

# CyberAI: zintegrowane bezpieczeństwo i sztuczna inteligencja

STUDIA PODYPLOMOWE

**Sposób realizacji:** Hybrydowe

**Obszar studiów:** IT / Big Data / AI

**Cechy:** Od października • Polski

**Miasto:** Wrocław

**To kierunek dla osób, które::**

- pracują w IT i chcą łączyć AI z nowoczesnym podejściem do cyberbezpieczeństwa,
- tworzą lub wdrażają rozwiązania AI i zależy im na ochronie danych użytkowników,
- zarządzają projektami i chcą skutecznie wdrażać bezpieczne systemy oparte na AI,
- pracują w instytucjach, gdzie AI musi działać zgodnie z przepisami i standardami,
- szukają wiedzy, która łączy nowoczesne technologie z praktycznym podejściem do ryzyk.



**4**

bezpłatne szkolenia.

#### Dostęp online

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

#### 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,
- prace projektowe przygotowywane są zespołowo.

**1**

**certyfikat specjalistyczny:**

- Cyber AI

**91%**

pracodawców ocenia bardzo dobrze lub dobrze współpracę z naszymi uniwersytetami.

Źródło: "Badanie opinii pracodawców, 2024"

#### Networking i rozwój kompetencji

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

## Program studiów

**9**

Liczba miesięcy nauki

**176**

Liczba godzin zajęć

**11**

Liczba zjazdów

**2**

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 na studia

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

- Oferujemy specjalne, większe zniżki dla naszych absolwentów.
- Możesz skorzystać z dofinansowania z Bazy Usług Rozwojowych.
- 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 **solidne podstawy z obszaru uczenia maszynowego i deep learningu**, co ułatwi Ci projektowanie i wdrażanie modeli AI.
- Nauczysz się **identyfikować i przeciwdziałać nowym formom ataków** na modele AI (adversarial attacks).
- Zrozumiesz, **jak prawidłowo zarządzać danymi uczącymi się**, uwzględniając kwestie RODO, prywatności i bezpieczeństwa danych.
- Przećwiczysz **zabezpieczanie rozwiązań AI w chmurze oraz w środowiskach IoT**, z uwzględnieniem najnowszych regulacji i norm.
- Poznasz **metody oceny bezpieczeństwa systemów AI**, w tym audyty, narzędzia do



monitorowania pod kątem nadużyć i luk bezpieczeństwa.

- Dzięki **analizie praktycznych wdrożeń, projektów zespołowych będziesz lepiej przygotowany do pracy** w realnych projektach biznesowych lub sektorze publicznym.
- Wiedza z **cyberbezpieczeństwa i AI** daje Ci przewagę konkurencyjną na rynku pracy.
- Spotkasz **wykładowców-praktyków oraz uczestników z różnych branż**, co pozwoli Ci budować cenne relacje i wymieniać doświadczenia.

## Ceny

### Dla Kandydatów

**1 rok**

10 rat

**671 zł** ~~765 zł~~ (10 x 671 zł)  
Najniższa cena z ostatnich 30 dni: 665zł

### Dla naszych absolwentów

**1 rok**

10 rat

**631 zł** ~~765 zł~~ (10 x 631 zł)  
Najniższa cena z ostatnich 30 dni: 625zł

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.