UNIWERSYTET WSB MERITO POZNAŃ

wcześniej Wyższa Szkoła Bankowa

Bezpieczeństwo i ochrona cyberprzestrzeni

STUDIA PODYPLOMOWE

Sposób realizacji: Online

Obszar studiów: IT / Big Data / AI

Cechy: Od października • Polski • Dofinansowane • Rekrutacja zakończona • W partnerstwie

Miasto: Poznań

To kierunek dla osób, które:

- chcą rozwijać się w obszarze bezpieczeństwa IT i tworzyć skuteczne procedury ochrony,
- pracują w administracji publicznej lub planują karierę w sektorze bezpieczeństwa,
- zajmują się sieciami komputerowymi i chcą je zabezpieczać zgodnie z normami,
- myślą o objęciu funkcji pełnomocnika ds. cyberbezpieczeństwa w firmie,
- szukają praktycznego kierunku, który pomoże zdobyć prestiżowe certyfikaty.

5
bezpłatnych szkoleń realizowanych online

3
certyfikaty specjalistyczne

Microsoft 365

Nasi uczestnicy otrzymują darmową licencję A1, która obejmuje popularne aplikacje, takie jak Outlook, Teams, Word, PowerPoint, Excel, OneNote, SharePoint, Sway i Forms.

1
partner kierunku:

Networking i rozwój kompetencji

Studia rozwijają kompetencje niezależnie od doświadczenia. Dzięki **interaktywnym zajęciom i wymianie doświadczeń** z innymi zyskasz wiedzę, umiejętności i cenne kontakty.

Kadra złożona z praktyków

Zajęcia prowadzą **eksperci i pasjonaci** swojej dziedziny, którzy mają realne doświadczenie.

Praktyczny charakter studiów:

- na zajęciach dominują **warsztaty, ćwiczenia i case studies,**
- wszystkie **materiały dydaktyczne** będą dostępne online.

Program studiów

9	186	12	2
Liczba miesięcy nauki	Liczba godzin zajęć	Liczba zjazdów	Liczba semestrów

Społeczeństwo informacyjne (8 godz.)

- Podstawy funkcjonowania społeczeństwa informacyjnego
- Rola informacji i technologii w nowoczesnym świecie

Pełnomocnik ds. cyberbezpieczeństwa wg ISO 27001, ISO 22301 i RODO (32 godz.)

- Zadania i odpowiedzialność pełnomocnika
- Wymagania norm ISO 27001 i ISO 22301
- Cyberbezpieczeństwo a ochrona danych osobowych

Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji ISO

27001 (16 godz.)

- Planowanie i prowadzenie audytów wewnętrznych
- Dokumentacja i raportowanie audytów
- Doskonalenie systemu zarządzania bezpieczeństwem informacji

Organizacja Krajowego Systemu Cyberbezpieczeństwa (8 godz.)

- Struktura i zadania KSC
- Obowiązki operatorów usług kluczowych
- Współpraca z organami nadzoru

Organizacja i zadania Security Operations Center (8 godz.)

- Funkcje i modele SOC
- Monitorowanie bezpieczeństwa
- Reagowanie na zagrożenia

Prawno-karne aspekty cyberprzestępczości (8 godz.)

- Regulacje prawne dotyczące cyberprzestępstw
- Odpowiedzialność karna i administracyjna
- Przestępstwa komputerowe i dowody cyfrowe

Zarządzanie i obsługa incydentów cyberbezpieczeństwa (16 godz.)

- Procedury reagowania na incydenty
- Narzędzia wspierające obsługę incydentów
- Raportowanie i analiza incydentów

Postępowanie wyjaśniające i dochodzenie w przypadku incydentów (8 godz.)

- Zasady prowadzenia dochodzeń
- Dokumentowanie i analiza dowodów
- Współpraca z organami ścigania

Wykorzystanie Internetu jako narzędzia śledczego (16 godz.)

- OSINT – otwarte źródła informacji

- Monitorowanie aktywności w sieci
- Narzędzia do analizy śladów cyfrowych

Techniki analizy elektronicznego materiału dowodowego (32 godz.)

- Metody zabezpieczania dowodów cyfrowych
- Analiza dysków, pamięci i sieci
- Rekonstrukcja zdarzeń z danych cyfrowych

Metodyka przeprowadzania analizy śledczej (16 godz.)

- Etapy analizy śledczej
- Tworzenie hipotez i scenariuszy
- Raportowanie wyników analizy

Szacowanie ryzyka w systemach informatycznych (16 godz.)

- Identyfikacja zagrożeń i podatności
- Metody oceny ryzyka
- Zarządzanie ryzykiem w systemach IT

Forma zaliczenia (2 godz.)

- Test semestralny
- Test końcowy

Partnerzy kierunku

Warunki przyjęcia

Aby zostać uczestnikiem studiów podyplomowych na Uniwersytecie WSB Merito, należy:

Możliwości dofinansowania

- **Pierwsi zyskują najwięcej!** Im szybciej się zapiszesz, z tym większej zniżki skorzystasz.
- Oferujemy specjalne, **większe zniżki dla**

- mieć ukończone studia licencjackie, inżynierskie lub magisterskie,
- złożyć komplet dokumentów i spełnić wymogi rekrutacyjne,
- o przyjęciu decyduje kolejność zgłoszeń.

Dowiedz się więcej

naszych absolwentów.

- Możesz skorzystać z dofinansowania z **Bazy Usług Rozwojowych**.
- Funkcjonuje u nas **Program Poleceń**.
- Pracodawca może dofinansować Ci studia, otrzymując dodatkową zniżkę w ramach **Programu Firma**.
- Warto sprawdzić możliwości dofinansowania z **KFS**.

Dowiedz się więcej

Czego się nauczysz?

- Zdobędziesz **praktyczne umiejętności** w zakresie tworzenia i wdrażania polityki bezpieczeństwa teleinformatycznego, zgodnie z międzynarodowymi standardami.
- **Nauczysz się identyfikować zagrożenia** w cyberprzestrzeni oraz skutecznie reagować na incydenty bezpieczeństwa.
- Poznasz **metody analizy elektronicznego materiału dowodowego** oraz techniki informatyki śledczej.
- Zrozumiesz **aspekty prawne związane z cyberprzestępczością**, w tym regulacje dotyczące **ochrony danych i RODO**.
- Przygotujesz się do pełnienia funkcji **Pełnomocnika Bezpieczeństwa Cyberprzestrzeni**, zgodnie z krajowymi strategiami i politykami.

Ceny

Dla Kandydatów

	1 rok
1 rata	**6150 zł** (1 x 6150 zł)
2 raty	**3165 zł** (2 x 3165 zł)
10 rat	**650 zł** (10 x 650 zł)
12 rat	**555 zł** (12 x 555 zł)

Dla naszych absolwentów

	1 rok
1 rata	**6150 zł** (1 x 6150 zł)
2 raty	**3165 zł** (2 x 3165 zł)
10 rat	**650 zł** (10 x 650 zł)
12 rat	**555 zł** (12 x 555 zł)

W oparciu o art. 80 ust. 3 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce uczelnia raz w roku akademickim zwiększa wysokość czesnego określonego w § 3 ust. 1 Umowy o wskaźnik równy wskaźnikowi wzrostu cen towarów i usług konsumpcyjnych za rok kalendarzowy poprzedzający rok, w którym dokonuje się waloryzacji, ogłoszony przez Prezesa Głównego Urzędu Statystycznego, łącznie nie więcej niż o 30 % do czasu ukończenia studiów określonych w Umowie.

Wykładowcy

dr Marek Jasztal

- Obszary zainteresowań obejmują zarządzanie ryzykiem, finanse jednostek, cyberbezpieczeństwo, zarządzanie kryzysowe oraz identyfikację źródeł finansowania i logistykę terroryzmu.
- Doświadczony ekspert w zarządzaniu jednostką sektora finansów publicznych w obszarach finansów, zamówień publicznych, pozyskiwania funduszy zewnętrznych, IT oraz inwestycji.
- Autor kilkunastu publikacji z zakresu audytu wewnętrznego, zarządzania ryzykiem, badania sprawozdań finansowych oraz identyfikacji zagrożeń terrorystycznych.
- Biegły w zakresie audytu, finansów i rachunkowości.