Możliwość dofinansowania

Uniwersytet WSB Merito w Poznaniu

★★★★½

Bezpieczeństwo i ochrona cyberprzestrzeni

Numer usługi 2024/11/28/7405/2437971

zdalna w czasie rzeczywistym
Studia podyplomowe
184 h
29.03.2025 do 28.02.2026

6 200,00 PLN brutto
6 200,00 PLN netto
33,70 PLN brutto/h
33,70 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
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. Usługa adresowana również dla Uczestników Projektu Małopolski Pociąg do Kariery
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	22-03-2025
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
1. WIEDZA Zrozumienie zagrożeń cybernetycznych Podstawy kryptografii Prawne i regulacyjne aspekty cyberbezpieczeństwa Architektura bezpieczeństwa IT Zarządzanie incydentami bezpieczeństwa	Rozróżnia zagrożenia cybernetyczne, w tym wirusy, malware, ataki DDoS, phishing, ransomware i inne formy cyberataków. Definiuje podstawowe zasady kryptografii oraz jej zastosowanie w zabezpieczaniu danych. Charakteryzuje krajowe oraz międzynarodowe regulacje i normy prawne dotyczące ochrony danych i cyberbezpieczeństwa. Projektuje zasady implementacji systemów zabezpieczeń w sieciach komputerowych i systemach informatycznych. Organizuje procedury i narzędzia służące do identyfikacji, analizowania i reagowania na incydenty bezpieczeństwa w cyberprzestrzeni.	Test teoretyczny
2. UMIEJĘTNOŚCI Identyfikacja zagrożeń i ocena ryzyka Projektowanie systemów zabezpieczeń Implementacja mechanizmów ochrony danych Monitorowanie i analiza ruchu sieciowego Reagowanie na incydenty bezpieczeństwa	Ocenia potencjalne zagrożenia w cyberprzestrzeni oraz poziom ryzyka z nimi związany. Projektuje systemy zabezpieczeń chroniące przed zagrożeniami cybernetycznymi. Implementuje mechanizmy kryptograficzne oraz inne technologie zabezpieczeń do ochrony danych. Monitoruje ruch sieciowy oraz analizuje logi w celu wykrywania i przeciwdziałania zagrożeniom. Reaguje na incydenty bezpieczeństwa, minimalizując ich skutki i zapobiegając przyszłym zagrożeniom.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
3. KOMPETENCJE Praca w zespole Stałe doskonalenie zawodowe Etyka i odpowiedzialność zawodowa	Organizuje pracę zespołową w zakresie cyberbezpieczeństwa, współpracując z innymi specjalistami oraz użytkownikami systemów informatycznych. Planuje rozwój zawodowy, uwzględniając dynamiczne zmiany w obszarze cyberbezpieczeństwa. Nadzoruje przestrzeganie zasad etyki zawodowej, uwzględniając przepisy prawa 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?

Dokument potwierdzający uzyskanie kompetencji 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

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

Czas trwania studiów (liczbę semestrów): 2 semestry

Częstotliwość zjazdów: Zjazdy odbywają się średnio raz lub dwa razy w miesiącu:

w soboty od 8:00 do 18:00, w niedziele od 8:00 do 18:00.

Liczba możliwych do zdobycia punktów ECTS: 30 pkt. ECTS

Rodzaj dokumentu potwierdzającego ukończenie studiów: Świadectwo ukończenia studiów podyplomowych

Liczbę godzin: 184 godzin (lekcyjnych)

Informację o sposobie walidacji: Test teoretyczny semestralny i końcowy

Harmonogram

Liczba przedmiotów/zajęć: 11

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001	29-03-2025	09:00	16:00	07:00
2 z 11 Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001	30-03-2025	09:00	16:00	07:00
3 z 11 Metodyka przeprowadzania analizy śledczej	12-04-2025	08:30	15:30	07:00
4 z 11 Metodyka przeprowadzania analizy śledczej	13-04-2025	08:30	15:30	07:00
5 z 11 Organizacja i zadania Security Operations Center	17-05-2025	09:00	16:00	07:00
6 z 11 Postępowanie wyjaśniające i dochodzenie w przypadku wystąpienia incydentów cyberbezpieczeństwa	18-05-2025	09:00	16:00	07:00
7 z 11 Szacowanie ryzyka w systemach informatycznych	07-06-2025	09:30	16:00	06:30

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 11 Organizacja Krajowego Systemu Cyberbezpieczeństwa	08-06-2025	09:00	16:00	07:00
9 z 11 Wykorzystanie Internetu jako narzędzia śledczego	14-06-2025	08:30	15:30	07:00
10 z 11 Wykorzystanie Internetu jako narzędzia śledczego	15-06-2025	08:30	15:30	07:00
11 z 11 Test semestralny	15-06-2025	15:40	16:40	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 200,00 PLN
Koszt przypadający na 1 uczestnika netto	6 200,00 PLN
Koszt osobogodziny brutto	33,70 PLN
Koszt osobogodziny netto	33,70 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

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

2 z 2

dr Marek Jasztal

Doktor nauk ekonomicznych, wykładowca akademicki, praktyk. Obszar jego działalności naukowej obejmuje tematy z zakresu analizy ryzyka, zarządzania finansowego oraz praktyki związanej z przygotowaniem, realizacją i rozliczeniem procesów inwestycyjnych, wyceny przedsiębiorstw, badania sprawozdań budżetowych i finansowych, zwalczanie przestępczości podatkowej, identyfikacji przestępstw przeciwko budżetowi państwa i budżetowi UE oraz finansowania terroryzmu. Zdobył doświadczenie w kluczowych obszarach zarządzania operacyjnego jednostką, tj. logistyce, teleinformatyce, w zamówieniach publicznych, wykorzystaniu środków europejskich, komunikacji, bezpieczeństwie. Pracował na stanowisku Kierownika Sekcji Księgowości i Rozliczeń. W 2004 został audytorem wewnętrznym, a następnie Zastępcą Komendanta Wojewódzkiego Policji. Nadzoruje obszar logistyki, finansów, łączności i informatyki, transportu, zamówień publicznych, funduszy UE oraz BHP. Ponadto posiada doświadczenie jako: Biegły sądowy z zakresu finansów publicznych i rachunkowości przy Sądzie Okręgowym w Szczecinie, certyfikowany księgowy i audytor wewnętrzny, Zastępca Przewodniczącego Komisji Rewizyjnej Stowarzyszenia Księgowych w Polsce Oddział w Szczecinie, Zastępca Przewodniczącego Rady Zachodniopomorskiego Oddziału Wojewódzkiego Narodowego Funduszu Zdrowia w Szczecinie, Zastępca Przewodniczącego Rady Społecznej przy Szpitalu MSWiA w Szczecinie. Autor kilkunastu publikacji naukowych oraz współautor wydawnictw książkowych.

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 08:00 do 18:00,
- w niedziele od godz. 08:00 do 18:00.

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.**

Zawarto umowę z WUP w Krakowie w ramach Projektu Małopolski Pociąg do Kariery

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

Biuro Rekrutacji

E-mail rekrutacja@szczecin.merito.pl
Telefon (+48) 914 225 858