



PROGRESSION
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ



Bezpieczeństwo w sieci w erze AI i cyberprzestępczości - Kierunek - Rozwój

Numer usługi 2025/02/21/160858/2573753

📍 zdalna w czasie rzeczywistym

📅 Usługa szkoleniowa

🕒 8 h

📅 10.05.2025 do 10.05.2025

740,00 PLN brutto

740,00 PLN netto

92,50 PLN brutto/h

92,50 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane jest do osób, które chcą zdobyć praktyczne umiejętności i poszerzyć swoją wiedzę w zakresie bezpieczeństwa w sieci, aby chronić swoje dane i prywatność oraz być na bieżąco z najnowszymi trendami w cyberbezpieczeństwie. Usługa adresowana również do uczestników projektu Kierunek - Rozwój.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	18
Data zakończenia rekrutacji	09-05-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
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

Uczestnik szkolenia "Bezpieczeństwo w sieci w erze AI i cyberprzestępczości" rozumie pojęcie cyberprzestępczości i posiada praktyczne umiejętności niezbędne do ochrony swoich danych oraz prywatności w środowisku cyfrowym, szczególnie w obliczu nowych wyzwań związanych z rozwojem sztucznej inteligencji i rosnącym zagrożeniem cyberprzestępczością.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisuje podstawowe zagrożenia, które można spotkać w sieci.	Uczestnik wskazuje rodzaje cyberzagrożeń.	Test teoretyczny
	Uczestnik wskazuje możliwe konsekwencje wybranych cyberzagrożeń.	Test teoretyczny
Potrafi tworzyć silne hasła oraz skutecznie nimi zarządzać.	Uczestnik wskazuje cechy silnego hasła.	Test teoretyczny
	Uczestnik wybiera poprawne zasady bezpiecznego zarządzania hasłami.	Test teoretyczny
Opisuje sposoby, w jakie sztuczna inteligencja jest wykorzystywana do zapewnienia bezpieczeństwa w Internecie.	Uczestnik wymienia przykłady narzędzi sztucznej inteligencji pomagające zachować bezpieczeństwo w sieci.	Test teoretyczny
	Uczestnik wskazuje sposób działania wybranego narzędzia AI w kontekście bezpieczeństwa.	Test teoretyczny
Opisuje, czym są dane osobowe, jak je chronić i jakie prawa przysługują w zakresie prywatności. Identyfikuje podejrzane aktywności w sieci i stosuje odpowiednie środki ostrożności.	Uczestnik wybiera poprawne sposoby ochrony danych osobowych.	Test teoretyczny
	Uczestnik wskazuje podstawę prawną i jakie prawa mu przysługują w zakresie prywatności.	Test teoretyczny
	Uczestnik rozpoznaje cechy podejrzanych aktywności w sieci.	Test teoretyczny
	Uczestnik wskazuje odpowiednie działania w przypadku zagrożenia cybernetycznego.	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

Szkolenie odbywa się w godzinach dydaktycznych. Przerwy nie są wliczane w czas trwania usługi.

FORMA REALIZACJI ZAJĘĆ:

Forma realizacji zajęć w ramach szkolenia będzie obejmowała różnorodne metody dydaktyczne, które zapewnią uczestnikom wszechstronne zrozumienie omawianych tematów oraz umożliwią praktyczne zastosowanie zdobytej wiedzy i umiejętności.

Szczegóły formy realizacji są następujące:

- **Wykłady interaktywne**:** Każdy moduł będzie rozpoczynał się interaktywnym wykładem, podczas którego trener wprowadzą teoretyczne podstawy tematu, używając prezentacji multimedialnych, studiów przypadków i przykładów z praktyki. Wykłady będą angażować uczestników poprzez pytania retoryczne, mini-dyskusje.
- **Sesje pytań i odpowiedzi**:** Po każdym wykładzie zaplanowane będą sesje pytań i odpowiedzi, w trakcie których uczestnicy będą mieli możliwość zadawania pytań dotyczących prezentowanych treści. Trener będzie odpowiadać na pytania, wyjaśniać wątpliwości i omawiać dodatkowe aspekty tematów.
- **Ćwiczenia grupowe i indywidualne**:** W trakcie zajęć uczestnicy będą brać udział w ćwiczeniach zarówno grupowych, jak i indywidualnych. Zadania te pozwolą na praktyczne zastosowanie wiedzy poprzez analizę przypadków, opracowywanie strategii i rozwiązywanie problemów. Uczestnicy będą mieli możliwość wymiany doświadczeń w grupach oraz refleksji nad zdobytą wiedzą podczas pracy indywidualnej.
- **Wspólne dyskusje**:** Przewidziane są regularne wspólne dyskusje, gdzie uczestnicy będą mieli okazję dzielić się swoimi spostrzeżeniami i refleksjami na temat omawianych zagadnień. Dyskusje te będą moderowane przez trenerów, co zapewni ich efektywność i merytoryczność.
- **Test końcowy**:** Na zakończenie szkolenia, uczestnicy przystąpią do testu teoretycznego, który będzie miał formę testu z pytaniami zamkniętymi i otwartymi. Egzamin ten posłuży do oceny przyswojonej wiedzy i umiejętności, a także weryfikacji osiągniętych efektów kształcenia.

Te różnorodne metody dydaktyczne zapewnią aktywny udział uczestników w szkoleniu, umożliwią wymianę doświadczeń oraz zwiększą efektywność nauki poprzez praktyczne zastosowanie zdobytej wiedzy.

Program

Moduł 1: Wprowadzenie do cyberbezpieczeństwa

- Czym jest cyberbezpieczeństwo i dlaczego jest ważne?
- Typowe zagrożenia w sieci (np. phishing, wirusy, wyłudzenia).
- Przykłady ataków cybernetycznych i ich skutki.

Moduł 2: Bezpieczne korzystanie z internetu

- Tworzenie silnych haseł i zarządzanie nimi.
- Jak bezpiecznie korzystać z poczty elektronicznej i rozpoznawać próby wyłudzenia (phishing)?
- Korzystanie z dwuetapowej weryfikacji.

Moduł 3: Rola sztucznej inteligencji w cyberbezpieczeństwie

- Jak AI wykrywa zagrożenia w sieci?
- Automatyczne systemy ochrony: jak sztuczna inteligencja analizuje zachowania użytkowników i identyfikuje anomalie?
- Przykłady zastosowań AI w ochronie danych.

Moduł 4: Ochrona prywatności w sieci

- Co to są dane osobowe i jak je chronić?
- Polityka prywatności i jak zrozumieć, jakie dane są zbierane przez strony internetowe?
- Jak minimalizować ilość udostępnianych danych?

Moduł 5: Cyberbezpieczeństwo w praktyce - jak unikać zagrożeń

- Praktyczne ćwiczenia w rozpoznawaniu zagrożeń online.
- Jak postępować w przypadku podejrzenia ataku? (np. zainfekowanie komputera, podejrzana wiadomość).
- Podstawowe zasady bezpiecznego korzystania z sieci społecznościowych.

Walidacja

Test teoretyczny przeprowadzany zdalnie w czasie rzeczywistym.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	740,00 PLN
Koszt przypadający na 1 uczestnika netto	740,00 PLN
Koszt osobogodziny brutto	92,50 PLN
Koszt osobogodziny netto	92,50 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Kacper Rzosiński

Doświadczenie:

Do 2024 przeprowadził łącznie 600 godzin warsztatów w obszarze mapowania procesów i wyznaczaniu kierunków działań, takich jak Event Storming czy Discovery Workshop, jako elementy audytu w Domain-Driven Design. Przeprowadził liczne warsztaty dotyczące budowania strategii marki, wykorzystując metody takie jak Brand Sprint i Design Sprint.

W ciągu ostatnich 5 lat wprowadzał kompleksowe procesy optymalizacji dla platform SaaS i sklepów e-commerce, skupiając się na aspektach User Experience, Customer Development oraz Customer Support.

Kwalifikacje

W 2016 roku ukończył Wyższą Szkołę Informatyki Stosowanej i Zarządzania WIT w Warszawie, zdobywając tytuł magistra na kierunku Projektowanie graficzne.

W 2021 roku ukończył studia podyplomowe UX Design/Product Design na Uniwersytecie SWPS. W latach 2021-2023, współpracując z najpopularniejszą platformą e-commerce w Polsce, ukończył liczne szkolenia wewnętrzne w zakresie: projektowania procesów, zarządzania zespołem projektowym, ekonomii behawioralnej. W ostatnich 5 latach ukończył liczne kursy UX/UI, blockchain, robotics for innovation, AI.

W 2024 r. zrealizował 53 godziny dydaktyczne szkolenia „Lider Transformacji cyfrowej” dla osób indywidualnych oraz szkolenia dla firm z zakresu Transformacji cyfrowej. Jest czynnym konsultantem wdrożeniowym nowych technologii w firmie Progression sp. z o.o.

Doświadczenie zawodowe i kwalifikacje nabyte nie wcześniej niż 5 lat.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzyma od organizatora materiały szkoleniowe - dydaktyczne w formie elektronicznej.

Warunki uczestnictwa

Wzięcie udziału w usłudze wymaga podpisania umowy dotyczącej świadczenia usług rozwojowych z usługodawcą firmą Progression sp. z o.o.

Informacje dodatkowe

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

Zwolnienie ze względu na rodzaj prowadzonej działalności (art. 43 ust 1 ustawy o VAT).

Warunki techniczne

- **Sprzęt komputerowy:**
 - Wymagany komputer PC lub Mac z dostępem do internetu.
 - Zalecana kamera internetowa oraz mikrofon dla udziału w sesjach wideo.

- **Przeglądarka internetowa:**
- Zalecane przeglądarki: Google Chrome, Mozilla Firefox, Safari.
- Wymagane zaktualizowane wersje przeglądarek dla optymalnej wydajności.
- **Stabilne połączenie internetowe:**
- Minimalna prędkość łącza: 2 Mbps dla udziału w sesjach wideo.
- Zalecane połączenie kablowe dla stabilności.
- **Platforma MS Teams:**
- Konieczne pobranie i zainstalowanie najnowszej wersji aplikacji MS Teams przed szkoleniem.
- Aktywne konto MS Teams (możliwość utworzenia bezpłatnego konta).
- **System operacyjny:**
- Kompatybilność z systemem Windows lub macOS.
- **Oprogramowanie dodatkowe:**
- Zalecane zainstalowanie najnowszych wersji programów, takich jak przeglądarka, Java, Flash itp.
- **Dźwięk i słuchawki:**
- Zalecane użycie słuchawek z mikrofonem dla lepszej jakości dźwięku.
- Sprawdzenie działania dźwięku przed rozpoczęciem szkolenia.

Kontakt



Patrycja Gumkowska

E-mail gumkowska@progression.pl

Telefon (+48) 798 959 667