UNIWERSYTET WSB MERITO WROCŁAW

wcześniej Wyższa Szkoła Bankowa

CyberAI: zintegrowane bezpieczeństwo i sztuczna inteligencja

STUDIA PODYPLOMOWE

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