kod szkolenia: E-AI-BEZP / PL e-learning

Bezpieczne korzystanie z AI w organizacji – e-learning

Korzystanie ze sztucznej inteligencji w pracy wiąże się nie tylko z nowymi możliwościami, ale również z ryzykiem dotyczącym danych, wiarygodności odpowiedzi i bezpieczeństwa informacji. Kurs pokazuje, jak świadomie oceniać dane przed przekazaniem ich do AI, ograniczać zakres udostępnianych informacji, weryfikować odpowiedzi modeli językowych oraz rozpoznawać zagrożenia takie jak deepfake czy fałszywe komunikaty. Porusza także zagadnienia odpowiedzialności użytkownika, zasad organizacyjnych, AI Act, RODO i praw autorskich w kontekście codziennego korzystania z AI. Po ukończeniu kursu będziesz potrafić podejmować bardziej świadome decyzje dotyczące tego, jakie informacje przekazywać do AI, jak bezpiecznie z niego korzystać i kiedy wynik wymaga dodatkowej weryfikacji.

Dostęp do kursu e-learningowego przysługuje przez 365 dni.

Odbiorcy szkolenia

- Pracownicy wykorzystujący narzędzia generatywnej AI w codziennych zadaniach
- Osoby pracujące z dokumentami, danymi i informacjami wewnętrznymi organizacji
- Menedżerowie i liderzy zespołów korzystających z narzędzi AI
- Specjaliści marketingu, sprzedaży, HR, administracji i obsługi klienta
- Osoby wykorzystujące AI do analizy informacji, tworzenia treści i przygotowywania rekomendacji
- Użytkownicy chcący ograniczyć ryzyko związane z przekazywaniem danych i wykorzystywaniem wyników generowanych przez AI

Korzyści

1. Klasyfikacja danych – nauczysz się oceniać informacje pod względem poziomu poufności oraz rodzaju danych przed przekazaniem ich do narzędzia AI.
2. Bezpieczne przekazywanie informacji – zastosujesz minimalizację danych, anonimizację i dane przykładowe, aby ograniczać ilość rzeczywistych informacji przekazywanych do AI.
3. Świadome korzystanie z narzędzi AI – będziesz potrafić sprawdzić, czy dane narzędzie jest zatwierdzone przez organizację i jaki zakres informacji można w nim przetwarzać.
4. Weryfikacja odpowiedzi AI – rozpoznasz ryzyko halucynacji i nauczysz się sprawdzać źródła, fakty, autorów, instytucje oraz aktualność informacji.
5. Rozpoznawanie oszustw – zwiększysz umiejętność identyfikowania deepfake'ów, fałszywych wiadomości i prób manipulacji wykorzystujących presję czasu.
6. Odpowiedzialne wykorzystanie wyników – nauczysz się oceniać, czy odpowiedź AI może zostać bezpośrednio wykorzystana, wymaga dodatkowej weryfikacji czy konsultacji zgodnie z zasadami organizacji.
7. Bezpieczeństwo i zgodność – uporządkujesz podstawowe zasady dotyczące AI Act, RODO, praw autorskich i odpowiedzialności użytkownika w codziennej pracy z AI.

Program szkolenia

Moduł 1: Dane wprowadzane do AI

Moduł obejmuje klasyfikację informacji według poziomu poufności i rodzaju danych oraz zasady oceny, jakie informacje można bezpiecznie przekazywać do narzędzi AI zgodnie z zasadami organizacji.

Moduł 2: Bezpieczny prompt

Moduł koncentruje się na ograniczaniu ryzyka poprzez anonimizację, stosowanie danych przykładowych, minimalizację zakresu informacji oraz rozróżnienie anonimizacji i pseudonimizacji.

Moduł 3: Halucynacje i błędne odpowiedzi

Moduł wyjaśnia przyczyny powstawania błędnych lub niepotwierdzonych odpowiedzi AI oraz zasady weryfikowania źródeł, autorów, instytucji, dat i aktualności informacji.

Moduł 4: Nowe formy oszustw

Moduł omawia zagrożenia związane z deepfake audio i wideo, fałszywymi wiadomościami, presją czasu w socjotechnice oraz oceną wiarygodności podejrzanych materiałów.

Moduł 5: Prawo, odpowiedzialność i zasady organizacji

Moduł porusza podstawowe obowiązki użytkownika, zagadnienia AI Act, RODO i praw autorskich oraz odpowiedzialność za sposób wykorzystania treści generowanych przez AI.

Test końcowy

Oczekiwane przygotowanie uczestnika

Nie jest wymagane specjalne przygotowanie uczestników ani wcześniejsze doświadczenie z narzędziami sztucznej inteligencji.

Szkolenie obejmuje

Dostęp do kursu e-learningowego przysługuje przez 365 dni.
Czas trwania szkolenia: 90 minut

Czas trwania

1 dni / 1 godzin

Język

język: polski