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: komputer z procesorem Intel Pentium 4 lub nowszy, obsługujący SSE2, 2 GB pamięci RAM, zainstalowany jeden z systemów operacyjnych Windows 7, 8, 10, macOS 10.9 lub nowszy. Dodatkowo wbudowany lub zewnętrzny mikrofon, opcjonalnie kamera video. (Do obsługi wideo w jakości HD wymagany jest procesor Intel drugiej generacji i3/i5/i7 2,2 GHz, odpowiednik firmy AMD lub lepszy). Android z systemem 5.0 lub nowszy/iPhone z systemem iOS 11.0 lub nowszy.

3) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: https://support.google.com/a/answer/1279090

4) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Przeglądarka Google Chrome lub Mozilla Firefox, Adobe Reader, pakiet biurowy np. Libre Office, Open Office lub Microsoft Office.

Kontakt

Anna Stefańska

E-mail podyplomowe.warszawa@swps.edu.pl

Telefon (+48) 22 1032 631