



Centrum
Szkoleniowe

Progres Jagóra i
Nordyński Spółka
Jawna

★★★★★ 4,5 / 5

1 199 ocen

AI i cyberbezpieczeństwo – bezpieczne wykorzystanie technologii w organizacji - 20 godzin (20x60minut) - zdalnie w czasie rzeczywistym *

Numer usługi 2026/07/27/11855/3712440

- 🏠 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 👤 Zajęcia indywidualne
- 🕒 20:00 h
- 📅 24.08.2026 do 16.09.2026

5 904,00 PLN brutto
4 800,00 PLN netto
295,20 PLN brutto/h
240,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Usługa skierowana jest do osób dorosłych wykorzystujących lub planujących wykorzystywać narzędzia AI w pracy. Przeznaczona jest dla pracowników administracji, kadry kierowniczej, HR, marketingu, sprzedaży, obsługi klienta oraz osób odpowiedzialnych za ochronę danych, bezpieczeństwo informacji i cyberbezpieczeństwo. Wymagana jest jedynie podstawowa obsługa komputera i Internetu.

UWAGA: Usługa adresowana jest między innymi dla Uczestników Projektów:

Grupa docelowa usługi

- Małopolski Pociąg do Kariery - sezon 1 (WUP Kraków)
- Nowy start w Małopolsce z EURESem (WUP Kraków)
- NetBon 2 (WUP Kraków)
- Kierunek - Rozwój (WUP Toruń)
- Zawodowa Reaktywacja (Bełchatowsko-Kleszczowski Park Przemysłowo-Technologiczny)
- ABONament na rozwój - Instytut Nauk Społeczno-Ekonomicznych
- Łódzkie Bony Rozwojowe - Fundacja Inicjatyw Regionalnych
- Usługa rozwojowa adresowana również dla Uczestników projektu Zachodniopomorskie Bony Szkoleniowe

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

1

Data zakończenia rekrutacji

21-08-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Cel

Cel edukacyjny

Celem usługi jest przygotowanie uczestników do świadomego, bezpiecznego i zgodnego z przepisami wykorzystywania narzędzi sztucznej inteligencji w pracy. Po ukończeniu szkolenia uczestnicy będą potrafili wykorzystywać AI do usprawniania procesów zawodowych, tworzyć skuteczne polecenia (prompty), identyfikować zagrożenia cyberbezpieczeństwa oraz stosować zasady ochrony danych osobowych i bezpieczeństwa informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik charakteryzuje możliwości i ograniczenia narzędzi sztucznej inteligencji oraz wyjaśnia podstawowe zagadnienia związane z cyberbezpieczeństwem, ochroną danych osobowych, AI Act i odpowiedzialnym wykorzystaniem AI w organizacji.	-rozdziela podstawowe rodzaje narzędzi AI i wskazuje przykłady ich zastosowania, -omawia najważniejsze zagrożenia związane z wykorzystaniem AI w środowisku pracy, wyjaśnia podstawowe obowiązki wynikające z przepisów dotyczących ochrony danych osobowych i AI Act.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wykorzystuje narzędzia sztucznej inteligencji do realizacji zadań zawodowych z zachowaniem zasad bezpieczeństwa informacji i ochrony danych.	-przygotowuje poprawnie sformułowany prompt dostosowany do określonego zadania, -ocenia wiarygodność odpowiedzi wygenerowanych przez AI oraz wskazuje sposoby ich weryfikacji, -identyfikuje potencjalne zagrożenia związane z wykorzystaniem AI podczas wykonywania zadania.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady odpowiedzialnego i bezpiecznego korzystania z narzędzi sztucznej inteligencji oraz podejmuje działania wspierające bezpieczeństwo cyfrowe organizacji.	-wskazuje właściwy sposób postępowania w sytuacji podejrzenia incydentu bezpieczeństwa, -uzasadnia konieczność stosowania zasad ochrony danych oraz bezpieczeństwa informacji podczas korzystania z AI.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

MODUŁ I. Wykorzystanie sztucznej inteligencji w środowisku pracy biurowej – podstawy, zastosowania i bezpieczeństwo

Charakterystyka rozwiązań opartych na sztucznej inteligencji

Przegląd dostępnych technologii AI, w tym modeli językowych (LLM), oraz omówienie ich zastosowania w realizacji zadań administracyjnych, organizacyjnych i biurowych.

Identyfikacja ryzyk związanych z wdrażaniem AI

Analiza zagrożeń wynikających z wykorzystania narzędzi sztucznej inteligencji w organizacji, ze szczególnym uwzględnieniem bezpieczeństwa informacji, poufności danych oraz odpowiedzialnego korzystania z technologii.

Projektowanie skutecznych poleceń dla systemów AI

Zasady formułowania zapytań umożliwiających uzyskanie precyzyjnych i użytecznych odpowiedzi. Omówienie metod zwiększających jakość generowanych rezultatów oraz praktyczne zastosowanie technik tworzenia promptów.

Bezpieczeństwo dostępu do narzędzi AI

Dobre praktyki w zakresie ochrony kont użytkowników, zarządzania uprawnieniami oraz stosowania mechanizmów uwierzytelniania wieloskładnikowego w środowisku pracy.

MODUŁ II. Uwarunkowania prawne i ochrona danych podczas korzystania z narzędzi AI

Regulacje dotyczące wykorzystania sztucznej inteligencji

Omówienie obowiązujących i planowanych przepisów regulujących stosowanie AI, w tym podstawowych założeń AI Act oraz ich znaczenia dla organizacji.

Ochrona danych osobowych

Zasady zgodnego z RODO przetwarzania danych z wykorzystaniem narzędzi AI, w tym ograniczanie zakresu danych, ocena ryzyka oraz bezpieczne praktyki ich przetwarzania.

Przygotowanie danych do wykorzystania przez systemy AI

Praktyczne metody anonimizacji i pseudonimizacji danych oraz ich znaczenie dla zachowania poufności informacji przetwarzanych w środowisku cyfrowym.

Prawa autorskie i odpowiedzialność za treści generowane przez AI

Omówienie zagadnień związanych z własnością intelektualną, licencjonowaniem rozwiązań AI oraz zasadami korzystania z materiałów tworzonych przy wsparciu sztucznej inteligencji.

MODUŁ III. Cyberbezpieczeństwo i zagrożenia wykorzystujące sztuczną inteligencję

Nowoczesne metody socjotechniczne

Charakterystyka współczesnych zagrożeń wykorzystujących AI, w tym phishingu nowej generacji, oraz sposobów ich rozpoznawania.

Fałszywe materiały audio i wideo (Deepfake)

Mechanizmy powstawania materiałów typu deepfake, ich wpływ na bezpieczeństwo organizacji oraz metody weryfikacji autentyczności informacji i tożsamości.

Bezpieczna współpraca z systemami AI

Omówienie prób manipulowania modelami sztucznej inteligencji oraz sposobów ograniczania ryzyka uzyskania nieprawidłowych lub zmanipulowanych wyników.

Analiza przykładów naruszeń bezpieczeństwa

Przegląd rzeczywistych przypadków wykorzystania AI w cyberatakach oraz identyfikacja dobrych praktyk ograniczających ryzyko wystąpienia podobnych incydentów.

MODUŁ IV. Wykorzystanie AI do analizy informacji i automatyzacji procesów

Ocena wiarygodności informacji generowanych przez AI

Metody weryfikowania poprawności odpowiedzi uzyskiwanych z systemów AI oraz wykorzystanie wiarygodnych źródeł do potwierdzania informacji.

Bezpieczna analiza danych z wykorzystaniem AI

Wykorzystanie narzędzi sztucznej inteligencji do przygotowywania analiz, zestawień i raportów przy zachowaniu zasad bezpieczeństwa informacji.

Automatyzacja procesów administracyjnych

Możliwości wykorzystania AI do usprawniania powtarzalnych czynności oraz wspierania realizacji procesów biurowych z zachowaniem wymogów bezpieczeństwa.

Ocena narzędzi wspierających pracę z AI

Kryteria wyboru bezpiecznych aplikacji, rozszerzeń i usług wspomagających pracę użytkownika oraz identyfikacja potencjalnych zagrożeń wynikających z ich stosowania.

MODUŁ V. Organizacja bezpiecznej pracy z AI i weryfikacja kompetencji

Postępowanie w przypadku incydentów bezpieczeństwa

Omówienie zasad reagowania na zdarzenia związane z naruszeniem bezpieczeństwa danych lub niewłaściwym wykorzystaniem narzędzi AI.

Budowanie kultury cyberbezpieczeństwa w organizacji

Rola pracowników w ograniczaniu ryzyka cyberzagrożeń, rozwijanie świadomości bezpieczeństwa oraz stosowanie dobrych praktyk podczas codziennej pracy.

Zasady korzystania z narzędzi AI w organizacji

Opracowanie podstawowych wytycznych dotyczących bezpiecznego, odpowiedzialnego i zgodnego z przepisami wykorzystania sztucznej inteligencji w środowisku pracy.

Jest to szkolenie indywidualne; za godzinę przyjmuje się 60min.

Szkolenie składa się z 20 godzin zegarowych. Harmonogram uwzględnia przerwy.

Wszystkie godziny szkoleniowe stanowią praktyczną naukę.

Walidacja składa się z testu teoretycznego z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	24-08-2026	17:00	18:45	01:45
2 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	25-08-2026	17:00	18:45	01:45
3 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	26-08-2026	17:00	18:45	01:45
4 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	31-08-2026	17:00	18:45	01:45
5 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	01-09-2026	17:00	18:45	01:45
6 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	02-09-2026	17:00	18:45	01:45
7 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	07-09-2026	17:00	18:45	01:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	08-09-2026	17:00	18:45	01:45
9 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	09-09-2026	17:00	18:45	01:45
10 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	14-09-2026	17:00	18:45	01:45
11 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	15-09-2026	17:00	18:00	01:00
12 z 13 AI i cyberbezpieczeństwo	Zajęcia	Dariusz Nowak	16-09-2026	17:00	18:00	01:00
13 z 13 -	Walidacja	Dariusz Nowak	16-09-2026	18:15	18:45	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	20:00
w tym suma godzin zajęć	19:30
w tym suma godzin walidacji	00:30
Suma godzin dydaktycznych bez przerw	26:30

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 904,00 PLN
Koszt przypadający na 1 uczestnika netto	4 800,00 PLN
Koszt osobogodziny brutto	295,20 PLN
Koszt osobogodziny netto	240,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	20:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Dariusz Nowak

Trener posiada wieloletnie doświadczenie zawodowe w obszarze technologii informatycznych, transformacji cyfrowej oraz wdrażania rozwiązań wspierających zarządzanie organizacją. Realizował wdrożenia systemów ERP i MRP oraz świadczył usługi z zakresu obsługi informatycznej przedsiębiorstw. Prowadzi szkolenia z zakresu nowoczesnych technologii, sztucznej inteligencji, cyberbezpieczeństwa, e-administracji oraz systemów wspomagających zarządzanie, w tym szkolenia dla pracowników administracji publicznej oraz przedsiębiorstw. Doświadczenie trenera zdobyte nie wcześniej niż 5 lat przed opublikowaniem usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne

- prezentacja multimedialna przygotowana przez trenera,
- skrypt lub materiały szkoleniowe w formie elektronicznej (PDF),
- instrukcje i checklisty dotyczące bezpiecznego korzystania z AI,
- przykładowe polityki korzystania z narzędzi AI w organizacji,
- zestaw dobrych praktyk z zakresu cyberbezpieczeństwa i ochrony danych,
- przykładowe scenariusze promptów oraz szablony ich tworzenia,
- studia przypadków dotyczące wykorzystania AI i incydentów cyberbezpieczeństwa,
- zestaw ćwiczeń praktycznych i kart pracy.

Narzędzia wykorzystywane podczas szkolenia

- ChatGPT,
- Google Gemini,
- NotebookLM,
- Google AI Studio,
- Microsoft Copilot (jeżeli dostępny),
- Canva AI (Magic Write, Magic Design),
- Miro lub inne narzędzie do pracy warsztatowej,
- przeglądarka internetowa z dostępem do wybranych serwisów.

Materiały źródłowe i akty prawne

- AI Act,
- RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679),
- wytyczne dotyczące cyberbezpieczeństwa publikowane przez CERT Polska,
- materiały edukacyjne

Informacje dodatkowe

- Zapewniamy podstawowe materiały szkoleniowe.
- Za godzinę zajęć przyjmuje się 60 minut.
- Każdy Uczestnik po zakończeniu szkolenia otrzymuje zaświadczenie.
- Na zakończenie kursu uczestnik przystępuje do walidacji - testu teoretycznego z wynikiem generowanym automatycznie.

Usługa ma charakter **przykładowy**. Zapraszamy do kontaktu w celu spersonalizowania oferty.

Warunki techniczne

„Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników, oraz zastosowanego narzędzia.”

SZCZEGÓŁOWE INFORMACJE:

Udostępniony w korespondencji mailowej link dostępowy do zajęć ważny jest do dnia zakończenia realizacji usługi zgodnie z obecną kartą.

określone warunki techniczne do udziału w usłudze:

- rodzaj platformy – teams
- oprogramowanie – Windows / Mac OS X
- wymagania sprzętowe – PC lub laptop z dostępem do Internetu, kamerką i mikrofonem
- prędkość Internetu:
- minimalna szybkość dla połączeń video 128 kb/s
- zalecana: 300 kb/s

Warunki minimalne łącza internetowego prędkość pobierania – 1 Mb/s; prędkość wysyłania 1 Mb/s.

Kontakt



Anna Kuźnicka

E-mail anna.kuznicka@progres.edu.pl

Telefon (+48) 795 532 467