OUCH! Maj 2023

Sztuczna inteligencja: Co warto o niej wiedzieć

Co to jest i dlaczego warto się tym zainteresować?

Sztuczna inteligencja (AI) opisuje systemy stworzone i zaprogramowane w taki sposób, aby myślały i reagowały jak ludzie. Ciekawostka, poniżej znajduje się pytanie oraz odpowiedź wypracowane przez sztuczną inteligencję ChatGPT.

Czym jest Sztuczna inteligencja?

Sztuczna inteligencja odnosi się do symulacji ludzkiej inteligencji w maszynach, które są zaprogramowane, aby myśleć i uczyć się jak ludzie. Polega na opracowaniu algorytmów, które mogą wykonywać zadania wymagające zwykle ludzkiej inteligencji, takie jak rozpoznawanie mowy, rozumienie języka naturalnego, podejmowanie decyzji i chociażby granie w gry. Istnieje kilka rodzajów sztucznej inteligencji, m.in. AI oparte na regułach, systemy eksperckie i uczenie maszynowe.

To, co czyni AI tak potężną, to fakt, że może ona symulować inteligencję i zdolność rozumienia ludzkiego umysłu, ale może także analizować dużo więcej informacji niż człowiek i robić to znacznie szybciej.

Koncepcja AI nie jest nowa. Pierwsze pomysły AI pojawiają się w powieściach science fiction, sztuczna inteligencja jest czymś, co jest rozwijane od dziesięcioleci. Powodem, dla którego tak wiele się o tym teraz słyszy, jest to, że po raz pierwszy każdy ma możliwość interakcji i zobaczenia prawdziwej funkcjonalności sztucznej inteligencji.

ChatGPT, to czat online napędzany AI. Jest jednym z pierwszych publicznie dostępnych rozwiązań, które jest w stanie odpowiedzieć jak prawdziwy człowiek, rozwiązując jednocześnie test Turinga. Test ten określa zdolność maszyny do wykazywania inteligentnego zachowania poprzez interakcję prawdziwego człowieka z maszyną za pośrednictwem tekstowego kanału czatu. Jeśli człowiek nie mógł stwierdzić, czy rozmawia z maszyną czy osobą, mówi się, że maszyna przeszła test. Rozwiązania AI są dziś pierwszymi publicznie dostępnymi, które zdają test Turinga.

Rozmowy online to jednak dopiero początek tego, co potrafi sztuczna inteligencja. Istnieją obecnie rozwiązania AI, które mogą stworzyć wideo nauczyciela uczącego klasę w dowolnym języku, przeanalizować dokumentację zdrowotną i szybko określić, kto najprawdopodobniej jest chory na raka. Dodatkowo potrafi stworzyć artykuły informacyjne lub eseje na wybrany temat, wygenerować obrazki do książek dla dzieci lub stworzyć kod do nowych programów komputerowych. Choć AI niekoniecznie jest czymś, czego należy się obawiać, istnieją pewne zagrożenia, których należy być świadomym.

Niebezpieczeństwa Sztucznej inteligencji

1. **Podszywanie się**: Rozwiązania AI mogą na podstawie nagranie głosu danej osoby, wykorzystać je do stworzenia w czasie rzeczywistym dźwięku, który brzmi tak jak prawdziwa osoba, mówiąc to, co chce, aby się pod nią podszyć. Oszust może więc nagrać wiadomość głosową, która brzmi jak Ty, oszukując Twoich współpracowników, bank lub członka rodziny, że dzwonisz i prosisz ich o podjęcie jakiegoś działania. Sztuczna inteligencja może to zrobić również ze zdjęciami lub filmami wideo. Rozwiązania te nazywane są Deep Fake. AI może na podstawie istniejącego zdjęcie lub wideo z tobą może użyć je do stworzenia całkowicie nowych zdjęć lub filmów (w tym twojego głosu) ukazujących, że robisz rzeczy, których nigdy nie zrobiłeś.

2. **Błędne odpowiedzi**: Dane lub odpowiedzi generowane przez AI, nie zawsze są doskonałe. Sztuczna inteligencja często wykorzystuje publiczne informacje z internetu, a jej odpowiedzi mogą być manipulowane przez jej twórców. Podczas gdy typowe wyszukiwarki internetowe są zaprojektowane tak, aby dostarczyć użytkownikowi "najlepszą" lub najbardziej poprawną odpowiedź na zapytanie, rozwiązania AI mogą być zaprojektowane tak, aby dać użytkownikowi najbardziej zbliżoną do ludzkiej odpowiedź. To, które jest lepsze, zależy od tego, na czym aktualnie Ci zależy.

3. **Nie wszyscy są równi**: AI staje się bardzo pożądaną technologią. Istnieją setki firm startupowych oferujących różne rozwiązania i usługi sztucznej inteligencji. Wiele z nich chce wykorzystać wzmożone zainteresowanie AI i pod pretekstem uzyskania dostępu do wersji testowej ich produktu, próbują jedynie wykraść informacje osobowe lub karty płatniczej. Z tego powodu bądź ostrożny - nie wszystkie serwisy AI są godne zaufania. Zrób swój rekonesans przed zapisaniem się i korzystaniem z usługi wybranego projektu AI.

4. **Twoja Prywatność:** Podczas korzystania lub interakcji z systemem AI, m.in. takim jak czat online z ChatGPT, bądź świadomy, że wszelkie informacje, które wprowadzasz do systemu mogą być nie tylko przez niego przetwarzane, ale także zachowane i wykorzystane do udzielania odpowiedzi innym. Oznacza to, że jeśli wprowadzisz jakiekolwiek informacje osobiste lub poufne z pracy, informacje te będą przechowywane i potencjalnie udostępniane lub sprzedawane innym. Nie udostępniaj ani nie wprowadzaj żadnych informacji, które uważasz za wrażliwe, osobiste lub poufne.

Przyszłość Sztucznej Inteligencji

Sztuczna inteligencja jest wciąż w bardzo zaawansowanej fazie rozwoju, podobnej do tej, w której ponad dwadzieścia lat temu była sieć Internet. Możemy się spodziewać szybkiej ewolucji i ogólnego przyjęcia AI w wielu branżach, jednakże trudno jest przewidzieć, jaki będzie jej wpływ na naszą przyszłość. Po prostu bądź świadomy, że istnieją takie rozwiązania, a podczas korzystania ze sztucznej inteligencji bądź bardzo ostrożny i zwracaj uwagę jakie informacje wprowadzasz i udostępniasz.

Źródła

ChatGPT: https://chat.openai.com/chat
Test Turinga: https://pl.wikipedia.org/wiki/Test_Turinga

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz