



AI w Cyberbezpieczeństwie

Numer usługi 2026/03/16/7733/3410612

1 722,00 PLN brutto

1 400,00 PLN netto

215,25 PLN brutto/h

175,00 PLN netto/h

183,33 PLN cena rynkowa ⓘ

Comarch SA

★★★★★ 4,5 / 5

1 063 oceny

📍 Kraków

🏢 Usługa szkoleniowa

📄 stacjonarna

🕒 08:00 h

📅 07.12.2026 do 07.12.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Aplikacje biznesowe

Identyfikatory projektów

Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe, Kierunek - Rozwój, Regionalny Fundusz Szkoleniowy II

Grupa docelowa usługi

Szkolenie skierowane jest do:

- Specjalistów ds. bezpieczeństwa IT.
- Analityków danych i programistów.
- Menedżerów IT i kierowników projektów.
- Osób odpowiedzialnych za zarządzanie ryzykiem w organizacjach.
- Wszystkich zainteresowanych tematyką AI i cyberbezpieczeństwa.

Przygotowanie uczestników

- Podstawowa wiedza z zakresu IT i bezpieczeństwa informatycznego.
- Znajomość podstawowych pojęć związanych z sztuczną inteligencją będzie dodatkowym atutem.

Czas trwania kursu wynosi 8 godzin lekcyjnych, godzina lekcyjna to 45 minut.

Usługa jest dedykowana dla uczestników projektu Małopolski pociąg do kariery.

Usługa również adresowana dla uczestników projektu Małopolskie Bony rozwojowe Plus" i "Małopolski Pociąg do Kariery"

"Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój"

Minimalna liczba uczestników

4

Maksymalna liczba uczestników

12

Data zakończenia rekrutacji	01-12-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Szkolenie to ma na celu nie tylko przekazanie wiedzy teoretycznej, ale także praktyczne przygotowanie uczestników do wyzwań, jakie niesie ze sobą dynamicznie rozwijająca się dziedzina cyberbezpieczeństwa w kontekście sztucznej inteligencji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe pojęcia związane z cyberbezpieczeństwem i sztuczną inteligencją.	definiuje kluczowe pojęcia z zakresu cyberbezpieczeństwa i AI, rozdziela podstawowe typy zagrożeń cybernetycznych, opisuje rolę sztucznej inteligencji w systemach bezpieczeństwa informatycznego.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i analizuje zagrożenia związane z wykorzystaniem AI w kontekście cyberbezpieczeństwa.	wskazuje przykłady zagrożeń wynikających z wykorzystania AI, analizuje scenariusze ataków wykorzystujących technologie AI, ocenia wpływ zagrożeń na bezpieczeństwo systemów informatycznych.	Test teoretyczny z wynikiem generowanym automatycznie
Wykorzystuje narzędzia oparte na AI do identyfikacji i neutralizacji zagrożeń cybernetycznych.	dobiera narzędzia AI wspierające wykrywanie zagrożeń, analizuje dane w celu identyfikacji potencjalnych incydentów bezpieczeństwa, proponuje działania ograniczające skutki wykrytych zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>Oceni ryzyko cyberbezpieczeństwa oraz proponuje zabezpieczenia na podstawie analizy danych.</p>	<p>identyfikuje potencjalne źródła ryzyka w systemie informatycznym,</p> <p>analizuje dane dotyczące incydentów bezpieczeństwa,</p> <p>proponuje środki zabezpieczające adekwatne do zidentyfikowanego ryzyka.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>
<p>Rozpoznaje techniki ataków socjotechnicznych oraz stosuje działania zapobiegawcze.</p>	<p>identyfikuje przykłady ataków socjotechnicznych (np. phishing),</p> <p>analizuje scenariusze wykorzystania socjotechniki w cyberatakach,</p> <p>wskazuje działania ograniczające skuteczność takich ataków.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>
<p>Stosuje zasady cyberhigieny w pracy z systemami informatycznymi i narzędziami AI.</p>	<p>opisuje zasady bezpiecznego korzystania z systemów informatycznych,</p> <p>stosuje dobre praktyki w zakresie ochrony danych i dostępu do systemów,</p> <p>ocenia poprawność stosowanych procedur bezpieczeństwa.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>

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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Usługa jest realizowana w godzinach lekcyjnych, tj. za godzinę usługi szkoleniowej rozumie się 45 minut, łącznie 8 godzin lekcyjnych.

Planowane przerwy w trakcie zajęć: 10:30-10:45, 13:00-13:30, 14:45-15:00. Przerwy nie są wliczone w godziny zajęć usługi. Liczba godzin zajęć praktycznych: 4 godziny lekcyjne, liczba godzin zajęć teoretycznych: 4 godziny lekcyjne, w tym test 10 min.

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

2. Grupa docelowa: Szkolenie skierowane jest do: Specjalistów ds. bezpieczeństwa IT, Analityków danych i programistów, Menedżerów IT i kierowników projektów, Osób odpowiedzialnych za zarządzanie ryzykiem w organizacjach, Wszystkich zainteresowanych tematyką AI i cyberbezpieczeństwa.

Przygotowanie uczestników: Podstawowa wiedza z zakresu IT i bezpieczeństwa informatycznego, Znajomość podstawowych pojęć związanych z sztuczną inteligencją będzie dodatkowym atutem.

Wprowadzenie do cyberbezpieczeństwa i sztucznej inteligencji

- Definicja cyberbezpieczeństwa: Zrozumienie podstawowych terminów i koncepcji związanych z ochroną danych, systemów i sieci przed zagrożeniami, w tym atakami hakerskimi i złośliwym oprogramowaniem.
- OWASP Top 10 dla LLM: Przegląd najważniejszych zagrożeń związanych z modelami językowymi, takich jak manipulacja danymi wejściowymi, generowanie dezinformacji oraz ryzyko związane z przechowywaniem danych.
- Zastosowanie sztucznej inteligencji: Jak AI może wspierać cyberbezpieczeństwo, identyfikując i neutralizując zagrożenia w czasie rzeczywistym.
- Zrozumienie ryzyk: Analiza potencjalnych skutków cyberataków na organizację w kontekście rosnącej popularności modeli AI.

Wykorzystanie AI w obronie przed cyberzagrożeniami

- Detekcja anomalii: Jak algorytmy AI mogą analizować ruch sieciowy w poszukiwaniu nietypowych wzorców, które mogą wskazywać na atak.
- Automatyzacja odpowiedzi: Wykorzystanie AI do automatyzacji procesów odpowiedzi na incydenty, co pozwala na szybsze reagowanie na zagrożenia.
- Predykcja zagrożeń: Modele AI mogą przewidywać przyszłe ataki na podstawie analizy danych historycznych, co umożliwia wcześniejsze wprowadzenie środków ochronnych.
- Współpraca z zespołami IT: AI jako narzędzie wspierające zespoły bezpieczeństwa w codziennych zadaniach, takich jak analiza logów czy monitorowanie systemów.

Analiza ryzyk i zabezpieczeń z wykorzystaniem AI

- Identyfikacja ryzyk: Jak AI może wspierać proces identyfikacji i oceny ryzyk związanych z infrastrukturą IT.
- Ocena efektywności zabezpieczeń: Wykorzystanie technik AI do oceny, jak skuteczne są obecne zabezpieczenia w organizacji i gdzie można je poprawić.
- Modelowanie scenariuszy ataków: AI może symulować różne scenariusze ataków, co pozwala na lepsze przygotowanie się na potencjalne zagrożenia.
- Dostosowywanie zabezpieczeń: Zastosowanie uczenia maszynowego do ciągłego dostosowywania zabezpieczeń w odpowiedzi na zmieniające się zagrożenia.

Rola AI w zapobieganiu atakom socjotechnicznym

- Wykrywanie phishingu: Jak AI może analizować wiadomości e-mail i inne formy komunikacji, aby identyfikować potencjalnie złośliwe treści.
- Edukacja użytkowników: Użycie AI do tworzenia spersonalizowanych programów szkoleniowych, które zwiększają świadomość pracowników na temat technik socjotechnicznych.
- Analiza zachowań użytkowników: AI może monitorować zachowania pracowników, aby szybko identyfikować nietypowe aktywności, które mogą sugerować próby oszustwa.
- Tworzenie polityk bezpieczeństwa: Wspieranie organizacji w opracowywaniu polityk mających na celu przeciwdziałanie atakom socjotechnicznym przy użyciu analizy danych.

AI w rękach atakujących – Jak się chronić?

- Zrozumienie narzędzi atakujących: Przegląd technik i narzędzi AI, które mogą być wykorzystywane przez cyberprzestępców, takich jak generowanie fałszywych treści.

- Edukacja i świadomość: Szkolenie pracowników w zakresie zagrożeń związanych z użyciem AI przez atakujących oraz wskazówki, jak rozpoznać potencjalne ataki.
- Wdrażanie zaawansowanych zabezpieczeń: Wykorzystanie AI do wzmocnienia zabezpieczeń, np. poprzez analizę ryzyk w czasie rzeczywistym i wprowadzanie dynamicznych środków ochronnych.
- Monitorowanie i analiza: Utworzenie systemów monitorujących, które wykorzystują AI do identyfikacji podejrzanych działań i potencjalnych naruszeń bezpieczeństwa.

Przyszłość cyberbezpieczeństwa z AI

- Ewolucja zagrożeń: Jak rozwój AI może prowadzić do powstawania nowych form cyberzagrożeń oraz jak organizacje powinny się na nie przygotować.
- Kooperacja AI i ludzi: Zrozumienie, jak AI może wspierać ludzkich specjalistów w dziedzinie bezpieczeństwa, a nie ich zastępować.
- Regulacje i etyka: Wyzwania związane z regulacją użycia AI w cyberbezpieczeństwie oraz kwestie etyczne z tym związane.
- Innowacyjne technologie: Zastosowanie nowych technologii, takich jak blockchain czy kwantowe szyfrowanie w połączeniu z AI, w celu wzmocnienia bezpieczeństwa.

Cyber higiena, a AI

- Podstawy cyber higieny: Definicja i znaczenie cyber higieny w kontekście ochrony danych i systemów.
- Zastosowanie AI w monitorowaniu: Jak narzędzia AI mogą wspierać organizacje w utrzymaniu odpowiednich standardów cyber higieny poprzez automatyczne skanowanie i analizę systemów.
- Personalizacja praktyk bezpieczeństwa: Użycie AI do dostosowywania praktyk cyber higieny do specyficznych potrzeb i ryzyk danej organizacji.
- Wzmacnianie kultury bezpieczeństwa: Jak AI może pomóc w tworzeniu kultury bezpieczeństwa w organizacjach, w tym poprzez analizę danych dotyczących zachowań użytkowników i identyfikację obszarów do poprawy.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 722,00 PLN
Koszt przypadający na 1 uczestnika netto	1 400,00 PLN
Koszt osobogodziny brutto	215,25 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Marek Jeleśniański

Ekspert i trener i doradca z zakresu AI, wykształcenie wyższe, od 20 lat związany z branżą IT, wspiera zarówno międzynarodowe korporacje, jak i małe firmy. W swojej karierze pełnił różne role – od programisty po dyrektora. Jako pasjonat sztucznej inteligencji i jej wpływu na przyszłość rynku pracy, dzieli się swoją wiedzą i przewidywaniami na blogu: <https://jelesnianski.pl/>.

Autor programów szkoleniowych i publikacji. Bardzo dobrze oceniany przez uczestników swoich szkoleń.

Doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują podręcznik w wersji elektronicznej.

W czasie zajęć wykorzystywane są autorskie materiały dydaktyczne przygotowane przez wykładowcę oraz inne materiały dydaktyczne przygotowane przez organizatora szkolenia.

Warunki uczestnictwa

Warunkiem skorzystania ze szkolenia jest dokonanie równoległe rejestracji na kurs na stronie www.comarch.pl/szkolenia w formie:

- elektronicznego zamówienia szkolenia (przycisk "Zamów" przy wybranym temacie i terminie). Opcja ta dotyczy osób fizycznych oraz firm/institucji

albo

- poprzez uzupełnienie i odesłanie na adres szkolenia@comarch.pl tradycyjnego formularza zgłoszeniowego który jest dostępny na stronie www.comarch.pl/szkolenia (przycisk "Pobierz formularz zgłoszeniowy"). Opcja ta dotyczy wyłącznie firm/Instytucji.

W obu przypadkach przy dokonaniu zgłoszenia prosimy o informacje dotyczącą projektu z którego dofinansowania korzysta Uczestnik.

Planowana przerwa: –obiadowa 30 min plus 2 kawowe po 15 minut.

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

Informacje dodatkowe

Szkolenie zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być zwolnione z VAT-u w zależności od rodzaju dofinansowania

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Małopolski Pociąg do Kariery” i "Małopolskie Bony Rozwojowe Plus"

Szkolenie może być nagrywane /rejestrowane w celu kontroli/audytu zgodnie z Regulaminem Świadczenia Usług Szkoleniowych Organizatora.

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój.

Adres

ul. prof. Michała Życzkowskiego 33/SSE VII

31-864 Kraków

woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt



Aneta Lewkowska

E-mail aneta.lewkowska@comarch.pl

Telefon (+48) 126 877 811