



## Kompetencje cyfrowe w pracy: analiza danych, AI i cyberbezpieczeństwo w praktyce

Numer usługi 2026/04/08/158240/3470442

6 300,00 PLN brutto  
6 300,00 PLN netto  
116,67 PLN brutto/h  
116,67 PLN netto/h  
261,33 PLN cena rynkowa ⓘ

Szkolenia i Rozwój  
Ewelina Zięcina

★★★★★ 5,0 / 5

19 ocen

📄 Usługa szkoleniowa

📺 zdalna w czasie rzeczywistym

🕒 54:00 h

📅 29.05.2026 do 07.06.2026

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Grupa docelowa usługi

Szkolenie w głównym stopniu kierowane jest do pracowników oraz przedsiębiorców, którzy pracują lub chcą podjąć prace w obszarze analizy danych, chcących zwiększyć swoją efektywność zawodową lub potrzebujących usystematyzować posiadaną do tej pory wiedzę.

Kierowane jest również do osób narażonych na cyberzagrożenia, a także wszystkich osób zainteresowane poruszaną tematyką.

Usługa adresowana również dla Uczestników projektu **Kierunek – Rozwój**

### Minimalna liczba uczestników

2

### Maksymalna liczba uczestników

12

### Data zakończenia rekrutacji

28-05-2026

### Forma prowadzenia usługi

zdalna w czasie rzeczywistym

### Liczba godzin usługi

54

### 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

Szkolenie przygotowuje do pracy w szybko zmieniających się realiach cyfrowego świata. Uczestnik pozna metody efektywnej pracy z danymi, metody jej usprawniania i automatyzacji. Pozna również zróżnicowane źródła zagrożeń ataków cyfrowych i będzie potrafił samodzielnie je identyfikować, co przyczyni się do podniesienia świadomości pracowników w firmie, tym samym skutecznie podnosząc jej bezpieczeństwo.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>Posługuje się wiedzą z dziedziny cybersecuritiy:</p>	<p>Charakteryzuje potencjalne źródła ataków cyfrowych w firmie (zagrożenia).            Charakteryzuje podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości.            Charakteryzuje normy: ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania; ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa -Wymagania; oraz ISO/IEC 27005, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem bezpieczeństwa informacji.</p>	<p>Test teoretyczny</p>
<p>Posługuje się wiedzą z dziedziny cybersecurity:</p>	<p>Charakteryzuje podstawowe różnice pomiędzy modelem zabezpieczeń oprogramowania typu open-source i closedsource.            Charakteryzowania podstaw zagadnień dotyczące zagrożeń cyberbezpieczeństwa wynikających ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych.</p>	<p>Test teoretyczny</p>
<p>Umiejętności: stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji.</p>	<p>Zapewnia ciągłość działania organizacji w procesie transformacji cyfrowej.            Szacuje ryzyko w odniesieniu do poszczególnych aktywów informatycznych firmy i wpływ wystąpienia potencjalnych ryzyk na działanie firmy.            Współpracuje ze specjalistami ds. cyberbezpieczeństwa danych i systemów w zakresie projektów realizowanych w transformacji cyfrowej firmy.</p>	<p>Test teoretyczny</p>

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności: stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji.	<p>Wdraża odpowiednie procedury bezpieczeństwa.</p> <p>Identyfikuje niezbędne akty prawne, dokumenty i zapisy w nich zawarte, określające podstawy bezpieczeństwa cyfrowego w firmie.</p> <p>Zachęca pracowników do przestrzegania zasad cyberbezpieczeństwa</p>	Wywiad swobodny
Stosuje nowo nabyte kompetencje społeczne	<p>Komunikuje się efektywnie ze specjalistami ds. cyberbezpieczeństwa.</p> <p>Przekonuje współpracowników i interesariuszy do własnego zdania</p>	Obserwacja w warunkach rzeczywistych

## 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

1. Podstawy pracy z danymi: rodzaje i źródła danych, przygotowanie i porządkowanie danych, wprowadzenie do analizy danych
2. Excel w praktyce: formuły i funkcje, filtrowanie i sortowanie danych, tabele przestawne, tworzenie raportów i zestawień.
3. Wizualizacja i interpretacja danych: tworzenie wykresów, prezentowanie danych w sposób czytelny, wyciąganie wniosków i podejmowanie decyzji.
4. Automatyzacja pracy: usprawnianie codziennych zadań, wykorzystanie funkcji automatyzujących w Excelu, organizacja pracy z danymi
5. Wykorzystanie AI w pracy: zastosowanie narzędzi takich, jak chatGPT
6. Podstawowe definicje w zakresie cybersecurity.
7. Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji.

8. Sposoby ochrony, metody rozpoznawania incydentów, monitoring, reagowanie.
9. Źródła ataków cyfrowych.
10. Zasada działania ransomware, sposoby ochrony - praktyczne przykłady w tym ćwiczenia.
11. Szyfrowanie poczty oraz danych wrażliwych, tworzenie szyfrowanych magazynów danych, metody bezpiecznej wymiany danych.
12. Jak poprawnie tworzyć bezpieczne hasła oraz jak korzystać z tzw. menadżerów haseł, mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F.
13. Czym jest phishing, w jaki sposób poprawnie rozpoznać próbę oszustwa, wyłudzenia danych w tym danych autoryzacyjnych.
14. Zasady dotyczące bezpieczeństwa wysyłanych danych oraz ich przechowywania.

## Harmonogram

Liczba pozycji harmonogramu: 0

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

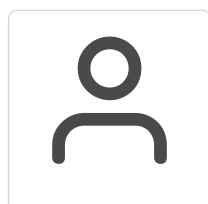
## Cennik

### Cennik

Rodzaj ceny	Cena
<b>Koszt przypadający na 1 uczestnika brutto</b>	6 300,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
<b>Koszt przypadający na 1 uczestnika netto</b>	6 300,00 PLN
<b>Koszt osobogodziny brutto</b>	116,67 PLN
<b>Koszt osobogodziny netto</b>	116,67 PLN

## Prowadzący

Liczba prowadzących: 2



1 z 2

### Kamila Borowicka

Zdobywane od 2019 nieprzerwanie doświadczenie w działalności szkoleniowej, w tym procesach walidacji efektów kształcenia. Wykształcenie wyższe na kierunku filologia angielska i niemiecka, znajomość metodologii procesów oraz metod walidacji.

Kwalifikacje nabyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.



2 z 2

## EWELINA ZIĘCINA

Posiada wykształcenie wyższe kierunkowe (prawo i administracja) oraz techniczne.  
Od 2016r nieprzerwane doświadczenie w prowadzeniu usług szkoleniowych oraz pracy z klientem.  
Ukończone certyfikowane szkolenia Microsoft, doświadczenie w dziedzinie cybersecurity.  
W ciągu ostatnich 2 lat przeprowadziła ponad 200 godzin usług szkoleniowych.

Kwalifikacje nabyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma niezbędne skrypty oraz materiały szkoleniowe.

Wszelkie niezbędne materiały zapewnia Organizator.

### Informacje dodatkowe

Usługa realizowana jest w godzinach dydaktycznych (1h dydaktyczna = 45min)

Usługa obejmuje 54h dydaktycznych.

Podczas jej realizacji zapewniony jest dobrostan uczestników poprzez zaplanowane przerwy, natomiast czas przerw nie jest wliczany do czasu usługi.

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

## Warunki techniczne

Usługa będzie realizowana przy użyciu Microsoft Teams.

Minimalne wymagania sprzętowe dla uczestników:

Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy)

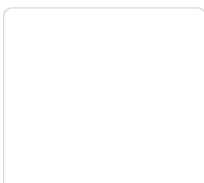
2GB pamięci RAM (zalecane 4GB lub więcej)

System operacyjny taki jak Windows 11, Mac OS (zalecana najnowsza wersja), Linux,

Chrome OS.

Niezbędne oprogramowanie - przeglądarka internetowa. Polecamy szczególnie przeglądarki Chrome, Opera, Firefox.

## Kontakt



EWELINA ZIĘCINA

**E-mail** ew.ziecina@o2.pl



**Telefon** (+48) 790 838 434