



FIRMA HANDLOWO-
USŁUGOWA "MIJA"
MICHAŁ JAROSZ
★★★★★ 4,8 / 5
207 ocen

Sztuczna Inteligencja Generatywna z naciskiem na cyberbezpieczeństwo. Narzędzia, Strategie, Praktyka - szkolenie

Numer usługi 2025/08/07/157015/2927640

📍 Kielce / stacjonarna
🏠 Usługa szkoleniowa
🕒 16 h
📅 06.10.2025 do 07.10.2025

4 000,00 PLN brutto
4 000,00 PLN netto
250,00 PLN brutto/h
250,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie dedykowane jest dla właścicieli i pracowników firm oraz administracji publicznej, a także osób indywidualnych w celu wypełnienia zobowiązań prawnych oraz podniesienia kompetencji w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych, cyberbezpieczeństwa we współpracy z AI zapewniając ciągłość działania podmiotu.
Minimalna liczba uczestników	7
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	05-10-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Cele szkolenia to uzyskanie świadomości i kompetencji w zakresie we współpracy z AI, wymagań prawnych oraz norm, standardów pisania promptów, kodowania AI, w celu stosowania technicznych i organizacyjnych metod ochrony informacji, danych osobowych oraz stosowanie odpowiedniego zarządzania bezpieczeństwem informacji (ochroną

danych osobowych), zdobycie wiedzy w dziedzinie stosowania etycznego kodowania promptów AI, zabezpieczeń w zakresie zarządczym, technicznym,uwzględniając aspekt organizacyjny

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Uczestnik zna podstawowe wymagania prawne, standardy we współpracy z AI i normy dotyczące bezpieczeństwa informacji (cyberbezpieczeństwa AI oraz aspektów organizacyjnych, technicznych i zarządczych w kodowaniu promptów AI. Poznał źródła cyberzagrożeń AI i wektora ataku takiego cyberzagrożenia oraz etyki we współpracy z AI	Pytania dotyczące danego zakresu tematycznego.	Test teoretyczny
Umiejętności: Identyfikuje zagrożenia w organizacji wraz z doborem odpowiedniej reakcji na zagrożenia związane z cyberbezpieczeństwem AI, dobiera działania, jakie należy podjąć w celu ich niwelowania. Wybiera działania zarządcze w zakresie stosowania bezpieczeństwa informacji w oparciu o etykę we współpracy z AI	Pytania dotyczące danego zakresu tematycznego.	Test teoretyczny
Kompetencje: Uczestnik zdobył kompetencje dotyczące wymagań technicznych, organizacyjnych i zarządczych z zakresu bezpieczeństwa informacji we współpracy z AI, w tym działań zarządczych, jakie należy podjąć w celu zapewnienia bezpieczeństwa informacji, danych osobowych oraz zasobów organizacji niwelujących wystąpienie cyberzagrożenia we współpracy z AI	Pytania dotyczące danego zakresu tematycznego.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień 1

Blok 1: Fundamenty LLM

- Wprowadzenie do LLM, RAG, agentów
- Jak działają LLM'y – perspektywa praktyczna
- Ewolucja modeli - przykłady
- Vector DB, grafywność, RAG - szybki przegląd
- Agenci: MCP, A2A - o co chodzi?

Blok 2: Predictive Coding + promptowanie

- Predictive Coding – co to znaczy?
- Parametry modeli - co realnie zmieniają?
- Podstawy dobrego prompta
- Ćwiczenie: wpływ parametrów na wynik (testy i kod)

Blok 3: Techniki promptowania + warsztaty

- Zero-shot vs Few-shot
- Chain-of-Thought (CoT) i Self-Consistency
- ReAct (Reactive Prompting)
- Prompt-chaining, MetaPrompting, Decision Trees
- RAG i GraphRAG – teoria i praktyka
- Warsztaty: Testujemy techniki promptowania

Dzień 2

Blok 4: Copilot + Debug + VSCode

- Copilot w IDE i GitHub Organization
- C++ i legacy code – realne ograniczenia
- Debugowanie i testowanie z Copilotem/Cursorem

Blok 5: Projekty + warsztaty. Test-Gen

- Warsztaty: Test-Gen (Meta, Cover Agent)
- Projekty grupowe - propozycje

Blok 6: Bezpieczeństwo + Etyka+Trendy

- Prompt Injection / Prompt Leaking - przykłady
- Jailbreaking, Waluigi Effect, game simulations
- Jak się bronić? (praktycznie)
- Checklist: bezpieczeństwo AI w SDLC
- Halucynacje i biasy - jak sobie radzić?
- AI Pair Programmers – co dalej?
- LLM Ops - operacjonalizacja AI w SDLC
- Top narzędzia i biblioteki (subiektywnie)
- Podsumowanie i następne kroki
- Materiały dodatkowe (dla chętnych)

Harmonogram

Liczba przedmiotów/zajęć: 14

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Podstawowe informacje dotyczące szkolenia, pretest.	-	06-10-2025	08:30	08:45	00:15
2 z 14 Blok 1: Fundamenty LLM	PIOTR DYNIAKOWSKI	06-10-2025	08:45	10:00	01:15
3 z 14 Przerwa	PIOTR DYNIAKOWSKI	06-10-2025	10:00	10:10	00:10
4 z 14 Blok 2: Predictive Coding + promptowanie	PIOTR DYNIAKOWSKI	06-10-2025	10:10	12:10	02:00
5 z 14 Przerwa	PIOTR DYNIAKOWSKI	06-10-2025	12:10	12:15	00:05
6 z 14 Blok 3: Techniki promptowania + warsztaty	PIOTR DYNIAKOWSKI	06-10-2025	12:15	13:00	00:45
7 z 14 Przerwa	PIOTR DYNIAKOWSKI	06-10-2025	13:00	13:20	00:20
8 z 14 Blok 3: Techniki promptowania + warsztaty - ciąg dalszy	PIOTR DYNIAKOWSKI	06-10-2025	13:20	15:05	01:45
9 z 14 Blok 4: Copilot + Debug + VSCode	PIOTR DYNIAKOWSKI	07-10-2025	08:30	10:30	02:00
10 z 14 Przerwa	PIOTR DYNIAKOWSKI	07-10-2025	10:30	10:40	00:10
11 z 14 Blok 5: Projekty + warsztaty. Test-Gen	PIOTR DYNIAKOWSKI	07-10-2025	10:40	12:40	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 14 Przerwa	PIOTR DYNIAKOWSKI	07-10-2025	12:40	13:00	00:20
13 z 14 Blok 6: Bezpieczeństwo + Etyka+Trendy	PIOTR DYNIAKOWSKI	07-10-2025	13:00	14:40	01:40
14 z 14 Pytania i odpowiedzi, podsumowanie szkolenia, post-test.	-	07-10-2025	14:40	15:00	00:20

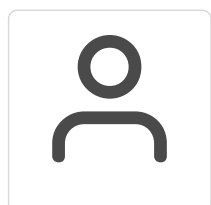
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 000,00 PLN
Koszt przypadający na 1 uczestnika netto	4 000,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	250,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

PIOTR DYNIAKOWSKI

Doświadczony specjalista z ponad 25-letnią praktyką w branży IT, automatyki oraz zarządzania projektami technologicznymi. Posiada szeroką wiedzę w zakresie bezpieczeństwa sieciowego, wdrażania rozwiązań IT i zarządzania infrastrukturą. Zrealizował szereg projektów z zakresu budowy sieci komputerowych, zarządzania systemami oraz świadczenia usług IT dla firm i instytucji publicznych. Charakteryzuje się umiejętnościami w sprzedaży B2B, negocjacjach z klientami oraz w organizowaniu szkoleń technicznych. Lektor /Wykładowca Uniwersytetu Warszawskiego , UJ Kraków, Politechniki Łódzkiej oraz prowadzenie szkoleń w ramach kursu z cyberbezpieczeństwa do certyfikatu OSCP, doradztwo informatyczne.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacja powerpoint, celem utrwalenia informacji przekazanych w trakcie szkolenia, przesłana będzie drogą mailową.

Warunki uczestnictwa

Warunkiem uczestnictwa jest zarejestrowanie się i założenie konta w Bazie Usług Rozwojowych oraz zapisanie się na szkolenie za pośrednictwem Bazy.

Informacje dodatkowe

Po zakończeniu usługi uczestnik otrzyma certyfikat. Usługa szkoleniowa podzielona jest na godziny dydaktyczne (1 godzina dydaktyczna = 45 minut).

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Adres

ul. 1 Maja 191/parter
25-646 Kielce
woj. świętokrzyskie

Miejsce realizacji usługi sala wykładowa mieszcząca się w biurowcu przy
ul. 1-go Maja 191, 25-646 Kielce "BUSINESS HORIZON OFFICE"

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Udogodnienia dla osób ze szczególnymi potrzebami

Kontakt



Elżbieta Ludwikowska

E-mail e.ludwikowska.mija@gmail.com

Telefon (+48) 609 718 185