



Digital Marketing
Krzysztof Szymak

★★★★★ 4,9 / 5

612 ocen

Cyberbezpieczeństwo w zrównoważonej transformacji cyfrowej. Kwalifikacje. Szkolenie.

Numer usługi 2026/07/24/163842/3707639

📍 Katowice

🏢 Usługa szkoleniowa

📅 stacjonarna

👥 Zajęcia grupowe

🕒 16:00 h

📅 03.10.2026 do 09.10.2026

6 081,12 PLN brutto

4 944,00 PLN netto

380,07 PLN brutto/h

309,00 PLN netto/h

233,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Internet

Grupa docelowa usługi

Szkolenie skierowane jest do osób, które planują z **własnej inicjatywy** podnieść swoje umiejętności w zakresie kwalifikacji cyfrowych, w obszarze cyberbezpieczeństwa. Prowadzi do zdobycia kwalifikacji międzynarodowej **GCCS/ICVC Specjalista ds. cyberbezpieczeństwa (ICVC/CBB 207771.19)**.

Usługa szkoleniowa dedykowana jest także dla osób chcących podnieść swoje zielone kompetencje w zakresie bezpiecznego i zrównoważonego wykorzystywania technologii cyfrowych - od ograniczania śladu węglowego infrastruktury IT i zarządzania danymi, po odpowiedzialne, etyczne podejście do ochrony informacji i prywatności.

Usługa skierowana m.in. do:

- właścicieli i pracowników MŚP,
- osób pracujących z danymi (administracja, marketing, sprzedaż, HR),
- osób odpowiedzialnych za bezpieczeństwo informacji w organizacji,
- osób pracujących zdalnie lub hybrydowo
- wszystkich, którzy chcą zwiększyć swoje bezpieczeństwo cyfrowe i jednocześnie działać zgodnie z zasadami zrównoważonego rozwoju.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji

02-10-2026

Forma prowadzenia usługi

stacjonarna

Cel

Cel edukacyjny

Usługa szkoleniowa przygotowuje do identyfikowania phishingu i innych zagrożeń, zabezpieczania kont, haseł, sieci Wi-Fi i urządzeń, tworzenia kopii zapasowych, szyfrowania danych oraz reagowania na incydenty. Usługa rozwija umiejętności w obszarze technologii informacyjno-komunikacyjnych (ICT) i zielone kompetencje związane z bezpiecznym, energooszczędnym zarządzaniem danymi, sprzętem i zasobami cyfrowymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisuje rodzaje zagrożeń cyberbezpieczeństwa i etapy współczesnego ataku.	Charakteryzuje podstawowe rodzaje zagrożeń, w tym phishing, smishing, vishing, ransomware, malware, deepfake oraz wycieki danych.	Test teoretyczny
	Opisuje etapy łańcucha ataku: rekonesans, uzyskanie dostępu, eskalację uprawnień oraz exfiltrację danych.	Test teoretyczny
	Wyjaśnia konsekwencje biznesowe i organizacyjne cyberataków dla sektora MŚP.	Test teoretyczny
Wyjaśnia zasady energooszczędnego projektowania infrastruktury bezpieczeństwa IT i jej wpływ na środowisko. Wyjaśnia znaczenie green IT i cyfrowego minimalizmu w cyberbezpieczeństwie.	Charakteryzuje wpływ serwerów i urządzeń sieciowych na zużycie energii i emisję CO2.	Test teoretyczny
	Opisuje technologie optymalizacji energetycznej w systemach bezpieczeństwa.	Test teoretyczny
	Opisuje wpływ infrastruktury IT, nadmiaru danych i incydentów bezpieczeństwa na zużycie energii oraz zasobów cyfrowych.	Test teoretyczny
	Charakteryzuje znaczenie ograniczania duplikacji plików, archiwizacji i redukcji zbędnych danych.	Test teoretyczny
	Wyjaśnia związek między cyklem życia sprzętu IT, e-odpadami, recyklingiem i bezpiecznym usuwaniem danych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje mechanizmy socjotechniczne wykorzystywane w atakach cyfrowych.	Wyjaśnia znaczenie presji czasu, autorytetu, strachu i emocji w działaniach cyberprzestępców.	Test teoretyczny
	Rozróżnia phishing, smishing i vishing na podstawie sposobu działania oraz kanału komunikacji.	Test teoretyczny
	Wskazuje cechy wiadomości, linków i połączeń telefonicznych mogące świadczyć o próbie oszustwa.	Test teoretyczny
	Wyjaśnia zastosowanie szyfrowania danych na urządzeniach końcowych, w tym BitLocker i FileVault.	Test teoretyczny
Charakteryzuje zasady ochrony danych, wykonywania kopii zapasowych i szyfrowania informacji.	Opisuje zasadę kopii zapasowych 3-2-1 oraz jej znaczenie w ochronie przed utratą danych i ransomware.	Test teoretyczny
	Porównuje przechowywanie danych lokalnie i w chmurze pod kątem bezpieczeństwa, dostępności i zarządzania zasobami.	Test teoretyczny
Stosuje zasady efektywnego i bezpiecznego zarządzania tożsamością cyfrową i dostępem do danych.	Tworzy bezpieczne frazy hasłowe zgodnie z dobrymi praktykami.	Analiza dowodów i deklaracji
	Weryfikuje, czy dane logowania zostały ujawnione w znanych wyciekach danych.	Analiza dowodów i deklaracji
	Konfiguruje sposób wdrożenia uwierzytelniania wieloskładnikowego.	Analiza dowodów i deklaracji
	Dobiera działania zwiększające bezpieczeństwo dostępu do kont i danych.	Analiza dowodów i deklaracji
Opracowuje procedurę reagowania na incydent cyberbezpieczeństwa.	Korzysta z menadżera haseł w celu ich bezpiecznego przechowywania.	Analiza dowodów i deklaracji
	Tworzy procedurę reagowania na incydent obejmującą identyfikację zagrożenia, zabezpieczenie zasobów, zgłoszenie incydentu, dokumentację oraz działania naprawcze.	Analiza dowodów i deklaracji
	Opracowuje procedury archiwizacji danych zgodnie z wymogami prawnymi i efektywnością zasobów.	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zarządza cyklem życia oprogramowania wspierając open-source i długoterminowe wsparcie.	Planuje strategię aktualizacji oprogramowania, minimalizującą niepotrzebne zmiany sprzętu.	Analiza dowodów i deklaracji
	Dokumentuje proces oceny oprogramowania open-source w kontekście bezpieczeństwa i ekologii.	Analiza dowodów i deklaracji
Wyjaśnia zasady etyki zawodowej i odpowiedzialności zasobowej w komunikacji z zespołem IT.	Identyfikuje świadome podejście do zasobów poprzez wspieranie inicjatyw zielonego cyberbezpieczeństwa.	Test teoretyczny
	Opisuje rolę odpowiedzialnej komunikacji w przeciwdziałaniu panice, dezinformacji i błędnym decyzjom użytkowników.	Test teoretyczny
	Wskazuje znaczenie współpracy pracowników, kadry zarządzającej i osób odpowiedzialnych za IT w ograniczaniu ryzyka cyberataków.	Test teoretyczny
	Opisuje znaczenie zgłaszania podejrzanych zdarzeń oraz dzielenia się informacjami o zagrożeniach.	Test teoretyczny
Charakteryzuje zasady współpracy zespołowej przy wdrażaniu procedur cyberbezpieczeństwa.	Wyjaśnia rolę stałego doskonalenia kompetencji cyfrowych w dynamicznie zmieniającym się środowisku cyberzagrożeń.	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

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

TAK

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

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

Informacje

Nazwa Podmiotu prowadzącego walidację

ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Program

Usługa prowadzi do nabycia kwalifikacji: międzynarodowej **GCCS/ICVC Specjalista ds. cyberbezpieczeństwa (ICVC/CBB 207771.19)**. W ramach szkolenia zapewniono **walidację efektów uczenia się**, mającą na celu ocenę poziomu osiągnięcia efektów kształcenia.

Szkolenie stanowi odpowiedź na cele i kierunki rozwoju wskazane w **Regionalnej Strategii Innowacji Województwa Śląskiego 2030 (RIS WSL 2030)**, w szczególności w obszarach inteligentnych specjalizacji:

- **OBZAR TECHNOLOGICZNY - TECHNOLOGIE INFORMACYJNE I TELEKOMUNIKACYJNE: 4.2. Technologie informacyjne**

Zakres szkolenia wpisuje się w Priorytetowe Technologie Rozwójowe (**PRT**) wskazane w **Regionalnej Strategii Innowacji Województwa Śląskiego 2030** oraz **Programie Rozwoju Technologii Województwa Śląskiego 2019-2030**, w szczególności w obszarach:

1. Technologie informacyjno-komunikacyjne (ICT),
2. Technologie cyfrowe wspierające transformację przedsiębiorstw,
3. Technologie związane ze zrównoważonym rozwojem i zieloną transformacją,
4. Technologie multimedialne i kreatywne,
5. Sztuczna inteligencja i analiza danych.

Przykładowe perspektywy zawodowe:

- specjalista ds. cyberbezpieczeństwa w MŚP,
- koordynator bezpieczeństwa informacji,
- specjalista ds. ochrony danych i RODO,
- specjalista ds. green IT,
- konsultant ds. bezpieczeństwa cyfrowego.

Szkolenie będzie miało formę głównie warsztatową. Każdy uczestnik będzie pracował przy komputerze. **Forma warsztatowa zapewni realizację celu edukacyjnego usługi.**

Usługa realizowana jest w godzinach zegarowych, tj. 1 godzina lekcyjna = 60 minut.

Uwaga do harmonogramu: przerwy na lunch są wliczone w czas trwania usługi i zostały ustalone na godzinę 12:00-13:00 - uwzględniono w harmonogramie.

!!! WAŻNE: Szkolenie realizowane jest w terminie 03-04.10.2026 r. Po zakończeniu szkolenia uczestnicy przystępują do egzaminu certyfikującego, który jest organizowany i oceniany przez międzynarodowy podmiot zewnętrzny. Czas oczekiwania na wynik walidacji wynosi średnio ok. 5 dni roboczych od dnia przeprowadzenia egzaminu. W związku z tym - według Zał. 2 (2.4) do Regulaminu BUR **termin realizacji usługi został określony w karcie na 03-09.10.2026, ponieważ obejmuje:**

- **okres prowadzenia szkolenia (3-4 października)**
- **oraz okres oczekiwania na wynik walidacji (do 9 października).**

PROGRAM:

I DZIEŃ SZKOLENIA [teoria: 1h 45min, praktyka: 5h, przerwa: 60 min, kwestie organizacyjne: 15 min] - 03.10.2026:

08:30 - 08:45 Przywitanie uczestników, omówienie szkolenia, przeprowadzenie pre-testów w celu oceny początkowego poziomu wiedzy uczestników.

08:45 - 10:15 MODUŁ I: Anatomia współczesnego ataku i jego wpływ na zasoby organizacji.

1. Dlaczego sektor MŚP jest celem numer jeden - aktualne statystyki i konsekwencje biznesowe.
2. Łańcuch ataku (rekonesans → dostęp → eskalacja → exfiltracja danych).
3. Rodzaje zagrożeń: phishing, ransomware, malware, ataki socjotechniczne, wycieki danych.
4. Wartość danych i wpływ incydentów na środowisko (np. utrata danych = konieczność ich odtwarzania = dodatkowe zużycie energii i zasobów IT).
5. Wprowadzenie do metod detekcji zagrożeń (monitoring, analiza logów, systemy SIEM).

10:15 - 12:00 MODUŁ II: Psychologia oszustwa i zagrożenia komunikacyjne (Phishing, Smishing, Vishing).

1. Mechanizmy manipulacji: presja czasu, autorytet, strach, emocje.
2. Analiza rzeczywistych przypadków phishingu - identyfikacja zagrożeń w praktyce.
3. Scenariusze ataków telefonicznych i SMS.
4. Warsztat: rozpoznawanie zagrożeń i podejmowanie decyzji.
5. Jak ograniczenie liczby incydentów wpływa na zmniejszenie strat zasobów i energii w organizacji.

12:00 - 13:00 Przerwa.

13:00 - 14:30 MODUŁ III: Zarządzanie tożsamością i bezpieczeństwo dostępu (warsztat).

1. Hasła: frazy zamiast schematów - jak zwiększyć bezpieczeństwo i ograniczyć potrzebę resetów (redukcja obciążenia systemów).
2. Menedżery haseł (Bitwarden, 1Password) - konfiguracja i praktyczne użycie.
3. Weryfikacja wycieków danych (Have I Been Pwned).
4. Wpływ bezpiecznego zarządzania dostępem na ograniczenie incydentów i zużycia zasobów IT.

14:30 - 16:30 MODUŁ IV: AI w cyberbezpieczeństwie i efektywność energetyczna systemów.

1. Deepfake i klonowanie głosu - rozpoznawanie zagrożeń.
2. AI w atakach (automatyzacja phishingu).
3. AI w ochronie - jak nowoczesne programy antywirusowe wykorzystują uczenie maszynowe do wykrywania nieznanych wcześniej wirusów.
4. Wpływ systemów AI na zużycie energii - jak wybierać rozwiązania efektywne energetycznie.
5. Warsztat: analiza przypadków + wykorzystanie narzędzi AI w cyberbezpieczeństwie.

**II DZIEŃ SZKOLENIA [teoria: 1h 15 min, praktyka: 4,5h, przerwa: 60 min, kwestie organizacyjne: 30 min, walidacja oraz egzamin: 45 min]
- 04.10.2026:**

08:30 - 08:45 Przywitanie uczestników, krótkie przypomnienie materiału z poprzedniego dnia, sprawdzenie i rozwiązywanie ewentualnych trudności na aktualnym etapie szkolenia.

08:45 - 10:15 MODUŁ V: Bezpieczeństwo sieci i energooszczędna infrastruktura IT.

1. Konfiguracja sieci Wi-Fi - bezpieczeństwo i optymalizacja zużycia energii.
2. Publiczne sieci i zagrożenia.
3. VPN - zastosowanie, wybór dostawcy (rozwiązania przyjazne środowisku i efektywne energetycznie).
4. Monitoring sieci - jak ograniczyć obciążenie infrastruktury.
5. Warsztat: konfiguracja bezpiecznego i odpowiedzialnego środowiska pracy.

10:15 - 12:00 MODUŁ VI: Ochrona danych i zarządzanie sprzętem w duchu gospodarki obiegu zamkniętego.

1. Szyfrowanie danych (BitLocker, FileVault).
2. Backup (zasada 3-2-1) - efektywne zarządzanie kopiami. Ograniczanie duplikacji plików i archiwizacja jako element redukcji zużycia energii i zasobów cyfrowych.
3. Chmura kontra dysk - porównanie bezpieczeństwa dokumentów trzymanyh lokalnie i w profesjonalnej chmurze.
4. Cykl życia sprzętu IT - kiedy modernizować, a kiedy wymieniać urządzenia w kontekście ograniczania e-odpadów.
5. Wydłużanie życia sprzętu - dobre praktyki użytkowania i konserwacji urządzeń jako element strategii zrównoważonego rozwoju.
6. Recykling sprzętu i bezpieczne usuwanie danych.
7. Warsztat: plan zabezpieczenia danych i sprzętu w organizacji.

12:00 - 13:00 Przerwa.

13:00 - 14:15 MODUŁ VII: Prywatność, komunikacja i bezpieczeństwo w organizacji.

1. Cyfrowy ślad i over-sharing. Jak informacje publikowane w social mediach (LinkedIn, FB) ułatwiają hakerom precyzyjne ataki?
2. Narzędzia ochrony prywatności (przeglądarki, blokery).
3. Bezpieczne komunikatory (Signal, WhatsApp) - efektywna i odpowiedzialna komunikacja cyfrowa w organizacji.
4. Ochrona kont firmowych - minimalizacja ryzyka przejęć i strat danych.
5. Tryb incognito - co naprawdę ukrywa, a czego nie?
6. Warsztat: analiza ryzyk i wdrożenie dobrych praktyk z uwzględnieniem ograniczania nadmiarowych danych i optymalizacji ich przechowywania.
7. Jak komunikować zasady cyberbezpieczeństwa w organizacji - budowanie świadomości pracowników w zakresie bezpieczeństwa i odpowiedzialnego korzystania z zasobów cyfrowych.
8. Wprowadzenie do polityki „data minimalism” - ograniczanie przechowywania danych jako element strategii bezpieczeństwa i zrównoważonego rozwoju.

14:15 - 15:30 MODUŁ VIII: Prawo, procedury i green IT w cyberbezpieczeństwie.

- 1. RODO i obowiązki przedsiębiorcy.
 - 2. Zgłaszanie incydentów (CERT Polska).
 - 3. Standardy i dobre praktyki bezpieczeństwa.
 - 4. Green IT:
 - cyfrowy minimalizm (redukcja danych, maili, plików),
 - wpływ infrastruktury IT na emisję CO2,
 - optymalizacja systemów bezpieczeństwa pod kątem zużycia energii.
1. Warsztat: opracowanie procedury reagowania na incydent.

15:30 - 15:45 Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.

15:45 - 16:30 Walidacja - analiza dowodów i deklaracji oraz test teoretyczny online (egzamin).

*UWAGI DOTYCZĄCE WALIDACJI:

Walidacja (test teoretyczny online oraz analiza dowodów i deklaracji) określona jest w harmonogramie w ostatniej pozycji "Walidacja" w postaci jednego punktora i trwa łącznie 45 minut. Walidacja przeprowadzana jest w formie ZDALNEJ [forma zdalna dotyczy tylko i wyłącznie instytucji walidującej i certyfikującej - uczestnicy wypełniają test i realizują ćwiczenia, będąc na sali szkoleniowej] - i podzielona jest na 2 etapy:

- walidację **części praktycznej**: uczestnicy podczas szkolenia wykonują ćwiczenia, gromadząc tym samym dowody pracy własnej i nabycia efektów uczenia się prowadzących do zdobycia umiejętności, pod koniec szkolenia zostają one przesłane do weryfikacji przez instytucję zewnętrzną (analiza dowodów i deklaracji).
- walidację **części teoretycznej**: uczestnicy pod koniec szkolenia wypełniają elektroniczny test teoretyczny, który zostaje przygotowany i przesłany przez instytucję zewnętrzną, na podstawie efektów uczenia się określonych w karcie usługi (test teoretyczny online).

Warunki organizacyjne dla przeprowadzenia usługi: szkolenie będzie realizowane w formie warsztatowej, z wykorzystaniem **indywidualnych stanowisk komputerowych**. Każdy uczestnik będzie pracował **samodzielnie** przy komputerze, wykonując ćwiczenia z zakresu cyberbezpieczeństwa.

Każdy uczestnik wykonuje ćwiczenia praktyczne **indywidualnie**, przy bieżącym wsparciu trenera. Sala szkoleniowa będzie wyposażona w dostęp do Internetu/Wi-Fi oraz zasilania umożliwiającego pracę na komputerach przez cały czas trwania zajęć.

Wszystkie narzędzia używane podczas szkolenia działają w przeglądarce. Specyfikacja sprzętowa: dowolny laptop z minimum 4 GB RAM, procesorem klasy np. Intel Core i3 (lub nowszym) oraz sprawną kartą Wi-Fi.

Harmonogram

Liczba pozycji harmonogramu: 14

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Przywitanie uczestników, omówienie szkolenia, przeprowadzenie pre-testów w celu oceny początkowego o poziomie wiedzy uczestników.	Zajęcia	Kamil Urbacz	03-10-2026	08:30	08:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 14 MODUŁ I: Anatomia współczesnego ataku i jego wpływ na zasoby organizacji.	Zajęcia	Kamil Urbacz	03-10-2026	08:45	10:15	01:30
3 z 14 MODUŁ II: Psychologia oszustwa i zagrożenia komunikacyjne (Phishing, Smishing, Vishing).	Zajęcia	Kamil Urbacz	03-10-2026	10:15	12:00	01:45
4 z 14 -	Przerwa	-	03-10-2026	12:00	13:00	01:00
5 z 14 MODUŁ III: Zarządzanie tożsamością i bezpieczeństwem dostępu.	Zajęcia	Kamil Urbacz	03-10-2026	13:00	14:30	01:30
6 z 14 MODUŁ IV: AI w cyberbezpieczeństwie i efektywność energetyczna systemów.	Zajęcia	Kamil Urbacz	03-10-2026	14:30	16:30	02:00
7 z 14 Przywitanie uczestników, krótkie przypomnienie materiału z poprzedniego dnia, sprawdzenie i rozwiązanie ewentualnych trudności na aktualnym etapie szkolenia.	Zajęcia	Kamil Urbacz	04-10-2026	08:30	08:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 14 MODUŁ V: Bezpieczeństwo sieci i energooszczędna infrastruktura IT.	Zajęcia	Kamil Urbacz	04-10-2026	08:45	10:15	01:30
9 z 14 MODUŁ VI: Ochrona danych i zarządzanie sprzętem w duchu gospodarki obiegu zamkniętego.	Zajęcia	Kamil Urbacz	04-10-2026	10:15	12:00	01:45
10 z 14 -	Przerwa	-	04-10-2026	12:00	13:00	01:00
11 z 14 MODUŁ VII: Prywatność, komunikacja i bezpieczeństwo w organizacji.	Zajęcia	Kamil Urbacz	04-10-2026	13:00	14:15	01:15
12 z 14 MODUŁ VIII: Prawo, procedury i green IT w cyberbezpieczeństwie.	Zajęcia	Kamil Urbacz	04-10-2026	14:15	15:30	01:15
13 z 14 Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.	Zajęcia	Kamil Urbacz	04-10-2026	15:30	15:45	00:15
14 z 14 -	Walidacja	-	04-10-2026	15:45	16:30	00:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00

Rodzaj godzin	Liczba godzin
w tym suma godzin zajęć	13:15
w tym suma godzin walidacji	00:45
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

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	6 081,12 PLN
Koszt przypadający na 1 uczestnika netto	4 944,00 PLN
Koszt osobogodziny brutto	380,07 PLN
Koszt osobogodziny netto	309,00 PLN
W tym koszt walidacji brutto	100,00 PLN
W tym koszt walidacji netto	81,30 PLN
W tym koszt certyfikowania brutto	150,00 PLN
W tym koszt certyfikowania netto	121,95 PLN

Liczba godzin usługi

Prowadzący

Liczba prowadzących: 1



1 z 1

Kamil Urbacz

Informatyk, projektant energooszczędnych stron internetowych, ekspert w dziedzinie green marketingu oraz doświadczony trener z wieloletnią praktyką w dziedzinie technologii cyfrowych. Od 2017 roku nieustannie zdobywa doświadczenie w programowaniu i projektowaniu stron i aplikacji webowych (m.in. HTML, Python, WordPress, CSS, Java).

Jako ekspert specjalizuje się w obszarach: generatywnej sztucznej inteligencji i projektowaniu stron internetowych zgodnych z zasadami no-code. Kładzie nacisk na przekazywanie praktycznych umiejętności, dzięki czemu uczestnicy zdobywają wiedzę gotową do natychmiastowego wdrożenia, co stanowi realne wsparcie w ich rozwoju zawodowym.

Doświadczenie zawodowe lub kwalifikacje zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia usługi: m.in.: PARP - Komunikacja marketingowa (2021), PARP - Cyberbezpieczeństwo w MŚP (2021), Google - Podstawy marketingu internetowego (2021), IT & Desktop Computer Support (2021), Google - Foundations of User Experience (UX) Design (2021), Google - Crash Course of Python (2022), Google - Technical Support Fundamentals (2022), Poznaj AI - Praktyka, narzędzia, ciekawostki (2025), Oracle Certified Associate Java Programmer (2025), Climate Change: From Learning to Action (UN-CC Learn, 2025), How to prevent e-waste? (UN-CC Learn, 2025), Gemini Certified Educator (2025), Google & SGH: Wykorzystanie AI w rozwoju firmy (2025).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy Uczestnik otrzyma **konspekt z materiałami w wersji drukowanej**, który zdecydowanie ułatwia pracę podczas szkolenia, a także posłuży utrwaleniu wiadomości po odbytych szkoleniu. Zapewniamy także notesy i długopisy. Dla chętnych udostępniamy również konspekt w wersji cyfrowej.

Informacje dodatkowe

Kontakt do osoby prowadzącej usługę: kamil.urbacz@simply.edu.pl

Uprzejmie prosimy uczestników **o zabranie ze sobą laptopa**. W przypadku braku dostępu do wymienionego sprzętu lub niemożności jego zabrania na szkolenie, **prosimy o wcześniejsze poinformowanie Dostawcy Usługi**. Dostawca ma możliwość zapewnienia sprzętu dla każdego Uczestnika.

Możliwość zwolnienia z VAT na podstawie: Dz.U. 2013 poz. 1722 (Rozporządzenie Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień) §3, ust. 1, pkt 14.

Adres

ul. Henryka Jordana 18

40-043 Katowice

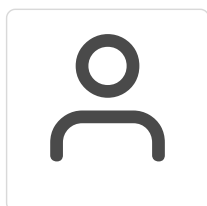
woj. śląskie

Centrum Konferencyjne "Jordana18", budynek Instytutu/Wydziału Nauk Teologicznych Uniwersytetu Śląskiego

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt



Maria Szymak

E-mail maria.szymak@simply.edu.pl

Telefon (+48) 721 324 130