



OŚRODEK
SZKOLENIA
DOKSZTAŁCANIA I
DOSKONALENIA
KADR KURSÓR
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,5 / 5

1 002 oceny

AI i cyberbezpieczeństwo – bezpieczne wykorzystanie narzędzi sztucznej inteligencji w pracy

Numer usługi 2026/10/15/30963/3881560

-  Usługa szkoleniowa
-  zdalna w czasie rzeczywistym
-  Zajęcia grupowe
-  14:00 h
-  19.11.2026 do 04.12.2026

2 000,00 PLN brutto
2 000,00 PLN netto
142,86 PLN brutto/h
142,86 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie przeznaczone jest dla pracowników wykorzystujących lub planujących wykorzystywać narzędzia sztucznej inteligencji w pracy, w szczególności pracowników administracyjnych, biurowych, HR, marketingu, sprzedaży, obsługi klienta, kadry kierowniczej oraz właścicieli przedsiębiorstw.

Oferta dostępna również dla uczestników projektów:

- Kierunek – Rozwój WUP Toruń
- Usługi rozwojowe województwa śląskiego
- Małopolski pociąg do kariery – sezon 1
- Nowy start w Małopolsce z EURESem1

Minimalna liczba uczestników

3

Maksymalna liczba uczestników

30

Data zakończenia rekrutacji

12-11-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do bezpiecznego wykorzystywania narzędzi generatywnej sztucznej inteligencji w środowisku zawodowym. Uczestnik po zakończeniu szkolenia identyfikuje ryzyka związane z przekazywaniem informacji do narzędzi AI, rozróżnia dane, które mogą i nie powinny być wprowadzane do ogólnodostępnych systemów AI, stosuje zasady bezpiecznego tworzenia poleceń, weryfikuje treści generowane przez AI oraz rozpoznaje cyberzagrożenia wykorzystujące sztuczną inteligencję.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje ryzyka związane z wykorzystaniem generatywnej AI w organizacji.	wskazuje zagrożenia związane z przekazywaniem danych do narzędzi AI;	Test teoretyczny
	rozpoznaje ryzyko ujawnienia informacji poufnych;	Test teoretyczny
	wskazuje ograniczenia wiarygodności treści generowanych przez AI.	Test teoretyczny
	rozróżnia informacje publiczne, wewnętrzne i poufne;	Test teoretyczny
Klasyfikuje informacje pod kątem możliwości ich wykorzystania w narzędziach AI.	rozpoznaje dane, których nie należy przekazywać do ogólnodostępnych narzędzi AI;	Test teoretyczny
	wskazuje możliwość anonimizacji lub ograniczenia zakresu danych.	Test teoretyczny
Dobiera bezpieczny sposób korzystania z narzędzi AI.	rozpoznaje bezpieczne i ryzykowne prompty;	Test teoretyczny
	wskazuje informacje, które należy usunąć przed przekazaniem treści do AI;	Test teoretyczny
	stosuje zasadę minimalizacji przekazywanych danych.	Test teoretyczny
	rozpoznaje możliwość wystąpienia halucynacji;	Test teoretyczny
Weryfikuje treści generowane przez AI.	wskazuje informacje wymagające dodatkowej weryfikacji;	Test teoretyczny
	dobiera sposób sprawdzenia wiarygodności rezultatu.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje cyberzagrożenia wykorzystujące sztuczną inteligencję.	identyfikuje phishing i socjotechnikę wspomagane AI;	Test teoretyczny
	rozpoznaje ryzyko wykorzystania deepfake;	Test teoretyczny
	wskazuje cechy treści wymagających dodatkowej weryfikacji.	Test teoretyczny
Dobiera sposób reagowania na incydent związany z wykorzystaniem AI.	wskazuje sposób postępowania po przypadkowym ujawnieniu informacji;	Test teoretyczny
	określa zasady zgłoszenia incyduentu;	Test teoretyczny
	wskazuje działania ograniczające jego skutki.	Test teoretyczny
	wskazuje zasady odpowiedzialnego korzystania z AI;	Test teoretyczny
Stosuje zasady bezpiecznego wykorzystywania AI w środowisku pracy.	określa konieczność weryfikacji rezultatów przed ich wykorzystaniem;	Test teoretyczny
	rozpoznaje działania niezgodne z zasadami bezpieczeństwa informacji.	Test teoretyczny

Kwalifikacje i kompetencje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://standardgccs.com/qualifications/>

Strona internetowa Instytucji Walidującej: <https://icvc.eu/>

Informacje

Nazwa Podmiotu prowadzącego walidację	ICVC Certyfikacja Sp. z o.o.
Nazwa Podmiotu certyfikującego	Talent Odyssey Ltd, Ateny, Grecja

Program

Godziny realizacji szkolenia:

- Szkolenie obejmuje 16 godzin edukacyjnych tj. 12 godzin zegarowych.
- Walidacja wliczona jest w czas trwania zajęć.
- Przerwy nie są wliczone w czas trwania zajęć.

Metody pracy:

- wykład interaktywny, prezentacja, analiza przypadków, ćwiczenia praktyczne, praca z narzędziami AI, dyskusja.

Certyfikat ukończenia:

- Zaświadczenie wydane na podstawie § 23 ust. 4 rozporządzenia Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz. U. poz. 2175).
- Certyfikat ICVC - "Bezpieczna praca z narzędziami sztucznej inteligencji " - kod ICVC-C-Q04

Program szkolenia:

16 godz. (7 godz. teorii, 8,34 godz. praktyki, 0,66 godz. walidacji)

Moduł 1. Generatywna sztuczna inteligencja w środowisku pracy

- czym jest generatywna AI,
- sposób działania modeli językowych,
- ChatGPT, Microsoft Copilot, Gemini i inne narzędzia,
- zastosowania biznesowe,
- możliwości i ograniczenia AI,
- odpowiedzialność użytkownika.

Moduł 2. Dane firmowe i poufność podczas korzystania z AI

- dane osobowe,
- informacje poufne,
- tajemnica przedsiębiorstwa,
- dane klientów i kontrahentów,
- dokumenty wewnętrzne,
- klasyfikowanie informacji przed użyciem AI,
- anonimizacja i minimalizacja danych,
- analiza przykładowych promptów pod kątem bezpieczeństwa.

Moduł 3. Bezpieczne korzystanie z narzędzi AI

- tworzenie promptów bez ujawniania zbędnych informacji,
- minimalizacja zakresu przekazywanych danych,
- bezpieczna praca z dokumentami,
- ocena odpowiedzi modelu,
- halucynacje,
- weryfikowanie informacji,
- praktyczne tworzenie bezpiecznych promptów.

Moduł 4. AI jako narzędzie cyberprzestępców

- phishing generowany przy pomocy AI,
- fałszywe wiadomości,
- automatyzacja socjotechniki,
- podszywanie się pod pracowników i kontrahentów,
- deepfake,
- dezinformacja,
- analiza przykładów potencjalnych ataków.

Moduł 5. Rozpoznawanie zagrożeń i reagowanie na incydenty

- rozpoznawanie podejrzanych treści,

- weryfikowanie źródeł,
- reagowanie na próbę manipulacji,
- przypadkowe przekazanie informacji do AI,
- zgłaszanie incydentów,
- ograniczanie skutków zdarzenia.

Moduł 6. Zasady bezpiecznego wykorzystania AI w organizacji

- dobre praktyki korzystania z AI,
- zasady dopuszczania danych do przetwarzania,
- odpowiedzialność pracownika,
- weryfikacja rezultatów,
- zasady tworzenia wewnętrznych wytycznych dotyczących AI.

Walidacja

Szkolenie realizowane jest w terminie 19.11.2026 - 20.11.2026. Po jego zakończeniu uczestnicy przystępują do egzaminu certyfikującego organizowanego i ocenianego przez podmiot zewnętrzny. Czas oczekiwania na wynik walidacji wynosi do 10 dni roboczych od dnia egzaminu.

- okres realizacji szkolenia (19.11.2026 - 20.11.2026)
- okres oczekiwania na wynik walidacji (do 04.12.2026)

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Generatywna sztuczna inteligencja w środowisku pracy/Dane firmowe i poufność podczas korzystania z AI/Bezpieczne korzystanie z narzędzi AI	Zajęcia	Stanisław Hady-Głowiak	19-11-2026	08:30	10:30	02:00
2 z 11 -	Przerwa	-	19-11-2026	10:30	11:00	00:30
3 z 11 Generatywna sztuczna inteligencja w środowisku pracy/Dane firmowe i poufność podczas korzystania z AI/Bezpieczne korzystanie z narzędzi AI	Zajęcia	Stanisław Hady-Głowiak	19-11-2026	11:00	13:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 11 -	Przerwa	-	19-11-2026	13:00	13:30	00:30
5 z 11 Generatywna sztuczna inteligencja w środowisku pracy/Dane firmowe i poufność podczas korzystania z AI/Bezpieczne korzystanie z narzędzi AI	Zajęcia	Stanisław Hady-Głowiak	19-11-2026	13:30	15:30	02:00
6 z 11 Bezpieczne korzystanie z narzędzi AI/AI jako narzędzie cyberprzestępców/Rozpoznanie zagrożeń i reagowanie na incydenty/Zasady bezpiecznego wykorzystania AI w organizacji	Zajęcia	Stanisław Hady-Głowiak	20-11-2026	08:30	10:30	02:00
7 z 11 -	Przerwa	-	20-11-2026	10:30	11:00	00:30
8 z 11 Bezpieczne korzystanie z narzędzi AI/AI jako narzędzie cyberprzestępców/Rozpoznanie zagrożeń i reagowanie na incydenty/Zasady bezpiecznego wykorzystania AI w organizacji	Zajęcia	Stanisław Hady-Głowiak	20-11-2026	11:00	13:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 11 -	Przerwa	-	20-11-2026	13:00	13:30	00:30
10 z 11 Bezpieczne korzystanie z narzędzi AI/AI jako narzędzie cyberprzestępców/Rozpoznawanie zagrożeń i reagowanie na incydenty/Zasady bezpiecznego wykorzystania AI w organizacji	Zajęcia	Stanisław Hady-Głowiak	20-11-2026	13:30	15:00	01:30
11 z 11 -	Walidacja	-	20-11-2026	15:00	15:30	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:30
w tym suma godzin walidacji	00:30
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	16:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 000,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	

Koszt przypadający na 1 uczestnika netto	2 000,00 PLN
Koszt osobogodziny brutto	142,86 PLN
Koszt osobogodziny netto	142,86 PLN
W tym koszt walidacji brutto	70,00 PLN
W tym koszt walidacji netto	70,00 PLN
W tym koszt certyfikowania brutto	100,00 PLN
W tym koszt certyfikowania netto	100,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Stanisław Hady-Głowiak

Doktor nauk prawnych, radca prawny, partner w spółce KHG Radcowie Prawni, wieloletni pracownik administracji publicznej, audytor wiodący wg normy PN/EN ISO 27001, autor wielu publikacji naukowych, branżowych, doświadczony Inspektor Ochrony Danych, absolwent studiów doktoranckich na Wydziale Prawa i Administracji Uniwersytetu Śląskiego, wykładowca na UE w Katowicach oraz prowadzący szkolenia, kursy i wykłady na uczelniach publicznych, ekspert ds. bezpieczeństwa informacji. Posiada bogate doświadczenie w sektorze publicznym zarówno w organach administracji publicznej, jak i jednostek samorządu terytorialnego, w tym jako audytor i ekspert w dziedzinie bezpieczeństwa informacji i prawnego otoczenia funkcjonowania organizacji. Posiada doświadczenie zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W ramach przygotowania do szkolenia uczestnicy otrzymają materiały dydaktyczne w formie elektronicznej. Zostaną one przesłane w postaci plików i dokumentów (np. PDF, prezentacje, arkusze informacyjne).

Materiały będą wysyłane na podane wcześniej adresy e-mail uczestników. Prosimy o upewnienie się, że wiadomości nie trafiają do folderu SPAM oraz o zapisanie plików na własnych urządzeniach.

Warunki uczestnictwa

1. Umiejętność obsługi komputera w stopniu dobrym.
2. Uczestnik zobowiązany jest do korzystania z komputera wyposażonego w sprawną kamerę internetową, mikrofon oraz głośniki, umożliwiające aktywny udział w szkoleniu i swobodną komunikację z trenerem oraz pozostałymi uczestnikami.
3. Uczestnik zobowiązany jest do korzystania z włączonej kamery internetowej przez cały czas trwania zajęć, z wyłączeniem przerw. Kamera powinna być ustawiona w sposób zapewniający stałą i wyraźną widoczność twarzy uczestnika.
4. **Obowiązek uczestnictwa w co najmniej 80% zajęć. Obecność potwierdzana jest na podstawie raportu z logowań z Platformy Zoom.**

Nie jest wymagane wcześniejsze doświadczenie w korzystaniu z narzędzi AI.

Informacje dodatkowe

Kluczowe elementy organizacyjne oraz etapy uczestnictwa w kursie:

- **Prezentacje na żywo** – trener prowadzi interaktywne sesje online, w trakcie których omawia kluczowe zagadnienia i odpowiada na pytania uczestników.
- **Zadania praktyczne** – uczestnicy realizują ćwiczenia związane z tematyką szkolenia; każde zadanie jest oceniane przez prowadzącego.
- **Egzamin końcowy** – po zakończeniu wszystkich modułów uczestnicy przystępują do testu końcowego weryfikującego poziom opanowania materiału.

Podstawa zwolnienia z vat: art 43 ust.1 pkt 26a ustawy o VAT

Warunki techniczne

Warunki techniczne szkolenia na platformie Zoom:

1. Sprzęt komputerowy:
 - Wymagany komputer z dostępem do internetu wraz z kamerą.
2. Przeglądarka internetowa
 - Zalecane przeglądarki: Google Chrome, Mozilla Firefox, Safari.
3. Stabilne połączenie internetowe o minimalnej prędkości 5 Mb/s (pobieranie i wysyłanie)
4. Platforma Zoom:
 - Konieczne pobranie i zainstalowanie najnowszej wersji aplikacji Zoom przed szkoleniem.
 - Aktywne konto Zoom (możliwość utworzenia bezpłatnego konta).
5. Dźwięk i słuchawki:
 - Zalecane użycie słuchawek z mikrofonem dla lepszej jakości dźwięku.
 - Sprawdzenie działania dźwięku przed rozpoczęciem szkolenia.
6. Przygotowanie przed sesją:
 - Testowanie sprzętu i połączenia przed planowanym szkoleniem.
 - Zapewnienie cichego miejsca pracy dla minimalizacji zakłóceń.

Zapewnienie powyższych warunków technicznych umożliwi płynny przebieg szkolenia na platformie Zoom, zminimalizuje zakłócenia i zagwarantuje efektywną interakcję między prowadzącym a uczestnikiem.

Uczestnikom zapewnione jest wsparcie techniczne i organizacyjne przez cały okres realizacji szkolenia. Problemy techniczne można zgłaszać mailowo: szkolenia.lublin@kursor.edu.pl lub telefonicznie: 531191181. Wsparcie obejmuje w szczególności pomoc w logowaniu i obsłudze platformy, dostępie do materiałów oraz rozwiązywaniu problemów technicznych. Instrukcja korzystania z platformy przekazywana jest uczestnikom przed rozpoczęciem szkolenia.

Dlaczego warto skorzystać z naszej usługi:

Godziny realizacji szkolenia:

- Szkolenie obejmuje 8 godzin edukacyjnych tj. 6 godzin zegarowych.
- Walidacja wliczona jest w czas trwania zajęć.
- Przerwy nie są wliczone w czas trwania zajęć.

Metody pracy:

- wykład interaktywny, prezentacja, analiza przypadków, ćwiczenia praktyczne, praca z narzędziami AI, dyskusja.

Kontakt



Anna Mirosław

E-mail szkolenia.lublin@kursor.edu.pl

Telefon (+48) 531 191 181