UNIWERSYTET WSB MERITO ŁÓDŹ



Prywatność i Cyberodporność w Organizacji

STUDIA PODYPLOMOWE

UNIWERSYTET WSB MERITO ŁÓDŹ

Program studiów

9	160	10	5
Liczba miesięcy nauki	Liczba godzin zajęć	Liczba zjazdów	Liczba modułów

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

- 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) - 16 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 – 12 godz.
- Analiza ryzyka w bezpieczeństwie informacji (ISO/IEC 27005, rejestry ryzyka, apetyt na ryzyko) – 14 godz.
- DPIA i FRIA w praktyce – ocena skutków dla ochrony danych i praw podstawowych – 10 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 – 14 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 – 14 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.

Dane zamieszczone w niniejszej karcie kierunku mają charakter wyłącznie informacyjny. Dane te nie stanowią oferty zawarcia umowy w rozumieniu art. 66 i nast. kodeksu cywilnego. Zgodnie z art. 160 ust. 3 ustawy z dnia 27 lipca 2005 roku Prawo o szkolnictwie wyższym, umowa między Uniwersytetem WSB Merito w Łodzi, studentem zawierana jest w formie pisemnej.

- 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) – 10 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 – 8 godz.
- Warsztat projektowy – zintegrowany case study (DPIA/FRIA, analiza ryzyka, plan reagowania, raport) – 4 godz.
- Seminarium dyplomowe i obrona projektu - 4 godz.

Dane zamieszczone w niniejszej karcie kierunku mają charakter wyłącznie informacyjny. Dane te nie stanowią oferty zawarcia umowy w rozumieniu art. 66 i nast. kodeksu cywilnego. Zgodnie z art. 160 ust. 3 ustawy z dnia 27 lipca 2005 roku Prawo o szkolnictwie wyższym, umowa między Uniwersytetem WSB Merito w Łodzi, studentem zawierana jest w formie pisemnej.