UNIWERSYTET WSB MERITO TORUŃ

wcześniej Wyższa Szkoła Bankowa

CyberAI: zintegrowane bezpieczeństwo i sztuczna inteligencja

STUDIA PODYPLOMOWE

Sposób realizacji: Online

Obszar studiów: IT / Big Data / AI

Cechy: Od października • Polski

Miasto: Toruń

To kierunek dla osób, które::

- pracują lub chcą pracować w IT i bezpieczeństwie, rozwijając kompetencje w AI i nowych zagrożeniach,
- tworzą lub integrują rozwiązania AI z naciskiem na bezpieczeństwo i prywatność,
- zarządzają projektami i potrzebują wiedzy o wdrażaniu AI w organizacjach,
- działają w sektorze publicznym i muszą znać regulacje dotyczące AI i bezpieczeństwa.

1

certyfikat specjalistyczny:
■ ukończenia szkolenia Cyber AI wydany przez Uniwersytet WSB Merito,

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

9	176	11	2
Liczba miesięcy nauki	Liczba godzin zajęć	Liczba zjazdów	Liczba semestrów

Wprowadzenie do AI i cyberbezpieczeństwa (8 godz.)

- Historia i podstawy sztucznej inteligencji
- Kluczowe technologie AI w kontekście bezpieczeństwa
- Ramy prawne i regulacje (RODO, AI Act)

Podstawy uczenia maszynowego i deep learningu (24 godz.)

- Algorytmy uczenia maszynowego (supervised, unsupervised, reinforcement)
- Wprowadzenie do sieci neuronowych
- Zastosowania uczenia maszynowego w bezpieczeństwie

Ataki na modele AI: Adversarial AI (16 godz.)

- Charakterystyka ataków typu adversarial
- Praktyczne przykłady i demonstracje ataków

- Metody zabezpieczania modeli (adversarial training, robust learning)

Prywatność i etyka w AI (16 godz.)

- Ochrona danych osobowych w kontekście AI
- Differential Privacy – podstawy i zastosowanie
- Etyczne dylematy i odpowiedzialność za decyzje AI

Bezpieczeństwo danych: zarządzanie danymi uczącymi AI (16 godz.)

- Bezpieczne przetwarzanie i przechowywanie danych
- Mechanizmy ochrony przed manipulacją i nieautoryzowanym dostępem
- Fairness i bias w zestawach danych

Zabezpieczanie modeli AI (16 godz.)

- Metody bezpieczeństwa modeli w środowiskach fizycznych i cyfrowych
- Rozproszone uczenie (federated learning) i implikacje bezpieczeństwa
- AI w chmurze (Azure, Google AI) – aspekty wdrożeniowe i studium przypadku

AI w systemach krytycznych: bezpieczeństwo i regulacje (16 godz.)

- Zastosowanie AI w sektorach krytycznych (energetyka, zdrowie, transport)
- Normy i standardy regulujące AI w systemach krytycznych
- Analiza ryzyka i przykłady awarii AI

AI i Internet Rzeczy (IoT): bezpieczeństwo i zagrożenia (16 godz.)

- Zastosowanie AI w IoT, przegląd ataków i metod ochrony
- Skalowalność i odporność systemów AI w sieciach urządzeń
- Praktyczne metody wykrywania i neutralizacji zagrożeń

Zautomatyzowane systemy bezpieczeństwa z AI (24 godz.)

- Systemy wykrywania zagrożeń i anomalii oparte na AI (SIEM, SOAR)
- Automatyzacja w walce z malware i ransomware
- Case studies: wdrożenia systemów automatycznego reagowania

Audyt i ocena bezpieczeństwa AI (8 godz.)

- Metody audytu systemów AI
- Ocena ryzyka wdrożeń i narzędzia do monitorowania
- Best practices w walidacji systemów AI

Projekty końcowe i warsztaty (16 godz.)

- Projekty grupowe związane z bezpieczeństwem AI
- Studia przypadków oparte na realnych wdrożeniach i zagrożeniach
- Prezentacja i omówienie projektów – feedback wykładowców oraz praktyków

Forma zaliczenia

- Praktyczny projekt końcowy realizowany indywidualnie lub w grupie

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?

- **Zdobędziesz kompleksowe zrozumienie AI** – opanujesz podstawy uczenia maszynowego i deep learningu, co pozwoli Ci projektować i wdrażać modele sztucznej inteligencji.
- **Nauczysz się wykrywać zagrożenia** – poznasz techniki identyfikacji i przeciwdziałania atakom na modele AI, w tym tzw. adversarial attacks.
- **Zrozumiesz zasady zarządzania danymi uczącymi się** – dowiesz się, jak przetwarzać dane zgodnie z RODO i wymogami bezpieczeństwa oraz ochrony prywatności.

- **Przećwiczysz zabezpieczanie rozwiązań AI** – nauczysz się chronić systemy AI w środowiskach chmurowych i IoT, zgodnie z aktualnymi regulacjami i standardami.
- **Poznasz metody audytu i oceny ryzyka** – opanujesz narzędzia do monitorowania bezpieczeństwa systemów AI oraz wykrywania nadużyć i luk.
- **Zdobędziesz doświadczenie praktyczne** – dzięki pracy zespołowej i analizie realnych wdrożeń przygotujesz się do działań w środowiskach biznesowych i publicznych.

Ceny

Dla Kandydatów

	1 rok
1 rata	**6320 zł** ~~7200 zł~~ (1 x 6320 zł) Najniższa cena z ostatnich 30 dni: 6260zł
2 raty	**3160 zł** ~~3600 zł~~ (2 x 3160 zł) Najniższa cena z ostatnich 30 dni: 3130zł
10 rat	**632 zł** ~~720 zł~~ (10 x 632 zł) Najniższa cena z ostatnich 30 dni: 626zł
12 rat	**526 zł** ~~600 zł~~ (12 x 526 zł) Najniższa cena z ostatnich 30 dni: 521zł

Dla naszych absolwentów

	1 rok
1 rata	**5920 zł** ~~7200 zł~~ (1 x 5920 zł) Najniższa cena z ostatnich 30 dni: 5860zł
2 raty	**2960 zł** ~~3600 zł~~ (2 x 2960 zł) Najniższa cena z ostatnich 30 dni: 2930zł
10 rat	**592 zł** ~~720 zł~~ (10 x 592 zł) Najniższa cena z ostatnich 30 dni: 586zł
12 rat	**493 zł** ~~600 zł~~ (12 x 493 zł) Najniższa cena z ostatnich 30 dni: 488zł

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.