Sztuczna inteligencja w cyberbezpieczeństwie

Głównym celem zajęć powinno być zapoznanie studenta w jaki sposób sztuczna inteligencja może wspierać, ale również i zagrażać cyberbezpieczeństwu.

W tym celu student powinien zostać zaznajomiony:

- pozytywnymi aspektami AI
  - możliwość tworzenia automatycznych narzędzi do wykrywania niepożądanych działań w celu uzyskania dostępu do danych wrażliwych poprzez analizę logów w celu wykrycia wzorców czy anomalii,
  - możliwość tworzenia automatycznych narzędzi do monitorowaniu ruchu sieciowego w celu wykrycia anomalii,
  - możliwość tworzenia narzędzi do wykrywania prób phishingowych poprzez analizowanie treść wiadomości, identyfikowanie podejrzane linki i ostrzegać użytkowników przed zagrożeniami,
  - możliwość tworzenia narzędzi do wykrywania złośliwego oprogramowania,
  - możliwość tworzenia narzędzi wspierających podejmowanie decyzji w sferze bezpieczeństwa i obronności państwa.
- negatywnymi aspektami AI
  - wykorzystanie istniejących narzędzi do sianie dezinformacji, tworzenia fake newsów, tworzenia fałszywych tożsamości, podszywania się pod znane osoby (Fake Data Injection),
  - wykorzystanie AI do generowania złośliwego oprogramowania lub biblioteki w celu wykonania złośliwego kodu lub w celu znalezienia i wykorzystania luk w zabezpieczeniach,
  - wykorzystanie AI do zautomatyzowanych cyberataków: wysyłanie spamu, wiadomości phishingowych, ataków kryptograficznych, itp.,
  - ataki na modele uczenia maszynowego wykorzystane w AI, np. wprowadzanie fałszywych lub zmienionych danych.

Pomocna literatura:

1. Jerzy Surma, Hakowanie Sztucznej Inteligencji, Redakcja naukowa, PWN, 2020
2. Cyberbezpieczeństwo w AI. AI w cyberbezpieczeństwie https://cyberpolicy.nask.pl/cyberbezpieczenstwo-ai-ai-w-cyberbezpieczenstwie/