



Szkolenia i Rozwój
Ewelina Zięcina



Cyberbezpieczeństwo organizacji - Kierunek Rozwój

Numer usługi 2025/04/01/158240/2663286

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 28 h

📅 01.05.2025 do 03.05.2025

3 300,00 PLN brutto

3 300,00 PLN netto

117,86 PLN brutto/h

117,86 PLN netto/h

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	<p>Uczestnicy projektu Kierunek Kariera</p> <p>Przedsiębiorcy i pracownicy przedsiębiorstw wykorzystujący lub zamierzający wykorzystywać narzędzia internetowe (szczególnie social media) w pracy i kreowaniu wizerunku firmy.</p> <p>Szkolenie w głównym stopniu kierowane jest do pracowników oraz przedsiębiorców którzy posiadają mniejszą świadomość możliwości i zagrożeń płynących z publikowanych informacji, nie mają też wiedzy o zachodzących relacjach między profilami prywatnymi, a firmowymi.</p> <p>Wszystkie osoby zainteresowane poruszaną tematyką.</p> <p>Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój</p>
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	30-04-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28
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 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
Posługuje się wiedzą z dziedziny cybersecurity:	<p>Charakteryzuje potencjalne źródła ataków cyfrowych w firmie (zagrożenia).</p> <p>Charakteryzuje podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości.</p> <p>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>	Test teoretyczny
Posługuje się wiedzą z dziedziny cybersecurity:	<p>Charakteryzuje podstawowe różnice pomiędzy modelem zabezpieczeń oprogramowania typu open-source i closedsource.</p> <p>Charakteryzowania podstaw zagadnień dotyczące zagrożeń cyberbezpieczeństwa wynikających ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych.</p> <p>Zapewnia ciągłość działania organizacji w procesie transformacji cyfrowej.</p>	Test teoretyczny
Umiejętności: stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji.	<p>Szacuje ryzyko w odniesieniu do poszczególnych aktywów informatycznych firmy i wpływ wystąpienia potencjalnych ryzyk na działanie firmy.</p> <p>Współpracuje ze specjalistami ds. cyberbezpieczeństwa danych i systemów w zakresie projektów realizowanych w transformacji cyfrowej firmy.</p>	Test teoretyczny

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 symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

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

Dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielanie procesów kształcenia i szkolenia od walidacji.

Program

1. Podstawowe definicje w zakresie cybersecurity.
2. Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji.
3. Sposoby ochrony, metody rozpoznawania incydentów, monitoring, reagowanie.
4. Źródła ataków cyfrowych.
5. Zasada działania ransomware, sposoby ochrony - praktyczne przykłady w tym ćwiczenia.
6. Szyfrowanie poczty oraz danych wrażliwych, tworzenie szyfrowanych magazynów danych, metody bezpiecznej wymiany danych.
7. Jak poprawnie tworzyć bezpieczne hasła oraz jak korzystać z tzw. menadżerów haseł, mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F.

8. Czym jest phishing, w jaki sposób poprawnie rozpoznać próbę oszustwa, wyłudzenia danych w tym danych autoryzacyjnych.

9. Zasady dotyczące bezpieczeństwa wysyłanych danych oraz ich przechowywania.

Harmonogram

Liczba przedmiotów/zajęć: 26

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 Moduł I - wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	01-05-2025	08:00	09:30	01:30
2 z 26 Przerwa	EWELINA ZIĘCINA	01-05-2025	09:30	09:45	00:15
3 z 26 Moduł I - wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	01-05-2025	09:45	11:15	01:30
4 z 26 Przerwa	EWELINA ZIĘCINA	01-05-2025	11:15	11:30	00:15
5 z 26 Moduł I - warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	EWELINA ZIĘCINA	01-05-2025	11:30	13:00	01:30
6 z 26 Przerwa	EWELINA ZIĘCINA	01-05-2025	13:00	13:30	00:30
7 z 26 Moduł II - wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	01-05-2025	13:30	15:00	01:30
8 z 26 Przerwa	EWELINA ZIĘCINA	01-05-2025	15:00	15:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 26 Moduł II-warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	EWELINA ZIĘCINA	01-05-2025	15:15	16:45	01:30
10 z 26 Moduł III - wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	02-05-2025	08:00	09:30	01:30
11 z 26 Przerwa	EWELINA ZIĘCINA	02-05-2025	09:30	09:45	00:15
12 z 26 Moduł III wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	02-05-2025	09:45	11:15	01:30
13 z 26 Przerwa	EWELINA ZIĘCINA	02-05-2025	11:15	11:30	00:15
14 z 26 Moduł III wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	02-05-2025	11:30	13:00	01:30
15 z 26 Przerwa	EWELINA ZIĘCINA	02-05-2025	13:00	13:30	00:30
16 z 26 Moduł III-warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	EWELINA ZIĘCINA	02-05-2025	13:30	15:00	01:30
17 z 26 Przerwa	EWELINA ZIĘCINA	02-05-2025	15:00	15:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 26 Moduł III-warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	EWELINA ZIĘCINA	02-05-2025	15:15	16:00	00:45
19 z 26 Moduł IV wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	03-05-2025	08:00	09:30	01:30
20 z 26 Przerwa	EWELINA ZIĘCINA	03-05-2025	09:30	09:45	00:15
21 z 26 Moduł IV-warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	EWELINA ZIĘCINA	03-05-2025	09:45	11:15	01:30
22 z 26 Przerwa	EWELINA ZIĘCINA	03-05-2025	11:15	11:30	00:15
23 z 26 Moduł V wykład (prezentacja, czat, rozmowa na żywo)	EWELINA ZIĘCINA	03-05-2025	11:30	13:00	01:30
24 z 26 Przerwa	EWELINA ZIĘCINA	03-05-2025	13:00	13:30	00:30
25 z 26 Moduł V-warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	EWELINA ZIĘCINA	03-05-2025	13:30	15:15	01:45
26 z 26 Walidacja	-	03-05-2025	15:15	15:45	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 300,00 PLN
Koszt przypadający na 1 uczestnika netto	3 300,00 PLN
Koszt osobogodziny brutto	117,86 PLN
Koszt osobogodziny netto	117,86 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

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

Wszelkie niezbędne materiały zapewnia Organizator.

Informacje dodatkowe

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

Usługa obejmuje 28h 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 **ProjektuKierunek – 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 10, 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) 514 426 116