Możliwość dofinansowania

Uniwersytet WSB Merito w Poznaniu

★★★★½

Bezpieczeństwo i ochrona cyberprzestrzeni

Numer usługi 2024/07/15/7405/2221889

zdalna w czasie rzeczywistym
Studia podyplomowe
184 h
19.10.2024 do 30.09.2025

5 900,00 PLN brutto
5 900,00 PLN netto
32,07 PLN brutto/h
32,07 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Absolwenci uczelni wyższych, pracownicy sektora przedsiębiorstw, funkcjonariusze służb porządku publicznego, także pracownicy zatrudnieni w organach administracji rządowej i oraz samorządowej , realizujących czynności związane z administrowaniem sieciami IT lub planujących w przyszłości zajmować się zawodowo bezpieczeństwem teleinformatycznym w sektorze przedsiębiorstwa oraz sektorze publicznym.
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	18-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	184
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 przygotowanie uczestników do pracy w komórkach IT w zakresie kreowania właściwej polityki bezpieczeństwa teleinformatycznego, tworzenia bezpiecznego środowiska gromadzenia i przesyłania danych, zgodnie z przyjętymi standardami oraz nabytymi umiejętnościami praktycznymi. Program studiów oparty jest na wymaganiach międzynarodowych kwalifikacji pełnomocnika ds. cyberprzestępczości oraz doświadczeniach z międzynarodowej i polskiej praktyki w tym zakresie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA Zrozumienie zagrożeń cybernetycznych Podstawy kryptografii Prawne i regulacyjne aspekty cyberbezpieczeństwa Architektura bezpieczeństwa IT Zarządzanie incydentami bezpieczeństwa	bsolwent zna i rozumie różne rodzaje zagrożeń w cyberprzestrzeni, w tym wirusy, malware, ataki DDoS, phishing, ransomware i inne formy cyberataków. Absolwent zna podstawowe zasady kryptografii i jej zastosowanie w zabezpieczaniu danych. bsolwent zna i rozumie krajowe oraz międzynarodowe regulacje i normy prawne dotyczące ochrony danych i cyberbezpieczeństw. Absolwent zna zasady projektowania i implementacji systemów zabezpieczeń w sieciach komputerowych i systemach informatycznych. Absolwent zna procedury i narzędzia służące do identyfikacji, analizowania i reagowania na incydenty bezpieczeństwa w cyberprzestrzeni.	Test teoretyczny
UMIEJĘTNOŚCI Identyfikacja zagrożeń i ocena ryzyka Projektowanie systemów zabezpieczeń Implementacja mechanizmów ochrony danych Monitorowanie i analiza ruchu sieciowego Reagowanie na incydenty bezpieczeństwa	Absolwent potrafi identyfikować potencjalne zagrożenia w cyberprzestrzeni oraz oceniać poziom ryzyka z nimi związany. Absolwent potrafi projektować systemy zabezpieczeń, które chronią przed zagrożeniami cybernetycznymi. Absolwent potrafi wdrażać mechanizmy kryptograficzne oraz inne technologie zabezpieczeń do ochrony danych. Absolwent potrafi monitorować ruch sieciowy oraz analizować logi w celu wykrywania i przeciwdziałania zagrożeniom. Absolwent potrafi skutecznie reagować na incydenty bezpieczeństwa, minimalizując ich skutki i zapobiegając przyszłym zagrożeniom.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETENCJE Praca w zespole Stałe doskonalenie zawodowe Etyka i odpowiedzialność zawodowa	Absolwent potrafi efektywnie pracować w zespole, współpracując z innymi specjalistami ds. bezpieczeństwa oraz z użytkownikami systemów informatycznych. Absolwent rozumie potrzebę ciągłego doskonalenia swoich umiejętności i wiedzy w szybko zmieniającym się środowisku cyberbezpieczeństw. Absolwent działa zgodnie z zasadami etyki zawodowej, respektując prawo i normy dotyczące ochrony danych oraz prywatności.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Świadectwo studiów podyplomowych zawiera program kierunku wraz ze zrealizowanymi godzinami i punktami ECTS. Absolwent uzyskuje zaświadczenie potwierdzające zdobyte efekty kształcenia.

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

Świadectwo ukończenia studiów podyplomowych jest wydawane na podstawie uzyskania pozytywnej oceny z każdego semestru zgodnie z Regulaminem Studiów Podyplomowych.
Studia kończą się zaliczeniem na ocenę określonym w karcie kierunku.

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

Świadectwo ukończenia studiów podyplomowych jest potwierdzeniem uzyskania pozytywnego wyniku z dwóch testów semestralnych i egzaminu końcowego.

Program

1. Społeczeństwo informacyjne - 8 godz.
2. Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO - 32 godz.
3. Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 2700 - 16 godz.
4. Organizacja Krajowego Systemu Cyberbezpieczeństwa - 8 godz.
5. Organizacja i zadania Security Operations Center - 8 godz.
6. Prawno-karne aspekty cyberprzestępczości - 16 godz.
7. Zarządzanie i obsługa incydentów cyberbezpieczeństwa - 16 godz.
8. Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa - 8 godz.
9. Wykorzystanie Internetu jako narzędzia śledczego - 16 godz.
10. Techniki analizy elektronicznego materiału dowodowego - 32 godz.

11. Metodyka przeprowadzania analizy śledczej - 16 godz.
12. Szacowanie ryzyka w systemach informatycznych - 8 godz.

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	5 900,00 PLN
Koszt przypadający na 1 uczestnika netto	5 900,00 PLN
Koszt osobogodziny brutto	32,07 PLN
Koszt osobogodziny netto	32,07 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Dariusz Kozłowski

Ekspert z zakresu zarządzania ryzykiem nadużyć, audytu śledczego i analizy śledczej. Były oficer polskich służb policyjnych i specjalnych. Przez blisko 25 lat służył w formacjach zajmujących się zwalczaniem przestępczości gospodarczej i korupcyjnej oraz przeciwdziałaniem nadużyciom godzącym w interesy ekonomiczne Rzeczypospolitej. Specjalizował się w eliminacji zorganizowanych grup przestępczych parających się fałszowaniem i praniem pieniędzy, oszustwami bankowymi, ubezpieczeniowymi oraz innymi nadużyciami w obrocie gospodarczym, a także korupcją i wyłudzaniem środków publicznych. Uczestniczył w projektowaniu i wdrażaniu systemów ochrony antykorupcyjnej w administracji publicznej. Jest doświadczonym wykładowcą oraz trenerem z zakresu metodyki przeciwdziałania oszustwom, korupcji i innym nadużyciom, jak również technik prowadzenia rozmów i wysłuchań oraz taktyki komunikacji interpresonalnej z wykorzystaniem metod przesłuchań stosowanych przez FBI i polskie służby specjalne. Od 2018 roku wdraża praktyczne i efektywne systemy antykorupcyjne, proetyczne, whistleblowingowe i ochrony

danych osobowych dla sektora publicznego i prywatnego. Przeprowadza również audyty oraz analizy ryzyka w obszarze compliance. Od 2021 roku pełni funkcję Wiceprezesa Zarządu Stowarzyszenia Ekspertów ds. Przeciwdziałania Oszustwom, Nadużyciom Gospodarczym i Korupcji (ACFE Poland Chapter #183). Jest audytorem wiodącym ISO 27001. Publikuje również artykuły naukowe i popularnonaukowe w branżowych wydawnictw

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podczas zjazdu każdy uczestnik programu otrzymuje komplet materiałów dydaktycznych na platformie MS Teams. Materiały te przygotowują wykładowcy, dostosowując je do specyfiki prowadzonego tematu.

Uczestnicy studiów pracują na platformie MS Teams, to platforma komunikacyjna Uczelni WSB Merito, stworzona w celu ograniczenia formalności oraz ułatwienia przepływu informacji między uczestnikami a uczelnią. Za jej pomocą przez całą dobę i z każdego miejsca na świecie uczestnicy mają dostęp do:

- harmonogramu zajęć,
- materiałów dydaktycznych,
- informacji dotyczących zmian w planach zajęć, ogłoszeń i aktualności.

Warunki uczestnictwa

Zapisu można dokonać na stronach Uniwersytetu WSB Merito w wybranych filiach w:

- Chorzowie,
- Poznaniu,
- Szczecinie,
- Warszawie

poprzez formularz online znajdujący się na stronie: www.wsb.pl/rekrutacja/krok1 oraz dostarczyć komplet dokumentów do Biura Rekrutacji do wybranej filii.

Kryteria uczestnictwa w Programie

- ukończone studia wyższe I lub II stopnia
- spełnienie warunków rekrutacyjnych

Warunki zaliczenia

Test semestralny oraz test końcowy.

Interaktywna forma zajęć

Wykłady uzupełniane są ćwiczeniami, warsztatami, studiami przypadków, treningami i symulacją biznesową, dzięki którym uczestnicy mogą na bieżąco weryfikować swoje umiejętności menedżerskie.

Zjazdy odbywają się średnio raz lub dwa razy w miesiącu:

- w soboty od 9:00 do 16:00/17:45,
- w niedziele od godz. 9:00 do 16:00/17:45.

Informacje dodatkowe

Dodatkowe szkolenia

Uczestnicy naszych programów mogą brać udział w ciekawych szkoleniach, które prowadzą doświadczeni trenerzy. Udział w spotkaniach jest bezpłatny. Dzięki szkoleniom można uzupełnić wiedzę i potwierdzić ją certyfikatem.

Informacje dodatkowe

- Szczegółowy harmonogram usługi może ulec zmianie w postaci realizowanych przedmiotów w danym dniu i osób prowadzących. **Zmianie nie ulegają terminy zjazdów na studiach podyplomowych oraz ilość godzin usługi.**
- **Harmonogram zjazdów zostanie upubliczniony na stronach Uczelni lub w BUR na 2 tygodnie przed zajęciami**
- **Godziny zajęć podane w harmonogramie są godzinami zegarowymi, zaś ilość godzin programowych jest podana w godzinach dydaktycznych. 184 godzin dydaktycznych = 138 godzin zegarowych**
- **Cena usługi nie obejmuje opłaty wpisowej oraz końcowej.**

Warunki techniczne

Nową wiedzę i umiejętności zdobywasz, dzięki zajęciom realizowanym na platformie MS Teams. Z wykładowcami i uczestnikami studiów kontaktujesz się przez internet, w czasie rzeczywistym (synchronicznie). W zajęciach uczestniczysz w weekendy, zgodnie z ustalonym harmonogramem zjazdów.

Techniczne wymagania do zajęć:

- ***komputer (z wbudowanymi lub podłączonymi głośnikami i mikrofonem),***
- ***dostęp do Internetu,***
- ***słuchawki (opcjonalnie),***
- ***jeśli chcesz aby Cię widziano, możesz użyć kamery umieszczonej w laptopie/komputerze.***

Kontakt

Magdalena Dolata

E-mail dsp@szczecin.merito.pl
Telefon (+48) 914 526 970