UNIWERSYTET WSB MERITO BYDGOSZCZ

wcześniej Wyższa Szkoła Bankowa

Ochrona Danych, Cyberbezpieczeństwo i AI Governance

STUDIA PODYPLOMOWE

Sposób realizacji: Hybrydowe

Obszar studiów: Administracja i bezpieczeństwo • IT / Big Data / AI • Prawo

Cechy: Od marca • Polski • Certyfikat

Miasto: Bydgoszcz

To kierunek dla osób, które: :

- pełnią lub obejmą funkcję Inspektora Ochrony Danych i chcą rozszerzyć kompetencje o cyberbezpieczeństwo oraz AI,
- planują pracować w cyberbezpieczeństwie, compliance i potrzebują zrozumieć regulacje RODO, NIS2, DORA, AI Act – w kontekście własnych projektów,
- odpowiadają za compliance lub zarządzanie ryzykiem w firmach objętych RODO, NIS2 czy DORA,
- są prawnikami obsługującymi projekty technologiczne i chcą mówić jednym językiem z IT.

Dostęp online
Wysoka jakość kształcenia. Wszystkie materiały dydaktyczne będą dostępne dla Ciebie online.

92%
Uczestników poleca studia podyplomowe
Źródło: „Badanie satysfakcji ze studiów 2025”.

Microsoft 365
Nasi uczestnicy otrzymują darmową licencję A1, która obejmuje popularne aplikacje, takie jak Outlook, Teams, Word, PowerPoint, Excel, OneNote, SharePoint, Sway i Forms.

91%
Pracodawców ocenia bardzo dobrze lub dobrze współpracę z naszymi uniwersytetami
Źródło: "Badanie opinii pracodawców, 2024"

Kadra złożona z praktyków
Zajęcia prowadzą eksperci i pasjonaci swojej dziedziny, którzy mają realne doświadczenie.

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

Praktyczny charakter studiów:
• na zajęciach dominują warsztaty, ćwiczenia i case studies,
• prace projektowe przygotowywane są zespołowo.

Program studiów

10	160	10	5
Liczba miesięcy nauki	Liczba godzin zajęć	Liczba zjazdów	Liczba modułów

MODUŁ I – Ramy prawne i etyczne (32 godz. / 5,5 ECTS)

Zacznijmy od mapy regulacyjnej: jak poskładać w całość RODO, UODO, NIS2/ustawę o KSC, DORA, Data Act oraz AI Act. Zobaczysz, które regulacje dotyczą Twojej organizacji i w jakiej kolejności je wdrażać.

W ramach modułu zrealizujesz przedmioty:

- Ramy prawne ochrony danych i cyberbezpieczeństwa (RODO, UODO, NIS2/UKSC, DORA, Data Act, DGA) – 8 godz.
- AI Act w praktyce organizacji: klasyfikacja systemów, obowiązki dostawców i operatorów, FRIA, interakcja z RODO – 12 godz.
- Etyka danych i odpowiedzialna AI – 6 godz.
- Ochrona danych w sektorach: HR, marketing/e-commerce, ochrona zdrowia, produkcja (dane wrażliwe, art. 9 RODO) – 6 godz.

MODUŁ II – Audyt i analiza ryzyka (32 godz. / 5 ECTS)

Moduł warsztatowy. Przechodzisz pełny cykl: od planu audytu, przez analizę ryzyka wg ISO/IEC 27005, aż po DPIA i FRIA wykonane równolegle na realnym systemie AI wspierającym HR.

W ramach modułu zrealizujesz przedmioty:

- Audyt zgodności (RODO, ISO 27001, NIS2) – metodyki, checklisty, raportowanie – 10 godz.
- Analiza ryzyka w bezpieczeństwie informacji (ISO/IEC 27005, rejestry ryzyka, apetyt na ryzyko) – 10 godz.
- DPIA i FRIA w praktyce – ocena skutków dla ochrony danych i praw podstawowych – 12 godz.

MODUŁ III – Systemy zarządzania i governance (32 godz. / 4,5 ECTS)

Jak zbudować w organizacji spójny ekosystem ISMS (ISO 27001), PIMS (ISO 27701) i AIMS (ISO 42001)? Jak zintegrować role IOD, CISO i AI Officera zamiast tworzyć z nich rywalizujące silosy?

W ramach modułu zrealizujesz przedmioty:

- Systemy zarządzania bezpieczeństwem, prywatnością i AI (ISO/IEC 27001, 27701, 42001) – privacy & AI by design – 12 godz.
- Zintegrowane governance privacy–security–AI (model operacyjny, raportowanie do zarządu, KPI) – 10 godz.
- Zarządzanie łańcuchem dostaw i outsourcingiem w świetle CRA, DORA i Data Act – 10 godz.

MODUŁ IV – Technologia, chmura i zarządzanie incydentami (32 godz. / 5 ECTS)

Tu wyrównujesz poziom techniczny – prawnicy uczą się czytać logi i rozmawiać z IT, a specjaliści IT poznają perspektywę compliance. Symulujemy prawdziwy incydent ransomware od wykrycia po zgłoszenie do UODO i CSIRT.

W ramach modułu zrealizujesz przedmioty:

- Podstawy technologiczne dla nietechnicznych (sieci, szyfrowanie, uwierzytelnianie, typy cyberzagrożeń) – 10 godz.
- Bezpieczeństwo danych w chmurze i środowiskach rozproszonych (IaaS/PaaS/SaaS, lokalizacja danych, transfery) – 8 godz.
- Zarządzanie tożsamością i dostępem (IAM, MFA, SSO, uprawnienia, self-sovereign identity) – 6 godz.
- Strategia cyberodporności i zarządzanie incydentami (NIS2, BCP/DRP, Zero Trust, zgłoszenia do CSIRT) – 8 godz.

MODUŁ V – Kultura bezpieczeństwa i projekt dyplomowy (32 godz. / 5 ECTS + egzamin 5 ECTS)

Ostatni moduł łączy „miękką” stronę bezpieczeństwa (kultura, komunikacja, social engineering) z intensywną pracą nad projektem dyplomowym obejmującym dla wybranej organizacji pełny plan zgodności RODO + NIS2 + AI Act.

W ramach modułu zrealizujesz przedmioty:

- Kultura bezpieczeństwa, komunikacja kryzysowa i social engineering – 10 godz.

- Warsztat projektowy – zintegrowany case study (DPIA/FRIA, analiza ryzyka, plan reagowania, raport) – 14 godz.
- Seminarium dyplomowe i obrona projektu – 8 godz.

Warunki przyjęcia

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

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

Dowiedz się więcej

Możliwości dofinansowania

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

- Zrozumiesz, jak w organizacji współgrają **RODO, NIS2, AI Act, DORA i Data Act** – i jak zbudować jeden spójny program zgodności zamiast pięciu osobnych.
- Nauczysz się klasyfikować systemy **AI według AI Act, prowadzić FRIA oraz łączyć ją z DPIA** tam, gdzie AI przetwarza dane osobowe.
- Przećwiczysz analizę ryzyka wg **ISO/IEC 27005 i audyty zgodności (RODO, ISO 27001, NIS2)** na realnych case'ach z produkcji, e-commerce i ochrony zdrowia.
- Poznasz techniczne podstawy **cyberbezpieczeństwa w ujęciu biznesowym** – bez wchodzenia w kod, ale wystarczająco by rozmawiać z IT i czytać raporty.
- Przejdziesz symulację incydentu: od wykrycia, przez zgłoszenie do **UODO i CSIRT, po komunikację kryzysową i raport naprawczy dla zarządu**.
- Zbudujesz w zespole zintegrowany projekt dyplomowy – **plan zgodności RODO + NIS2 + AI Act z rekomendacjami dla zarządu** – gotowy do dołączenia do portfolio.

Kadra złożona z praktyków

Zajęcia poprowadzi grono praktyków z ponad dwudziestoletnim doświadczeniem w

ochronie danych, cyberbezpieczeństwie i nowych technologiach: doświadczeni Inspektorzy Ochrony Danych i audytorzy wiodący **ISO 27001**, adwokaci i radcowie prawni specjalizujący się w **RODO i AI**, eksperci obsługujący realne naruszenia i kontrole **UODO**, wykładowcy łączący pracę w biznesie z działalnością akademicką. To osoby, które na co dzień wdrażają **RODO, NIS2 i AI Act** w polskich i międzynarodowych organizacjach – od start-upów po podmioty z sektora regulowanego.